WWW.INFOPULSAS.LT / info@infopulsas.lt

×

SHROOM



UR32&UR35 User Guide

Xiamen Ursalink Technology Co., Ltd.





www.ursalink.com

Preface

Thanks for choosing Ursalink UR32&UR35 industrial cellular router. The UR32&UR35 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 UR32&UR35 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

© 2017 Xiamen Ursalink Technology 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 Ursalink Technology Co., Ltd.

Products Covered

This guide explains how to configure the following devices:

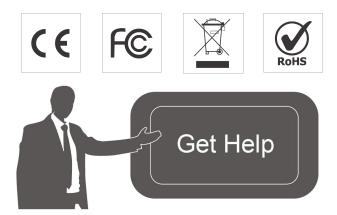
- Ursalink UR32 Industrial Cellular Router
- Ursalink UR35 Industrial Cellular Router

Related Documents

Document	Description
Ursalink UR32 Datasheet	Datasheet for the Ursalink UR32 industrial cellular router.
Ursalink UR35 Datasheet	Datasheet for the Ursalink UR35 industrial cellular router.
Ursalink UR32 Quick Start Guide	Quick Installation guide for the Ursalink UR32 series industrial cellular router.
Ursalink UR35 Quick Start Guide	Quick Installation guide for the Ursalink UR35 series industrial cellular router.

Declaration of Conformity

UR32/UR35 is in conformity with the essential requirements and other relevant provisions of the CE, FCC, and RoHS.



For assistance, please contact Ursalink technical support: Email: support@ursalink.com Tel.: 86-592-5023060 Fax: 86-592-5023065

Revision History

Date	Doc Version	Description
May. 16, 2019	V.1.0.0	UR32 Initial version
July 19, 2019	V.1.1.0	UR32&UR35 Initial version

Contents

Chapter 1 Product Introduction	
1.1 Overview	8
1.2 Advantages	8
1.3 Specifications	9
1.4 Dimensions (mm)	12
Chapter 2 Access to Web GUI	13
2.1 PC Configuration for Web GUI Access to Router	13
2.2 Access to Web GUI of Router	
Chapter 3 Web Configuration	16
3.1 Status	16
3.1.1 Overview	16
3.1.2 Cellular	
3.1.3 Network	
3.1.4 WLAN (Only Applicable to Wi-Fi Version)	
3.1.5 VPN	20
3.1.6 Routing Information	21
3.1.7 Host List	
3.1.8 GPS (Only Applicable to GPS Version)	23
3.2 Network	24
3.2.1 Interface	
3.2.1.1 Port	24
3.2.1.2 WAN	
3.2.1.3 Bridge	
3.2.1.4 Switch	
3.2.1.5 WLAN (Only Applicable to Wi-Fi Version)	
3.2.1.6 Cellular	
3.2.1.7 Loopback	
3.2.2 Firewall	
3.2.2.1 Security	
3.2.2.2 ACL	
3.2.2.3 DMZ	
3.2.2.4 Port Mapping	
3.2.2.5 MAC Binding	
3.2.2.6 SPI	
3.2.3 QoS	
3.2.4 DHCP	45
3.2.4.1 DHCP Server	
3.2.4.2 DHCP Relay	
3.2.5 DDNS	
3.2.6 Link Failover	
3.2.6.1 SLA	
3.2.6.2 Track	

3.2.6.3 VRRP	50
3.2.6.4 WAN Failover	51
3.2.7 Routing	
3.2.7.1 Static Routing	52
3.2.7.2 RIP	
3.2.7.3 OSPF	
3.2.7.4 Routing Filtering	
3.2.8 VPN	62
3.2.8.1 DMVPN	63
3.2.8.2 IPSec Server	
3.2.8.3 IPSec	67
3.2.8.4 GRE	69
3.2.8.5 L2TP	70
3.2.8.6 PPTP	
3.2.8.7 OpenVPN Client	75
3.2.8.8 OpenVPN Server	76
3.2.8.9 Certifications	
3.3 System	
3.3.1 General Settings	81
3.3.1.1 General	81
3.3.1.2 System Time	82
3.3.1.3 SMTP	
3.3.1.4 Phone	
3.3.1.5 Email	85
3.3.1.6 Storage	
3.3.2 User Management	87
3.3.2.1 Account	
3.3.2.2 User Management	
3.3.3 SNMP	
3.3.3.1 SNMP	
3.3.3.2 MIB View	
3.3.3.3 VACM	90
3.3.3.4 Trap	
3.3.3.5 MIB	
3.3.4 AAA	
3.3.4.1 Radius	92
3.3.4.2 TACACS+	
3.3.4.3 LDAP	
3.3.4.4 Authentication	94
3.3.5 Device Management	
3.3.5.1 DeviceHub	95
3.3.5.2 Ursalink VPN	
3.3.6 Events	
3.3.6.1 Events	

3.3.6.2 Events Settings	
3.4 Industrial Interface	100
3.4.1 I/O	100
3.4.1.1 DI	
3.4.1.2 DO	101
3.4.2 Serial Port	
3.4.3 Modbus TCP	
3.4.3.1 Modbus TCP	
3.4.3.2 Modbus RTU	106
3.4.3.3 Modbus RTU Over TCP	
3.4.4 Modbus Master	108
3.4.4.1 Modbus Master	
3.4.4.2 Channel	
3.4.5 GPS (Only Applicable to GPS Version)	
3.4.5.1 GPS	
3.4.5.2 GPS IP Forwarding	
3.4.5.3 GPS Serial Forwarding	
3.5 Maintenance	
3.5.1 Tools	115
3.5.1.1 Ping	
3.5.1.2 Traceroute	
3.5.1.3 Packet Analyzer	116
3.5.2 Schedule	
3.5.3 Log	117
3.5.3.1 System Log	
3.5.3.2 Log Settings	
3.5.4 Upgrade	
3.5.5 Backup and Restore	
3.5.6 Reboot	
Chapter 4 Application Examples	123
4.1 Restore Factory Defaults	123
4.1.1 Via Web Interface	
4.2.2 Via Hardware	
4.2 Firmware Upgrade	
4.3 Events Application Example	
4.4 Logs and Diagnostics	
4.5 SNMP Application Example	
4.6 Network Connection	
4.6.1 Cellular Connection	132
4.6.2 Ethernet WAN Connection	134
4.7 WAN Failover/Backup Application Example	136
4.7.1 Dual SIM Backup	
4.7.2 WAN Failover	139
4.8 Wi-Fi Application Example (Only Applicable to Wi-Fi Version)	

4.8.1 AP Mode	143
4.8.2 Client Mode	144
4.9 VRRP Application Example	145
4.10 NAT Application Example	
4.11 Access Control Application Example	151
4.12 QoS Application Example	
4.13 DTU Application Example	154
4.14 PPTP Application Example	157

Chapter 1 Product Introduction

1.1 Overview

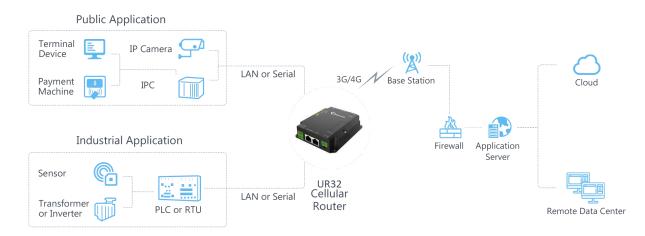
Ursalink UR32/UR35 is an industrial cellular router with embedded intelligent software features that are designed for multifarious M2M/IoT applications. Supporting global WCDMA and 4G LTE, UR32/UR35 provides drop-in connectivity for operators and makes a giant leap in maximizing uptime.

Adopting high-performance and low-power consumption industrial grade CPU and wireless module, the UR32/UR35 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.

Meanwhile, the UR32/UR35 also supports Fast Ethernet ports, serial port (RS232/RS485) and I/O (input/output), which enables you to scale up M2M application combining data and video in limited time and budget.

The UR32/UR35 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 UR32&UR35 Quick Start Guide.





1.2 Advantages

Benefits

- Built-in industrial strong CPU, big memory
- Fast Ethernet is applied to all models of Ursalink routers for lightning transmission of data
- Dual SIM cards for backup between multiple carriers networking and global 2G/3G/LTE options make it easy to get connected
- Flexible modular design provides users with different connection modules like Ethernet, I/O, serial port, Wi-Fi, GPS for connecting diverse field assets
- Rugged enclosure, optimized for DIN rail or shelf mounting
- 3-year warranty included

Security & Reliability

- Automated failover/failback between Ethernet and Cellular (dual SIM)
- Enable unit with security frameworks like IPsec/OpenVPN/GRE/L2TP/PPTP/ DMVPN
- Embed hardware watchdog, able to automatically recover from various failure, ensure 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

- Ursalink 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

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 with 128 MB memory available to support more applications
- Support rich protocols like SNMP, Modbus bridging, RIP, OSPF
- Support wide operating temperature ranging from -40°C to 70°C/-40°F to 158°F

1.3 Specifications

Hardware System		
CPU	528MHz, 32-bit ARM Cortex-A7	
Memory	128 MB Flash, 128 MB DDR3 RAM	
Storage	1 × Micro SD	
Cellular Interfaces		
Connectors	$2 \times 50 \Omega$ SMA (Center pin: female)	
SIM Slots	2	
Wi-Fi Interface (Optional)		
Connectors	$1 \times 50 \Omega$ SMA (Center pin: male)	

	IEEE 802.11 b/g/n
Tx Power	802.11b: 16 dBm +/-1.5 dBm (11 Mbps)
	802.11g: 14 dBm +/-1.5 dBm (54 Mbps)
	802.11n: 13 dBm +/-1.5 dBm (65 Mbps, HT20/40 MCS7)
Modes	Support AP and Client mode
Security	WPA/WPA2 authentication, WEP/TKIP/AES encryption
GPS (Optional)	
Connectors	$1 \times 50 \Omega$ SMA (Center pin: female)
Protocols	NMEA 0183, PMTK
Ethernet	
Ports	UR32: 2 × RJ-45 (PoE PSE Optional)
	UR35: 5 × 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)
Serial Interface	
Ports	UR32: 1 × RS232
	UR35: 1 × RS232 + 1 × RS485
Connector	Terminal block
Baud Rate	300bps to 230400bps
10	
Connector	Terminal block
Digital	$1 \times DI + 1 \times DO$
Software	
Software Network Protocols	PPP, PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS,
	PPP, PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QoS, SNTP, Telnet, VLAN, SSH, etc.
Network Protocols	VRRP, HTTP, HTTPS, DNS, ARP, QoS, SNTP, Telnet, VLAN, SSH, etc.
Network Protocols VPN Tunnel	VRRP, HTTP, HTTPS, DNS, ARP, QoS, SNTP, Telnet, VLAN, SSH, etc. DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE
Network Protocols VPN Tunnel Access Authentication	VRRP, HTTP, HTTPS, DNS, ARP, QoS, SNTP, Telnet, VLAN, SSH, etc. DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE CHAP/PAP/MS-CHAP/MS-CHAPV2
Network Protocols VPN Tunnel Access Authentication Firewall	VRRP, HTTP, HTTPS, DNS, ARP, QoS, SNTP, Telnet, VLAN, SSH, etc. DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE CHAP/PAP/MS-CHAP/MS-CHAPV2 ACL/DMZ/Port Mapping/MAC Binding/SPI/DoS&DDoS Protection
Network Protocols VPN Tunnel Access Authentication Firewall Management	VRRP, HTTP, HTTPS, DNS, ARP, QoS, SNTP, Telnet, VLAN, SSH, etc. DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE CHAP/PAP/MS-CHAP/MS-CHAPV2 ACL/DMZ/Port Mapping/MAC Binding/SPI/DoS&DDoS Protection Web, CLI, SMS, On-demand dial up, DeviceHub

Serial Port	Transparent (TCP Client/Server, UDP), Modbus Gateway (Modbus RTU to Modbus TCP)
Power Supply and Consump	tion
Connector	2-pin with 5.08 mm terminal block
Input Voltage	9-48 VDC
Power Consumption	UR32: Typical 1.9 W, Max 2.4 W
	UR35: Typical 3.9 W, Max 4.6 W
Power Output	UR32: 2 × 802.3 af/at PoE output
	UR35: 4 × 802.3 af/at PoE output
Physical Characteristics	
Ingress Protection	IP30
Housing & Weight	UR32: Metal, 271g
	UR35: Metal, 485g
Dimensions	UR32: 108 x 90 x 26 mm (4.25 x 3.54 x 1.02 in)
	UR35: 135 x 100 x 45 mm (5.31 x 4.06 x 1.77 in)
Mounting	Desktop, wall or DIN rail mounting
Others	
Reset Button	1 × RESET
LED Indicators	UR32: 1 × POWER, 1 × SYSTEM, 1 × SIM, 3 × Signal strength
	UR35: 1 × POWER, 1 × SYSTEM, 1 × SIM, 1 × Wi-Fi, 1 × VPN, 3 × Signal
	strength
Built-in	Watchdog, Timer
Certifications	RoHS, CE, FCC
Environmental	
Operating Temperature	-40°C to +70°C (-40°F to +158°F)
	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)

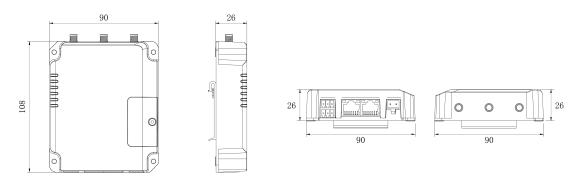


Figure 1-2

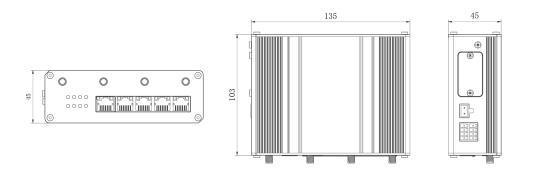


Figure 1-3

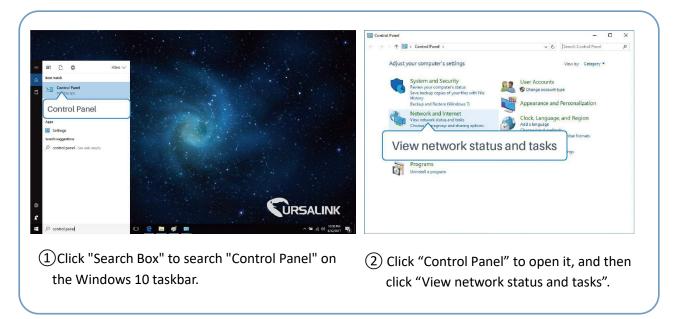
Chapter 2 Access to Web GUI

This chapter explains how to access to Web GUI of the UR32/UR35 router.

2.1 PC Configuration for Web GUI Access to Router

Please connect PC to LAN port of UR32/UR35 router directly. PC can obtain an IP address, or you can configure a static IP address manually.

The following steps are based on Windows 10 operating system for your reference.



	– 🗆 X	Ethernet Status	×
and Internet > Network and Sharing Center	✓ ຽ Search Control Panel ,		
View your basic network information an	d set up connections	General	
View your active networks		Connection	
No. 10	Access type: Internet	IPv4 Connectivity: No network acces	s
Private network	HomeGroup: Ready to create	IPv6 Connectivity: No network acces	s
	Connections: Wi-Fi (Yeastar5G)	Media State: Enable	ed b
	Lange and the second se	Duration: 00:01:2	1
Identifying		Speed: 1.0 Gbp	os
		Details .	
Change your petworking settings		Details	
	Ethermore		
	tion: Etnernet	A	
The block of webber		Activity	
	get troubleshooting information.	t Receive	d
		Properties	
			0
		Properties Diagnose Diagnose	
			1
		Clo	se
	View your active networks Yeastar3G Private network Identifying Change your networking settings Set up a new somection er network Set up a trasbard (ai)-up, or VPN conne ToubleShoot problems	and Internet > Network and Sharing Center v © Search Centrol Panel p View your basic network information and set up connections View your active network View your active network View your active network View your active network View your active network Provatar3G Private network No retwork access Connections @ Ethernet Change your networking settings Set up a broadband, dial-up, or VPN connections	and Internet 3 Metwork and Sharing Center View your basic network information and set up connections View your active network No network access Connection: Access type Internet Connection: Wief (Vestar5G) Access type Internet Connection: Mentifying_ Access type Internet Connection: Connection:

Ethernet Properties ×	Internet Protocol Version 4 (TCP/IPv4) Properties	Internet Protocol Version 4 (TCP/IPv4) Properties
Networking Sharing	General Alternate Configuration	General
Connect using:	You can get IP settings assigned automatically if your network supports	You can get IP settings assigned 192.168.1.20 ts
Configure	this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.	for the appropriate IP settings. 255.255.255.0
This connection uses the following items:	Obtain an IP address automatically	Obtain an ℙaddress autor 192.168.1.1
Elient for Microsoft Networks	OUse the following IP address:	Use the following IP address:
File and Printer Sharing for Microsoft Networks GoS Packet Scheduler	IP address:	IP address: 192 . 168 . 1 . 20
✓ Internet Protocol Version 4 (TCP/IPv4)	Subnet mask:	Subnet mask: 255 . 255 . 255 . 0
Microsoft Net Adapter Multiplexor Protocol	Default gateway:	Default gateway: 192 . 158 . 1 . 1
Internet Protocol Version 4 (TCP/IPv4)	Obtain DNS server address automatically	Obtain DNS server address automatically
	O Use the following DNS server addresses:	Use the following DNS server addresses:
Install Uninstall Properties	Preferred DNS server:	Preferred DNS server: 192.168.1.1
Description	Alternate DNS server:	Alternate DNS server:
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks		192,168, 1,1
across diverse interconnected networks.	Validate settings upon exit Advanced	Validate settings upon exit
OK Cancel	OK Cancel	OK Cancel
Double Click "Internet		Mathad 2: click "Lica the following
) Double Click "Internet	(6) Method 1: click "Obtain an IP	Method 2: click "Use the following
Protocol Version 4 (TCP/IPv4)	' address automatically";	IP address" to assign a static IP
		0
to configure IP address and		manually within the same subnet of
DNS server.		the router.

(Note: remember to click "OK" to finish configuration.)

2.2 Access to Web GUI of Router

Ursalink router provides Web-based configuration interface for management. If this is the first time you configure the router, please use the default settings below.

Username: admin Password: password

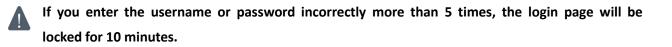
IP Address: 192.168.1.1

DHCP Server: Enabled

- 1. Start a Web browser on your PC (Chrome and IE are recommended), type in the IP address, and press Enter on your keyboard.
- 2. Enter the username, password, and click "Login".

(C)	INK X	
	Lusemame	
	Password	
	Login	

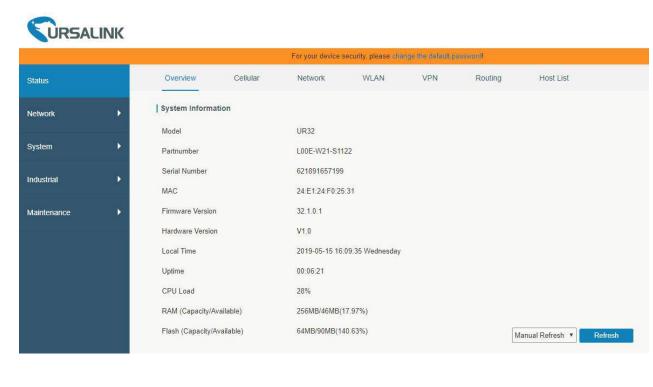
If the SIM card is connected to cellular network with public IP address, you can access WEB GUI remotely via the public IP address when remote access is enabled.



3. 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.

Chang	ge Password	
Old Password		
New Password		
Confirm New Password		
	2-	
	0-	
Save	Cancel	

4. 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.

URSAL	.INK				
				For your device	security, please change
Status		Overview	Cellular	Network	WLAN
Network	Þ	System Informa	tion		
		Model		UR32	
System	•	Partnumber		L00E-W21-S11	122
Industrial		Serial Number		621891657199)
masanar		MAC		24:E1:24:F0:25	5:31
Maintenance	×	Firmware Version		32.1.0.1	
		Hardware Version	į	V1.0	
		Local Time		2019-05-15 16	:09:35 Wednesday
		Uptime		00:06:21	
		CPU Load		28%	
		RAM (Capacity/A	vailable)	256MB/46MB(17.97%)
		Flash (Capacity/A	vailable)	64MB/90MB(1-	40.63%)

Figure 3-1-1-1

System Information		
Item	Description	
Model	Show the model name of router.	
Part Number	Show the part number 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.	
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.	
RAM (Capacity/Available)	Show the RAM capacity and the available RAM memory.	
Flash (Capacity/Available)	Show the Flash capacity and the available Flash memory.	

Table 3-1-1-1 System Information

3.1.2 Cellular

Overview	Cellular	Network	VPN	Routing	Host List
Modem					
Status		Ready			
Model		EC25			
Current SIM		SIM1			
Signal Level		15asu (-83dBm)		
Register Status		Registered (Ho	me network)		
IMSI		460019987103	071		
		898601 <mark>1</mark> 78380	19196629		
ISP		CHN-UNICOM			
Network Type		LTE			
PLMN ID		46001			
LAC		<mark>5922</mark>			
Cell ID		812c63d			
IMEI		861107031710	008		

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

Figure 3-1-2-1

Modem Information	Modem Information		
Item	Description		
Status	Show corresponding detection status of module and SIM card.		
Model	Show the model name of cellular module.		
Current SIM	Show the current SIM card used.		
Signal Level	Show the cellular signal level.		
Register Status	Show the registration status of SIM card.		
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.		
IMEI	Show the IMEI of the module.		

Table 3-1-2-1 Modem Information

Network		
Status	Connected	
IP Address	10.53.2 <mark>4</mark> 1.18	
Netmask	255.255.255.252	
Gateway	10.53.241.17	
DNS	218.104.128.106	
Connection Duration	0 days, 00:04:26	

Figure 3-1-2-2

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

Table 3-1-2-2 Network Status

3.1.3 Network

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

WAN-IPv4							
Port	Status	Туре	IP	Netmask	Gateway	DNS	Connection Duration
LAN1/WAN	up	Static	192.168.23.247	255.255.255.0	192.168.23.1	114.114. <mark>1</mark> 1 4.114	11h 07m 45s
WAN-IPv6							
Port	Status	Туре	IP	Prefix-length	Gateway	DNS	Connection Duration
LAN1/WAN	up	Static	fe80::26e1:24ff:fef0:257 9	64	i n t		11h 07m 45s



WAN Status	
Item	Description
Port	Show the name of WAN port.
Ctatura	Show the status of WAN port. "up" refers to a status that WAN is enabled and
Status	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.
IP Address	Show the IPv4 or IPv6 address of WAN port.
Netmask	Show the IPv4 netmask of WAN port.
Prefix-length	Show the IPv6 Prefix-length of WAN port.
Gateway	Show the gateway of WAN port.
DNS	Show the DNS of WAN port.
	Show the information on how long the Ethernet cable has been connected on
Connection Duration	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	IP	Netmask	Members	
Bridge0	Disabled	192.168.140.1	255 255 255 0	vlan 1,WLAN1	



Bridge		
Item	Description	
Name	Show the name of the bridge interface.	
STP	Show if STP is enabled.	
IP	Show the IP address 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 WLAN (Only Applicable to Wi-Fi Version)

You can check Wi-Fi status on this page, including the information of access point and client.

ALC: NOT THE REAL PROPERTY OF	C	40	0.010	15 4 1 1	
Name	Status	Туре	SSID	IP Address	Netmask
WLAN1	Running	AP	Ursalink_F0257A	192.168.140.1	255 255 255 0
sociated Statio	ns				
	D		Address	IP Address	Connection Duration

Figure 3-1-4-1

WLAN Status		
Item	Description	
WLAN Status		
Name	Show the name of the Wi-Fi interface .	

Status	Show the status of the Wi-Fi interface.
Туре	Show the Wi-Fi interface type.
SSID	Show the SSID of the router when the interface type is AP. Show the SSID of AP which the router connected to when the interface type is Client.
IP Address	Show the IP address of the router when the interface type is AP. Show the IP address of AP which the router connected to when the interface type is Client.
Netmask	Show the netmask of the router when the interface type is AP. Show the netmask of AP which the router connected to when the interface type is Client.
Associated Stations	
SSID	Show the SSID of the router when the interface type is AP. Show the SSID of AP which the router connected to when the interface type is Client.
MAC Address	Show the MAC address of the client which connected to the router when the interface type is AP. Show the MAC address of the AP which the router connected to when the interface type is Client.
IP Address	Show the IP address of the client which connected to the router when the interface type is AP. Show the IP address of the AP which the router connected to when the interface type is Client.
Connection Duration	Show the connection duration between client device and router when the interface type is AP. Show the connection duration between router and the AP when the interface type is Client.

Table 3-1-4-1 WLAN Status

3.1.5 VPN

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

Overview	Cellular	Network	WLAN	VPN	Routing	Host List
Clients						
	Name	Status		Local IP		Remote IP
Server						
	Nam	e			Status	
	OpenVPN	Server			Disabled	
	Ipsec Se	erver			Disabled	1
Connected List						
	Server Type		Client I	Р		Duration

Figure 3-1-5-1

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
Status	client is connected to the server. "Disconnected" means client
	is disconnected to the server.
Local IP	Show the local IP address of the tunnel.
Remote IP Show the real remote IP address of the tunnel.	
Server	
Name	Show the name of the enabled VPN Server.
Status Show the status of Server.	
Connected List	
Server Type	Show the type of the server.
Client IP	Show the IP address of the client which connected to the
Client IP	server.
	Show the information about how long the client has been
Duration	connected to this server when the server is enabled. Once the
Duration	server is disabled or connection is disconnected, the duration
	will stop counting.
	Table 2.1.5.1.VDN Status

Table 3-1-5-1 VPN Status

3.1.6 Routing Information

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

Overview	Cellular	Network	WLAN	VPN	Routing	Host List
Routing Tab	le					
	Destination	Netmask	Gatewa	у	Interface	Metric
	0.0.0	0.0.0.0	192.168.2	3.1	LAN1/WAN	đ
	8.8.8.8	255 255 255 255	192.168.2	3.1	LAN1/WAN	1
	114.114.114.114	255 255 255 255	192.168.2	3.1	LAN1/WAN	1
	127.0.0.0	255.0.0.0	(æ)		Loopback	
	192.168.1.0	255.255.255.0	~		WLAN1	54) (44)
	192.168.23.0	255.255.255.0	-		LAN1/WAN	-
	192.168.140.0	255.255.255.0	1220		Bridge0	8 <u>8</u> 0
ARP Cache						
	IP		MAC			Interface
	192.168.140.122		b0:e1:7e:10:2f:6e			Bridge0
	192.168. <mark>140.171</mark>		78:62:56:e5:43:2d			Bridge0

Figure 3-1-6-1

Item	Description		
Routing Table			
Destination	Show the IP address of destination host or destination network.		
Netmask	Show the netmask 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 3-1-6-1 Routing Information

3.1.7 Host List

You can view the host information on this page.

Overview	Cellular	Network	VPN	Routing	Host List	GPS
DHCP Leases						
	IP		MAC	R.	Lease	Remaining Time
MAC Binding						
	IF	2			MAC	

Figure 3-1-7-1

Host List				
Item	Description			
DHCP Leases				
IP Address Show IP address of DHCP client				
MAC Address	Show MAC address of DHCP client			
Lease Time Remaining	Show the remaining lease time of DHCP client.			
MAC Binding				
IP & MAC	Show the IP address and MAC address set in the Static IP list of DHCP service.			

Table 3-1-7-1 Host List Description

3.1.8 GPS (Only Applicable to GPS Version)

When GPS function is enabled and the GPS information is obtained successfully, you can view the latest

GPS information including GPS Time, Latitude, Longitude and Speed on this page.

Disabled	
	Disabled



GPS Status		
Item	Description	
Status	Show the status of GPS.	
Time for Locating	Show the time for locating.	
Latitude	Show the Latitude of the location.	

Longitude	Show the Longitude of the location.
Speed	Show the speed of movement.

Table 3-1-8-1 GPS Status Description

3.2 Network

3.2.1 Interface

3.2.1.1 Port

This section describes how to configure the Ethernet port parameters.

The UR32 cellular router supports 2 LAN ports and LAN1 can be configured as WAN port. The UR35 cellular router supports 1 WAN port and 4 LAN ports.

			For y	our device securit	y, please char	nge the de	fault passwo	rrsil		
Status	Port	WAN	Bridge	Switch	WLA	AN	Cellula	r	Loopback	
Vetwork 🗸	Port Settin	g								
		Port		Status	Propert	ty	Spee	d	Duple	ж
Interface		LAN1/WAN	u	p •	wan	•	auto	•	auto	•
Firewall		LAN2	U	p •	lan		auto	•	auto	



			Fr	nr your dev	rice security	r please cha	inge the d	stault passw	ordi		
Status	Port	WAN	Bridge		Switch	Ce	llular	Loopi	back		
Network	Port Setting	9									
		Port		Statu	15	Prope	rty	Spee	ed	Duple	x
Interface		WAN	[up	*	wan	¥	auto	•	auto	•
Firewall		LAN1	[up	•	lan	*	auto	٠	auto	۲
QoS		LAN2	[up	•	lan		auto	٠	auto	۲
DHCP		LAN3	[up	•	len		auto	•	auto	•
Unice		LAN4	1	up	•	lan		auto	•	auto	

Figure 3-2-1-2

Port Setting	
Item	Description
Port	Users can define the Ethernet ports according to their needs.
Status	Set the status of Ethernet port; select "up" to enable and "down" to disable.
Property	Set 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".

Duralay	Set the Ethernet port's mode. The options are "auto", "full", and
Duplex	"half".

Table 3-2-1-1 Port Parameters

3.2.1.2 WAN

WAN port can be connected with Ethernet cable to get Internet access. It supports 3 connection types.

- Static IP: configure IP address, netmask and gateway for Ethernet WAN interface.
- DHCP Client: configure Ethernet WAN interface as DHCP Client to obtain IP address automatically.
- **PPPoE**: configure Ethernet WAN interface as PPPoE Client.

URSALINK		
		For your device security, please change
Status	Port WAN	Bridge Switch WLAN
Network 🔻	— WAN_1	
Interface	Enable	
Firewall	Port	LAN1/WAN
r ii ewaii	Connection Type	Static IP 🔹
QoS	IPv4 Address	192.168.23.247
DHCP	Netmask	255.255.255.0
DDNS	IPv4 Gateway	192.168.23.1
Link Failover	IPv6 Address	fe80::26e1:24ff:fef0:2579
LINK Fallover	Prefix-length	64
Routing	IPv6 Gateway	
VPN	MTU	1500
System 🕨	Primary DNS	114.114.114
	Secondary DNS	8.8.8.8
Industrial	Enable NAT	

Figure 3-2-1-3

WAN Setting						
Item	Description	Default				
Enable	Enable WAN function	Enable				
Port	The port that is currently set as WAN port.					
Connection Type	Select from "Static IP", "DHCP Client" and "PPPoE".	Static IP				
MTU	Set the maximum transmission unit.	1500				

Primary DNS Server	Set the primary DNS.	Null
Secondary DNS Server	Set the secondary DNS.	Null
Enable NAT	Enable or disable NAT function. When enabled, a private IP can be translated to a public IP.	Enable

Table 3-2-1-2 WAN Parameters

1. Static IP Configuration

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

t	WAN	Bridge	Switch	WLAN	Cellular	Loopback
WAN_	1					
Enable	e					
Port		1	LAN1/WAN			
Conne	ection Type		Static IP			
IPv4 A	Address		192.168.23.247			
Netma	ask		255.255.255.0]		
IPv4 C	3ateway		192.168.23.1			
IPv6 A	\ddress	1	e80::26e1:24 <mark>ff.f</mark> ef0:25	579		
Prefix-	-length		54			
IPv6 C	3ateway					
MTU			1500			
Prima	ry DNS		114.11 <mark>4</mark> .114.114			
Secon	idary DNS	8	8.8.8.8]		
Enable	e NAT					
Multip	ole IP Address					
		IP Address			Netmask	Operati

Figure 3-2-1-4

Static IP	Static IP						
Item	Description	Default					
IPv4 Address	Set the IPv4 address which can access Internet. E.g. 192.168.1.2.	192.168.0.1					
Netmask	Set the Netmask for WAN port.	255.255.255.0					
lPv4 Gateway	Set the gateway for WAN port's IPv4 address.	192.168.0.2					
IPv6 Address	Set the IPv6 address which can access 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 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 3-2-1-3 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, user can select "DHCP client" mode to obtain IP address automatically.

			For you	ur device security, p	please change t	
Status	Port	WAN	Bridge	Switch	WLAN	
Network	- WAN_	1				
Interface	Enabl	е.	9			
Firewall	Port		LAN1/	WAN		
QoS	Conne	Connection Type		DHCP Client		
	MTU	MTU		1500		
DHCP	Use P	eer DNS				
DDNS	Prima	ry DNS	114.11	4.114.114		
Link Failover	Secor	dary DNS	8.8.8.8	1		
Routing	Enabl	e NAT				

Figure 3-2-1-5

			For you	ur device security, j	please change
Status	Port	WAN	Bridge	Switch	WLAN
Network 🔻	WAN Settin	gs			
Interface	- WAN_	1			
Firewall	Enable	3			
QoS	Port		LAN1/	WAN	
DHCP	Conne	ction Type	DHCF	Pv6 Client	•
DITCF	Reque	st IPv6-address	none		¥
DDNS	Reque	st IPv6-prefix of leng	gth 0-64		
Link Failover	MTU		1500		
Routing	Enable	NAT			

Figure 3-2-1-6

DHCP Client	
Item	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 3-2-1-4 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 original connection way. With PPPoE, remote access devices can get control of each user.

URSALINK					
			For yo	ur device security, (please change t
Status	Port	WAN	Bridge	Switch	WLAN
Network	- WAN_1				
Interface	Enable		2		
	Port		LAN1	WAN	
Firewall	Connee	ction Type	PPPo	ε	•
QoS	Userna	me			
DHCP	Passwe	ord			
DDNS	Link De	etection Interval(s	s) <u>60</u>		
Link Failover	Max Re	etries	0		
	MTU		1500		
Routing	Use Pe	er DNS			
VPN	Primary	DNS	114.1	14.114.114	
System 🕨	Second	lary DNS	8.8.8.	В	
	Enable	NAT			

Figure 3-2-1-7

PPPoE	
Item	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	Set the heartbeat interval for link detection. Range: 1-600.
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 3-2-1-5 PPOE Parameters

Related Configuration Example

Ethernet WAN Connection

3.2.1.3 Bridge

Bridge setting is used for managing local area network devices which are connected to LAN ports of the UR32/UR35, allowing each of them to access the Internet.

Port	WAN	Bridge	Switch	WLAN	Cellular	Loopback	
Bridge Set	ting						
Name		Bridg	e0 I				
STP							
IP Add	Iress	192.1	68.140.1				
Netma	sk	255.2	255.255.0				
MTU		1500					
Multip	le IP Address						
		IP Addre	SS		Netmask	Operation	
						Œ	



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
MTU	Set the maximum transmission unit. Range: 68-1500.	1500
Multiple IP Address	Set the multiple IP addresses for bridge.	Null

Table 3-2-1-6

3.2.1.4 Switch

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

Port	WAN	Bridge	Switch	Cellular	Loopback		
AN Settings							
Nan	ne	VLAN ID	IP Ad	dress	Netmask	MTU	Operation
vlan1		1	• 192.168.1.	1	255.255.255.0	1500	×
LAN Setting	js						
10 411	D	LAN 1	LAN 2	LAN 3	LAN 4	CPU	Operation
VLAN II							
VLAN II	Unt	agged 🔻	Untagged •	Untagged	▼ Untagged	▼ Tagged	•

Figure 3-2-1-9

Switch	
Item	Description
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.
	Set the maximum transmission unit of LAN port. Range:
MTU	68-1500.
VLAN Settings	
VLAN ID	Set the label ID of the VLAN. Range: 1-4094.
LAN1, LAN2(, LAN3,	Make the VLAN bind with the corresponding ports and select
LAN4)	status from "Tagged", "Untagged" and "Close" for Ethernet
	frame on trunk link.
CPU	Control communication between VLAN and other networks.
	Table 3-2-1-7 VLAN Trunk Parameters

3.2.1.5 WLAN (Only Applicable to Wi-Fi Version)

This section explains how to set the related parameters for Wi-Fi network. UR32/UR35 supports 802.11 b/g/n, as AP or client mode. Wi-Fi is optional.

Port	WAN	Bridge	Switch	WLAN	
WLAN					
Enable		۲			
Work Mode		AP		•	
BSSID		24:e1	:24:f0:25:7a		
Radio Type		802.1	11n(2.4GHz)	•	
Channel		Auto		•	
3andwidth		20M	20MHz		
SSID		Ursali	ink_F0257A		
Encryption	Mode	No E	ncryption	¥	
SSID Broad	dcast				
AP Isolation	n				
Guest Mod	e	۲			
Max Client	Number	128	128		
P Setting					
Protocol		Statio	c IP	•	
P Address		192.1	192.168.140.1		
Netmask		255.2	55.255.0		

Figure 3-2-1-10

WLAN Settings	
Item	Description
Enable	Enable/disable WLAN.
Work Mode	Select router's work mode. The options are "Client" or "AP".
	Select encryption mode. The options are "No Encryption", "WEP
Encryption Mode	Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and
	"WPA-PSK/WPA2-PSK".
BSSID	Fill in the MAC address of the access point. Either SSID or BSSID can
00010	be filled to joint the network.
SSID	Fill in the SSID of the access point.
Client Mode	
Scan	Click "Scan" button to search the nearby access point.
SSID	Show SSID.
Channel	Show wireless channel.
Signal	Show wireless signal.
BSSID	Show the MAC address of the access point.
Security	Show the encryption mode.
Frequency	Show the frequency of radio.
Join Network	Click the button to join the wireless network.
AP Mode	
Radio Type	Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g
	(2.4 GHz)", "802.11n (2.4 GHz)".
Channel	Select wireless channel. The options are "Auto", "1", "2""11".
Cipher	Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".
Кеу	Fill the pre-shared key of WPA encryption.
Bandwidth	Select bandwidth. The options are "20MHz" and "40MHz".
	When SSID broadcast is disabled, other wireless devices can't not
SSID Broadcast	find the SSID and users have to enter the SSID manually to access
	find the SSID, and users have to enter the SSID manually to access
	to the wireless network.
	to the wireless network. When AP isolation is enabled, all users which access to the AP are
AP Isolation	to the wireless network.
AP Isolation	to the wireless network. When AP isolation is enabled, all users which access to the AP are
	to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. The internal network is not allowed to visit if the guest mode is enabled.
AP Isolation Guest Mode	 to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. The internal network is not allowed to visit if the guest mode is enabled. Set the maximum number of client to access when the router is
AP Isolation Guest Mode Max Client Number	to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. The internal network is not allowed to visit if the guest mode is enabled.
AP Isolation Guest Mode Max Client Number IP Setting	 to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. The internal network is not allowed to visit if the guest mode is enabled. Set the maximum number of client to access when the router is configured as AP.
AP Isolation Guest Mode Max Client Number IP Setting Protocol	 to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. The internal network is not allowed to visit if the guest mode is enabled. Set the maximum number of client to access when the router is configured as AP. Set the IP address in wireless network.
AP Isolation Guest Mode Max Client Number IP Setting Protocol IP Address	 to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. The internal network is not allowed to visit if the guest mode is enabled. Set the maximum number of client to access when the router is configured as AP. Set the IP address in wireless network. Set the IP address in wireless network.
AP Isolation Guest Mode Max Client Number IP Setting Protocol	 to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. The internal network is not allowed to visit if the guest mode is enabled. Set the maximum number of client to access when the router is configured as AP. Set the IP address in wireless network.

Table 3-2-1-8 WLAN Parameters

Related Topic

Wi-Fi Application Example

3.2.1.6 Cellular

This section explains how to set the related parameters for cellular network. The UR32/UR35 cellular router has two cellular interfaces, namely SIM1 and SIM2. Only one cellular interface is active at one time. If both cellular interfaces are enabled, then SIM1 interface takes precedence by default.

A typical use case would be to have SIM1 configured as the primary cellular interface and SIM2 as a backup. If the UR32/UR35 cannot connect to the network via SIM1, it will automatically fail over to SIM2.

Port	WAN	LAN	VLAN Trunk	Cellula	Loopback	
Cellular Se	tting					
		SIM1		SIM	2	
Enable						
Network Typ	pe	Auto)	• A	uto	
APN						
Username						0
Password						
Access Nun	nber					
PIN Code						
Authentica t i	on Type	Auto)	• A	uto	Ŧ
Roaming						
SMS Center	r					

Figure 3-2-1-1:	re 3-2-1-2	11
-----------------	------------	----

Connection Setting	$\mathbf{\Sigma}$	
Dual SIM Strategy	$\mathbf{\Sigma}$	
Enable NAT		
Restart When Dial-up Fails		
ICMP Server	8.8.8.8	
Secondary ICMP Server	114.114.114.114	
ICMP Detection Max Retries	3	
ICMP Detection Timeout	5	s
ICMP Detection Interval	15	s

Figure 3-2-1-12

General Settings	General Settings		
Item	Description	Default	
Enable	Check the option to enable the corresponding SIM card.	Enable	
Network Type	 Select from "Auto", "4G First", "4G Only", "3G First", "3G Only", "2G Frist", and "2G Only". Auto: connect to the network with the strongest signal automatically. 4G First: 4G network takes precedence. 4G Only: connect to 4G network only. And so on. 	Auto	
APN	Enter the Access Point Name for cellular dial-up connection provided by local ISP.	Null	
Username	Enter the username for cellular dial-up connection provided by local ISP.	Null	
Password	Enter the password for cellular dial-up connection provided by local ISP.	Null	
Access Number	Enter the dial-up center NO. For cellular dial-up connection provided by local ISP.	Null	
PIN Code	Enter a 4-8 characters PIN code to unlock the SIM.	Null	
Authentication Type	Select from "Auto", "PAP", "CHAP", "MS-CHAP", and "MS-CHAPv2".	Auto	
Roaming	Enable or disable roaming.	Disable	
SMS Center	Enter the local SMS center number for storing, forwarding, converting and delivering SMS message.	Null	
Enable NAT	Enable or disable NAT function.	Enable	
Restart When Dial-up Fails	When this function is enabled, the router will restart automatically if the number of dial-up failure reaches a certain limit.	Disable	
ICMP Server	Set the ICMP detection server's IP address.	8.8.8.8	
Secondary ICMP Server	Set the secondary ICMP detection server's IP address.	114.114.114.114	
ICMP Detection Max Retries	When a host doesn't respond, retries the host.	5	
ICMP Detection Timeout	Timeout for individual targets.	5	
ICMP Detection Interval	Interval between Pings to an individual target.	30	

Table 3-2-1-9 Cellular Parameters

Connection Setting		
Connection Mode	Connect on Demand	•
Redial Interval(s)	5	
Max Idle Time(s)	60	
Triggered by Call		
Triggered by SMS		
Triggered by IO		
Dual SIM Strategy	\square	
Primary SIM Card	SIM1	•
Switch to backup SIM card when ICMP detection fails		
Swtich to backup SIM card when the connection fails		
Switch to backup SIM card when roaming is detected		
Data Traffic Limit Strategy		
Data Allowance	1024	МВ
Billing Day	1	

Figure 3-2-1-13

Connection Setting		
Item	Description	
Connection Mode	Select from "Always Online" and "Connect on Demand".	
Connect on Demand	"Connect on Demand" includes "Triggered by Call", "Triggered by SMS", and "Triggered by IO".	
Triggered by Call	The router will switch from offline mode to cellular network mode automatically when it receives a call from the specific phone number.	
Call Group	Select a call group for call trigger. Go to "System > General > Phone" 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 trigger. Go to "System > General > Phone" to set up SMS group.	
SMS Text	Fill in the SMS content for triggering.	
Triggered by IO	The router will switch from offline mode to cellular network mode automatically when the DI status is changed. Go to "Industrial > I/O > DI" to configure trigger condition.	

Table 3-2-1-10 Cellular Parameters

Dual SIM Strategy	
Item	Description
Current SIM Card	Select between "SIM1" and "SIM2" as a current SIM card used.
Switch to backup SIM card when ICMP detection fails	The router will switch to the backup SIM card when packet loss rate in IMCP detection exceeds the preset value.
Switch to backup SIM card when the connection fails	The router will switch to the backup SIM card when the primary one fails to connect with cellular network.
Switch to backup SIM card when roaming is detected	The router will switch to the backup SIM card when the primary one is roaming.
Data Traffic Limit Strategy	Enable/disable Data Traffic Limit Strategy.
Data Allowance	Set the monthly maximum data traffic allowed. The router will switch to the backup SIM card if the used data traffic exceed the allowance.
Billing Day	Set monthly billing date. The cellular data usage will reset and restart to count on this day. Range: 1-28

Table 3-2-1-11 Cellular Parameters

SMS Settings		
SMS Mode	PDU	¥
SMS Remote Control		
Authentication Type	Password+Phone	•
Password		
Phone Group		¥

SMS Settings	
Item	Description
SMS Mode	Select SMS mode from "TEXT" and "PDU".
SMS Remote Control	Enable/disable SMS Remote Control.
Authentication Type	You can choose "phone number" or "password + phone number". Phone number: Use phone number for authentication. Password + phone number: Use both ""Password"" and ""Phone number"" for authentication.
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 3-2-1-12 Cellular Parameters

Related Topics

Cellular Network Connection Dual SIM Failover Application Example WAN Failover Application Example Phone Group DI Setting

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.

Port	WAN	LAN	VLAN Trunk	Cellular	Loopback	
Loopback	Address					
IP Address		127.	0.0.1			
Netmask		255.	0.0.0			
Multiple IP	Addresses					
	IP A	ddress		Netma	ask	Operation
]	255.255.255.255		×
						B



Loopback		
Item	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 3-2-1-13 Loopback Parameters

3.2.2 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.

3.2.2.1 Security

			For your d	evice security, please chang	e the default passw	ordl
	Security	ACL	DMZ	Port Mapping	MAC Binding	SF
	Prevent Attac	ĸ				
	DoS/DDoS Pro	tection				
	Access Servio	ce Control				
	Sen	vice	Port	Local		Remote
	нт	TP	80	×		
	нт	TPS	443	2		
	TEL	NET	23	2		
;	SS	SH	22			
	FT	ſP	21			
	Website Block	king				
۲	URL Blocking		http://	×		
F				0		
	Keyword Block	ing		×		

Figure 3-2-2-1

Item	Description	Default				
Prevent Attack						
DoS/DDoS Protection	Enable/disable Prevent DoS/DDoS Attack.	Disable				
Access Service Control						
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				
нттрѕ	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	You can block specific website by entering keyword. The maximum number of character allowed is 64.				
	Table 3-2-2-1 Security Parameters				

3.2.2.2 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.

	*		r or you	device security, please ch	ange me beraumpassy	ional.
Status	Security	ACL	DMZ	Port Mapping	MAC Binding	Ş
ietwork 🔻	ACL Setting					
Interface	Default Filter Po	licy	Accept	*		
III. III.	Access Contro	ol List				
Firewall			Type	е	xtended	•
QoS			ID			
DHCP			Action	P	ermit	•
DDNS			Protocol	ļ	2	•
			Source IP			
Link Failover			Source Wild	card Mask 0.	0.0.0	
Routing			Destination	IP		
VPN			Destination	Wildcard Mask 0	0.0.0	
			Description			
ystem 🕨				Save	Cancel	
		Figur	re 3-2-2-2			
erface List						
Interface		In ACL		Out ACL		Operation

Figure 3-2-2-3

Item	Description
ACL Setting	

Select from "Accept" and "Deny".Default Filter PolicyThe packets which are not included in the access control list will be processed by the default filter policy.Access Control ListTypeTypeSelect type from "Extended" and "Standard".IDUser-defined ACL number. Range: 1-199.ActionSelect from "Permit" and "Deny".ProtocolSelect protocol from "ip", "icmp", "tcp", "udp", and "1-255".Source IPSource network address (leaving it blank means all).Source Wildcard MaskWildcard mask of the source network address.Destination IPDestination network address (0.0.0.0 means all).Destination Wildcard MaskWildcard mask of destination address.DescriptionFill in a description for the groups with the same ID.ICMP TypeEnter the type of ICMP packet. Range: 0-255.Source Port TypeSelect source port type, such as specified port, port range, etc.Source PortSelect destination port type, such as specified port, port range, etc.Source PortSelect destination port number. Range: 1-65535.Start Source PortSelect destination port number. Range: 1-65535.Start Destination PortSelet destination port number. Range: 1-65535.Destination PortSelet destination port number. Range: 1-65535.Start Destination PortSet end destination port number. Range: 1-		
Access Control ListTypeSelect type from "Extended" and "Standard".IDUser-defined ACL number. Range: 1-199.ActionSelect from "Permit" and "Deny".ProtocolSelect protocol from "ip", "icmp", "tcp", "udp", and "1-255".Source IPSource network address (leaving it blank means all).Source Wildcard MaskWildcard mask of the source network address.Destination IPDestination network address (0.0.0.0 means all).Destination WildcardWildcard mask of destination address.MaskWildcard mask of destination address.DescriptionFill in a description for the groups with the same ID.ICMP TypeEnter the type of ICMP packet. Range: 0-255.Source Port TypeSelect source port type, such as specified port, port range, etc.Source PortSet source port number. Range: 1-65535.Start Source PortSet end source port number. Range: 1-65535.Destination Port TypeSelect destination port type, such as specified port, port range, etc.Destination Port TypeSelect destination port number. Range: 1-65535.Start Destination PortSet start destination port number. Range: 1-65535.Start Destination PortSet start destination port number. Range: 1-65535.Start Destination PortSet destination port number. Range: 1-65535.Start Destination PortSet destination port number. Range: 1-65535.Start Destination PortSet destination port number. Range: 1-65535.More DetailsShow information of the port.Interface ListInterface Intervork interface for access contr	Default Filter Policy	The packets which are not included in the access control list will
IDUser-defined ACL number. Range: 1-199.ActionSelect from "Permit" and "Deny".ProtocolSelect protocol from "ip", "icmp", "tcp", "udp", and "1-255".Source IPSource network address (leaving it blank means all).Source Wildcard MaskWildcard mask of the source network address.Destination IPDestination network address (0.0.0.0 means all).Destination Wildcard MaskWildcard mask of destination address.Destination Wildcard MaskWildcard mask of destination address.DescriptionFill in a description for the groups with the same ID.ICMP TypeEnter the type of ICMP packet. Range: 0-255.ICMP CodeEnter the code of ICMP packet. Range: 0-255.Source Port TypeSelect source port number. Range: 1-65535.Source PortSet start source port number. Range: 1-65535.Source PortSet end source port number. Range: 1-65535.End Source PortSet et destination port type, such as specified port, port range, etc.Destination Port TypeSelect destination port number. Range: 1-65535.Start Destination PortSet destination port number. Range: 1-65535.Start Destination PortSet end destination port number. Range: 1-65535.More DetailsShow information of the port.Interface ListSelect network interface for access control.In	Access Control List	
ActionSelect from "Permit" and "Deny".ProtocolSelect protocol from "ip", "icmp", "tcp", "udp", and "1-255".Source IPSource network address (leaving it blank means all).Source Wildcard MaskWildcard mask of the source network address.Destination IPDestination network address (0.0.0.0 means all).Destination Wildcard MaskWildcard mask of destination address.DescriptionFill in a description for the groups with the same ID.ICMP TypeEnter the type of ICMP packet. Range: 0-255.Source Port TypeSelect source port type, such as specified port, port range, etc.Source Port TypeSelect destination port type, such as specified port, port range, etc.Destination Port TypeSelect destination port type, such as specified port, port range, etc.Destination PortSet start destination port number. Range: 1-65535.Start Destination PortSet set ad source port number. Range: 1-65535.Start Destination PortSet set ad stination port number. Range: 1-65535.Start Destination PortSet set destination port number. Range: 1-65535.Start Destination PortSet set ad top ont number. Range: 1-65535.Start Destination PortSet end destination port number. Range: 1-65535.More DetailsShow information of the port.Interface ListSelect network interface for access control.InterfaceSelect network interface for access control.In ACLSelect a rule for incoming traffic from ACL ID.	Туре	Select type from "Extended" and "Standard".
ProtocolSelect protocol from "ip", "icmp", "tcp", "udp", and "1-255".Source IPSource network address (leaving it blank means all).Source Wildcard MaskWildcard mask of the source network address.Destination IPDestination network address (0.0.0.0 means all).Destination Wildcard MaskWildcard mask of destination address.DescriptionFill in a description for the groups with the same ID.ICMP TypeEnter the type of ICMP packet. Range: 0-255.ICMP CodeEnter the code of ICMP packet. Range: 0-255.Source Port TypeSelect source port type, such as specified port, port range, etc.Source Port TypeSet source port number. Range: 1-65535.Start Source PortSet end source port number. Range: 1-65535.Destination Port TypeSelect destination port type, such as specified port, port range, etc.Destination Port TypeSet end source port number. Range: 1-65535.Start Destination PortSet destination port number. Range: 1-65535.Start Destination PortSet end destination port number. Range: 1-65535.Start Destination PortSet end destination port number. Range: 1-65535.Start Destination PortSet end destination port number. Range: 1-65535.Ind Destination PortSet end destination port number. Range: 1-65535.Ind Destination PortSet end destination port number. Range: 1-65535.Interface ListShow information of the port.InterfaceSelect network interface for access control.InterfaceSelect a rule for incoming traffic from ACL ID.	ID	User-defined ACL number. Range: 1-199.
Source IPSource network address (leaving it blank means all).Source Wildcard MaskWildcard mask of the source network address.Destination IPDestination network address (0.0.0.0 means all).Destination Wildcard MaskWildcard mask of destination address.DescriptionFill in a description for the groups with the same ID.ICMP TypeEnter the type of ICMP packet. Range: 0-255.ICMP CodeEnter the code of ICMP packet. Range: 0-255.Source Port TypeSelect source port type, such as specified port, port range, etc.Source PortSet source port number. Range: 1-65535.Start Source PortSet end source port number. Range: 1-65535.Destination Port TypeSelect destination port type, such as specified port, port range, etc.Destination Port TypeSelect destination port number. Range: 1-65535.Start Source PortSet end source port number. Range: 1-65535.Destination Port TypeSelect destination port number. Range: 1-65535.Start Destination PortSet start destination port number. Range: 1-65535.Start Destination PortSet end destination port number. Range: 1-65535.Ind Destination PortSet end destination port number. Range: 1-65535.More DetailsShow information of the port.Interface ListSelect network interface for access control.In ACLSelect a rule for incoming traffic from ACL ID.	Action	Select from "Permit" and "Deny".
Source Wildcard MaskWildcard mask of the source network address.Destination IPDestination network address (0.0.0 means all).Destination Wildcard MaskWildcard mask of destination address.DescriptionFill in a description for the groups with the same ID.ICMP TypeEnter the type of ICMP packet. Range: 0-255.ICMP CodeEnter the code of ICMP packet. Range: 0-255.Source Port TypeSelect source port type, such as specified port, port range, etc.Source PortSet source port number. Range: 1-65535.Start Source PortSet end source port number. Range: 1-65535.Destination Port TypeSelect destination port type, such as specified port, port range, etc.Destination Port TypeSelect destination port type, such as specified port, port range, etc.Destination PortSet end source port number. Range: 1-65535.Start Destination PortSet destination port number. Range: 1-65535.Start Destination PortSet start destination port number. Range: 1-65535.More DetailsShow information of the port.Interface ListSelect network interface for access control.InterfaceSelect a rule for incoming traffic from ACL ID.	Protocol	Select protocol from "ip", "icmp", "tcp", "udp", and "1-255".
Destination IPDestination network address (0.0.0 means all).Destination Wildcard MaskWildcard mask of destination address.DescriptionFill in a description for the groups with the same ID.ICMP TypeEnter the type of ICMP packet. Range: 0-255.ICMP CodeEnter the code of ICMP packet. Range: 0-255.Source Port TypeSelect source port type, such as specified port, port range, etc.Source PortSet source port number. Range: 1-65535.Start Source PortSet end source port number. Range: 1-65535.End Source PortSelect destination port type, such as specified port, port range, etc.Destination Port TypeSelect destination port type, such as specified port, port range, etc.Destination Port TypeSelect destination port number. Range: 1-65535.Start Destination PortSet end source port number. Range: 1-65535.Start Destination PortSet start destination port number. Range: 1-65535.More DetailsShow information of the port.Interface ListSelect network interface for access control.InterfaceSelect a rule for incoming traffic from ACL ID.	Source IP	Source network address (leaving it blank means all).
Destination Wildcard MaskWildcard mask of destination address.DescriptionFill in a description for the groups with the same ID.ICMP TypeEnter the type of ICMP packet. Range: 0-255.ICMP CodeEnter the code of ICMP packet. Range: 0-255.Source Port TypeSelect source port type, such as specified port, port range, etc.Source PortSet source port number. Range: 1-65535.Start Source PortSet end source port number. Range: 1-65535.Destination Port TypeSelect destination port type, such as specified port, port range, etc.Destination Port TypeSelect destination port type, such as specified port, port range, etc.Destination Port TypeSelect destination port type, such as specified port, port range, etc.Destination Port TypeSelect destination port number. Range: 1-65535.Start Destination PortSet end destination port number. Range: 1-65535.End Destination PortSet end destination port number. Range: 1-65535.Interface ListShow information of the port.Interface ListSelect network interface for access control.In ACLSelect a rule for incoming traffic from ACL ID.	Source Wildcard Mask	Wildcard mask of the source network address.
MaskWildcard mask of destination address.DescriptionFill in a description for the groups with the same ID.ICMP TypeEnter the type of ICMP packet. Range: 0-255.ICMP CodeEnter the code of ICMP packet. Range: 0-255.Source Port TypeSelect source port type, such as specified port, port range, etc.Source PortSet source port number. Range: 1-65535.Start Source PortSet end source port number. Range: 1-65535.End Source PortSet end source port number. Range: 1-65535.Destination Port TypeSelect destination port type, such as specified port, port range, etc.Destination PortSet destination port number. Range: 1-65535.Start Destination PortSet destination port number. Range: 1-65535.Start Destination PortSet destination port number. Range: 1-65535.More DetailsShow information port number. Range: 1-65535.InterfaceSelect network interface for access control.InterfaceSelect network interface for access control.InterfaceSelect a rule for incoming traffic from ACL ID.	Destination IP	Destination network address (0.0.0.0 means all).
ICMP TypeEnter the type of ICMP packet. Range: 0-255.ICMP CodeEnter the code of ICMP packet. Range: 0-255.Source Port TypeSelect source port type, such as specified port, port range, etc.Source PortSet source port number. Range: 1-65535.Start Source PortSet end source port number. Range: 1-65535.End Source PortSet end source port number. Range: 1-65535.Destination Port TypeSelect destination port type, such as specified port, port range, etc.Destination PortSet destination port number. Range: 1-65535.Start Destination PortSet end destination port number. Range: 1-65535.End Destination PortSet end destination port number. Range: 1-65535.More DetailsShow information of the port.Interface ListSelect network interface for access control.In ACLSelect a rule for incoming traffic from ACL ID.		Wildcard mask of destination address.
ICMP CodeEnter the code of ICMP packet. Range: 0-255.Source Port TypeSelect source port type, such as specified port, port range, etc.Source PortSet source port number. Range: 1-65535.Start Source PortSet end source port number. Range: 1-65535.End Source PortSet end source port number. Range: 1-65535.Destination Port TypeSelect destination port type, such as specified port, port range, etc.Destination PortSet destination port number. Range: 1-65535.Start Destination PortSet destination port number. Range: 1-65535.End Destination PortSet end destination port number. Range: 1-65535.Ind Destination PortSet end destination port number. Range: 1-65535.Interface ListShow information of the port.InterfaceSelect network interface for access control.In ACLSelect a rule for incoming traffic from ACL ID.	Description	Fill in a description for the groups with the same ID.
Source Port TypeSelect source port type, such as specified port, port range, etc.Source PortSet source port number. Range: 1-65535.Start Source PortSet start source port number. Range: 1-65535.End Source PortSet end source port number. Range: 1-65535.Destination Port TypeSelect destination port type, such as specified port, port range, etc.Destination PortSet destination port number. Range: 1-65535.Start Destination PortSet destination port number. Range: 1-65535.Start Destination PortSet start destination port number. Range: 1-65535.Ind Destination PortSet end destination port number. Range: 1-65535.More DetailsShow information of the port.Interface ListSelect network interface for access control.In ACLSelect a rule for incoming traffic from ACL ID.	ІСМР Туре	Enter the type of ICMP packet. Range: 0-255.
Source PortSet source port number. Range: 1-65535.Start Source PortSet start source port number. Range: 1-65535.End Source PortSet end source port number. Range: 1-65535.Destination Port TypeSelect destination port type, such as specified port, port range, etc.Destination PortSet destination port number. Range: 1-65535.Start Destination PortSet destination port number. Range: 1-65535.Start Destination PortSet start destination port number. Range: 1-65535.End Destination PortSet end destination port number. Range: 1-65535.More DetailsShow information of the port.Interface ListSelect network interface for access control.In ACLSelect a rule for incoming traffic from ACL ID.	ICMP Code	Enter the code of ICMP packet. Range: 0-255.
Start Source PortSet start source port number. Range: 1-65535.End Source PortSet end source port number. Range: 1-65535.Destination Port TypeSelect destination port type, such as specified port, port range, etc.Destination PortSet destination port number. Range: 1-65535.Start Destination PortSet start destination port number. Range: 1-65535.End Destination PortSet start destination port number. Range: 1-65535.More DetailsSet end destination port number. Range: 1-65535.More DetailsShow information of the port.Interface ListSelect network interface for access control.In ACLSelect a rule for incoming traffic from ACL ID.	Source Port Type	Select source port type, such as specified port, port range, etc.
End Source PortSet end source port number. Range: 1-65535.Destination Port TypeSelect destination port type, such as specified port, port range, etc.Destination PortSet destination port number. Range: 1-65535.Start Destination PortSet start destination port number. Range: 1-65535.End Destination PortSet end destination port number. Range: 1-65535.More DetailsShow information of the port.Interface ListSelect network interface for access control.In ACLSelect a rule for incoming traffic from ACL ID.	Source Port	Set source port number. Range: 1-65535.
Destination Port TypeSelect destination port type, such as specified port, port range, etc.Destination PortSet destination port number. Range: 1-65535.Start Destination PortSet start destination port number. Range: 1-65535.End Destination PortSet end destination port number. Range: 1-65535.More DetailsShow information of the port.Interface ListSelect network interface for access control.In ACLSelect a rule for incoming traffic from ACL ID.	Start Source Port	Set start source port number. Range: 1-65535.
Destination Port Typeetc.Destination PortSet destination port number. Range: 1-65535.Start Destination PortSet start destination port number. Range: 1-65535.End Destination PortSet end destination port number. Range: 1-65535.More DetailsShow information of the port.Interface ListSelect network interface for access control.In ACLSelect a rule for incoming traffic from ACL ID.	End Source Port	Set end source port number. Range: 1-65535.
Start Destination PortSet start destination port number. Range: 1-65535.End Destination PortSet end destination port number. Range: 1-65535.More DetailsShow information of the port.Interface ListInterfaceInterfaceSelect network interface for access control.In ACLSelect a rule for incoming traffic from ACL ID.	Destination Port Type	
End Destination PortSet end destination port number. Range: 1-65535.More DetailsShow information of the port.Interface ListInterfaceInterfaceSelect network interface for access control.In ACLSelect a rule for incoming traffic from ACL ID.	Destination Port	Set destination port number. Range: 1-65535.
More DetailsShow information of the port.Interface ListInterfaceInterfaceSelect network interface for access control.In ACLSelect a rule for incoming traffic from ACL ID.	Start Destination Port	Set start destination port number. Range: 1-65535.
Interface ListInterfaceSelect network interface for access control.In ACLSelect a rule for incoming traffic from ACL ID.	End Destination Port	Set end destination port number. Range: 1-65535.
InterfaceSelect network interface for access control.In ACLSelect a rule for incoming traffic from ACL ID.	More Details	Show information of the port.
In ACL Select a rule for incoming traffic from ACL ID.	Interface List	
	Interface	Select network interface for access control.
Out ACL Select a rule for outgoing traffic from ACL ID.	In ACL	Select a rule for incoming traffic from ACL ID.
	Out ACL	Select a rule for outgoing traffic from ACL ID.

Table 3-2-2-2 ACL Parameters

Related Configuration Example

Access Control Application Example

3.2.2.3 DMZ

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

Security	ACL	DMZ	Port Mapping
DMZ			
Enable			
DMZ Host			
Source Address			

Figure 3-2-2-4

DMZ				
Item	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. "0.0.0.0/0" means any address.			

Table 3-2-2-3 DMZ Parameters

3.2.2.4 Port Mapping

Click 🛨 to add a new port mapping rules.

Port mapping is an application of network address translation (NAT) that redirects a communication request from the combination of an address and port number to another while the packets are traversing a network gateway such as a router or firewall.

Security	ACL	DMZ	Port Mapping	MAC E	Binding	SPI	
Port Mapping							
Source II	Р	Source Port	Destination IP	Destination Port	Protocol	Description	Operation
0.0.0/0]				TCP 🔻		
							8



Port Mapping				
Item	Description			
Source IP	Specify the host or network which can access local IP address.			
Source IP	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 3-2-2-4 Port Mapping Parameters

Related Configuration Example

NAT Application Example

3.2.2.5 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.

Security	ACL	DMZ	Port Mapping	MAC Binding	SPI	
MAC Binding	List					
	MAC		IP		Description	Operation
						H



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 3-2-2-5 MAC Binding Parameters

3.2.2.6 SPI

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

Securi	y ACL	DMZ	Port Mapping	MAC Binding	SPI
SPI Fire	wall				
	Enable				
	Filter Proxy				
	Filter Cookies				
	Filter Activex				
	Filter Java Applets				
	Filter Multicast				
	Filter IDENT(port 113)				
	Block Wan SNMP access				
	Filter WAN NAT Redirection				
	Block Anonymous	s Wan Request			

Figure 3-2-2-7

SPI Firewall	
Item	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 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.
Filter WAN NAT Redirection	Prevent hosts on LAN from using WAN address of router to 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 3-2-2-6 MAC Binding Parameters

3.2.3 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.

DDNS Link Fallovor Service Category Rules Routing Name Source IP Source Destination IP Destination Protocol Service Operation				For your device sec	urity, please change the	a default password	0		
Network Enable Interface Default Category Default Category Image: Category Download Bandwidth 0 CoS Download Bandwidth Capacity Capacity DHCP Name Percent(%) Max BW(kbps) Min BW(kbps) Operation DDNS Image: Category Rules Enable Source Download Bandwidth 0 Capacity Image: Category Rules	Status	- QoS(Download)	QoS(Uplo	ad)					
Network Enable Interface Dafault Category Differentiation Download Bandwidth Capacity Capacity CoS		Download Bandwid	th						
Firewall Download Bandwidth 0 kbits/s Capacity Capacity Capacity QoS Service Category DHCP Name Percent(%) Max BW(kbps) Min BW(kbps) Operation DDNS	Network 👻	Enable							
Firewall Capacity Cos Service Category DHCP Name Percent(%) Max BW(kbps) Min BW(kbps) Operation DDNS Link Fallovor Service Category Rules Image: Category Rules Source Destination Destination Service Destination	Interface	Default Category		٠					
QoS Service Category DHCP Name Percent(%) Max BW(kbps) Min BW(kbps) Operation DDNS Image: Category Rules Routing Name Source Destination Service Category Rules	Firewall		0	k	bits/s				
DHCP Name Percent(%) Max BW(kbps) Min BW(kbps) Operation DDNS Image: Category Rules Image: Category Rules Image: Category Rules Image: Category Rules	QoS								
Name Percent(%) Max BW(kbps) Min BW(kbps) Operation DDNS Image: Service Category Rules Image: Service Category Rules Image: Service Category Rules		Service Category							
Link Fallover Service Category Rules Routing Source Destination Destination Service Destination	DHCP	Name		Percent(%)	Max BW(kbps)	Min BW	(kbps)	Operation
Routing Service Category Rules									
Name Source Destination Destination Destination	DDNS								H
Port Port Category Category		Service Category R	ules						Đ

Figure 3-2-3-1

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
Bandwidth Capacity	the 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
Name	Give the rule a descriptive name.
Source IP	Source address of flow control (leaving it blank means any).
Source Port	Source port of flow control. Range: 0-65535 (leaving it blank means any).
Destination IP	Destination address of flow control (leaving it blank means any).
Destination Port	Destination port of flow control. Range: 0-65535 (leaving it

	blank means any).		
Protocol	Select protocol from "ANY", "TCP", "UDP", "ICMP", and "GRE".		
Service Category	Set service category for the rule.		

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

Related Configuration Example

QoS Application Example

3.2.4 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.

3.2.4.1 DHCP Server

The UR32/UR35 can be set as a DHCP 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.

Status	BHCP Server DHCP Rela	y.		
Network 👻	- DHCP Server_1			
	Enable	×		
Interface	Interface	bridge0 🔻		
Firewall	Start Address	192 168 1 100		
QoS	End Address	192.168.1.199		
DHCP	Netmask	255 255 255 0		
DDNS	Lease Time(Min)	1440		
	Primary DNS Server	114 114 114 114		
Link Failover	Secondary DNS Server			
Routing	Windows Name Server			
VPN	Static IP			
System 🕨	MAC 4	Address	IP Address	Operation

Figure 3-2-4-1

DHCP Server			
Item	Description	Default	
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.	192.168.1.100	
End Address	Define the end of the pool of IP addresses which will be	192.168.1.199	

	leased to DHCP clients.	
Netmask	Define the subnet mask of IP address obtained by DHCP clients from DHCP server.	255.255.255.0
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.	114.114.114.114
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
IP Address	Set a static and specific IP address for the DHCP client (it should be outside of the DHCP range).	Null

Table 3-2-4-1 DHCP Server Parameters

3.2.4.2 DHCP Relay

The UR32/UR35 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	DHCP Relay
DHCP Relay	
Enable	
DHCP Server	



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 3-2-4-2 DHCP Relay Parameters

3.2.5 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.

URSALINK For your device security, pleas DDNS Status DDNS Method List Network Enable 1 Interface Name Ŧ cellular0 Interface Firewall DynDNS ۷ Service Type QoS Username DHCP User ID DDNS Password Server Link Failover Server Path Routing Hostname VPN Append IP

Figure 3-2-5-1

DDNS	
Item	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.

Table 3-2-5-1 DDNS Parameters

3.2.6 Link Failover

This section describes how to configure link failover strategies, including VRRP strategies and WAN failover strategies between Ethernet WAN and cellular.

Configuration Steps

- 1. Define one or more SLA operations (ICMP probe).
- 2. Define one or more track objects to track the status of SLA operation.
- 3. Define applications associated with track objects, such as VRRP, WAN failover or static routing.

3.2.6.1 SLA

SLA setting is used for configuring link probe method. The default probe type is ICMP.

Status	SLA	Track	VRRP	WAN Fallover							
Network 👻	SLA Entry										
Interface	D	Туре	Destination Addres	Secondary Destination Address	Data Size	Interval(s)	Timeout(ms)	PING Timea	Packet Loss Rate	Start Time	Operation
Firewall	1	Icmp-echo	• 114.114.114.114	8.8.8.8	66	30	5000	6	20	now 🔻	
QoS											0
DHCP	Save										
DDNS											
Link Fallover											

Figure 3-2-6-1

SLA		
Item	Description	Default
ID	SLA index. Up to 10 SLA settings can be added. Range: 1-10.	1
Туре	ICMP-ECHO is the default type to detect if the link is alive.	icmp-echo
Destination Address	The detected IP address.	114.114.114.114
Secondary Destination Address	The secondary detected IP address.	8.8.8.8
Data Size	User-defined data size. Range: 0-1000.	56
Interval (s)	User-defined detection interval. Range: 1-608400.	30
Timeout (ms)	User-defined timeout for response to determine ICMP detection failure. Range: 1-300000.	5000
PING Times	Define PING packet numbers in each SLA probe. Range: 1-1000.	5
Packet Loss Rate	Define packet loss rate in each SLA probe. SLA probe fails when the preset packet loss rate is exceeded.	20
Start Time	Detection start time; select from "Now" and blank character. Blank character means this SLA detection doesn't start.	now

Table 3-2-6-1 SLA Parameters

3.2.6.2 Track

Track setting is designed for achieving linkage among SLA module, Track module and Application module. Track setting is located between application module and SLA module with main function of shielding the differences of various SLA modules and providing unified interfaces for application module.

Linkage between Track Module and SLA module

Once you complete the configuration, the linkage relationship between Track module and SLA module will be established. SLA module is used for detection of link status, network performance and notification of Track module. The detection results help track status change timely.

- For successful detection, the corresponding track item is Positive.
- For failed detection, the corresponding track item is Negative.

Linkage between Track Module and Application Module

After configuration, the linkage relationship between Track module and application module will be established. When any change occurs in track item, a notification that requires corresponding treatment will be sent to Application module.

Currently, the application modules like VRRP, WAN failover and static routing can get linkage with track module.

If it sends an instant notification to Application module, the communication may be interrupted in some circumstances due to routing's failure like timely restoration or other reasons. Therefore, user can set up a

period of time to delay notifying application module when the track item status changes.

SLA	Track	VRRP	WAN Failover			
Track Object						
ID	Туре	SLA ID	Interface	Negative Delay(s)	Positive Delay(s)	Operation
1	sla	• 1 •	cellular0 •	0	1	×
						æ



Item	Description	Default
Index	Track index. Up to 10 track settings can be configured. Range: 1-10.	1
Туре	The options are "sla" and "interface".	SLA
SLA ID	Defined SLA ID.	1
Interface	Select the interface whose status will be detected.	cellular0
Negative Delay (s)	When interface is down or SLA probing fails, it will wait according to the time set here before actually changing its status to Down. Range: 0-180 (0 refers to immediate switching).	0
Positive Delay (s)	When failure recovery occurs, it will wait according to the time set here before actually changing its status to Up. Range: 0-180 (0 refers to immediate switching).	1

Table 3-2-6-2 Track Parameters

3.2.6.3 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	SLA	Track	VRRP	WAN Failover	
Network 👻	VRRP Status	5	DISA	BLE	
Interface	VRRP Settin	gs			
Firewall	Enable				
1927/127	Interface		Bri	dge0 🔻	
QoS	Virtual Router	D	1		
DHCP	Virtual IP		192	.168.3.152	
DDNS	Priority		100		
Link Failover	Advertisemer	t Interval(s)	1		
	Preemption M	lode			
Routing	Track ID			•	

Figure 3-2-6-3

VRRP						
Item	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				
Track ID	Trace detection, select the defined track ID or blank character.	None				

Table 3-2-6-3 VRRP Parameters

Related Configuration Example

VRRP Application Example

3.2.6.4 WAN Failover

WAN failover refers to failover between Ethernet WAN interface and cellular interface. When service transmission can't be carried out normally due to malfunction of a certain interface or lack of bandwidth, the rate of flow can be switched to backup interface quickly. Then the backup interface will carry out service transmission and share network flow so as to improve reliability of communication of data equipment.

When link state of main interface is switched from up to down, system will have the pre-set delay works instead of switching to link of backup interface immediately. Only if the state of main interface is still down after delay, will the system switch to link of backup interface. Otherwise, system will remain unchanged.

Status SLA Track VRRP WAN Failover Network WAN Failover Main Interface Backup Interface Startup Delay(s) Up Delay(s) Down Delay(s) Firewall Cellular 0 LAN1/WAN 30 0 0 1	Track ID Operatio
Interface Main Interface Backup Interface Startup Delay(s) Up Delay(s) Down Delay(s)	Track ID Operatio
Interface	Track ID Operatio
Cellular 0 v LAN1/WAN v 30. 0 0 1	
	▼ ×
QoS	H
DHCP Save	
DDNS	

Figure 3-2-6-4

WAN Failover						
Parameters	Description	Default				
Main Interface	Select a link interface as the main link.	Cellular0				
Backup Interface	Select a link interface as the backup link.	WAN				
Startup Delay (s)	Set how long to wait for the startup tracking detection policy to take effect. Range: 0-300.	3				
Up Delay (s)	When the primary interface switches from failed detection to successful detection, switching can be delayed based on the set time. Range: 0-180 (0 refers to immediate switching).	0				
Down Delay (s)	When the primary interface switches from successful detection to failed detection, switching can be delayed based on the set time. Range: 0-180 (0 refers to immediate switching).	0				
Track ID	Track detection, select the defined track ID.	1				

Table 3-2-6-4 WAN Failover Parameters

Related Configuration Example

WAN Failover Application Example

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.

			For your devic	e security, piease c	hange the default passy	ordl		
Network 🝷	Static Routing	RIP	OSPF	Routing Fill	tering			
Interface	Static Routing							
Firewall	Destination		Netmask	Interface	Gateway	Distance	Track ID	Operation
QoS	0.0.0	0.0	0.0	Bridge 🔻	192.168.23,1	1	•	×
DHCP								æ
DDNS	Save							
Link Failover								
Routing								



Static Routing	
Item	Description
Destination	Enter the destination IP address.
Netmask	Enter the subnet mask 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.
Track ID	Track detection, select the defined track ID. You can leave it blank.

Table 3-2-7-1 Static Routing Parameters

Related Topics

Track Setting

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	Rout	ing Filtering
RIP Settings				
Enable				
Update Timer	30			5
Timeout Timer	180		3	5
Garbage Collection Timer	120			5
Version	v2		•	
Show Advanced Options	>			
Default Information Origina	te 🔟			
Default Metric	1			
Redistribute Connected				
Redistribute Static				
Redistribute OSPF				

Figure 3-2-7-2

RIP	
Item	Description
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

Distance/Metric M	Management						
Distanc	e	IP Add	Iress	Netmas	k	ACL Name	Operation
							8
Metric		Policy	n/Out	Interfac	۵	ACL Name	Operation
		1 only 1	in out		-		
Filter Policy							
Policy Ty	ре	Policy	Name	Policy In/0	Dut	Interface	Operation
							8
Passive Interface	(
			Passive	Interface			Operation
							8
Interface							
Interface	Send Version	Receive Version	Split- Horizon	Authentication Mode	Authentication String	Authentication Key-chain	Operation
							Ð
Neighbor							
			IP Ad	Idress			Operation
							8
Network							
	IP Addre	ISS			Netmask		Operation
							8

Figure 3-2-7-3

Item	Description
Distance/Metric Manag	gement
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", "WAN" and "Bridge0".
Passive Interface	
Passive Interface	Select interface from "cellular0" and "WAN", "Bridge0".
Interface	
Interface	Select interface from "cellular0", "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.

Static Routing	RIP	OSPF	Routing Filtering
OSPF Settings			
Enable			
Router ID			
ABR Type	cisco		¥
RFC1583 Compatibility	V		
OSPF Opaque-LSA			
SPF Delay Time	0		ms
SPF Initial-holdtime	50		ms
SPF Max-holdtime	5000		ms
Reference Bandwidth	100		mbit

Figure 3-2-7-4

OSPF	
Item	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	erface	Hello Interval(s)	Dead Inte	erval(s)	Retransmit Interval(s)	Transmit Delay(s)	Operation
Bridge0	۲	10	40	5] [1	
Interface Adva	anced Options						
Interface	Network	Cost	Priority	Authenticat ion	Key ID	Key	Operation
Bridge 🔻	broad 🔻	10 1		`			\mathbf{x}
							H

Figure 3-2-7-5

Item		Description
Interface		
Interface	Selec	t 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 adjac	Time. If no Hello packet is received from the neighbours within the time, then the neighbour is considered failed. If dead times of two tent routers are different, the neighbour relationship cannot be blished.
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 O	ptions
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				
	Passiv	e Interface		Operation
				Ð
Network				
IP Address	Ne	tmask	Area ID	Operation
				8
Neighbor				
IP Address	Pi	iority	Poll	Operation
				Ð
Area				
Area ID	Area	No Summary	Authentication	Operation
				E



Item	Description
Passive Interface	
Passive Interface	Select interface from "cellular0", "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

Area Advanced Options								
Area Range								
Area ID	IP Addre	ess	Netr	nask	No Advertise	Co	ost	Operation
Area Filter								Œ
Area ID			Filter Type			ACL Name		Operation
								Đ
Area Virtual Link								
Area ID ABR Address	Authentica tion	Key ID	Key	Hello Interval	Dead Interval	Retransmit Interval	Transmit Delay	Operation
								æ

Figure 3-2-7-7

Area Advanced Opti	ons
Item	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.
Кеу	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		Metric Type	Route Map	Operation
connected 🔻		1	•		
					H
Redistribution Advanced Options	2				
Always Redistribute Default Route					
Redistribute Default Route Metric	0				
Redistribute Default Route Metric Type	1	•			
Distance Management					
Area Typ	e		Dista	nce	Operation

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	d 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

Static Routing	RIP	OSPF	Routing Fi	Itering		
ccess Control List						
Name	Ac	tion	Match Any	IP Address	Netmask	Operation
	deny	•				×
						Ð
Prefix-List						
	Sequence Number	Action	Match Any	IP Address Netmask	GE Length LE Length	Operation
Name	Humber					
Name		deny 🔻				

Figure 3-2-7-9

Routing Filtering	
Item	Description
Access Control 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 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 UR32/UR35 supports DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN, as well as GRE over IPsec and L2TP over IPsec.

3.2.8.1 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.

tatus	DMVPN	IPsec	GRE	L2TP	PPTP	
twork 🔻	DMVPN Settin	gs				
Interface	Enable					
Firewall	Hub Address					
	Local IP Addres	S				
QoS	GRE HUB IP Ac	ldress				
DHCP	GRE Local IP A	ddress				
DDNS	GRE Mask	GRE Mask			255.255.255.0	
AAND	GRE Key					
- - -	Negotiation Mod	le		Main	2	
	Authentication A	lgorithm		DES		
010	Encryption Algo	rithm		MD5		
nk Failover	DH Group			MODP768-1	•	
outing	Key					
	Local ID Type			Default	1	
PN	IKE Life Time(s)			10800		
em 🕨	SA Algorithm			DES-MD5		
strial 🕨	PFS Group			NULL	5.	
suiai 💌	Life Time(s)			3600		
ntenance	DPD Time Interv	val(s)		30		
	DPD Timeout(s)			150		
2	Cisco Secret					



DMVPN	
Item	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 Algorithm	Select from "DES", "3DES", "AES128", "AES192" and "AES256".
Encryption Algorithm	Select from "MD5" and "SHA1".
DH Group	Select from "MODP768_1", "MODP1024_2" and "MODP1536_5".
Кеу	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",
	"3DES_SHA1", "AES128_MD5", "AES128_SHA1",
SA Algorithm	"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.

Table 3-2-8-1 DMVPN Parameters

3.2.8.2 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.

DMVPN	IPsec Server	IPsec	GRE
OpenVPN Server	Certificati	ons	
IPsec Server			
Enable			
IPsec Mode	Tun	inel	•
IPsec Protocol	ESI	Þ	•
Local Subnet			
Local Subnet Mask			
Local ID Type	Def	ault	•
Remote Subnet			
Remote Subnet Mask			
Remote ID Type	Def	ault	•

Figure 3-2-8-2

IPsec Server			
Item	Description		
Enable	Enable IPsec tunnel. A maximum of 3 tunnels is allowed.		
IPsec Mode	Select from "Tunnel" and "Transport".		
IPsec Protocol	Select from "ESP" and "AH".		
Local Subnet	Enter the local subnet IP address that IPsec protects.		
Local Subnet Netmask	Enter the local netmask that IPsec protects.		
Local ID Type	Select from "Default", "ID", "FQDN", and "User FQDN".		
Remote Subnet	Enter the remote subnet IP address that IPsec protects.		
Remote Subnet Mask	Enter the remote netmask that IPsec protects.		
Remote ID type	Select from "Default", "ID", "FQDN", and "User FQDN".		

Table 3-2-8-2 IPsec Parameters

UR32&UR35 User Guide

IKE Parameter	2			
IKE Version	IKEv1	¥		
Negotiation Mode	Main	T		
Encryption Algorithm	DES	•		
Authentication Algorithm	MD5	T		
DH Group	MODP768-1	•		
Local Authentication	PSK	Ŧ		
XAUTH	8			
Lifetime(s)	10800			
XAUTH List				
U	sername		Password	Operation
				8
PSK List				
3	Selector		PSK	Operation
				8

Figure 3-2-8-3

SA Parameter	ø	
SA Algorithm	DES-MD5	•
PFS Group	NULL	•
Lifetime(s)	3600	
DPD Time Interval(s)	30	
DPD Timeout(s)	150	
IPsec Advanced		
Enable Compression		
VPN Over IPsec Type	NONE	•



IKE Parameter		
Item	Description	
IKE Version	Select from "IKEv1" and "IKEv2".	
Negotiation Mode	Select from "Main" and "Aggressive".	
Encryption Algorithm	Select from "DES", "3DES", "AES128", "AES192" and "AES256".	
Authentication Algorithm	Select from "MD5" and " SHA1"	
DH Group	Select from "MODP768_1", "MODP1024_2" and "MODP1536_5".	
Local Authentication	Select from "PSK" and "CA".	
XAUTH	Enter 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	
	Select from "DES_MD5", "DES_SHA1", "3DES_MD5", "3DES_SHA1",
SA Algorithm	"AES128_MD5", "AES128_SHA1", "AES192_MD5", "AES192_SHA1",
	"AES256_MD5" and "AES256_SHA1".
PFS Group	Select from "NULL", "MODP768_1" , "MODP1024_2" and "MODP1536_5".
Lifetime (s)	Set the lifetime of IPsec SA. Range: 60-86400.
DPD Interval Time(s)	Set DPD interval time to detect if the remote side fails.
DPD Timeout(s)	Set DPD timeout. Range: 10-3600.
IPsec Advanced	
Enable Compression	The head of IP packet will be compressed after it's enabled.
VPN Over IPsec Type	Select from "NONE", "GRE" and "L2TP" to enable VPN over IPsec function.

Table 3-2-8-3 IPsec Server Parameters

3.2.8.3 IPSec

DMVPN	IPsec Server	IPsec	GRE
OpenVPN Server	Certifica	tions	
IPsec Settings			
- IPsec_1			
Enable			
IPsec Gatewa	y Address		ĺ
IPsec Mode		Tunnel	¥
IPsec Protoco	d	ESP	Ŧ
Local Subnet			
Local Subnet	Mask		
Local ID Type		Default	٣
Remote Subn	et		
Remote Subn	et Mask		
Remote ID Ty	pe	Default	v

Figure 3-2-8-5

IPsec		
Description		
Enable IPsec tunnel. A maximum of 3 tunnels is allowed.		
Enter the IP address or domain name of remote IPsec server.		
Select from "Tunnel" and "Transport".		
Select from "ESP" and "AH".		
Enter the local subnet IP address that IPsec protects.		
Enter the local netmask that IPsec protects.		
Select from "Default", "ID", "FQDN", and "User FQDN".		
Enter the remote subnet IP address that IPsec protects.		
Enter the remote netmask that IPsec protects.		
Select from "Default", "ID", "FQDN", and "User FQDN".		

Table 3-2-8-4 IPsec Parameters

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

Figure 3-2-8-6

IKE Parameter			
Item	Description		
IKE Version	Select from "IKEv1" and "IKEv2".		
Negotiation Mode	Select from "Main" and "Aggressive".		
Encryption Algorithm	Select from "DES", "3DES", "AES128", "AES192" and "AES256".		
Authentication Algorithm	Select from "MD5" and " SHA1"		
DH Group	Select from "MODP768_1", "MODP1024_2" and "MODP1536_5".		
Local Authentication	Select from "PSK" and "CA".		
Local Secrets	Enter the pre-shared key.		
XAUTH	Enter XAUTH username and password after XAUTH is enabled.		
Lifetime (s)	Set the lifetime in IKE negotiation. Range: 60-86400.		
SA Parameter			
	Select from "DES_MD5", "DES_SHA1", "3DES_MD5", "3DES_SHA1",		
SA Algorithm	"AES128_MD5", "AES128_SHA1", "AES192_MD5", "AES192_SHA1", "AES256_MD5" and "AES256_SHA1".		
PFS Group	Select from "NULL", "MODP768_1", "MODP1024_2" and "MODP1536_5".		
Lifetime (s)	Set the lifetime of IPsec SA. Range: 60-86400.		
DPD Interval Time(s)	Set DPD interval time to detect if the remote side fails.		
DPD Timeout(s)	Set DPD timeout. Range: 10-3600.		
IPsec Advanced			
Enable Compression	The head of IP packet will be compressed after it's enabled.		
VPN Over IPsec Type	Select from "NONE", "GRE" and "L2TP" to enable VPN over IPsec function.		

Table 3-2-8-5 IPsec Parameters

3.2.8.4 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.

DMVPN	IPsec	GRE	L2TP	PPTP
GRE Settings				
- GRE_1				
Enable				
Remote IP	Address			
Local IP A	ddress			0
Local Virtu	ial IP Address			
Netmask		2	55.255.255.0	
Peer Virtu	al IP Address			
Global Tra	ffic Forwarding			
Remote S	ubnet			j.
Remote N	etmask			
MTU		1	500	
Key				
Enable NA	AT			

Figure 3-2-8-7

GRE	
Item	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.
Кеу	Set GRE tunnel key.
Enable NAT	Enable NAT traversal function.

Table 3-2-8-6 GRE Parameters

3.2.8.5 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.

DMVPN	IPsec	GRE	L2TP	PPTP
L2TP Settings				
— L2TP_1				
Enable				
Remote IP	Address			
Username				/2
Password				
Authentical	tion	A	uto	•
Global Traf	fic Forwarding			
Remote Su	ibnet			
Remote Su	ibnet Mask			
Key				

Figure 3-2-8-8

L2TP	
Item	Description
Enable	Check to enable L2TP function.
Remote IP Address	Enter the public IP address or domain name of 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 this
Forwarding	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 3-2-8-7 L2TP Parameters

Advanced Settings	
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 3-2-8-9

Advanced Settings		
Item	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	For PPP initialization. User can keep the default option.	
Compression		
Protocol Field	For DDD initialization. Upon one loop the default entire	
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 3-2-8-8 L2TP Parameters

3.2.8.6 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.

DMVPN	IPsec	GRE	L2TP	PPTP
PPTP Settings				
- PPTP_1				
Enable				
Remote IP	Address			
Username				
Password				
Authenticat	tion	A	luto	•
Global Traf	fic Forwarding			
Remote Su	ıbnet			
Remote Su	ibnet Mask			

Figure 3-2-8-10

РРТР				
Item	escription			
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 Forwarding	All of the data traffic will be sent out via PPTP tunnel once enable this function.			
Remote Subnet	Set the peer subnet of PPTP.			
Remote Subnet Mask	Set the netmask of peer PPTP server.			

Table 3-2-8-9 PPTP Parameters

Advanced Settings	
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 3-2-8-11

PPTP Advanced Settings				
Item	Description			
Local IP Address	Set IP address of PPTP client.			
Peer IP Address	Enter tunnel IP address of PPTP server.			
Enable NAT	Enable the NAT faction of PPTP.			
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	Enter the maximum receive unit. Range: 0-1500.			
MTU	Enter the maximum transmission unit. Range: 0-1500.			
Link Detection Interval (s)	Set the link detection interval time to ensure tunnel connection. Range: 0-600.			
Max Retries	Set the maximum times of retrying to detect the PPTP 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 3-2-8-10 PPTP Parameters

Related Configuration Example

PPTP Application Example

3.2.8.7 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.

Advantages of OpenVPN include:

- Security provisions that function against both active and passive attacks.
- Compatibility with all major operating systems.
- High speed (1.4 megabytes per second typically).
- Ability to configure multiple servers to handle numerous connections simultaneously.
- All encryption and authentication features of the OpenSSL library.
- Advanced bandwidth management.
- A variety of tunneling options.
- Compatibility with smart cards that support the Windows Crypt application program interface (API).

//VPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client	OpenVPN Server	Certific
enVPN Client S	ettings						
OpenVPN_1							
Enable							
Protocol		UDF	>	*			
Remote IP Ad	dress						
Port		1194					
Interface		tun		•			
Authentication		Non	e	¥			
Local Tunnel I	P						
Remote Tunne	el IP						
Enable NAT							
Compression		LZC		v			
Link Detection	Interval(s)	60					
Link Detection	Timeout(s)	300					
Cipher		Non	e	•			
MTU		1500					
Max Frame Si	ze	1500					
Verbose Level		ERF	lor	T			
Expert Options	3						
Local Route							
		Subnet			Subnet Mas	sk	Operation

Figure 3-2-8-12

OpenVPN Client	
Item	Description
Enable	Enable OpenVPN client. A maximum of 3 tunnels is allowed.

Protocol	Select from "UDP" and "TCP".
Remote IP Address	Enter remote OpenVPN server's IP address or domain name.
Port	Enter the listening port number of remote OpenVPN server. Range:
	1-65535.
Interface	Select from "tun" and "tap".
Authentication	Select from "None", "Pre-shared", "Username/Password", "X.509 cert",
Authentication	and "X.509 cert+user".
Local Tunnel IP	Set local tunnel address.
Remote Tunnel IP	Enter remote tunnel address.
Global Traffic Forwarding	All the data traffic will be sent out via OpenVPN tunnel when this function
Clobal Hamer of warding	is enabled.
Enable TLS Authentication	Check to enable TLS authentication.
Username	Enter username provided by OpenVPN server.
Password	Enter password provided by OpenVPN server.
Enable NAT	Enable NAT traversal function.
Compression	Select LZO to compress data.
Link Detection Interval (s)	Set link detection interval time to ensure tunnel connection. Range:
LINK Delection Interval (S)	10-1800.
Link Detection Timeout (s)	Set link detection timeout. OpenVPN will be reestablished after timeout.
LINK Detection Timeout (S)	Range: 60-3600.
Ciphor	Select from "NONE", "BF-CBC", "DE-CBC", "DES-EDE3-CBC",
Cipher	"AES-128-CBC", "AES-192-CBC" and "AES-256-CBC".
MTU	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".
Evenent Options	User can enter some other PPP initialization strings in this field and
Expert Options	separate the strings with blank space.
Local Route	
Subnet	Set the local route's IP address.
Subnet Mask	Set the local route's netmask.
	·

Table 3-2-8-11 OpenVPN Client Parameters

3.2.8.8 OpenVPN Server

The UR32/UR35 supports OpenVPN server to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.

DMVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client	OpenVPN Server
OpenVPN Serv	ver Settings					
Enable						
Protocol		UDP		*		
Port		1194				
Listening IP						
Interface		tun		Ŧ		
Authentication		None		*		
Local Virtual IP						
Remote Virtual I	P					
Enable NAT		×.				
Compression		LZO		Ŧ		
Link Detection Ir	nterval	60				
Cipher		None		*		
мти		1500				
Max Frame Size		1500				
Verbose Level		ERROR		•		
Expert Options						

Figure 3-2-8-13

Local Route			
	Subnet	Netmask	Operation
			(H)
Account			
	Username	Password	Operation
			H.



OpenVPN Server			
Item	Description		
Enable	Enable/disable OpenVPN server.		
Protocol	Select from TCP and UDP.		
Port	Fill in listening port number. Range: 1-65535.		
Listoning ID	Enter WAN IP address or LAN IP address. Leaving it blank refers to all active		
Listening IP	WAN IP and LAN IP address.		
Interface	Select from " tun" and "tap".		
Authentication	Select from "None", "Pre-shared", "Username/Password", "X.509 cert" and		
Authentication	"X. 509 cert +user".		
Local Virtual IP	The local tunnel address of OpenVPN's tunnel.		
Remote Virtual IP	The remote tunnel address of OpenVPN's tunnel.		

Client Subnet	Local subnet IP address of OpenVPN client.			
Client Netmask	Local netmask of OpenVPN client.			
Renegotiation Interval(s)	Set interval for renegotiation. Range: 0-86400.			
Max Clients	Maximum OpenVPN client number. Range: 1-128.			
Enable CRL	Enable CRL			
Enable Client to Client	Allow access between different OpenVPN clients.			
Enable Dup Client	Allow multiple users to use the same certification.			
Enable NAT	Check to enable the NAT traversal function.			
Compression	Select "LZO" to compress data.			
Link Datastian later al	Set link detection interval time to ensure tunnel connection. Range:			
Link Detection Interval	10-1800.			
Cinhar	Select from "NONE", "BF-CBC", "DES-CBC", "DES-EDE3-CBC",			
Cipher	"AES-128-CBC", "AES-192-CBC" and "AES-256-CBC".			
MTU	Enter the maximum transmission unit. Range: 64-1500.			
Max Frame Size	Set the maximum frame size. Range: 64-1500.			
Verbose Level	Select from "ERROR", "WARING", "NOTICE" and "DEBUG".			
Fundant Onting	User can enter some other PPP initialization strings in this field and			
Expert Options	separate the strings with blank space.			
Local Route				
Subnet	The real local IP address of OpenVPN client.			
Netmask	The real local netmask of OpenVPN client.			
Account				
Username & Password	Set username and password for OpenVPN client.			

Table 3-2-8-12 OpenVPN Server Parameters

3.2.8.9 Certifications

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

DMVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client	OpenVPN Server	Certifications
OpenVPN Clie	ent						
- OpenVPM	V client_1						
CA				Browse	Import Export Dele	ete	
Public Ke	ŧΥ			Browse	Import Export Dele	ete	
Private K	ey 🔒			Browse	Import Export Dele	ete	
TA				Browse	Import Export Dele	ete	
Preshare	d Key			Browse	Import Export Dele	ete	
PKCS12				Browse	Import Export Dele	ete	

Figure 3-2-8-15

OpenVPN Client	
Item	Description
CA	Import/Export CA certificate file.
Public Key	Import/Export public key file.
Private Key	Import/Export private key file.
ТА	Import/Export TA key file.
Preshared Key	Import/Export static key file.
PKCS12	Import/Export PKCS12 certificate file.

Table 3-2-8-13 OpenVPN Client Certification Parameters

OpenVPN Server

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

Figure 3-2-8-16

OpenVPN Server					
Item	Description				
CA	Import/Export CA certificate file.				
Public Key	Import/Export public key file.				
Private Key	Import/Export private key file.				
DH	Import/Export DH key file.				
ТА	Import/Export TA key file.				
CRL	Import/Export CRL.				
Preshared Key	Import/Export static key file.				

Table 3-2-8-14 OpenVPN Server Parameters

IPsec				
- IPsec_1				
CA	Browse	Import	Export	Delete
Client Key	Browse	Import	Export	Delete
Server Key	Browse	Import	Export	Delete
Private Key	Browse	Import	Export	Delete
CRL	Browse	Import	Export	Delete

Figure 3-2-8-17

IPsec	
Item	Description
CA	Import/Export CA certificate.
Client Key	Import/Export client key.
Server Key	Import/Export server key.
Private Key	Import/Export private key.
CRL	Import/Export certificate recovery list.

Table 3-2-8-15 IPsec Parameters

IPsec Server

- IPsec Server				
CA	Browse	Import	Export	Delete
Local Certificate	Browse	Import	Export	Delete
Private Key	Browse	Import	Export	Delete
CRL	Browse	Import	Export	Delete

Figure 3-2-8-18

IPsec Server				
Item	Description			
CA	Import/Export CA certificate.			
Local Certificate	Import/Export Local Certificate file.			
Private Key	Import/Export private key.			
CRL	Import/Export certificate recovery list.			

Table 3-2-8-16 IPsec Server Parameters

3.3 System

This section describes how to configure general settings, such as administration account, access service, system time, common user management, SNMP, AAA, event alarms, etc.

3.3.1 General Settings

3.3.1.1 General

General settings include system info and HTTPS certificates.

			For your device sec	urity, please chang	e the default passv	vordl
Network	General	System Time	SMTP	Phone	Email	Storage
System 🔻	System					
	Hostname		ROUTER			
General Settings	Web Login Time	eout(s)	1800			
User Management	Encrypting Clea	intext Passwords				
SNMP	HTTPS Certific	cates				
ААА	Certificate	https.crt	Browse	Import Expo		
Device Management	Key	https.key	Browse	Import Expo	ort Delete	
Events	Save					

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	This function will encrypt all of cleartext passwords into	Enable				
Passwords	ciphertext passwords.	Ellable				
HTTPS Certificates						
	Click "Browse" button, choose certificate file on the PC, and					
Certificate	then click "Import" button to upload the file into router.					
Certificate	Click "Export" button will export the file to the PC. Click					
	"Delete" button will delete the file.					
	Click "Browse" button, choose key file on the PC, and then					
Кеу	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.

			For your device see	curity, please chang	e the default pass	wordl
etwork	General	System Time	SMTP	Phone	Email	Storag
	System Time S	ettings				
rstem 🔻	Current Time		2019-05-14 14:4	48:58 Tues		
General Settings	Time Zone		8 China (Beijin	g) 🔻		
User Management	Sync Type		Sync with Brow	/ser 🔻		
SNMP	Browser Time		2019-05-14 14:4	19:08 Tues		
ААА	Save					
		Figure 3-3	1 2			
URSALINK						
URSALINK			For your device se	curity, please chang	je the default pass	swordl
*	General	System Time	For your device se	curity, please chang Phone	e the default pass Email	CONCERN.
						and an and a second
work	System Time Se					and an and a second
vork	System Time Se Current Time			Phone		CONCERN.
work	System Time Se		SMTP	Phone		COMPLETE:
work	System Time Se Current Time		SMTP 2019-05-14 14:	Phone 48:58 Tues g) •		CONCERN.
work	 System Time Se Current Time Time Zone		SMTP 2019-05-14 14: 8 China (Beijin	Phone 48:58 Tues g) •		and an and a second
work	System Time Se Current Time Time Zone Sync Type		SMTP 2019-05-14 14: 8 China (Beijin Set up Manual	Phone 48:58 Tues g)		CONCERN.
*	System Time Se Current Time Time Zone Sync Type Date Time		SMTP 2019-05-14 14: 8 China (Beijin Set up Manual 2019-05-14	Phone 48:58 Tues g)		CONCERN.
work	System Time Se Current Time Time Zone Sync Type Date		SMTP 2019-05-14 14: 8 China (Beijin Set up Manual 2019-05-14	Phone 48:58 Tues g)		swordl Stora

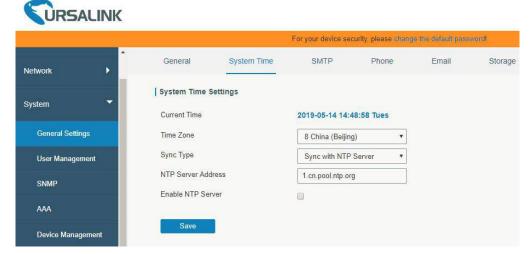


Figure 3-3-1-4

System Time	
Item	Description
Current Time	Show the current system time.
Time Zone	Click the drop down list to select the time zone you are in.
Sync Type	Click the drop down list to select the time synchronization type.
Sync with Browser	Synchronize time with browser.
Browser Time	Show the current time of browser.
Set up Manually	Manually configure the system time.
Superwith NTD Server	Synchronize time with NTP server so as to achieve time synchronization of all
Sync with NTP Server	devices equipped with a clock on network.
Sync with NTP Server	
NTP Server Address	Set NTP server address (domain name/IP).
Enable NTP Server	NTP client on the network can achieve time synchronization with router after
Endule INTP Server	"Enable NTP Server" option is checked.

Table 3-3-1-2 System Time Parameters

3.3.1.3 SMTP

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.

URSALINK				
			For your device sec	urity, please chang
Status	General	System Time	SMTP	Phone
Network 🕨	SMTP Client S	ettings		
	Enable			
System 🔻	Email Address			
General Settings	Password			
	SMTP Server A	ddress		
User Management	Port		25	
SNMP	Encryption		STARTTLS	•
ААА	Save	Test		

Figure 3-3-1-5

SMTP	
Item	Description
SMTP Client Settings	
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

Related Topics

DI Setting Events Setting Events Application Example

3.3.1.4 Phone

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

- 1. Add phone list.
- 2. Select phone numbers and add them to the phone group.
- Go to "Network > Interface > Cellular > Connection Mode > Connect on Demand > Trigger by Call / Trigger by SMS" or go to "System > Events > Event Settings > SMS" and then select the phone group ID.

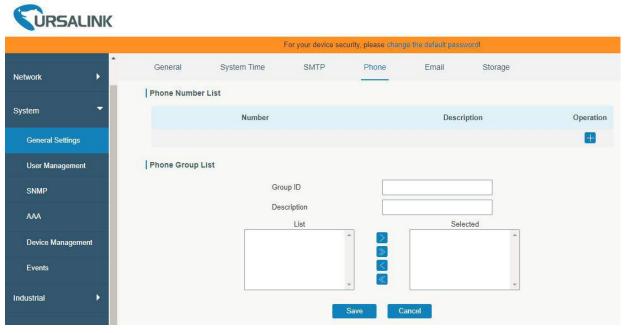


Figure 3-3-1-6

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 3-3-1-4 Phone Settings

Related Topic

Connect on Demand

3.3.1.5 Email

Email settings involve email alarm for events.

- 1. Add email list.
- 2. Select email addresses and add them to the phone group.
- 3. Go to "System > Events > Event Settings > Email" and then select the email group ID.

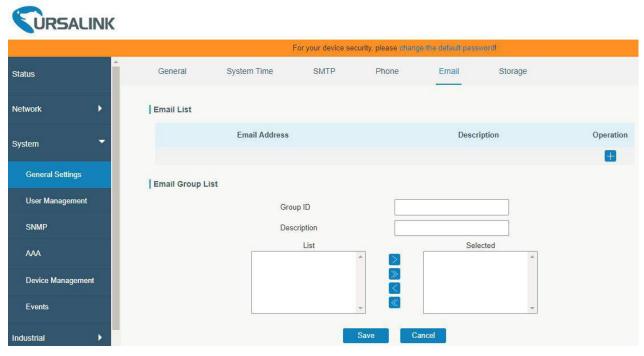


Figure 3-3-1-7

Email				
Description				
Enter the Email address.				
The description of the Email address.				
Set number for email group. Range: 1-100.				
The description of the Email group.				
Show the Email address list.				
Show the selected Email address.				

Table 3-3-1-5 Email Settings

3.3.1.6 Storage

You can view Micro SD card information on this page.

Status	Available
Storage (Capacity/Available)	7.2G/6.8G(1%)
Format	

Figure 3-3-1-8

Storage			
Item	Description		
Status	Show the status of Micro SD card, such as "Available" or "Not Inserted".		
Storage (Capacity/Available)	The total capacity of the Micro SD Card $_{\circ}$		
Format	Format the Micro SD card.		

Table 3-3-1-6 Storage Information

3.3.2 User Management

3.3.2.1 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.

Status	Account	User Management		
Network	Change Account I	nfo	admin	
System	Old Password			
General Settings	New Password Confirm New Passw	ord		
User Management		Ļ		
SNMP	Save			
ААА				
Device Management				



Account	
Item	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.
Confirm New Password	Enter the new password again.

Table 2-3-2-1 Account Settings

3.3.2.2 User Management

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

VRS A	ALINK	(Apply
Status		Acco	unt	User Management			
Network		User L	.ist				
				Username	Password	Permission	Operation
System		1				Read-Only T	
General Settin	gs						•
User Managen	nont						
SNMP			Save				
AAA							
Device Manag	ement						

Figure 3-3-2-2

User Management			
Item	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.		
Permission	 Select user permission from "Read-Only" and "Read-Write". Read-Only: users can only view the configuration of router in this level. Read-Write: users can view and set the configuration of router in this level. 		

Table 3-3-2-2 User Management

3.3.3 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

3.3.3.1 SNMP

The UR32/UR35 supports SNMPv1, SNMPv2c and SNMPv3 version. SNMPv1 and SNMPv2c employ

community name authentication. SNMPv3 employs authentication encryption by username and password.

itatus	SNMP	MIB View	VACM	Trap	MIB
letwork 🕨	SNMP Settin	gs			
	Enable				
System 🔻	Port		161		
General Settings	SNMP Version	n <mark>k</mark>	SNMPv2		*
	Location Infor	mation	Xiamen_C	hina	
User Management	Contact Inform	nation	Xiamen_L	Irsalink_co,.ltd	
SNMP					



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

Table 3-3-3-1 SNMP Parameters

3.3.3.2 MIB View

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

r	View Filter		View OID	Operation
Inclu	ded	•		
Inclu	ded	• 1:	3.6.1.2.1.1	
		View Filter Included Included	Included •	Included • 1

Figure 3-3-3-2

MIB View		
Item	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 3-3-3-2 MIB View Parameters

3.3.3.3 VACM

This section describes how to configure VCAM parameters.

SNMP	MIB View	VACM	Тгар	MIB		
NMP v1 & v2 L	Jser List					
Commun	nity	Permission	MIB Vi	ew	Network	Operation
private	Read	d-write	- ILA	•	0.0.0/0	×
public	Rea	d-only 🔻	none	•	0.0.0.0/0	

Figure 3-3-3-3

VACM			
Item	Description		
SNMP v1 & v2 Use	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 List	:		
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.		

Table 3-3-3-3 VACM Parameters

3.3.3.4 Trap

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

SNMP	MIB View	VACM	Trap	MIB
SNMP Trap				
Enable				
SNMP Version	ı	SNMPv2		Ŧ
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 3-3-3-4 Trap Parameters

3.3.3.5 MIB

This section describes how to download MIB files. The last MIB file "URSA-ROUTER-MIB.txt" is for the UR32/UR35 router.

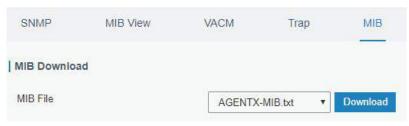


Figure 3-3-3-5

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

Table 3-3-3-5 MIB Download

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.

URSALIN	IK			
Status	Radius	Tacacs+	LDAP	Authentication
Network	Radius Settir	ngs		
System 🔻	Server IP Add	ress]
General Settings	Server Port Key		1812]
User Management	itey			
SNMP	Save			
AAA				



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.

atus	Radius	Tacacs+	LDAP	Authentication
twork 🕨	Tacacs+ Sett	ings		
	Enable		$\underline{\bullet}$	
stem 👻	Server IP Add	ress		
General Settings	Server Port		49	
	Key			
User Management				
SNMP	Save			



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

Table 3-3-4-2 TACACS+ Parameters

3.3.4.3 LDAP

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.

tus	Radius	Tacacs+	LDAP	Authentication
work 🕨	LDAP Settings			
	Enable			
ystem 🔻	Server IP Addres	is		
General Settings	Server Port		389	
	Base DN			
User Management	Security		None	
SNMP	Username			
AAA	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	
	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 3-3-4-3 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.

Status	Radius	Tacacs+	LDAP		Authentication			
Network	Authentication	n Settings						
	Ser	vice	1		2		3	
System 🔻	Con	sole	None	¥	None	٣	None	¥
General Settings	W	eb	None	•	None	*	None	v
	Tel	net	None	T	None	٠	None	Y
User Management	S	SH	None	•	None	v	None	v

Figure 3-3-4-4

Authentication		
Item	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 Ursalink DeviceHub on this page so as to manage the router centrally and

remotely.

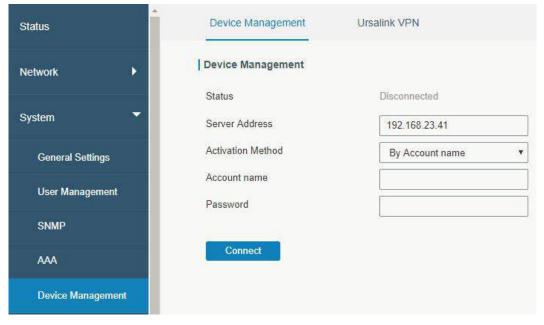


Figure 3-3-5-1

DeviceHub	
Item 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 Device Hub account (amail) and pacculard
Password	Fill in the registered DeviceHub account (email) and password.

Table 3-3-5-1

3.3.5.2 Ursalink VPN

You can connect the device to the UrsalinkVPN on this page so as to manage the router and connected devices centrally and remotely.

Status	Device Management	Ursalink VPN
Network •	UrsalinkVPN Setting	
	Server	
System	Port	8443
General Settings	Authorization Code	
User Management	Device Name	
SNMP	Connect	
AAA		
Davies Menorement	UrsalinkVPN Status	
Device Management	Status	Disconnected
Events	Local IP	1770)
Industrial 🕨	Remote IP	and (
	Duration	ज



UrsalinkVPN		
Item	Description	
UrsalinkVPN Settings		
Server	Enter the IP address or domain name of UrsalinkVPN.	

Port	Enter the HTTPS port number.
Authorization code	Enter the authorization code which generated by UrsalinkVPN.
Device Name	Enter the name of the device.
UrsalinkVPN Status	
UrsalinkVPN Status	Show the connection information about whether the router is connected to the UrsalinkVPN.
Local IP	Show the virtual IP of the router.
Remote IP	Show the virtual IP of the UrsalinkVPN.
Duration	Show the information on how long the router has been connected to the UrsalinkVPN.

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.

URSALINK					💄 admin	E
Status	Events	Events Settin	gs			
Network 🕨	Mark as Read	Delete	Mark All as R	ead Delete All Alarms	l	
System 🝷		Status	Туре	Time	Message	
General Settings	< > 10 ▼	Go to:	GO			
User Management						
SNMP						
AAA						
Events						



Events			
Item	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 Even	ts Settings			
Events Settings				
Enable				
Phone Group List		•		
Email Group List		•		
Events	Record	Email Email Setting	SMS SMS Setting	SNMP
System Startup				
System Reboot				
System Time Upda	te			
VPN Up				
VPN Down				
WAN Up	(
WAN Down				
Link switch		0		
Weak Signal				
Cellular Up				

Figure 3-3-6-2

Cellular Down		
Cellular Data Stats Clear		0
Cellular Data Traffic is running out		
Cellular Data Traffic Overflow		
WLAN Up(AP)		
WLAN Down(AP)		
WLAN Up(Client)		
WLAN Down(Client)		

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.
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.
WLAN Up(AP)	The WLAN(AP) is enabled.
WLAN Down(AP)	The WLAN(AP) has stopped working.

WLAN Up(Client)	The WLAN(Client) is enabled.
WLAN Down(Client)	The WLAN(Client) has stopped working.

Table 4-3-6-2 Events Parameters

Related Topics

Email Setting Events Application Example

3.4 Industrial Interface

The UR32/UR35 router is capable of connecting with terminals through industrial interfaces so as to realize wireless communication between terminals and remote data center.

There are two types of the router's industrial interface: serial port (RS232 and RS485) and I/O (digital input and digital output).

RS232 adopts full-duplex communication. It's generally used for communication within 20m.

RS485 adopts half-duplex communication to achieve transmission of serial communication data with distance up to 120m.

Digital input of I/O interface is a logical variable or switch variable with only two values of 0 and 1. "0" refers to low level and "1" refers to high level .

3.4.1 I/O

3.4.1.1 DI

This section explains how to configure monitoring condition on digital input, and take certain actions once the condition is reached.

	ζ.		
		For your device security, please c	hange the default pa
Status			
Network 🕨	DI Setting		
80 1/20 V	Enable	<u> </u>	
System 🕨	Mode	High Level 🔹	
Industrial	Duration(ms)	100	
muusunai	Action	SMS Email DO	Cellular UP
VO	Save		
Serial Port	Jave		

Figure 3-4-1-1

DI	
Item	Description
Enable	Enable or disable DI.
Mode	Options are "High Level", "Low Level", and "Counter".
Duration (ms)	Set the duration of high/low level in digital input. Range: 1-10000.
Condition	Select from "Low->High", and "High-> Low".
Low->High	The counter value will increase by 1 if digital input's status changes from low level to high level.
High->Low	The counter value will increase by 1 if digital input's status changes from high level to low level.
Counter	The system will take actions accordingly when the counter value reach the preset one, and then reset the counter value to 0. Range: 1-100.
Action	Select the corresponding actions that the system will take when digital input mode meets the preset condition or duration.
SMS	Check to enable SMS alarm.
Phone Group	Set phone group to receive SMS alarm.
SMS Content	Set the content of SMS alarm.
Email	Check to enable Email alarm.
Email Group	Set phone group to receive email alarm.
Email Content	Set the content of email alarm.
DO	Control output status of DO.
Cellular UP	Trigger the router to switch from offline mode to cellular network mode.

Table 3-4-1-1 DI Parameters

Related Topics

DO Setting

Email Setting

Connect on Demand

3.4.1.2 DO

This section describes how to configure digital output mode.

URSALINK For your device security, plea DI DO Status DO Setting Network ۲ Enable . > System Mode v High Level Duration(*10ms) 100 Industrial Save VO

Figure 3-4-1-2

DO		
Item	Description	
Enable	Enable or disable DO.	
Mode	Select from "High Level", "Low Level", "Pulse" and "Custom" .	
Duration (*10ms)	Set duration of high/low level on digital output. Range: 1-10000.	
Initial Status	Select high level or low level as the initial status of the pulse.	
Duration of High Level (*10ms)	Set the duration of pulse's high level. Range: 1-10000.	
Duration of Low Level (*10ms)	Set the duration of pulse's low level. Range: 1-10000.	
The Number of Pulse	Set the quantity of pulse. Range: 1-100.	
Phone Group	Select phone group which will be used for I/O configuration. User can click the Phone Group and set phone number.	

Table 3-4-1-2 DO Settings

Related Topics

DI Setting

3.4.2 Serial Port

This section explains how to configure serial port parameters to achieve communication with serial terminals, and configure work mode to achieve communication with the remote data center, so as to achieve two-way communication between serial terminals and remote data center.



				For your device s
Status		Serial		
Network	•	Serial Settings		
		Enable		
System	×	Serial Type	RS232	•
	-	Baud Rate	9600	•
Industrial		Data Bits	8	•
vo		Stop Bits	1	•
Serial Port		Parity	None	•
		Software Flow Cont	trol 👩	
Modbus Slave		Serial Mode	DTU Mode	•
Modbus Master		DTU Protocol	Transparent	•

Fi	gure	3-	4-2	-1

Serial Settings			
Item	Description	Default	
Enable	Enable or disable serial port function.		
	For UR32, Serial Port is a RS232 port.		
Serial Type	For UR35, Serial Port 1 is a RS232 port and Serial Port 2 is a		
	RS485 port.		
Baud Rate	Range is 300-230400. Same with the baud rate of the	9600	
Daud Nate	connected terminal device.	9000	
Data Bits	Options are "8" and "7". Same with the data bits of the	8	
	connected terminal device.	0	
Stop Bits	Options are "1" and "2". Same with the stop bits of the	1	
	connected terminal device.	T	
Parity	Options are "None", "Odd" and "Even". Same with the parity of	None	
T difty	the connected terminal device.	None	
Software Flow Control	Enable or disable software flow control.	Disable	
Serial Mode	Select work mode of the serial port. Options are "DTU Mode",	Disable	
Senarwoode	"Modbus Master", "Modbus Slave" and "GPS".	DISable	
DTU Mode	In DTU mode, the serial port can establish communication with		
DIOMODE	the remote server/client.		
	In GPS mode, go to "Industrial > GPS > GPS Serial Forwarding"		
GPS	to select corresponding Serial Type, then GPS data will be		
	forwarded to this serial port.		
Modbus Master	In Modbus Master mode, go to "Industrial > Modbus Master"		
	to configure basic parameters and channels.		
Modbus Slave	In Modbus Slave mode, go to "Industrial > Modbus Slave" to		

	configure b	asic parameters.		
		Table 3-4-2-1 Serial Paramete	ers	
Serial Mode	DTU Mode	¥		
DTU Protocol	Transparent	×		
Protocol	ТСР	×		
Keepalive Interval	75	s		
Keepa <mark>live Retry Times</mark>	9			
Packet Size	1024	Bytes		
Serial Frame Interval	100	ms		
Reconnect Interval	10	s		
Specific Protocol				
Register String				
Destination IP Address	5			
Server Ad	dress	Server Port	Status	Operation
				A

Figure 3-4-2-2

DTU Mode				
Item	Description	Default		
DTU Protocol	 Select from "None", "Transparent", "Modbus", "UDP server" and "TCP server". Transparent: the routed is used as TCP client/UDP and transmits data transparently. TCP server: the router is used as TCP server and transmits data transparently. UDP server: the router is used as UDP server and transmits data transparently. Modbus: the router will be used as TCP server with modbus gateway function, which can achieve conversion between Modbus RTU and Modbus TCP. 			
TCP/UDP Server				
Listening port	Set the router listening port. Range: 1-65535.	502		
Keepalive Interval	After TCP connection is established, client will send heartbeat packet regularly by TCP to keep alive. The interval range is 1-3600 in seconds.	75		
Keepalive Retry Times	When TCP heartbeat times out, router will resend heartbeat. After it reaches the preset retry times, TCP connection will be reestablished. The retry times range is 1-16.	9		
Packet Size	Set the size of the serial data frame. Packet will be sent out when preset frame size is reached. The size range is 1-1024. The unit is byte.	1024		
Serial Frame	The interval that the router sends out real serial data stored in the	100		

Interval	buffer area to public network. The range is 10-65535, in milliseconds.	
	Note: data will be sent out to public network when real serial data size	
	reaches the preset packet size, even though it's within the serial frame	
	interval.	

Item I	Description	Default
Transparent		
Protocol	Select "TCP" or "UDP" protocol.	ТСР
Keepalive Interv (s)	After TCP client is connected with TCP server, the client will send heartbeat packet by TCP regularly to keep alive. The interval range is 1-3600, in seconds.	75
Keepalive Retry Times	When TCP heartbeat times out, the router will resend heartbeat. After it reaches the preset retry times, router will reconnect to TCP server. The range is 1-16.	9
Packet Size	Set the size of the serial data frame. Packet will be sent out when preset frame size is reached. The range is 1-1024. The unit is byte.	1024
Serial Frame Interval	The interval that the router sends out real serial data stored in the buffer area to public network. The range is 10-65535, in milliseconds. Note: data will be sent out to public network when real serial data size reaches the preset packet size, even though it's within the serial frame interval.	100
Reconnect Interval	After connection failure, router will reconnect to the server at the preset interval, in seconds. The range is 10-60.	10
Specific Protoco	By Specific Protocol, the router will be able to connect to the TCP2COM software.	
Heartbeat Interv	al By Specific Protocol, the router will send heartbeat packet to the server regularly to keep alive. The interval range is 1-3600, in seconds.	30
ID	Define unique ID of each router. No longer than 63 characters without space character.	
Register String	Define register string for connection with the server.	Null
Server Address	Fill in the TCP or UDP server address (IP/domain name).	Null
Server Port	Fill in the TCP or UDP server port. Range: 1-65535.	Null
Status	Show the connection status between the router and the server.	
Modbus		
Local Port	Set the router listening port. Range: 1-65535.	502

Table 3-4-2-2 DTU Parameters

Table 3-4-2-3 DTU Parameters

Related Configuration Example

DTU Application Example

3.4.3 Modbus TCP

This section describes how to achieve I/O status via Modbus TCP, Modbus RTU and Modbus RTU over TCP.

3.4.3.1 Modbus TCP

You can define the address of the DI and DO ports so as to poll DI's status and control DO's status via Modbus TCP protocol.

Status	Î	Modbus TCP	Modbus RTU	Modbus RTU Over TCP
Network	•	Modbus TCP		
		Enable		
System	•	Port	50	2
- 100 - 100 - 1000-100		DI Address	0	
Industrial	-	DO Address	0	
VO)				
Serial Port		Save		
Modbus Slave				

Figure 3-4-3-1

Modbus TCP			
Item	Description	Default	
Enable	Enable/disable Modbus TCP.	Disable	
Port	Set the router listening port. Range: 1-65535.	502	
DI Address	Define the address of DI, range: 0-255.	0	
DO Address	Define the address of DO, range: 0-255.	0	

Table 3-4-3-1 Modbus TCP Parameters

3.4.3.2 Modbus RTU

You can define the address of the DI and DO ports so as to poll DI's status and control DO's status via Modbus RTU protocol.

Status	Î	Modbus TCP	Modbus RTU	Modbus RTU Over TCP
Network	•	Modbus RTU		
	_	Enable		
System		Serial Port	serial	Ŧ
and the second second		Slave ID	1	
Industrial		DI Address	0	
VO		DO Address	0	
Serial Port		Save		
Modbus Slave				



Modbus RTU			
Item	Description	Default	
Enable	Enable/disable Modbus RTU.	Disable	
Serial Port	Select the corresponding serial port.	serial	
Slave ID	Set slave ID is used for distinguishing different devices on the same link.	1	
DI Address	Define the address of DI, range: 0-255.	0	
DO Address	Define the address of DO, range: 0-255.	0	

Table 3-4-3-2 Modbus RTU Parameters

3.4.3.3 Modbus RTU Over TCP

You can define the address of the DI and DO ports so as to poll DI's status and control DO's status via Modbus RTU over TCP.

Status		Modbus TCP	Modbus RTU	Modbus RTU Over TCP		
Network	•	Modbus RTU Over 1				
System	×	Slave ID	1			
Industrial	•	Device ID Reconnect Interval	10	s		
VO		DI Address DO Address	0			
Serial Port		Server List	U			
Modbus Slave						
Modbus Master		IF)	Port	Status	Operation
						(+

Figure 3-4-3-3

Modbus RTU Over TCP				
Item	Description	Default		
Enable	Enable/disable Modbus RTU over TCP function.	Disable		
Slave ID	Set slave ID is used for distinguishing different devices on the same link.	1		
Device ID	Set device ID. The server will get the device ID to the server for identifying identity so that the server can manage multiple devices.			
Reconnection Interval	The reconnection interval when the device and the server fails to establish connection or disconnected.	10		
DI Address	Define the address of DI, range: 0-255.	0		
DO Address	Define the address of DO, range: 0-255.	0		
Server List				
IP	Enter the IP address of the server.			
Port	Enter the port of the server.Range: 0-65535.			
Status Show the connection status between the router and the server.				

Table 3-4-3-3 Modbus RTU Over TCP Parameters

3.4.4 Modbus Master

UR32/UR35 router can be set as Modbus Master to poll the remote Modbus Slave and send alarm according to the response.

3.4.4.1 Modbus Master

You can configure Modbus Master's parameters on this page.



				For your device s	ecurity, please chan
Status	Î	Modbus Master	Channel		
Network	•	Modbus Master Setti	ng		
		Enable			
System	•	Read Interval	0		s
		Max. Retries	3		
Industrial		Max. Response Time	500		ms
VO		Execution Interval	50] ms
Serial Port		Channel Name		٠	Read
Modbus Slave		Save & Apply			
Modbus Master					

Figure 3-4-4-1

Modbus Master					
Item	Description	Default			
Enable	Enable/disable Modbus master.				
Read Interval/s	Set the interval for reading remote channels. When the read cycle ends, the commands which haven't been sent out will be discard, and the new read cycle begins. If it is set to 0, the device will restart the new read cycle after all channels have been read. Range: 0-600.	0			
Max. Retries	Set the maximum retry times after it fails to read, range: 0-5.	3			
Max. Response Time/ms	Set the maximum response time that the router waits for the response to the command. If the device does not get a response after the maximum response time, it's determined that the command has timed out. Range: 10-1000.	500			
Execution Interval/ms	The execution interval between each command. Range: 10-1000.	50			
Channel Name	Select a readable channel form the channel list.				

Table 3-4-4-1

3.4.4.2 Channel

You can add the channels and configure alarm setting on this page, so as to connect the router to the remote Modbus Slave to poll the address on this page and receive alarms from the router in different conditions.

Modbus Mas	ster	Cha	nnel							
Channel Set	ting									
Channel Sett	ing									
Name	Slave ID	Addres s	Numbe r	Туре	Link	IP Address	Port	Sign	Decima I Place	Operation
	1	0	1	Holding R	TCP 🔻				0	×
										H

Figure 3-4-4-2

Channel Setting				
ltem	Description			
Name	Set the name to identify the remote channel. It cannot be blank.			
Slave ID	Set Modbus slave ID.			
Address	The starting address for reading.			
Number	The address number for reading.			
T	Read command, options are "Coil", "Discrete", "Holding Register (INT16)", "Input			
Туре	Register (INT16)", "Holding Register (INT32)" and "Holding Register (Float)".			
Link	Select TCP for transportation.			
IP address	Fill in the IP address of the remote Modbus device.			
Port	Fill in the port of the remote Modbus device.			
Sign	To identify whether this channel is signed. Default: Unsigned.			
	Used to indicate a dot in the read into the position of the channel. For example: read			
Decimal Place	the channel value is 1234, and a Decimal Place is equal to 2, then the actual value is			
	12.34.			

Table 3-4-4-2

Modbus Master	Channel	
Alarm Setting		
	Name	tunnel1 🔹
	Condition	GE(>) •
	Max. Threshold	0
	Alarm	🗷 SMS 🛛 Email
	Phone Group	
	Email Group	
	Normal Content	Note: \$YEAR/\$MON/\$DAY \$TIME, get NORMAL data \$VALUE from address \$ADDRESS of channel \$NAME. (Abnormal scope is
	Abnormal Content	Note: \$YEAR/\$MON/\$DAY \$TIME, get ABERRANT data \$VALUE from address \$ADDRESS of channel \$NAME. (Abnormal scope is
	Contínuous Alarm	
	Sav	/e Cancel

Figure	3-4-4-3
inguic	5 5

Alarm Setting	
Item	Description
Name	Set the same name with the channel name to identify the remote
	channel.
Condition	The condition that triggers alert.
Min.	Set the min. value to trigger the alert. When the actual value is less than
Threshold	this value, the alarm will be triggered.
Max.	Set the max. value to trigger the alert. When the actual value is more
Threshold	than this value, the alarm will be triggered.
Alarm	Select the alarm method, e.g SMS.
SMS	The preset alarm content will be sent to the specified phone number.
Phone Group	Select the phone group to receive the alarm SMS.
Email Group	Select the Email group to receive the alarm Email.
Normal	When the actual value is restored to the normal value from exceeding the
Content	threshold value, the router will automatically cancel the abnormal alarm
content	and send the preset normal content to the specified phone group.
Abnormal	When the actual value exceeds the preset threshold, the router will
Content	automatically trigger the alarm and send the preset abnormal content to

	the specified phone group.
Continuous	Once it is enabled, the same alarm will be continuously reported.
Alarm	Otherwise, the same alarm will be reported only one time.

Table 3-4-4-3

TCP Forwading

Name	IP	Port	Operation
All			
			A



TCP Forwarding				
ltem	Description			
Name	The name of Modbus Master's channel.			
IP	The IP address of the server which the packets are forwarded to.			
Port	The port of the server's which the packets are forwarded to.			

Table 3-4-4-4

3.4.5 GPS (Only Applicable to GPS Version)

This section give you a detailed introduction to GPS settings, including GPS IP forwarding and GPS serial forwarding.

3.4.5.1 GPS

When you want to receive GPS data, you should enable GPS function on this page.

Status		GPS	GPS IP Forwarding	GPS Serial Forwading
Network	•	Enable		
System	•	Save		
Industrial				
Vo				
Serial Port				
Modbus TCP				
GPS				

Figure 3-4-5-1

3.4.5.2 GPS IP Forwarding

GPS IP forwarding means that GPS data can be forwarded over the Internet.

Status		GPS G	PS IP Forwarding	GPS Serial Forwading
Network	×	GPS IP Forwardin	9	
System	Þ	Enable Type	Client	T
Industrial	-	Protocol Keepalive Interval	TCP Protocol	▼ S
VO		Keepalive Retry	9	times
Serial Port		Reconnect Interval	10	s
Modbus TCP		Include RMC		
GPS		Include GSA		
Maintenance	۲	Include GGA		
		Message Prefix Message Suffix		

Figure 3-4-5-2

Destination IP Address			
Server Address	Server Port	Status	Operation
			+

Figure 3-4-5-3

GPS IP Forwarding					
Item	Description	Default			
Enable	Forward the GPS data to the client or server.	Disable			
Туре	Select connection type of the router. The options are "Client" and "Server".	Client			
Protocol	Select protocol of data transmission. The options are "TCP" and "UDP".	ТСР			
Keepalive Interval	After it's connected with server/client, the router will send heartbeat packet regularly to the server/client to keep alive. The interval range is 1-3600, in seconds.	75			
Keepalive Retry	When TCP heartbeat times out, the router will resend heartbeat. After it reaches the preset retry times, router will reconnect to TCP server. The range is 1-16.	9			
Local Port	Set the router listening port. Range: 1-65535.				
Reconnect Interval	After connection failure, router will reconnect to the server at the preset interval, in seconds. The range is 10-60.	10			
Report Interval	Router will send GPS data to the server/client at the preset interval, in seconds. The range is 1-60.	30			
Include RMC	Whether include RMC in GPS data.				

Include GSA	Whether include GSA in GPS data.			
Include GGA	Whether include GGA in GPS data.			
Include GSV	Whether include GSV in GPS data.			
Message Prefix	Add a prefix to the GPS data.	Null		
Message Suffix	Add a suffix to the GPS data.	Null		
Destination IP Address				
Server Address	Fill in the server address to receive GPS data (IP/domain name).			
Server Port	Fill in the port to receive GPS data. Range: 1-65535.			
Status	Show the connection status between the router and the server.			

Table 3-4-5-1 GPS IP Forwarding Parameters

3.4.5.3 GPS Serial Forwarding

GPS IP forwarding means that GPS data can be forwarded to the serial port.

Status		GPS	GPS IP Forwarding	GPS Serial Forwading
Network	•	GPS Serial Fo	orwading	
System	•	Enable Serial Type	Serial	Ŧ
	-	Trap Interval	30	
Industrial		Include RMC	Ø	
VO		Include GSA Include GGA	2	
Serial Port		Include GSV	2	
Modbus Slave Modbus Master		Save		
GPS				



GPS Serial Forwarding					
Item	Description	Default			
Enable	Forward the GPS data to the preset serial port.	Disable			
Serial Type	Select the serial port to receive GPS data.	serial			
	Router will forward the GPS data to the serial port at the	20			
Report Interval	preset interval, in seconds. The range is 1-60.	30			
Include RMC	Whether include RMC in GPS data.				
Include GSA	Whether include GSA in GPS data.				
Include GGA	Whether include GGA in GPS data.				
Include GSV	Whether include GSV in GPS data.				

Table 3-4-5-2 GPS Serial Forwarding Parameters

3.5 Maintenance

This section describes system maintenance tools and management.

3.5.1 Tools

Troubleshooting tools includes ping, traceroute and packet analyzer.

3.5.1.1 Ping

Ping tool is engineered to ping outer network.

URSA	LINK			
				For your device security, please change the default
Network	•	Ping	Traceroute	Packet Analyzer
System	۲	IP Ping Host		Ping Stop
Industrial	•			
Maintenance	-			
Tools				

Figure 3-5-1-1

PING	
Item	Description
Host	Ping outer network from the router.

Table 3-5-1-1 IP Ping Parameters

3.5.1.2 Traceroute

Traceroute tool is used for troubleshooting network routing failures.

			For your device security, please change the
Network I	Ping	Traceroute	Packet Analyzer
System I	Traceroute		Trace
Industrial I			
Maintenance	-		
Tools			
		Figure 3-5-1-2	

Item	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.

URSA	LINK				
				For your device security,	please chan
Network	,	Ping	Traceroute	Packet Analyzer	
System	•	Packet Ana		Алу	•
Industrial	•	IP Address			
Maintenance	-	Port Advanced			
Tools		Start	Stop	Download	

Figure 3-5-1-3

Packet Analyzer			
Item	Description		
Ethernet Interface	Select the interface. Select from: ANY/LAN/WAN/Cellular/gre0/gretap0/Looplack/tepl0/tun I0/WLAN1 (default is ANY).		
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

3.5.2 Schedule

This section explains how to configure scheduled reboot on the router.

VRS	ALINK	K				2 2	admin E
Status		Schedule					
Network	×	Schedule					
System	×	Schedule	Fre	equency	Hour	Minute 0	Operation
Industrial	×			<u>, </u>			
Maintenance	•	Save					
Tools							
Schedule							

Figure 3-5-2-1

Schedule		
Item	Description	
Schedule	Select schedule type.	
Reboot	Reboot the router regularly.	
Frequency	Select the frequency to execute the schedule.	
Hour & Minute	Select the time to execute the schedule.	

Table 3-5-2-1 Schedule 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.

Related Configuration Example

Logs and Diagnostics

3.5.3.1 System Log

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

	System Log Log Settings	
к 🕨	Download	
	File Log File Download	
1 •	Log	
ial 🕨	View recent(lines) 20 v	
nance 🔹	Tue Oct 31 10:15:35 2017 daemon.warn zebra[1164]: libgsm/gsm.c:376 yeastar_mobile_handle_event: fail Tue Oct 31 10:15:45 2017 daemon.warn zebra[1164]: [1509416145.356771] GSM Event: sim failed! Tue Oct 31 10:15:53 2017 daemon.warn zebra[1164]: [1509416153.913374] GSM Event: sim failed! Tue Oct 31 10:15:53 2017 daemon.warn zebra[1164]: libgsm/gsm.c:376 yeastar_mobile_handle_event: fail Tue Oct 31 10:15:03 2017 daemon.warn zebra[1164]: [1509416163.531890] GSM Event: sim failed!	
edule	Tue Oct 31 10:16:12 2017 daemon.warn zebra[1164]: [1509416172.75885] GSM Event: sim failed! Tue Oct 31 10:16:12 2017 daemon.warn zebra[1164]: libgsm/gsm.c:376 yeastar_mobile_handle_event: fail	count 2!
	Tue Oct 31 10:16:21 2017 daemon.warn zebra[1164]: [1509416181.925775] GSM Event: sim failed! Tue Oct 31 10:16:30 2017 daemon.warn zebra[1164]: [1509416190.474367] GSM Event: sim failed!	
rade	Tue Oct 31 10:16:30 2017 daemon.warn zebra[1164]: libgsm/gsm.c:376 yeastar_mobile_handle_event: fail_ Tue Oct 31 10:16:39 2017 daemon.warn zebra[1164]: [1509416199.822249] GSM Event: sim failed! Tue Oct 31 10:16:48 2017 daemon.warn zebra[1164]: [1509416208.932086] GSM Event: sim inserted!	count 21
kup and Restore	Tue Oct 31 10:17:11 2017 daemon.warn zebra[1164]: [1509416231.793745] GSM Event: SIM 1 dchan is up Tue Oct 31 10:17:15 2017 daemon.info zebra[1164]: Try to set TE Link Param	- And
oot	Tue Oct 31 10:17:15 2017 daemon.info zebra[1164]: Try to set TE Link Param Tue Oct 31 10:17:18 2017 daemon.info ntpd[1506]: Listen normally on 12 cellular0 10.53.241.18:123 Tue Oct 31 10:17:18 2017 daemon.info ntpd[1506]: Listen normally on 13 cellular0 [fe80::9417.ceff.fe8c:8cf. Tue Oct 31 10:17:35 2017 daemon.info ntpd[1506]: 108.59.2.24 local addr 10.53.241.18 -> Tue Oct 31 10:19:30 2017 daemon.info ntpd[1506]: 108.59.2.24 local addr 10.53.241.18 ->	7%9] 123

Figure 3-5-3-1

System Log	
Item	Description
Download	Download log file.
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

3.5.3.2 Log Settings

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

System Log	Log Settings			
Remote Log Server				
Enable				
Syslog Server Address]
Port		514		
Local Log File				
Storage		local	۲]
Size		1024		кв
Log Severity		Info	v	
		6	1	1

Figure 3-5-3-2

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

Table 3-5-3-2 System Log 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.

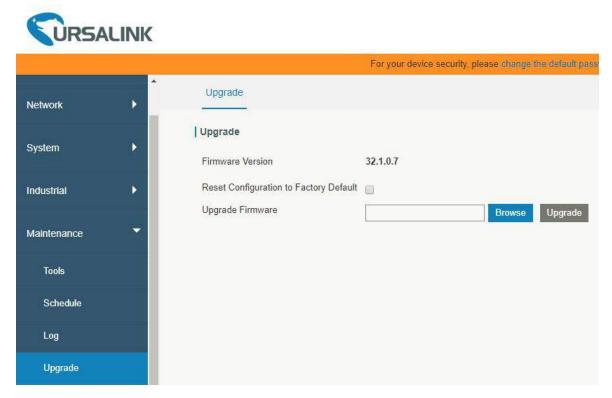


Figure 3-5-4-1

Upgrade			
Item	Description		
Firmware Version	Show the current firmware version.		
Reset Configuration to	When this option is checked, the router will be reset to factory		
Factory Default	defaults after upgrade.		
Upgrade Firmware	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.

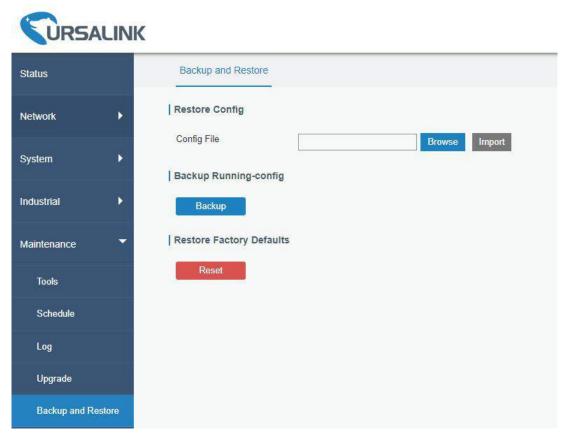


Figure 3-5-5-1

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 and return to the login page. We strongly recommend clicking "Save" button before rebooting the router so as to avoid losing the new configuration.

URSALINK				
Status		Reboot		
Network	Þ	Reboot		
System	X			
Industrial	F			
Maintenance	•			
Tools				
Schedule				
Log				
Upgrade				
Backup and Rest	ore			
Reboot				

Figure 3-5-6-1

Chapter 4 Application Examples

4.1 Restore Factory Defaults

4.1.1 Via Web Interface

- 1. Log in web interface, and go to "Maintenance > Backup and Restore".
- 2. Click "Reset" button under the "Restore Factory Defaults".

You will be asked to confirm if you'd like to reset it to factory defaults. Then click "Reset" button.

Status	Backup and Restore
Network	Restore Config
System 🕨	Config File Browse Import
Industrial 🕨 🕨	Backup Running-config
Maintenance 🔻	Restore Factory Defaults
Tools	Reset 3
Schedule	
Log	
Upgrade	
Backup and Restore (1)	
Backup Running-config	
Backup	
Restore Factory Defaults	
Reset	×
	Reset operation will erase all configuration data on Router and
	reset the system to factory defaults. Continue?
	Reset Cancel

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 login page pops up again, which means the router has already been reset to factory defaults successfully.



Related Topic

Restore Factory Defaults

4.2.2 Via Hardware

Locate the reset button on the router, and take corresponding actions based on the status of SYSTEM LED.

SYSTEM LED	Action
Blinking	Press and hold the reset button for more than 15 seconds.
Static Green \rightarrow	Release the button and wait.
Rapidly Blinking	
$Off \rightarrow Blinking$	The router is now reset to factory defaults.

4.2 Firmware Upgrade

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

1. Go to "Maintenance > Upgrade".

- 2. Click "Browse" and select the correct firmware file from the PC.
- 3. 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.

	LINK
Status	Upgrade 2
Network	Firmware Version 2.0.0.19
System	Reset Configuration to Factory Default 3 4
Industrial	Upgrade Firmware Browse Upgrade
Maintenance	-
Tools	
Schedule	
Log	
Upgrade	1
VIRSA	LINK
Status	Upgrade
Network	Firmware Version 2.0.0.19
System	Reset Configuration to Factory Default
Industrial	Upgrade Firmware C:\fakepath\2.0.0.19.bin Browse Upgrade D:\fakepath\2.0.0.19.bin Browse Upgrade D:\fakepath\2.0.0.19.bin Browse Browse Upgrade D:\fakepath\2.0.0.19.bin Browse Brow
Maintenance	•
Tools	
Schedule	
Log	
Upgrade	

URSA	IK	2
Status	Upgrade	
Network	Upgrade	
System	Firmware Version Reset Configuration to Factory Default	2.0.0.19
Industrial	Upgrade Firmware	C:\fakepath\2.0.0.19.bin Browse Upgrade 🔇 Importing firmware Please stay on this page till upgrade is finished.
Maintenance		
Tools	·	
Schedule	Please keep t	he power on during upgrade.
Log		
Upgrade		

Related Topic

Upgrade

4.3 Events Application Example

Example

In this section, we will take an example of sending alarm messages by email when the following events occur and recording the event alarms on the Web GUI.

Events	Actions to make events occur (for test)
Router system start up.	Plug the power supply of the router.
Router system time update.	Set up system time manually.

Configuration Steps

- 1. Go to "System > Events > Events Settings" and enable Event settings.
- 2. Check corresponding events for record and email alarm, and then click "Save" button as below.

Network	Events Even	nts Settings			
System 🔻	Events Settings	Ø			
General Settings	Phone Group List	X	•		
User Management	Email Group List	1	•		
SNMP	Events	Record	Email Email Setting	SMS SMS Setting	SNMP
ААА	System Startup	o 🖉	2		
Device Management	System Reboo	t			
Events	System Time Upd	late 🖉			

Configure the corresponding parameters including email sending settings and email groups as below.
 Click "Save" and "Apply" button to make the changes take effect.

URSALIN	K						
				For your device :	security, please	change the defau	It password!
Status	G	eneral	System Time	SMTP	Phone	e Emai	I Storage
Network	SN	ITP Client Setting	js				
	En	able					
System 🔻	En	nail Address		admin@ursal	link.com		
General Settings	Pa	ssword					
	SN	ITP Server Address	3	smtp.ursalink	com		
User Management	Po	rt		25			
SNMP	En	cryption		STARTTLS		v	
							Apply
*			For your device	security, please change	the default passw	ordl	
etwork	General	System Time	SMTP	Phone	Email	Storage	
rstem 🔻	Email List						
General Settings		Email Addre	ess		Desc	ription	Operation
User Management		support@ursalink.co	m		test		
							+
SNMP	Email Group	List					
AAA		Group ID		Description		Email Address	Operation
Device Management		4		test		support@ursalink.cor	
Events							H
dustrial 🕨	Save						

To test the functionality of Alarm, please take the corresponding actions listed above.
 It will send an alarm e-mail to you when the relevant event occurs.
 Refresh the web GUI, go to "Events > Events", and you will find the events records.

rk as Read	Delete	Mark All as Read	Delete All Alarms	
	Status	Туре	Time	Message
0	Unread	System Time Update	2019-05-15 09:39:08	system time update
	Unread	System Startup	2019-05-09 11:48:25	system startup

Related Topics

Events Email Setting

4.4 Logs and Diagnostics

System log of the UR32/UR35 supports 3 types of output method, including Web and Remote Log Server.

Application 1

Obtain system log on Web.

Go to "Maintenance > Log > System log", and you will see the log is listed in the box.

		in
Status	System Log 2 Log Settings	
Network	Download	
System	File Log File Download	
Industrial 🕨 🕨	View recent(lines)	
Maintenance T	Thu Nov 2 09:33:56 2017 daemon.warn zebra[1287]; [1509586436.196318] GSM Event: SIM 1 dchan is down! Thu Nov 2 09:34:01 2017 daemon.warn zebra[1287]; [1509586441.264493] GSM Event: SIM 1 dchan is down! Thu Nov 2 09:34:03 2017 daemon.warn zebra[1287]; [1509586443.323906] GSM Event: SIM 1 dchan is down!	-
Tools	Thu Nov 2 09:34:12 2017 daemon.warn zebra[1287]: [1509586452.671092] GSM Event: sim failed! Thu Nov 2 09:34:20 2017 daemon.warn zebra[1287]: [1509586460.948779] GSM Event: sim failed!	
Schedule	Thu Nov 2 09:34:21 2017 daemon.warn zebra[1287]: libgsm/gsm.c:377 yeastar_mobile_handle_event: fail_count 2! Thu Nov 2 09:34:31 2017 daemon.warn zebra[1287]: [1509586471.305038] GSM Event: sim inserted! Thu Nov 2 09:34:44 2017 daemon.warn zebra[1287]: [1509586484.538713] GSM Event: SIM 1 dchan is down!	
Log (1)	Thu Nov 2 09:34:49 2017 daemon.warn zebra[1287]: [1509586489.610319] GSM Event: SIM 1 dchan is down! Thu Nov 2 09:34:50 2017 daemon.warn zebra[1287]: [1509586490.663912] GSM Event: SIM 1 dchan is down! Thu Nov 2 09:35:04 2017 daemon.warn zebra[1287]: [1509586504.391406] GSM Event: sim failed!	
Upgrade	Thu Nov 2 09:35:12 2017 daemon.warn zebra[1207]; [1509586512:973232] GSM Event: sim failed! Thu Nov 2 09:35:13 2017 daemon.warn zebra[1287]: [1509586512:973232] GSM Event: sim failed!	
Backup and Restore	Thu Nov 2 09:35:22 2017 daemon.warn zebra[1287]: [1509586522 984902] GSM Event: sim inserted! Thu Nov 2 09:35:36 2017 daemon.warn zebra[1287]: [1509586536 260947] GSM Event: SIM 1 dchan is down! Thu Nov 2 09:35:41 2017 daemon.warn zebra[1287]: [1509586541.326197] GSM Event: SIM 1 dchan is down!	
Reboot	Thu Nov 2 09:35:43 2017 daemon.warn zebra[1287]: [1509586543.379108] GSM Event: SIM 1 dchan is down! Thu Nov 2 09:35:52 2017 daemon.warn zebra[1287]: [1509586552.870213] GSM Event: sim failed!	
АРР 🕨	Thu Nov 2 09:36:01 2017 daemon.warn zebra[1287]: [1509586561.139046] GSM Event: sim failed! Thu Nov 2 09:36:01 2017 daemon.warn zebra[1287]: libgsm/gsm.c:377 yeastar_mobile_handle_event: fail_count 2!	•

Application 2

Send the system log to the remote syslog server. Server IP: 110.22.14.43; Port: 514 Go to "Maintenance > Log > Log Settings" to configure the parameters as below.

	LINK	ζ		5 Apply admin
Status		System Log	Log Settings	
Network	×	Remote Log Server		
System	•	Enable Syslog Server Address	3 < 110.22.14.43	
Industrial	•	Port	514	
Maintenance	•	Storage	local •	
Tools		Size	1024 KB	
Schedule		Log Severity	Info •	
Log	1	Save (4)		

Then click "Save" and "Apply" button.

Related Topic

System Log

4.5 SNMP Application Example

Before you configure SNMP parameters, please download the relevant "MIB" file from the router'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 "System > SNMP > MIB" and download the MIB file "URSA-ROUTER-MIB.txt" to PC.

CURSAL	INK					
Status		SNMP	MIB View	VACM	Тгар	мів (2)
Network	×	MIB Download				
System	•	MIB File		3 URSA-RC	OUTER-MIE 🔻	Download (4)
General Settings						
User Management						
SNMP	1					

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

ManageEngine MibBrov	wser Free Tool			_		×
<u>File</u> dit <u>View</u> <u>Operations</u>	s <u>H</u> elp					
، 🖬 🔥 🖻 🏀	🎒 🖻 🖷) 🗊 🔊 🧠 🏹 🖄 🖬 🛎 🛫 🔤) 🧔 🖉	More F	unload Tee Tools	
Loaded MibModules 	Host Community Set Value Device Type Device Type Ider Suggested OIDs Object ID	ocalhost Port Write Communit ified Not Available None	161 tv	C Reload		

Click the "+" button beside "URSA-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>F</u> ile <u>E</u> dit ⊻iew <u>O</u> perations <u>H</u> elp										
🗞 🍰 🗈 ጰ 🖶 🎒 🖻	a 🐚 🗊 🔊	0 3 (🔬 📾	*	🛫 🚥	٩	×	More F	unioad Tee Tools	
Loaded MibModules URSA-ROUTER-MIB Constraints URSA-CUTER-MIB Constraints URSA-CONTER-MIB Constraints URSA-CONTER-MIB URSA-	Host Community Set Value Device Type — Device Type Ider Suggested OIDs Object ID . Loading MIBs "E:0 MIB(s) Loaded Su	Nc iso. org. do URSA MIB\	URSA-ROUTE		Port Write Comm enterprises.	nunity	161	~	Reload	
usCellularApn wsCellularUsernar usCellularPasswo	Description Mul	tiVer.								~
uscendrar asswu 	Syntax Access	ti yar			Status Reference	9				
< >>	Object ID . 1.	3.6.1.4.1	. 50234. 1. 6							
Global View 🗌	Description									

 Go to "System > SNMP > SNMP" on the router's WEB GUI. Check "Enable" option, then click "Save" button.

Status	SNMP 6 MIB View VACM Trap MIB
Network	SNMP Settings
System 🔻	Enable Port 161
General Settings	SNMP Version
User Management	Location Information Xiamen_China Contact Information Xiamen_Ursalink_co,.ltd
snmp (5)	
AAA	Save (8)

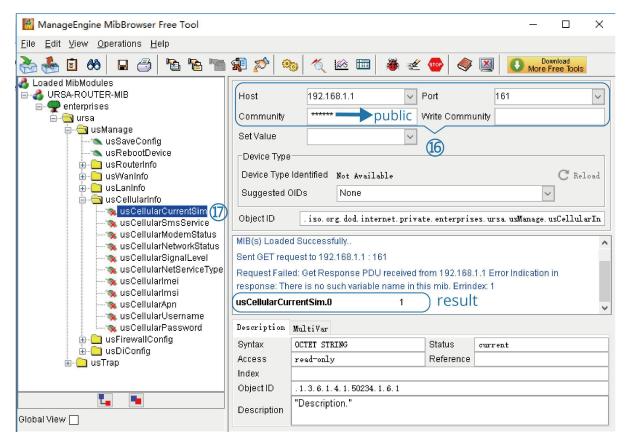
4. Go to "System > SNMP > MIB View". Click + to add a new MIB view and define the view to be accessed from the outside network. Then click "Save" button.

Status		SNMP	MIB View	9	VACM	Тгар	MIB	
Network		View List						
		Vi	ew Name		Vie	w Filter	View OID	Operation
System	10	Cellular			Included	۲	1.3.6.1.4.1.50234.1.6	
General Setting	S							8

5. Go to "System > SNMP > VACM". Click 🛨 to add a new VACM setting to define the access authority for the specified view from the specified outside network. Click "Save" and "Apply" to make the changes take effect.

	NK (5 Apply 2 admin	n E
Status	SNMP MIB View VACM (1) Trap MIB	
Network 🕨	SNMP v1 & v2 User List	
	Community Permission MIB View Network C	Operation
System 🔻	Image:	×
General Settings		8
User Management	Save 14	
SNMP		

 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.



Related Topic

<u>SNMP</u>

4.6 Network Connection

4.6.1 Cellular Connection

The UR32/UR35 routers have two cellular interfaces, named SIM1 & SIM2. Only one cellular interface is active at one time. If both cellular interfaces are enabled, SIM1 interface takes precedence as default.

Example

We are about to take an example of inserting a SIM card into SIM1 slot of the UR32/UR35 and configuring the router to get Internet access through cellular.

Configuration Steps

- 1. Go to "Network > Interface > Cellular > Cellular Setting" and configure the cellular info.
- 2. Enable SIM1.
- Choose relevant network type. "Auto", "4G First", "4G Only", "3G First", "3G Only", "2G First" and "2G only" are optional.

CURSALIN	K			1 atres 6
Skatusi.	Pod WAN	LAN VLAN Trank	Cellin	
ebucat -	Cellular Setting		2 Cellula	r
		SIM1	SIM2	
Interface -	Enable	*	*	
Frend	Tietwork Type	4G Pine	* Auto *	
1 Inter	face	4G First 4G Only		
Turren	IdCe seruns	3G Finit 3G Dely		
DONS	innert.	2G Paul 2G Only		
	Access Number			
Link Beckup	PIN Code	3"Auto	or others	
Routing	Authentication Type Roamting	S Auto	or others	
VEN	SWS Center			
yalates 1	Connection Setting			
	Dual SIM Strategy	8		
oustral	Englis NAT			
tertenarice	ICMP Server	8888		
	Secondary ICMP Server	114-114-114-114		
PP	PNG times	5		
	Total Packof Loss Rate	20		
	SWS Settings			
	SVS Myde	PDU	*	
	10.000			
Status Notwork	Port www.	LAN YLAN THIN	Creater Loopbark	(5) Apply
	Endle	SIM1	5862	
	Linese Nations Type	H Auto		
Fiswall	APN		Auto Y	
Qeti i	Usernanta	1	-	
	Passent	1		
CONS	Acties Number		5 i	
Link Beckup	PIN Code	1		
Faulty	Authentication Type	Asto	* Auto *	
	Roaming	0		
VEN	SNS Carter			
system	Connection Setting Dual SBM Strategy	8		
marchie	Enable NAT	2		
	ICHIP Server	8888		
Martenance	Secondary ICMP Server	114 TH		
ARD	PhG times	5		
1.00	Trial Packet Loss Rate	29		
	④ Save			
	3 Jave	PDU	•	
		landing.		
	Saint			

Click "Save" and "Apply" for configuration to take effect.

4. Check the cellular connection status by WEB GUI of router.

Click "Status > Cellular" to view the status of the cellular connection. If it shows 'Connected', SIM1 has dialed up successfully.

URSALIN	IK							🙎 admin
		Summary	Celular	Network	VPN	Router Information	Host List	
	12.51	Modem						
		Status		Ready				
ystem		Modern Model		EC25				
	/862	Current SIM		SM1				
oustrial		Signal Level		28asu (-67dBm	0			
		Register Status		Registered (Ho	me metwork)			
Maintenance		ilidiSi		460019235512	954			
		ICCID		898601178380	19237649			
		Network Provider		CHNUNCOM				
		Network Type		UE				
		PLMN ID		46001				
		Local Area Code		6922				
		Cell ID		812c63d				
		IME)		861107030259	185			
		Network			-			
		Status		Connected	$< c_{c}$	onnected		
		IP Address		10.63 188.23	1			
		Netmask		265 256 256 24	10		-	
		Gateway		10.63 188.24				
		ONS		218 104 128 10	16			
		Connection time		0 days, 00:001	n l			

5. Check out if network works properly by browser on PC.

Open your preferred browser on PC, type any available web address into address bar and see if it is able to visit Internet via the UR32/UR35 router.

Related Topic

Cellular Setting

Cellular Status

4.6.2 Ethernet WAN Connection

When both "WAN" and "Cellular" interfaces are enabled and available, cellular interfaces will take precedence by default.

Example

WAN port of the UR32/UR35 is connected with Ethernet cable to get Internet access.

Configuration Steps

1. Go to "Network > Interface > Cellular" and disable "SIM1" and "SIM2". Then click "Save" button.

	<					
Status	Port	WAN	LAN	VLAN Trunk	Cellular (2)	Loopback
Network 🔻	Cellular Se	tting				
Interface ①	Enable		SIM1		SIM2	
Firewall	Network Typ	De	Auto		Auto	Ŧ

2. Go to "Network > Interface > WAN" to configure WAN parameters. The following examples of static IP type, DHCP Client type, and PPPoE type are listed for your reference.

(1) Static IP

(2)

VPN

		please change the default password!
Status		LAN Cellular Loopback
Network -	Port LAN1/WAN	
Interface (4)	Connection Type Static IP	v
Firewall	IPv4 Address 192.168.23.249	
QoS	Netmask 255.255.255.0	
DHCP	IPv4 Gateway 192.168.23.1	
DDNS	Prefix-length	
Link Failover	IPv6 Gateway	
	MTU 1500	
Routing	Primary DNS 114.114.114	
VPN	Secondary DNS 8.8.8.8	
System	Enable NAT	
Industrial	Multiple IP Address	
Maintenance	IP Address	Netmask Operation
		+
	Save & Apply	
DHCP Client		
	For you	r device security, please change the default passwor
Status	Port WAN (5) Bridge	Switch WLAN Cellular
Network 👻	— WAN_1	
Interface (4)	Enable	
Firewall	Port LAN1/V	WAN
		Client
QoS		
DHCP	Use Peer DNS	
DDNS		
	Primary DNS 114.114	4.114.114
Link Failover	Secondary DNS 8.8.8.8	

Save & Apply 🔿

(3) PPPoE

		For your device securit	y, please change the defa	ult password!
▲ Status	Port WAN 5	Bridge Switch	WLAN	Cellular
Network 🔻	— WAN_1			
Interface (4)	Enable	✔ LAN1/WAN		
Firewall	Connection Type	PPPoE		
QoS	Username	059293684762		
DHCP	Password	•••••		
DDNS	Link Detection Interval(s)	60		
Link Failover	Max Retries	3		
	MTU	1500		
Routing	Use Peer DNS			
VPN	Primary DNS	114.114.114.114		
System 🕨	Secondary DNS	8.8.8.8		
	Enable NAT			
Industrial 🕨 🕨				
Maintenance	Save & Apply (7)			

Note: if you select PPPoE type, please check the "Username" & "Password" with your local ISP. Click "Save & Apply" button to make the changes take effect.

Related Topic

WAN Setting WAN Status

4.7 WAN Failover/Backup Application Example

4.7.1 Dual SIM Backup

Example

In this section we will take an example of inserting two SIM cards into the UR32/UR35. When one SIM fails, router will try to connect with the other SIM as backup link.

Configuration Steps

 Go to "Network > Interface > Cellular" to enable SIM1 and SIM2. Leave the network type as "Auto" by default.

Status	Port	WAN	LAN	N	VLAN Trunk		Cellular (2)	Loopback
Network 🔻	Cellular Set	ting						
Interface (1)	Enable		3	SIM1			SIM2	
Firewall	Network Type	e	U	Auto		•	Auto	T
QoS	APN							
DHCP	Username							
DDNS	Password Access Num	bor						
Link Failover	PIN Code	bei						
Routing	Authenticatio	n Type		Auto		•	Auto	•
VPN	Roaming							
	SMS Center							
System 🕨	Connection	Setting						
	Dual SIM Str	ategy						

2. Enable "Dual SIM Strategy", and configure the corresponding options as below. ICMP server can be configured as any reachable IP address.

					8 Apply
Status	Port WAN	LAN	VLAN Trunk	Cellular	Loopback
Network 🔻	Roaming SMS Center				
Interface	Connection Setting				
Firewall	Dual SIM Strategy Primary SIM Card	5 C	1	•	
QoS	Switch to backup SIM card w	hen ICMP 🖉			
DHCP	detection fails Swtich to backup SIM card w	hen the 🖉		> 6	
DDNS	connection fails Switch to backup SIM card wi				
Link Failover	roaming is detected	hen			
Routing	Enable NAT				
VPN	Secondary ICMP Server	8.8.8	8		
System 🕨	PING times	5			
Cystem P	Packet Loss Rate	20		%	
Industrial 🕨 🕨	SMS Settings				
Maintenance	SMS Mode	PDU		•	
	Save 7				

Then click "Save" and "Apply" button.

	ALINK					
Status		Overview	Cellular	Network	VPN	Routing
Network	•	Modem				
		Status		Ready		
System	•	Model		EC25		
Industrial	۱.	Current SIM		SIM1		
muusinai		Signal Level		15asu (-83dBr	n)	
Maintenance	•	Register Status		Registered (Ho	ome network)	
		IMSI		460019987103	3071	
		ICCID		898601178380	19196629	
		ISP		CHN-UNICOM	I	
		Network Type		LTE		
[N	etwork					
S	tatus		Connected)		
IF	Address		10.105.39.3	3		

3. Go to "Status > Cellular", and you will see the router is connected to the network via SIM1.

4. You can remove SIM1 to make the router fail to connect to network via it. Go to "Status > Cellular" again, and you will see the router is connected to the network through SIM2.

Status		Overview	Cellular	Network	VPN	Routing
Network	•	Modem				
		Status		Ready		
System	×	Modei		EC25		
Industrial		Current SIM		SIM2		
indecinal a		Signal Level		15asu (-83dBm	i)	
Maintenance	Þ	Register Status		Registered (Ho	me network)	
		IMSI		460019987103	071	
APP		ICCID		898601178380	19196629	
	Netw	ork				
	Statu	S	Co	nnected		
		dress		.63.223.44		

Now SIM2 becomes the main SIM, and SIM1 runs as the backup. The router won't reconnect via SIM1 until SIM2 fails.

Related Topic

Cellular Setting Cellular Status

4.7.2 WAN Failover

WAN failover involves in Ethernet WAN interface and cellular interface. Either can be used as main WAN interface. If the main interface fails, the router will automatically failover to the backup interface until the main interface functions properly again.

Application Example

An UR32 router is connected with PC via LAN port, and WAN of the UR32 is connected to Internet via wired network. Configure WAN failover in the router so that it can failover to cellular to get Internet access in case of the malfunction of wired network and failback to wired network when it's available again. Please refer to the topological graph below.



Configuration Steps

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

URSALINK			
		For your device security, please change the de	fault password!
Status	Port WAN Dridg	e Switch WLAN Cell	ular Loopback
Network 🔫	Enable Port	Z LAN1/WAN	
Interface ①	Connection Type	Static IP V	
Firewall	IPv4 Address	192.168.23.249	
QoS	Netmask IPv4 Gateway	255.255.255.0	
DHCP	IPv6 Address	fe80::26e1:24ff:fef0:2579	
DDNS	Prefix-length	64	
Link Failover	IPv6 Gateway		
Routing	MTU	1500	
VPN	Primary DNS Secondary DNS	8.8.8	
System >	Enable NAT		
Industrial >	Multiple IP Address		
	IP Addre	ss	Netmask Operation
Maintenance >			H
	Save & Apply (4)		

When configuration is done, click "Save & Apply" button.

Then confirm if it is able to visit Internet on PC through the UR32.

2. Go to "Network > Interface > Cellular", enable cellular settings and click "Save" button.

Status	Port WAN	LAN VLAN Trunk	Cellular (5) Loopback
	Joenana oetang		
Network 🔻		SIM1	SIM2
Interface	Enable	6	
Firewall	Network Type	Auto	▼ Auto ▼
	APN		
QoS	Username		
DHCP	Password		
DDNS	Access Number		
Link Failover	PIN Code		
	Authentication Type	Auto	▼ Auto ▼
Routing	Roaming		
VPN	SMS Center		
Queters 1	Connection Setting		
System 🕨	Dual SIM Strategy		
Industrial 🕨 🕨	Enable NAT ICMP Server		
	Secondary ICMP Server	8.8.8	
Maintenance 🕨 🕨	PING times	114.114.114	
	Packet Loss Rate	5	%
	Fackel LUSS Rale	20	/0
	SMS Settings		
	SMS Mode	PDU	v
	Save (7)		

3. Go to "Network > Link Failover > SLA" and configure SLA probe. The default probe type is ICMP. The destination address is the host address which can be probed by ICMP in public network or private network. Other parameters can be kept as default value.

Status	SLA	Track	VRRP	WA	N Fallover							
Vetwork	SLA Entry											
Interface	ID	Туре	Destination	i Address	Secondary Destination Address	Data Size	Interval(s)	Timeout(ms)	PING Times	Packet Loss Rate	Start Time	Operation
Firewall	1	icmp-echo	• 114 114 11	4.114	88.8.8	56	30	5000	5	20	now 🔻	×
QoS												0
DHCP	Save											
DONS												

4. Go to "Network > Link Failover > Track" for Track parameters configuration. You can use the default Track settings.

Status	SLA	Track	VRRP	WAN Fa	ilover		
Network	Track Objec	at .					
Interface	ID	Туре	SLA ID	Interface	Negative Delay(s)	Positive Delay(s)	Operation
Firewall	1	sla	<u> </u>	cellular0 🔻	0		
QoS							
DHCP	Save						
DDNS							

5. Go to "Network > Link Failover > WAN Failover" and select "LAN1/WAN" as main interface, "cellular0" as backup interface. Other parameters can be kept as default value.

	LINK		Apply
		For your device security, please change the default password!	
Network	•	SLA Track VRRP 9 WAN Failover	
Interface		WAN Failover	
Firewall		Main Interface Backup Interface Startup Delay(s) Up Delay(s) Down Delay(s) Track ID Op	eration
QoS			×
DHCP			Ŧ
DDNS		Save	
Link Failover	8		

After all configurations are done, click "Apply" button.

 Go to "Status > Routing" to check the route table. And you will see the router access to the network via WAN interface (wired network).

Overview	Cellular	Network	WLAN VPN	Routing	Host List
Routing Tab	le				
	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.23.1	LAN1/WAN	1
	8.8.8.8	255.255.255.255	10.37.21.136	Cellular 0	1
	10.37.21.128	255.255.255.240	2	Cellular 0	123
	114.114.114.114	255.255.255.255	10.37.21.136	Cellular 0	1
	127.0.0.0	255.0.0.0	1.52	Loopback	-
	192.168.23.0	255.255.255.0	-	LAN1/WAN	-
	192.168.180.0	255.255.255.0	-	Bridge0	540

- 7. Check how WAN failover functions.
- (1) Unplug the Ethernet cable from WAN port of the router. Check the route table, and you will see the router access to the network via cellular0 interface (SIM).

Overview	Cellular	Network	WLAN VPN	Routing	Host List
Routing Tab	le				
	Destination	Netmask	Gateway	Interface	Metric
	0.0.0	0.0.0.0	10.37.21.136	Cellular 0	1
	8.8.8.8	255.255.255.255	10.37.21.136	Cellular 0	1
	10.37.21.128	255.255.255.240	×	Cellular 0	1001
	114.114.114.114	255.255.255.255	10.37.21.136	Cellular 0	1
	127.0.0.0	255.0.0.0	~	Loopback	343
	192.168.23.0	255.255.255.0	2	LAN1/WAN	
	192.168.180.0	255.255.255.0	2	Bridge0	124

(2) Plug the Ethernet cable to WAN port again. Check the route table, and you will see the router access to the network via WAN interface (wired network) again.

Overview	Cellular	Network	WLAN VPN	Routing	Host List
Routing Tabl	e				
	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.23.1	LAN1/WAN	1
	8.8.8	255.255.255.255	10.37.21.136	Cellular 0	1
	10.37.21.128	255.255.255.240	2	Cellular 0	150
	114.114.114.114	255.255.255.255	10.37.21.136	Cellular 0	1
	127.0.0.0	255.0.0.0	1	Loopback	(1 7 2)
	192.1 <mark>68.2</mark> 3.0	255.255.255.0	~	LAN1/WAN	-
	192.168.180.0	255.255.255.0	-1	Bridge0	(m)

Related Topics

WAN Setting Cellular Setting Track Setting SLA Setting WAN Failover Setting

4.8 Wi-Fi Application Example (Only Applicable to Wi-Fi Version)

4.8.1 AP Mode

Application Example

Configure UR32/UR35 as AP to allow connection from users or devices.

Configuration Steps

1. Go to "Network > Interface > WLAN" to configure wireless parameters as below.

		For your device security.	please change the	default password!	
Status	Port WAN	Bridge Switch	WLAN	Cellular	Loopbac
Naturat	Enable	×			
Network 👻	Work Mode	AP	•		
Interface	BSSID	24;e1:24:f0:25:7a			
Firewall	Radio Type	802.11n(2.4GHz)	•		
QoS	Channel	Auto	×		
405	Bandwidth	20MHz	•		
DHCP	SSID	Ursalink_F0257A			
DDNS	Encryption Mode	WPA-PSK/WPA2-PSK	•		
Link Failover	Cipher	Auto	•		
Routing	Key				
	SSID Broadcast				
VPN	AP Isolation	6			
System 🕨	Guest Mode				
	Max Client Number	128			

Click "Save" and "Apply" button after all configurations are done.

 Use a smart phone to connect by SSID "Ursalink_F0257A". Go to "Status > WLAN", and you can check the AP settings and information of the connected client/user.

Overview	Cellular	Network	WLAN	VPN	Routing	Host List
WLAN Status						
Name	Status	Туре	SSID	IP A	Address	Netmask
WLAN1	Running	AP	Ursalink_F0257A	192.1	68.140.1	255.255.255.0
Associated Statio	ins					
SSI	D	MAC A	ddress	IP Addre	ess	Connection Duration
Ursalink I	F0257A	3c:cd:5d:	47:10:8e	192.168.14	0 197	8 seconds

4.8.2 Client Mode

Application Example

Configure UR32/UR35 as Wi-Fi client to connect to an access point to have Internet access.

Configuration Steps

1. Go to "Network > Interface > WLAN" to configure wireless as below.

			For yo	ur device security, p	please change the c	efault password!	
status	Port	WAN	Bridge	Switch	WLAN	Cellular	Loopbac
letwork 🔻	WLAN						
Interface	Enable						
Interrace	Work Mode		Client		▼ Scan		
Firewall	SSID		Ursalink_	RD			
QoS	BSSID		24:e1:24:	0:25:5a			
DHCP	Encryption M	lode	WPA-PS	K/WPA2-PSK	•		
DDNS	Cipher		AES		Y		
	Key		••••••				
Link Failover	IP Setting						
Routing	Protocol		DHCP C	ient	•		

Click "Save" and "Apply" button after all configurations are done.

2. Go to "Status > WLAN", and you can check the connection status of the client.

Overview	Cellular	Network	WLAN	VPN	Routing	Host List
WLAN Status						
Name	Status	Туре	SSID	IP A	ddress	Netmask
WLAN1	Connected	Client	Ursalink_RD	192.1	68.1.108	255.255.255.0
Associated Static	ons					
SS	D	MAC Add	dress	IP Addre	955	Connection Duration

Related Topic

WLAN Setting

WLAN Status

4.9 VRRP Application Example

Application Example

A Web server requires Internet access through the UR32 router. To avoid data loss caused by router breakdown, two UR32 routers can be deployed as VRRP backup group, so as to improve network

reliability.

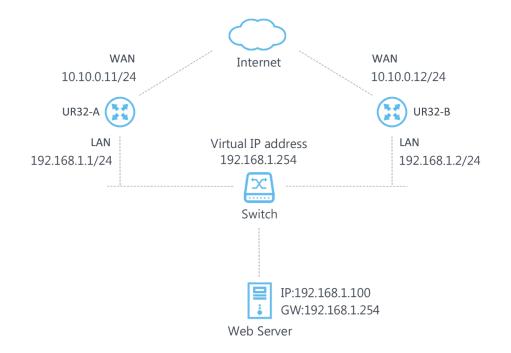
VRRP group:

WAN ports of the UR32 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.

UR32 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

Router A Configuration

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

URSALINK						
		For you	r device security, p	lease change the c	default password!	
Status	Port WAN	Bridge	Switch	WLAN	Cellular	Loopback
Network 👻	— WAN_1					
Interface	Enable		*****			
Firewall	Port Connection Type	LAN1/		T		
QoS	IPv4 Address	10.10.0).11			
DHCP	Netmask	255.25	5.255.0			
DDNS	IPv4 Gateway	10.10.0).1			
	IPv6 Address	fe80::2	6e1:24ff:fef0:2579			
Link Failover	Prefix-length	64				
Routing	IPv6 Gateway					
VPN	MTU	1500				
System 🕨	Primary DNS	114.11	4.114.114			
	Secondary DNS	8.8.8.8				
Industrial	Enable NAT					

2. Go to "Network > Link Failover > SLA" and configure SLA probe. The default probe type is ICMP. The destination address is the host address which can be probed by ICMP in public network or private network. Other parameters can be kept as default value.

CURSALINK									Apply	2	admin
Status	SLA	Track	VRRP W	AN Failover							
Network	SLA Entry										
Interface	ID	Туре	Destination Address	Secondary Destination Address	Data Size	Interval(s)	Timeout(ms)	PING Times	Packet Loss Rate	Start Time	Operation
Firewall	1	icmp-echo	• 114.114.114.114	8.8.8.8	56	30	5000	5	20	now 🔻	×
QoS											œ
DHCP	Save										
DDNS											
Link Failover											

 Go to "Network > Link Failover > Track" and configure link track parameters. You can use the default Track settings.

Status	SLA	Track	VRRP	WAN Failover	r		
Network 🔻	Track Objec	t					
	ID	Type	SLA ID	Interface	Negative Delay(s)	Positive Delay(s)	Operation
Interface	1	sla	• 1 •	cellular0 •	0] [1	
Firewall				a es	4		Ð
QoS							
DHCP	Save						
DDNS							

4. Go to "Network > Link Failover > VRRP" and configure VRRP parameters as below.

			Apply
		For your device security, please change the default password!	
Network 🗸	SLA Track	VRRP WAN Failover	
Interface	VRRP Status		
Firewall	Status	DISABLE	
QoS	VRRP Settings		
QUS	Enable		
DHCP	Interface	Bridge0 🔹	
DDNS	Virtual Router ID	1	
	Virtual IP	192.168.1.254	
Link Failover	Priority	110	
Routing	Advertisement Interval(s)	1	
VPN	Preemption Mode	v	
	Track ID	1	
System			
	Save		

Router B Configuration

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

	2	Foryo	our device security, p	blease change the	default password
Status	Port V	VAN Bridge	Switch	WLAN	Cellular
Network 🔻	- WAN_1				
Interface	Enable		/WAN		
Firewall	Port			•	
QoS	Pv4 Addres	10.10	10.10.0.12		
DHCP	Netmask	255.2	255.255.255.0		
DDNS	IPv4 Gatewa	y 10.10	0.0.1		
	IPv6 Address	fe80:	:26e1:24ff:fef0:2579		
Link Failover	Prefix-length	64			
Routing	IPv6 Gatewa	у			
VPN	МТО	1500			
System 🕨	Primary DNS	114.1	14.114.114		
-yokeni	Secondary D	NS 8.8.8	.8		

2. Go to "Network > Link Failover > SLA" and configure SLA probe. The default probe type is ICMP. The destination address is the host address which can be probed by ICMP in public network or private network. Other parameters can be kept as default value.

Hatus	SLA	Track	VRRP WAN F	ailovar						
letwork -	SLA Entry									
Interface	ID	Туре	Destination Address	Secondary Destination Address	Data Size	Interval(s) Ti		ING Packet mes Loss Rate	Start Time	Operation
Firewall	1	lcmp-echo	•] [114.114.114.114	8.8.8.8	56	30] [5	000 5	20	now 🔻	×
QoS										0
DHCP	Savo									
DDNS										

3. Go to "Network > Link Failover > Track" and configure link track parameters. You can use the default Track settings.

Status	SLA	Track	VRRP	WAN Failover			
Network	Track Object						
	ID	Type	SLA ID	Interface	Negative Delay(s)	Positive Delay(s)	Operation
Interface	1	sla	• <u>1</u> •	cellular0 •	0] [1	×
Firewall		-			ia i		
QoS							
DHCP	Save						
DDNS							

4. Go to "Network > Link Failover > VRRP" and configure VRRP parameters as below.

			Apply
		For your device security, please change the default password!	
Network 🗸	SLA Track	VRRP WAN Failover	
Interface	VRRP Status		
Firewall	Status	DISABLE	
QoS	VRRP Settings	ø	
DHCP	Interface	Bridge0	
DDNS	Virtual Router ID	1	
	Virtual IP	192.168.1.254	
Link Failover	Priority	100	
Routing	Advertisement Interval(s)	1	
VPN	Preemption Mode	0	
	Track ID	•	
System 🕨			
	Save		

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
Track Setting
SLA Setting

4.10 NAT Application Example

Example

An UR32/UR35 router can access Internet via cellular. LAN port is connected with a Web server whose IP address is 192.168.1.2 and port is 8000. Configure the router to make public network access the server.

Configuration Steps

Go to "Firewall > Port Mapping" and configure port mapping parameters.

	ALINH	<								5	Apply		adı	nin	6
Status			ACL	DMZ		Port Mappir	g (2)	MA	C Binding						
Network	-	Ð	Port Mappin	g											
Interface			Sou	rce IP		urce ort	Destinatio	n IP	Destination Port	Protocol	D	escriptio	1	Operatio	on
Firewall	1	3	0.0.0/0		800	0 192			8000	TCP •	server				
QoS														Ŧ	
DHCP			Save	4											

Click "Save" and "Apply" button.

Related Topic

Port Mapping

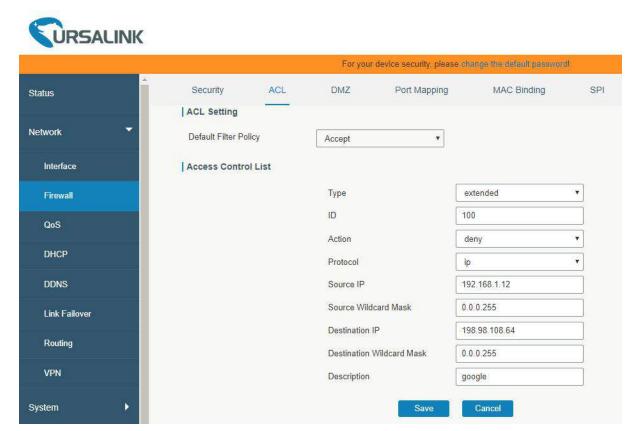
4.11 Access Control Application Example

Application Example

LAN port of the UR32/UR35 is set with IP 192.168.1.0/24. Then configure the router to deny accessing to Google IP 198.98.108.64 from local device with IP 192.168.1.12.

Configuration Steps

1. Go to "Network > Firewall > ACL" to configure access control list. Click "+" button to set parameters as below. Then click "Save" button.



2. Configure interface list. Then click "Save" and "Apply" button.

Security	ACL	DMZ	Port Map	ping MAC	Binding	SPI	
ACL Setting							
Default Filter F	Policy	Accept	ţ.	×			
Access Cont	rol <mark>List</mark>						
ID	Action	Protocol	Source IP	Destination IP	More Detail	Description	Operation
100	deny	ip	192.168.1.12/0.0.0. 255	198.98.108.64/0.0.0 .255		google	×
							Ŧ
Interface List	E.						
	Interface		In	ACL	Ou	t ACL	Operation
Bridge)	۲	100	¥		×	×
<u> </u>							Ð
-	-						
Save	_						

Related Topic

<u>ACL</u>

4.12 QoS Application Example

Example

Configure the UR32/UR35 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.

Enable		
		~
Default Category		
Download Bandwidth	75000	kbits/s

2. Please find "Service Category" option, and click "
"
to set up service classes.

Note: the percents must add up to 100%.

Name	Percent(%)	Max BW(kbps)	Min BW(kbps)	Operation
n <u>i</u>	40	30000	25000	
2	60	45000	40000	

3. Please find "Service Category Rules" option, and click "
"
to set up 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			ANY 🔻	2 •	×

Note:

1.213

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

Click "Save" and "Apply" button.

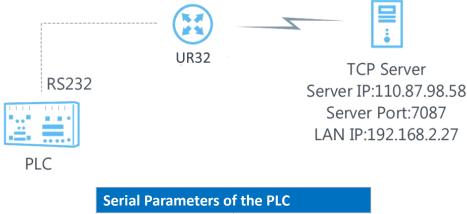
Related Topic

QoS Setting

4.13 DTU Application Example

Example

PLC is connected with the UR32 via RS232. Then enable DTU function of the UR32 to make a remote TCP server communicate with PLC. Refer to the following topological graph.



Serial Parameters o	Serial Parameters of the PLC				
Baud Rate	9600				
Data Bit	8				
Stop Bit	1				
Parity	None				

Configuration Steps

1. Go to "Industrial > Serial Port > Serial" and configure serial port parameters. The serial port parameter shall be kept in consistency with those of PLC, as shown in figure below.

			For your device security
Status	Serial		
	Serial Settings		
Network	Enable		
System 🕨	Serial Type	RS232	
cystem y	Baud Rate	9600	•
Industrial 🔻	Data Bits	8	
	Stop Bits	1	•
VO	Parity	None	•

2. Configure Serial Mode as "DTU Mode". The UR32 is connected as client in "Transparent" protocol.

System	Serial Mode	DTU Mode	•
Industrial	DTU Protocol	Transparent	•
	Protocol	ТСР	•
VO	 Keepalive Interval	75	s
Serial Port	Keepalive Retry Times	9	
Modbus TCP	Packet Size	1024	Bytes
	Serial Frame Interval	100	ms
GPS	Reconnect Interval	10	s
Maintenance	 Specific Protocol		
	Register String	modem1	

3. Configure TCP server IP and port.

Server Address	Server Port	Status	Operation
110.87.98.58	7087		×
			Ð

4. Once you complete all configurations, click "Save" and "Apply" button.

	Apply 2 admin		
Destination IP Address			
Server Address	Server Port	Status	Operation
110.87.98.58	7087	Connected	×

5. Start TCP server on PC.

Take "Netassist" test software as example. Make sure port mapping is already done.

TC	P Server	
(2)	Local host I	P
192	2.168.2	. 27
(3) 7087	Local host p	or
25875	Discon	

6. Connect the UR32 to PC via RS232 for PLC simulation. Then start "sscom" software on the PC to test communication through serial port.

ComNum	сомэ	•	CloseCom
BaudRa	9600	•	
DataBi	8	-	Send eve 10
StopBi	1	-	SendHEX 🗍
Verifyl	None	-	Data input:
FlowCon	None	-	helllo
		0.0	

7. After connection is established between the UR32 and the TCP server, you can send data between sscom and Netassit.

PC side

SSCOM3.2	_		×
testtesttesttesttesttesttesttesttest			~
OpenFile FileNm SendFile SaveDat ComNum COM13 - @ CloseCom Help	a Cle	ar	HexDats EXT
BaudRa 9600 V DTR RTS DataBi 8 V Send eve 1000 ms/Time StopBi 1 V SendHEX SendNew Verifyl None V Data input: SEND FlowCog None V hello		0	
ww.mcu51.cor S:42 R:48 COM13 opened 9600bp	s CTS=	1 DSR=	=0 RL /

TCP server side

	NetAssist (V3.7))
Settings	Data Receive
(1) Protocol	[Receive from 220.249.163.119 : 19049]:
TCP Server 📃	ursalink_modem1hellohellohellohellohellohellohellohell
(2) Local host IP 192.168, 2, 27	
(3) Local host por 7087	
• Disconnect	
Recv Options	
🔽 Receive to file	
🗖 Add line return	
🗌 Receive As HEX	
🗖 Receive Pause	
<u>Save</u> <u>Clear</u>	
Send Options	
🔲 🗖 Data from file	
🔲 Auto Checksum	
🔲 Auto Clear Input	
🔽 Send As Hex	
🥅 Send Cyclic	Peers: All Connections 💌
Interval 1000 ms	test
Load Clear	Send
🎯 Ready!	Send : 208 Recv : 177 Reset

8. After serial communication test is done, you can connect PLC to RS232 port of the UR32 for test.

Related Topic

Serial Port

4.14 PPTP Application Example

Example

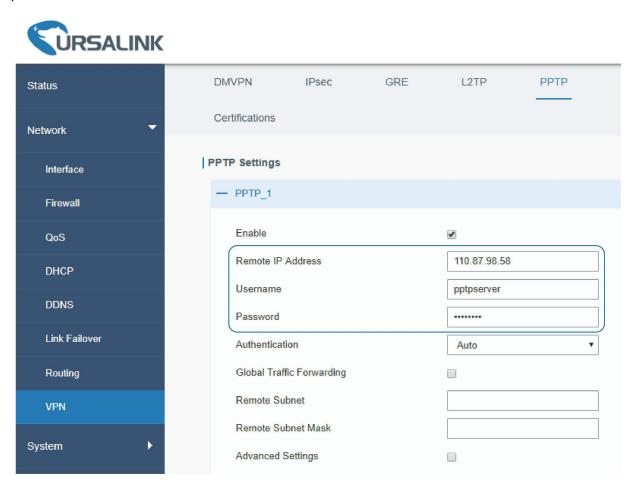


Configure the UR32 as PPTP client to connect to a PPTP server in order to have data transferred securely. Refer to the following topological graph.

Configuration Steps

 Go to "Network > VPN > PPTP", configure PPTP server IP address, username and password provided by PPTP server.

Note: If you want to have all data transferred through VPN tunnel, check "Global Traffic Forwarding" option.



If you want to access peer subnet such as 192.168.3.0/24, you need to configure the subnet and mask to add the route.

Remote Subnet	192,168.3.0	
Remote Subnet Mask	255.255.255.0	

2. Check "Show Advanced" option, and you will see the advanced settings.

DMVPN	IPsec	GRE	L2TP	PPTP
Show Adva	anced		2	
Local IP Ad	ddress			
Peer IP Ad	Idress		5 5	
Enable NA	Т			
Enable MP	PE			
Address/Co	ontrol Compressi	ion		
Protocol Fi	ield Compression	i		
Asyncmap	Value			
MRU			1500	
MTU			1500	
Link Detec	tion Interval (s)		60	
Max Retrie	S		0	
Expert Opt	ions			

If the PPTP server requires MPPE encryption, then you need to check "Enable MPPE" option.

Enable MPPE

-

If the PPTP server assigns fixed tunnel IP to the client, then you can fill in the local tunnel IP and remote tunnel IP, shown as below.

Local IP Address	205.205.0.100		
Peer IP Address	205.205.0.1		

Otherwise PPTP server will assign tunnel IP randomly.

Click "Save" button when you complete all settings, and then the advanced settings will be hidden again. Then click "Apply" button to have the configurations take effect.

3. Go to "Status > VPN" and check PPTP connection status.

PPTP is established as shown below.

Local IP: the client tunnel IP.

Remote IP: the server tunnel IP.

CURSALINK						
Status		Overview	Cellular	Network	VPN	Routing Host List
Network	×	PPTP Tunnel				
0			Name	Status	Local IP	Remote IP
System •			pptp_1	Connected	120.205.0.100	205.205.0.1/32
Industrial	•		pptp_2	Disconnected	-	-
Maintenance	•		pptp_3	Disconnected		

Related Topics

PPTP Setting

PPTP Status