

IOT-R32W



Updated on January 15, 2025

Preface

Thanks for choosing Linovision IOT-R32 industrial cellular router. The IOT-R32 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 IOT-R32 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

@ 2007-2025 Linovision 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 Linovision lot Co., Ltd.

Related Documents

Document	Description
Datasheet	Datasheet for the IOT-R32 industrial cellular router.
Quick Start Guide	Quick Installation guide for the IOT-R32 industrial cellular router.

Declaration of Conformity

IOT-R32 is in conformity with the essential requirements and other relevant provisions of the CE, FCC, and RoHS.







For assistance, please contact Linovision technical support: Email: sales@Linovision.com Tel: 86-571-86708175 Web: www.linovision.com/support/

Revision History

Date	Doc Version	Description
May. 16, 2019	V 1.1	Initial version
Nov. 14, 2019	V 1.2	Add Python, SMS, IP passthrough functions
May 11, 2020	V 1.3	Web interfaces upgrade
Dec. 9, 2020	V 2.0	Layout replace
Sept. 17, 2021	V 2.1	 Cellular and ping detection support IPv6 Add WAN connection type: DHCPv6 client, DS-Lite Add DHCPv6 Server feature Add IPv6 static routing feature Add Expert Option box in IPsec settings Support SMS inbox and outbox record clear

Contents

Chapter 1 Product Introduction	8
1.1 Overview	
1.2 Advantages	8
1.3 Specifications	
1.4 Dimensions (mm)	11
Chapter 2 Access to Web GUI	12
2.1 PC Configuration	12
2.2 Access to Web GUI of Router	13
Chapter 3 Web Configuration	
3.1 Status	
3.1.1 Overview	15
3.1.2 Cellular	
3.1.3 Network	
3.1.4 WLAN (Only Applicable to Wi-Fi Version)	19
3.1.5 VPN	
3.1.6 Routing	
3.1.7 Host List	21
3.1.8 GPS (Only Applicable to GPS Version)	22
3.2 Network	23
3.2.1 Interface	23
3.2.1.1 Link Failover	23
3.2.1.2 Cellular	25
3.2.1.3 Port	27
3.2.1.4 WAN	28
3.2.1.5 Bridge	
3.2.1.6 WLAN (Only Applicable to Wi-Fi Version)	
3.2.1.7 Switch	
3.2.1.8 Loopback	
3.2.2 DHCP	37
3.2.2.1 DHCP/DHCPv6 Server	37
3.2.2.2 DHCP Relay	
3.2.3 Firewall	
3.2.3.1 Security	40
3.2.3.2 ACL	
3.2.3.3 Port Mapping	
3.2.3.4 DMZ	
3.2.3.5 MAC Binding	44
3.2.3.6 Custom Rules	
3.2.3.7 SPI	45
3.2.4 QoS	46
3.2.5 VPN	
3.2.5.1 DMVPN	47

	3.2.5.2 IPSec Server	. 48
	3.2.5.3 IPSec	. 52
	3.2.5.4 GRE	. 54
	3.2.5.5 L2TP	. 55
	3.2.5.6 PPTP	. 57
	3.2.5.7 OpenVPN Client	59
	3.2.5.8 OpenVPN Server	. 61
	3.2.5.9 Certifications	. 63
	3.2.6 IP Passthrough	. 65
	3.2.7 Routing	. 65
	3.2.7.1 Static Routing	. 65
	3.2.7.2 RIP	. 66
	3.2.7.3 OSPF	.69
	3.2.7.4 Routing Filtering	.75
	3.2.8 VRRP	.75
	3.2.9 DDNS	.77
3.3	System	. 79
	3.3.1 General Settings	. 79
	3.3.1.1 General	.79
	3.3.1.2 System Time	.80
	3.3.1.3 Email	.82
	3.3.1.4 Storage	83
	3.3.2 Phone&SMS	84
	3.3.2.1 Phone	. 84
	3.3.2.2 SMS	. 85
	3.3.3 User Management	.86
	3.3.3.1 Account	.86
	3.3.3.2 User Management	. 87
	3.3.4 SNMP	.88
	3.3.4.1 SNMP	. 88
	3.3.4.2 MIB View	.89
	3.3.4.3 VACM	. 89
	3.3.4.4 Trap	. 90
	3.3.4.5 MIB	. 91
	3.3.5 AAA	. 91
	3.3.5.1 Radius	. 91
	3.3.5.2 TACACS+	.92
	3.3.5.3 LDAP	.93
	3.3.5.4 Authentication	.94
	3.3.6 Device Management	. 94
	3.3.6.1 DeviceHub	. 94
	3.3.6.2 Linovision VPN	.95
	3.3.7 Events	. 97
	3.3.7.1 Events	97

3.3.7.2 Events Settings	
3.4 Industrial Interface	
3.4.1 I/O	100
3.4.1.1 DI	100
3.4.1.2 DO	
3.4.2 Serial Port	
3.4.3 Modbus Slave	
3.4.3.1 Modbus TCP	
3.4.3.2 Modbus RTU	
3.4.3.3 Modbus RTU Over TCP	106
3.4.4 Modbus Master	107
3.4.4.1 Modbus Master	
3.4.4.2 Channel	108
3.4.5 GPS (Only Applicable to GPS Version)	110
3.4.5.1 GPS	110
3.4.5.2 GPS IP Forwarding	
3.4.5.3 GPS Serial Forwarding	112
3.5 Maintenance	
3.5.1 Tools	113
3.5.1.1 Ping	
3.5.1.2 Traceroute	113
3.5.1.3 Packet Analyzer	
3.5.1.4 Qxdmlog	
3.5.2 Debugger	115
3.5.2.1 Cellular Debugger	115
3.5.2.2 Firewall Debugger	115
3.5.3 Log	
3.5.3.1 System Log	
3.5.3.2 Log Download	117
3.5.3.3 Log Settings	118
3.5.4 Upgrade	119
3.5.5 Backup and Restore	119
3.5.6 Reboot	
3.6 APP	121
3.6.1 Python	
3.6.1.1 Python	121
3.6.1.2 App Manager Configuration	
3.6.1.3 Python App	
Chapter 4 Application Examples	124
4.1 Restore Factory Defaults	124
4.1.1 Via Web Interface	124
4.2.2 Via Hardware	125
4.2 Firmware Upgrade	
4.3 Events Application Example	

4.4 SNMP Application Example	127
4.5 Network Connection	130
4.5.1 Cellular Connection	130
4.5.2 Ethernet WAN Connection	132
4.6 Wi-Fi Application Example (Only Applicable to Wi-Fi Version)	134
4.6.1 AP Mode	134
4.6.2 Client Mode	135
4.7 VRRP Application Example	136
4.8 NAT Application Example	139
4.9 Access Control Application Example	139
4.10 QoS Application Example	
4.11 DTU Application Example	142
4.12 PPTP Application Example	145
4.13 Linovision Cloud Connection	147
4.13.1 Remotely view router information	147
4.13.2 Transmit Serial Data to the Cloud as a DTU	149

Chapter 1 Product Introduction

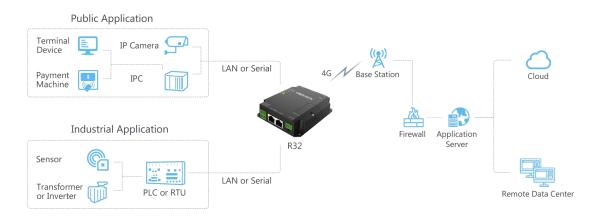
1.1 Overview

IOT-R32 is an industrial cellular router with embedded intelligent software features that are designed for multifarious M2M/IoT applications. Supporting global WCDMA and 4G LTE, IOT-R32 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 IOT-R32 is capable of providing wire-speed network with low power consumption and ultrasmall package to ensure the extremely safe and reliable connection to the wireless network. Meanwhile, the IOT-R32 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.

IOT-R32 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 IOT-R32 Quick Start Guide.





1.2 Advantages

Benefits

- Built-in industrial strong NXP CPU, big memory
- Fast Ethernet is applied to all models of Linovision 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
- Embedded Python SDK for second development
- 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, automatically recovering from various failure, and ensuring highest level of availability
- Establish a secured mechanism on centralized authentication and authorization of device access by supporting AAA (TACACS+, Radius, LDAP, local authentication) and multiple levels of user authority

Easy Maintenance

- Linovision 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 and 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 Platform	
CPU Platform	528 MHz, ARM Cortex A7
RAM	128 MB DDR3
Storage	Built-in 128 MB Flash storage, support extended Micro SD storage
otorago	(Max. 128 GB)
Interface	
Network Type	4G LTE (CAT 4)/WCDMA/GSM

Ethernet Port	2 × 10/100 Mbps fast Ethernet ports, include 1 × WAN + 1 × LAN (or 2 × LAN) Full or half duplex (Auto-Sensing), Auto MDI/MDIX
Serial Port	1 × DI + 1 × DO
I/O	IEEE 802.11 b/g/n
Power Supply	DC 9-48 V, 2-pin with 5.08 mm terminal block
Reset Button	Pinhole reset button
Built-in	Watchdog, Timer
SIM Card	Dual drawer-type SIM card slots. 2FF SIM. (SIM card priority can be customized)
Wi-Fi	Standards: IEEE 802.11b/g/n, 150Mbps Modes: AP and Client mode Security: WPA/WPA2 authentication, WEP/TKIP/AES encryption
Antenna Connector	3G/4G: 2 × 50 Ω SMA Connectors (Center PIN: SMA Female) Wi-Fi: 1 × 50 Ω RP-SMA Connector (Center PIN: RP-SMA Female)
Ground Terminal	Supports
Mechanical Specs	
Dimensions	108 x 90 x 26 mm (4.25 x 3.54 x 1.02 in)
Weight	271 g (0.6 lb)
Installation Method	DIN rail, wall mount, flat surface (all require additional kit)
Protection Rating	IP30
Housing	Metal
Cooling	Fanless
Power Rate	
Power Consumption	Typical 1.9 W, Max 2.4 W
Wi-Fi Transmit Power	
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)
Ambient Environment	
Storage Temperature	-40°C to +85°C (-40°F to +185°F)
Operating Temperature	-40°C to +70°C (-40°F to +185°F) Reduced Cellular Performance Above 60°C
Ambient Humidity	0% to 95% (non-condensing) at 25°C/77°F
Ethernet Isolation	1.5 kV RMS

Indicator LED 1 × POWER, 1 × SYSTEM, 1 × SIM, 3 × Signal strength Approvals Certificate CE, FCC, RCM, AT&T, T-mobile, Verizon Environmental RoHS Elocon EMC EN 55032, EN 55035 Elocon FMS Elocon-4-2 Level 3 Elocon-4-2 Level 3 EC 61000-4-2 Level 3 Elocon-4-3 Level 2 Elocon-4-3 Level 2 ELC 61000-4-4 Level 2 Elocon-4-4 Level 2 Elocon-4-4 Level 2 ELC 61000-4-5 Level 2 Elocon-4-4 Level 2 Elocon-4-4 Level 2 ELC 61000-4-4 Level 3 Elocon-4-4 Level 3 Elocon-4-4 Level 3 Radio Frequency EN 301 489-1/17/19/52, EN 301 511, EN 301 908-1/2/13, EN303 413 Safety Safety EN62368-1 Elocon-4-4 Level 3 Network Protocols IPv4/IPv6, PPP, PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QOS, SNTP, Teinet, VLAN, SSH, MQTT, MQTTS, TR069, etc. VPN DMVPN, IPsec, OpenVPN, PPTP, L2TP, GRE Security Access Control, DMZ, Port Mapping, MAC Binding, SPI Firewalls, DoS& DDOS Protection, Filtering(IP&Domain), IP Passthrough
CertificateCE, FCC, RCM, AT&T, T-mobile, VerizonEnvironmentalRoHSEMCEN 55032, EN 55035IEC 61000-4-2 Level 3 IEC 61000-4-3 Level 2IEC 61000-4-3 Level 2 IEC 61000-4-4 Level 2EMSIEC 61000-4-5 Level 2 IEC 61000-4-5 Level 1 IEC 61000-4-8 Level 1 IEC 61000-4-8 Level 1 IEC 61000-4-11 Level 3Radio FrequencyEN 301 489-1/17/19/52, EN 301 511, EN 301 908-1/2/13, EN303 413SafetyEN62368-1Software SystemIPv4/IPv6, PPP, PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QOS, SNTP, Telnet, VLAN, SSH, MQTT, MQTTS, TR069, etc.VPNDMVPN, IPsec, OpenVPN, PPTP, L2TP, GRESecurityAccess Control, DMZ, Port Mapping, MAC Binding, SPI Firewalls, DoS&
EnvironmentalRoHSEMCEN 55032, EN 55035EMCEN 55032, EN 55035IEC 61000-4-2 Level 3 IEC 61000-4-3 Level 2 IEC 61000-4-4 Level 2 IEC 61000-4-5 Level 2 IEC 61000-4-5 Level 2 IEC 61000-4-6 Level 3 IEC 61000-4-6 Level 3 IEC 61000-4-11 Level 3Radio FrequencyEN 301 489-1/17/19/52, EN 301 511, EN 301 908-1/2/13, EN303 413SafetyEN62368-1Software SystemIPv4/IPv6, PPP, PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QOS, SNTP, Telnet, VLAN, SSH, MQTT, MQTTS, TR069, etc.VPNDMVPN, IPsec, OpenVPN, PPTP, L2TP, GRESecurityAccess Control, DMZ, Port Mapping, MAC Binding, SPI Firewalls, DoS&
EMCEN 55032, EN 55035EMCEN 55032, EN 55035IEC 61000-4-2 Level 3 IEC 61000-4-3 Level 2 IEC 61000-4-4 Level 2 IEC 61000-4-5 Level 2 IEC 61000-4-5 Level 2 IEC 61000-4-5 Level 3 IEC 61000-4-6 Level 3 IEC 61000-4-8 Level 1 IEC 61000-4-11 Level 3Radio FrequencyEN 301 489-1/17/19/52, EN 301 511, EN 301 908-1/2/13, EN303 413SafetyEN62368-1Software SystemIPv4/IPv6, PPP, PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QOS, SNTP, Telnet, VLAN, SSH, MQTT, MQTTS, TR069, etc.VPNDMVPN, IPsec, OpenVPN, PPTP, L2TP, GRESecurityAccess Control, DMZ, Port Mapping, MAC Binding, SPI Firewalls, DoS&
IEC 61000-4-2 Level 3 IEC 61000-4-3 Level 2 IEC 61000-4-4 Level 2 IEC 61000-4-4 Level 2 IEC 61000-4-5 Level 2 IEC 61000-4-6 Level 3 IEC 61000-4-6 Level 3 IEC 61000-4-8 Level 1 IEC 61000-4-11 Level 3Radio FrequencyEN 301 489-1/17/19/52, EN 301 511, EN 301 908-1/2/13, EN303 413SafetyEN62368-1Software SystemIPv4/IPv6, PPP, PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QOS, SNTP, Telnet, VLAN, SSH, MQTT, MQTTS, TR069, etc.VPNDMVPN, IPsec, OpenVPN, PPTP, L2TP, GRESecurityAccess Control, DMZ, Port Mapping, MAC Binding, SPI Firewalls, DoS&
IEC 61000-4-3 Level 2 IEC 61000-4-4 Level 2 IEC 61000-4-4 Level 2 IEC 61000-4-5 Level 2 IEC 61000-4-6 Level 3 IEC 61000-4-8 Level 1 IEC 61000-4-11 Level 3Radio FrequencyEN 301 489-1/17/19/52, EN 301 511, EN 301 908-1/2/13, EN303 413SafetyEN62368-1Software SystemIPv4/IPv6, PPP, PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QOS, SNTP, Telnet, VLAN, SSH, MQTT, MQTTS, TR069, etc.VPNDMVPN, IPsec, OpenVPN, PPTP, L2TP, GRESecurityAccess Control, DMZ, Port Mapping, MAC Binding, SPI Firewalls, DoS&
SafetyEN62368-1Software SystemIPv4/IPv6, PPP, PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QOS, SNTP, Telnet, VLAN, SSH, MQTT, MQTTS, TR069, etc.VPNDMVPN, IPsec, OpenVPN, PPTP, L2TP, GRESecurityAccess Control, DMZ, Port Mapping, MAC Binding, SPI Firewalls, DoS&
Software SystemNetwork ProtocolsIPv4/IPv6, PPP, PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QOS, SNTP, Telnet, VLAN, SSH, MQTT, MQTTS, TR069, etc.VPNDMVPN, IPsec, OpenVPN, PPTP, L2TP, GRESecurityAccess Control, DMZ, Port Mapping, MAC Binding, SPI Firewalls, DoS&
Network ProtocolsIPv4/IPv6, PPP, PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QOS, SNTP, Telnet, VLAN, SSH, MQTT, MQTTS, TR069, etc.VPNDMVPN, IPsec, OpenVPN, PPTP, L2TP, GRESecurityAccess Control, DMZ, Port Mapping, MAC Binding, SPI Firewalls, DoS&
Network ProtocolsDDNS, VRRP, HTTP, HTTPS, DNS, ARP, QOS, SNTP, Telnet, VLAN, SSH, MQTT, MQTTS, TR069, etc.VPNDMVPN, IPsec, OpenVPN, PPTP, L2TP, GRESecurityAccess Control, DMZ, Port Mapping, MAC Binding, SPI Firewalls, DoS&
Access Control, DMZ, Port Mapping, MAC Binding, SPI Firewalls, DoS&
Security
Management Web, CLI, SMS, On-demand dial up, SNMP v1/v2/v3, DeviceHub
AAA Radius, Tacacs+, LDAP, Local Authentication
Multilevel Authority Multiple Levels of User Authority
Reliability VRRP, WAN Failover, Dual SIM Backup
Serial Port Transparent(TCP Client/Server, UDP), Modbus Server/Client, Modbus Gateway (Modbus RTU to Modbus TCP)
Development tools SDK package with build environment provided

1.4 Dimensions (mm)

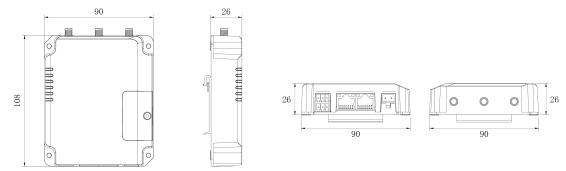


Figure 1-2

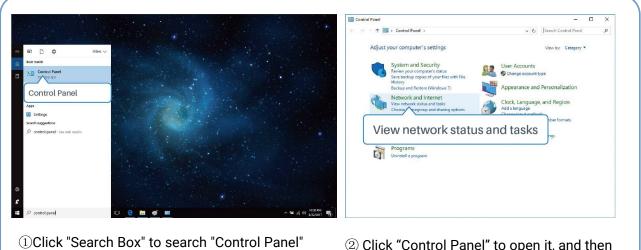
Chapter 2 Access to Web GUI

This chapter explains how to access to Web GUI of the IOT-R32 router.

2.1 PC Configuration

Please connect PC to LAN port of IOT-R32 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.



①Click "Search Box" to search "Control Panel" on the Windows 10 taskbar. ② Click "Control Panel" to open it, and then click "View network status and tasks".

Network and Sharing Center		– 🗆 X	Ethernet Status	×
> - 🛧 🔽 « Network	and Internet > Network and Sharing Center	✓ ♂ Search Control Panel		
Control Panel Home	View your basic network informa	ition and set up connections	General	
	View your active networks		Connection	
Change adapter settings		Access type: Internet	IPv4 Connectivity:	No network access
Change advanced sharing settings	Yeastar5G Private network	HomeGroup: Ready to create	IPv6 Connectivity:	No network access
	P I WATE I IELWOIK	Connections: MI-Fi (Yeastar5G)	Media State:	Enabled
			Duration:	00:01:21
	Identifying	Access type: No network access	Speed:	1.0 Gbos
	identifying	Connections: PEthernet		10 0000
			Details	
	Change your networking settings			
	Set up a new connection or netw			
	Set up a broadband, dial-up, or V	PN connection;	Activity	
	Troubleshoot problems			
	Diagnose and repair network pro	blems, or get troubleshooting information.		Received
			Properties	alter
			210	0
See also				
HomeGroup			Properties Disable	Diagnose
Infrared				
Internet Options Windows Firewall				
ering own incode				Close
			L	
		e different name).	④ Click "Propertie	

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
Intel(R) 82567LM Gigabit Network Connection	this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.	this capability. Otherwise, you ne 192.108.1.20 r for the appropriate IP settings. 255.255.255.0
Configure This connection uses the following items:	Obtain an IP address automatically	⊖ Obtain an IP address autor 192.168.1.1
Client for Microsoft Networks	Use the following IP address:	Use the following IP address:
File and Printer Sharing for Microsoft Networks	IP address:	IP address: 192 . 168 . 1 . 20
Gos Packet Scheduler Internet Protocol Version 4 (TCP/IPv4)	Subnet mask:	Subnet mask: 255 . 255 . 255 . 0
Microsoft Netv Adapter Multiplexor Protocol	Default gateway:	Default gateway: 192 . 168 . 1 . 1
nternet Protocol Version 4 (TCP/IPv4	Obtain DNS server address automatically	Obtain DNS server address automatically
	Use the following DNS server addresses:	OUse the following DNS server addresses:
Install Uninstall Properties	Preferred DNS server:	Preferred DNS server: 192 . 168 . 1 . 1
Description Transmission Control Protocol/Internet Protocol. The default	Alternate DNS server:	Alternate DNS server:
wide area network protocol that provides communication across diverse interconnected networks.	Validate settings upon exit Advanced	Validate settings upon exit 192.168.1.1
OK Cancel	OK Cancel	OK Cano
Double Click "Internet	⑥ Method 1: click "Obtain an IP	Method 2: click "Use the followi
Protocol Version 4	address automatically".	IP address" to assign a static IF

- (TCP/IPv4)" to configure IP address and DNS server.
- address automatically ;

manually within the same subnet of the router.

English

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

2.2 Access to Web GUI of Router

Linovision 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

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

Л.	2M ROUTER
	13690-530
Å	Usemame



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

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.

Chan	ge Password	
Old Password		
New Password		
Confirm New Password		
Save	Cancel	

Figure 2-2

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

			For your device se	curity, please change the default planament		
Ratus :		Overview Cellular	Network VPN Routing	Host List		Help
		System information		System Status		Model Show the model name of router
letwork	•	Model	R32-L00AU-485	Local Time	2021-09-22 17 47:31 Wednesday	Serial Number Show the serial number of router.
ystem	•	Serial Number	6218A1757711	Uptime	00.07.21	Firmware Version
		Firmware Version	32.3.0.2	CPU Load	13%	Show the current firmware version of router.
dustnal		Hardware Version	V2.0	RAM (Available/Capacity)	37MB/128MB(28.91%)	Hardware Version Show the current hardware version of
laintenance				Flash (Available/Capacity)	90MB/128MB(70.31%)	roufer
pp		Cellular		WAN Cirit in use		Local Time Show the current local time of system
PP	1	Status	No SIM Card	Status	Online	Uptime Show the information on how long the
		Current SIM	SIM2	IPv4	192 168 22 105/24	router has been running.
		IPv4	0.0.0.00	IPv6	fe80-26e1-24ff.fef0-b714/64	CPU Load Show the current CPU utilization of the
		IPv6		MAC	24 e1 24 f0 b7 16	router.
		Connection Duration	0 days, 00:00:00	Connection Duration	0 days, 00 06 07	RAM (Available/Capacity) Show the RAM available and the capacity
		Data Usage Monthly	0.0 MIB			RAM memory
		LAN				Flash (Available/Capacity) Show the Flash available and the capacit Flash memory.
		Pv4	192,168.0.1/24			Current SIM
						Show the current SIM card used
		IPv6 Connected Devices	fe00: 540b:71ff feed <21a/54 0			Data Usage Monthly Show the monthly data usage statistics o currently used SIM card.
						Connected Clients Amount of clients that connected to route's wirefeas access point
					Manual Refresh 🛩 Refrect	had had been been been been been been been bee

Figure 2-3

Chapter 3 Web Configuration

3.1 Status

3.1.1 Overview

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

Overview	Cellular	Network	VPN	Routing	Host List	
System Information	i				System Status	
Model		R32-L00AU-48	15		Local Time	2021-09-22 17:54:07 Wednesday
Serial Number		6218A175771	I.		Uptime	00:13:56
Firmware Version		32.3.0.2			CPU Load	75%
Hardware Version		V2.0			RAM (Available/Capacity)	37MB/128MB(28.91%)
					Flash (Available/Capacity)	90MB/128MB(70.31%)
Cellular					WAN Clink in use	
Status		No SIM Card			Status	Online
Current SIM		SIM1			IPv4	192.168.22.105/24
IPv4		0.0.0.0/0			IPv6	fe80::26e1:24ff.fef0.b714/64
IPv6					MAC	24:e1:24:f0:b7:16
Connection Duration		0 days, 00:00:1	00		Connection Duration	0 days, 00:12:43
Data Usage Monthly		0.0 MiB				
LAN						
IPv4		192.168.0.1/24	1			
IPv6		fe80::94 <mark>8b</mark> :7fff	feed:c2fa/64			
Connected Devices		0				

Figure 3-1-1-1

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

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

Table 3-1-1-2 System Status

Cellular		
Item	Description	
Status	Show the real-time status of the currently SIM card	
Current SIM Show the SIM card currently used for the data connection.		
IPv4/IPv6 Show the IPv4/IPv6 address obtained from the mobile of		
Connection Duration	Show the connection duration of the currently SIM card.	
Data Usage Monthly	Show the monthly data usage statistics of currently used SIM card.	

Table 3-1-1-3 Cellular Status

WAN		
Item Description		
Status	Show the currently status of WAN port.	
IPv4/IPv6	The IPv4/IPv6 address configured WAN port.	
MAC	The MAC address of the Ethernet port.	
Connection Duration	Show the connection duration of the WAN port.	

Table 3-1-1-4 WAN Status

WLAN (Only applicable for Wi-Fi model)		
Item Description		
Status	Show the currently status of WLAN.	
IP	Show the WLAN mode (AP or client).	
SSID Show the SSID of the WLAN AP or client.		
Connected Clients Show the amount of connected devices when mode		

Table 3-1-1-5 WLAN Status

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

Table 3-1-1-6 LAN Status

3.1.2 Cellular

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

Modem		Network	
Model	EC20F	Status	Connected
Version	EC20CEHCLGR06A05M1G	IPv4 Address	10.171.227.152/28
Current SIM	SIM1	IPv4 Gateway	10.171.227.153
Signal Level	31asu (-51dBm)	IPv4 DNS	211.143.147.120
Register Status	Registered (Home network)	IPv6 Address	2409:8934:1a1e:ca08:9c3f:1718:6fcd:4ad3/64
IMEI	861942056289607	IPv6 Gateway	2409:8934:1a1e:ca08:8e7:5c15:e8dd:111
IMSI	460005970144200	IPv6 DNS	2409:8034:2000:0:0:0:0:0:4
ICCID	898600511318F2001679	Connection Duration	0 days, 02:32:02
ISP	CHINA MOBILE	Data Usage Monthly	
Network Type	TDD LTE		
PLMN ID	46000	SIM-1	RX: 0.0 MIB TX: 0.0 MIB ALL: 0.0 MIB
LAC	592f	SIM-2	RX: 0.0 MIB TX: 0.0 MIB ALL: 0.0 MIB
Cell ID	3d98485		

Figure	3-1	-2-1
rigule	3-1	-7-1

Modem Information		
Item	Description	
Status	Show corresponding detection status of module and SIM card.	
Version	Show the cellular module firmware version.	
Current SIM	Show the current SIM card used.	
Signal Level	Show the cellular signal level.	
Register Status	Show the registration status of SIM card.	
IMEI	Show the IMEI of the module.	
IMSI	Show IMSI of the SIM card.	
ICCID	Show ICCID of the SIM card.	
ISP	Show the network provider which the SIM card registers on.	
Network Type	Show the connected network type, such as LTE, 3G, etc.	
PLMN ID	Show the current PLMN ID, including MCC, MNC, LAC and Cell ID.	
LAC	Show the location area code of the SIM card.	
Cell ID	Show the Cell ID of the SIM card location.	

Table 3-1-2-1 Modem Information

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

Table 3-1-2-2 Network Status

Data Usage Monthly		
Item	Description	
SIM-1	Show the monthly data usage statistics of SIM-1.	
SIM-2	Show the monthly data usage statistics of SIM-2.	

Table 3-1-2-3 Data Usage Information

3.1.3 Network

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

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

Figure	3-1	-3-1

WAN Status	WAN Status				
Item	Description				
Port	Show the name of WAN port.				
Status	Show the status of WAN port. "up" refers to a status that WAN is enabled and Ethernet cable is connected. "down" means Ethernet cable is disconnected or WAN function is disabled.				
Туре	Show the dial-up connection type of WAN port.				
IPv4/IPv6	Show the IPv4 address with netmask or IPv6 address with prefix-length of WAN port.				
Gateway	Show the gateway of WAN port.				
DNS	Show the DNS of WAN port.				
Connection Duration	Show the information on how long the Ethernet cable has been connected on WAN port when WAN function is enabled. Once WAN function is disabled or Ethernet connection is disconnected, the duration will stop.				

Table 3-1-3-1 WAN Status

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

Figure 3-1-3-2

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

Table 3-1-3-2 Bridge Status

3.1.4 WLAN (Only Applicable to Wi-Fi Version)

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

VLAN Status					
Name	Status	Туре	SSID	IP Address	Netmask
WLAN	Running	AP	Router_F02FEB	192.168.1.1	255.255.255.0
ssociated Static					
S SI	D	MAC	Address	IP Address	Connection Duration



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.
	Show the SSID of the router when the interface type is AP.
SSID	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

Overview	Cellular	Network	WLAN	VPN	Routing	Host List
Clients						
	Name	Status		Local IP		Remote IP
Server						
	Name				Status	
	OpenVPN S	Server			Disabled	
	Ipsec Ser	ver			Disabled	
Connected List						
	Server Type		Client IP			Duration

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

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
Status	that 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
	server.
	Show the information about how long the client has been
Duration	connected to this server when the server is enabled. Once
Duration	the server is disabled or connection is disconnected, the
	duration will stop counting.

Table 3-1-5-1 VPN Status

3.1.6 Routing

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

Routing Table					
	Destination	Netmask/Prefix Length	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.22.1	WAN	1
	127.0.0.0	255.0.0.0	÷	Loopback	-
	192.168.1.0	255.255.255.0	Ξ.	Bridge0	N20
	192.168.22.0	255.255.255.0	÷	WAN	-
		0	2408:844b:1a20:fc0:1d0a:9a67:4a3:3b 5a	Cellular 0	-
	21	128	-	Loopback	-
	2001:4860:4860::8888	128	2408:844b:1a20:fc0:1d0a:9a67:4a3:3b 5a	Cellular 0	1
	2004::	64		Bridge0	-
	2400:3200::1	128	2408:844b:1a20:fc0:1d0a:9a67:4a3:3b 5a	Cellular 0	1
	2408:844b:1a20:fc0::	64	ā.	Cellular 0	
ARP Cache					
	IP		MAC		Interface
	192.168.1.113		c8:5b:76:b2:56:1f		Bridge0
	192.168.22.127		24:e1:24:f0:47:e1		WAN
	192.168.22.1		5c:dd:70:6c:46:3d		WAN
	192.168.22.6		f4:b5:49:f1:1b:1f		WAN
	192.168.23.77		24:4b:fe:8d:95:ab		WAN Manual Refresh 🗸

Figure 3-1-6-1

Item	Description
Routing Table	
Destination	Show the IP address of destination host or destination network.
Netmask/Prefix	Show the netmask or prefix length of destination host or destination
Length	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	
DHCP Leases						
	IP				MAC/DUID	Lease Remaining Time
MAC Binding						
		IP				MAC/DUID



Host List					
Item	Description				
DHCP Leases					
IP Address	Show IP address of DHCP client				
MAC/DUID	Show MAC address of DHCPv4 client or DUID of DHCPv6 client.				
Lease Time Remaining Show the remaining lease time of DHCP client.					
MAC Binding	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.

GPS Status	
Status	Weak Signal
Time for Locating	-
Satellites In Use	-
Satellites In View	<u>1</u>
Latitude	-
Longitude	-
Altitude	-
Speed	7 .

Figure 3-1-8-1

GPS Status			
Item	Description		
Status	Show the status of GPS.		
Time for Locating	Show the time for locating.		
Satellites In Use	Show the quantity of satellites in use.		
Satellites In View	Show the quantity of satellites in view.		
Latitude	Show the Latitude of the location.		
Longitude	Show the Longitude of the location.		
Altitude	Show the Altitude of the location.		
Speed	Show the speed of movement.		
	Table 2-1-8-1 GDS Status Description		

Table 3-1-8-1 GPS Status Description

3.2 Network

3.2.1 Interface

3.2.1.1 Link Failover

This section describes how to configure link failover strategies, their priority and the ping settings, each rule owns its own ping rules by default. Router will follow the priority to choose the next available interface to access the internet, make sure you have enable the full interface that you need to use here. If priority 1 can only use IPv4, IOT-R32 will select a second link which IPv6 works as main IPv6 link and vice versa.

Link Failov	ver	Cellular	Port	WAN	Bridge	WLAN	Switch	Loopback	
Link Priorit	ity								
Prior	rity	Enable Rule	Link in use		Interface	Connecti	on Type	IP	Operation
1			•		WAN	Sta	tic	192.168.22.210	
2					Cellular-SIM1	DHO	CP	-	
3	č.				Cellular-SIM2	DHO	CP	-	
Settings									
Revert Inter	rval		300		s				
Emergency	Reboot								
Save									

Figure 3-2-1-1

Link Failover				
Item Description				
Link Priority				
Priority Display the priority of each interface, you can modify it by the operation's up and down button.				
Enable Rule	If enabled, the router will choose this interface into its switching rule. For the Cellular interface, if it's not enabled here, the interface will be disabled as well.			

Link In Use	Mark whether this interface is in use with Green color
Interface	Display the name of the interface.
Connection type	Display how to obtain the IP address in this interface, like static IP or DHCP.
IP	Display the IP address of the interface.
Operation	You can change the priority of the rules and configure the ping detection rules here.
Settings	
Revert Interval	Specify the number of seconds to waiting for switching to the link with higher priority, 0 means disable the function.
Emergency Reboot	Enable to reboot the device if no link is available.

Table 3-2-1-1 Link Failover Parameters

Enable			
IPv4 Primary Server	8.8.8.8		
IPv4 Secondary Server	114.114.114.114		
IPv6 Primary Server	2001:4860:4860::8888		
IPv6 Secondary Server	2400:3200::1		
Interval	300	s	
Retry Interval	5	s	
Timeout	3	s	
Max Ping Retries	3		

Figure 3-2-1-2

Ping Detection				
Item	Description			
Enable	If enabled, the router will periodically detect the connection status of the link.			
IPv4/IPv6 Primary Server	The router will send ICMP packet to the IPv4/IPv6 address or hostname to determine whether the Internet connection is still available or not.			
IPv4/IPv6 Secondary	The router will try to ping the secondary server name if			
Server	primary server is not available.			
Interval	Time interval (in seconds) between two Pings.			
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again in every retry interval.			
Timeout	The maximum amount of time the router will wait for a			

	response to a ping request. If it does not receive a response			
	for the amount of time defined in this field, the ping request			
	will be considered to have failed.			
	The retry times of the router sending ping request until			
Max Ping Retries	determining that the connection has failed.			
	Table 3-2-1-2 Ping Detection Parameters			

Table 3-2-1-2 Ping Detection Parameters

3.2.1.2 Cellular

This section explains how to set the related parameters for cellular network. The IOT-R32 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, it will follow the priority rule configured in 'Link Failover' page.

Link Failover	Cellular	Port	WAN	Bridge	WLAN	Switch	Loopback
Cellular Settings							
		SIM1			SIM2		
Protocol Type		IPv6		•	IPv6	~	
APN							
Username							
Password							
PIN Code							
Access Number							
Authentication Type		Auto	,	•	Auto	~	
Network Type		Auto	•	•	Auto	~	
PPP Preferred							
SMS Center							
Enable NAT							
Roaming							
Data Limit		0		MB	0		MB
Billing Day		Day 1	✓ of The Month		Day 1 🗸 of The	Month	
Connection Setting							
Connection Mode		Always Or	nline •	•			
Re-dial Interval(s)		5					

Figure 3-2-1-3

Cellular Settings	
Item	Description
Protocol	Select from "IPv4", "IPv6" and "IPv4/IPv6".
APN	Enter the Access Point Name for cellular dial-up connection provided by local ISP.

Username	Enter the username for cellular dial-up connection provided by local ISP.
Password	Enter the password for cellular dial-up connection provided by local ISP.
PIN Code	Enter a 4-8 characters PIN code to unlock the SIM.
Access Number	Enter the dial-up center NO. For cellular dial-up connection provided by local ISP.
Authentication Type	Select from "Auto", "PAP", "CHAP", "MS-CHAP", and "MS-CHAPv2".
Network Type	Select from "Auto", "4G Only", "3G Only", and "2G Only".Auto: connect to the network with the strongest signal automatically.4G Only: connect to 4G network only.And so on.
PPP Preferred	The PPP dial-up method is preferred.
SMS Center	Enter the local SMS center number for storing, forwarding, converting and delivering SMS message.
Enable NAT	Enable or disable NAT function.
Roaming	Enable or disable roaming.
Data Limit	When you reach the specified data usage limit, the data connection of currently used SIM card will be disabled. 0 means disable the function.
Billing Day	Choose the billing day of the SIM card, the router will reset the data used to 0.

Table 3-2-1-3 Cellular	Parameters
------------------------	------------

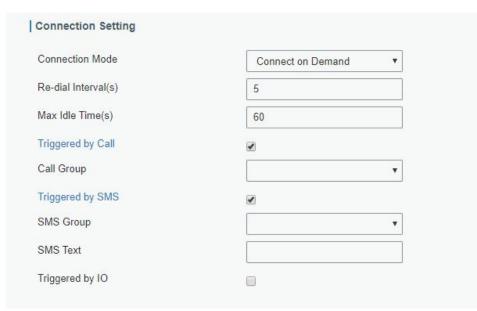


Figure 3-2-1-4

Connection Setting	
Item	Description
Connection Mode	Select from "Always Online" and "Connect on Demand".
Re-dial Interval(s)	Set the interval to dial into ISP when it lost connection, the default value is

	5s.
Max Idle Times	Set the maximum duration of router when current link is under idle status. Range: 10-3600
Triggered by Call	The router will switch from offline mode to cellular network mode automatically when it receives a call from the specific phone number.
Call Group	Select a call group for call trigger. Go to "System > Phone&SMS > 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 > Phone&SMS > SMS" 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 3-2-1-4 Cellular Parameters

Related Topics

Cellular Network Connection Phone Group DI Setting

3.2.1.3 Port

This section describes how to configure the Ethernet port parameters. IOT-R32 cellular router supports 2 Fast Ethernet ports.

Link Failover	Cellular	Port	WAN	Bridge	WLAN	Switch	Loopback
Port Setting							
	Port	Status	Propert	у	Speed	Duplex	
	LAN1/WAN	up 🗸	wan	~	auto 🗸	auto 🗸	
	LAN2	up 🗸	lan	~	auto 🗸	auto 🗸	
Save	l.						

Figure 3-2-1-5

Port Setting	
ltem	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	Show the Ethernet port's type, as a WAN port or a LAN port.
Speed	Set the Ethernet port's speed. The options are "auto", "100 Mbps",

	and "10 Mbps".
Duplex	Set the Ethernet port's mode. The options are "auto", "full", and "half".

Table 3-2-1-5 Port Parameters

3.2.1.4 WAN

WAN port can be connected with Ethernet cable to get Internet access. It supports 5 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.

- **DHCPv6 Client**: configure Ethernet WAN interface as DHCP Client to obtain IPv6 address automatically.

- Dual-Stack Lite: use IPv4-in-IPv6 tunneling to send terminal device's IPv4 packet through a tunnel on

the IPv6 access network to the ISP.

Status	Link Failover	Cellular	Port	WAN	Bridge	WLAN
Network	WAN Settings					
Interface	— WAN_1					
DHCP	Enable					
Firewall	Port			LAN1/WAN		
QoS	Connection Type	e		Static IP	~	
VPN	IPv4 Address Netmask			192.168.22.210		
IP Passthrough	IPv4 Gateway			192.168.22.1		
Routing	IPv6 Address			fe80::26e1:24ff:	fef1:2fea	
VRRP	Prefix Length			64		
DDNS	IPv6 Gateway					
	MTU			1500		
System >	IPv4 Primary DN	NS		114.114.114.114	•	
Industrial	IPv4 Secondary	DNS		8.8.8.8		
industrial ,	IPv6 Primary DN	VS				
Maintenance F	IPv6 Secondary	DNS				
	Enable NAT					

Figure 3-2-1-6

WAN Setting		
Item	Description	Default
Enable	Enable WAN function.	Enable
Port	The port that is currently set as WAN port.	WAN

Connection Type	Select from "Static IP", "DHCP Client", "DHCPv6 Client" , "Dual-Stack Lite" and "PPPoE".	Static IP
MTU	Set the maximum transmission unit.	1500
IPv4 Primary DNS	Set the primary IPv4 DNS server.	8.8.8.8
IPv4 Secondary DNS	Set the secondary IPv4 DNS server.	
IPv6 Primary DNS	Set the primary IPv6 DNS server.	
IPv6 Secondary DNS	Set the secondary IPv6 DNS server.	
Enable NAT	Enable or disable NAT function. When enabled, a private IP can be translated to a public IP.	Enable

Table 3-2-1-6 WAN Parameters

1. Static IP Configuration

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

Enable			
Port	LAN1/WAN		
Connection Type	Static IP 🗸		
IPv4 Address	192.168.22.210		
Netmask	255.255.255.0		
IPv4 Gateway	192.168.22.1		
IPv6 Address	fe80::26e1:24ff:fef1:2fea		
Prefix Length	64		
IPv6 Gateway			
MTU	1500		
IPv4 Primary DNS	114.114.114		
IPv4 Secondary DNS	8.8.8		
IPv6 Primary DNS			
IPv6 Secondary DNS			
Enable NAT			
Multiple IP Address			
	IP Address	Netmask	

Figure 3-2-1-7

Static IP					
Item	Description	Default			
IPv4 Address	Set the IPv4 address of the WAN port.	192.168.0.1			
Netmask	Set the Netmask for WAN port.	255.255.255.0			

IPv4 Gateway	Set the gateway for WAN port's IPv4 address.	192.168.0.2
IPv6 Address	Set the IPv6 address which can access 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 3-2-1-7 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.

LAN1/WAN		
DHCP Client	~	
1500		
114.114.114.114		
8.8.8.8		
3-2-1-8		
LAN1/WAN		
DHCPv6 Client	~	
None	~	
0-64		
1500		
	DHCP Client 1500 114.114.114 8.8.8.8 ✓ 3-2-1-8 ✓ LAN1/WAN DHCPv6 Client None 0-64	

Figure 3-2-1-9

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 3-2-1-8 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.

Enable	
Port	LAN1/WAN
Connection Type	PPP₀E ✓
Username	
Password	
Link Detection Interval(s)	60
Max Retries	0
мти	1500
Use Peer DNS	
IPv4 Primary DNS	114.114.114
IPv4 Secondary DNS	8.8.8.8
Enable NAT	



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 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 3-2-1-9 PPPoE Parameters

4. Dual-Stack Lite

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

Enable	
Port	LAN1/WAN
Connection Type	Dual-Stack Lite 🗸
IPv6 Gateway	
DS-Lite AFTR Address	
Local IPv6 Address	
MTU	1500
IPv4 Primary DNS	114.114.114
IPv4 Secondary DNS	8.8.8
IPv6 Primary DNS	
IPv6 Secondary DNS	
Enable NAT	



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

Table 3-2-1-10 Dual-Stack Lite Parameters

Related Configuration Example

Ethernet WAN Connection

3.2.1.5 Bridge

- - -

Bridge setting is used for managing local area network devices which are connected to LAN ports of the IOT-R32, allowing each of them to access the Internet.

Link Failover	Cellular	Port	WAN	Bridge	WLAN	Switch	Loopback
Bridge Setting							
Name	Brie	dge0					
STP							
IP Address	192	2. <mark>1</mark> 68.1.1					
Netmask	255	5.255. <mark>2</mark> 55.0					
IPv6 Address	200)4::1/64					
MTU	150	0					
Multiple IP Address							
	IP Add	ress		Netmask		Operation	
						Ð	

Figure	3-2-1	-12
--------	-------	-----

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

Table 3-2-1-11 Bridge Settings

3.2.1.6 WLAN (Only Applicable to Wi-Fi Version)

This section explains how to set the related parameters for Wi-Fi network. IOT-R32 supports 802.11 b/g/n, as AP or client mode.

Link Failover	Cellular	Port	WAN	Bridge	WLAN
WLAN					
Enable					
Work Mode	AF)	~		
BSSID	24:	e1:24:f0:2f:eb			
Radio Type	80	2. <mark>1</mark> 1n(2.4GHz)	~		
Channel	Au	to	~		
Bandwidth	20	MHz	~		
SSID	Ro	uter_F02FEB			
Encryption Mode	W	PA-PSK/WPA2-PS	к 🗸		
Cipher	Au	to	~		
Key					
SSID Broadcast					
AP Isolation					
Guest Mode					
Max Client Number	128	3			

Figure 3-2-1-13

WLAN	
ltem	Description
Enable	Enable/disable WLAN.
Work Mode	Select router's work mode. The options are "Client" or "AP".
Encryption Mode	Select encryption mode. The options are "No Encryption", "WEP 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 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.

CipnerShow the cipner of the access point.SecurityShow the encryption mode.FrequencyShow the frequency of radio.Join NetworkClick the button to join the wireless network. AP Mode	Cinhar	Chow the sinher of the second point
FrequencyShow the frequency of radio.Join NetworkClick the button to join the wireless network.AP ModeRadio TypeSelect Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)".ChannelSelect wireless channel. The options are "Auto", "1", "2""11".CipherSelect cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".KeyFill the pre-shared key of WPA encryption.BandwidthSelect bandwidth. The options are "20MHz" and "40MHz".SSID BroadcastWhen SSID broadcast is disabled, other wireless devices can't not find the SSID, and users have to enter the SSID manually to access to the wireless network.AP IsolationWhen AP isolation is enabled, all users which access to the AP are isolated without communication with each other.Guest ModeThe internal network is not allowed to visit if the guest mode is enabled.Max Client NumberSet the IP address in wireless network.IP SettingProtocolProtocolSet the IP address in wireless network.NetmaskSet the netmask in wireless network.	Cipher	Show the cipher of the access point.
Join NetworkClick the button to join the wireless network.AP ModeRadio TypeSelect Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)".ChannelSelect wireless channel. The options are "Auto", "1", "2""11".CipherSelect cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".KeyFill the pre-shared key of WPA encryption.BandwidthSelect bandwidth. The options are "20MHz" and "40MHz".SSID BroadcastWhen SSID broadcast is disabled, other wireless devices can't not find the SSID, and users have to enter the SSID manually to access to the wireless network.AP IsolationWhen AP isolation is enabled, all users which access to the AP are isolated without communication with each other.Guest ModeThe internal network is not allowed to visit if the guest mode is enabled.Max Client Number as AP.Set the IP address in wireless network.IP SettingSet the IP address in wireless network.IP AddressSet the netmask in wireless network.	Security	Show the encryption mode.
AP ModeRadio TypeSelect Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)".ChannelSelect wireless channel. The options are "Auto", "1", "2""11".CipherSelect cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".KeyFill the pre-shared key of WPA encryption.BandwidthSelect bandwidth. The options are "20MHz" and "40MHz".SSID BroadcastWhen SSID broadcast is disabled, other wireless devices can't not find the SSID, and users have to enter the SSID manually to access to the wireless network.AP IsolationWhen AP isolation is enabled, all users which access to the AP are isolated without communication with each other.Guest ModeThe internal network is not allowed to visit if the guest mode is enabled.Max Client Number as AP.Set the IP address in wireless network.IP SettingSet the IP address in wireless network.IP AddressSet the netmask in wireless network.	Frequency	Show the frequency of radio.
Radio TypeSelect Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)".ChannelSelect wireless channel. The options are "Auto", "1", "2""11".CipherSelect cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".KeyFill the pre-shared key of WPA encryption.BandwidthSelect bandwidth. The options are "20MHz" and "40MHz".SSID BroadcastWhen SSID broadcast is disabled, other wireless devices can't not find the SSID, and users have to enter the SSID manually to access to the wireless network.AP IsolationWhen AP isolation is enabled, all users which access to the AP are isolated without communication with each other.Guest ModeThe internal network is not allowed to visit if the guest mode is enabled.Max Client NumberSet the IP address in wireless network.IP AddressSet the IP address in wireless network.NetmaskSet the netmask in wireless network.	Join Network	Click the button to join the wireless network.
Radio Type"802.11n (2.4 GHz)".ChannelSelect wireless channel. The options are "Auto", "1", "2""11".CipherSelect cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".KeyFill the pre-shared key of WPA encryption.BandwidthSelect bandwidth. The options are "20MHz" and "40MHz".SSIDWhen SSID broadcast is disabled, other wireless devices can't not find the SSID, and users have to enter the SSID manually to access to the wireless network.AP IsolationWhen AP isolation is enabled, all users which access to the AP are isolated without communication with each other.Guest ModeThe internal network is not allowed to visit if the guest mode is enabled.Max ClientSet the maximum number of client to access when the router is configured as AP.IP SettingProtocolSet the IP address in wireless network.NetmaskSet the netmask in wireless network.	AP Mode	
CipherSelect cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".KeyFill the pre-shared key of WPA encryption.BandwidthSelect bandwidth. The options are "20MHz" and "40MHz".SSID BroadcastWhen SSID broadcast is disabled, other wireless devices can't not find the SSID, and users have to enter the SSID manually to access to the wireless network.AP IsolationWhen AP isolation is enabled, all users which access to the AP are isolated without communication with each other.Guest ModeThe internal network is not allowed to visit if the guest mode is enabled.Max Client NumberSet the maximum number of client to access when the router is configured as AP.ProtocolSet the IP address in wireless network.IP AddressSet the IP address in wireless network.NetmaskSet the netmask in wireless network.	Radio Type	
KeyFill the pre-shared key of WPA encryption.BandwidthSelect bandwidth. The options are "20MHz" and "40MHz".SSID BroadcastWhen SSID broadcast is disabled, other wireless devices can't not find the SSID, and users have to enter the SSID manually to access to the wireless network.AP IsolationWhen AP isolation is enabled, all users which access to the AP are isolated without communication with each other.Guest ModeThe internal network is not allowed to visit if the guest mode is enabled.Max Client NumberSet the maximum number of client to access when the router is configured as AP.IP SettingFortocolProtocolSet the IP address in wireless network.IP AddressSet the IP address in wireless network.NetmaskSet the netmask in wireless network.	Channel	Select wireless channel. The options are "Auto", "1", "2""11".
BandwidthSelect bandwidth. The options are "20MHz" and "40MHz".SSID BroadcastWhen SSID broadcast is disabled, other wireless devices can't not find the SSID, and users have to enter the SSID manually to access to the wireless network.AP IsolationWhen AP isolation is enabled, all users which access to the AP are isolated without communication with each other.Guest ModeThe internal network is not allowed to visit if the guest mode is enabled.Max Client NumberSet the maximum number of client to access when the router is configured as AP.IP SettingProtocolProtocolSet the IP address in wireless network.IP AddressSet the IP address in wireless network.NetmaskSet the netmask in wireless network.	Cipher	Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".
SSID BroadcastWhen SSID broadcast is disabled, other wireless devices can't not find the SSID, and users have to enter the SSID manually to access to the wireless network.AP IsolationWhen AP isolation is enabled, all users which access to the AP are isolated without communication with each other.Guest ModeThe internal network is not allowed to visit if the guest mode is enabled.Max ClientSet the maximum number of client to access when the router is configured as AP.IP SettingProtocolSet the IP address in wireless network.IP AddressSet the IP address in wireless network.NetmaskSet the netmask in wireless network.	Key	Fill the pre-shared key of WPA encryption.
SSID BroadcastSSID, and users have to enter the SSID manually to access to the wireless network.AP IsolationWhen AP isolation is enabled, all users which access to the AP are isolated without communication with each other.Guest ModeThe internal network is not allowed to visit if the guest mode is enabled.Max Client NumberSet the maximum number of client to access when the router is configured as AP.ProtocolSet the IP address in wireless network.IP AddressSet the IP address in wireless network.NetmaskSet the netmask in wireless network.	Bandwidth	Select bandwidth. The options are "20MHz" and "40MHz".
AP Isolationwithout communication with each other.Guest ModeThe internal network is not allowed to visit if the guest mode is enabled.Max ClientSet the maximum number of client to access when the router is configured as AP.IP SettingIP SettingProtocolSet the IP address in wireless network.IP AddressSet the IP address in wireless network.NetmaskSet the netmask in wireless network.		SSID, and users have to enter the SSID manually to access to the wireless
Max Client NumberSet the maximum number of client to access when the router is configured as AP.IP SettingProtocolSet the IP address in wireless network.IP AddressSet the IP address in wireless network.NetmaskSet the netmask in wireless network.	AP Isolation	
Numberas AP.IP SettingProtocolSet the IP address in wireless network.IP AddressSet the IP address in wireless network.NetmaskSet the netmask in wireless network.	Guest Mode	The internal network is not allowed to visit if the guest mode is enabled.
IP SettingProtocolSet the IP address in wireless network.IP AddressSet the IP address in wireless network.NetmaskSet the netmask in wireless network.	Max Client	Set the maximum number of client to access when the router is configured
ProtocolSet the IP address in wireless network.IP AddressSet the IP address in wireless network.NetmaskSet the netmask in wireless network.	Number	as AP.
IP AddressSet the IP address in wireless network.NetmaskSet the netmask in wireless network.	IP Setting	
Netmask Set the netmask in wireless network.	Protocol	Set the IP address in wireless network.
	IP Address	Set the IP address in wireless network.
Gateway Set the gateway in wireless network.	Netmask	Set the netmask in wireless network.
	Gateway	Set the gateway in wireless network.

Table 3-2-1-12 WLAN Parameters

MAC Filtering			
Туре	Allow and Block the Rest		
	MAC Address	Description	Operation
			H
Save & Apply			

Figure 3-2-1-14

MAC Filtering				
Item	Description			
Туре	In this mode, you can choose the rule according to your security policy, which is 'Allow and Block the Rest' and 'Block and Allow the Rest', the default value is Disabled.			
Allow and block the rest	Only the listed MAC addresses are allowed to connect to the router's wireless access point.			

Block and allow the rest	The listed MAC addresses are not allowed to connect to the					
	router's wireless access point.					

Table 3-2-1-13 MAC Filtering Parameters

Related Topic

Wi-Fi Application Example

3.2.1.7 Switch

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

Link Failover	Cellular	Port	WAN	Bridge	WLAN	Switch	Loopback		
AN Settings									
Nam	е	VLA	1 ID	IP /	Address	Netr	mask	MT	U Operation
vlan1		1	*	192.168.1.1		255.255.255.0		1500	
									+
/LAN Settings									
V	LAN ID		LAN 1		LAN	2		CPU	Operation
1		Close		~	Untagged	~	Tagged		 ✓
									•

Figure 3-2-1-15

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

Table 3-2-1-14 VLAN Trunk Parameters

3.2.1.8 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.

Link Failover	Cellular	Port	WAN	Bridge	WLAN	Switch	Loopback
Loopback Address							
IP Address		127.0.0.1					
Netmask		255.0.0.0					
Multiple IP Address	es						
	IP Addres	55			Netmask		Operation
Save							

Figure 3-2-1-16

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

Table 3-2-1-15 Loopback Parameters

3.2.2 DHCP

DHCP adopts Client/Server communication mode. The Client sends configuration request to the Server which feeds back corresponding configuration information and distributes IP address to the Client so as to achieve the dynamic configuration of IP address and other information.

3.2.2.1 DHCP Server/DHCPv6 Server

IOT-R32 can be set as a DHCP server or DHCPv6 server to distribute IP address when a host logs on and ensures each host is supplied with different IP addresses. DHCP Server has simplified some previous network management tasks requiring manual operations to the largest extent. IOT-R32 only supports stateful DHCPv6 when working as DHCPv6 server.

DHCP Server	DHCPv6 Server	DHCP Relay		
- DHCP Server_	1			
Enable				
Interface		Bridge0 🗸		
Start Address		192.168.1.113		
End Address		192.168.1.126		
Netmask		255.255.255.0		
Lease Time(Mir	n)	1440		
Primary DNS S	Server	8.8.8.8		
Secondary DNS	S Server	114.114.114.114		
Windows Name	e Server			
Static IP				
	MAC Add	ress	IP Address	Operation
				8



P Server	DHCPv6 Server	DHCP Relay		
	()			
DHCPv6 Server	_1			
Enable		٥		
Interface		Bridge0 🗸		
Start Address		2004:0:0:0:0:0:0:100		
End Address		2004:0:0:0:0:0:0:200		
Prefix Length		64		
Lease Time(Min)	1440		
Primary DNS Se	erver	2001:D0B0:3000:3001::1		
Secondary DNS	Server	2001:4860:4860::8888		
Static IP				
	DUID		IPv6 Address	Operat
				H



DHCP Server				
Item	Item Description			
Enable	Enable or disable DHCP server.	Enable		
Interface	Select interface.	Bridge0		
Start Address	Define the beginning of the pool of IP addresses which will	192.168.1.1		
Start Address	be leased to DHCP clients.	00		
End Address	Define the end of the pool of IP addresses which will be	192.168.1.1		
Ellu Auuless	leased to DHCP clients.	99		
Netmask	Define the subnet mask of IPv4 address obtained by DHCP	255.255.255		
INCUIIDSN	clients from DHCP server.	.0		

Prefix Length	Length Set the IPv6 prefix length of IPv6 address obtained by DHCP clients from DHCP server.		
Lease Time (Min)	Set the lease time on which the client can use the IP address obtained from DHCP server. Range: 1-10080.	1440	
Primary DNS Server	Set the primary DNS server.	192.168.1.1	
Secondary DNS Server	Set the secondary DNS server.	Null	
Windows Name Server	Define the Windows Internet Naming Service obtained by DHCP clients from DHCP sever. Generally you can leave it blank.	Null	
Static IP			
MAC Address	Set a static and specific MAC address for the DHCP client (it should be different from other MACs so as to avoid conflict).	Null	
DUID	Set a static and specific DUID for the DHCPv6 client (it should be different from other DUID so as to avoid conflict).	Null	
IP Address	Set a static and specific IP address for the DHCP client (it should be outside of the DHCP range).	Null	

Table 3-2-2-1 DHCP Server Parameters

3.2.2.2 DHCP Relay

IOT-R32 can be set as DHCP Relay to provide a relay tunnel to solve the problem that DHCP Client and DHCP Server are not in the same subnet.

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

Figure 3-2-2-3

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

Table 3-2-2-2 DHCP Relay Parameters

3.2.3 Firewall

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

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

3.2.3.1 Security

Security	ACL	Port Mapping	DMZ	MAC Binding	Custom Rules
Prevent Attack					
DoS/DDoS Prot	ection				
Access Servic	e Control				
Serv	ice	Port	Local		Remote
нтт	ſP	80	Ø		ø
нтт	PS	443	ø		Ø
TELN	IET	23	×		Ø
SS	н	22	۲		Ø
FT	P	21			Ø
Website Block	ing				
URL Blocking	[http://			
Keyword Blocki	na l				
Noyword DioChi			X		



Item	Description	Default
Prevent Attack		
DoS/DDoS Protection	Enable/disable Prevent DoS/DDoS Attack.	Disable
Access Service Contro	l	
Port	Set port number of the services. Range: 1-65535.	
Local	Access the router locally.	Enable
Remote	Access the router remotely.	Disable
HTTP	Users can log in the device locally via HTTP to	80

	access and control it through Web after the option is checked.		
HTTPS	Users can log in the device locally and remotely via HTTPS to access and control it through Web after option is checked.	443	
TELNET	Users can log in the device locally and remotely via Telnet after the option is checked.	23	
SSH	Users can log in the device locally and remotely via SSH after the option is checked.	22	
FTP	Users can log in the device locally and remotely via FTP after the option is checked.	21	
Website Blocking			
URL Blocking	_ Blocking Enter the HTTP address which you want to block.		
Keyword BlockingYou can block specific website by entering keyword. The maximum number of character allowed is 64.			

Table 3-2-3-1 Security Parameters

3.2.3.2 ACL

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

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

Security	ACL	Port Mapping	DMZ	MAC Binding	Custom R	ules	SPI
ACL Setting	Policy	Accept	Ţ				
Access Cont	rol List						
ID	Action	Protocol So	urce IP	Destination IP	More Detail	Description	Operation
							Ð
Interface List							
	Interface		In ACL		Out A	CL.	Operation
							H
Save							
			Figure	3-2-3-2			
ltem		Descripti	ion				
ACL Setting							

	Select from "Accept" and "Deny".
Default Filter Policy	The packets which are not included in the access control list
	will be processed by the default filter policy.
Access Control List	
Туре	Select type from "Extended" and "Standard".
ID	User-defined ACL number. Range: 1-199.
Action	Select from "Permit" and "Deny".
Protocol	Select protocol from "ip", "icmp", "tcp", "udp", and "1-255".
Source IP	Source network address (leaving it blank means all).
Source Wildcard Mask	Wildcard mask of the source network address.
Destination IP	Destination network address (0.0.0.0 means all).
Destination Wildcard Mask	Wildcard mask of destination address.
Description	Fill in a description for the groups with the same ID.
ICMP Type	Enter the type of ICMP packet. Range: 0-255.
ICMP Code	Enter the code of ICMP packet. Range: 0-255.
Source Port Type	Select source port type, such as specified port, port range, etc.
Source Port	Set source port number. Range: 1-65535.
Start Source Port	Set start source port number. Range: 1-65535.
End Source Port	Set end source port number. Range: 1-65535.
Destination Port Type	Select destination port type, such as specified port, port range, etc.
Destination Port	Set destination port number. Range: 1-65535.
Start Destination Port	Set start destination port number. Range: 1-65535.
End Destination Port	Set end destination port number. Range: 1-65535.
More Details	Show information of the port.
Interface List	
Interface	Select network interface for access control.
In ACL	Select a rule for incoming traffic from ACL ID.
Out ACL	Select a rule for outgoing traffic from ACL ID.
	Table 3-2-3-2 ACL Parameters

Table 3-2-3-2 ACL Parameters

Related Configuration Example

Access Control Application Example

3.2.3.3 Port Mapping

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.

Click \blacksquare to add a new port mapping rules.

	Security	ACL	Port Mapping	DMZ	MAC Binding	1	Custom Rules	SPI	
ļ	Port Mapping								
	Source I	P	Source Port	Destination IP	Destination Port	Protocol	Description		Operation
									Ð
	Save								

Figure 3-2-3-3

Port Mapping	
Item	Description
Source IP	Specify the host or network which can access local IP address.
	0.0.0/0 means all.
Source Port	Enter the TCP or UDP port from which incoming packets are
Source Fort	forwarded. Range: 1-65535.
Destination IP	Enter the IP address that packets are forwarded to after being
Destination	received on the incoming interface.
Destination Port	Enter the TCP or UDP port that packets are forwarded to after
Destination For	being received on the incoming port(s). Range: 1-65535.
Protocol	Select from "TCP" and "UDP" as your application required.
Description	The description of this rule.

Table 3-2-3-3 Port Mapping Parameters

Related Configuration Example

NAT Application Example

3.2.3.4 DMZ

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

Security	ACL	Port Mapping	DMZ	ħ
DMZ				
Enable				
DMZ Host				
Source Address				
Save				

Figure 3-2-3-4

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" means any address.

Table 3-2-3-4 DMZ Parameters

3.2.3.5 MAC Binding

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

Security	ACL	Port Mapping	DMZ	MAC Binding	Custom Rules	SPI
MAC Binding	List					
	MAC		IP		Description	Operation
						•
Save						

Figure 3-2-3-5

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

3.2.3.6 Custom Rules

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

Security	ACL	Port Mapping	DMZ	MAC Binding	Custom Rules	SPI
Custom F	Rules					
		Rule			Description	Operation
	Eg: -t filter -I INPU	T -s 192.168.3.240 -j DR	OP			×
						+
Sav	e					

Figure 3-2-3-6

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

Table 3-2-3-6 Custom Rules Parameters

3.2.3.7 SPI

Se	ecurity	ACL	Port Mapping	DMZ	MAC Binding	Custom Rules	SPI
SPI	Firewall						
	Enable						
	Filter P	roxy					
	Filter C	ookies					
	Filter A	ctivex					
	Filter J	ava Applets					
2	Filter N	lulticast					
	Filter II	DENT(port 113)					
1	Block \	Van SNMP access	1				
1	Filter V	/AN NAT Redirecti	ion				
	Block A	Anonymous Wan R	lequest				
	Save						

Figure 3-2-3-7

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 3-2-3-7 SPI Parameters

3.2.4 QoS

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

Status	Î	QoS(Download)	QoS(Upload)						
Network	•	Download Bandwidt	n						
Interface		Enable							
DHCP		Default Category Download Bandwidth	0	• kbits	/s				
Firewall		Capacity							
QoS		Service Category							
VPN		Name		Percent(%)	Max BW(kbps)	Min BW(kbps)	Operation
IP Passthrough									Đ
Routing		Service Category Ru	les						
VRRP		Name	Source IP	Source Port	Destination IP	Destination Port	Protocol	Service Category	Operation
DDNS									Ð
System	•	Save							

Figure 3-2-4-1

QoS	QoS				
Item	Description				
Download/Upload					
Enable	Enable or disable QoS.				
Default Category	Select the default category from Service Category list.				
Download/Upload Bandwidth Capacity	The download/upload bandwidth capacity of the network that 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	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 3-2-4-1 QoS (Download/Upload) Parameters

Related Configuration Example

QoS Application Example

3.2.5 VPN

Virtual Private Networks, also called VPNs, are used to securely connect two private networks together so that devices can connect from one network to the other network via secure channels. The IOT-R32 supports DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN, as well as GRE over IPsec and L2TP over IPsec.

3.2.5.1 DMVPN

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

Status	DMVPN IPsec Serve	r IPsec	GRE	L2TP	PPTP	OpenVPN Client	OpenVPN Server	Certifications
Network -	DMVPN Settings							
Interface	Enable							
DHCP	Hub Address Local IP Address			_				
Firewall	GRE HUB IP Address							
QoS	GRE Local IP Address							
VPN	GRE Mask	255.25	5.255.0					
IP Passthrough	GRE Key Negotiation Mode	Main		*				
Routing	Authentication Algorithm	DES		*				
VRRP	Encryption Algorithm	MD5		٣				
DDNS	DH Group	MODE	P768-1	w.				
System 🕨	Key							
System	Local ID Type	Defau	it.	٣				
Industrial	IKE Life Time(s)	10800						
Second C	SAAlgorithm	DES-I	MD5	٣				
Maintenance	PFS Group	NULL		٣				
APP 🕨	Life Time(s)	3600						
	DPD Time Interval(s)	30						
	DPD Timeout(s)	150						
	Cisco Secret							
	NHRP Holdtime(s)	7200						
	Save							
	Save							

Figure 3-2-5-1

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	Select from "DES", "3DES", "AES128", "AES192" and			
Algorithm	"AES256".			
Encryption Algorithm	Select from "MD5" and "SHA1".			
DH Group	Select from "MODP768_1", "MODP1024_2" and			
ла стопр	"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",			
SA Algorithm	"3DES_SHA1", "AES128_MD5", "AES128_SHA1",			
SA Algontinin	"AES192_MD5", "AES192_SHA1", "AES256_MD5" and			
	"AES256_SHA1".			
PFS Group	Select from "NULL", "MODP768_1", "MODP1024_2" and			
•	"MODP1536-5".			
Life Time (s) Set the lifetime of IPsec SA. Range: 60-86400.				
DPD Interval Time (s)	Set DPD interval time			
DPD Timeout (s) Set DPD timeout.				
Cisco Secret	Cisco Nhrp key.			
NHRP Holdtime (s)	The holdtime of NHRP protocol.			

Table 3-2-5-1 DMVPN Parameters

3.2.5.2 IPSec Server

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

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

DMVPN	IPsec Server	IPsec	GRE	L2TP
IPsec Server				
Enable				
IPsec Mode			Tunnel	~
IPsec Protocol			ESP	~
Local Subnet				
Local Subnet Ma	ask			
Local ID Type			Default	~
Remote Subnet				
Remote Subnet	Mask			
Remote ID Type	9		Default	~
IKE Parameter				
SA Parameter				
IPsec Advance	d		\geq	
Expert Options				

Figure 3-2-5-2

Save

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 3-2-5-2 IPsec Parameters

IKE Parameter	۲			
IKE Version	IKEv1	۲		
Negotiation Mode	Main			
Encryption Algorithm	DES	•		
Authentication Algorithm	MD5	¥		
DH Group	MODP768-1	•		
Local Authentication	PSK	•		
XAUTH				
Lifetime(s)	10800			
XAUTH List				
Us	sername		Password	Operation
				•
PSK List				
S	elector		PSK	Operation
				8

Figure 3-2-5-3

SA Parameter		
SAAlgorithm	DES-MD5	~
PFS Group	NULL	~
Lifetime(s)	3600	
DPD Time Interval(s)	30	
DPD Timeout(s)	150	
IPsec Advanced	\bigtriangledown	
Enable Compression		
VPN Over IPsec Type	NONE	*
Expert Options		



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	al 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			
SA Algorithm	Select from "DES_MD5", "DES_SHA1", "3DES_MD5", "3DES_SHA1", "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.		
Expert OptionsUser can enter some other initialization strings in this field and separate the strings with ";". For example, if more local or remo- subnet need to be added, users can add contents here.			

Table 3-2-5-3 IPsec Server Parameters

3.2.5.3 IPSec

DM	VPN	IPsec Server	IPsec	GRE	L2TP	PPTP	OpenVPN Client
IPse	c Settings						
-	IPsec_1						
	Enable		(
	IPsec Gatewa	y Address	[
	IPsec Mode			Tunnel	*		
	IPsec Protoco	Г	[ESP	~		
	Local Subnet		[
	Local Subnet I	Mask	[
	Local ID Type		[Default	*		
	Remote Subne	et	[
	Remote Subne	et Mask	[
	Remote ID Typ	pe	[Default	~		
	IKE Paramete	۲					
	SA Parameter	r					
	IPsec Advance	ed	[$\overline{\mathbf{N}}$			
	Expert Options	5					
+	IPsec_2						
+	IPsec_3						

Figure 3-2-5-5

IPsec				
Item	Description			
Enable Enable IPsec tunnel. A maximum of 3 tunnels is allowed.				
IPsec Gateway Address	Enter the IP address or domain name of remote IPsec server.			
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 3-2-5-4 IPsec Parameters

IKE Parameter		
IKE Version	IKEv1	~
Negotiation Mode	Main	~
Encryption Algorithm	AES128	~
Authentication Algorithm	SHA1	~
DH Group	MODP768-1	~
Local Authentication	PSK	~
Local Secrets	•••••	
XAUTH		
Username		
Password		
Lifetime(s)	28800	
SA Parameter		
IPsec Advanced		
Enable Compression		
VPN Over IPsec Type	NONE	~
Expert Options		



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.
Expert Option	User can enter some other initialization strings in this field and separate the strings with ";". For example, if more local or remote subnet need to be added, users can add contents here.

Table 3-2-5-5 IPsec Parameters

3.2.5.4 GRE

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

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

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

DN	IVPN	IPsec Server	IPsec	GRE	L2TP	PPTP	OpenVPN Client
GRI	E Settings						
-	GRE_1						
	Enable						
	Remote IP Ad	dress					
	Local IP Addre	BSS					
	Local Virtual I	P Address					
	Netmask			255.25	5.255.0		
	Peer Virtual IF	^o Address					
	Global Traffic	Forwarding					
	Remote Subn	et					
	Remote Netm	ask					
	MTU			1500			
	Key						
	Enable NAT			×			
+	GRE_2						
+	GRE_3						

Figure 3-2-5-7

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 3-2-5-6 GRE Parameters

3.2.5.5 L2TP

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

DM	IVPN	IPsec Server	IPsec	GRE	L2TP	PPTP	OpenVPN Client
L2TI	P Settings						
-	L2TP_1						
	Enable						
	Remote IP Ac	ddress		58.63.12	28.250		
	Username			user2			
	Password			•••••			
	Authenticatio	n		CHAP		•	
	Global Traffic	Forwarding					
	Key						
	Advanced Se	ttings		Σ			
+	L2TP_2						
+	L2TP_3						

Figure 3-2-5-8

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

Table 3-2-5-7 L2TP Parameters

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



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	Torrer initialization. Oser can keep the default option.
Protocol Field	For PPP initialization. User can keep the default option.
Compression	For FFF initialization. Oser can keep the default option.
Asyncmap Value	One of the PPP protocol initialization strings. User can
Asyncinap value	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
LINK Detection Interval (S)	connection. Range: 0-600.
Max Retries	Set the maximum times of retry to detect the L2TP
Max Retries	connection failure. Range: 0-10.
Expert Options	User can enter some other PPP initialization strings in this
	field and separate the strings with blank space.

Table 3-2-5-8 L2TP Parameters

3.2.5.6 PPTP

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

DMVPN	IPsec Server	IPsec	GRE	L2TP	PPTP	OpenVPN Client
PPTP Settings						
- PPTP_1						
Remote S	ition ffic Forwarding ubnet ubnet Mask		Auto			
Advanced	Settings		Σ			
+ PPTP_2						
+ PPTP_3						
Save						

Figure 3-2-5-10

РРТР			
Item	Description		
Enable	Enable PPTP client. A maximum of 3 tunnels is allowed.		
Remote IP Address	Enter the public IP address or domain name of PPTP server.		
Username	Enter the username that PPTP server provides.		
Password	Enter the password that PPTP server provides.		
Authentication	Select from "Auto", "PAP", "CHAP", "MS-CHAPv1", and "MS-CHAPv2".		
Global Traffic 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 3-2-5-9 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
МТО	1500
Link Detection Interval(s)	60
Max Retries	0
Expert Options	

Figure 3-2-5-11

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	For PPP initialization. User can keep the default option.		
Compression	For FFF initialization. Oser can keep the default option.		
Protocol Field	For PPP initialization. User can keep the default option.		

Compression	
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	Set the link detection interval time to ensure tunnel
(s)	connection. Range: 0-600.
Max Retries	Set the maximum times of retrying to detect the PPTP
Wax Relifes	connection failure. Range: 0-10.
Export Options	User can enter some other PPP initialization strings in this
Expert Options	field and separate the strings with blank space.

Table 3-2-5-10 PPTP Parameters

Related Configuration Example

PPTP Application Example

3.2.5.7 OpenVPN Client

OpenVPN is an open source virtual private network (VPN) product that offers a simplified security framework, modular network design, and cross-platform portability.

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).

IVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client	OpenVPN Server	Certifi
enVPN Clier	nt Settings						
- OpenVPN							
openvi it <u>i</u>	-1						
Enable							
Protocol		UDI	þ	•			
Remote IP	Address						
Port		1194	Ĺ				
Interface		tun	N	•			
Authentica	ition	Nor	ie	•			
Local Tunr	nel IP						
Remote Tu	unnel IP						
Enable NA	AT						
Compress	ion	LZC)	•			
Link Detec	ction Interval(s)	60					
Link Detec	ction Timeout(s)	300					
Cipher		Nor	ie	•			
MTU		1500)				
Max Fram	e Size	1500)				
Verbose L	evel	ERI	ROR	•			
Expert Op	tions						
Local Rou	ıte						
		Subnet			Subnet Mas	k	Operation

Figure 3-2-5-12

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", 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 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: 10-1800.
Link Detection Timeout (s)	Set link detection timeout. OpenVPN will be reestablished after timeout. Range: 60-3600.
Cipher	Select from "NONE", "BF-CBC", "DE-CBC", "DES-EDE3-CBC", "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".
Expert Options	User can enter some other PPP initialization strings in this field and 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 3-2-5-11 OpenVPN Client Parameters

3.2.5.8 OpenVPN Server

The IOT-R32 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		v		
Authentication		None		*		
Local Virtual IP						
Remote Virtual I	Ρ					
Enable NAT		1				
Compression		LZO		*		
Link Detection In	nterval	60				
Cipher		None		Ŧ		
MTU		1500				
Max Frame Size	3	1500				
Verbose Level		ERROR		v		
Expert Options						

Figure 3-2-5-13

Local Route			
	Subnet	Netmask	Operation
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.
Listening IP	Enter WAN IP address or LAN IP address. Leaving it blank refers to all active WAN IP and LAN IP address.
Interface	Select from " tun" and "tap".
Authentication	Select from "None", "Pre-shared", "Username/Password", "X.509 cert" and "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 Detection Interval	Set link detection interval time to ensure tunnel connection. Range: 10-1800.
Cipher	Select from "NONE", "BF-CBC", "DES-CBC", "DES-EDE3-CBC", "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".
Expert Options	User can enter some other PPP initialization strings in this field and 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 3-2-5-12 OpenVPN Server Parameters

3.2.5.9 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	nt						
- OpenVPN	client_1						
CA				Browse	Import Export Delet	e	
Public Key	4			Browse	Import Export Delet	e	
Private Ke	зу 📕			Browse	Import Export Delet	e	
TA				Browse	Import Export Delet	e	
Preshared	l Key			Browse	Import Export Delet	e	
PKCS12				Browse	Import Export Delet	e	

Figure 3-2-5-15

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 3-2-5-13 OpenVPN Client Certification Parameters

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

Figure 3-2-5-16

OpenVPN Server		
Item	Description	
СА	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 3-2-5-14 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 3-2-5-17

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 3-2-5-15 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 3-2-5-18

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 3-2-5-16 IPsec Server Parameters		

Table 3-2-5-16 IPsec Server Parameters

3.2.6 IP Passthrough

IP Passthrough mode shares or "passes" the Internet providers assigned IP address to a single LAN

client device connected to the router.

Status	IP Passthrough	
Network	IP Passthrough	
transfer data	Enable	
Interface	Passthrough Mode	DHCPS-Fixed •
DHCP	MAC	
Firewall		
QoS	Save	
VPN		
IP Passthrough		

Figure 3-2-6-1

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

Table 3-2-6-1 IP Passthrough Parameters

3.2.7 Routing

3.2.7.1 Static Routing

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

atic Routing	RIP	OSPF	Routing Filtering				
tic Routing							
	Destination		Netmask/Prefix Length	Interface	Gateway	Distance	Operation
114.1	14.114.114		255.255.255.255	LAN1/WAN 🗸	192.168.5.1	1	×
8.8.8.	8		255.255.255	LAN1/WAN 🗸	192.168.5.1	1	×
0.0.0.	0		0.0.0.0	LAN1/WAN 🗸	192.168.5.1	1	×
							Ŧ



Static Routing	
ltem	Description
Destination	Enter the destination IP address.
Netmask/Prefix Length	Enter the subnet mask or prefix length of destination address.
Interface	The interface through which the data can reach the destination address.
Gateway	IP address of the next router that will be passed by before the input data reaches the destination address.
Distance	Priority, smaller value refers to higher priority. Range: 1-255.

Table 3-2-7-1 Static Routing Parameters

3.2.7.2 RIP

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

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

Static Routing	RIP	OSPF	Routi	ng Filtering
RIP Settings				
Enable				
Update Timer	30		s	
Timeout Timer	180		s	
Garbage Collection Timer	120		s	
Version	v2		Ŧ	
Show Advanced Options				
Default Information Originat	e 📄			
Default Metric	1			
Redistribute Connected				
Redistribute Static				
Redistribute OSPF				



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 Ma	anagement						
Distance		IP Add	Iress	Netmas	¢	ACL Name	Operation
							Ð
Metric		Policy I	n/Out	Interface	3	ACL Name	Operation
							±
Filter Policy							
Policy Typ	e	Policy	Name	Policy In/C)ut	Interface	Operation
							•
Passive Interface							
			Passive	Interface			Operation
							•
Interface							
Interface	Send Version	Receive Version	Split- Horizon	Authentication Mode	Authentication String	Authentication Key-chain	Operation
							•
Neighbor							
			IP Ad	ldress			Operation
							•
Network							
	IP Addre	55			Netmask		Operation
							Ð

Figure 3-2-7-3

ltem	Description		
Distance/Metric Management			
Distance	Set the administrative distance that a RIP route learns. Range:		

	1-255.		
IP Address	Set the IP address of RIP route.		
Netmask	Set the netmask of RIP route.		
ACL Name	Set ACL name of RIP route.		
Metric	The metric of received route or sent route from the interface. Range: 0-16.		
Policy in/out	Select from "in" and "out".		
Interface	Select interface of the route.		
ACL Name	Access control list name of the route strategy.		
Filter Policy			
Policy Type	Select from "access-list" and "prefix-list".		
Policy Name	User-defined prefix-list name.		
Policy in/out	Select from "in" and "out".		
Interface	Select interface from "cellular0", "LAN1/WAN" and "Bridge0".		
Passive Interface			
Passive Interface	Select interface from "cellular0" and "LAN1/WAN", "Bridge0".		
Interface			
Interface	Select interface from "cellular0", "LAN1/WAN" and "Bridge0".		
Send Version	Select from "default", "v1" and "v2".		
Receive Version	Select from "default", "v1" and "v2".		
Split-Horizon	Select from "enable" and "disable".		
Authentication Mode	Select from "text" and "md5".		
Authentication String	The authentication key for package interaction in RIPV2.		
Authentication Key-chain	The authentication key-chain for package interaction in RIPV2.		
Neighbor			
IP Address	Set RIP neighbor's IP address manually.		
Network			
IP Address	The IP address of interface for RIP publishing.		
Netmask	The netmask of interface for RIP publishing.		

Table 3-2-7-3

3.2.7.3 OSPF

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

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

as the Router ID. The selection order is as follows:

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

Five types of packets of OSPF:

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

Neighbor and Neighboring

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

Static Routing	RIP	OSPF	Routing Filtering
OSPF Settings			
Enable			
Router ID			
ABR Type	cisco		¥
RFC1583 Compatibility			
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.
	Enable/Disable
OSPF Opaque-LSA	LSA: a basic communication means of the OSPF routing
	protocol for the Internet Protocol (IP).
SDE Dolov Timo	Set the delay time for OSPF SPF calculations.
SPF Delay Time	Range: 0-6000000, in milliseconds.
CDE Initial haldtime	Set the initialization time of OSPF SPF.
SPF Initial-holdtime	Range: 0-6000000, in milliseconds.
	Set the maximum time of OSPF SPF.
SPF Max-holdtime	Range: 0-6000000, in milliseconds.
Reference Bandwidth	Range: 1-4294967, in Mbit.

Table 3-2-7-4 OSPF Parameters

Interface						
Interface	Hello Interva	al(s) Dead Inte	rval(s)	letransmit nterval(s)	Transmit Delay(s)	Operation
Bridge0	▼ 10	40	5		1	×
Interface Advanced O	ptions 🖂					Ħ
Interface Netwo	ork Cost	Priority	Authenticat ion	Key ID	Key	Operation
Bridge v broad	I v 10] [1				×
						H

Figure 3-2-7-5

Item	Description
Interface	
Interface	Select interface from "cellular0","WAN" and "Bridge0".
	Send interval of Hello packet. If the Hello time between two adjacent
Hello Interval (s)	routers is different, the neighbour relationship cannot be established.
	Range: 1-65535.
Deed Interval (a)	Dead Time. If no Hello packet is received from the neighbours within the
	dead time, then the neighbour is considered failed. If dead times of two
Dead Interval (s)	adjacent routers are different, the neighbour relationship cannot be
	established.
	When the router notifies an LSA to its neighbour, it is required to make
Retransmit Interval	acknowledgement. If no acknowledgement packet is received within the
(s)	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 C	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.
AuthenticationSet the authentication mode that will be used by the OSPF area.AuthenticationSimple: 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	etmask	Area ID	Operation
				B
Neighbor				
IP Address	Р	riority	Poll	Operation
				æ
Area				
Area ID	Area	No Summary	Authentication	Operatio
				•



Item	Description			
Passive Interface	Passive Interface			
Passive Interface	Select interface from "cellular0", "LAN1/WAN" and "Bridge0".			
Network				
IP Address	The IP address of local network.			
Netmask	The netmask of local network.			
Area ID	The area ID of original LSA's router.			
Area				
Area ID	Set the ID of the OSPF area (IP address).			
Area	Select from "Stub" and "NSSA".			
	The backbone area (area ID 0.0.0.0) cannot be set as "Stub" or "NSSA".			

o Summary	Forbid route summarization.					
uthentication	Select authentication from "simple" and "md5".					
	Table	e 3-27-6 OSPF Para	meters			
Area Advanced Options						
Area Range						
Area ID	IP Address	Netmask	No Advertise	Cos	t	Operation
						Ð
Area Filter						
Area ID		Filter Type		ACL Name		Operation
						•
Area Virtual Link						
Area ID ABR Address	Authentica tion Key ID	Key Hello Interval	Dead Interval	Retransmit Interval	Transmit Delay	Operation
						•

Figure 3-2-7-7

Area Advanced Opti	ions
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.
Key	The authentication key for OSPF packet interaction.
Hello Interval	Set the interval time for sending Hello packets through the interface. Range: 1-65535.
Dead Interval	The dead interval time for sending Hello packets through the interface. Range: 1-65535.
Retransmit	The retransmission interval time for re-sending LSA. Range: 1-65535.

Interval				
Transmit Delay	The delay time for LSA	transmission. Range: 1	-65535.	
	Table 3-2	-7-7 OSPF Parameters		
Redistribution				

Redistribution Type	Metric	Metric	Туре	Route Map	Operation
connected •		1	•		×
					Đ
Redistribution Advanced Options	•				
Always Redistribute Default Route					
Redistribute Default Route Metric	0				
Redistribute Default Route Metric Type	1	•			
Distance Management					
Агеа Тур	e		Distance		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 Advanced	Options	
Always Redistribute	Cand radiatribution default route ofter starting up	
Default Route	Send redistribution default route after starting up.	
Redistribute Default	Send redistribution default route metric. Range: 0-16777214.	
Route Metric	Send redistribution default route metric. Range. 0-10777214.	
Redistribute Default	Select from "0", "1" and "2".	
Route Metric Type		
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

RIP	OSPF	Routing F	iltering				
Act	tion	Match Any	IP Ad	dress	Netr	nask	Operation
deny	•						×
							Ð
Sequence Number	Action	Match Any	IP Address	Netmask	GE Length	LE Length	Operation
	deny 🔻						×
	Act deny Sequence	Action deny	Action Match Any deny Sequence Action Match Any	Action Match Any IP Ad deny Sequence Action Match Any IP Address	Action Match Any IP Address deny Sequence Action Match Any IP Address Netmask	Action Match Any IP Address Netr deny Sequence Action Match Any IP Address Netmask GE Length	Action Match Any IP Address Netmask deny Image: Constraint of the second se

Figure 3-2-7-9

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

Table 3-2-7-9 Routing Filtering Parameters

3.2.8 VRRP

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

an IP sub-network.

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

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

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

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

VRRP has the following characteristics:

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

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

Status	VRRP	
Network	VRRP Status	DISABLE
Interface	VRRP Settings	
DHCP	Enable	
Firewall	Interface	Bridge0 •
Filewall	Virtual Router ID	1
QoS	Virtual IP	
VPN	Priority	100
IP Passthrough	Advertisement Interval (s)	1
n i usatirougi	Preemption Mode	
Routing	IPV4 Primary Server	8.8.8
VRRP	IPV4 Secondary Server	114.114.114.114
DDNS	Interval	300 s
	Retry Interval	5 s
System •	Timeout	3 s
	Max Ping Retries	3
Industrial		
Maintenance	Save	

Figure 3-2-8-1

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.		
Priority	The VRRP priority range is 1-254 (a bigger number indicates a higher priority). The router with higher priority will be more likely to become the gateway router.	100	
Advertisement Interval (s)	Heartbeat package transmission time interval between routers in the virtual ip group. Range: 1-255.	1	
Preemption Mode	If the router works in the preemption mode, once it finds that its own priority is higher than that of the current gateway router, it will send VRRP notification package, resulting in re-election of gateway router and eventually replacing the original gateway router. Accordingly, the original gateway router will become a Backup router.	Disable	
IPV4 Primary Server	The router will send ICMP packet to the IP address or hostn ame to determine whether the Internet connection is still av ailable or not.	8.8.8.8	
IPV4 Secondary Server	The router will try to ping the secondary server name if prim ary server is not available.	114.114. 114.114	
Interval	Time interval (in seconds) between two Pings.	300	
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again every retry interval.	5	
Timeout	The maximum amount of time the router will wait for a resp onse to a ping request. If it does not receive a response for the amount of time defined in this field, the ping request will be considered as failure.	3	
Max Ping Retries	The retry times of the router sending ping request until dete rmining that the connection has failed.	3	

Table 3-2-8-1 VRRP Parameters

Related Configuration Example

VRRP Application Example

3.2.9 DDNS

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

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

DDNS Status	
Status	-
DDNS Method List	
Enable	0
Name	
Service Type	DynDNS 🗸
Username	
User ID	
Password	
Server	
Server Path	
Hostname	
Append IP	
Use HTTPS	

Figure 3-2-9-1

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.

Use HTTPS	Enable HTTPS for some DDNS providers.	
Table 3-2-9-1 DDNS 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

System Time General Email Storage System Hostname ROUTER Web Login Timeout(s) 1800 Encrypting Cleartext Passwords 1 HTTPS Certificates Certificate https.crt Browse Delete Import Export Key Import Delete https.key Browse Export Save

General settings include system info and HTTPS certificates.

Figure 3	3-3-1-1
----------	---------

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

click "Import" button to upload the file into router. Click	
"Export" button will export file to the PC.	
Click "Delete" button will delete the file.	

Table 3-3-1-1 General Setting Parameters

3.3.1.2 System Time

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

time when configuring the router.

Status	General	System Time	Email	Storage	
Network •	System Time Se	ttings			
	Current Time		2020-04-30 17:58	3:27 Thur	
System	Time Zone		8 China (Beijing)	T	
General Settings	Sync Type		Sync with NTP S	Server 🔻	
Phone & SMS	Primary NTP Serv	er	1.cn.pool.ntp.org	•	
	Secondary NTP S	Secondary NTP Server		•	
User Management					
SNMP	NTP Server				
	Enable NTP Serve	er			
AAA					
Device Management	Save				

Figure 3-3-1-2

Status	General	System Time	Email	Storage	
Network •	System Time S	ettings			
	Current Time		2020-04-30 17:5	3:45 Thur	
System 👻	Time Zone		8 China (Beijing)	
General Settings	Sync Type		Set up Manually	•	
Phone & SMS	Date		2020-04-30		
User Management	Time		17 • 58	▼ 45 ▼	
SNMP	Save				
ААА					

Figure 3-3-1-3

Status	General	System Time	Email	Storage	
Network 🕨	System Time S	ettings			
	Current Time		2020-04-30 18:)1:37 Thur	
System	Time Zone		8 China (Beijin	g) v	
General Settings	Sync Type		GPS Time Syn	chronization v	
Phone & SMS	Save	1			
User Management					
SNMP					
ΑΑΑ					

Figure 3-3-1-4

Status	General	System Time	Email	Storage	
Network 🕨	System Time Se	ettings			
	Current Time		2020-04-30 18:0	1:48 Thur	
System	Time Zone		8 China (Beijing) •	
General Settings	Sync Type		Sync with Brows	ser 🔻	
Phone & SMS	Browser Time		2020-04-30 18:0	1:48 Thur	
User Management	Save				
SNMP					
ААА					

Figure 3-3-1-5

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.
GPS Time Synchronization	Synchronize time with GPS.
Primary NTP Server	Enter primary NTP Server's IP address or domain name.
Secondary NTP Server	Enter secondary NTP Server's IP address or domain name.
NTP Server	

Enchle NED Conver	NTP client on the network can achieve time synchronization with router
Enable NTP Server	after "Enable NTP Server" option is checked.

Table 3-3-1-2 System Time Parameters

3.3.1.3 Email

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

System 👻	General	System Time	Email	Storage
General Settings	SMTP Client Set	tings		
Phone & SMS	Enable			
User Management	Email Address Password			
SNMP	SMTP Server Add	ress		
ААА	Port	25		
Device Management	Encryption	STARTTLS	¥	
Events	Test			

Figure 3-3-1-6

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

Table 3-3-1-3 SMTP Setting

General	System Time	Email	Storage			
Email List						
	Email Address			Description		Operation
						\times
						•
Email Group List						
	Grou	p ID				
	Desc	ription				
		List		Selected	1771	
			 ▲ > > <li< td=""><td></td><td>*</td><td></td></li<>		*	
			*		*	
			Save	Cancel		

Figure 3-3-1-7

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

Table 3-3-1-4 Email Settings

Related Topics

DI Setting Events Setting Events Application Example

3.3.1.4 Storage

You can view Micro SD card information on this page.

atus	Available
torage (Capacity/Available)	7.2G/6.8G(1%)



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.
Format	Format the Micro SD card.

Table 3-3-1-5 Storage Information

3.3.2 Phone&SMS

3.3.2.1 Phone

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

Phone	SMS						
Phone Num	ber List						
	Num	ber		ì	Description		Operation
							×
							8
Phone Grou	p List						
		Group ID					
		Description					
		List	_		Selected	1001	
						*	
			Ţ			-	
		1	Save	Cancel			
			Figure 3-3	3-2-1			

Phone	
Item	Description
Phone Number List	
Number	Enter the telephone number. Digits, "+" and "-" are allowed.

Description	The description of the telephone number.		
Phone Group List			
Group ID	Set number for phone group. Range: 1-100.		
Description	The description of the phone group.		
List	Show the phone list.		
Selected	Show the selected phone number.		
	Table 2.2-2-1 Dhone Settinge		

Table 3-3-2-1 Phone Settings

Related Topic

Connect on Demand

3.3.2.2 SMS

SMS settings involve in remote SMS control, sending SMS and SMS receiving and sending status.

Status	Phone SMS	
Network 🕨	General Setting	
	SMS Mode	PDU 🔻
System 🔻	SMS Remote Control	 Image: A start of the start of
General Settings	Authentication Type	Password+Phone •
	Password	
Phone & SMS	Phone Group	
User Management		
SNMP	Save	

Figure 3-3-2-2

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 3-3-2-2 SMS Remote Control Parameters

Send SMS					
Phone Number					
Content					
Send					
Inbox					
From	То	Sender	Search Clear All		
	Sender	Time		Content	
< 1 > 10 v Go to	r GO				
Outbox					
From	То	Recipient	Search Clear A		
R	ecipient	Time	Content	Status	
< 1 > 10 🗸 Go to	c. GO				

Figure 3-3-2-3

SMS			
Item	Description		
Send SMS			
Phone Number	Enter the number to receive the SMS.		
Content	SMS content.		
Inbox/Outbox			
Sender	SMS sender from outside.		
Recipient	SMS recipient which IOT-R32 send to.		
From	Select the start date.		
То	Select the end date.		
Search	Search for SMS record.		
Clear All	Clear all SMS records in web GUI.		

Table 3-3-2-3 SMS Settings

3.3.3 User Management

3.3.3.1 Account

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

Status		Account User Management	
Network	F	Change Account Info	
		Username admin	
System	-	Old Password	
		New Password	
General Settings		Confirm New Password	
Phone & SMS			
User Management		Save	

Figure 3-3-3-1

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 3-3-3-1 Account Settings

3.3.3.2 User Management

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

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

Figure 3-3-3-2

User Manager	User Management		
ltem	Description		
Username	Enter a new username. You can use characters such as a-z, 0-9, "_", "-", "\$". The first character can't be a digit.		
Password	Set password.		
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 3-3-3-2 User Management

3.3.4 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

3.3.4.1 SNMP

IOT-R32 supports SNMPv1, SNMPv2c and SNMPv3 version. SNMPv1 and SNMPv2c employ community name authentication. SNMPv3 employs authentication encryption by username and password.

NMP Setting	gs			
Enable				
Port		161		
SNMP Version		SNMPv2		•
Location Information		225_location		
Contact Information		225_Conta	act	



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

Contact Information Fill in the contact informati	on.
---	-----

Table 3-3-4-1 SNMP Parameters

3.3.4.2 MIB View

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

SNMP	MIB View	VACM	Тгар	MIB	
View List					
v	iew Name		Filter	View OID	Operation
All		Included	•	1	×
system		Included	•	1.3.6.1.2.1.1	
					Ŧ

Figure 3-3-4-2

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 3-3-4-2 MIB View Parameters

3.3.4.3 VACM

This section describes how to configure VCAM parameters.

SNMP	MIB View	VACM	Trap	MIB		
NMP v1 & v2	2 User List					
Corr	nmunity	Permissio	n	MIB View	Network	Operation
private		Read-Write	• AI	I	▼ 0.0.0.0/0	×
public		Read-Write	▼ AI	1	▼ 0.0.0.0/0	×

Figure 3-3-4-3

VACM			
Item		Description	
SNMP v1 & v2 U	SNMP v1 & v2 User List		
Community	Set the community	Set the community name.	
Permission	Select from "Read-	-Only" and "Read-Write".	

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

Table 3-3-4-3 VACM Parameters

3.3.4.4 Trap

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

SNMP	MIB View	VACM	Тгар	MIB
SNMP Trap				
Enable				
SNMP Version		SNMPv2		T
Server Address	6			
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 3-3-4-4 Trap Parameters

3.3.4.5 MIB

This section describes how to download MIB files. The last MIB file "LTE-ROUTER-MIB.txt" is for the IOT-R32 router.

SNMP	MIB View	VACM	Тгар	MIB
MIB Download				
MIB File		LTE-ROU	TER-MIB.D 🔻	Download

Figure 3-3-4-5

MIB		
1IB file to PC.		
M		

3.3.5 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.

3.3.5.1 Radius

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

Radius	Tacacs+	LDAP	Authentication
Radius Settin	gs		
Enable		۲	
Server IP Addr	ess		
Server Port		1812	
Shared Secret			
_	_		
Save			

Figure 3-3-5-1

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

Table 3-3-5-1 Radius Parameters

3.3.5.2 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.

Radius	Tacacs+	LDAP	Authentication
Tacacs+ Sett	ings		
Enable			
Server IP Add	ress		
Server Port		49	
Shared Secret	t		
	_	8	
Save			

Figure 3-3-5-2

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 3-3-5-2 TACACS+ Parameters

3.3.5.3 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.

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



LDAP	
Item	Description
Enable	Enable or Disable LDAP.
Server IP Address	Fill in the LDAP server's IP address/domain name. The
Server IF Address	maximum count is 10.
Server Port	Fill in the LDAP server's port. Range: 1-65535
Base DN	The top of LDAP directory tree.
Security	Select secure method from "None", "StartTLS" and "SSL".

Username	Enter the username to access the server.
Password	Enter the password to access the server.

Table 3-3-5-3 LDAP Parameters

3.3.5.4 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.

hentication	Settings					
Serv	vice	1	2		3	
Cons	sole	None	None	Ŧ	None	۳
We	b	None	None	¥	None	. T
Telr	net	None	None	¥	None	٧
\$\$	Н	None	None	Ŧ	None	: v

Figure 3-3-5-4

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 3-3-5-4 Authentication Parameters

3.3.6 Device Management

3.3.6.1 DeviceHub

You can connect the device to the Linovision DeviceHub on this page so as to manage the router centrally and remotely. For more details please contact *Linovision support*.

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

Figure 3-3-6-1

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 DeviceHub account (email) and	
Password	password.	

Table 3-3-6-1

3.3.6.2 Linovision VPN

You can connect the device to the Linovision VPN on this page so as to manage the router and connected devices centrally and remotely. For more details please contact *Linovision support*.

Linovision VPN
18443
Disconnected
æ



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

Table 3-3-6-2

3.3.7 Events

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

3.3.7.1 Events

You can view alarm messages on this page.

Status	Events	Events Settings		
Network	Mark as Read	Delete	All as Read Delete All Ala	arms
System 🔻	Sta	tus Type	Time	Message
General Settings	< > 10 ▼	Go to: GO		
User Management				
SNMP				
AAA				
Events				

Figure 3-3-7-1

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 3-3-7-1 Events Parameters

3.3.7.2 Events Settings

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

Events Settings

Events Settings

Events

Enable	
Phone Group List	•
Email Group List	•

Events	Record	Email 🗔 Email Group List	SMS Phone Group List	SNMP
System Startup				
System Reboot				
System Time Update				
VPN Up				
VPN Down				
WAN Up				
WAN Down				
Link switch				
Weak Signal				
Cellular Up				

Figure 3-3-7-2

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

Figure 3-3-7-3

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	
Record	"Event" page if this option is checked.	
Email	The relevant content of event alarm will be sent out via email	
LIIIdii	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
31013	if this option is checked.
CMC Catting	Click and you will be redirected to the page of "Phone" to
SMS Setting	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 4-3-7-2 Events Parameters

Related Topics

Email Setting

Events Application Example

3.4 Industrial Interface

IOT-R32 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.

Status		DI DO			
Network	×	DI Setting			
		Enable			
System	•	Mode	High Level	¥	
the second		Duration(ms)	100		
Industrial		Action	SMS Email	DO	Cellular UP
VO		Save			
Serial Port		Jave			



DI	
ltem	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.

Status	Î	DI DO		
Network	•	DO Setting		
		Enable		
System	•	Mode	High Level	¥
		Duration(*10ms)	100	
Industrial	•		kin	
I/O		Save		

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.

Status	Serial		
Network 🕨	Serial Settings		
	Enable		
System 🕨	Serial Type	RS232	Ŧ
	Baud Rate	9600	۲
Industrial	Data Bits	8	Ŧ
I/O	Stop Bits	1	۲
Serial Port	Parity	None	Ŧ
	Software Flow Contr	rol 💼	
Modbus Slave	Serial Mode	DTU Mode	۲
Modbus Master	DTU Protocol	Transparent	Ŧ

Figure 3-4-2-1

Serial Settings			
Item	Description	Default	
Enable	Enable or disable serial port function.	Disable	
Serial Type	RS232 or RS485.		
Baud Rate	Range is 300-230400. Same with the baud rate of the connected terminal device.	9600	
Data Bits	Options are "8" and "7". Same with the data bits of the connected terminal device.	8	
Stop Bits	Options are "1" and "2". Same with the stop bits of the connected terminal device.	1	
Parity	Options are "None", "Odd" and "Even". Same with the parity of 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" , "Modbus Master", "Modbus Slave" and "GPS".	Disable	
DTU Mode	In DTU mode, the serial port can establish communication with the remote server/client.		
GPS	In GPS mode, go to "Industrial > GPS > GPS Serial Forwarding" 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 basic parameters.		

Table 3-4-2-1 Serial Parameters

Serial Mode	DTU Mode	v		
DTU Protocol	Transparent	•		
Protocol	ТСР	•		
Keepalive Interval	75	s		
Keepalive Retry Times	9			
Packet Size	1024	Bytes		
Serial Frame Interval	100	ms		
Reconnect Interval	10	s		
Specific Protocol				
Register String				
Destination IP Address	S			
Server Ad	Idress	Server Port	Status	Operat
				•

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 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	100	

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	Description	Default	
Transparent			
Protocol	Select "TCP" or "UDP" protocol.	ТСР	
Keepalive Interval (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.		
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.		
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 Protocol	col By Specific Protocol, the router will be able to connect to the TCP2COM software.		
Heartbeat Interval	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	
Maximum TCP Clients	Specify the maximum number of TCP clients allowed to connect th e router which act as a TCP server.	32	
Connection Timeout	If the TCP server does not receive any data from the slave device w ithin the connection timeout period, the TCP connection will be bro ken.	60	
Reading Interval	Set the interval for reading remote channels. When a read cycle end	100	

Table 3-4-2-2 DTU Pa	arameters
----------------------	-----------

	s, the new read cycle begins until this interval expires. If it is set to 0, the device will restart the new read cycle after all channels have been read.	
Response Timeout	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.	3000
Maximum Retries	Set the maximum retry times after it fails to read.	3

Table 3-4-2-3 DTU Parameters

Related Configuration Example

DTU Application Example

3.4.3 Modbus Slave

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	Modbus TCP	Modbus RTU	Modbus RTU Over TCP
Network	Modbus TCP		
	Enable		
System 🕨	Port	502	
	DI Address	0	
Industrial 🔻	DO Address	0	
VO			
Serial Port	Save		
Modbus Slave			



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, 2-255.	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	Modbus TCP	Modbus RTU	Modbus RTU Over TCP
Network 🕨	Modbus RTU		
	Enable		
System	Serial Port	serial	Ŧ
	Slave ID	1	
Industrial 🔻	DI Address	0	
I/O	DO Address	0	
Serial Port	Save		
Modbus Slave			

Figure 3-4-3-2

Modbus RTU					
ltem	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, 2-255.	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	٠	Modbus RTU Over 1	ср П			
System	۲	Slave ID Device ID	1			
Industrial	-	Reconnect Interval	10	s		
VO		DI Address DO Address	0			
Serial Port		Server List	U			
Modbus Slave						
Modbus Master		IF	(Port	Status	Operation
CDC						œ

Figure 3-4-3-3

Modbus RTU Over TCP						
ltem	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, 2-255.	0				
Server List						
IP	Enter the IP address of the server.					
Port	Enter the port of the server.Range: 0-65535.					
Status	Status Show the connection status between the router and the server.					
	Table 2.4.2.2 Madhua DTU Over TCD Decemptore					

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

3.4.4 Modbus Master

IOT-R32 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.

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		Read
Modbus Slave		Save & Apply		
Modbus Master				

Figure 3-4-4-1

Modbus Master						
Item	Description					
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 Ma	ster	Char	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 ⁱ	TCP 🔻				0	×
										H



Channel Settin	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.					
Туре	Read command, options are "Coil", "Discrete", "Holding Register (INT16)", "Input 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.
Decimal Place	Used to indicate a dot in the read into the position of the channel. For example: read 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

	[
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
Continuous Alarm	

Figure 3-4-4-3

Alarm Setting	Alarm Setting		
ltem	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		
Threshold	than 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	Select the phone group to receive the alarm SMS.		
Group			
Email Group	Select the Email group to receive the alarm Email.		
Normal	When the actual value is restored to the normal value from exceeding		
Content	the threshold value, the router will automatically cancel the abnormal		

	alarm and send the preset normal content to the specified phone group.
Abnormal Content	When the actual value exceeds the preset threshold, the router will automatically trigger the alarm and send the preset abnormal content to the specified phone group.
Continuous Alarm	Once it is enabled, the same alarm will be continuously reported. Otherwise, the same alarm will be reported only one time.

Table 3-4-4-3

TCP Fo	rwa	di	n	g
--------	-----	----	---	---

Name	IP	Port	Operation
All			×

Figure 3-4-4-4

TCP Forwa	arding
Item	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.

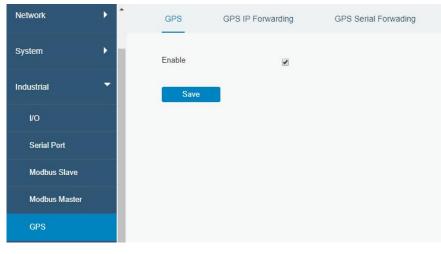


Figure 3-4-5-1

3.4.5.2 GPS IP Forwarding

GPS G	PS IP Forwarding	GPS S	erial Forwading
Enable			
Туре	Client	۲	
Protocol	TCP Protocol	•	
Keepalive Interval	75		s
Keepalive Retry	9		times
Reconnect Interval	10		s
Report Interval	30		s
Include RMC			
Include GSA			
Include GGA			
Include GSV			
Message Prefix			
Message Suffix			

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

Figure 3-4-5-2

Destination IP Address			
Server Address	Server Port	Status	Operation
			8

Figure 3-4-5-3

GPS IP Forwarding			
ltem	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. Afterit 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 A	ddress	
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.

GPS	GPS IP Forwarding	GPS Serial Forwading
GPS Serial Fo	rwading	
Enable		
Serial Type	Serial	T
Trap Interval	30	
Include RMC		
Include GSA		
Include GGA		
Include GSV		



GPS Serial Forwarding			
Item Description Default		Default	
Enable	Forward the GPS data to the preset serial port.	Disable	
Serial Type	Select the serial port to receive GPS data.	Serial	

Report Interval	Router will forward the GPS data to the serial port 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.	

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, packet analyzer and qxdmlog.

3.5.1.1 Ping

Ping tool is engineered to ping outer network.

System	•	Ping	Traceroute	Packet Analyzer	Qxdmlog
Industrial	•	IP Ping			Ping Stop
Maintenance	-	11001			Thig
Tools					



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.

Ping	Traceroute	Packet Analyzer	Qxdn	nlog
Traceroute				
Host			Trace	Stop



Traceroute		
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.

Ping	Traceroute	Packet Analyzer	Qxdmlog
Packet Ana	alyzer		
Ethernet Int	erface	Any	Ŧ
IP Address			
Port			
Advanced			
Start	Stop	Download	

Figure 3-5-1-3

Packet Analyzer		
Item	Description	
Ethernet Interface	Select the interface to capture packages.	
IP Address Set the IP address that the router will capture.		
Port	Set the port that the router will capture.	
Advanced	Set the rules for sniffer. The format is tcpdump.	
	Table 3-5-1-3 Packet Analyzer Parameters	

3.5.1.4 Qxdmlog

This section allow collecting diagnostic logs via QXDM tool.

Ping	Traceroute	Packet Analyzer	Qxdmlog
Start	Stop	Download	

Figure 3-5-1-4

3.5.2 Debugger

3.5.2.1 Cellular Debugger

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

Cellular Debugger	Firewall Debugger	
Cellular Debugger		
Command	Eg: AT+CGREG? Send	
View Recent Logs (lines)	20 •	
Result	2020-05-08 19:23:38: [SEQ2,ID2]<<< OK	
		efresh

Figure 3-5-2-1

Cellular Debugger		
Item	Description	
Command	Enter the AT command that you want to send to cellular modem.	
View Recent Logs (lines) View the specified lines of the result.		
Result	Show the response result from cellular modem.	
	Table 3-5-2-1 Cellular Debugger Parameters	

Table 3-5-2-1 Cellular Debugger Parameters

3.5.2.2 Firewall Debugger

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

Cellular Debugger	Firewall Debugger	
Firewall Debugger		
Command	Eg: -t nat -nvL INPUT Send	L.
Result		
	Clear Log Download	

Figure 3-5-2-2

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

Table 3-5-2-2 Firewall Debugger Parameters

3.5.3 Log

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

3.5.3.1 System Log

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

System Log	Log Download	Log Settings				
Log						
View recent(lines)	2	0	T			
Fri May 8 19:32:32 Fri May 8 19:32:35 Fri May 8 19:32:35 Fri May 8 19:32:36 Fri May 8 19:32:36 Fri May 8 19:32:36 Fri May 8 19:32:38 Fri May 8 19:32:38 Fri May 8 19:32:340 Fri May 8 19:32:40 Fri May 8 19:32:42	2020 daemon.debug vtysl 2020 user.debug httpd[311 2020 user.info : Failed to d 2020 user.info : START 2020 user.debug httpd[311 2020 daemon.debug vtysl 2020 user.debug httpd[311 2020 daemon.info dhclien 2020 user.info : Failed to d 2020 user.info : START 2020 user.debug httpd[311 2020 daemon.debug vtysl	77]: finish yruo_log.get pen GPS device. COLLECTION 77]: ==call yruo_log.get _ubus[1631]: ubus_lib.c. 77]: finish yruo_log.get : No DHCPOFFERS red : No working leases in pen GPS device. COLLECTION 77]: ==call yruo_log.get	c:428 call command 'e ceived. persistent database - s	nd' leeping.		*
				5s	•	Refresh
		Figu	ure 3-5-3-1			

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

Table 5 5 5 1 System Log 1 are

3.5.3.2 Log Download

This section describes how to download log files.

System Log	Log Download	Log Settings		
Download				
				Download All
File 1	Name	File Size/KB	Creation Time	Operation
vpn	log	1	2020/04/30 14:37:55	↓
syste	m.log	872	2020/05/08 19:35:03	↓
http	d.log	645	2020/05/08 19:34:12	↓
firewa	all.log	0	2020/04/30 14:37:09	↓
cellul	ar.log	1619	2020/05/08 19:35:01	.↓

Figure 3-5-3-2

Log Download	
Item	Description
Download All	Download all log files.

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

Table 3-5-3-2 System Log Parameter

3.5.3.3 Log Settings

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

System Log	Log Download		Log Settings		
Remote Log Server					
Enable					
Syslog Server Address					
		544			1
Port		514			
		514			
		Local	1	•	
Local Log File] КВ



Log Settings				
Item	Description			
Remote Log Server				
Enable	With "Remote Log Server" enabled, router will send all system logs to the remote server.			
Syslog Server Address	Fill in the remote system log server address (IP/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 2-5-2-2 Log Settings Parameters			

Table 3-5-3-3 Log Settings Parameters

3.5.4 Upgrade

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

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

Upgrade			
Upgrade			
Firmware Version	32.3.0.2		
Reset Configuration to Factory Default			
Upgrade Firmware		Browse	Upgrade

Figure 3-5-4-1

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

Backup and Restore			
Restore Config			
Config File		Browse	Import
Backup Running-confi	ig		
Backup			
Restore Factory Defau	ilts		
Reset			

Figure 3-5-5-1

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

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

Related Configuration Example

Restore Factory Defaults

3.5.6 Reboot

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

Reboot				
Reboot Device				
Reboot Now				
Schedule				
Enable				
Enable Cycles	Every Day	¥	0	0
			0	 0



Reboot		
Item	Description	
Reboot Now	Reboot the router immediately.	
Schedule		
Enable	Reboot the router at a scheduled frequency.	
Cycles	Select the date and time to execute the schedule.	
	Table 3-5-2-1 Schedule Parameters	

Table 3-5-2-1 Schedule Parameters

3.6 APP

3.6.1 Python

Python is an object-oriented programming language that has gained popularity because of its clear syntax and readability.

As an interpreted language, Python has a design philosophy that emphasizes code readability, notably using whitespace indentation to delimit code blocks rather than curly brackets or keywords, and a syntax that allows programmers to express concepts in fewer lines of code than it's used in other languages such as C++ or Java. The language provides constructs and intends to enable writing clear programs on both small and large scale.

Users can use Python to quickly generate the prototype of the program, which can be the final interface of the program, rewrite it with a more appropriate language, and then encapsulate the extended class library that Python can call.

This section describes how to view the relevant running status such as App-manager, SDK version, extended storage, etc. Also you can change the App-manager configuration, and import the Python App package from here.

3.6.1.1 Python

Micro SD card must be installed for Python App.

Status	Python	AppManager Configuratio	on Python API	P
Network 🕨	Python			
System 🕨	AppManager Status	s Uninsta	lled	
Industrial 🕨	SDK Path Available Storage		×	
Maintenance	SDK Upload		E	Browse Install
арр 🔻				
Python				



Python		
Item	Description	
AppMapagar Status	Show AppManager's running status, like "Uninstalled",	
AppManager Status	"Running" or "Stopped".	
SDK Version	Show the version of the installed SDK.	
SDK Path	Show the SDK installation path.	
Available Storage	Select available storage such as Micro SD to install SDK.	
SDK Upload	Upload and install SDK for Python.	
Uninstall	Uninstall SDK.	

View View application status managed by AppManager.	
---	--

Table 3-6-1-1 Python Parameters

3.6.1.2 App Manager Configuration

Python	AppManager Configuration	Python APP	
AppManager			
Enable			
App Manageme	nt		
IC) App Comn	nand Logfile Size(MB)	Uninstall
App Status			
	App Name	App Version	SDK Version

Figure 3-6-1-2

AppManager Configuration		
Item	Description	
Enable	After enabling Python AppManager, user can click "View" button on the "Python" webpage to view the application status managed by AppManager.	
App Management		
ID	Show the ID of the imported App.	
App Command	Show the name of the imported App.	
Logfile Size(MB)	User-defined Logfile size. Range: 1-50.	
Uninstall	Uninstall APP.	
App Status		
App Name	Show the name of the imported App.	
App Version	Show the version of the imported App.	
SDK Version	Show the SDK version which the imported App is based on.	

Table 3-6-1-2 APP Manager Parameters

3.6.1.3 Python App

Python	AppManager Configuration	Python APP
Import App P	ackage	
App Package		Browse Import
Import App C	onfiguration	
App Name		•
App Configurat	tion	Browse Import
Debug Script		
Debug File		Export
Debug Script		Browse



Python APP		
Item	Description	
App Package	Select App package and import.	
App Name	Select App to import configuration.	
App Configuration	Select configuration file and import.	
Debug File	Export script file.	
Debug Script	Select Python script to be debugged and import.	

Table 3-6-1-3 APP Parameters

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.

System 🕨	Backup and Restore
Industrial •	Restore Config
Maintenance	Config File Import
Tools	Backup
Debugger	Restore Factory Defaults
Log	Reset
Upgrade	
Backup and Restore	
	Figure 4-1-1-1

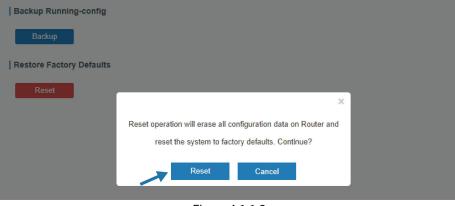


Figure 4-1-1-2

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	

Figure 4-1-1-3

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

Related Topic

Restore Factory Defaults

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 5 seconds.
Static Green → Rapidly Blinking	Release the button and wait.
$Off \rightarrow Blinking$	The router is now reset to factory defaults.

Table 4-2-1

4.2 Firmware Upgrade

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

- 1. Go to "Maintenance > Upgrade".
- 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.

Network	ľ	Upgrade			
System	•	Upgrade			
Industrial	•	Firmware Version	32.3.0.1		
		Reset Configuration to Factory Default			
Maintenance		Upgrade <mark>Firmwa</mark> re	C:\fakepath\32.3.0.2.bin	Browse	Upgrade
Tools					
Debugger					
Log					
Upgrade					
Related Topic		Figure 4-2-1			

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.

Table 4-3-1

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.

Events	Events Settings				
Events Settings					
Enable					
Phone Group List			•		
Email Group List		1	•		
Eve	nts	Record	Email Email Setting	SMS SMS Setting	SNMP
System	Startup				
System I	Reboot				



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

General S	system Time	Email	Storage
SMTP Client Setting	5		
Enable			
Email Address	andy@linovision	n.com	
Password	•••••		
SMTP Server Address	stmp.linovision.	com	
Port	25		
Encryption	STARTTLS	~	
Encryption	STARTTLS	~	

Figure 4-3-2

	Email Address		Description	Operation
	andy@linovision.com		upport	×
				Ŧ
mail Group	Group ID	Description	Email Address	Operatio

Figure 4-3-3

4. 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.

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

Figure 4-3-4

Related Topics

Events

Email Setting

4.4 SNMP Application Example

Before you configure SNMP parameters, please download the relevant "MIB" file from the IOT-R32'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 "LTE-ROUTER-MIB.txt" to PC.

System 🔻	SNMP	MIB View	VACM	Тгар	MIB	
General Settings	MIB Downloa	d				
Phone & SMS	MIB File		LTE-ROU	ITER-MIB.b 🔻	Download	
User Management						
SNMP						
AAA						

Figure 4-4-1

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

Eile Edit View Operations	Help 陷 🐃 🗊 💋	🏹 🖄 🛅 🛎 🍲	Q g 🔁	u 👌 🧇 🚺	Download Nore Free Tools
Loaded MibModules 		calhost	✓ Port Write Cor	161 nmunity	~
	Set Value Device Type Device Type Identif		~	C F	Reload
	Suggested OIDs Object ID	None		~	
	Loading MIBs Failed	ers\Ursalink\Desktop\LTE-ROUTE			
	Done.				,

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

ile Edit View Operations Help S 💑 🗊 🕺 階 🜇 🛸 🐲 💋	· 🔨 🖄 🛙	🗈 🐞 🛫 🚥	0 ₀ 🔁	🛛 🖬 🎒 🧇	Download More Free Tools	
enterprises iterouter if RouteManagement if RouteInfos if RouterInfos if RouterInfo if Rout	Community Set Value Device Type Device Type Ider Suggested OIDs Dbject ID oading MIBs Fail oading MIBs C:\L oading MIBs Fail	None et. private. enterpris ed: Jsers\Ursalink\Deskt	es.lteroute	TER-MIB.txt	C Reloa	
	escription Mul Syntax Access	tiVar		Status Reference		
		3. 6. 1. 4. 1. 50234. 1. 1	.3			

Figure 4-4-3

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

SNMP	MIB View	VACM	Тгар	MIB
SNMP Settin	gs			
Enable				
Port		161		
SNMP Version	n	SNMPv2	2	~
Location Infor	mation	Hangzho	u-China	
Contact Inform	nation	Hangzho	u-Linovision	
Save				
	Fic	ure 4-4-4		

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.

w List						
١	/iew Name		View Filter	i.	View OID	Operatio
cellular		Include	d	•	1.3.6.1.4.1.50234.1.3	
Save						

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

authority for the specified view from the specified outside network. Click "Save" and "Apply" to make the changes take effect.

SNMP v1 & v2 User List Community Perm			
Community Perm			
	nission MIB View	Network	Operation
public Read-Write	▼ cellular	▼ 0.0.0.0/0	



6. Go to MibBrowser, enter host IP address, port and community. Right click "usCellular CurrentSim"

and then click "FET". Then you will get the current SIM info on the result box. You can get other cellular info in the same way.

ManageEngine MibBrowser Free Tool <u>File Edit View Operations H</u> elp						_		×
🗞 📥 🗊 ጰ 🖻 🖻 👘 🧊 👔	🔊 🔨 🖄	🛅 🐞 🛫 🖣	🤌 🧠 🔁	830	۹ 🚺	Download More Free Tools	5	
aded MibModules	Host Community Set Value	192.168.22.225	public	Port Write Commu	161 Inity			~
trRouterInfo trNetworkInfo TrAllularInfo trAllularInfo trAllularInfo trAllularInfo	Device Type Device Type Id Suggested OII		ble			C Rel	load	
ricellularModel ricellularModemStat ricellularSignal ricellularRegister ricellularICCID ricellularPLMNID	Object ID Loading MIBs F Loading MIBs C	. iso. org. dod. inter ailed: :\Users\Ursalink\Des			router.rtRo	uteManagemen	t.rtRout	erIn
	Done. Sent GET reque	est to 192.168.22.225	: 161 Result					
	Description M		(court					*
tCelluarNetworkStat rest of the second sec		OCTET STRING		Status Reference	current			
<	Index	1. 3. 6. 1. 4. 1. 50234. 1	131					
Global View	Description	"The current SIN						

Figure 4-4-7

Related Topic

<u>SNMP</u>

4.5 Network Connection

4.5.1 Cellular Connection

The IOT-R32 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 IOT-R32 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.

Status	Link Failover Cellular	Port WAN	Bridge	Switch	Loopback
Network	Cellular Settings				
Network		SIM1	S	SIM2	
Interface	APN	vodafone			
DHCP	Username				
	Password				
Firewall	PIN Code				
QoS	Access Number				
VPN	Authentication Type	Auto	•	Auto	•
IP Passthrough	Network Type	Auto	•	Auto	•
	PPP Preferred				
Routing	SMS Center				
VRRP	Enable NAT			2	
DDNS	Roaming		æ		

Figure 4-5-1

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

2. Go to "Network > Interface > Link Failover" to enable correspond SIM and change link priority.

Status	Ť.	Link Failover	C	Cellular	Port	WAN	Bridge	Switch	Loopback
Network	•	Link Priority							
Interface		Priority	Enable Rule	Link in use	Interface	Connection	Туре	IP	Operation
DHCP		1		٠	Cellular-SIM1			-	
Firewall		2	•		Cellular-SIM2	DHCP		-	
QoS VPN		3		•	WAN	Static IF	0	192.168.22.225	
VIIN									



3. Click $\boxed{2}$ to configure ICMP ping detection information.

Enable		
IPv4 Primary Server	8.8.8.8	
IPv4 Secondary Server	114.114.114	
IPv6 Primary Server	2001:4860:4860::8888	
IPv6 Secondary Server	2400:3200::1	
Interval	300	s
Retry Interval	5	s
Timeout	3	s
Max Ping Retries	3	

Figure 4-5-3

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.

Overview	Cellular	Network	WLAN	VPN	Routing	Host List	GPS	
Modem					Network	t.		
Model		EC20F			Status			Connected
Version		EC20CEHCL	.GR06A05M1G		IPv4 Add	Iress		10.171.227.152/28
Current SIM		SIM1			IPv4 Gat	eway		10.171.227.153
Signal Level		31asu (-51dE	3m)		IPv4 DN	S		211.143.147.120
Register Status		Registered (H	lome network)		IPv6 Add	Iress		2409:8934:1a1e:ca08:9c3f:1718:6fcd:4ad3/64
IMEI		86194205628	39607		IPv6 Gat	eway		2409:8934:1a1e:ca08:8e7:5c15:e8dd:111
IMSI		46000597014	14200		IPv6 DN	S		2409:8034:2000:0:0:0:0:0:4
ICCID		89860051131	I8F2001679		Connecti	ion Duration		0 days, 02:32:02
ISP		CHINA MOBI	ILE		Data Lie	age Monthly		
Network Type		TDD LTE				age monuny		
PLMN ID		46000			SIM-1			RX: 0.0 MIB TX: 0.0 MIB ALL: 0.0 MIB
LAC		592f			SIM-2			RX: 0.0 MIB TX: 0.0 MIB ALL: 0.0 MIB
Cell ID		3d98485						

Figure 4-5-4

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 IOT-R32 router.

Related Topic

Cellular Setting Cellular Status

4.5.2 Ethernet WAN Connection

Example

WAN port of the IOT-R32 is connected with Ethernet cable to get Internet access.

Configuration Steps

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

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.

Status	Link Failover	Cellular	Port	WAN	Bridge	Switch
Network 🔻	— WAN_1					
Interface	Enable	Г			T I	
DHCP	Port		LAN1/WAN			
Firewall	Connection Typ	e	Static IP	v		
QoS	IPv4 Address		192.168.22.225			
VPN	Netmask		255.255.255.0]		
	IPv4 Gateway		192.168.22.1			
IP Passthrough	IPv6 Address		fe80::26e1:24ff:fe	ef0:3192		
Routing	Prefix-length		64			
VRRP	IPv6 Gateway					
DDNS	МТО		1500			
	Primary DNS		8.8.8.8			
System 🕨	Secondary DNS	S				
	Enable NAT		2		_	

Figure 4-5-5

2. Go to "Network > Interface > Link Failover" to change the WAN priority to 1.

Status	Î	Link Failover	(Cellular	Port	WAN E	tridge Switch	Loopback
Network	-	Link Priority						
Interface		Priority	Enable Rule	Link in use	Interface	Connection Ty	pe IP	Operation
DHCP		1	e	•	WAN	Static IP	192.168.22.225	
Firewall		2	•		Cellular-SIM1	DHCP	5	
QoS	_	3	•		Cellular-SIM2			
VPN								

Figure 4-5-6

Related Topic
WAN Setting
WAN Status

4.6 Wi-Fi Application Example (Only Applicable to Wi-Fi Version

4.6.1 AP Mode

Application Example

Configure IOT-R32 as AP to allow connection from users or devices.

Configuration Steps

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

Link Failover	Cellular	Port	WAN	Bridge	WLAN
WLAN					
Enable					
Work Mode	AF	2	~		
BSSID	24:	e1:24:f0:2f:eb			
Radio Type	80	02.11n(2.4GHz)	~		
Channel	Au	uto	~		
Bandwidth	20	MHz	~		
SSID	Ro	uter_F02FEB			
Encryption Mode	W	PA-PSK/WPA2-PSk	< ~		
Cipher	Au	ito	~		
Key	••••				
SSID Broadcast					
AP Isolation					
Guest Mode					
Max Client Number	10				

Figure 4-6-1-1

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

 Use a smart phone to connect the access point of IOT-R32. Go to "Status > WLAN", and you can check the AP settings and information of the connected client/user.

VLAN Status					
Name	Status	Туре	SSID	IP Address	Netmask
WLAN	Running	AP	Router_F02FEB	192.168.1.1	255.255.255.0
Associated Static	ons				
S SI	D	MAC	Address	IP Address	Connection Duration
Router F	02FEB	3c:cd:5c	1:47:10:8e	192.168.1.191	18 seconds

Figure 4-6-1-2

4.6.2 Client Mode

Application Example

Configure IOT-R32 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.

Clie	nt	~	Scan	
WIF	TEST			
3c:c	d:5d:47:10:8e			
WP	A2-PSK	~		
AES	3	~		
•••••	•••			
DH	CP Client	~		
	Clie WIF 3c:co WP, AES	Client WIFI TEST 3c:cd:5d:47:10:8e WPA2-PSK AES DHCP Client	Client ✓ WIFI TEST 3c:cd:5d:47:10:8e WPA2-PSK ✓ AES ✓	Client Scan WIFI TEST 3c:cd:5d:47:10:8e WPA2-PSK AES

Figure 4-6-2-1

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.

	Cellular	Network	WLAN	VPN	Routing	Host List	GP
WLAN Status							
Name	Status	Туре	SSID	IP A	Address	Netmask	
WLAN	Connected	Client	WIFI TEST				
Associated Stati	ons						
Associated Stati							
	SID	MAC Add	Iress	IP Addr	ess	Connection Duration	1



Related Topic

WLAN Setting

WLAN Status

4.7 VRRP Application Example

Application Example

A Web server requires Internet access through the IOT-R32 router. To avoid data loss caused by router breakdown, two IOT-R32 routers can be deployed as VRRP backup group, so as to improve network reliability.

VRRP group:

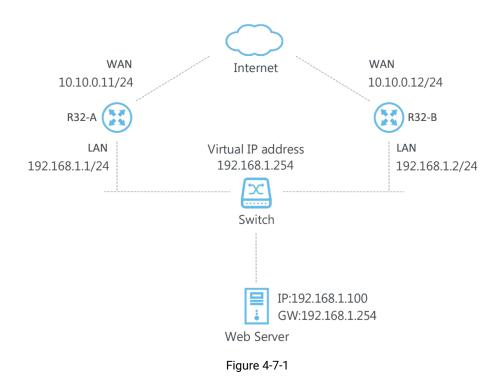
WAN ports of the IOT-R32 Router A and Router B are connected to the Internet via wired network. And LAN ports of them are connected to a switch.

Virtual IP is 192.168.1.254/24.

IOT-R32 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.

Lin	k Failover	Cellular	Port	WAN	Bridge
WAN	N Settings				
-	WAN_1				
	Enable		•		
	Port		LAN1/WAN		
	Connection Type		Static IP	,	•
	IPv4 Address		10.10.0.11		
	Netmask		255.255.255.0		
	IPv4 Gateway		10.10.0.1		
	IPv6 Address		fe80::26e1:24ff.fe	ef0:3192	
	Prefix-length		64		
	IPv6 Gateway				
	мти		1500		
	Primary DNS		8.8.8		
	Secondary DNS				
	Enable NAT				

Figure 4-7-2

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

197

Status	VRRP		
	VRRP Status		
Network 👻	Status	DISABLE	
Interface	VRRP Settings		
	Enable		
DHCP	Interface	Bridge0	v
Firewall	Virtual Router ID	1	
QoS	Virtual IP	192.168.1.254	
VPN	Priority	110	
VPN	Advertisement Interval (s)	1	
IP Passthrough	Preemption Mode		
Routing	IPV4 Primary Server	8.8.8.8	
VRRP	IPV4 Secondary Server	114.114.114.114	
VIUG	Interval	300	:
DDNS	Retry Interval	5	5
System	Timeout	3	5
	Max Ping Retries	3	

Figure 4-7-3

Router B Configuration

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

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

Figure 4-7-4

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

Status	VRRP		
Network 👻	Status	DISABLE	
Network	VRRP Settings		
Interface	Enable		
DHCP	Interface	Bridge0	v
DIICF	Virtual Router ID	1	
Firewall	Virtual IP	192.168.1.254	
QoS	Priority	100	
VPN	Advertisement Interval (s)	1	
	Preemption Mode		
IP Passthrough	IPV4 Primary Server	8.8.8.8	
Routing	IPV4 Secondary Server	114.114.114.114	
VRRP	Interval	300	s
	Retry Interval	5	s
DDNS	Timeout	3	s
System 🕨	Max Ping Retries	3	

Figure 4-7-5

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

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

Related Topics

VRRP Setting

4.8 NAT Application Example

Example

An IOT-R32 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.

M2M ROUTER	R								(5) Apply
			Fo	r your device sec	urity, please	change the def	ault password!		
Status		Security AC	L Port	Mapping 2	DMZ	MAC	Binding	Custom Rules	SPI
Network	1	Port Mapping							
Interface		Source IP	Source Port	Destinati	on IP	Destination Port	Protocol	Description	Operation
DHCP	3	0.0.0.0/0	8000	192.168.1.2		800	TCP 🗸		
Firewall (1)	-								•
QoS		Save 4							
				Figure 4-	8-1				

Click "Save" and "Apply" button.

Related Topic

Port Mapping

4.9 Access Control Application Example

Application Example

LAN port of the IOT-R32 is set with IP 192.168.1.0/24. Then configure the router to deny accessing to Google IP 172.217.160.100 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.

Security	ACL	Port Mapping	DMZ	MAC Binding		Custom Rules	SPI
ACL Setting							
Default Filter Po	blicy	Accept	•				
Access Contro	ol List						
		Туре	[extended	v		
		ID	[100			
		Action	[deny			
		Protocol	[ip	•		
		Source IP	[192.168.1.12			
		Source Wildcard Mask	[0.0.0.255			
		Destination IP	[172.217.160.100			
		Destination Wildcard Mas	k [0.0.0.255			
		Description	[google			
		Sa	ive	Cancel			

Figure 4-9-1

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

Secur	ity	ACL	Port	Mapping	DMZ	MAC Binding	Custom Rules	SPI
ACL Se	etting : Filter Pol	icy	Accep	t	•			
Access	s Contro	l List						
I	D	Action	Protocol	Source IP	Destination I	P More Deta	il Description	Operation
10	00	deny	ір	192.168.1.12/0.0.0. 255	172.217.160.10 0.0.255	0/0.	google	×
								Ð
Interfa	ce List							
		Interface		ln .	ACL		Out ACL	Operation
E	Bridge0		۲	100	۲		Ţ	×
				-				

Figure 4-9-2

Related Topic

4.10 QoS Application Example

Example

Configure the IOT-R32 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

Table 4-10-1

Configuration Steps

Service Category

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

Download Bandwidtl	n	
Enable		
Default Category]
Download Bandwidth	75000	kbits/s
Capacity		

Figure 4-10-1

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

Note: the percents must add up to 100%.

Name	Percent(%)	Max BW(kbps)	Min BW(kbps)	Operation
1	40	30000	25000	
2	60	45000	40000	×

Figure 4-10-2

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 V	1 •	×
ftp2	110.32.91.44	21	1		ANY 🔻	2 •	×

Figure 4-10-3

Note:

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

Click "Save" and "Apply" button.

Related Topic

QoS Setting

4.11 DTU Application Example

Example

PLC is connected with the IOT-R32 via RS232. Then enable DTU function of the IOT-R32 to make a remote TCP server communicate with PLC. Refer to the following topological graph.



Figure 4-11-1

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

Table 4-11-1

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.

Status	÷.	Serial		
		Serial Settings		
Network	•	Enable		
System	•	Serial Type	RS232	¥
System		Baud Rate	9600	¥
Industrial	-	Data Bits	8	T
	_	Stop Bits	1	Ŧ
I/O		Parity	None	•
Serial Port		Software Flow Cor	ntrol 📄	
		Figure 4-11-	2	

2. Configure Serial Mode as "DTU Mode". The IOT-R32 is connected as client in "Transparent" protocol.

System		Serial Mode	DTU Mode	۲	
Industrial	-	DTU Protocol	Transparent	۲	
		Protocol	ТСР	۲	
I/O		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		

Figure 4-11-3

3. Configure TCP server IP and port.

Server Address	Server Port	Status	Operatio
110.87.98.58	7087		×
			E

Figure 4-11-4

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

Destination IP Address			
Server Address	Server Port	Status	Operation
110.87.98.58	7087	Connected	×

Figure 4-11-5

5. Start TCP server on PC.

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

	Protocol P Server	
(2)	Local host II	Р
192	.168.2	. 27
(3) 7087	Local host p	or
78.9	Discon	

Figure 4-11-6

6. Connect the IOT-R32 to PC via RS232 for PLC simulation. Then start "sscom" software on the PC to test communication through serial port.

BaudRa	9600	-	DTR 🗆
DataBi	8	-	Send eve 10
StopBi	1	-	SendHEX 🗆
Verifyl	None	-	Data input:
FlowCon	None	-	helllo

7. After connection is established between the IOT-R32 and the TCP server, you can send data between sscom and Netassit.

PC side

SSCOM3.2	-		×
testtesttesttesttesttesttesttesttest			~
OpenFile FileNm SendFile SaveDa ComNum COMM13 V @ CloseCom Help	ta Clea	ur	HexDat: 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 FlowCo None V hello			
ww.mcu51.cor S:42 R:48 COM13 opened 9600b	ps CTS=	I DSR=	=0 RL

Figure 4-11-8

TCP server side

	NetAssist (V3.7) <u> ×</u>
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	
Tiscolliec(
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 Reov : 177 Reset

Figure 4-11-9

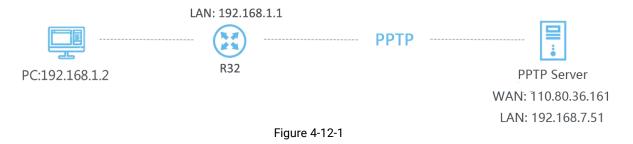
8. After serial communication test is done, you can connect PLC to RS232 port of the IOT-R32 for test.

Related Topic

Serial Port

4.12 PPTP Application Example

Example



Configure the IOT-R32 as PPTP client to connect to a PPTP server in order to have data transferred securely. Refer to the following topological graph.

Configuration Steps

1. 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.

	DMVPN	IPsec	GRE	L2TP	PPTP
	Certifications				
ļ	PPTP Settings				
	- PPTP_1				
	Enable			•	
	Remote IP Address		110.87.98.58		
	Username			pptpserver	
	Password			•••••	
	Authenticat	ion		Auto	٣
	Global Traf	fic Forwarding			
	Remote Subnet				
	Remote Su	bnet Mask			
	Advanced S	Settings			

Figure 4-12-2

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	

Figure 4-12-3

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

DMVPN	IPsec	GRE	L2TP	PPTP	
Show Adv	anced				
Local IP A	Local IP Address				
Peer IP A	Peer IP Address				
Enable NA	Enable NAT				
Enable M	Enable MPPE				
Address/C	Address/Control Compression				
Protocol F	Protocol Field Compression				
Asyncmap	Asyncmap Value				
MRU			1500		
MTU			1500		
Link Deteo	ction Interval (s)		60		
Max Retrie	es		0		
Expert Op	tions				

Figure 4-12-4

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

En	able	MAD	DE
EII	able	IVIP	FE

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.

Status		Overview	Cellular	Network	WLAN	VPN	Routing	Host List	GPS
Network	٠	Clients							
System			Name	Status		Local IP		Remote IP	
- of second			pptp_1	Connected		120.205.0.100	20	5.205.0.1/32	
Industrial	•		ipsec_1	Disconnected		÷		4	



Related Topics

PPTP Setting

PPTP Status

4.13 Linovision Cloud Connection

IOT-R32W can use MQTT to retrieve the router's own status or act as a DTU to transmit device data to the cloud.

4.13.1 Remotely view router information

1.Open Linovision's RemoteMonit platform [https://remotemonit.com/login] and log in to your account (or register a new account if you don't already have one).

		og en
	RemoteMonit	
	Welcome to LINOVISION RemoteMonit Platform	
	2 Email	
	A Password	
	Forget Password?	
	Login Create Account	
Frank -		-
	the states and a	
XEF		

Figure 4-13-1-1

2.Go to **Gateways > MQTT Gateways > New** to create a new MQTT gateway. Fill in the required information as follows:

📶 RemoteMonit						Q Help *****@linovision.com
A Home	Home MQTT Gatewa	ys ×				~
🚺 Data Display 🛛 🗸	Name	Ser	ial Number		Q Search C Reset	E Contraction of the second
💼 vSIM Data Plans 🛛 🗸						
👌 Workflow Manag 🗸	MQTT Gateway	5				New G
分 Cameras ✓	Name ≑	Serial Number ≑	Device status	Equipment type	CreateTime	Operate
😢 Sensors 🗸 🗸				\$	2024-07-05 13:41:3	
PoE Management	104	***********	offline	IOT-C104	5	🗹 Edit 🔾 Detail 🔾 Device 💼 Delete
🚽 Gateways 🔷 🔨	Total 1 10/	bage V < 1				
TCP Gateways						
CoraWan Gateways						
L Teltonika						
PhysicalCard						
<u>e</u>						

Figure 4-13-1-2

Item	Required Value
Name	Name of the router, can be customized
Equipment Type	Select " IOT-R32W "
Serial Number	Corresponding to the label on the back of the product
Time Interval	Router status query interval, measured in seconds (10-300)

Table 4-13-1-1 Device Information Description

3. Open the **Details** option of your newly added gateway and record relevant information including *clientId*, *mqttUsername*, *mqttPassword*, *Publish topic*, *Server address* and *Port*.

Name	R32W-MQTT	clientId	jqzg
mqttUsername	linovisioncom	mqttPassword	88223
Publish topic	QJzpX_7y	Subscribe topic	39XQDg4
Server address	44.205.170.12	Port	1883

Figure 4-13-1-3

4. Go to IOT-R32W Web GUI, select **Service > MQTT** from the sidebar, and create a new connection.

Industrial Cellular Router Apply For your device security, please change the default password! Status MQTT | Connections Network Addres ID Nan Statu System Service Serial Por Modbus S Modbus SNMP TR-069

Figure 4-13-1-4

5. Enter the recorded information from the cloud platform into the corresponding fields. Refer to the table below for specific items and save the changes:

Router Configuration Item Name	RemoteMonit Item Name	Router Configuration Item Name	RemoteMonit Item Name
Broker Address	Server address	System Info_Topic	Publish topic
Broker Port	Port	System Status_Topic	Publish topic
Client ID	clientId	Cellular_Topic	Publish topic
Username*	mqttUsername	Ethernet_Topic	Publish topic
Password*	mqttPassword		

Table 4-13-1-2 Configuration Item Correspondence

*Need to enable *User Credentials* first.

6. Refresh RemoteMonit and check if your IOT-R32W status is updated to "Online" and whether the "Check" button allows you to view router information.

4.13.2 Transmit Serial Data to the Cloud as a DTU

1.Open Linovision's RemoteMonit platform [https://remotemonit.com/login] and log in to your account (or register a new account if you don't already have one).

			🔟 en
	RemoteMo	nit	
	Welcome to LINOVISION RemoteMonit	Platform	
	🚊 Email		
	Password		
	For	rget Password?	
	Login Create Ac	count	•
1		····	
Frank -			-
	the state		>
XIII			

Figure 4-13-1-5

2. Go to **Gateways > TCP Gateways > New** to create a new TCP gateway. Fill in the required information as follows:

M RemoteMonit							Q Help	@linovision.com	۲
A Home	Home TCP Gateways	* Weather Station	PoE Management						~
🔕 Data Display 🛛 🗸	Name		Serial Number		Q Search	C Reset			
🧝 vSIM Data Plans 🛛 🗸									
🗟 Workflow Manag 🗸	TCP Gateways						-	⊖ New C	
5 Cameras V	Server address:	44.205.170.12 Port	8822						
🕑 Sensors 🛛 🗸	Name 💠	Serial Number	Mac address \$	Device status \Leftrightarrow	Equipment type	CreateTime \$	Oper	ate	
 PoE Management Gateways 	c101		076e831	online	IOT-C101	2024-07-15 09:41: 33	🖻 Edit 🔍 Dev	ice 🗇 Delete	
MOT Sateways	Total 1 10/r		3						
🛱 TCP Gateways									
a LoraWan Gateways									
H Teltonika									
PhysicalCard									
<u>e</u>									

Figure 4-13-1-6

Required Value
Name of the router, can be customized
Select " IOT-R32W "
Device's Mac address*
Corresponding to the label on the back of the product
Router status query interval, measured in seconds (10-300)

Table 4-13-2-1 Device Information Description

*All lowercase and ignore colons, e.g., 24e124fb3163.

3. Go to **Service > Serial** Port and adjust the Serial Settings to match your serial device. This includes *Serial Type, Baud Rate, Data Bits, Stop Bits, and Parity*. Then, fill in the remaining information as per the table below^{*}.



0		Serial		Help —
Status				Serial Settings
Network	٠	Serial Settings		The serial port parameters of the router and the terminal device should be the same for implementing the communication.
System	•			
System		Serial Type	RS485 ~	Enable
Service	-	Baud Rate	9600 ~	Enable/disable serial port function.
Gervice		Data Bits	8bits ~	Serial Type
VO		Stop Bits	1bits ~	Serial Port 1 is a RS232 port. Serial Port 2 is a RS485 port.
Serial Port		Parity	None	Baud Rate
	_	Software Flow Control	0	Same with the baud rate of the connected terminal device.
Modbus Server		Serial Mode	DTU Mode ~	Data Bits
Modbus Client		DTU Protocol	Transparent ~	Same with the data bits of the connected terminal device.
MQTT		Protocol	TCP ~	Stop Bits
		Keepalive Interval	75 s	Same with the stop bits of the connected terminal device.
SNMP		Keepalive Retry Times	9	Parity
TR-069		Packet Size	1024 Bytes	Same with the parity of the

Figure 4-13-2-1

Item	Required Value	Item	Required Value
Serial Mode	DTU Mode	Register String	Device's Mac address**
DTU Protocol	Transparent	Server	44.205.170.12
		Address	
Protocol	ТСР	Server Port	8822

Table 4-13-2-2 Configuration Item Correspondence

*For unmentioned configuration items, keep the default unless otherwise specified, including *Keepalive Interval, Keepalive Retry Times, Packet Size, Serial Frame Interval and Reconnect Interval.*

**All lowercase and ignore colons, e.g., 24e124fb3163.

4. Click **Save & Apply** button. After adding the serial device in the Sensor interface of RemoteMonit, check if the IOT-R32W status is "Online".

Note: If you haven't added the serial device in RemoteMonit or the serial device is not functioning properly, the IOT-R32W will remain in the "Offline" state.

[END]