SILVERNET
WIRELESS-NETWORK-SOLUTIONS

iSITE Industrial Router Range

User Guide

TABLE OF CONTENTS

INTRODUCTION

Thanks for choosing SilverNet's iSite industrial cellular router. The iSite 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 iSite industrial cellular router. You can refer to it for detailed functionality and router configuration.

This guide is intended for the following users:

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

SUPPORTED PRODUCTS

This manual covers the following products:

- SIL iSITE Switch
- SIL iSITE Connect
- SIL iSITE Lite

For more information, visit www.silvernet.com

iSITE SWIITCH

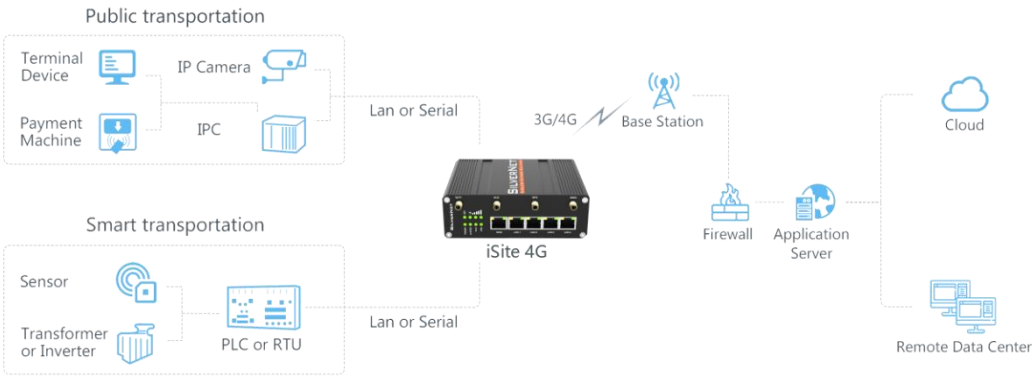
iSite is an industrial cellular router with embedded intelligent software features that are designed for multifarious M2M/IoT applications. Supporting global WCDMA and 4G LTE, iSite provides drop-in connectivity for operators and makes a giant leap in maximizing uptime.

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

Meanwhile, the iSite 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.

iSite 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 iSite Quick Start Guide.



ADVANTAGES

BENEFITS

- Built-in industrial strong NXP CPU
- Fast Ethernet for fast data transmission
- Dual SIM cards for backup between multiple carriers networking and global 2G/3G/LTE options make it easy to get connected
- Equipped with Ethernet, I/O, serial port, Wi-Fi, GPS for connecting diverse field assets
- FXS port for telephone communication
- Embedded Python SDK for second development
- Rugged enclosure, optimized for DIN rail or shelf mounting
- 2-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

- 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

SPECIFICATIONS

HARDWARE SYSTEM	
CPU	528MHz, 32-bit ARM Cortex-A7
Memory	128 MB Flash, 128 MB DDR3 RAM
Storage	1 × Micro SD

CELLULAR INTERFACES	
Connectors	2 × 50 Ω SMA (Centre pin: SMA Female)
SIM Slots	2

WI-FI INTERFACE (OPTIONAL)	
Connectors	1 × 50 Ω SMA (Centre pin: RP-SMA Female)
Standards	IEEE 802.11 b/g/n
Tx Power	802.11b: 16 dBm +/-1.5 dBm (11 Mbps) 802.11g: 14 dBm +/-1.5 dBm (54 Mbps) 802.11n: 13 dBm +/-1.5 dBm (65 Mbps, HT20/40 MCS7)
Modes	Support AP and Client mode, multiple SSID
Security	WPA/WPA2 authentication, WEP/TKIP/AES encryption

GPS (OPTIONAL)	
Connectors	1 × 50 Ω SMA (Centre pin: SMA Female)
Protocols	NMEA 0183, PMTK

ETHERNET	
Ports	5 × RJ-45 (PoE PSE Optional)
Physical Layer	10/100 Base-T (IEEE 802.3)
Data Rate	10/100 Mbps (auto-sensing)

Interface	Auto MDI/MDIX
Mode	Full or half duplex (auto-sensing)

SERIAL INTERFACE

Ports	1 × RS232 + 1 × RS485 (2 × RS485 Optional)
Connector	Terminal block
Baud Rate	300bps to 230400bps

IO

Connector	Terminal block
Digital	1 × DI + 1 × DO

SOFTWARE

Network Protocols	IPv4/IPv6, PPP, PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QoS, SNTP, Telnet, VLAN, SSH, etc.
VPN Tunnel	DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE
Access Authentication	CHAP/PAP/MS-CHAP/MS-CHAPV2
Firewall	ACL/DMZ/Port Mapping/MAC Binding/SPI/DoS&DDoS Protection /IP Passthrough
Management	Web, CLI, SMS, On-demand dial up, DeviceHub
AAA	Radius, TACACS+, LDAP, Local Authentication
Multilevel Authority	Multiple levels of user authority
Reliability	VRRP, WAN Failover, Dual SIM Backup
Serial Port	Transparent (TCP Client/Server, UDP), Modbus Gateway (Modbus RTU to Modbus TCP)

POWER SUPPLY AND CONSUMPTION

Connector	2-pin with 5.08 mm terminal block
Input Voltage	9-48 VDC

Power Consumption	Typical 3.9 W, Max 4.6 W
Power Output	4 × 802.3 af/at PoE output

PHYSICAL CHARACTERISTICS

Ingress Protection	IP30
Housing & Weight	Metal, 485g
Dimensions	135 x 100 x 45 mm (5.31 x 4.06 x 1.77 in)
Mounting	Desktop, wall, or DIN rail mounting

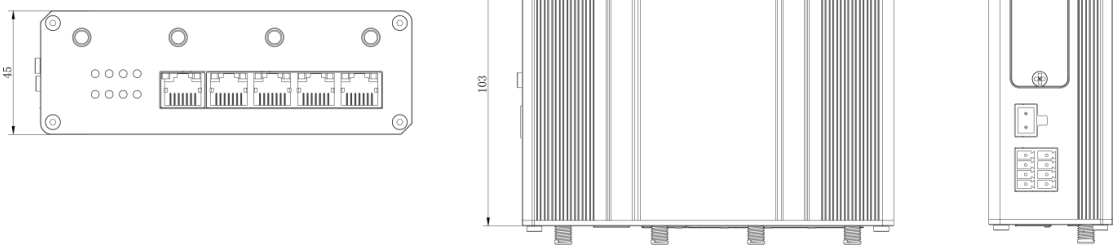
OTHERS

Reset Button	1 × RESET
LED Indicators	1 × POWER, 1 × SYSTEM, 1 × SIM, 1 × Wi-Fi, 1 × VPN, 3 × Signal strength
Built-in	Watchdog, Timer

ENVIRONMENTAL

Operating Temperature	-40°C to +70°C (-40°F to +158°F) Reduced cellular performance above 60°C
Storage Temperature	-40°C to +85°C (-40°F to +185°F)
Ethernet Isolation	1.5 kV RMS
Relative Humidity	0% to 95% (non-condensing) at 25°C/77°F

DIMENSIONS



ISITE CONNECT

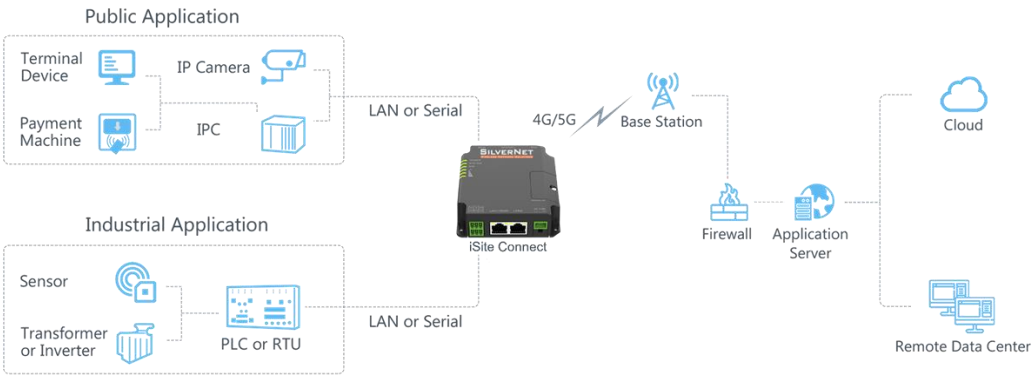
ISITE CONNECT is an industrial cellular router with embedded intelligent software features that are designed for multifarious M2M/IoT applications. Supporting global WCDMA and 4G LTE, ISITE CONNECT provides drop-in connectivity for operators and makes a giant leap in maximizing uptime.

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

Meanwhile, the ISITE CONNECT 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.

ISITE CONNECT 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 ISITE CONNECT Quick Start Guide.



ADVANTAGES

BENEFITS

- Built-in industrial strong NXP CPU
- Fast Ethernet for fast data transmission
- Dual SIM cards for backup between multiple carriers networking and global 2G/3G/LTE options make it easy to get connected
- Equipped with 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
- 2-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

- 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

SPECIFICATIONS

HARDWARE SYSTEM	
CPU	528MHz, 32-bit ARM Cortex-A7
Memory	128 MB Flash, 128 MB DDR3 RAM
Storage	1 × Micro SD
CELLULAR INTERFACES	
Connectors	2 × 50 Ω SMA (Centre pin: SMA Female)
SIM Slots	2
WI-FI INTERFACE (OPTIONAL)	
Connectors	1 × 50 Ω SMA (Centre pin: RP-SMA Female)
Standards	IEEE 802.11 b/g/n
Tx Power	802.11b: 16 dBm +/-1.5 dBm (11 Mbps) 802.11g: 14 dBm +/-1.5 dBm (54 Mbps) 802.11n: 13 dBm +/-1.5 dBm (65 Mbps, HT20/40 MCS7)
Modes	Support AP and Client mode, multiple SSID
Security	WPA/WPA2 authentication, WEP/TKIP/AES encryption
GPS (OPTIONAL)	
Connectors	1 × 50 Ω SMA (Centre pin: SMA Female)
Protocols	NMEA 0183, PMTK
ETHERNET	
Ports	2 × RJ-45 (PoE PSE Optional)
Physical Layer	10/100 Base-T (IEEE 802.3)
Data Rate	10/100 Mbps (auto-sensing)

Interface	Auto MDI/MDIX
Mode	Full or half duplex (auto-sensing)

SERIAL INTERFACE

Ports	1 × RS232 (1 × RS485 Optional)
Connector	Terminal block
Baud Rate	300bps to 230400bps

IO

Connector	Terminal block
Digital	1 × DI + 1 × DO

SOFTWARE

Network Protocols	IPv4/IPv6, PPP, PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QoS, SNTP, Telnet, VLAN, SSH, etc.
VPN Tunnel	DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE
Access Authentication	CHAP/PAP/MS-CHAP/MS-CHAPV2
Firewall	ACL/DMZ/Port Mapping/MAC Binding/SPI/DoS&DDoS Protection /IP Passthrough
Management	Web, CLI, SMS, On-demand dial up, DeviceHub
AAA	Radius, TACACS+, LDAP, Local Authentication
Multilevel Authority	Multiple levels of user authority
Reliability	VRRP, WAN Failover, Dual SIM Backup
Serial Port	Transparent (TCP Client/Server, UDP), Modbus Gateway (Modbus RTU to Modbus TCP)

POWER SUPPLY AND CONSUMPTION

Connector	2-pin with 5.08 mm terminal block
Input Voltage	9-48 VDC

Power Consumption	Typical 1.9 W, Max 2.4 W (In non-PoE mode)
Power Output (optional)	2 × 802.3 af/at PoE output

PHYSICAL CHARACTERISTICS

Ingress Protection	IP30
Housing & Weight	Metal, 271g
Dimensions	108 x 90 x 26 mm (4.25 x 3.54 x 1.02 in)
Mounting	Desktop, wall, or DIN rail mounting

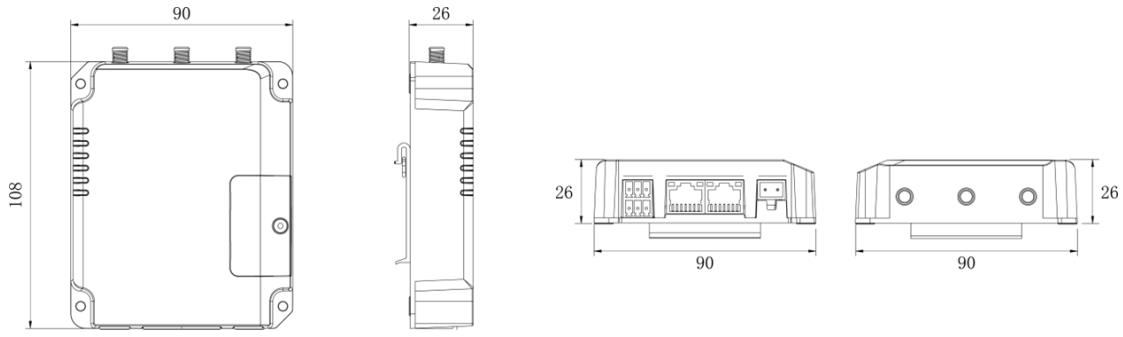
OTHERS

Reset Button	1 × RESET
LED Indicators	1 × POWER, 1 × SYSTEM, 1 × SIM, 3 × Signal strength
Built-in	Watchdog, Timer

ENVIRONMENTAL

Operating Temperature	-40°C to +70°C (-40°F to +158°F) Reduced cellular performance above 60°C
Storage Temperature	-40°C to +85°C (-40°F to +185°F)
Ethernet Isolation	1.5 kV RMS
Relative Humidity	0% to 95% (non-condensing) at 25°C/77°F

DIMENSIONS



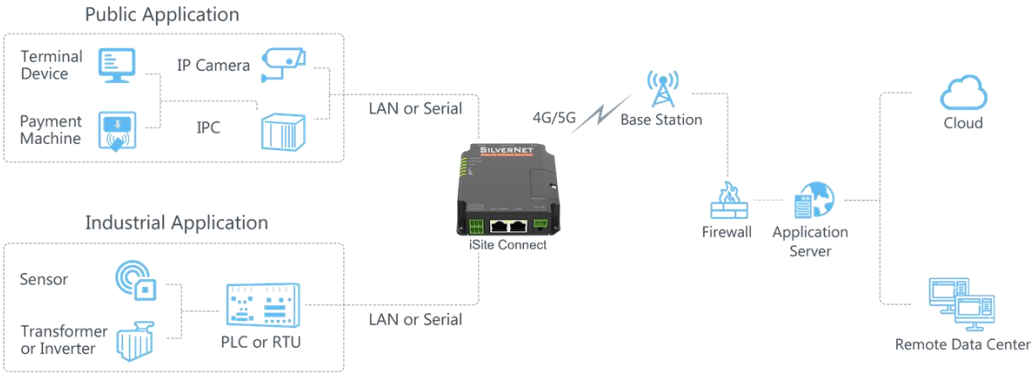
ISITE LITE

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

ISITE LITE 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 ISITE LITE Quick Start Guide.



ADVANTAGES

BENEFITS

- Built-in industrial strong NXP CPU
- Fast Ethernet for fast data transmission
- Rugged enclosure, optimized for DIN rail or shelf mounting
- 2-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

- 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

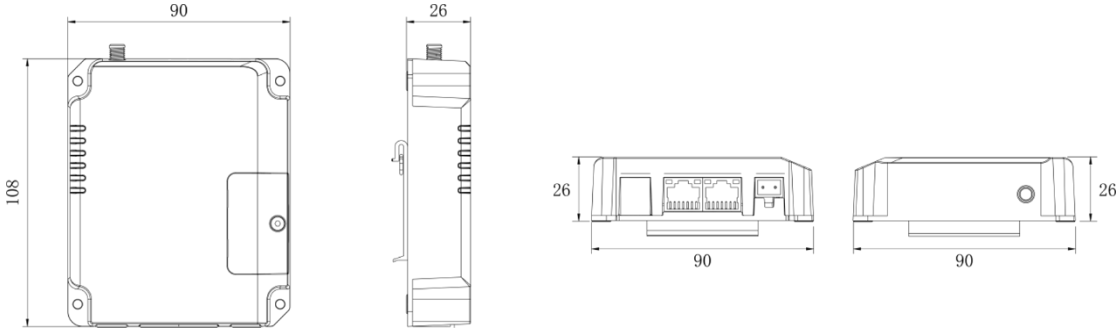
- Link remote devices in an environment where communication technologies are constantly changing
- Industrial 32-bit ARM Cortex-A7 processor, high-performance operating up to 528MHz and 128 MB memory available to support more applications
- Support rich protocols like SNMP, Modbus bridging, RIP, OSPF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

SPECIFICATIONS

HARDWARE SYSTEM	
CPU	528MHz, 32-bit ARM Cortex-A7
Memory	128 MB Flash, 128 MB DDR3 RAM
CELLULAR INTERFACES	
Connectors	1 × 50 Ω SMA (Centre pin: SMA Female)
SIM Slots	1 (Mini SIM-2FF)
ETHERNET	
Ports	2 × RJ-45 (PoE PSE Optional)
Physical Layer	10/100 Base-T (IEEE 802.3)
Data Rate	10/100 Mbps (auto-sensing)
Interface	Auto MDI/MDIX
Mode	Full or half duplex (auto-sensing)
SOFTWARE	
Network Protocols	IPv4/IPv6, PPP, PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QoS, SNTP, Telnet, VLAN, SSH, etc.
VPN Tunnel	DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE
Access Authentication	CHAP/PAP/MS-CHAP/MS-CHAPV2
Firewall	ACL/DMZ/Port Mapping/MAC Binding/SPI/DoS&DDoS Protection /IP Passthrough
Management	Web, CLI, SMS, On-demand dial up, DeviceHub
AAA	Radius, TACACS+, LDAP, Local Authentication
Multilevel Authority	Multiple levels of user authority
Reliability	VRRP, WAN Failover,

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

DIMENSIONS

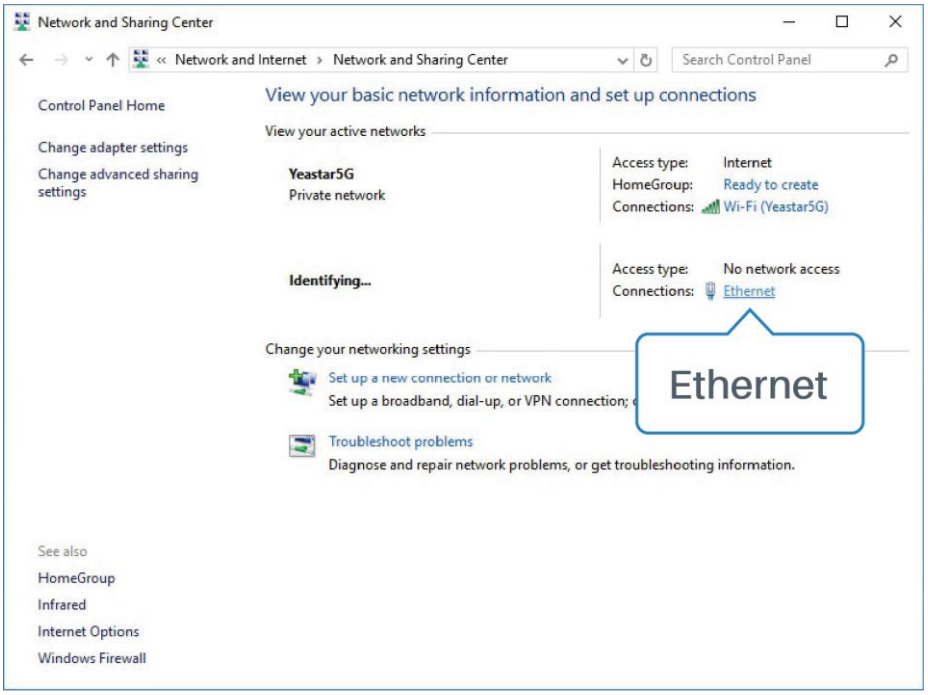


ACCESS TO THE WEB GUI

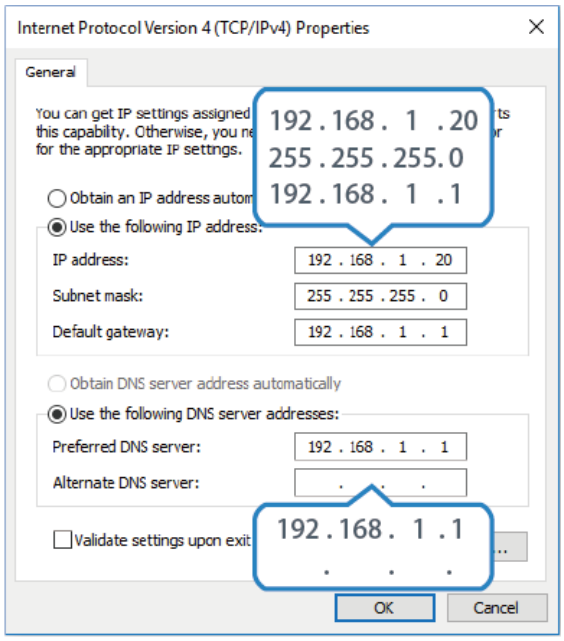
This chapter explains how to access to Web GUI of the iSite router. Connect PC to LAN port of iSite router directly. The following steps are based on Windows 10 operating system for your reference.

Username: admin
Password: password
IP Address: 192.168.1.1

1. Go to “Control Panel” → “Network and Internet” → “Network and Sharing Centre”, then click “Ethernet” (May have different names).



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

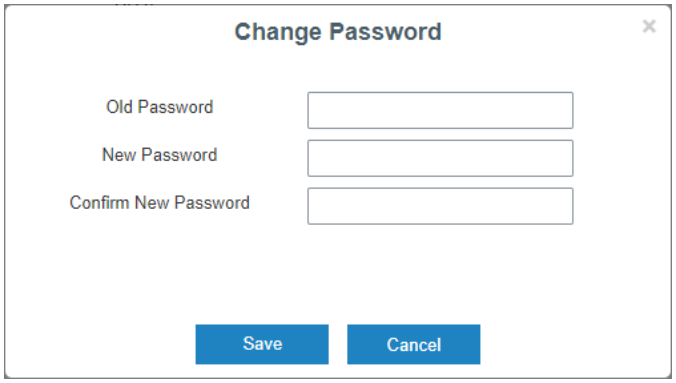


3. Open a Web browser on your PC (Chrome is recommended), type in the IP address 192.168.1.1, and press Enter on your keyboard.

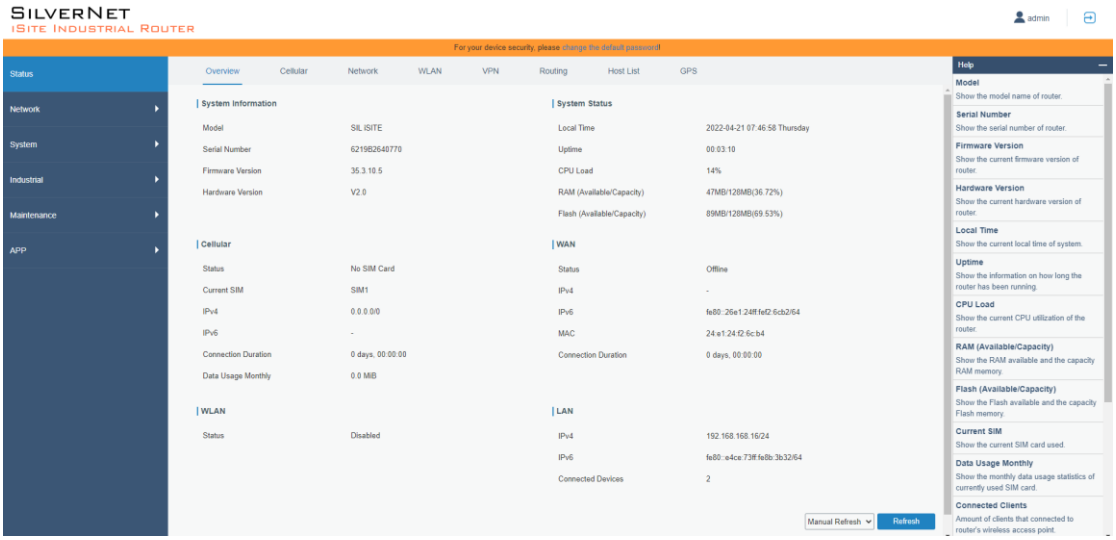
4. Enter the username, password, and click "Login".

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

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



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



STATUS

OVERVIEW

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

System Information

Model The model name of router.
Serial Number The serial number of the router.
Firmware Version The current firmware version of the router.
Hardware Version The current hardware version of the router.

System Status

Local Time The current local time of the router.
Uptime Displays the running time of the router.
CPU Load Displays the current CPU utilization of the router.
RAM (Available/Capacity) Displays the RAM capacity and available RAM memory.
Flash (Available/Capacity) Displays the Flash capacity and available Flash memory.

Cellular

Status Displays the real-time status of the installed SIM Card.
Current SIM Displays the SIM Card currently used for data connection.
IPv4/IPv6 Displays the IPv4/IPv6 address obtained from the mobile carrier.
Connection Duration Displays the connection uptime of the installed SIM Card.
Data Usage Monthly Displays monthly data usage statistics for the current SIM Card.

WAN

Status Displays current status of the WAN Port.
IPv4/IPv6 Displays the IPv4/IPv6 address configured on the WAN Port.
MAC The MAC Address of the Ethernet Port.
Connection Duration Displays the connection uptime of the WAN Port.

WLAN

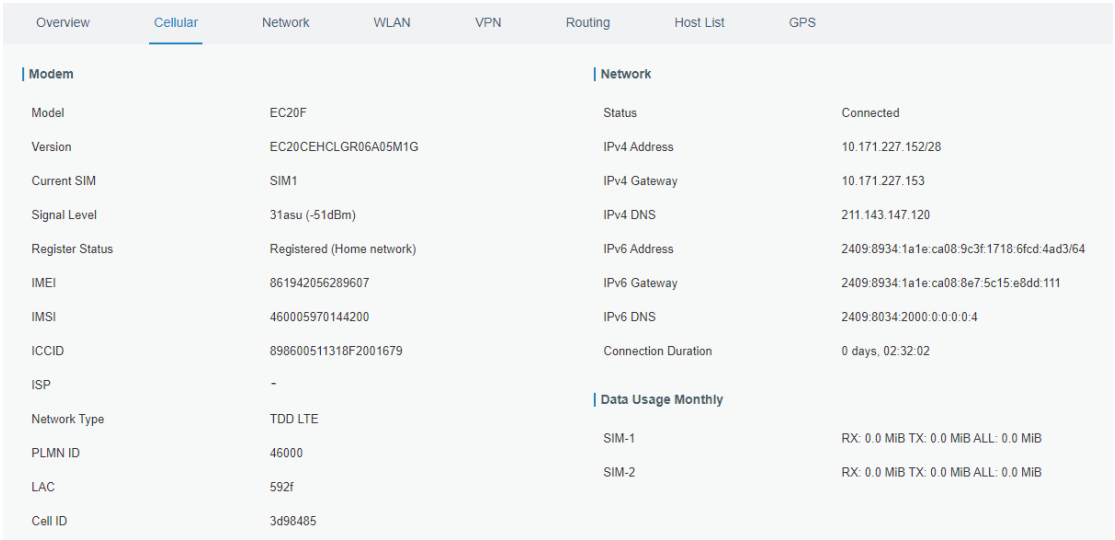
Status Displays current status of the WLAN.
IP Displays the WLAN Mode (AP or Client).
SSID Displays the SSID of the WLAN AP or Client.
Connected Clients Displays currently connected clients (when in AP Mode).

LAN

IP4/IPV6 Displays the IPv4/IPv6 address of the LAN Port.
Connected Devices Displays connected devices to the LAN Port.

CELLULAR

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



Modem Information

Status Displays detection status of module and SIM Card.
Version Display the cellular module firmware version.
Current SIM Displays the current SIM Card in use.
Signal Level The current cellular signal level.
Register Status Displays the registration status of the SIM Card.
IMEI Displays the IMEI of the module.
IMSI Displays the IMSI of the SIM card.

ICCID Displays the ICCID of the SIM card.
ISP Displays the current network provider for the SIM card.
Network Type Displays current connection type such as LTE, 3G etc.
PLMN ID Displays the PLMN ID, including MCC, MNC, LAC and Cell ID.
LAC Displays the location area code of the SIM card.
Cell ID Displays the Cell ID of the SIM card location.

Network

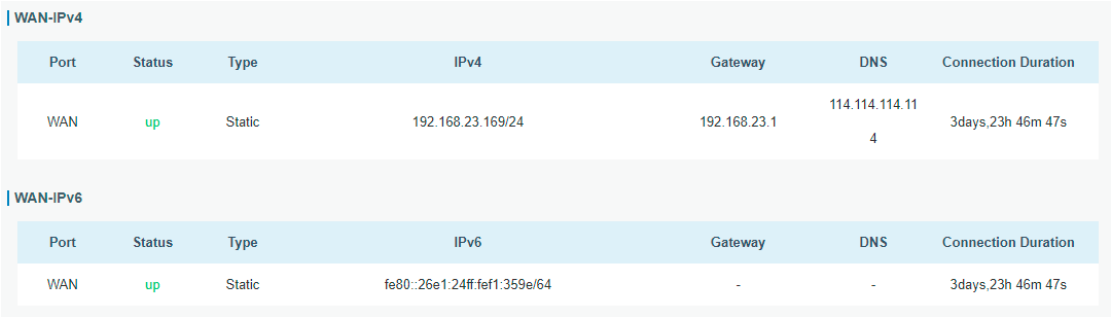
Status Displays the connection status of cellular network.
IPv4/IPv6 Address Displays the IPv4/IPv6 address and netmask of cellular network.
IPv4/IPv6 Gateway Displays the IPv4/IPv6 gateway and netmask of cellular network.
IPv4/IPv6 DNS Displays the IPv4/IPv6 DNS of cellular network.
Connection Duration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

Data Usage Monthly

SIM-1 Show the monthly data usage statistics of SIM-1.
SIM-2 Show the monthly data usage statistics of SIM-2.

NETWORK

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



| WAN-IPv4

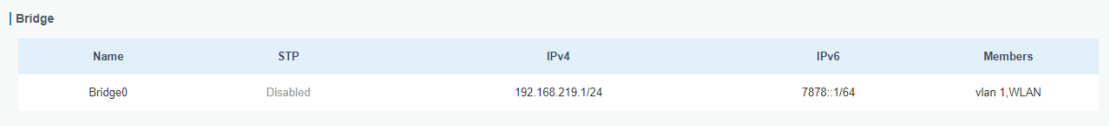
Port	Status	Type	IPv4	Gateway	DNS	Connection Duration
WAN	up	Static	192.168.23.169/24	192.168.23.1	114.114.114.114	3days,23h 46m 47s

| WAN-IPv6

Port	Status	Type	IPv6	Gateway	DNS	Connection Duration
WAN	up	Static	fe80::26e1:24ff:fef1:359e/64	-	-	3days,23h 46m 47s

WAN Status

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.
Type 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.

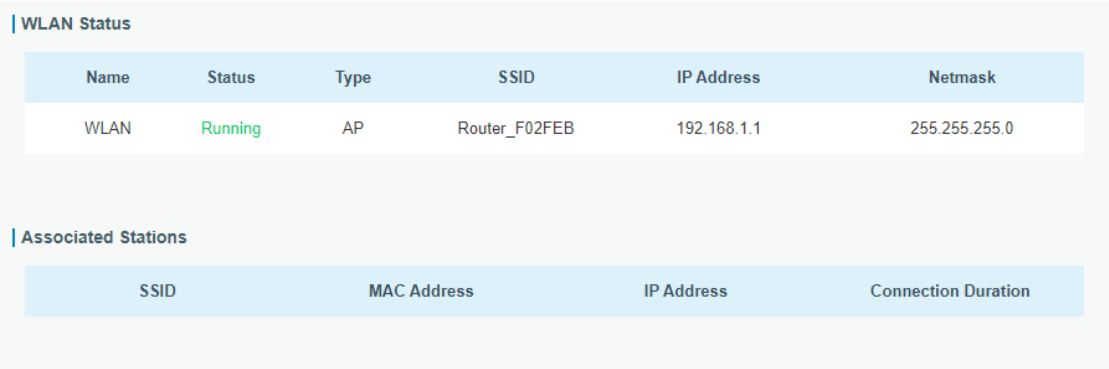


Bridge

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.

WLAN

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



WLAN Status

Name Show the name of the Wi-Fi interface .
Status Show the status of the Wi-Fi interface.
Type Show the Wi-Fi interface type.
SSID Show the SSID of the router when the interface type is AP. Show the SSID of AP which the router connected to when the interface type is Client.
IP Address Show the IP address of the router when the interface type is AP. Show the IP address of AP which the router connected to when the interface type is Client.
Netmask Show the netmask of the router when the interface type is AP. Show the netmask of AP which the router connected to when the interface type is Client.

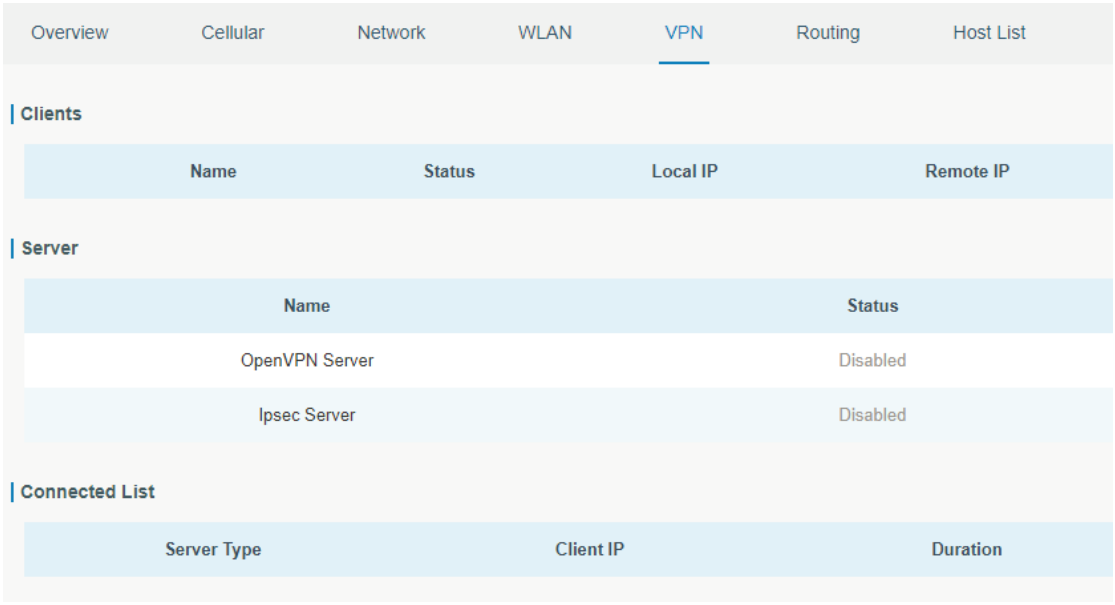
Associated Stations

SSID Show the SSID of the router when the interface type is AP. Show the SSID of AP which the router connected to when the interface type is Client.
MAC Address Show the MAC address of the client which connected to the router when the interface type is AP. Show the MAC address of the AP which the router connected to when the interface type is Client.
IP Address Show the IP address of the client which connected to the router when the interface type is AP. Show the IP address of the AP which the router connected to when the interface type is Client.

Connection Duration Show the connection duration between client device and router when the interface type is AP. Show the connection duration between router and the AP when the interface type is Client.

VPN

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



VPN Status

Name Show the name of the enabled VPN clients.
Status Show the status of client. "Connected" refers to a status that client is connected to the server. "Disconnected" means client is disconnected to the server.
Local IP Show the local IP address of the tunnel.
Remote IP Show the remote IP address of the tunnel.

Server

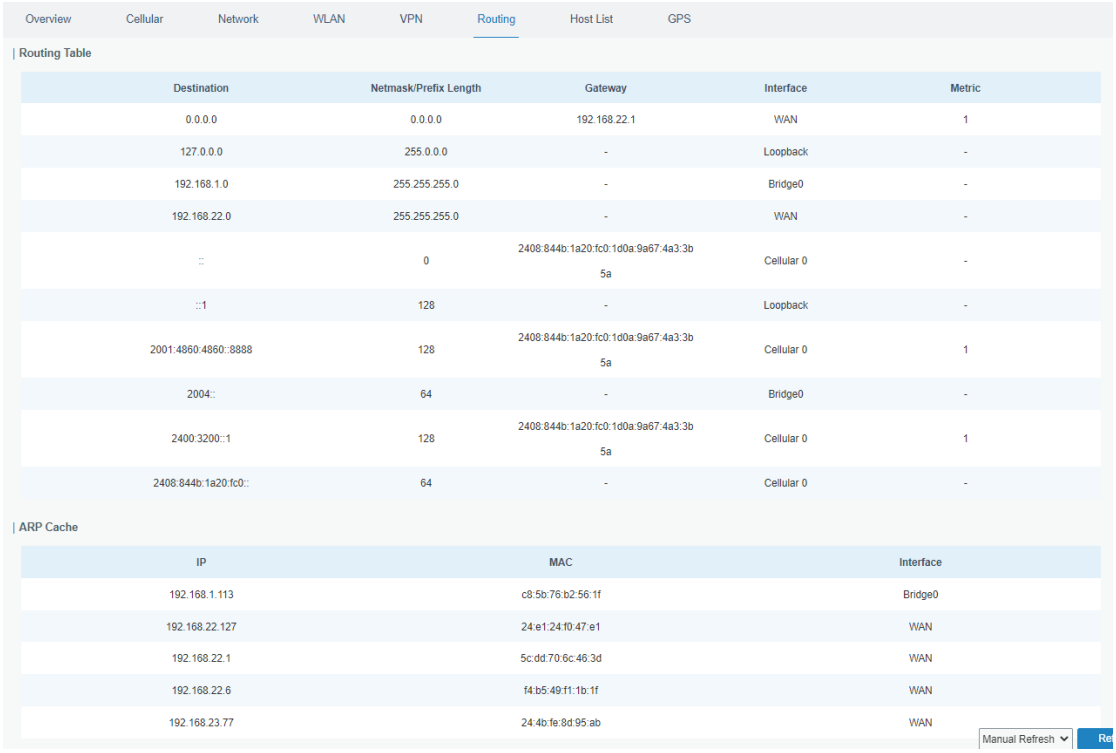
Name Show the name of the enabled VPN Server.
Status Show the status of Server.

Connected List

Server Type Show the type of the server.
Client IP Show the IP address of the client which connected to the server.
Duration Show the information about how long the client has been connected to this server when the server is enabled. Once the server is disabled or connection is disconnected, the duration will stop counting.

ROUTING

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



Routing Table

Destination Show the IP address of destination host or destination network.

Netmask/Prefix LengthShow the netmask or prefix length of destination host or destination network.

Gateway Show the IP address of the gateway.

Interface Show the outbound interface of the route.

Metric Show the metric of the route.

ARP Cache

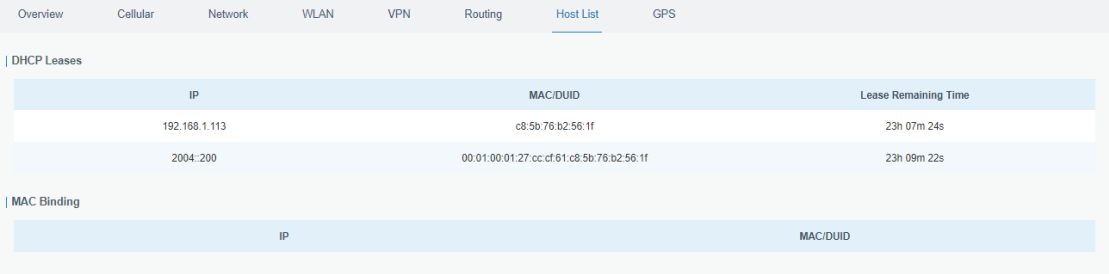
IP Show the IP address of ARP pool.

MAC Show the IP address's corresponding MAC address.

Interface Show the binding interface of ARP.

HOST LIST

You can view the host information on this page.



DHCP Leases

IP Address Show IP address of DHCP client

MAC/DUID Show MAC address of DHCPv4 client or DUID of DHCPv6 client.

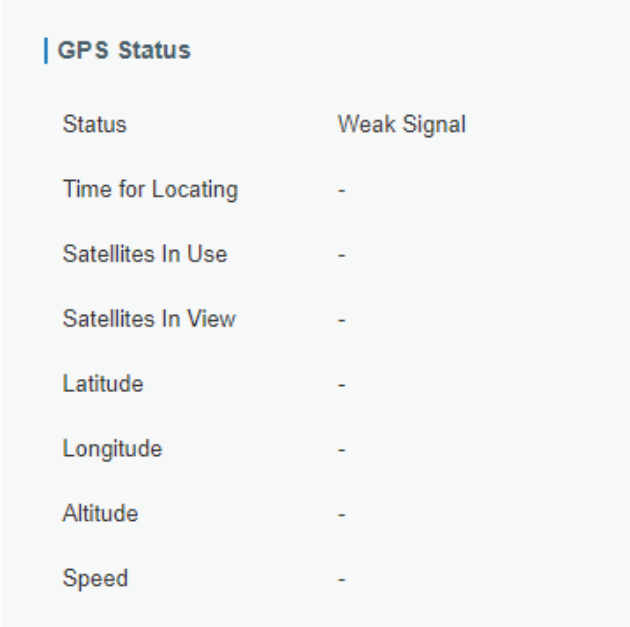
Lease Time Remaining Show the remaining lease time of DHCP client.

MAC Binding

IP & MAC Show the IP address and MAC address set in the Static IP list of DHCP service.

GPS

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.



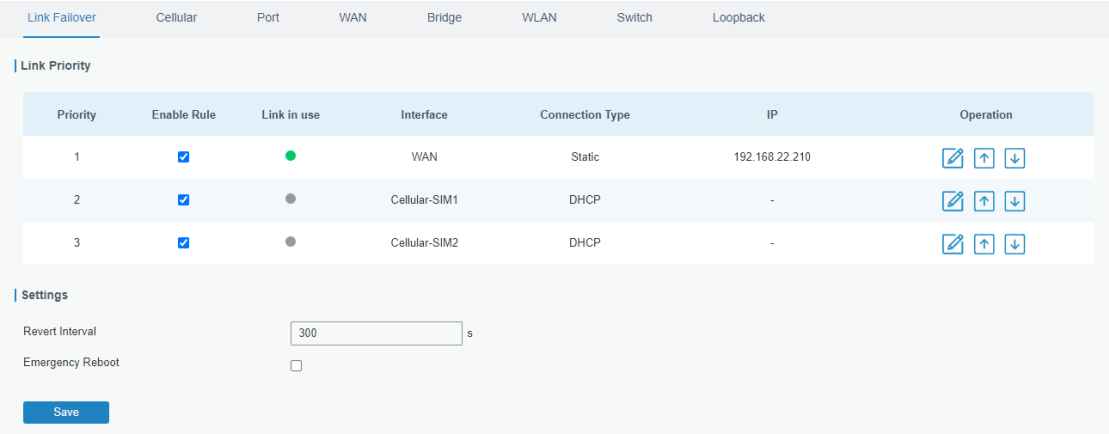
GPS Status

Status 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.

NETWORK

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 enabled the full interface that you need to use here. If priority 1 can only use IPv4, iSite will select a second link which IPv6 works as main IPv6 link and vice versa.



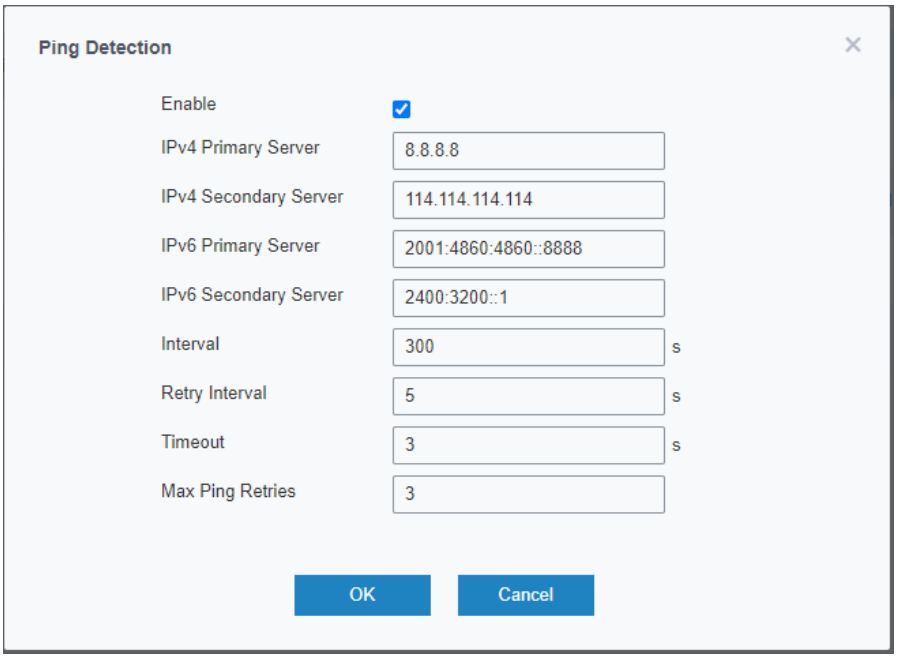
Link Priority

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 is not enabled here, the interface will be disabled as well.
Link In Use Mark whether this interface is in use with Green colour
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.



Ping Detection

Enable If enabled, the router will periodically detect the connection status of the link.

IPv4/IPv6 Primary Server The router will send ICMP packet to the IPv4/IPv6 address or hostname to determine whether the Internet connection is still available or not.

IPv4/IPv6 Secondary Server The router will try to ping the secondary server name if primary server is not available.

Interval Time interval (in seconds) between two Pings.

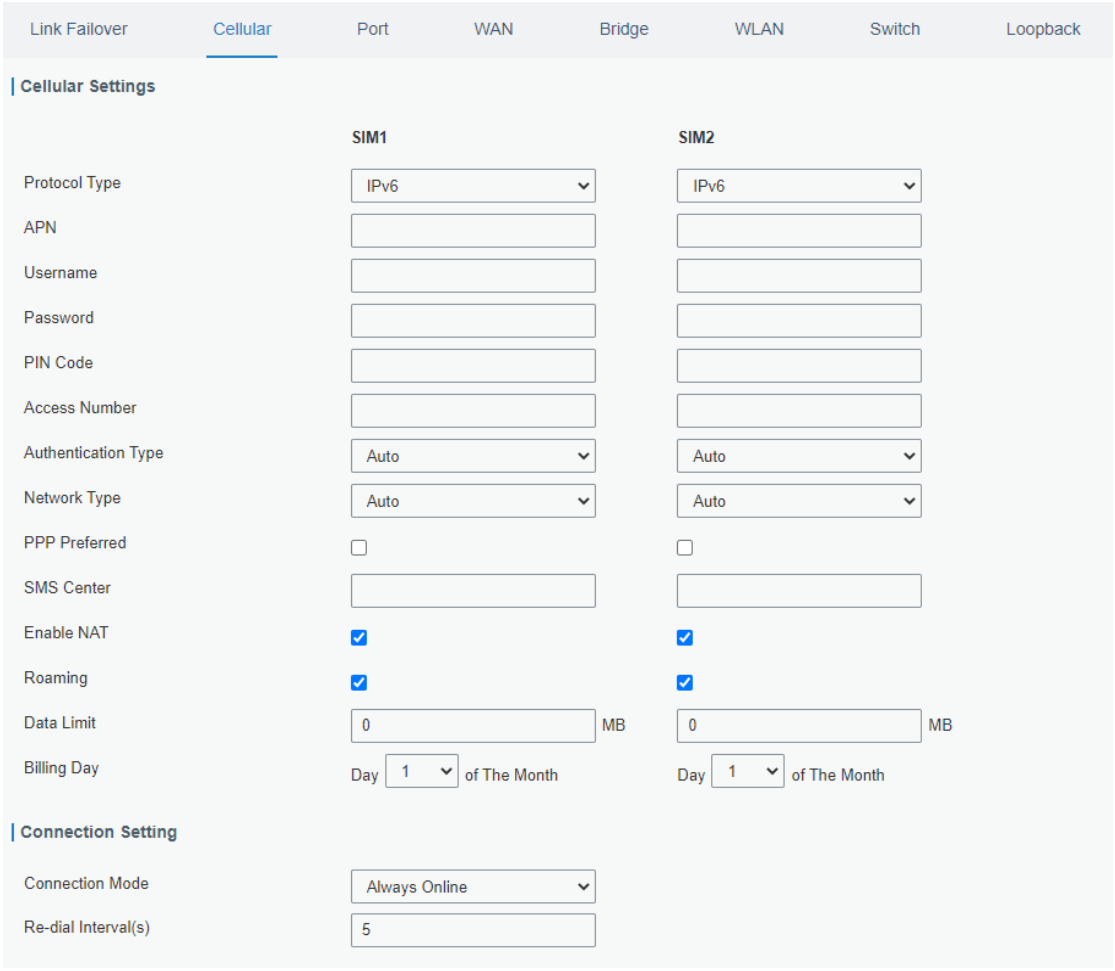
Retry Interval Set the ping retry interval. When ping failed, the router will ping again in every retry interval.

Timeout The maximum amount of time the router will wait for a response to a ping request. If it does not receive a response for the amount of time defined in this field, the ping request will be considered to have failed.

Max Ping Retries The retry times of the router sending ping request until determining that the connection has failed.

CELLULAR

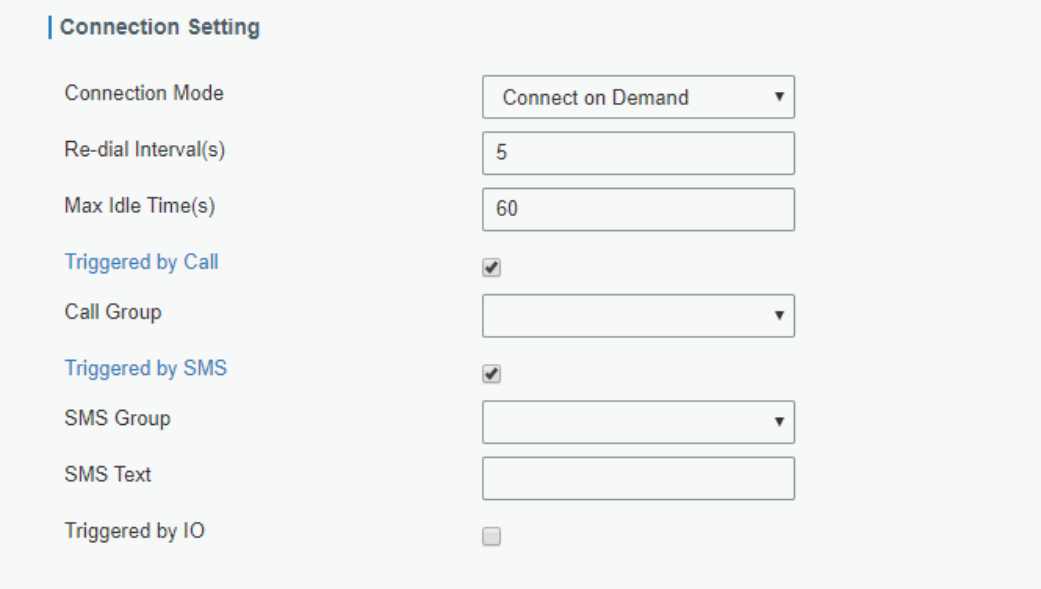
This section explains how to set the related parameters for cellular network. The iSite cellular router has two cellular interfaces, namely SIM1 and SIM2. Only one cellular interface is active at one time. If both cellular interfaces are enabled, it will follow the priority rule configured in 'Link Failover' page.



Cellular Settings

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 centre 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 Centre Enter the local SMS centre 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.

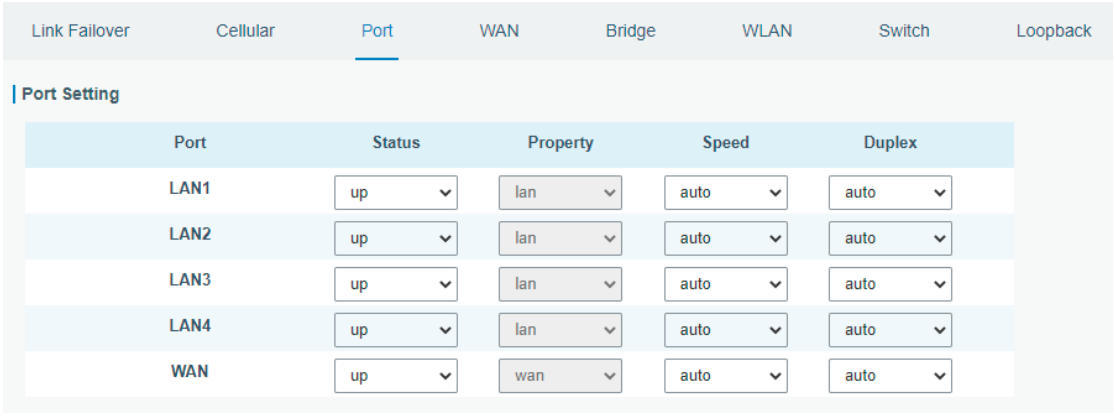


Connection Setting
Connection Mode Select from "Always Online" and "Connect on Demand".
Re-dial Interval(s) Set the interval to dial into ISP when it lost connection, the default value is 5s.
Max Idle Times Set the maximum duration of router when current link is under idle status. Range: 10-3600
Triggered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

Note: Voice call and data transmission being used simultaneously, depending upon your ISP network.

PORT

This section describes how to configure the Ethernet port parameters. iSite cellular router supports 5 Fast Ethernet ports.



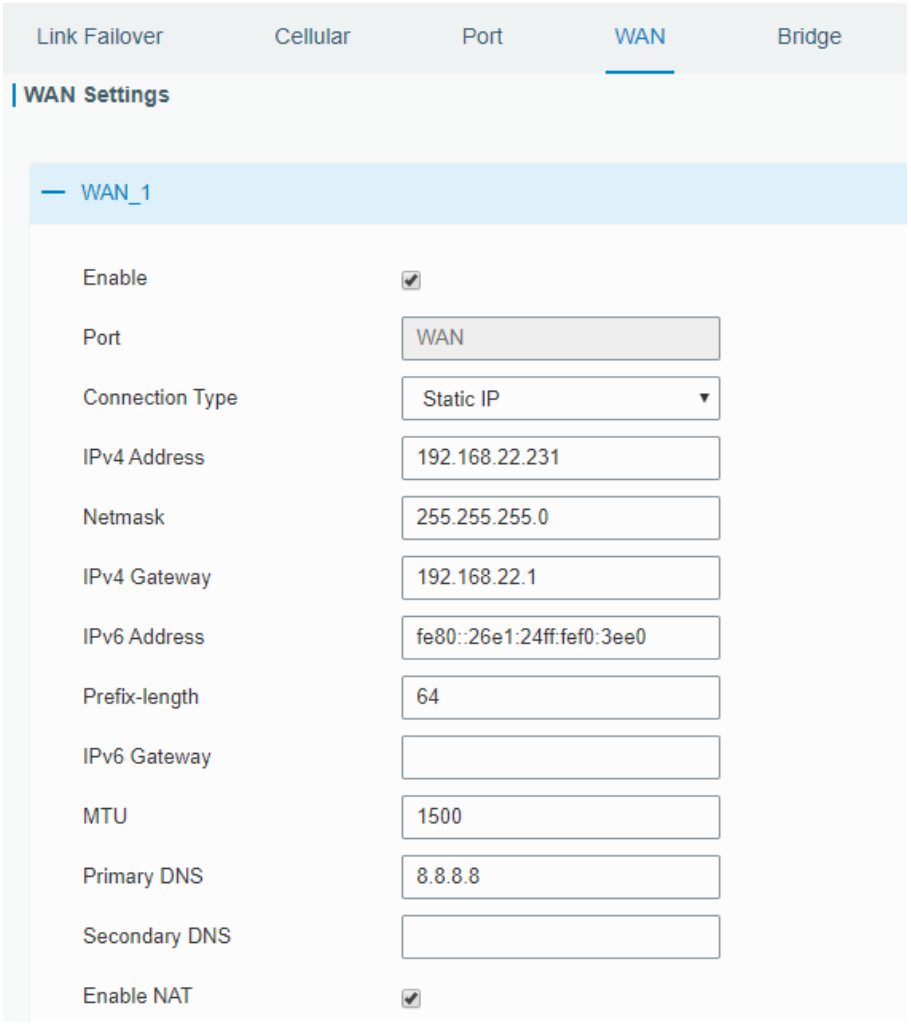
Port Setting

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".

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 tunnelling to send terminal device's IPv4 packet through a tunnel on the IPv6 access network to the ISP.



WAN Setting

Enable Enable WAN function.

Port The port that is currently set as WAN port.

Connection Type Select from "Static IP", "DHCP Client", “DHCPv6 Client” , "Dual-Stack Lite" and "PPPoE".

MTU Set the maximum transmission unit.

IPv4 Primary DNS Set the primary IPv4 DNS server.

IPv4 Secondary DNS Set the secondary IPv4 DNS server.

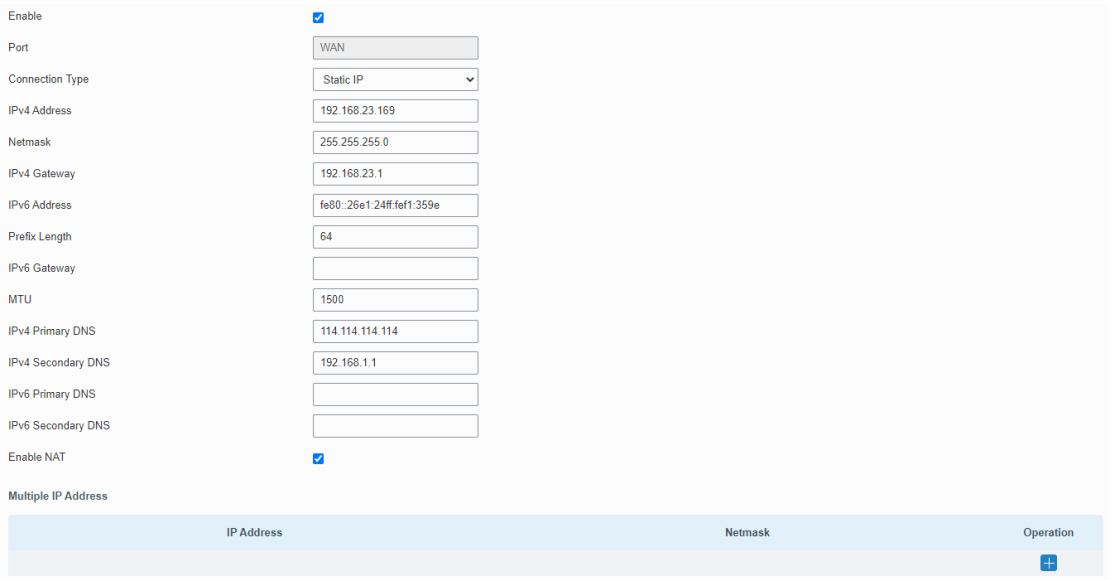
IPv6 Primary DNS Set the primary IPv6 DNS server.

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.

STATIC IP CONFIGURATION

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



Static IP

IPv4 Address Set the IPv4 address of the WAN port.

Netmask Set the Netmask for WAN port.

IPv4 Gateway Set the gateway for WAN port's IPv4 address.

IPv6 Address Set the IPv6 address which can access Internet.

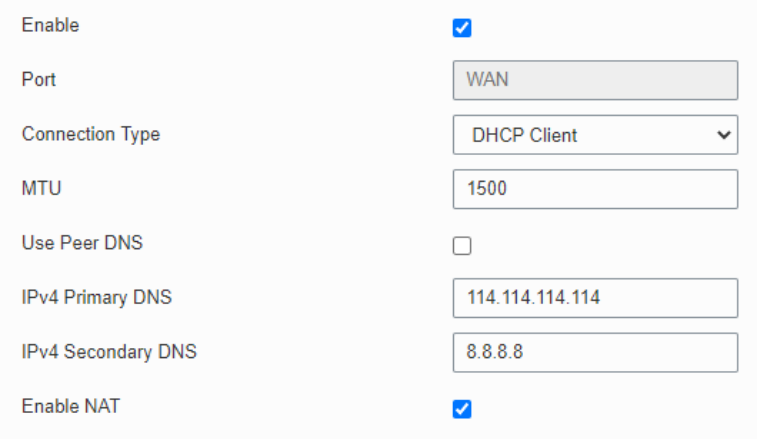
Prefix-length Set the IPv6 prefix length to identify how many bits of a Global Unicast IPv6 address are there in network part. For example, in 2001:0DB8:0000:000b::/64, the number 64 is used to identify that the first 64 bits are in network part.

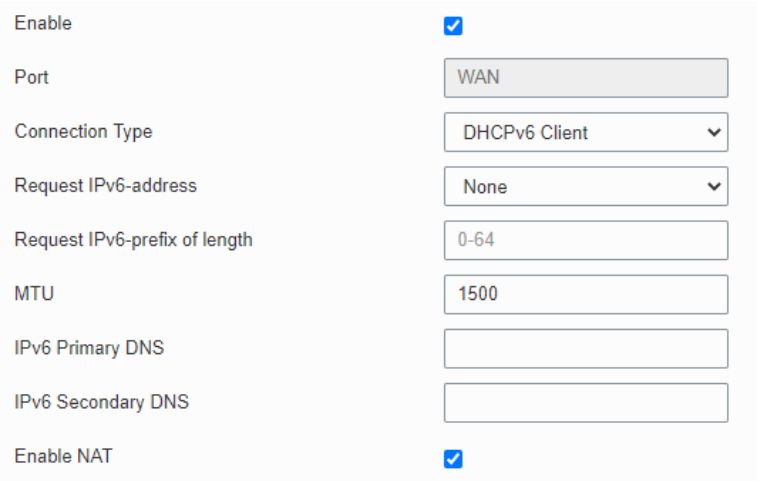
IPv6 Gateway Set the gateway for WAN port's IPv6 address. E.g.2001:DB8:ACAD:4::2.

Multiple IP Address Set the multiple IP addresses for WAN port

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.





DHCP Client

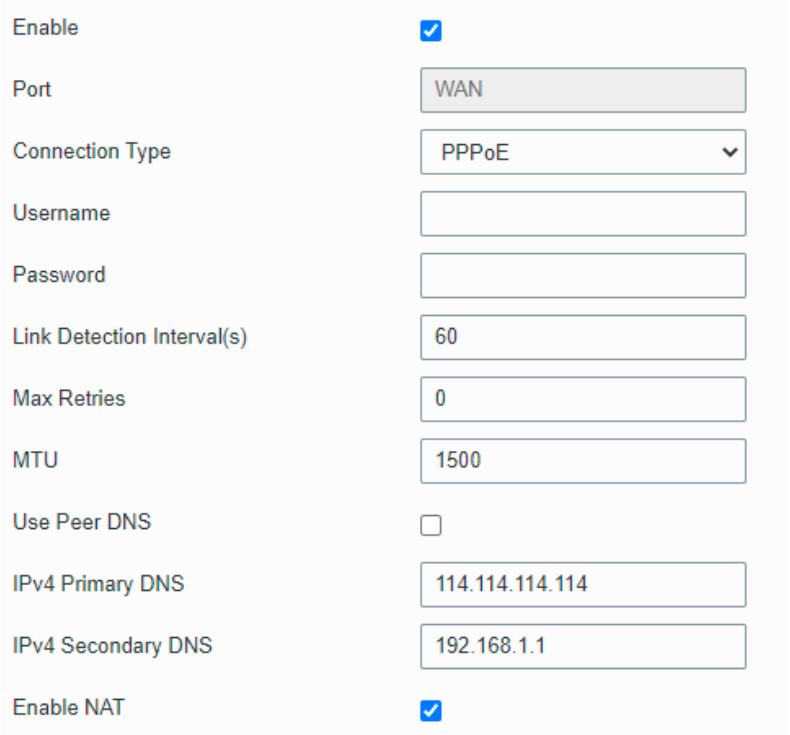
Use Peer DNS Obtain peer DNS automatically during PPP dialling. DNS is necessary when visiting domain name.

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.

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.

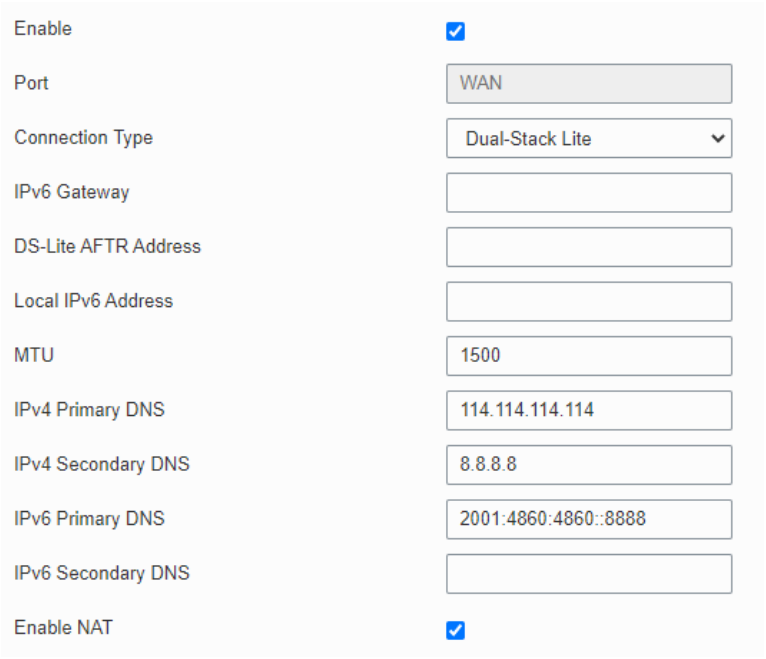


PPPoE

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 dialling. DNS is necessary when visiting domain name.

DUAL-STACK LITE

Dual-Stack Lite (DS-Lite) uses IPv4-in-IPv6 tunnelling 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.



Dual-Stack Lite

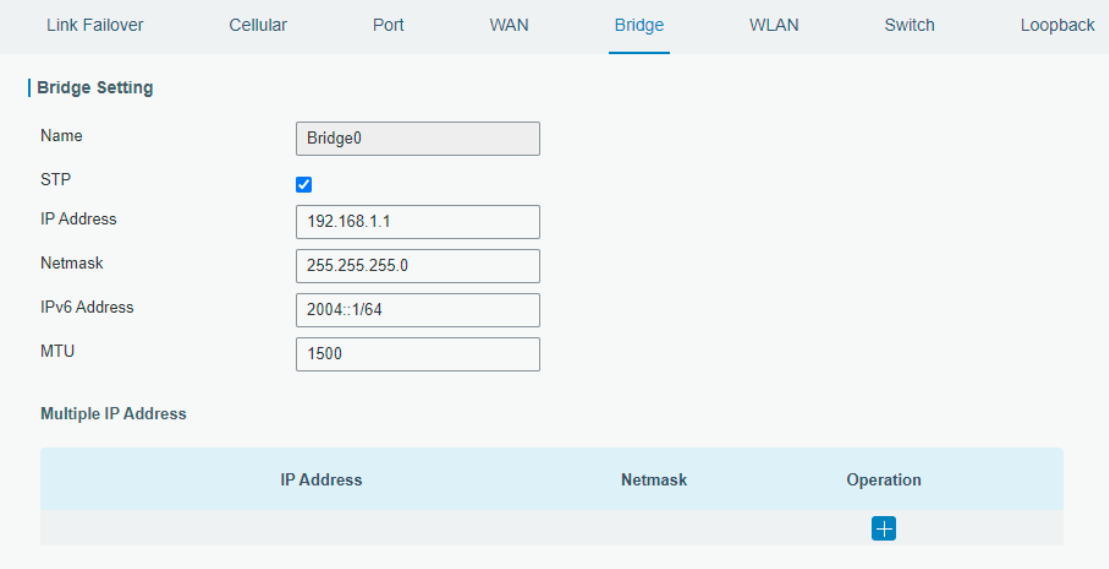
IPv6 Gateway Set the gateway for WAN port's IPv6 address.

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.

BRIDGE

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

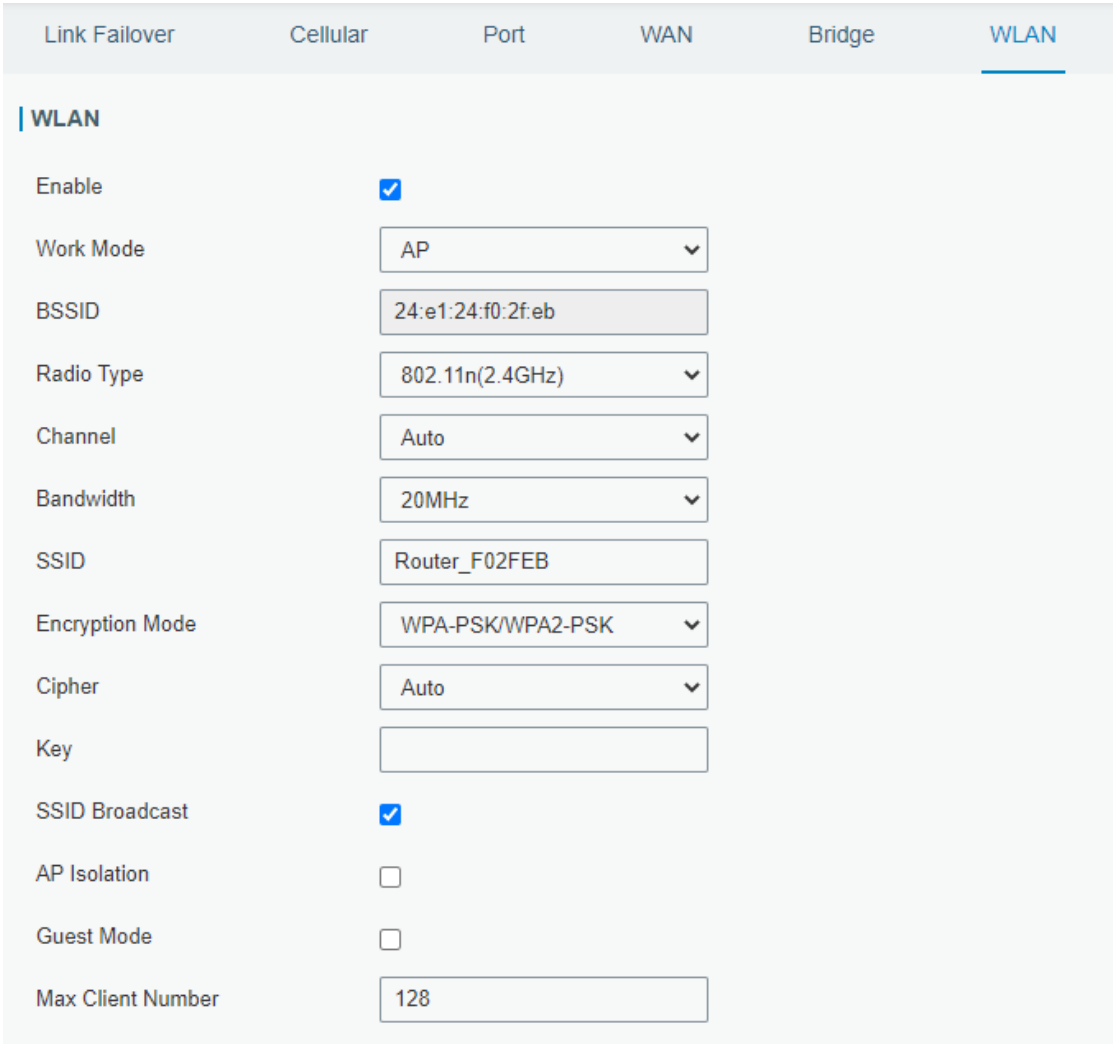


Bridge

Name Show the name of bridge. "Bridge0" is set by default and cannot be changed.
STP Enable/disable STP.
IP Address Set the IP address for bridge.
Netmask Set the Netmask for bridge.
IPv6 Address Set the IPv6 address for bridge.
MTU Set the maximum transmission unit. Range: 68-1500.
Multiple IP Address Set the multiple IP addresses for bridge.

WLAN

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



WLAN

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 join the network.

SSID Fill in the SSID of the access point.

Client Mode

ScanClick "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.

Cipher Show the cipher of the access point.

Security Show the encryption mode.

Frequency Show the frequency of radio.

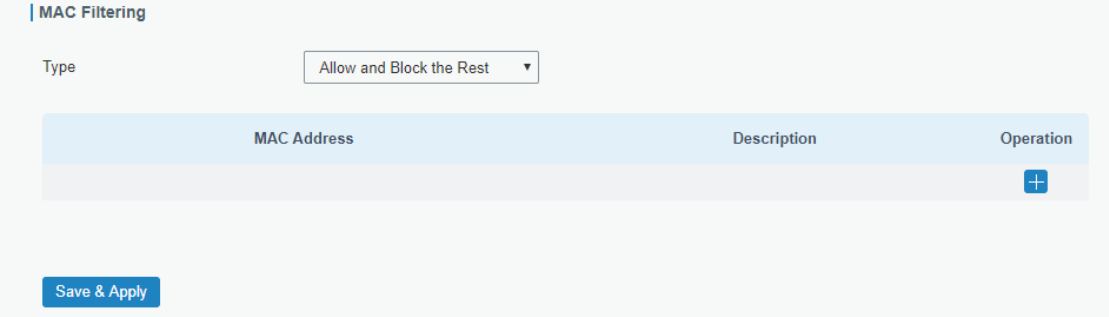
Join Network Click the button to join the wireless network.

AP Mode

Radio Type Select Radio type. The options are “802.11b (2.4 GHz)", “802.11g (2.4 GHz)", “802.11n (2.4 GHz).”
Channel Select wireless channel. The options are "Auto", "1", "2"....."11".
Cipher Select cipher. The options are “Auto", “AES", “TKIP" and “AES/TKIP".
Key Fill the pre-shared key of WPA encryption.
Bandwidth Select bandwidth. The options are "20MHz" and "40MHz".
SSID Broadcast When SSID broadcast is disabled, other wireless devices cannot find the SSID, and users have to enter the SSID manually to access to the wireless network.
AP Isolation When AP isolation is enabled, all users who access to the AP are isolated without communication with each other.
Guest Mode The internal network is not allowed to visit if the guest mode is enabled.
Max Client Number Set the maximum number of client to access when the router is configured as AP.

IP Setting

Protocol Set the IP address in wireless network.
IP Address Set the IP address in wireless network.
Netmask Set the netmask in wireless network.
Gateway Set the gateway in wireless network.

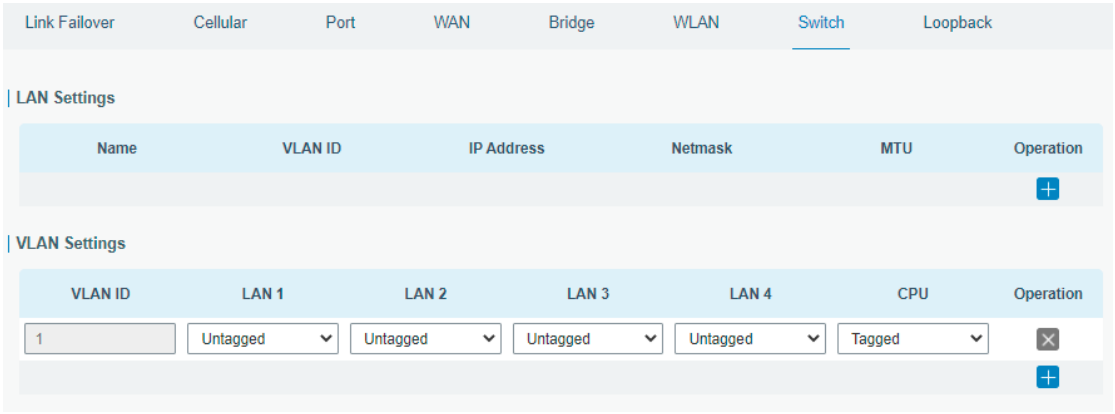


MAC Filtering

Type 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.

SWITCH

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



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.

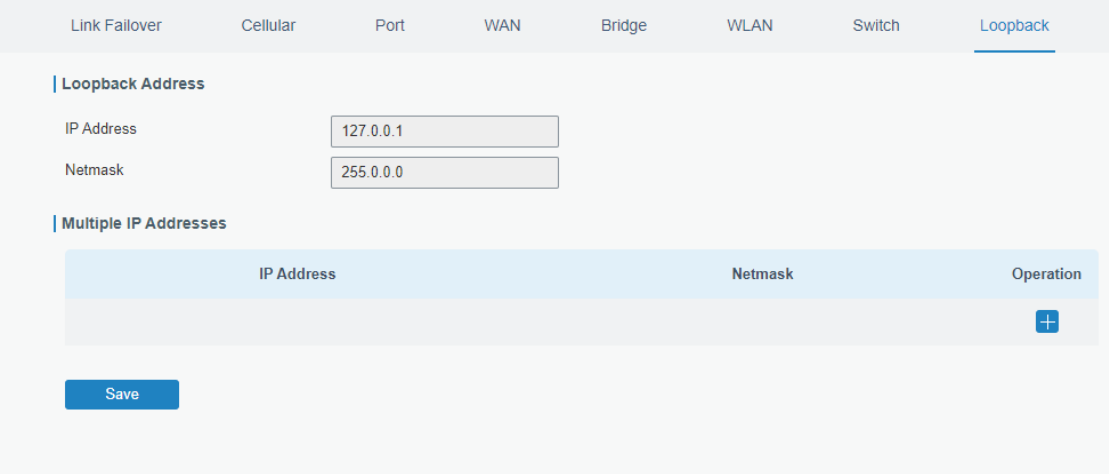
VLAN Settings

VLAN ID Set the label ID of the VLAN. Range: 1-4094.
LAN 1/2/3/4 Make the VLAN bind with the corresponding ports and select status from "Tagged", "Untagged" and "Close" for Ethernet frame on trunk link.
CPU Control communication between VLAN and other networks.

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 recommended as the ID of the router.

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



Loopback Settings

IP Address Unalterable, 127.0.0.1.

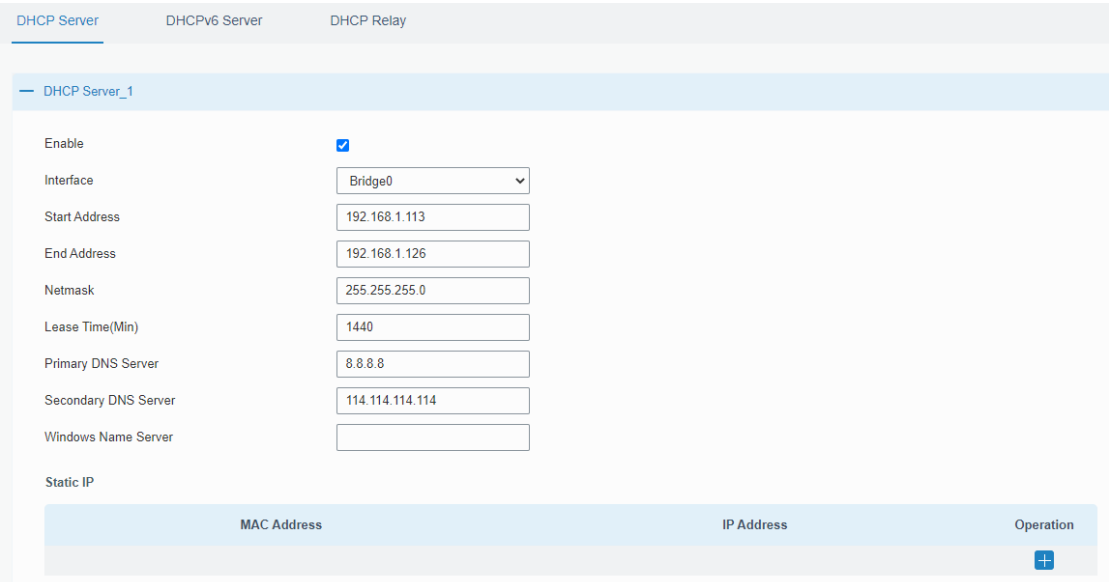
Netmask Unalterable, 255.0.0.0.

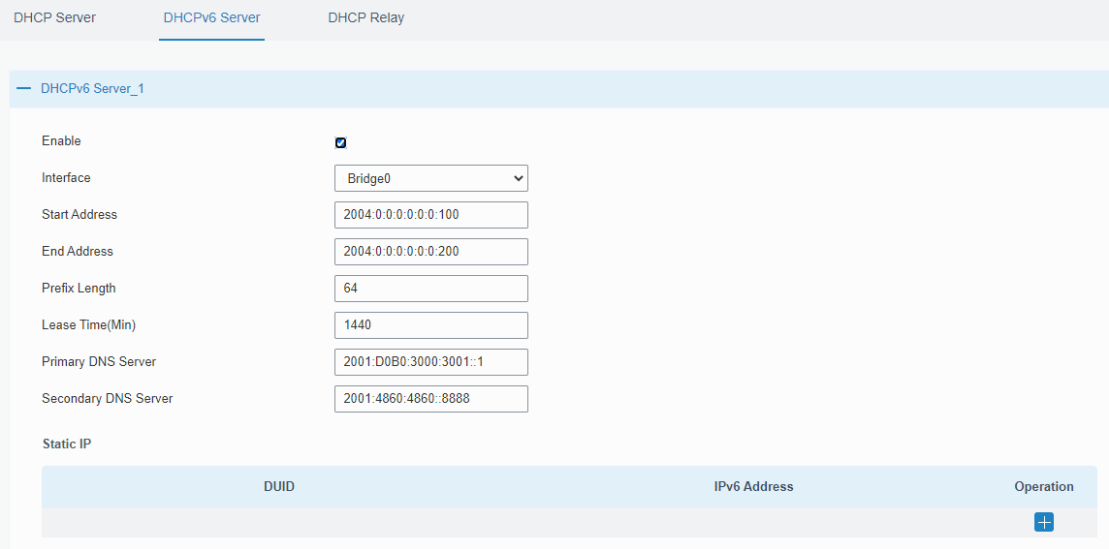
Multiple IP Addresses User can configure multiple separate IP addresses.

DHCP & DHCP Server / DHCPv6 Server

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.

iSite 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. iSite only supports stateful DHCPv6 when working as DHCPv6 server.





DHCP Server

Enable Enable or disable DHCP server.

Interface Select interface.

Start Address Define the beginning of the pool of IP addresses which will be leased to DHCP clients.

End Address Define the end of the pool of IP addresses which will be leased to DHCP clients.

Netmask Define the subnet mask of IPv4 address obtained by DHCP clients from DHCP server.

Prefix 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.

Primary DNS Server Set the primary DNS server.

Secondary DNS Server Set the secondary DNS server.

Windows Name Server Define the Windows Internet Naming Service obtained by DHCP clients from DHCP sever. Generally you can leave it blank.

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).

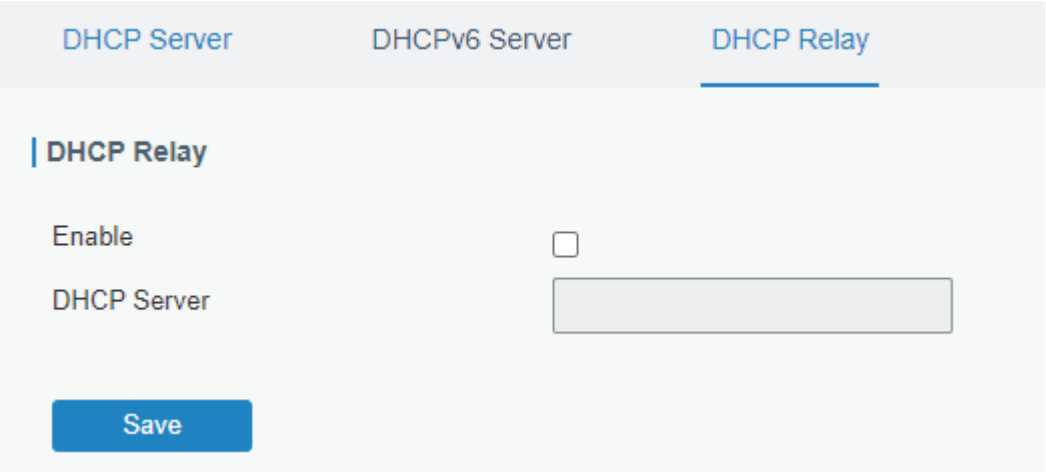
DUID Set a static and specific DUID for the DHCPv6 client (it should be different from other DUID so as to avoid conflict).

IP Address Set a static and specific IP address for the DHCP client (it should be outside of the DHCP range).

DHCP Relay

iSite 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 Relay



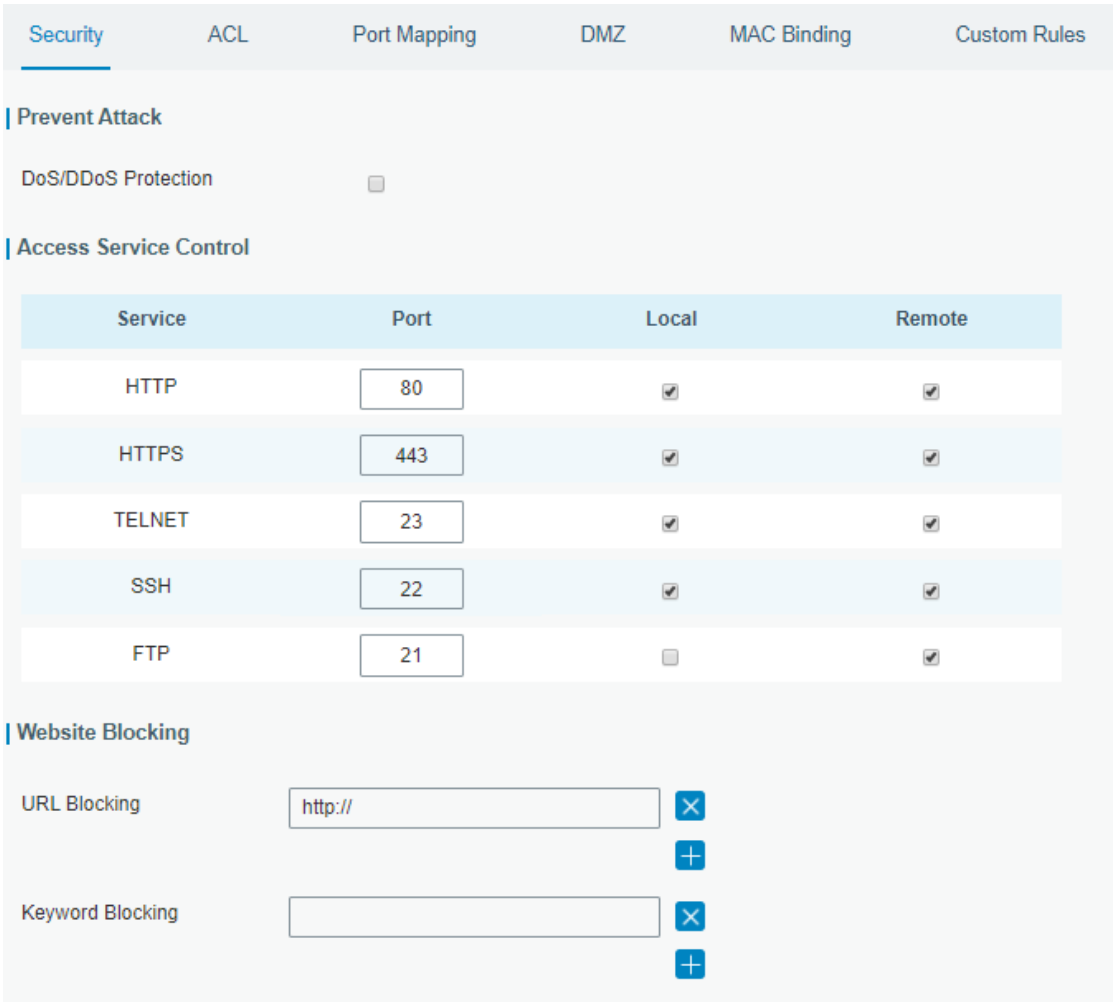
Enable Enable or disable DHCP relay.
DHCP Server Set DHCP server, up to 10 servers can be configured; separate them by blank space or ",".

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.

SECURITY



Prevent Attack

DoS/DDoS Protection Enable/disable Prevent DoS/DDoS Attack.

Access Service Control

Port Set port number of the services. Range: 1-65535.

Local Access the router locally.

Remote Access the router remotely.

HTTP Users can log in the device locally via HTTP to 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.

TELNET Users can log in the device locally and remotely via Telnet after the option is checked.

SSH Users can log in the device locally and remotely via SSH after the option is checked.

FTP Users can log in the device locally and remotely via FTP after the option is checked.

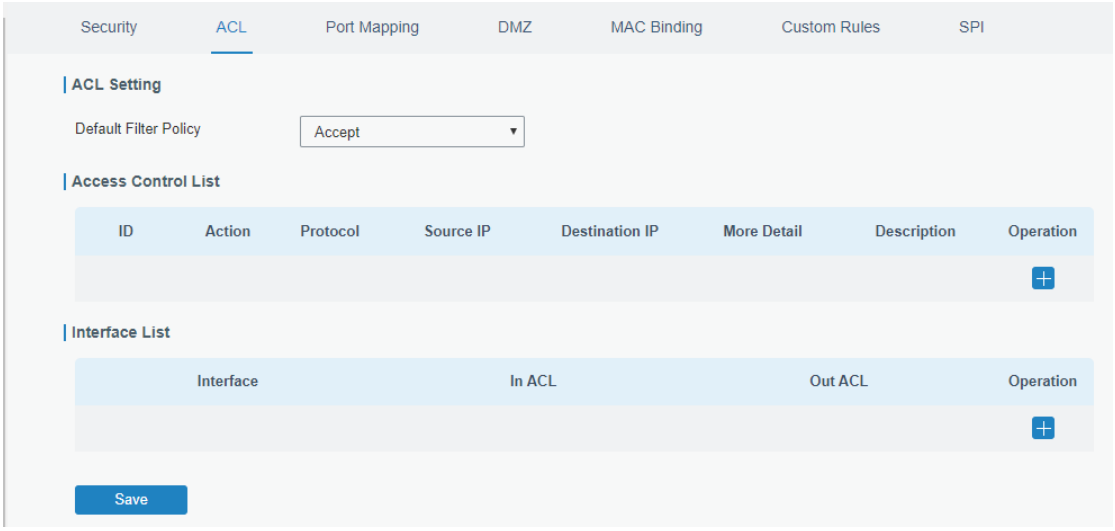
Website Blocking

URL Blocking Enter the HTTP address which you want to block.

Keyword Blocking You can block specific website by entering keyword. The maximum number of character allowed is 64.

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 analysed 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 pre-set strategy.
The data package matching rules defined by ACL can also be used by other functions requiring flow distinction.



ACL Setting

Default Filter Policy Select from "Accept" and "Deny". The packets which are not included in the access control list will be processed by the default filter policy.

Access Control List

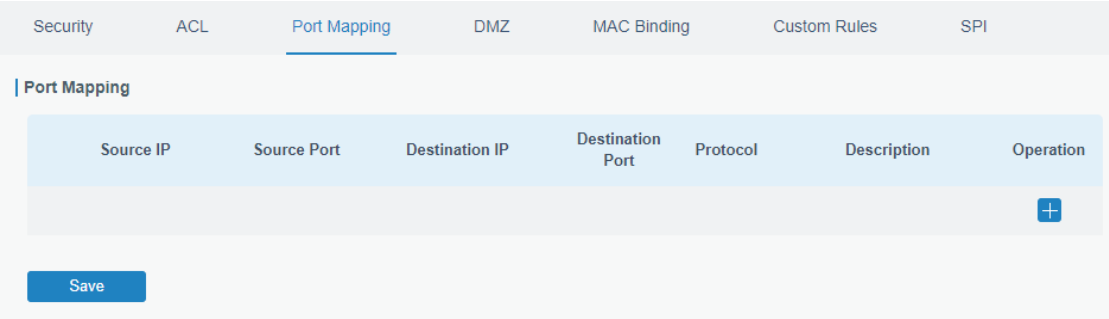
Type Select type from "Extended" and "Standard".
ID User-defined ACL number. Range: 1-199.
Action Select from "Permit" and "Deny".
Protocol Select protocol from "ip", "icmp", "tcp", "udp", and "1-255".
Source IP Source network address (leaving it blank means all).
Source Wildcard Mask Wildcard mask of 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
InterfaceSelect 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.

PORT MAPPING

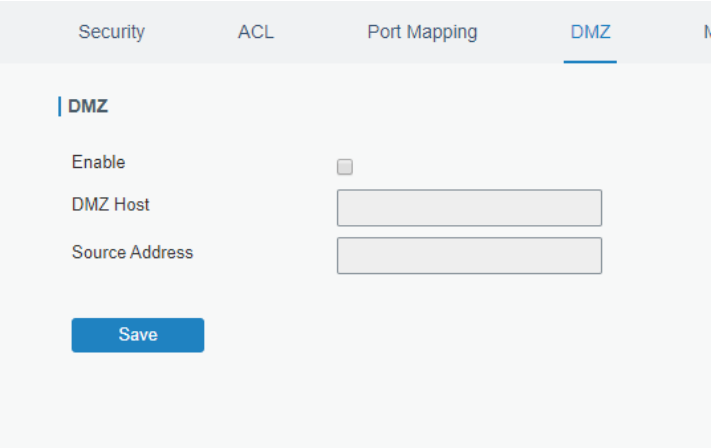
Port mapping is an application of network address translation (NAT) that redirects a communication request from the combination of an address and port number to another while the packets are traversing a network gateway such as a router or firewall.



Port Mapping
Source IP Specify the host or network which can access local IP address. 0.0.0.0/0 means all.
Source Port Enter the TCP or UDP port from which incoming packets are forwarded. Range: 1-65535.
Destination IP Enter the IP address that packets are forwarded to after being received on the incoming interface.
Destination Port Enter the TCP or UDP port that packets are forwarded to after being received on the incoming port(s). Range: 1-65535.
Protocol Select from "TCP" and "UDP" as your application required.
Description The description of this rule.

DMZ

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



DMZ

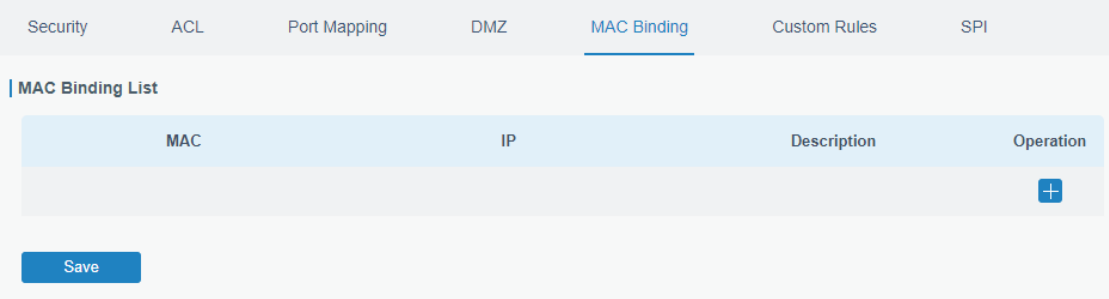
Enable Enable or disable DMZ.

DMZ Host Enter the IP address of the DMZ host on the internal network.

Source Address Set the source IP address which can access to DMZ host. "0.0.0.0/0" means any address.

MAC BINDING

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



MAC Binding List

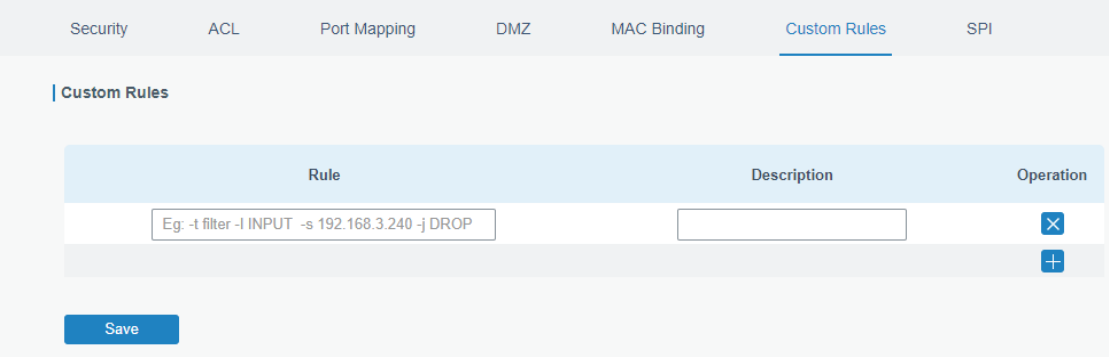
MAC Address Set the binding MAC address.

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.

CUSTOM RULES

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



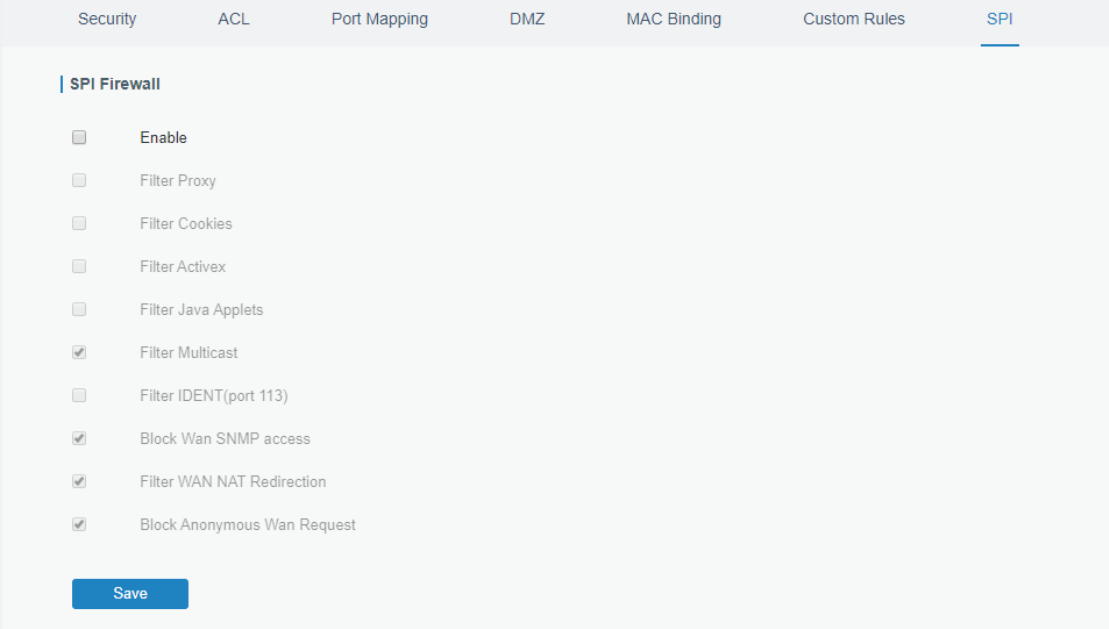
Custom Rules

Rule Specify an iptables rule like the example shows.

Tips: You must reboot the device to take effect after modifying or deleting the iptables rules.

Description Enter the description of the rule.

SPI



SPI Firewall

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".

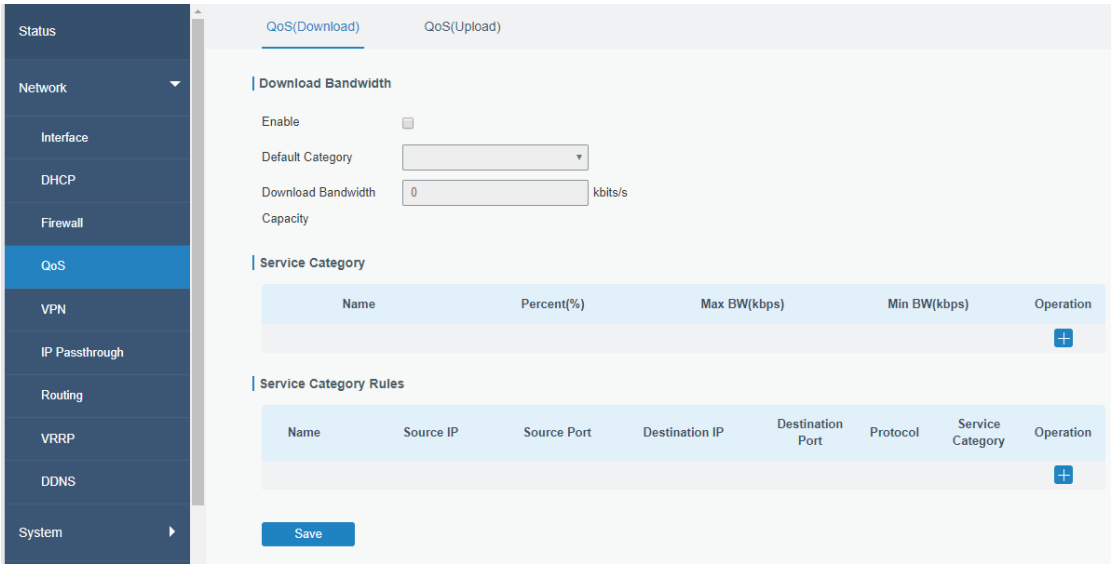
Filter Multicast Prevent multicast packets from reaching the LAN.

Filter IDENT(port 113) Prevent WAN access to Port 113.

Block WAN SNMP access Block SNMP requests from the WAN.
Filter WAN NAT RedirectionPrevent 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.

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.



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
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.

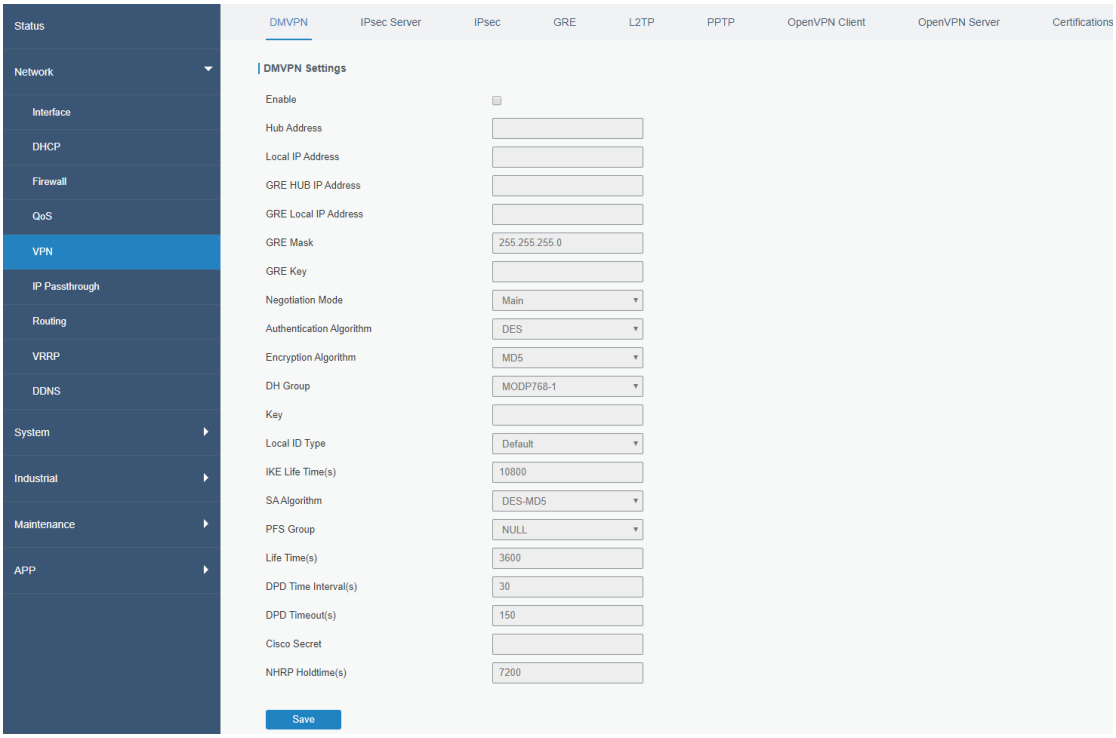
VPN

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 iSite supports DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN, as well as GRE over IPsec and L2TP over IPsec.

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.



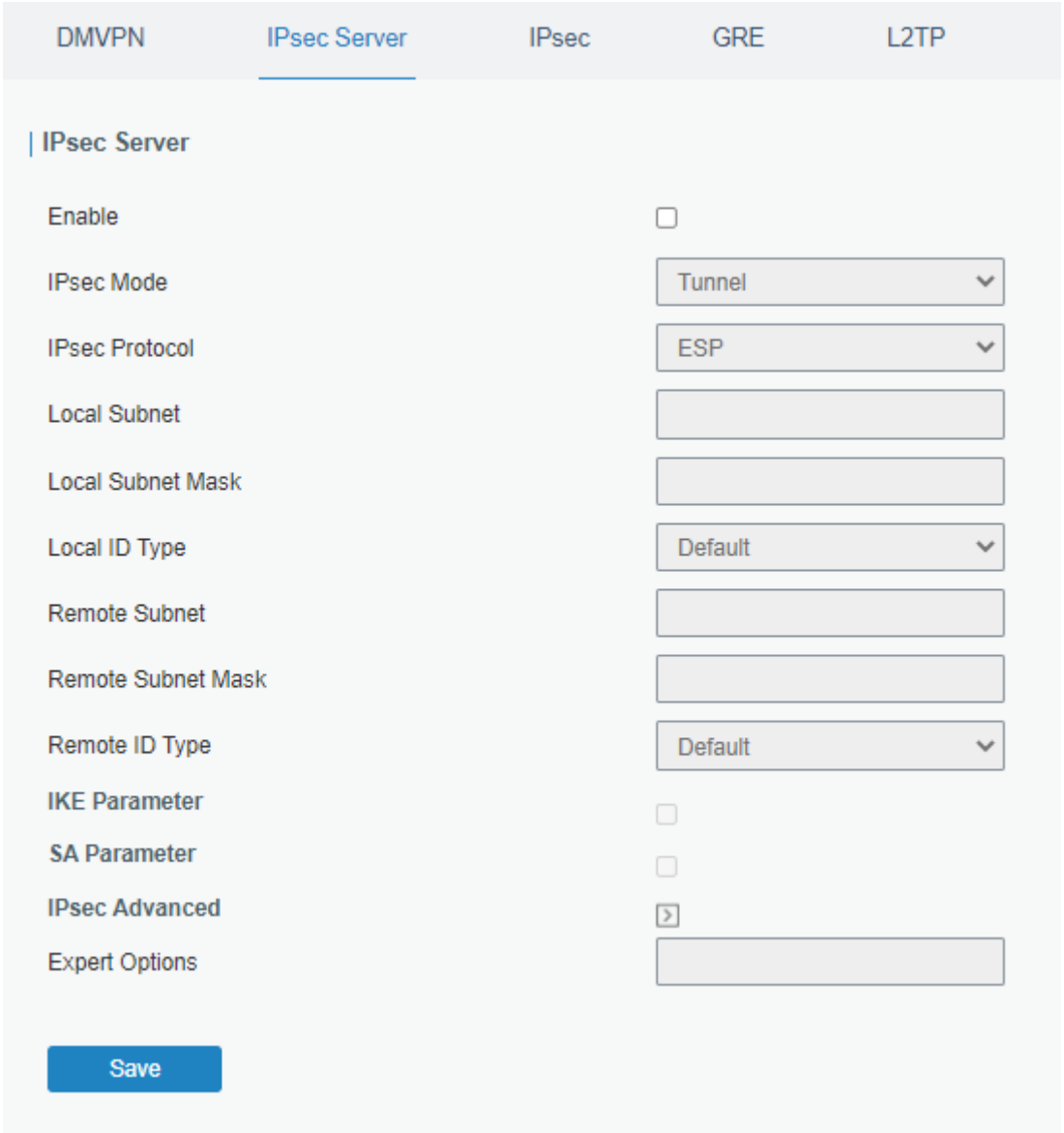
Enable Enable or disable DMVPN.
Hub Address The IP address or domain name of DMVPN Hub.
Local IP address DMVPN local tunnel IP address.
GRE Hub IP Address GRE Hub tunnel IP address.
GRE Local IP Address GRE local tunnel IP address.
GRE Netmask GRE local tunnel netmask.
GRE Key GRE tunnel key.

Negotiation Mode Select from "Main" and "Aggressive".
Authentication Algorithm Select from "DES", "3DES", "AES128", "AES192" and "AES256".
Encryption Algorithm Select from "MD5" and "SHA1".
DH Group Select from "MODP768_1", "MODP1024_2" and "MODP1536_5".
Key Enter the preshared key.
Local ID Type Select from "Default", "ID", "FQDN", and "User FQDN"
IKE Life Time (s) Set the lifetime in IKE negotiation. Range: 60-86400.
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".
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.

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 managed without requiring changes to individual user computers.

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



IPsec Server

Enable 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.

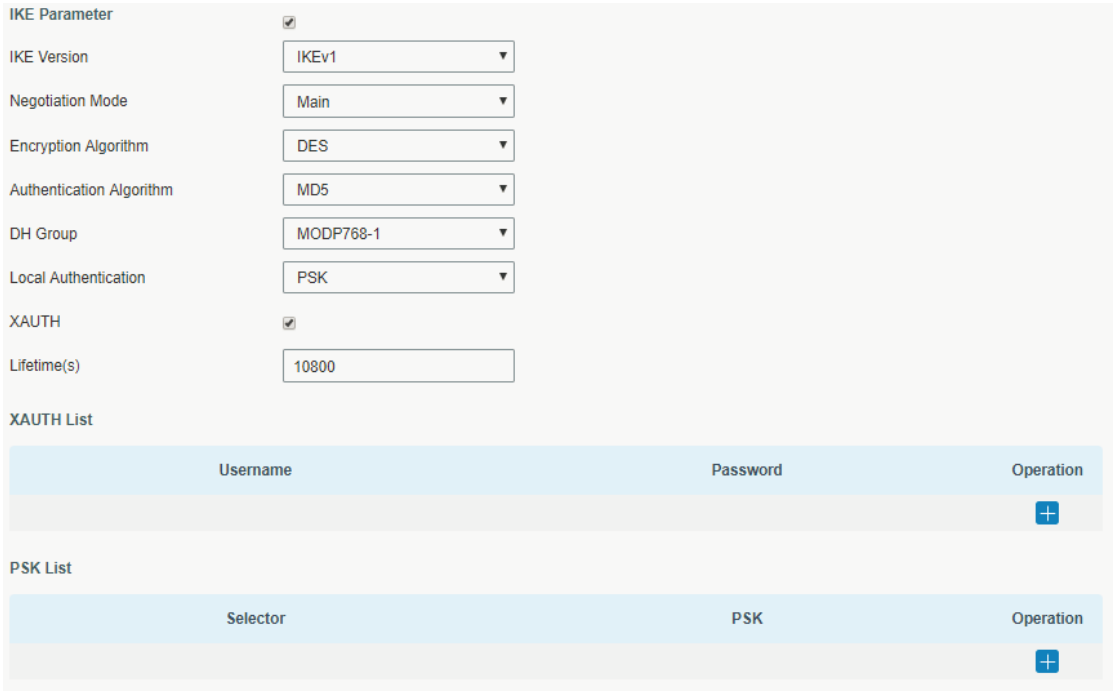
Local Subnet Netmask Enter the local netmask that IPsec protects.

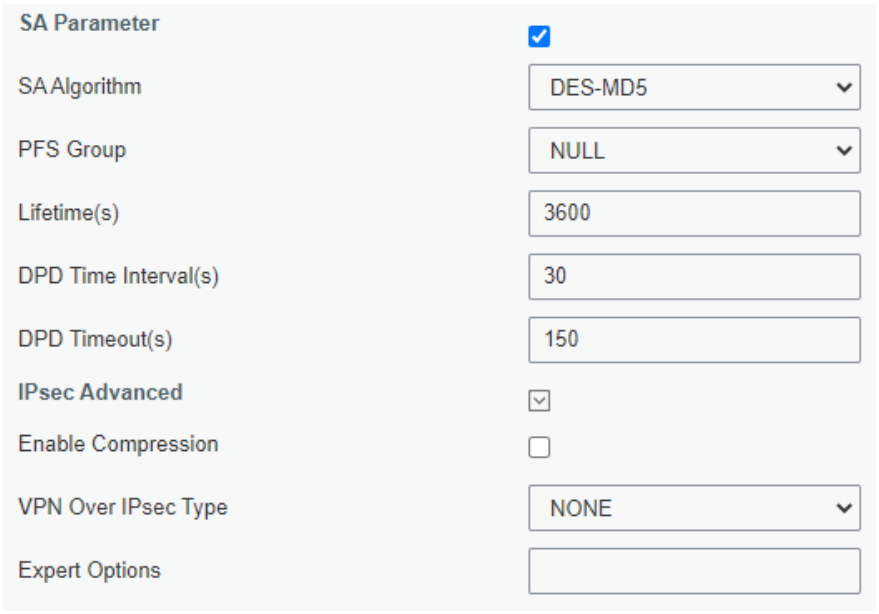
Local ID Type Select from "Default", "ID", "FQDN", and "User FQDN".

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".





IKE Parameter

IKE Version Select from "IKEv1" and "IKEv2".

Negotiation Mode Select from "Main" and "Aggressive".

Encryption Algorithm Select from "DES", "3DES", "AES128", "AES192" and "AES256".

Authentication Algorithm Select from "MD5" and " SHA1"

DH Group Select from "MODP768_1", "MODP1024_2" and "MODP1536_5".

Local Authentication Select from "PSK" and "CA".

XAUTH Enter XAUTH username and password after XAUTH is enabled.

Lifetime (s) Set the lifetime in IKE negotiation. Range: 60-86400.

XAUTH List

Username Enter the username used for the xauth authentication.

Password Enter the password used for the xauth authentication.

PSK List

Selector Enter the corresponding identification number for PSK authentication.

PSK Enter the pre-shared key.

SA Parameter

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.

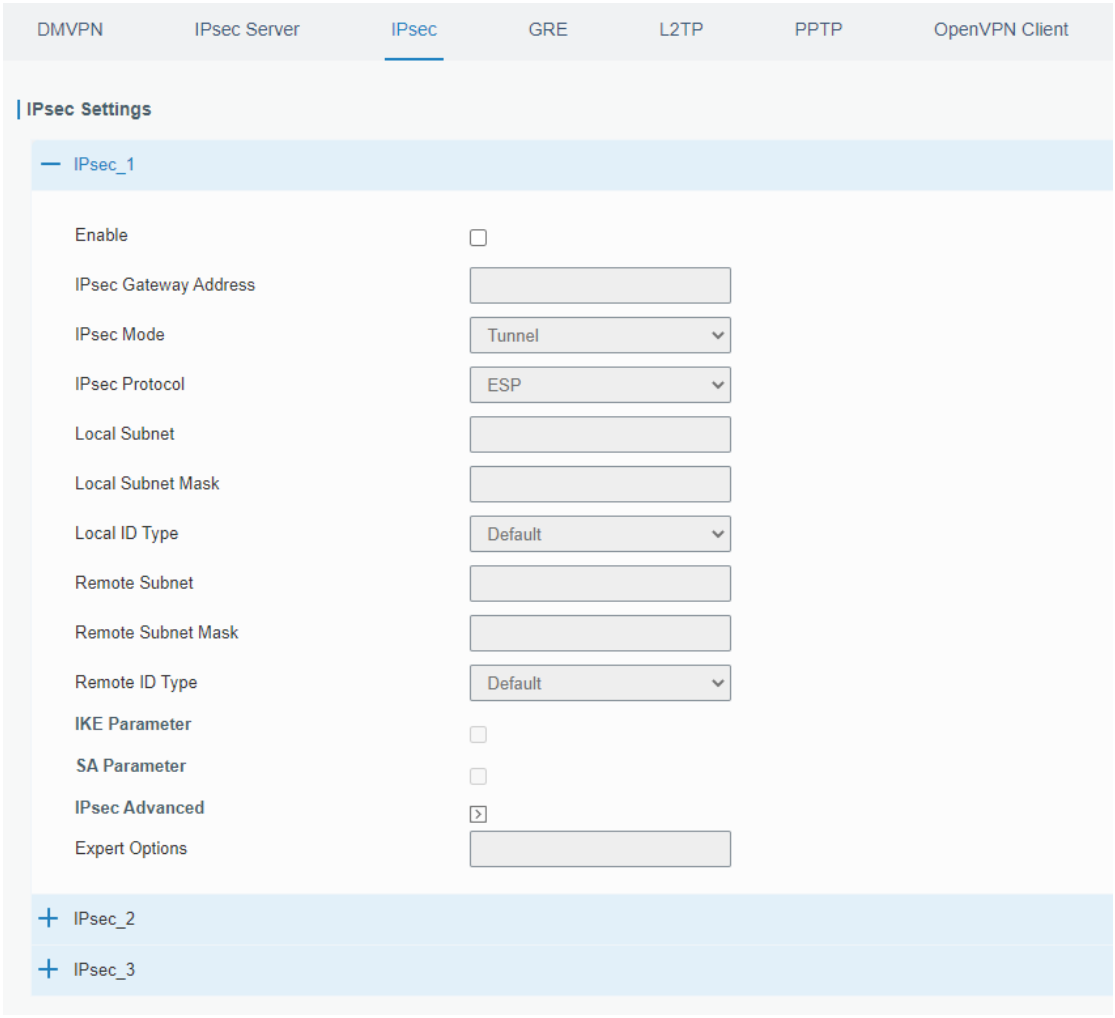
IPsec Advanced

Enable Compression The head of IP packet will be compressed after it is enabled.

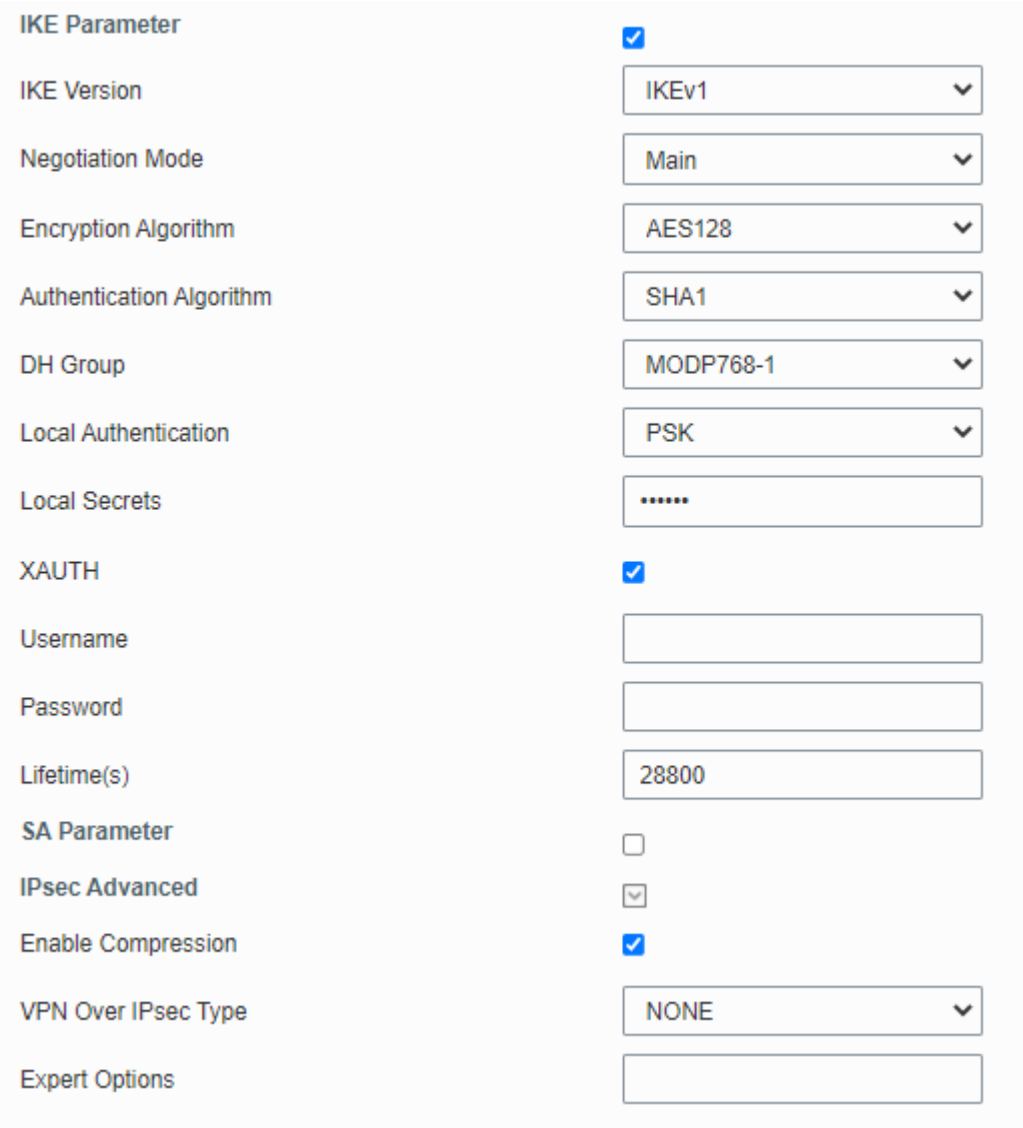
VPN Over IPsec Type Select from "NONE", "GRE" and "L2TP" to enable VPN over IPsec function.

Expert Options 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.

IPSEC



Enable Enable IPsec tunnel. A maximum of 3 tunnels is allowed.
IPsec Gateway AddressEnter 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".



IKE Parameter

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

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.

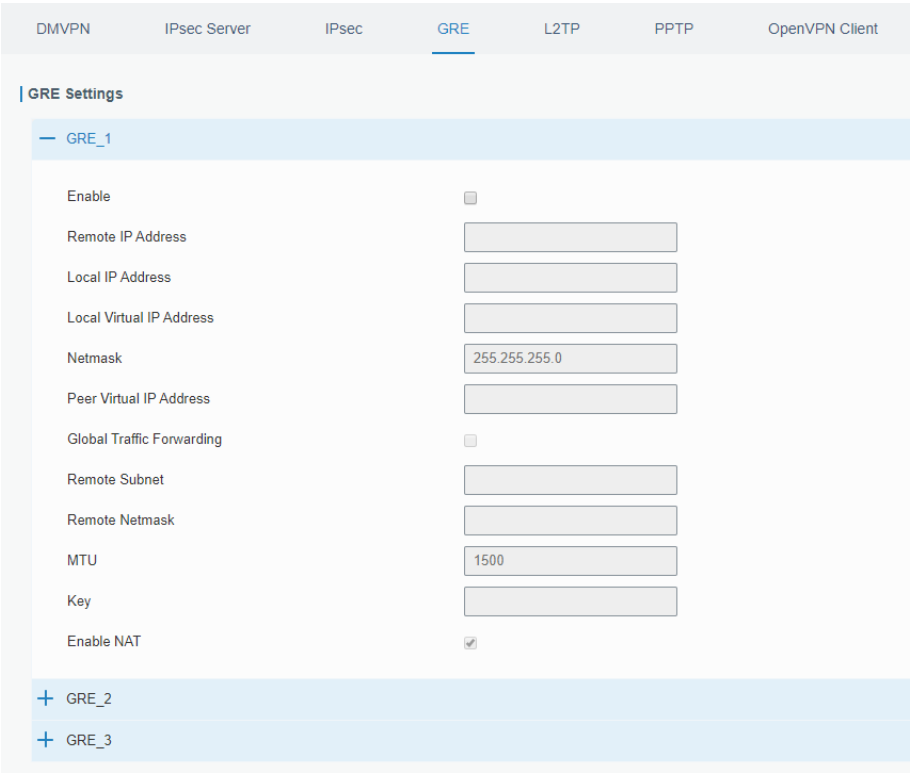
IPsec Advanced
Enable Compression The head of IP packet will be compressed after it is enabled.
VPN Over IPsec Type Select from "NONE", "GRE" and "L2TP" to enable VPN over IPsec function.
Expert Option User can enter some other initialization strings in this field and separate the strings with ";." For example, if more local or remote subnet need to be added, users can add contents here.

GRE

Generic Routing Encapsulation (GRE) is a protocol that encapsulates packets in order to route other protocols over IP networks. It is a tunnelling 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:

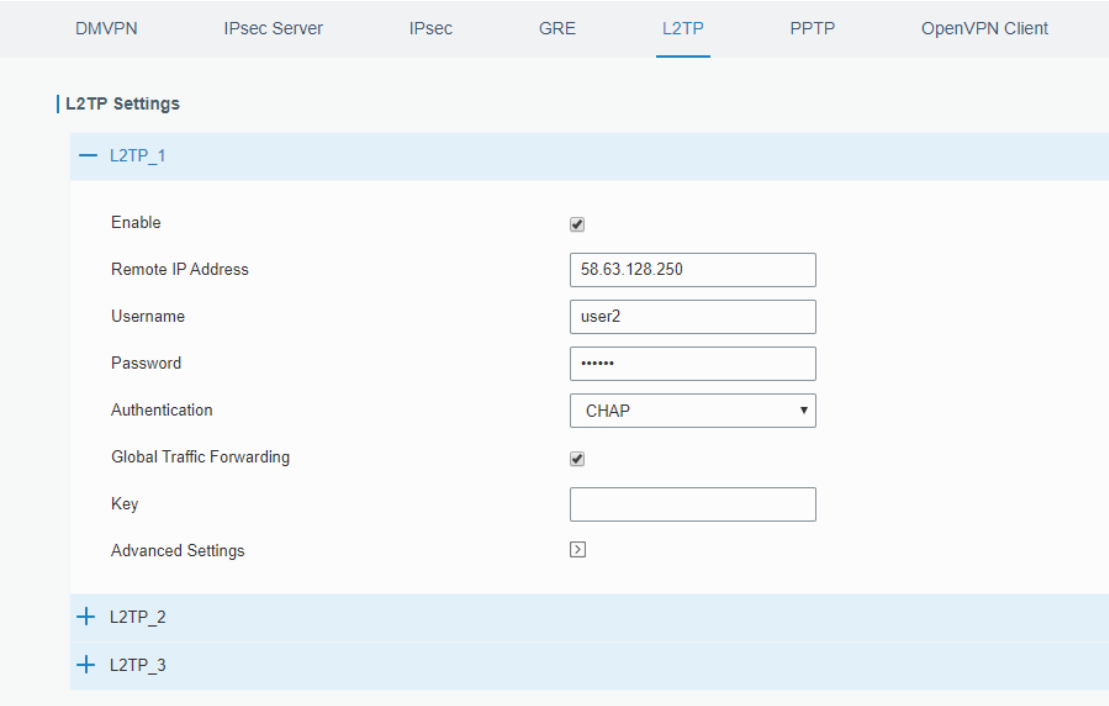
- GRE tunnel could transmit multicast data packets as if it were a true network interface. Sole use of IPsec cannot achieve the encryption of multicast.
- A certain protocol adopted cannot be routed.
- A network of different IP addresses shall be required to connect other two similar networks.



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

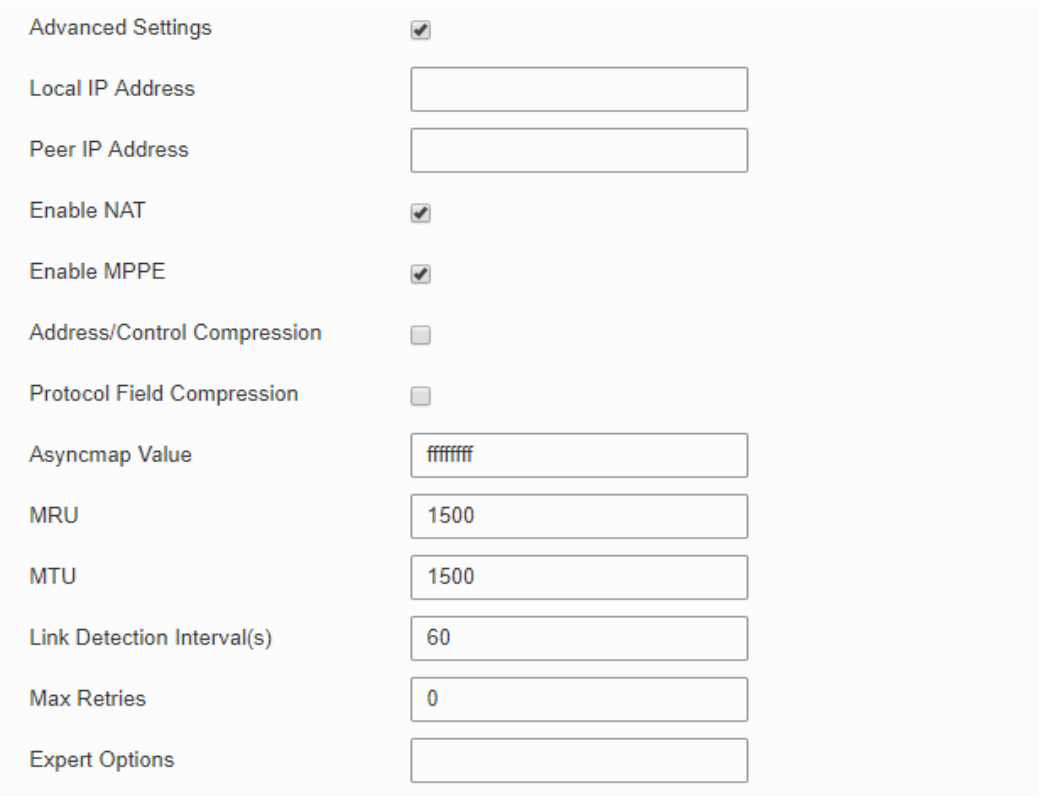
L2TP

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



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 Forwarding All of the data traffic will be sent out via L2TP tunnel after this function is enabled.
Remote Subnet Enter the remote IP address that L2TP protects.

Remote Subnet Mask Enter the remote netmask that L2TP protects.
Key Enter the password of L2TP tunnel.

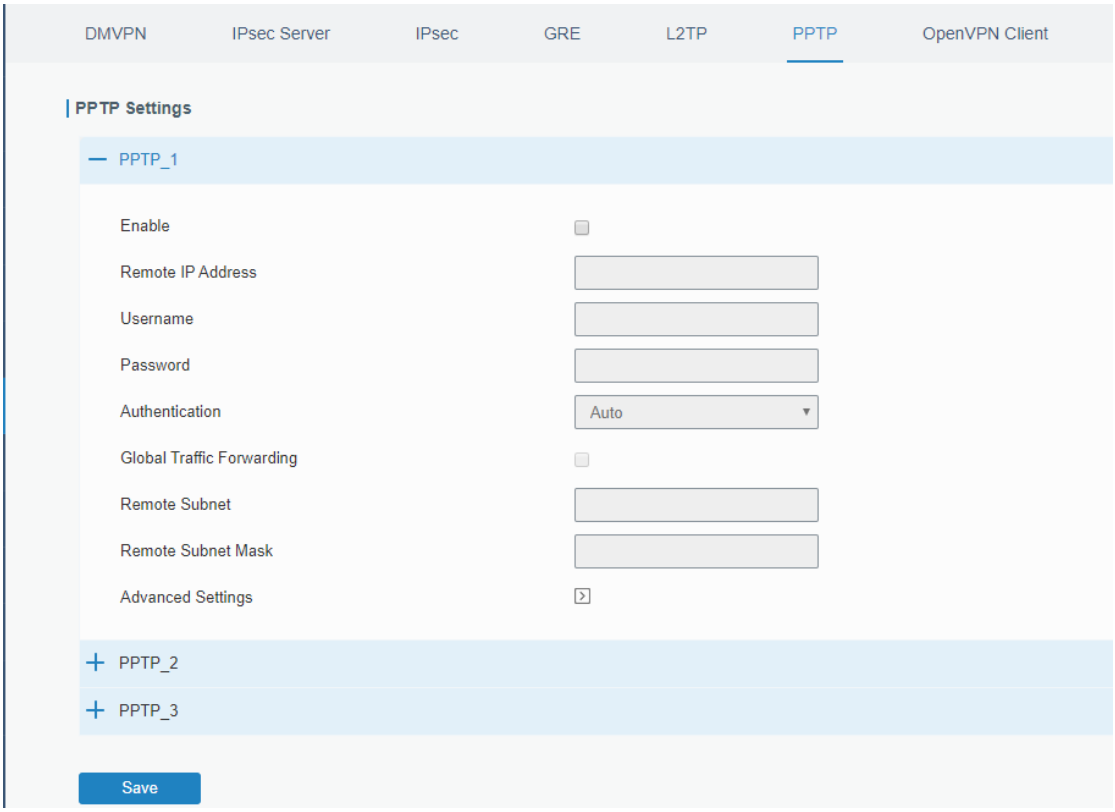


Advanced Settings

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

PPTP

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



PPTP

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.

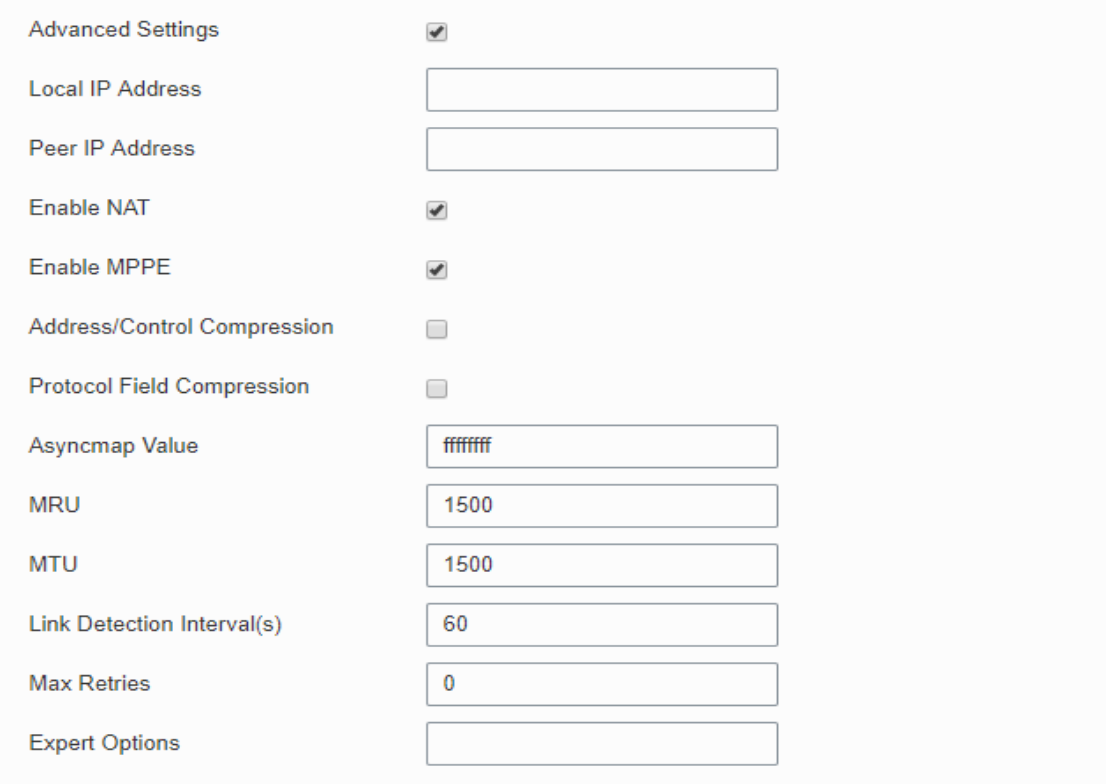
Password Enter the password that PPTP server provides.

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.



PPTP Advanced Settings

Local IP Address Set IP address of PPTP client.

Peer IP Address Enter tunnel IP address of PPTP server.

Enable NAT Enable the NAT faction of PPTP.

Enable MPPE Enable MPPE encryption.

Address/Control Compression For PPP initialization. User can keep the default option.

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

Asyncmap Value One of the PPP protocol initialization strings. User can keep the default value. Range: 0-ffffffff.

MRU Enter the maximum receive unit. Range: 0-1500.

MTU Enter the maximum transmission unit. Range: 0-1500.

Link Detection Interval (s) Set the link detection interval time to ensure tunnel connection. Range: 0-600.

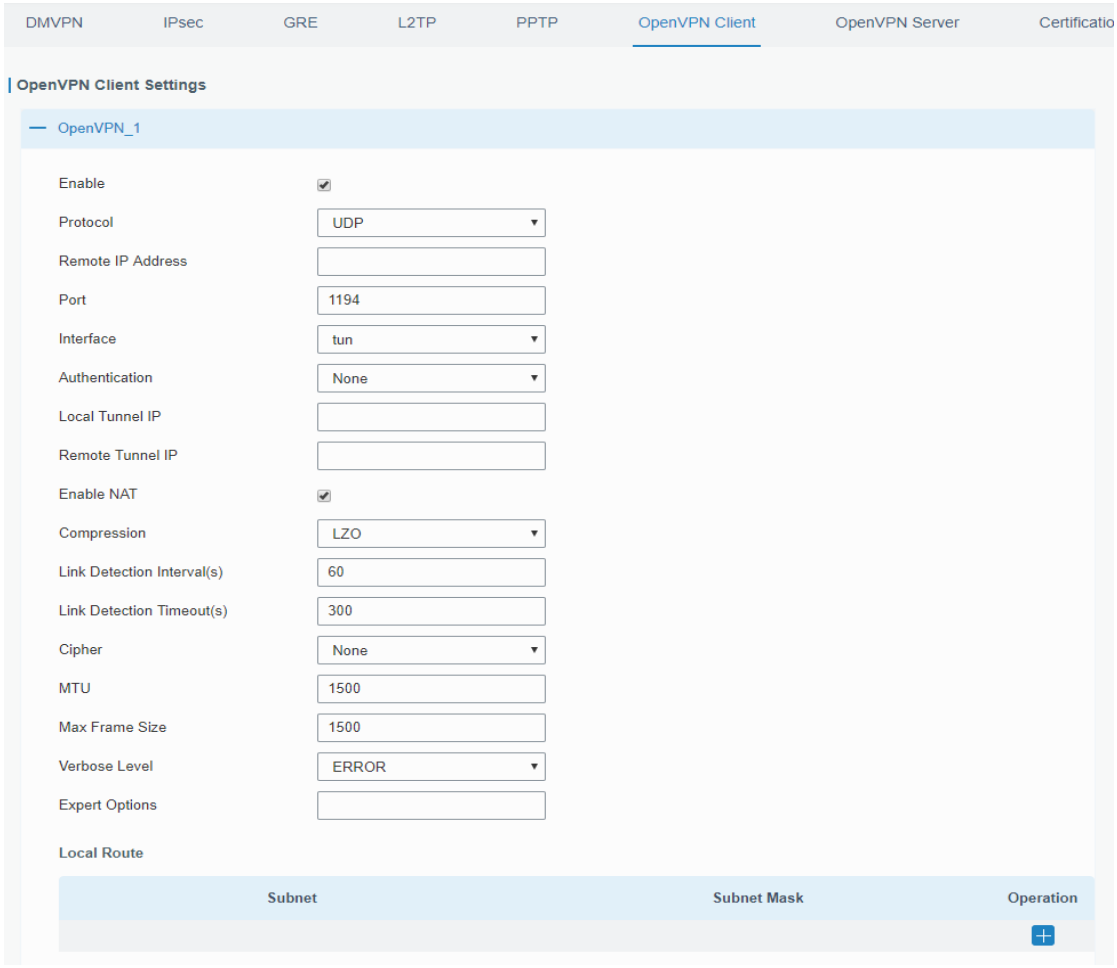
Max Retries Set the maximum times of retrying to detect the PPTP connection failure. Range: 0-10.

Expert Options User can enter some other PPP initialization strings in this field and separate the strings with blank space.

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 manage numerous connections simultaneously.
- All encryption and authentication features of the OpenSSL library.
- Advanced bandwidth management.
- A variety of tunnelling options.
- Compatibility with smart cards that support the Windows Crypt application program interface (API).



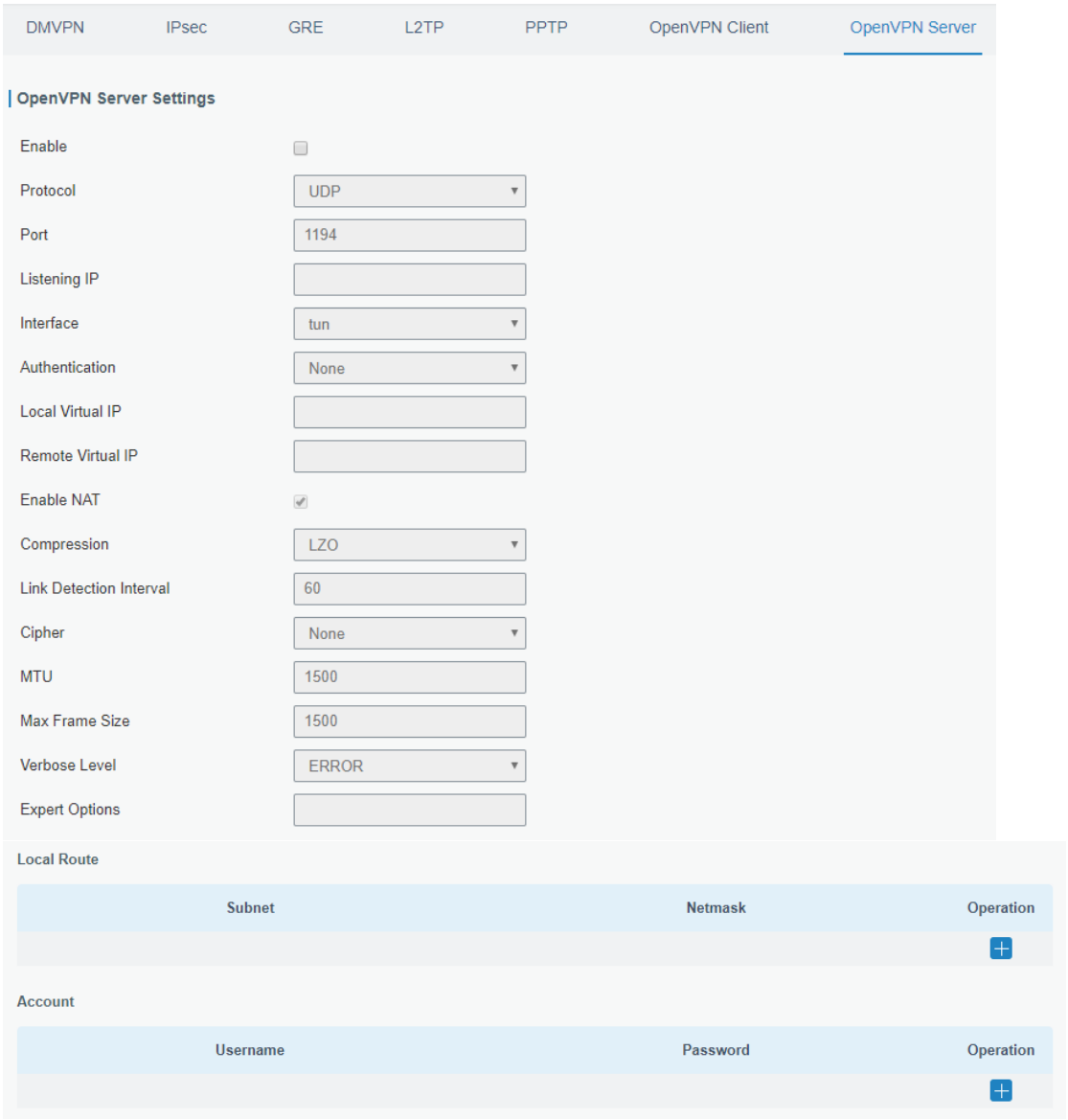
Enable Enable OpenVPN client. A maximum of 3 tunnels is allowed.
Protocol Select from "UDP" and "TCP".
Remote IP Address Enter remote OpenVPN server's IP address or domain name.
Port Enter the listening port number of remote OpenVPN server. Range: 1-65535.
Interface Select from "tun" and "tap".

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 re-established 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.

OPENVPN SERVER

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



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.

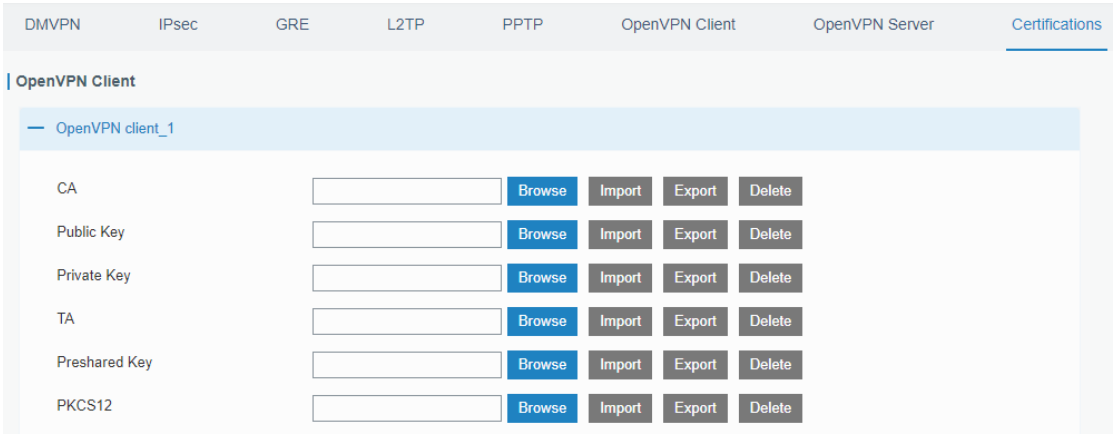
Renegotiation Interval(s) Set interval for renegotiation. Range: 0-86400.
Max Clients Maximum OpenVPN client number. Range: 1-128.
Enable CRL Enable CRL
Enable Client to Client Allow access between different OpenVPN clients.
Enable Dup Client Allow multiple users to use the same certification.
Enable 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 local IP address of OpenVPN client.
Netmask The local netmask of OpenVPN client.

Account
Username & Password Set username and password for OpenVPN client.

CERTIFICATIONS

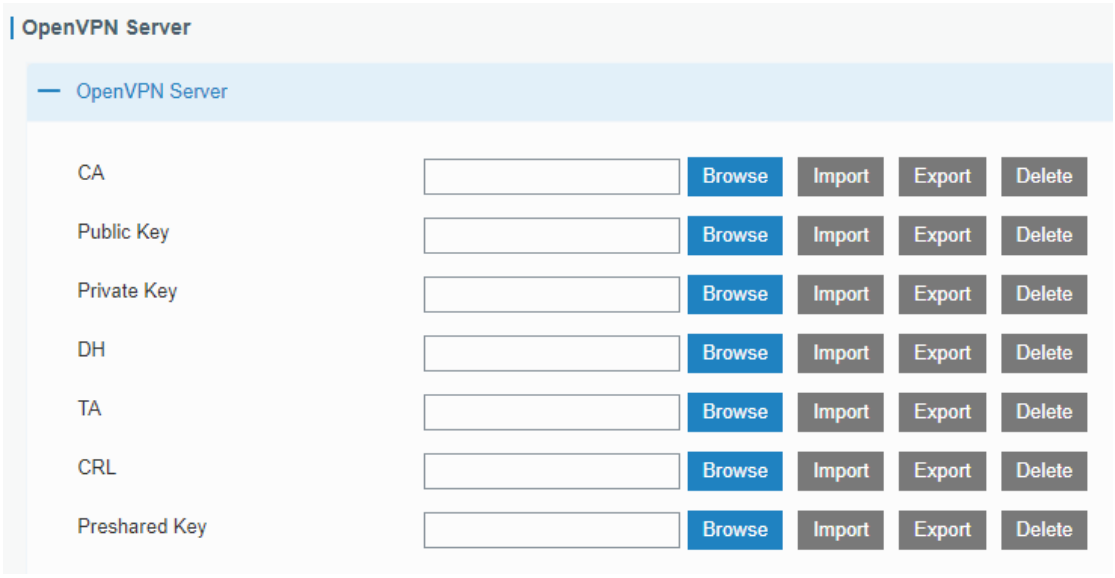
User can import/export certificate and key files for OpenVPN and IPsec on this page.



OpenVPN Client
CA Import/Export CA certificate file.
Public Key Import/Export public key file.
Private Key Import/Export private key file.
TA Import/Export TA key file.

Preshared Key Import/Export static key file.

PKCS12 Import/Export PKCS12 certificate file.



OpenVPN Server

CA Import/Export CA certificate file.

Public Key Import/Export public key file.

Private Key Import/Export private key file.

DH Import/Export DH key file.

TA Import/Export TA key file.

CRL Import/Export CRL.

Preshared Key Import/Export static key file.

IPsec

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.

IPsec Server

CA Import/Export CA certificate.

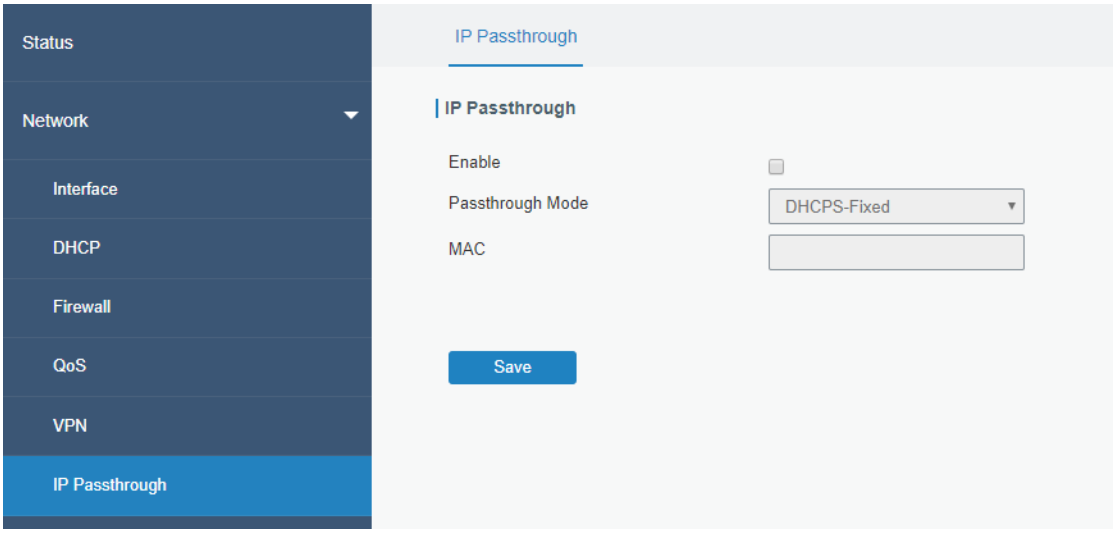
Local Certificate Import/Export Local Certificate file.

Private Key Import/Export private key.

CRL Import/Export certificate recovery list.

IP PASSTHROUGH

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



IP Passthrough

Enable Enable or disable IP Passthrough.

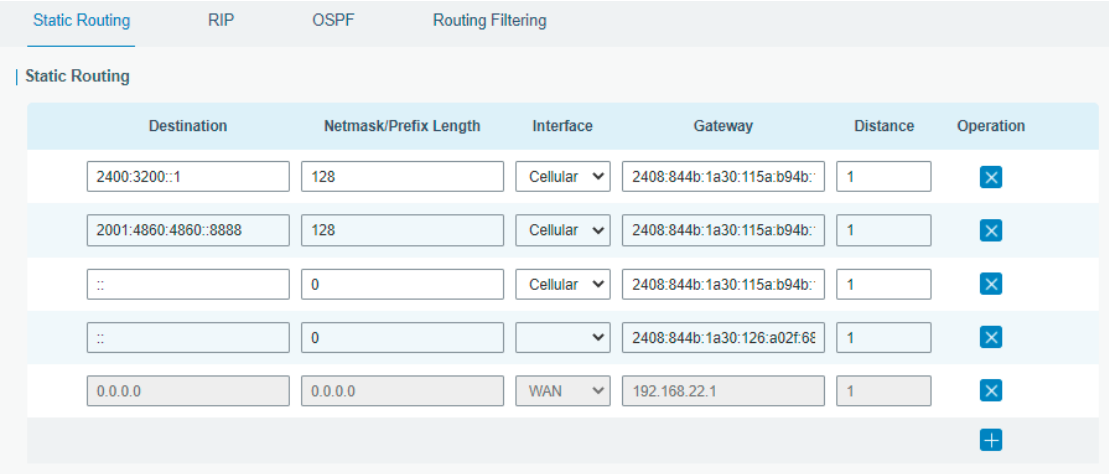
Passthrough Mode Select passthrough mode from “DHCPS-Fixed” and “DHCPS-Dynamic.”

MAC Set MAC address.

ROUTING

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.

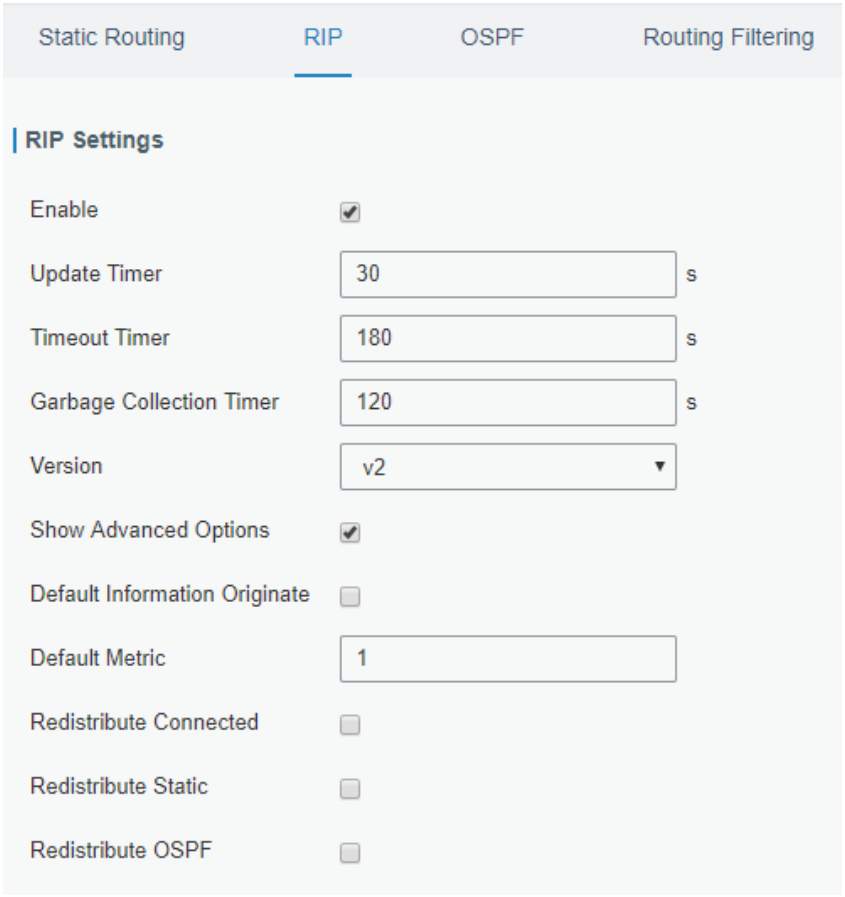


Destination Enter the destination IP address.
Netmask/Prefix Length Enter the subnet mask or prefix length of destination address.
Interface The interface through which the data can reach the destination address.
Gateway IP address of the next router that will be passed by before the input data reaches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

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.



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.

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", "WAN" and "Bridge0".

Passive Interface

Passive Interface Select interface from "cellular0" and "WAN", "Bridge0".

Interface

Interface Select interface from "cellular0", "WAN" and "Bridge0".
Send Version Select from "default", "v1" and "v2".
Receive Version Select from "default", "v1" and "v2".
Split-Horizon Select from "enable" and "disable".
Authentication Mode Select from "text" and "md5".
Authentication String The authentication key for package interaction in RIPV2.
Authentication Key-chain The authentication key-chain for package interaction in RIPV2.

Neighbour

IP Address Set RIP neighbour's IP address manually.

Network

IP Address The IP address of interface for RIP publishing.
Netmask The netmask of interface for RIP publishing.

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:

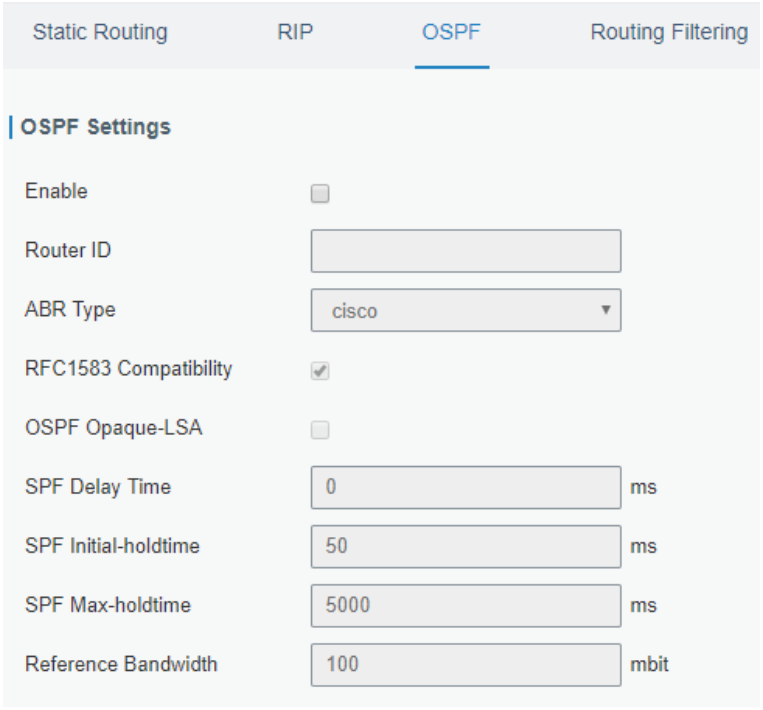
- If a Loopback interface address is configured, then the last configured IP address of Loopback interface will be used as the Router ID;
- If no Loopback interface address is configured, the system will choose the interface with the biggest IP address as the Router ID.

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)

Neighbour and Neighbouring

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 is consistent, a neighbour relationship will be formed. Not all matched sides in neighbour 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.



OSPF

Enable Enable or disable OSPF.

Router ID Router ID (IP address) of the originating LSA.

ABR Type Select from cisco, IBM, standard and shortcut.

RFC1583 Compatibility Enable/Disable.

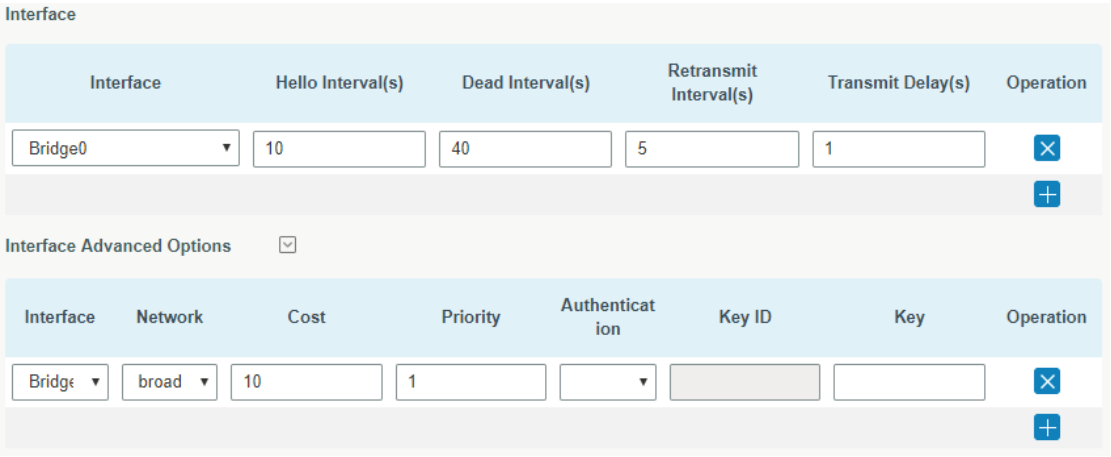
OSPF Opaque-LSA Enable/Disable. **LSA**: a basic communication means of the OSPF routing protocol for the Internet Protocol (IP)

SPF Delay Time Set the delay time for OSPF SPF calculations. Range: 0-6000000, in milliseconds.

SPF Initial-holdtime Set the initialization time of OSPF SPF. Range: 0-6000000, in milliseconds.

SPF Max-holdtime Set the maximum time of OSPF SPF. Range: 0-6000000, in milliseconds.

Reference Bandwidth Range: 1-4294967, in Mbit.



Interface

Interface Select interface from "cellular0",”WAN”and "Bridge0".

Hello Interval (s) Send interval of Hello packet. If the Hello time between two adjacent routers is different, the neighbour relationship cannot be established. Range: 1-65535.

Dead Interval (s) Dead Time. If no Hello packet is received from the neighbours within the dead time, then the neighbour is considered failed. If dead times of two adjacent routers are different, the neighbour relationship cannot be established.

Retransmit Interval (s) When the router notifies an LSA to its neighbour, it is required to make acknowledgement. If no acknowledgement packet is received within the retransmission interval, this LSA will be retransmitted to the neighbour. Range: 3-65535.

Transmit Delay (s) It will take time to transmit OSPF packets on the link. So a certain delay time should be increased before transmission the aging time of LSA. This configuration needs to be further considered on the low-speed link. Range: 1-65535.

Interface Advanced Options

Interface Select interface.

Network Select OSPF network type.

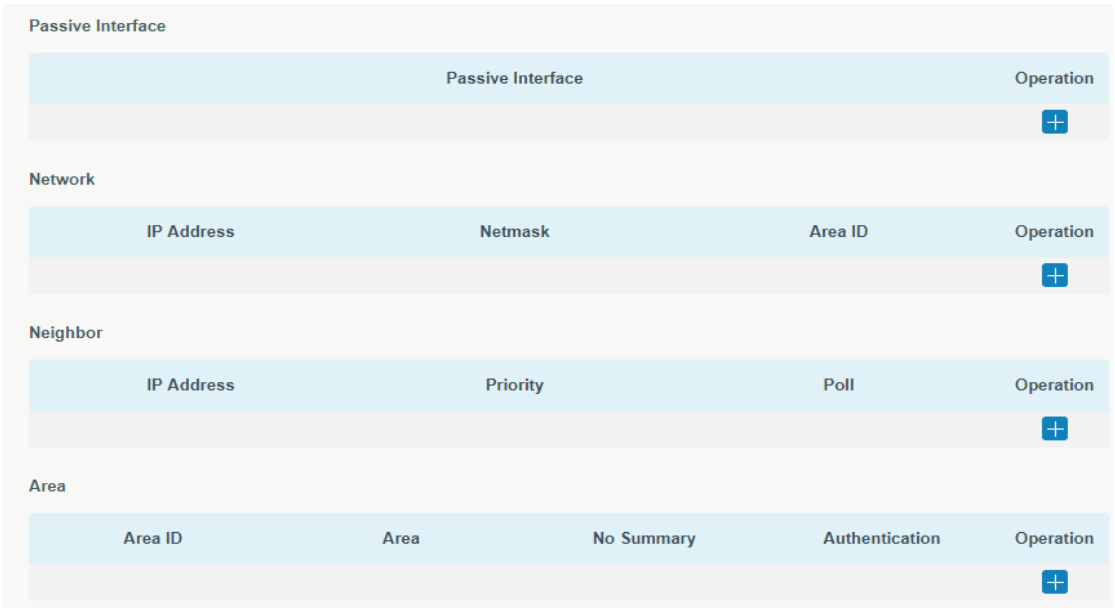
Cost Set the cost of running OSPF on an interface. Range: 1-65535.

Priority Set the OSPF priority of interface. Range: 0-255.

Authentication Set the authentication mode that will be used by the OSPF area. **Simple**: a simple authentication password should be configured and confirmed again. **MD5**: MD5 key & password should be configured and confirmed again.

Key ID It only takes effect when MD5 is selected. Range 1-255.

Key The authentication key for OSPF packet interaction.



Passive Interface

Passive Interface Select interface from "cellular0", "WAN" and "Bridge0".

Network

IP Address The IP address of local network.

Netmask The netmask of local network.

Area ID The area ID of original LSA's router.

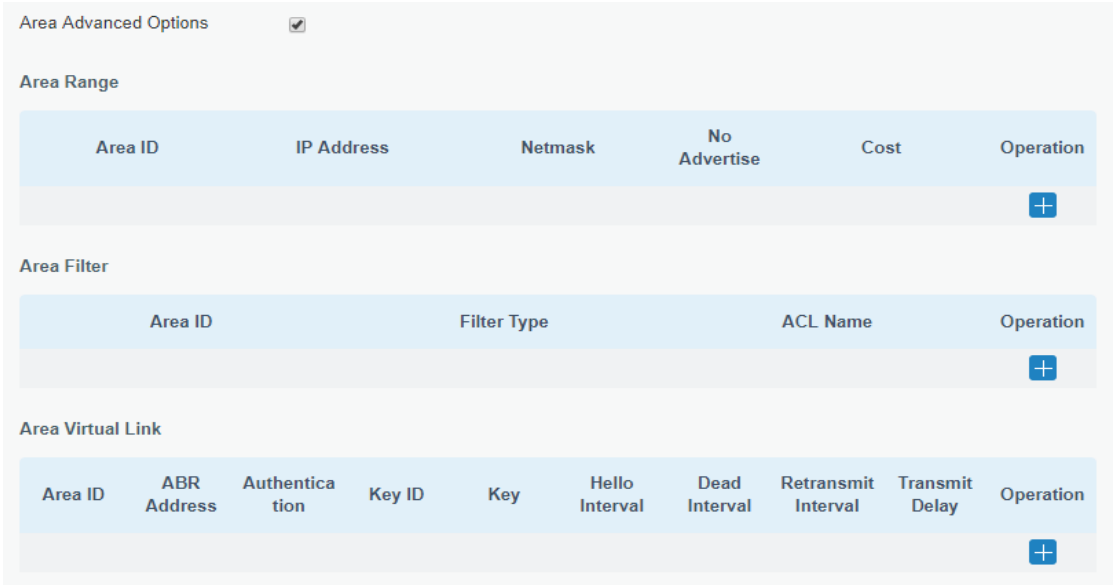
Area

Area ID Set the ID of the OSPF area (IP address).

Area Select from "Stub" and "NSSA". The backbone area (area ID 0.0.0.0) cannot be set as "Stub" or "NSSA".

No Summary Forbid route summarization.

Authentication Select authentication from "simple" and "md5".



Area Advanced Options

Area Range

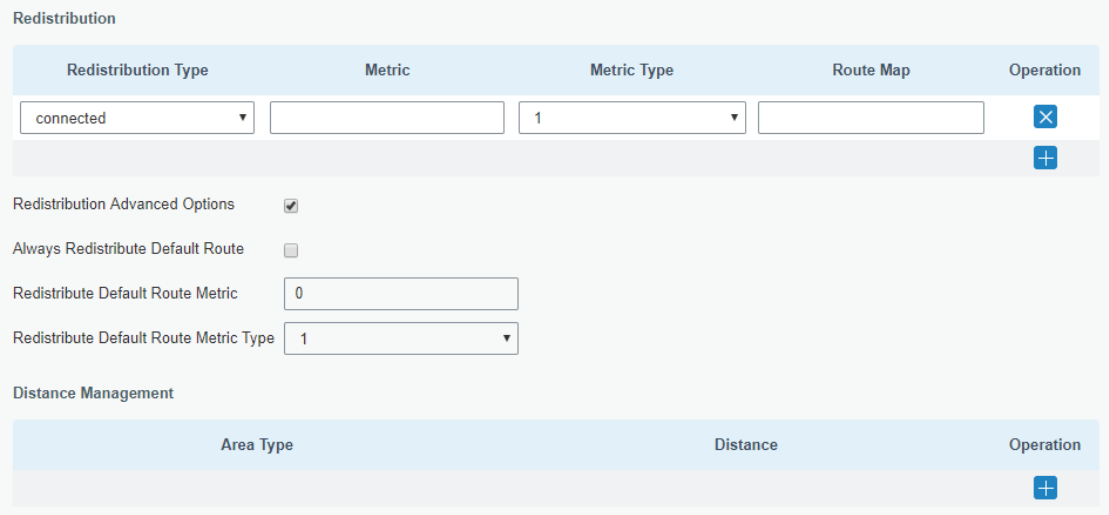
Area ID The area ID of the interface when it runs OSPF (IP address).
IP Address Set the IP address.
Netmask Set the netmask.
No Advertise Forbid the route information to be advertised among different areas.
Cost Range: 0-16777215

Area Filter

Area ID Select an Area ID for Area Filter.
Filter Type Select from "import", "export", "filter-in", and "filter-out".
ACL Name Enter an ACL name which is set on "Routing > Routing Filtering" webpage.

Area Virtual Link

Area ID Set the ID number of OSPF area.
ABR Address ABR is the router connected to multiple outer areas.
Authentication Select from "simple" and "md5".
Key ID It only takes effect when MD5 is selected. Range 1-15.
Key The authentication key for OSPF packet interaction.
Hello Interval Set the interval time for sending Hello packets through the interface. Range: 1-65535.
Dead Interval The dead interval time for sending Hello packets through the interface. Range: 1-65535.
Retransmit Interval The retransmission interval time for re-sending LSA. Range: 1-65535.
Transmit Delay The delay time for LSA transmission. Range: 1-65535.



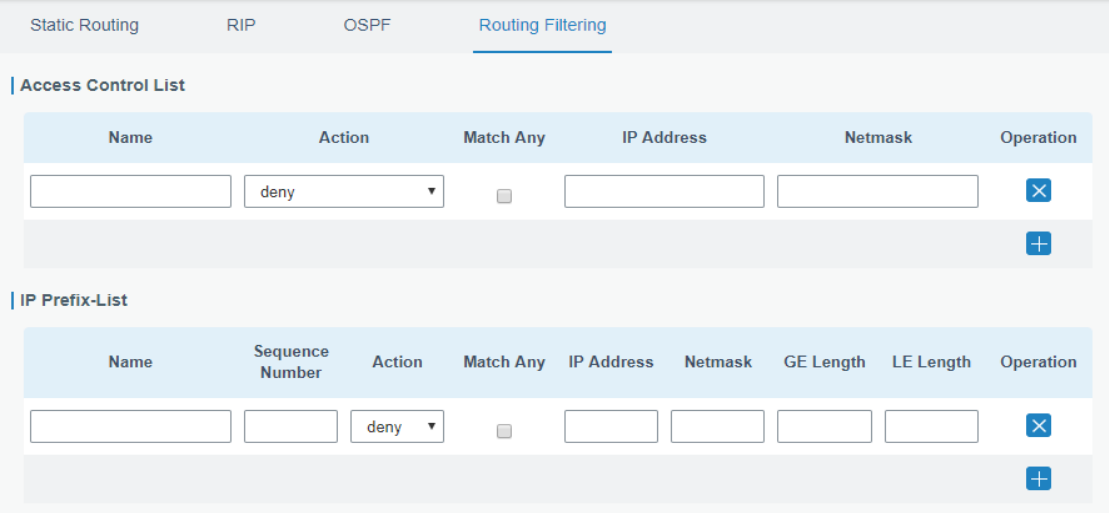
Redistribution

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 Default Route Send redistribution default route after starting up.
Redistribute Default Route Metric Send redistribution default route metric. Range: 0-16777214.
Redistribute Default Route Metric Type Select from "0", "1" and "2".
Distance Management
Area Type Select from "intra-area", "inter-area" and "external".
Distance Set the OSPF routing distance for area learning. Range: 1-255.

ROUTING FILTERING



Access Control List

Name User-defined name, need to start with a letter. Only letters, digits, and underline (_) are allowed.
Action Select from "permit" and "deny".
Match Any No need to set IP address and subnet mask.
IP Address User-defined.
Netmask User-defined.

IP Prefix-List

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

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.

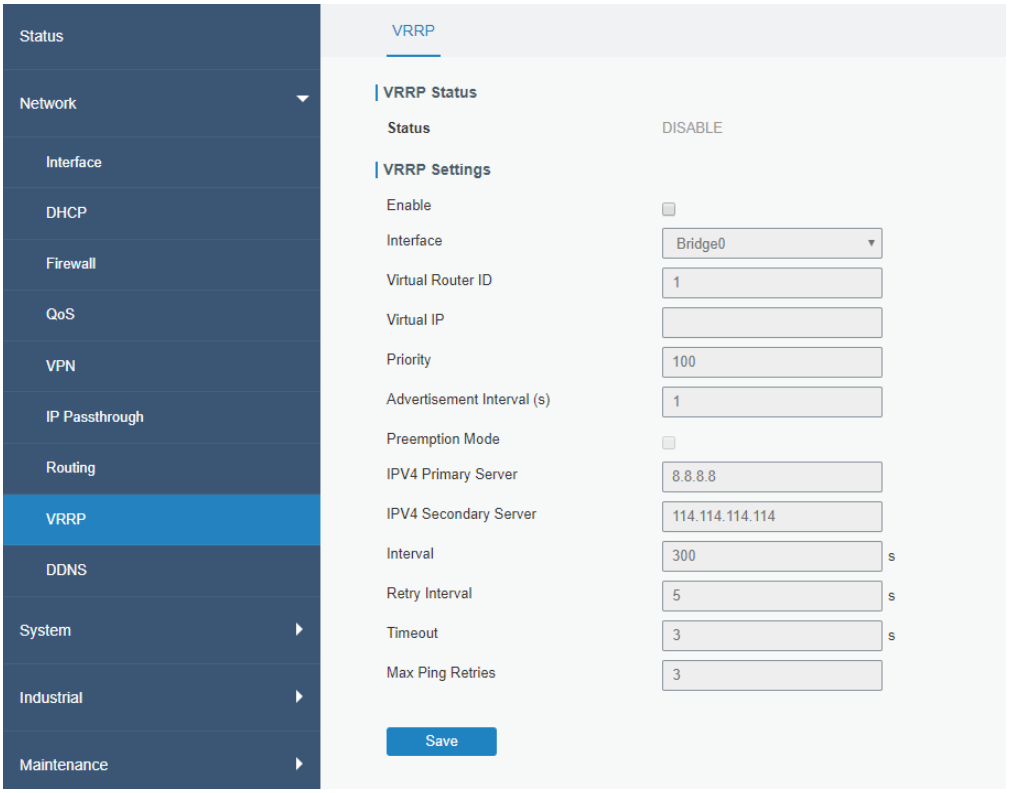
The VRRP router who has the highest number will become the virtual master router. The VRRP router number ranges from 1 to 255 and usually we use 255 for the highest priority and 100 for backup.

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.

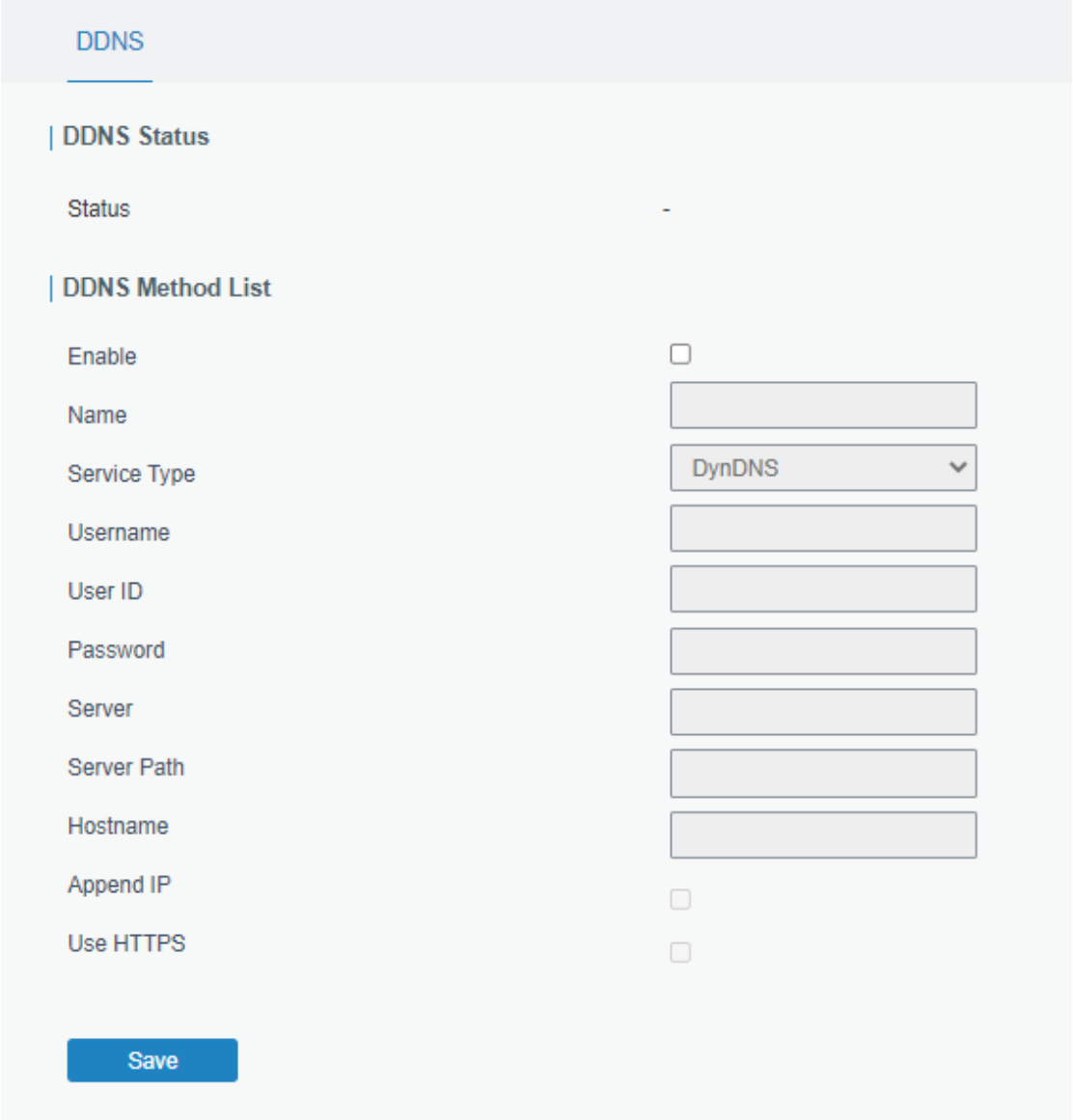
When interface connected with the uplink is at the state of Down or Removed, the router actively lowers its priority so that priority of other routers in the backup group will be higher. Thus the router with the highest priority becomes the gateway for the transmission task.



Enable Enable or disable VRRP.
Interface Select the interface of Virtual Router.
Virtual Router ID User-defined Virtual Router ID. Range: 1-255.
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.
Advertisement Interval (s) Heartbeat package transmission time interval between routers in the virtual ip group. Range: 1-255.
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.
IPV4 Primary Server The router will send ICMP packet to the IP address or hostname to determine whether the Internet connection is still available or not.
IPV4 Secondary Server The router will try to ping the secondary server name if primary server is not available.
Interval Time interval (in seconds) between two Pings.
Retry Interval Set the ping retry interval. When ping failed, the router will ping again 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 as failure.
Max Ping Retries The retry times of the router sending ping request until determining that the connection has failed.

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.



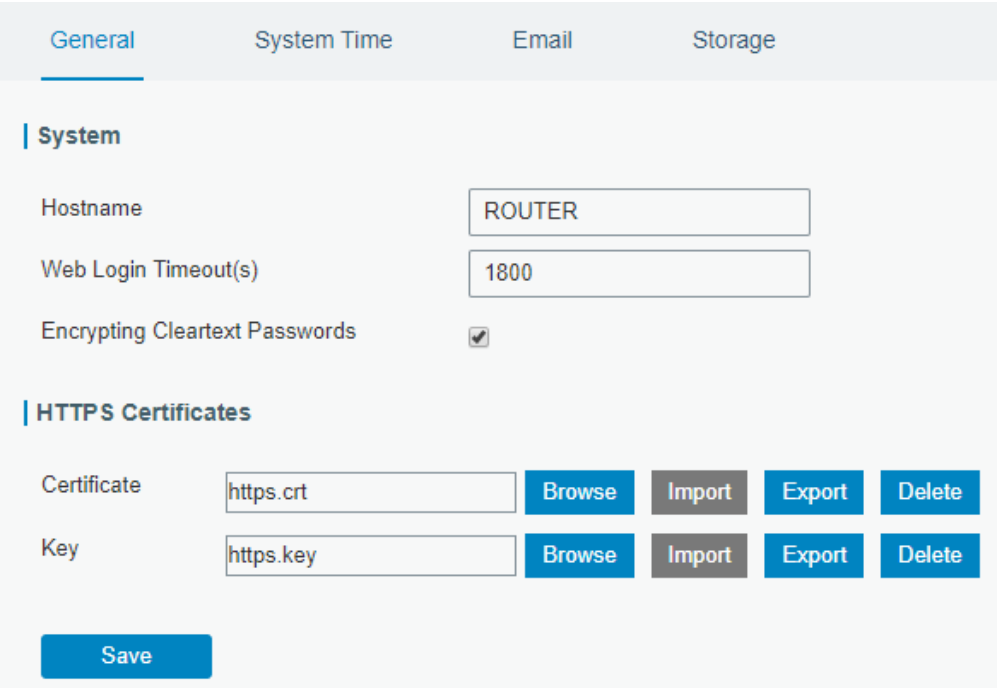
Enable Enable/disable DDNS.
Name Give the DDNS a descriptive name.
InterfaceSet interface bundled with the DDNS.
Service Type Select the DDNS service provider.
Username Enter the username for DDNS register.
User ID Enter User ID of the custom DDNS server.
Password Enter the password for DDNS register.
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.

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.

General settings include system info and HTTPS certificates.



Hostname User-defined router name, needs to start with a letter.
Web Login Timeout (s) You need to log in again if it times out. Range: 100-3600.
Encrypting Cleartext Passwords This function will encrypt all of cleartext passwords into ciphertext passwords.

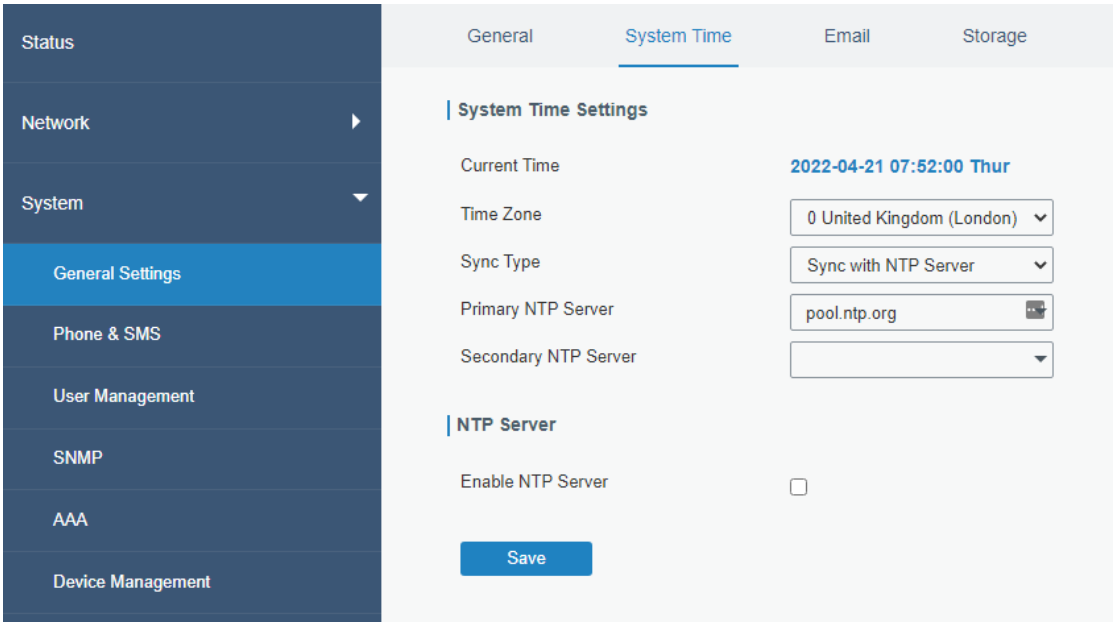
HTTPS Certificates

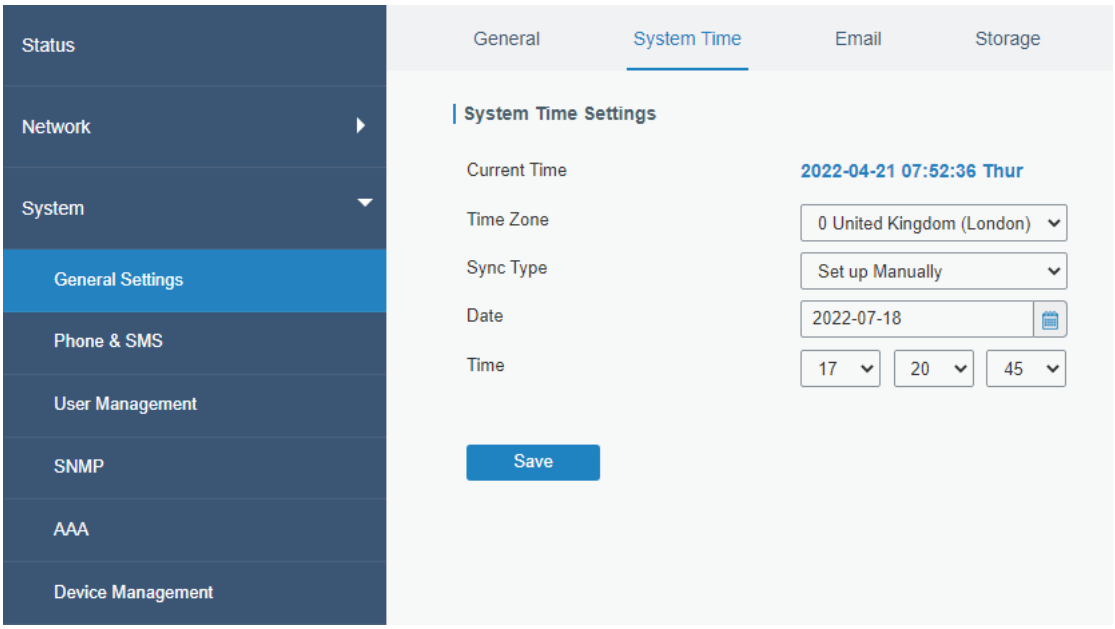
Certificate Click "**Browse**" button, choose certificate file on the PC, and then click "**Import**" button to upload the file into router. Click "**Export**" button will export the file to the PC. Click "**Delete**" button will delete the file.
Key Click "Browse" button, choose key file on the PC, 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.

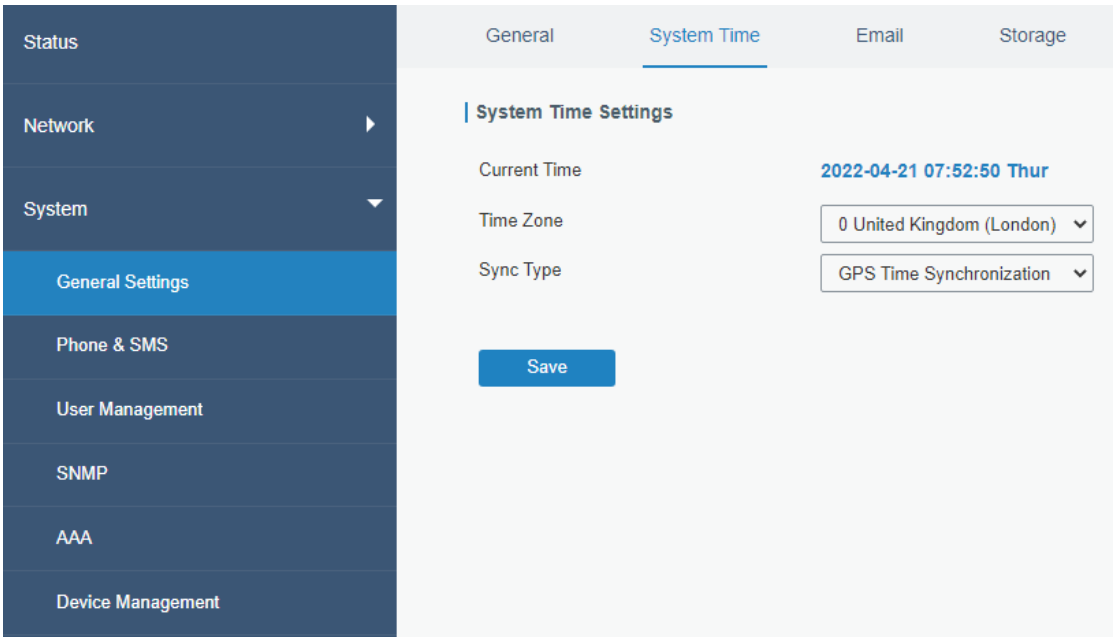
SYSTEM TIME

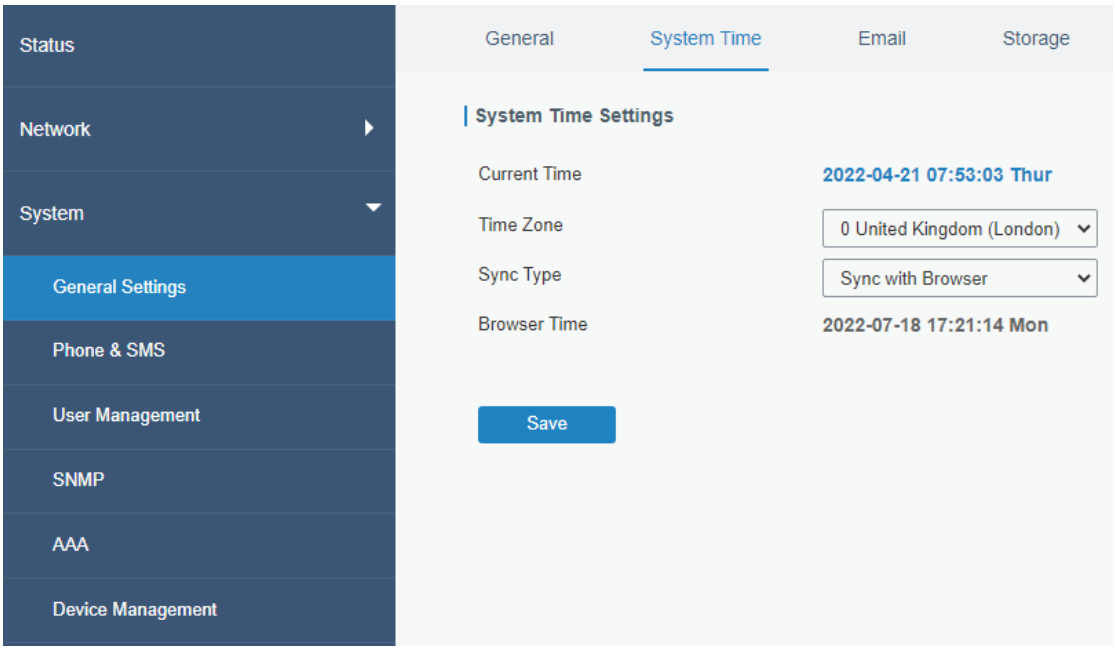
This section explains how to set the system time including time zone and time synchronization type.

Note: to ensure that the router runs with the correct time, it is recommended that you set the system time when configuring the router.









System Time

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.

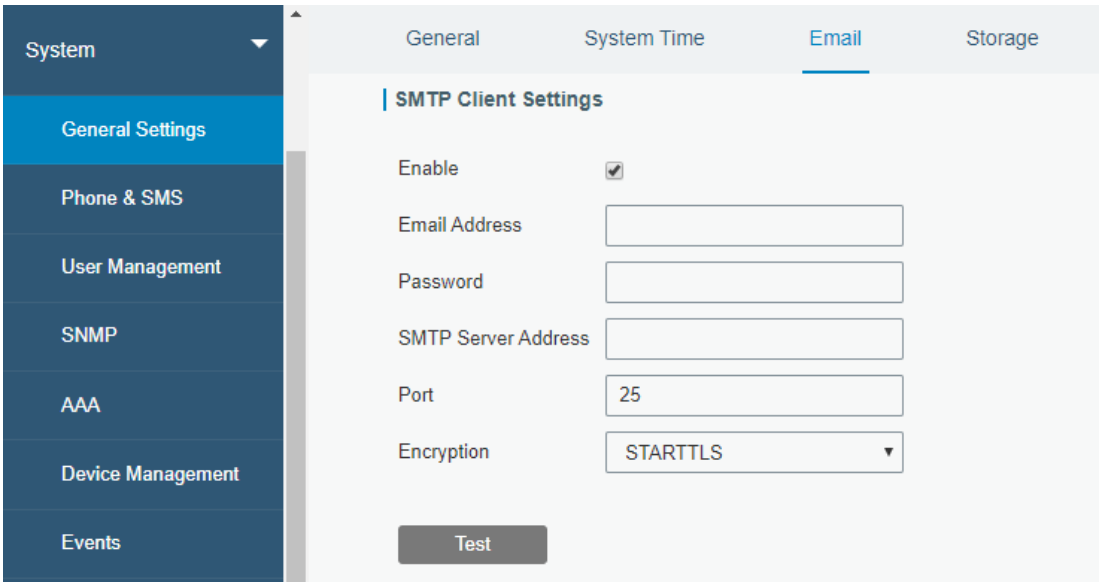
Secondary NTP Server Enter secondary NTP Server's IP address or domain name.

NTP Server

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

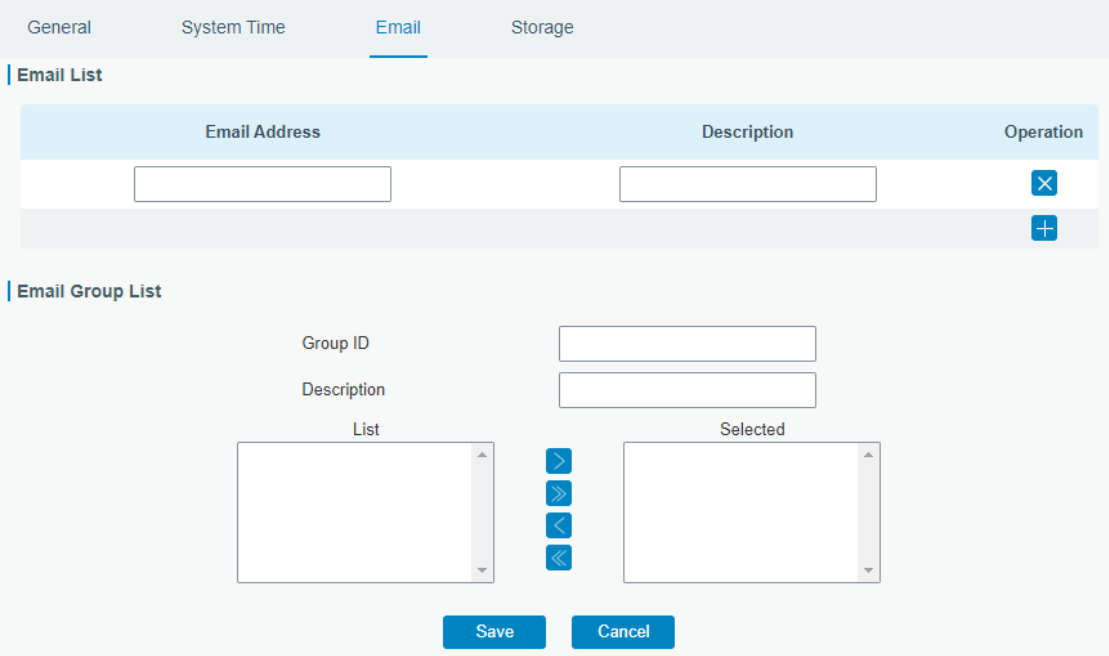
Email

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.



SMTP Client Settings

Enable Enable or disable SMTP client function.
Email Address Enter the sender's email account.
Password Enter the sender's email password.
SMTP Server Address Enter SMTP server's domain name.
Port Enter SMTP server port. Range: 1-65535.
Encryption 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. **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 are referring to a specific version of the protocol. The default port is 465.



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.

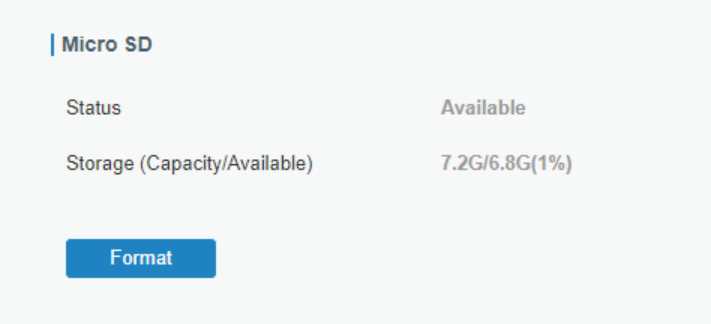
Description The description of the Email group.

List Show the Email address list.

Selected Show the selected Email address.

STORAGE

You can view Micro SD card information on this page.



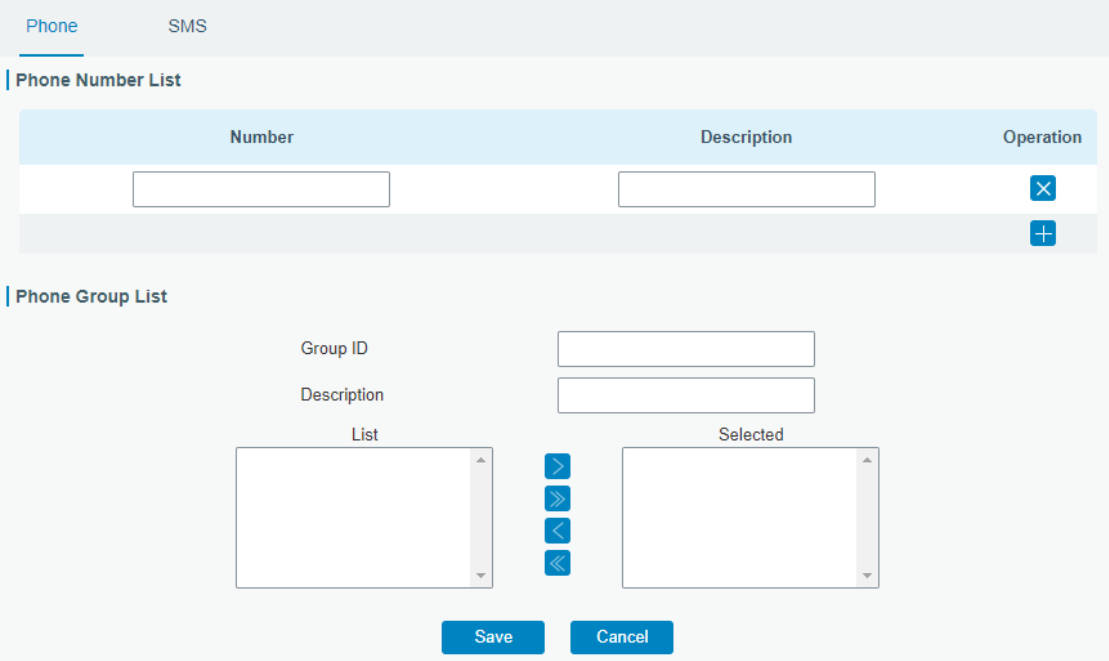
Status Show the status of Micro SD card, such as “Available” or “Not Inserted.”

Storage (Capacity/Available) The total capacity of the Micro SD Card.

Format Format the Micro SD card.

PHONE & SMS

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



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.

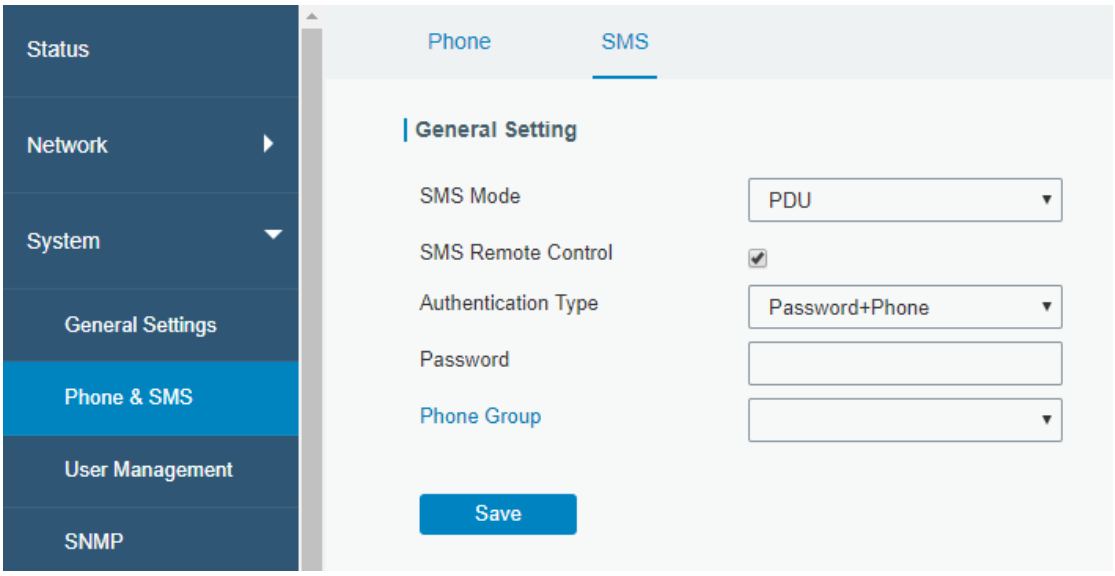
Description The description of the phone group.

List Show the phone list.

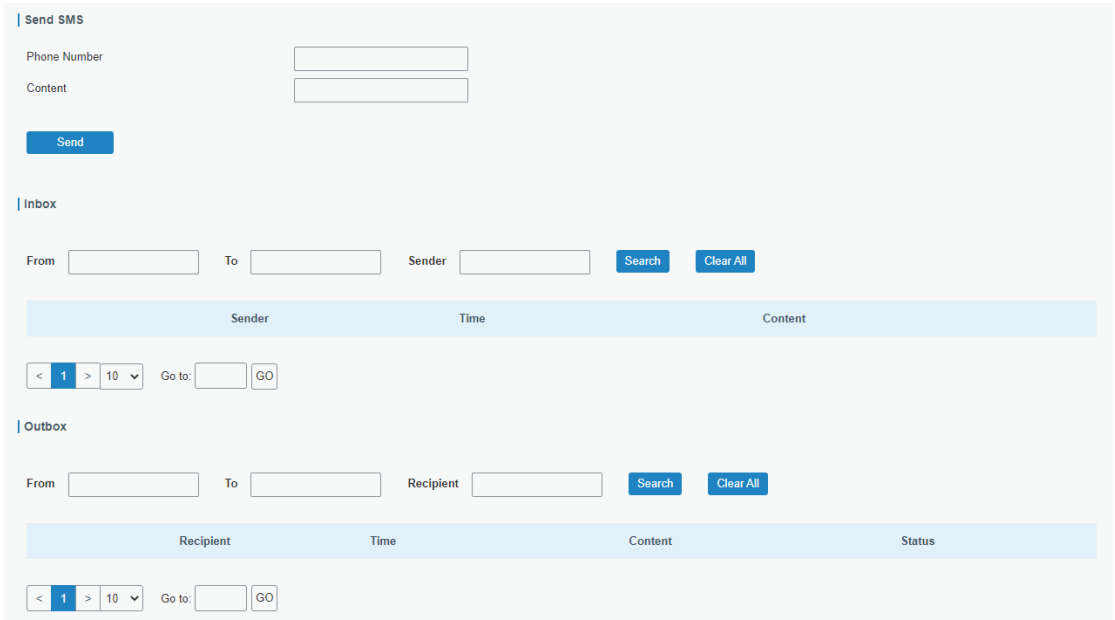
Selected Show the selected phone number.

SMS

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



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.



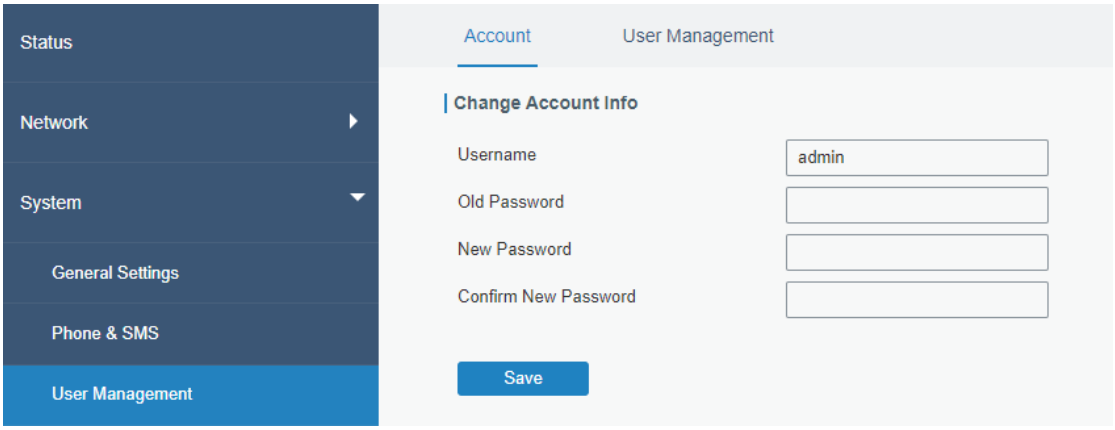
Send SMS
Phone Number Enter the number to receive the SMS.
Content SMS content.

Inbox/Outbox
Sender SMS sender from outside.

Recipient SMS recipient which iSite send to.
From Select the start date.
To Select the end date.
Search Search for SMS record.
Clear All Clear all SMS records in web GUI.

USER MANAGEMENT

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.

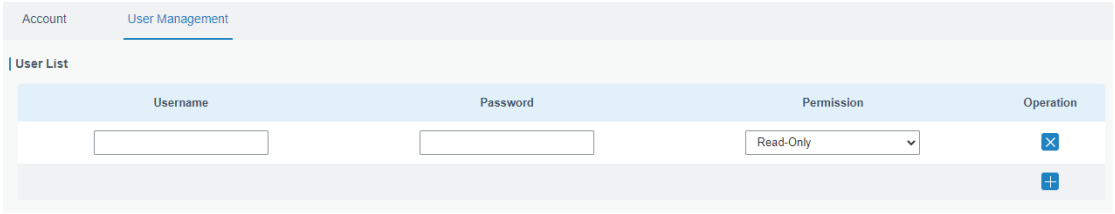


Account

Username Enter a new username. You can use characters such as a-z, 0-9, "_", "-", "$". The first character cannot be a digit.
Old Password Enter the old password.
New Password Enter a new password.
Confirm New Password Enter the new password again.

User Management

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



Username Enter a new username. You can use characters such as a-z, 0-9, "_", "-", "$". The first character cannot be a digit.
Password Set password.
Permission Select user permission from “Read-Only” and “Read-Write.”

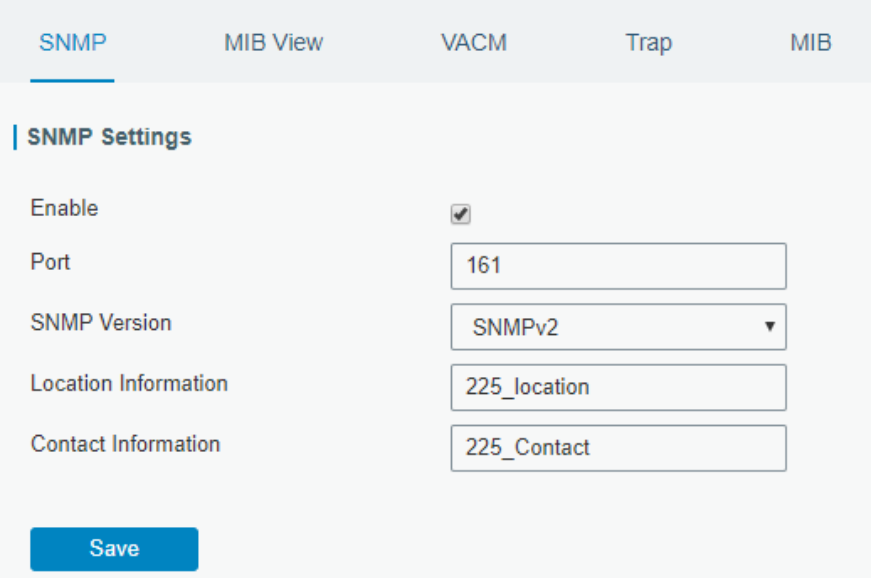
- Read-Only: users can only view the configuration of router in this level.
- Read-Write: users can view and set the configuration of router in this level.

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.

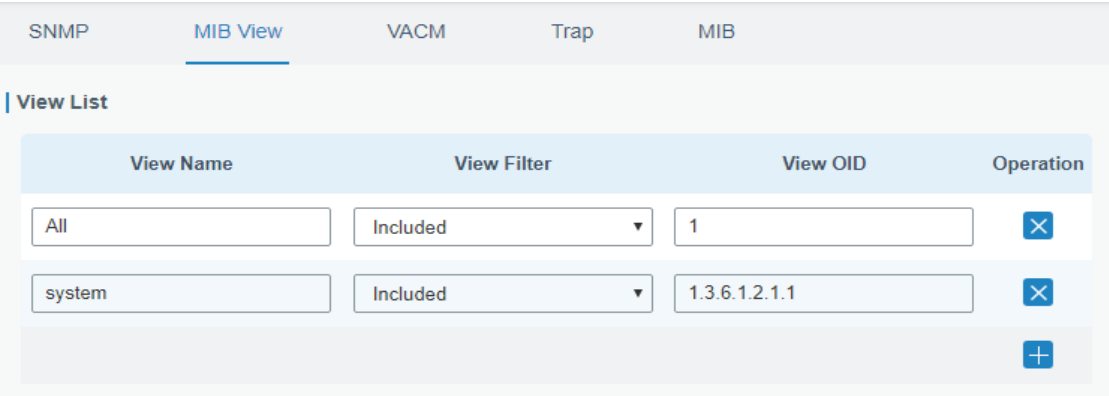
iSite supports SNMPv1, SNMPv2c and SNMPv3 version. SNMPv1 and SNMPv2c employ community name authentication. SNMPv3 employs authentication encryption by username and password.



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

MIB VIEW

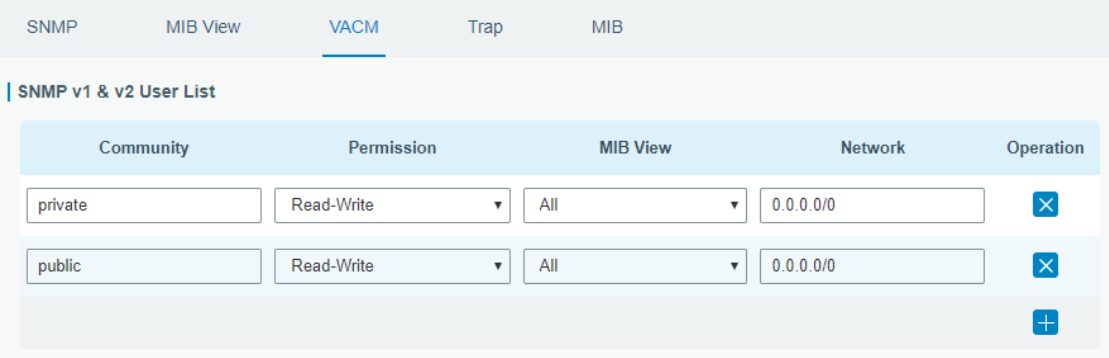
This section explains how to configure MIB view for the objects.



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.

VACM

This section describes how to configure VCAM parameters.



SNMP v1 & v2 User List
Community Set the community name.
Permission Select from "Read-Only" and "Read-Write".
MIB View Select an MIB view to set permissions from the MIB view list.
Network The IP address and bits of the external network accessing the MIB view.
Read-Write The permission of the specified MIB node is read and write.
Read-Only The permission of the specified MIB node is read only.

SNMP v3 User Group
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 List
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 Password The password should be filled in if authentication is "MD5" and "SHA".
Encryption Select from "AES", "DES", and "None".
Encryption Password The password should be filled in if encryption is "AES" and "DES".

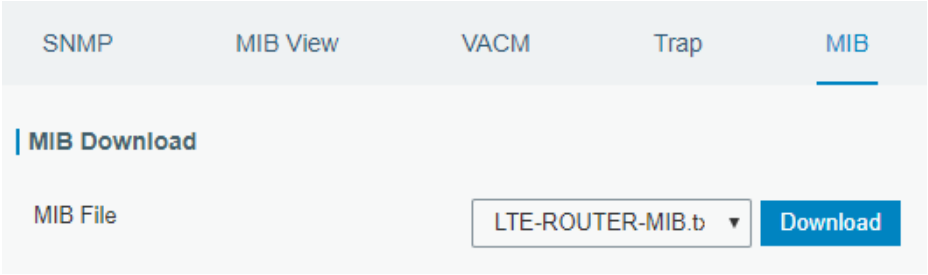
TRAP

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

SNMP Trap
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".

MIB

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



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

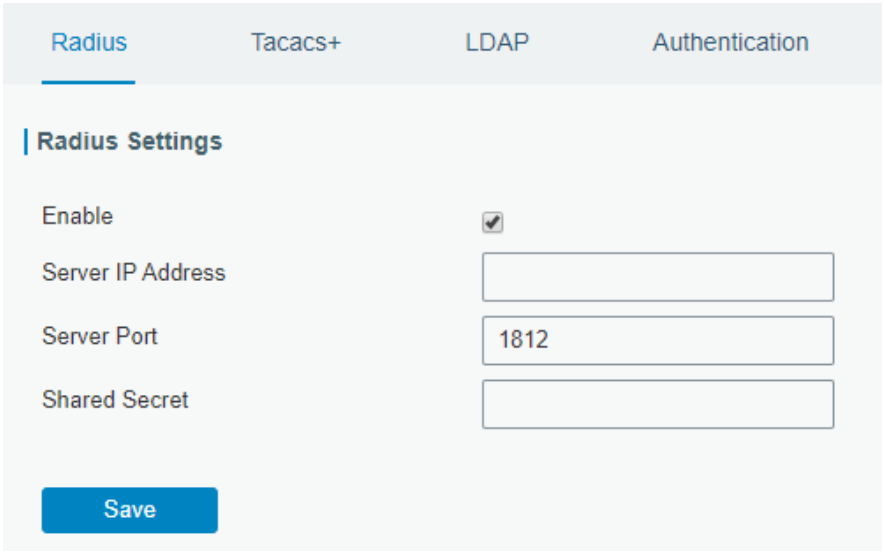
AAA

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.

RADIUS

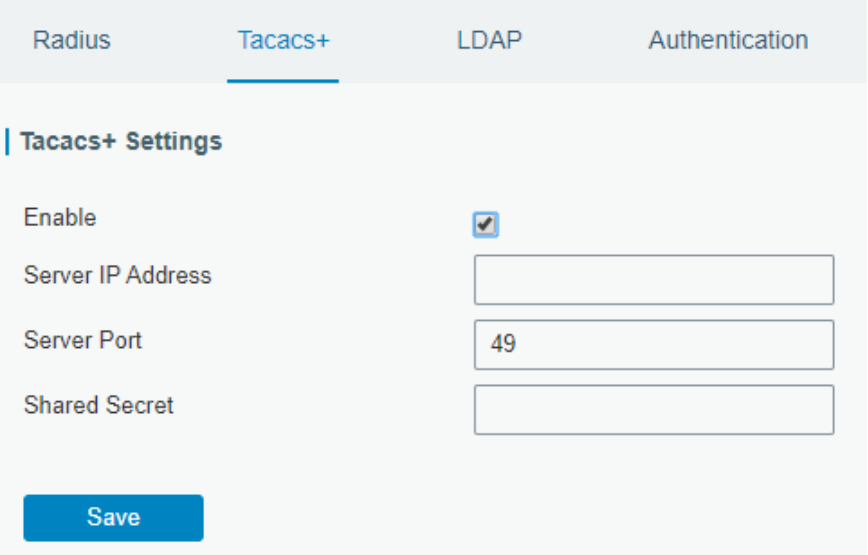
Using UDP for its transport, Radius is generally applied in various network environments with higher requirements of security and permission of remote user access.



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

TACACS+

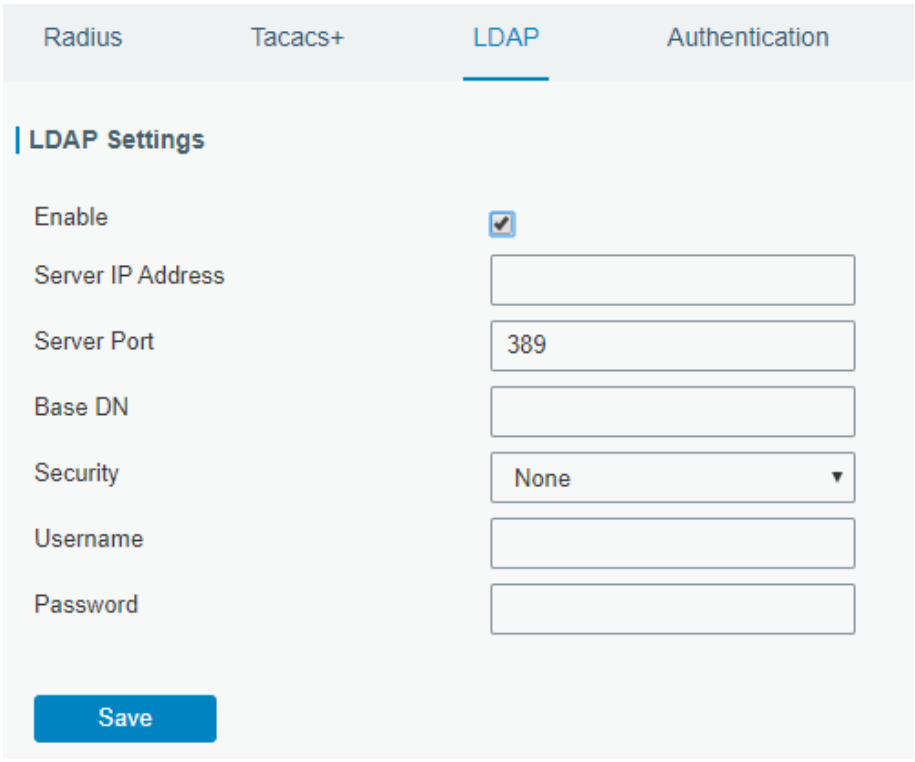
Using TCP for its transport, TACACS+ is mainly used for authentication, authorization and charging of the access users and terminal users by adopting PPP and VPDN.



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.
Key Fill in the key consistent with that of TACACS+ server in order to get connected with TACACS+ server.

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.



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

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.

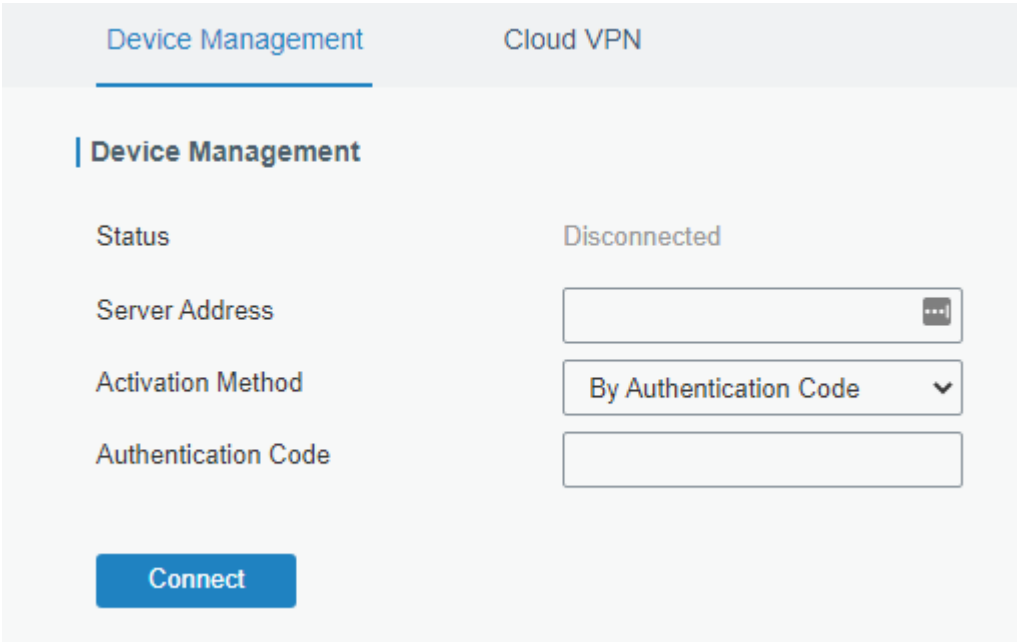
When radius, TACACS+, and local are configured at the same time, the priority level is: 1 >2 >3.

Console Select authentication for Console access.
Web Select authentication for Web access.
Telnet Select authentication for Telnet access.
SSH Select authentication for SSH access.

DEVICE MANAGEMENT

DEVICEHUB

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

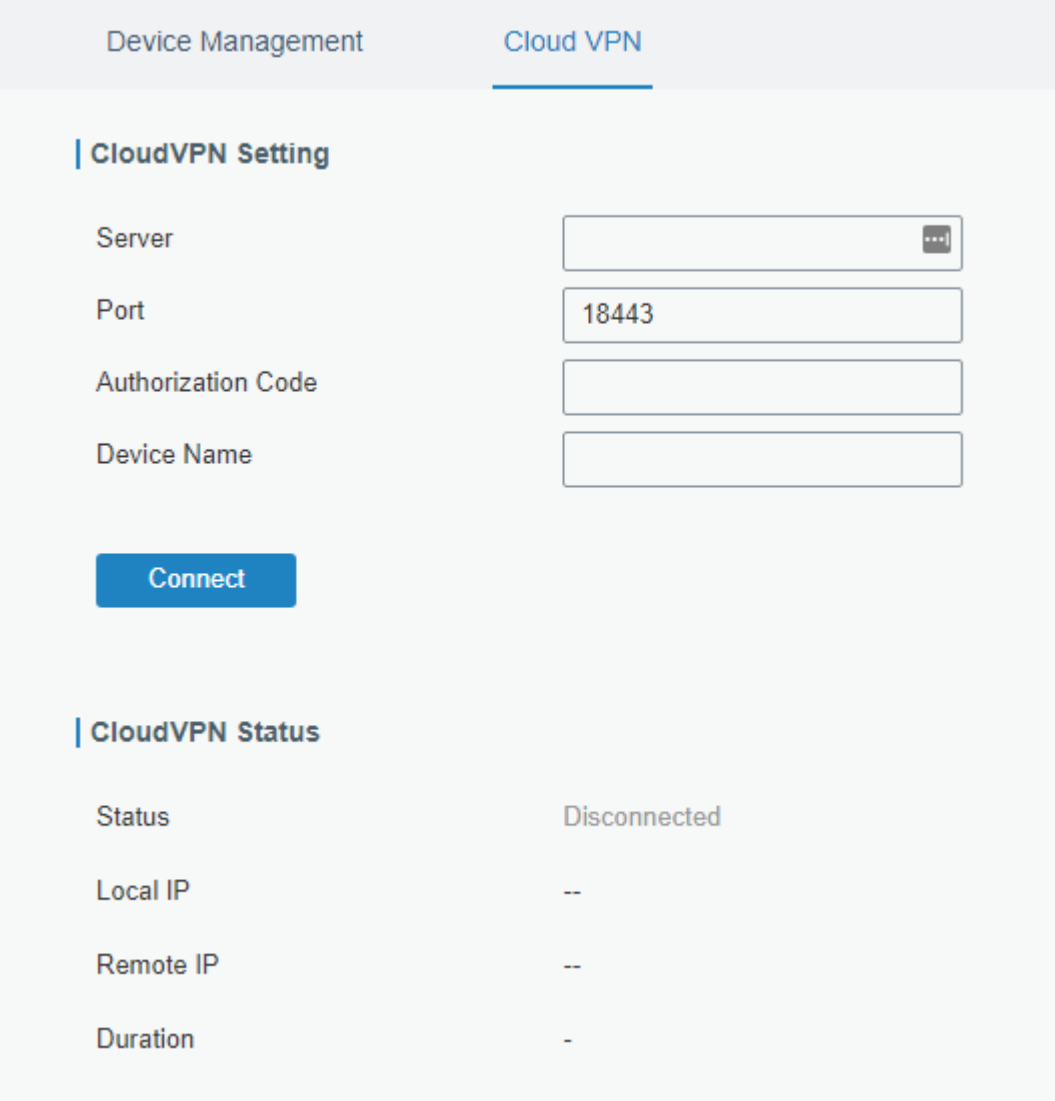


Status Show the connection status between the router and the DeviceHub.
Disconnected Click this button to disconnect the router from the DeviceHub.
Server Address IP address or domain of the device management server.

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.

CLOUD VPN

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



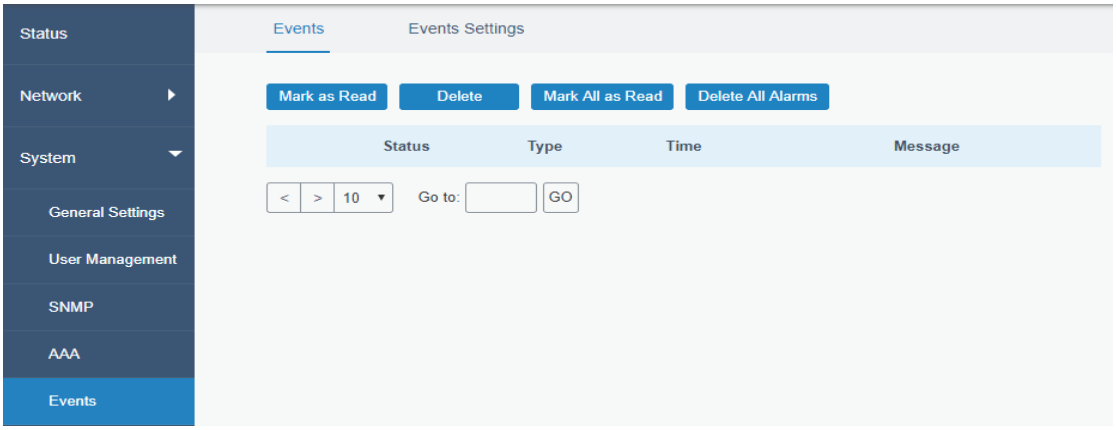
Server Enter the IP address or domain name of Cloud VPN.
Port Enter the HTTPS port number.
Authorization code Enter the authorization code which generated by Cloud VPN.
Device Name Enter the name of the device.

Cloud VPN Status
Status Show the connection information about whether the router is connected to the Cloud VPN.
Local IP Show the virtual IP of the router.

Remote IP Show the virtual IP of the Cloud VPN.
Duration Show the information on how long the router has been connected to the Cloud VPN.

EVENTS

Event feature is capable of sending alerts by Email when certain system events occur. You can view alarm messages on this page.



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

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.

Enable Check to enable "Events Settings".
Phone Group List Select phone group to receive SMS alarm.
Email Group List Select email group to receive alarm.
Record The relevant content of event alarm will be recorded on "Event" page if this option is checked.
Email The relevant content of event alarm will be sent out via email if this option is checked.
Email Setting Click and you will be redirected to the page "Email" to configure email group list.
SMS The relevant content of event alarm will be sent out via SMS if this option is checked.
SMS Setting Click and you will be redirected to the page of "Phone" to configure phone group list.

VPN Up VPN is connected.
VPN Down VPN is disconnected.
WAN Up Ethernet cable is connected to WAN port.
WAN Down Ethernet cable is disconnected to WAN port.
Link Switch Switch to use other interface for Internet access.
Weak Signal The signal level of cellular is low.
Cellular Up Cellular network is connected.
Cellular Down Cellular network is disconnected.
Cellular Data Stats Clear Zero out the data usage of the main SIM card.
Cellular Data Traffic is running out The main SIM card is reaching the data usage limit.
Cellular Data Traffic Over Flow The main SIM card has exceeded the data usage plan.
WLAN Up(AP) The WLAN(AP) is enabled.
WLAN Down(AP) The WLAN(AP) has stopped working.
WLAN Up(Client) The WLAN(Client) is enabled.
WLAN Down(Client) The WLAN(Client) has stopped working.

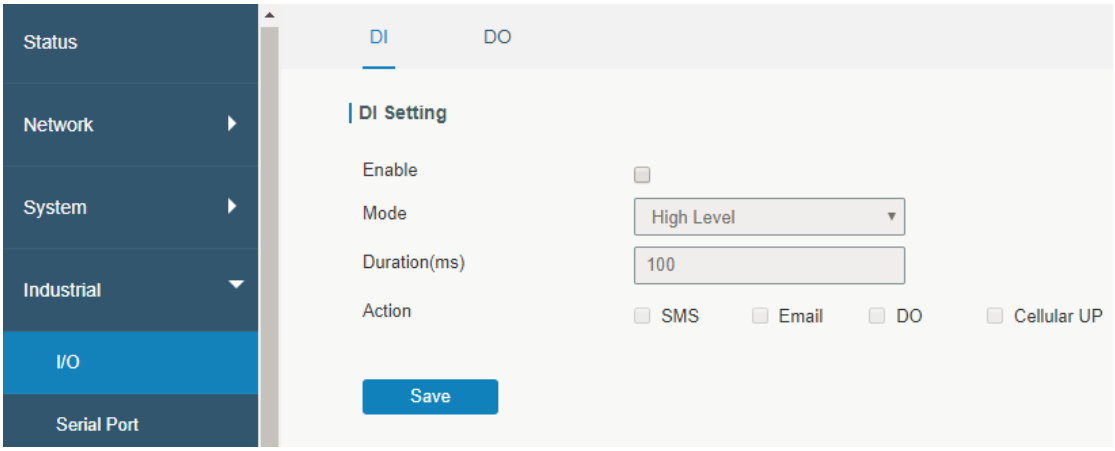
INDUSTRIAL INTERFACE

iSite router is capable of connecting with terminals through industrial interfaces so as to realize wireless communication between terminals and remote data centre.
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 is 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 .

I/O

DI

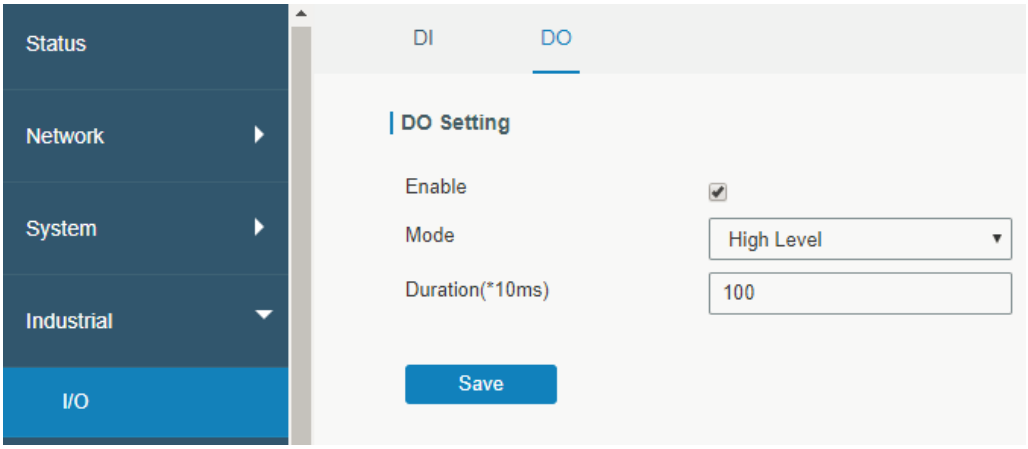
This section explains how to configure monitoring condition on digital input and take certain actions once the condition is reached.



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 pre-set 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 pre-set 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.

DO

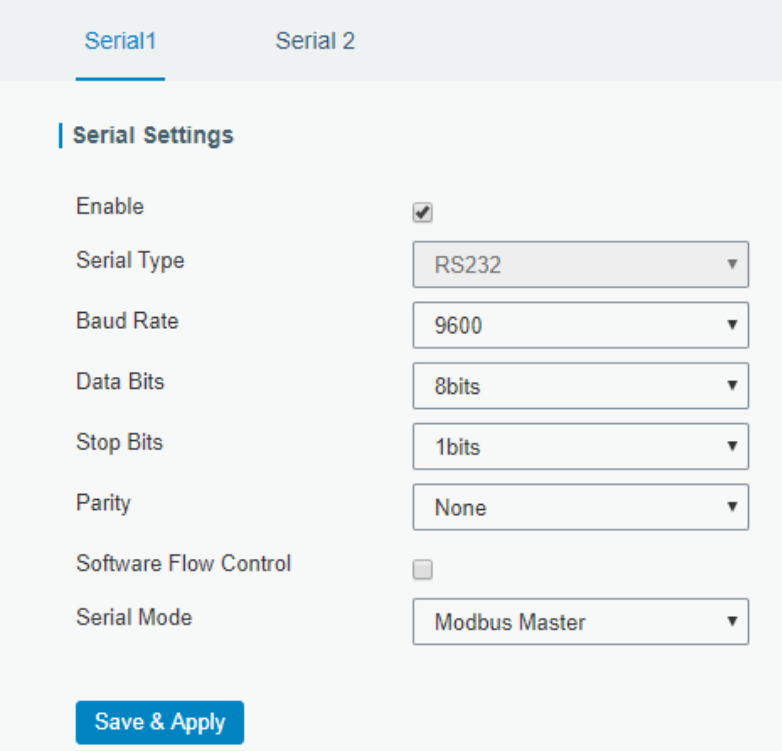
This section describes how to configure digital output mode.



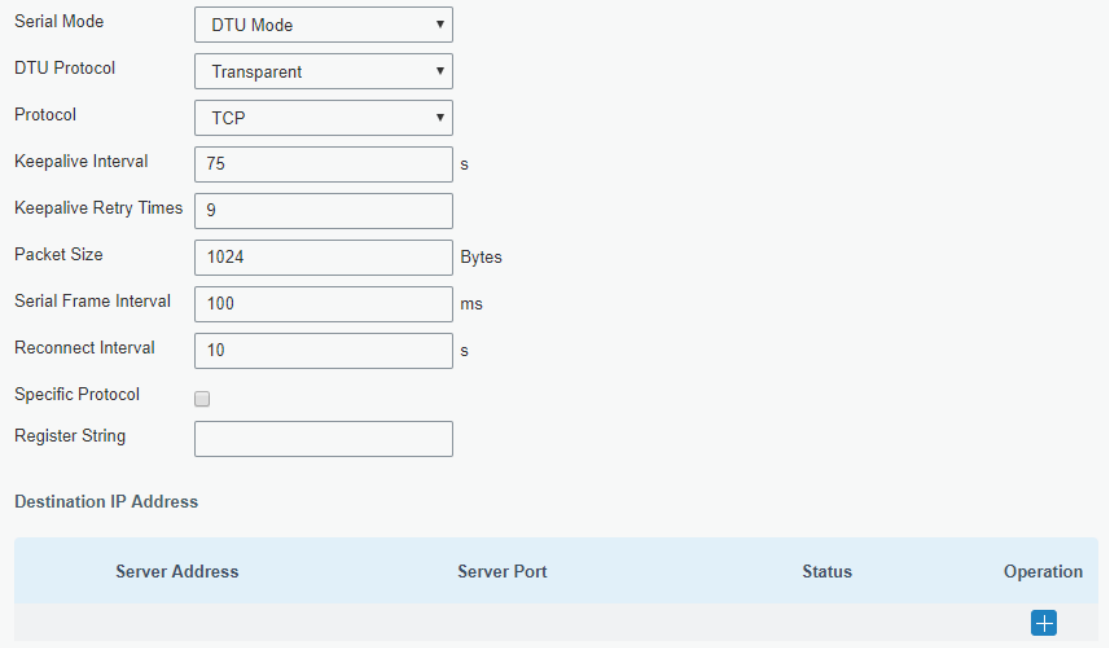
Enable Enable or disable DO.
Mode Select from "High Level", "Low Level", "Pulse" and “Custom” .
Duration (*10ms) Set duration of high/low level on digital output. Range: 1-10000.
Initial Status Select high level or low level as the initial status of the pulse.
Duration of High Level (*10ms) Set the duration 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.

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 centre, so as to achieve two-way communication between serial terminals and remote data centre.



Enable Enable or disable serial port function. Disable
Serial Type Serial Port 1 is a RS232 port and Serial Port 2 is a RS485 port. --
Baud Rate Range is 300-230400. Same with the baud rate of the connected terminal device.
Data Bits Options are “8” and “7”. Same with the data bits of the connected terminal device.
Stop Bits Options are “1” and “2”. Same with the stop bits of the connected terminal device.
Parity Options are “None,” “Odd” and “Even.” Same with the parity of the connected terminal device.
Software Flow Control Enable or disable software flow control.
Serial Mode Select work mode of the serial port. Options are "DTU Mode" , “Modbus Master,” “Modbus Slave” and "GPS".
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.



DTU Mode

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.

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.

Keepalive Retry Times When TCP heartbeat times out, router will resend heartbeat. After it reaches the pre-set retry times, TCP connection will be re-established. The retry times range is 1-16.

Packet Size Set the size of the serial data frame. Packet will be sent out when pre-set frame size is reached. The size range is 1-1024. The unit is byte.

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 pre-set packet size, even though it is within the serial frame interval.

Transparent

Protocol Select "TCP" or "UDP" protocol.

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 pre-set 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 pre-set frame size is reached. The range is 1-1024. The unit is byte.
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 pre-set packet size, even though it is within the serial frame interval.

Reconnect Interval After connection failure, router will reconnect to the server at the pre-set interval, in seconds. The range is 10-60.
Specific Protocol 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.
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.
Server Address Fill in the TCP or UDP server address (IP/domain name).
Server Port Fill in the TCP or UDP server port. Range: 1-65535.
Status Show the connection status between the router and the server.

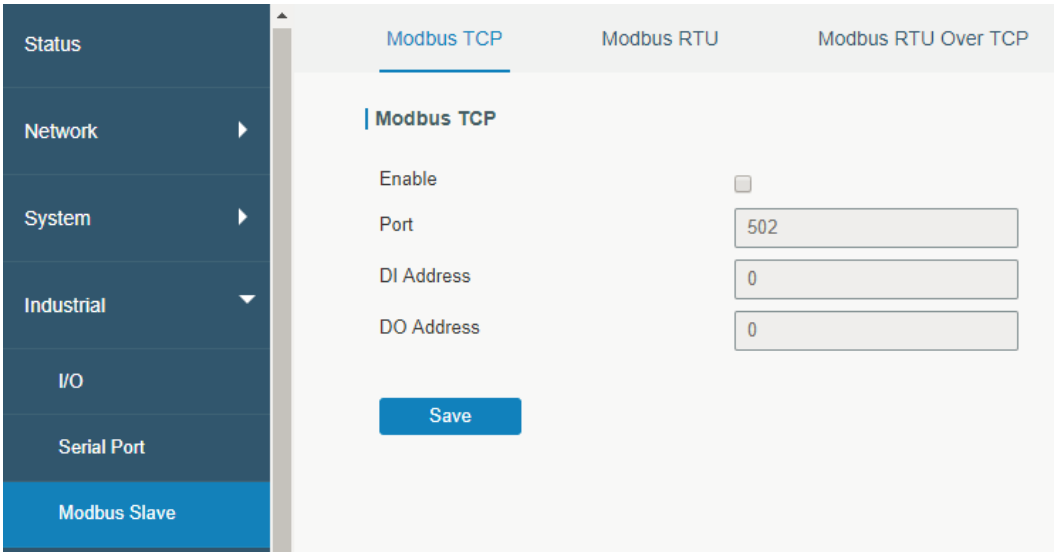
Modbus
Local Port Set the router listening port. Range: 1-65535.
Maximum TCP Clients Specify the maximum number of TCP clients allowed to connect the router which function as a TCP server.
Connection Timeout If the TCP server does not receive any data from the slave device within the connection timeout period, the TCP connection will be broken.
Reading Interval Set the interval for reading remote channels. When a read cycle ends, 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 is determined that the command has timed out.
Maximum Retries Set the maximum retry times after it fails to read.

MODBUS SLAVE

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

MODBUS TCP

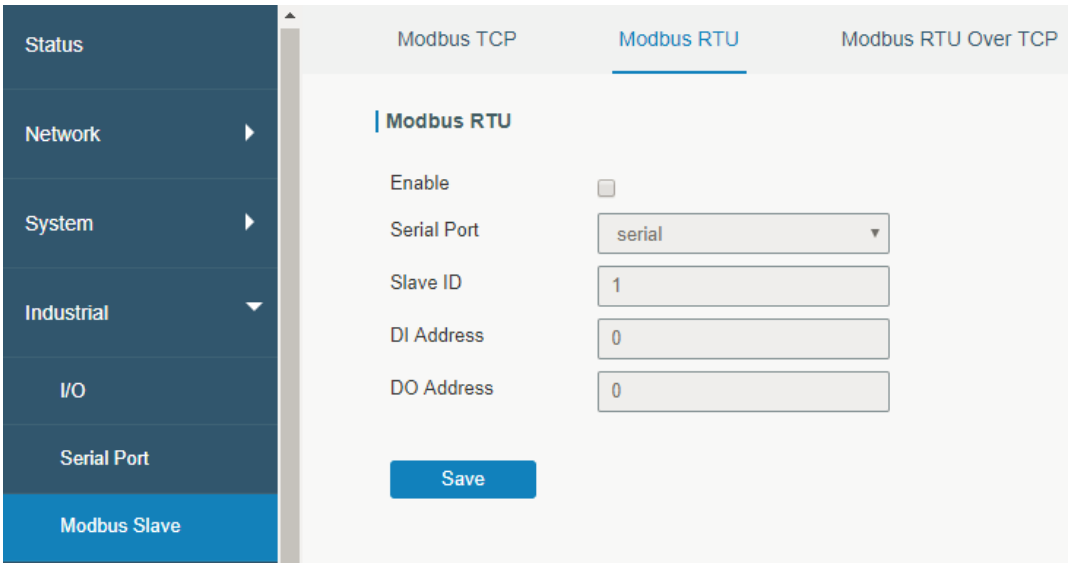
You can define the address of the DI and DO ports so as to poll DI's status and control DO's status via Modbus TCP protocol.



Enable Enable/disable Modbus TCP.
Port Set the router listening port. Range: 1-65535.
DI Address Define the address of DI, range: 0-255.
DO Address Define the address of DO, range: 0, 2-255.

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.

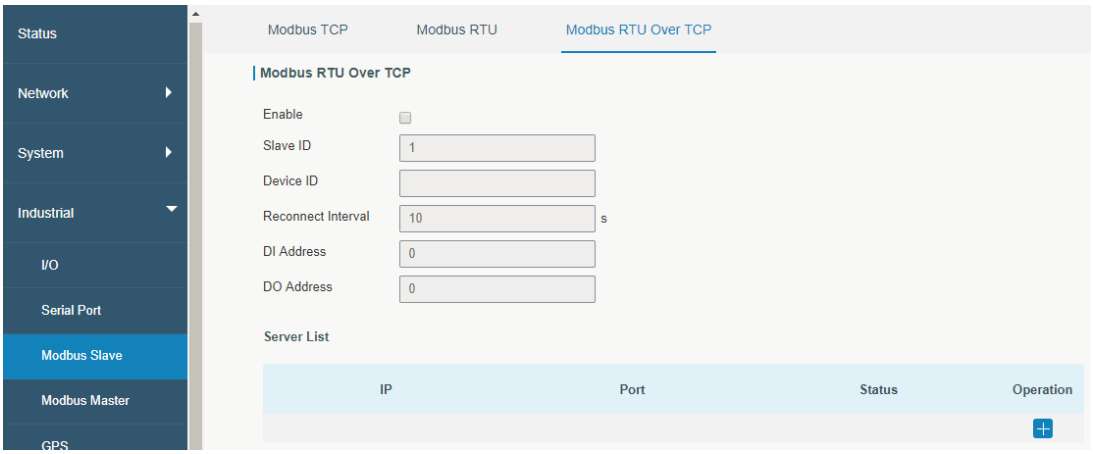


Enable Enable/disable Modbus RTU.
Serial Port Select the corresponding serial port.
Slave ID Set slave ID is used for distinguishing different devices on the same link.
DI Address Define the address of DI, range: 0-255.

DO Address Define the address of DO, range: 0, 2-255.

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.



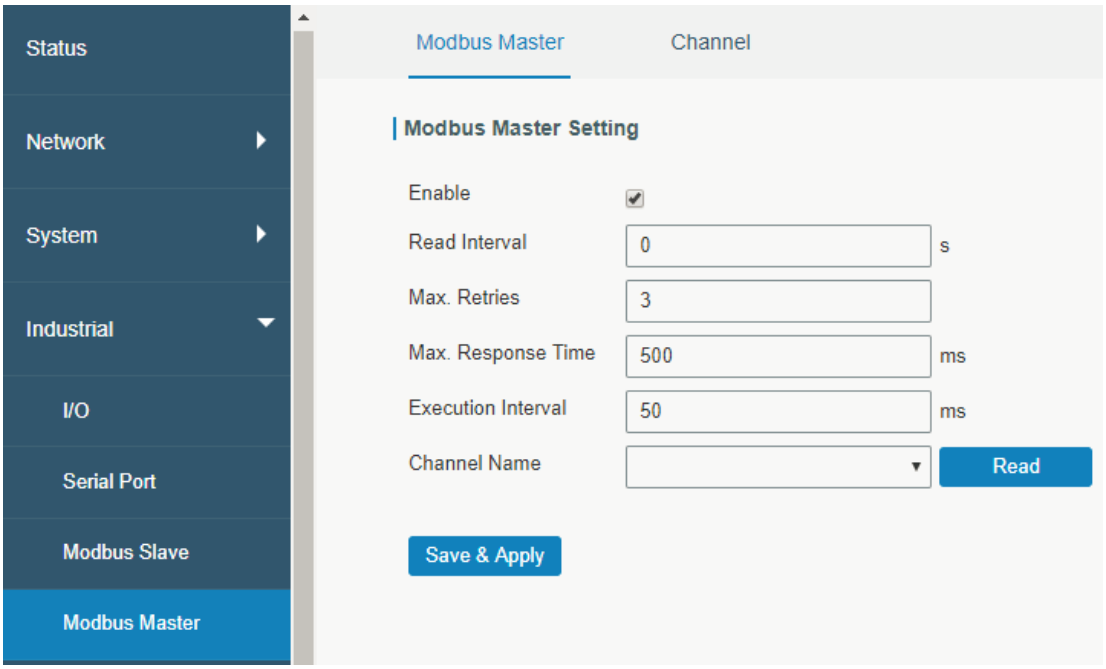
Enable Enable/disable Modbus RTU over TCP function.
Slave ID Set slave ID is used for distinguishing different devices on the same link.
Device ID Set device ID. The server will get the device ID to the server for identifying identity so that the server can manage multiple devices.
Reconnection Interval The reconnection interval when the device and the server fails to establish connection or disconnected.
DI Address Define the address of DI, range: 0-255.
DO Address Define the address of DO, range: 0, 2-255.

Server List
IP Enter the IP address of the server.
Port Enter the port of the server. Range: 0-65535.
Status Show the connection status between the router and the server.
Table 3-4-3-3 Modbus RTU Over TCP Parameters

MODBUS MASTER

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

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



Enable Enable/disable Modbus master.

Read Interval/s Set the interval for reading remote channels. When the read cycle ends, the commands which have not 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.

Max. Retries Set the maximum retry times after it fails to read, range: 0-5. 3

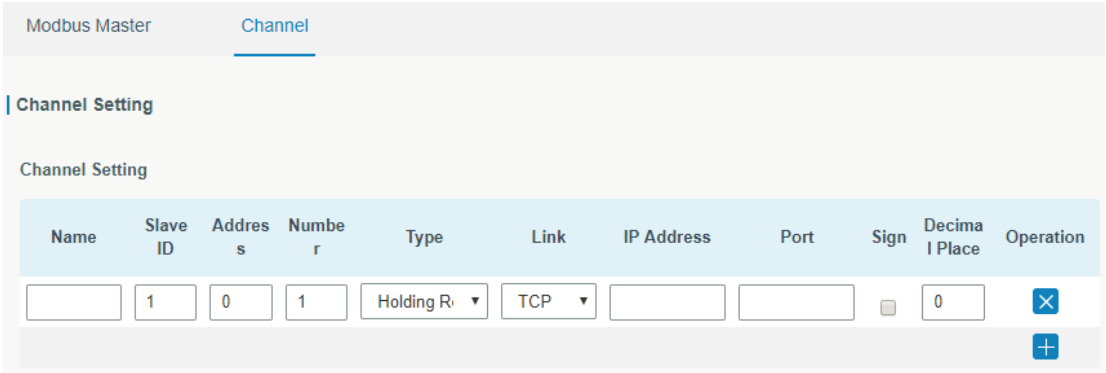
Max. Response Time/ms Set the maximum response time that the router waits for the response to the command. If the device does not get a response after the maximum response time, it is determined that the command has timed out. Range: 10-1000.

Execution Interval/ms The execution interval between each command. Range: 10-1000.

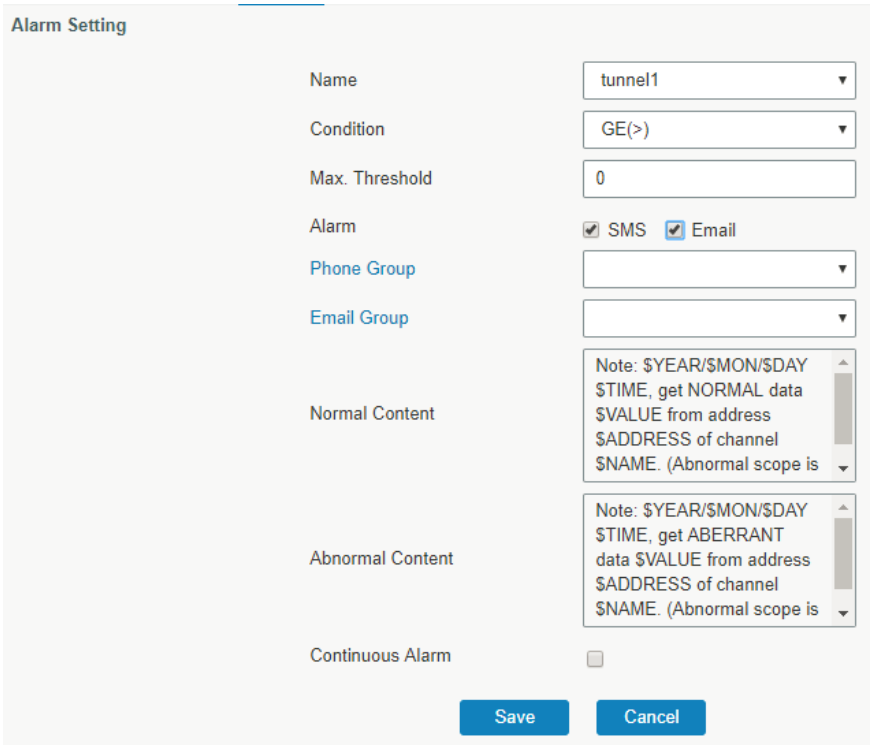
Channel Name Select a readable channel form the channel list.

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.



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.
Type 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.

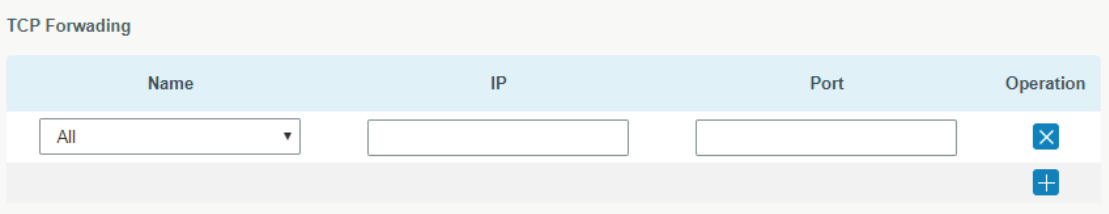


Alarm Setting

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

Abnormal Content When the actual value exceeds the pre-set threshold, the router will automatically trigger the alarm and send the pre-set 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.



TCP Forwarding

Name The name of Modbus Master's channel.

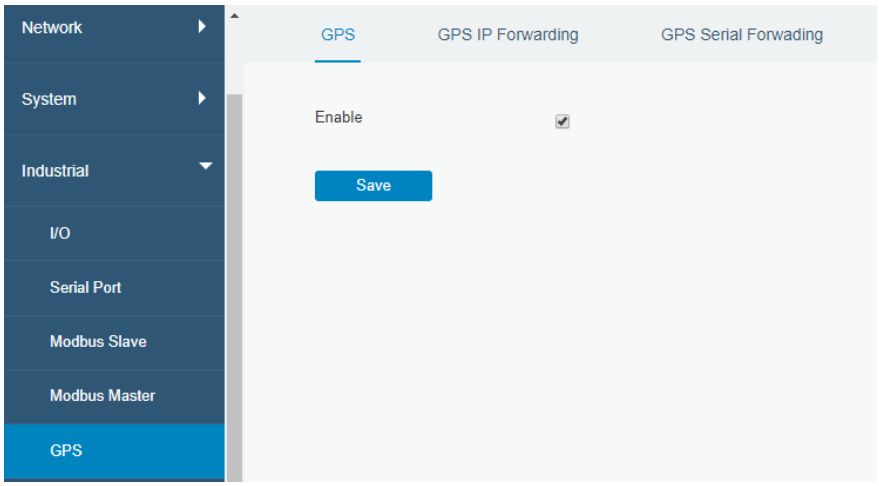
IP The IP address of the server which the packets are forwarded to.

Port The port of the server's which the packets are forwarded to.

GPS

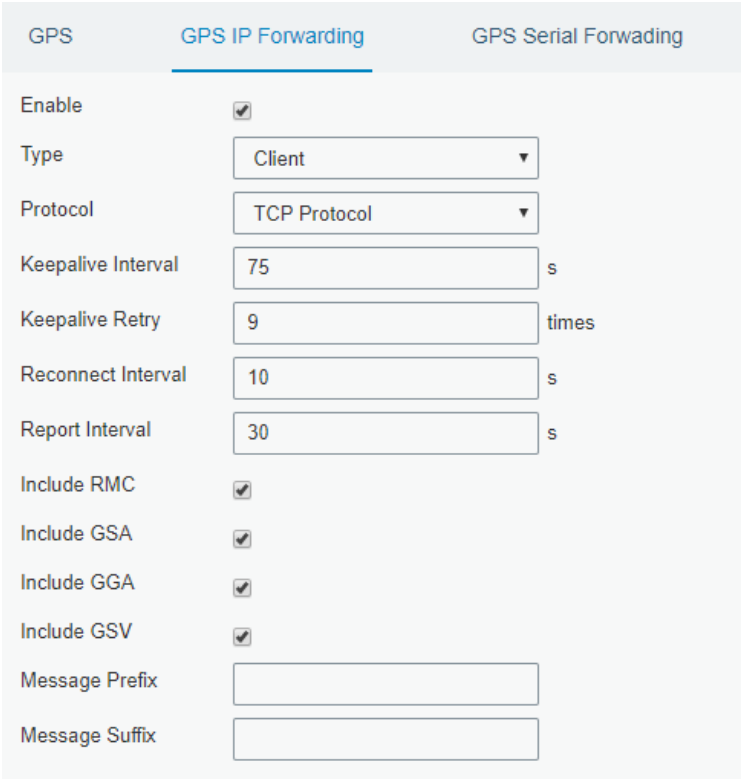
This section gives you a detailed introduction to GPS settings, including GPS IP forwarding and GPS serial forwarding.

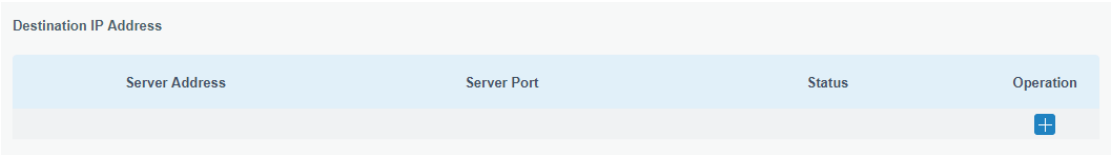
When you want to receive GPS data, you should enable GPS function on this page.



GPS IP FORWARDING

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





Enable Forward the GPS data to the client or server.
Type Select connection type of the router. The options are "Client" and "Server".
Protocol Select protocol of data transmission. The options are "TCP" and "UDP".
Keepalive Interval After it is 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.
Keepalive Retry When TCP heartbeat times out, the router will resend heartbeat. After it reaches the pre-set retry times, router will reconnect to TCP server. The range is 1-16.
Local Port Set the router listening port. Range: 1-65535.
Reconnect Interval After connection failure, router will reconnect to the server at the pre-set interval, in seconds. The range is 10-60.
Report Interval Router will send GPS data to the server/client at the pre-set interval, in seconds. The range is 1-60.
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.
Message Suffix Add a suffix to the GPS data.

Destination IP Address

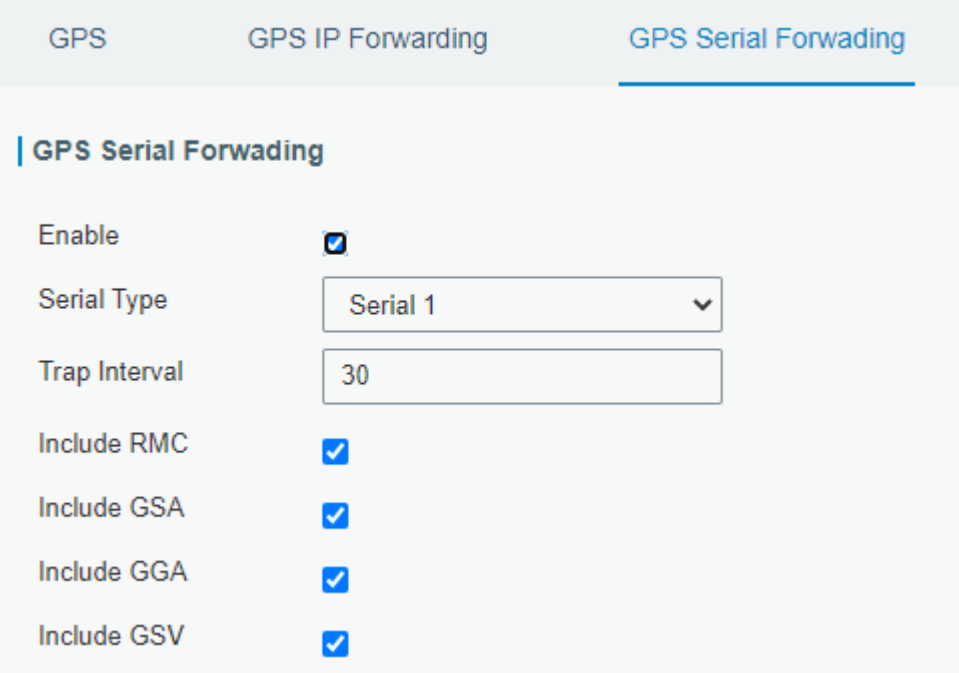
Server Address Fill in the server address to receive GPS data (IP/domain name). --

Server Port Fill in the port to receive GPS data. Range: 1-65535. --

Status Show the connection status between the router and the server. --

GPS SERIAL FORWARDING

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



Enable Forward the GPS data to the pre-set serial port.

Serial Type Select the serial port to receive GPS data.

Report Interval Router will forward the GPS data to the serial port at the pre-set interval, in seconds. The range is 1-60.

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.

MAINTENANCE

This section describes system maintenance tools and management.

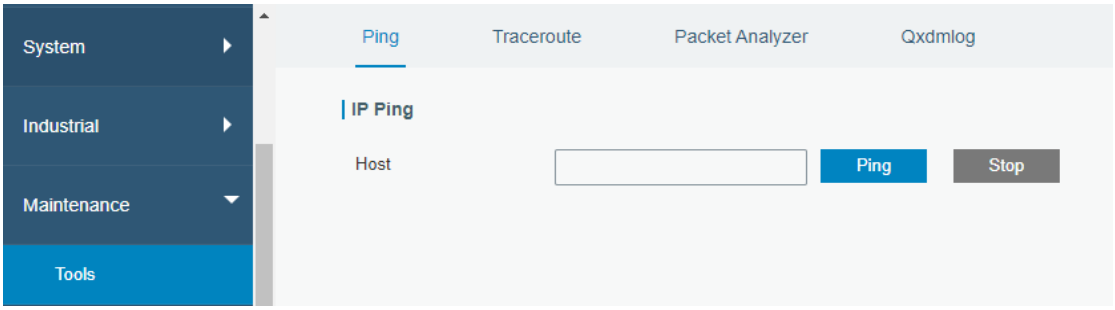
Tools

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

Ping

Ping tool is engineered to ping outer network.

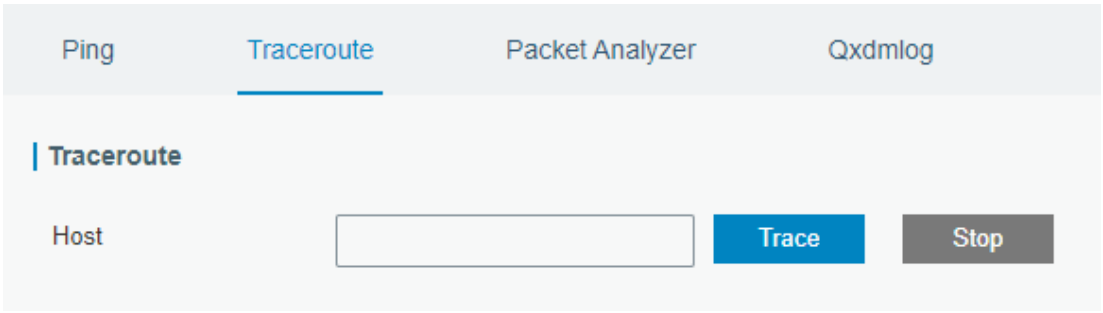
PING



Host Ping outer network from the router.

TRACEROUTE

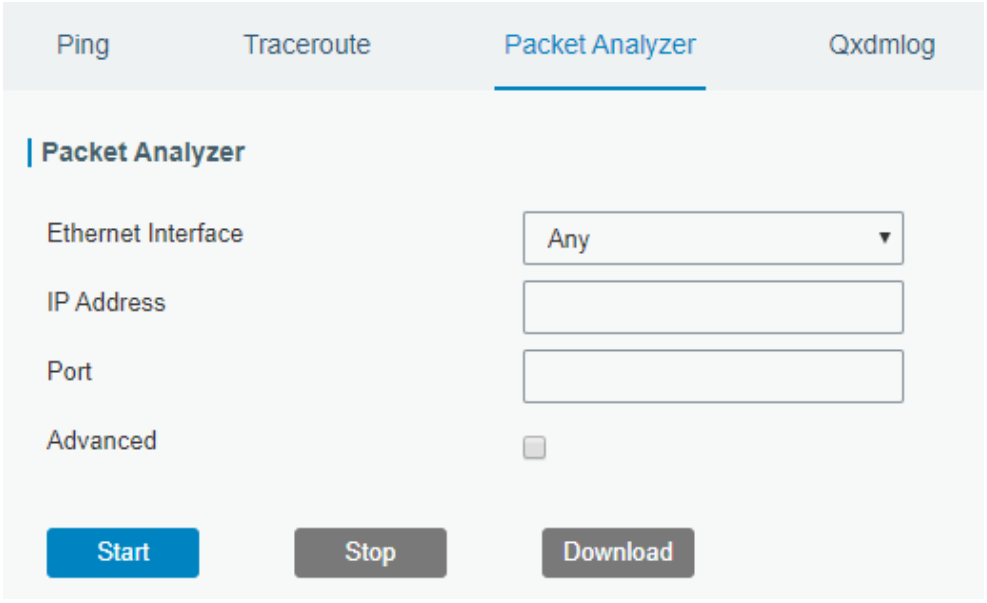
Traceroute tool is used for troubleshooting network routing failures.



Host Address of the destination host to be detected.

PACKET ANALYZER

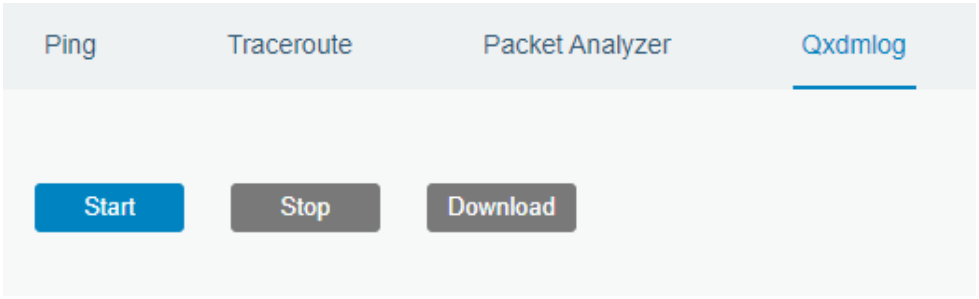
Packet Analyzer is used for capturing the packet of different interfaces.



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.

QXDMLOG

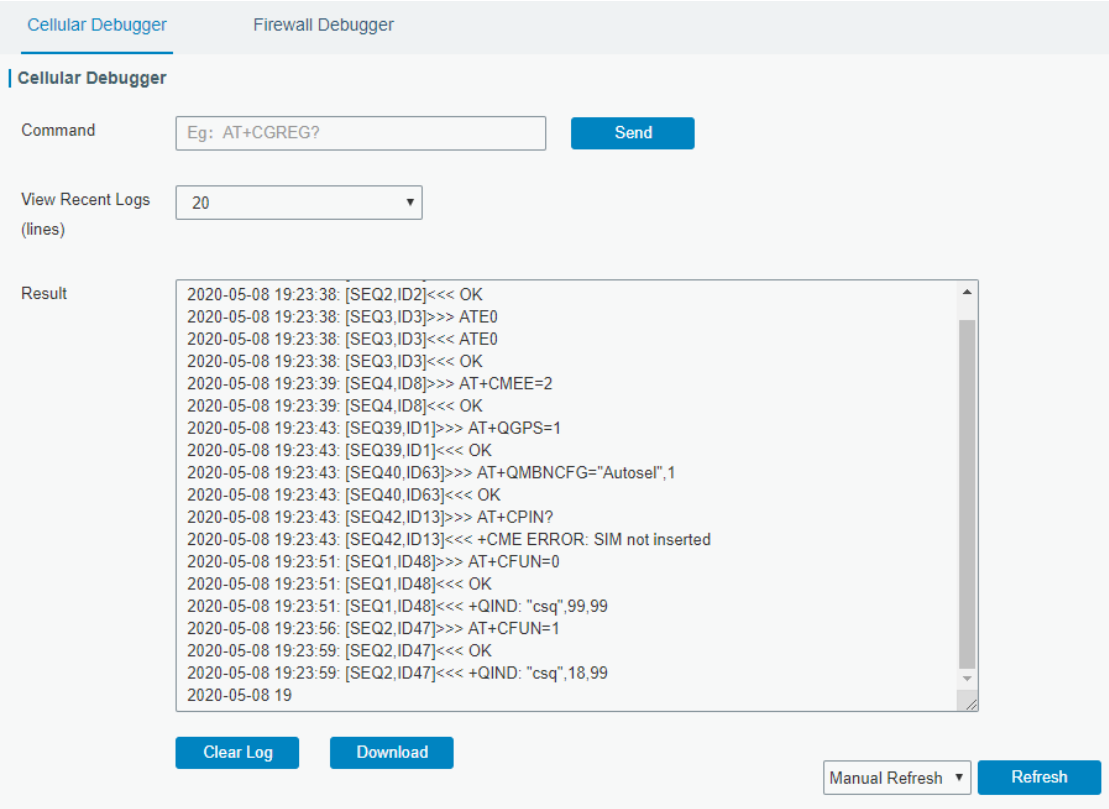
This section allow collecting diagnostic logs via QXDM tool.



DEBUGGER

CELLULAR DEBUGGER

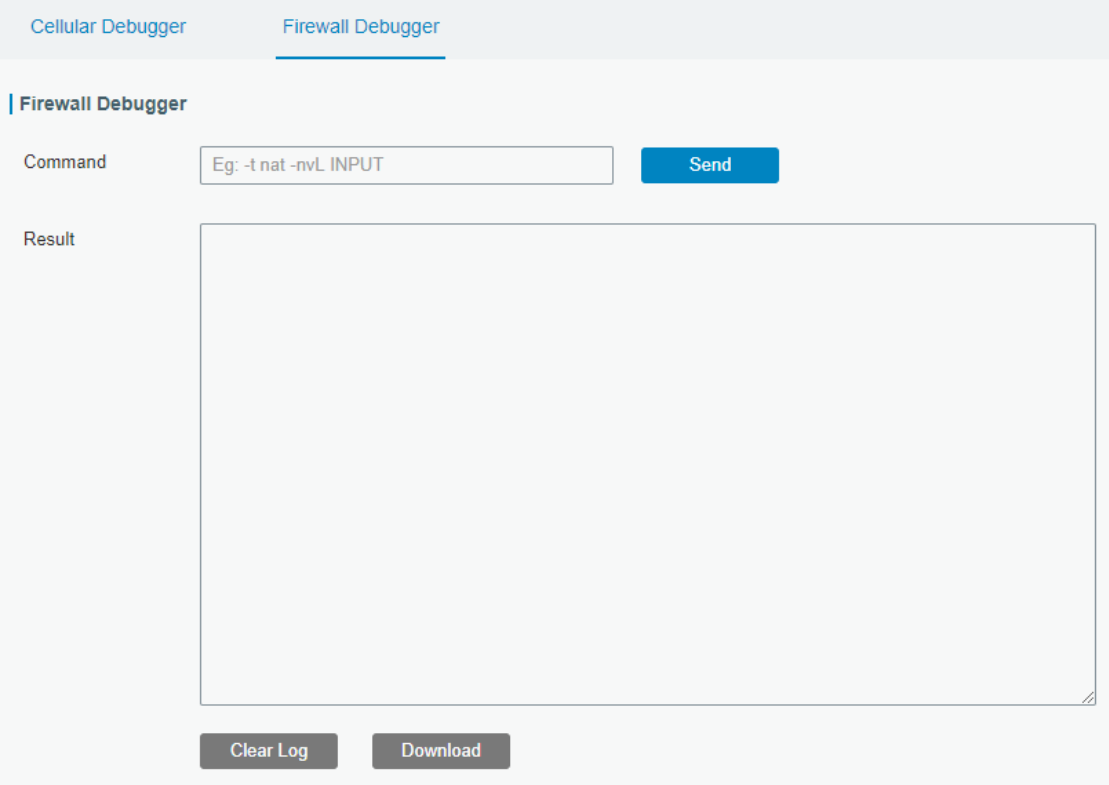
This section explains how to send AT commands to router and check cellular debug information.



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.

FIREWALL DEBUGGER

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



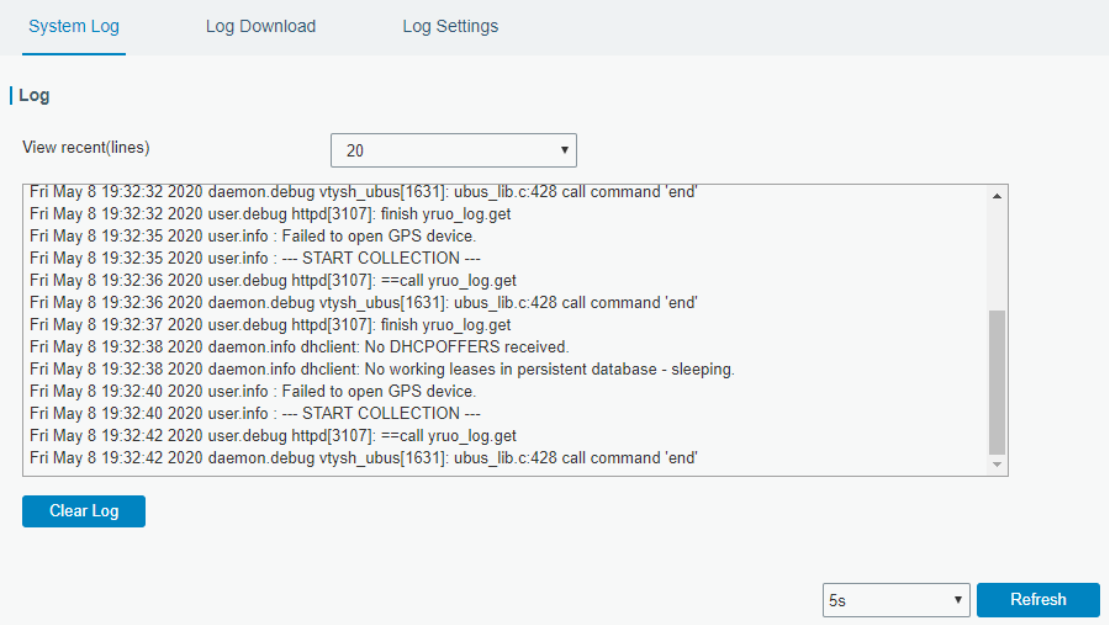
Command Enter the AT command that you want to send to firewall module.
Result Show the response result from firewall module.

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.

SYSTEM LOG

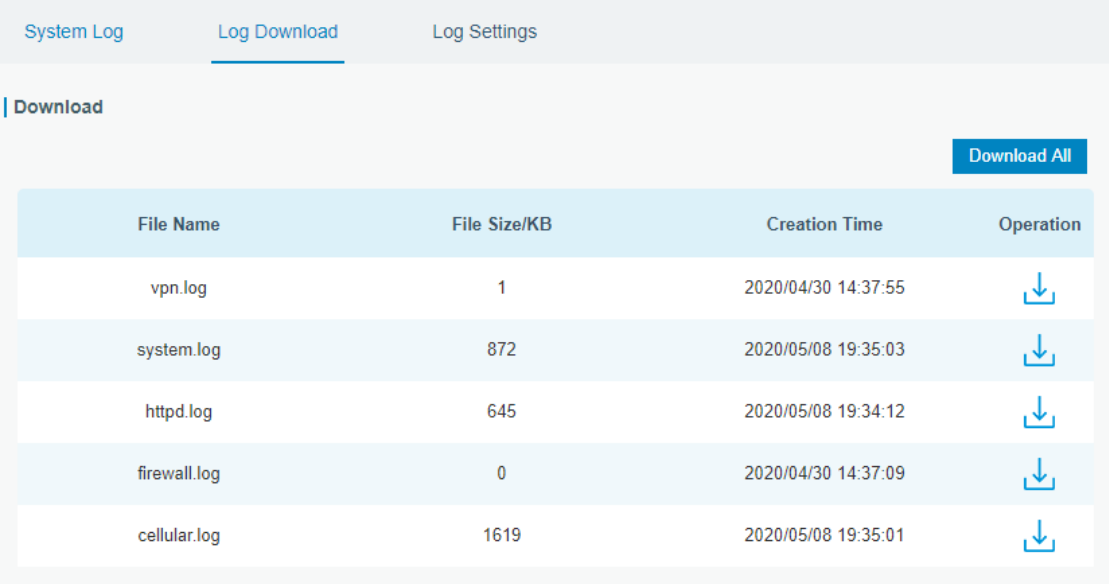
This section describes how to view the recent log on web.



View recent (lines) View the specified lines of system log.
Clear Log Clear the current system log.

LOG DOWNLOAD

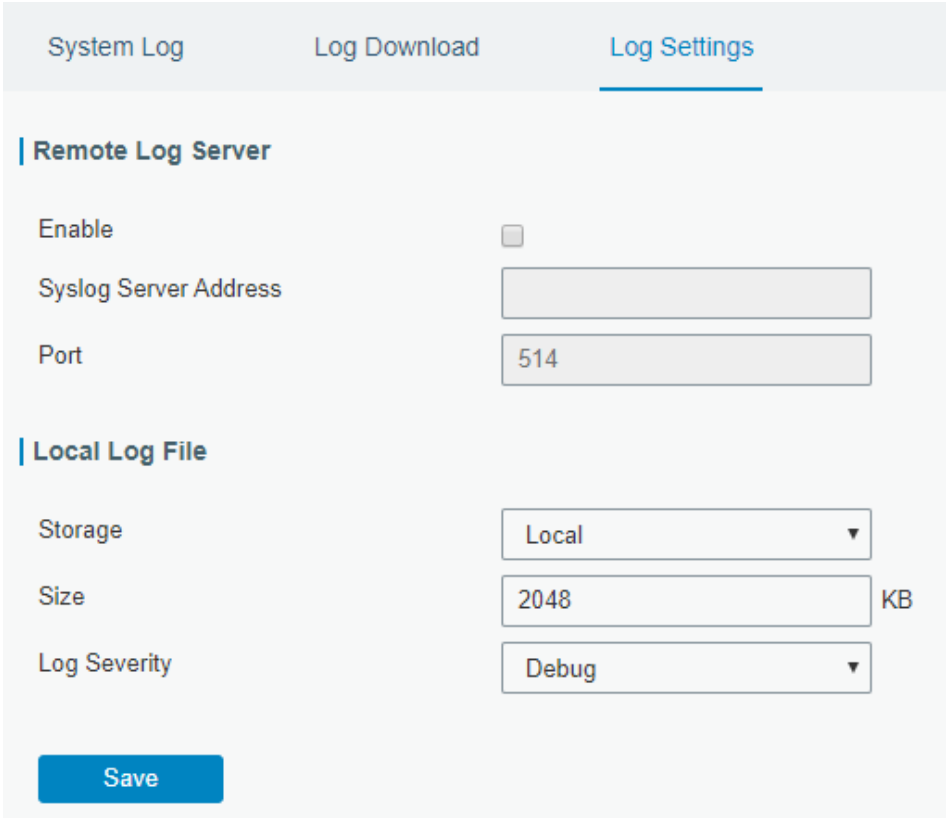
This section describes how to download log files.



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.

LOG SETTINGS

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



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

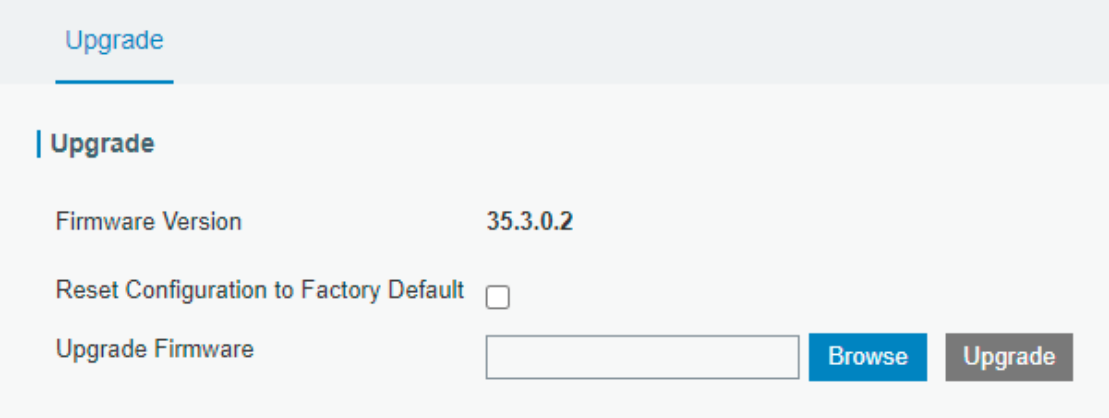
Storage User can store the log file in memory or TF card.

Size Set the size of the log file to be stored.

Log Severity The list of severities follows the syslog protocol.

UPGRADE

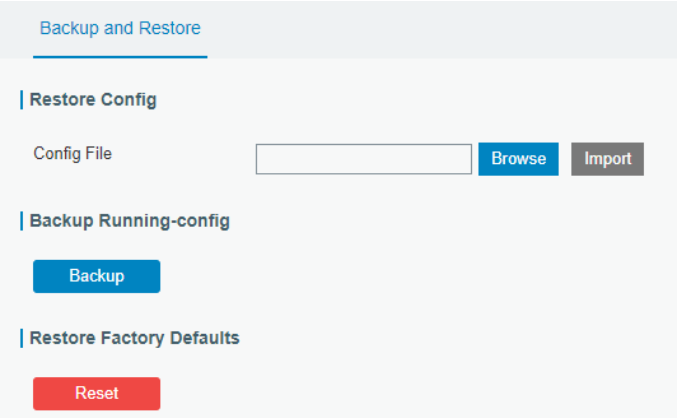
This section describes how to upgrade the router firmware via web. Generally you do not need to do the firmware upgrade.
Note: any operation on web page is not allowed during firmware upgrade, otherwise the upgrade will be interrupted, or even the device will break down.



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.

BACKUP AND RESTORE

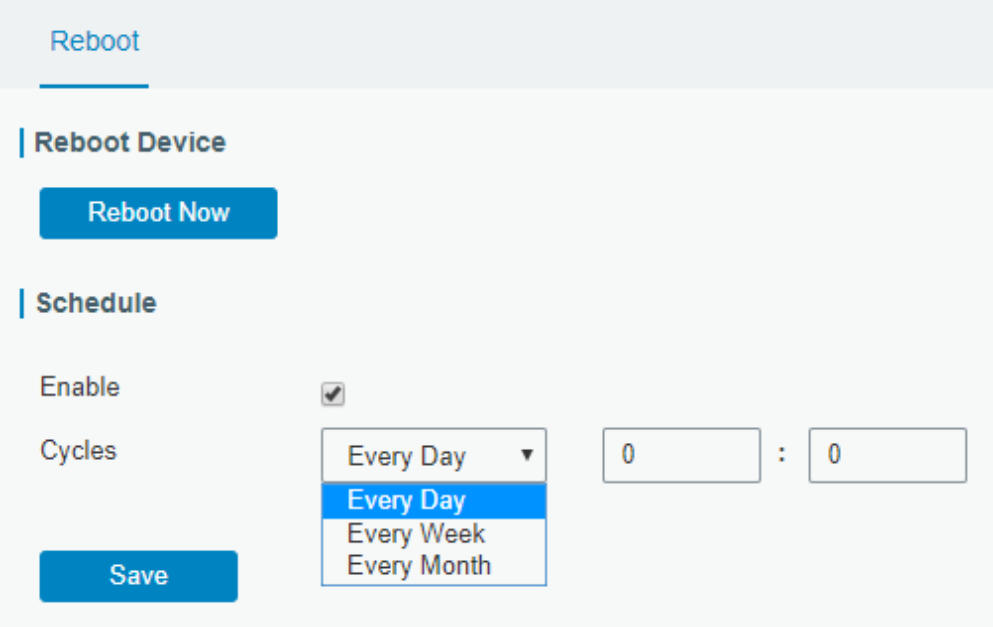
This section explains how to create a complete backup of the system configurations to a file, restore the config file to the router and reset to factory defaults.



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.

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 Now Reboot the router immediately.

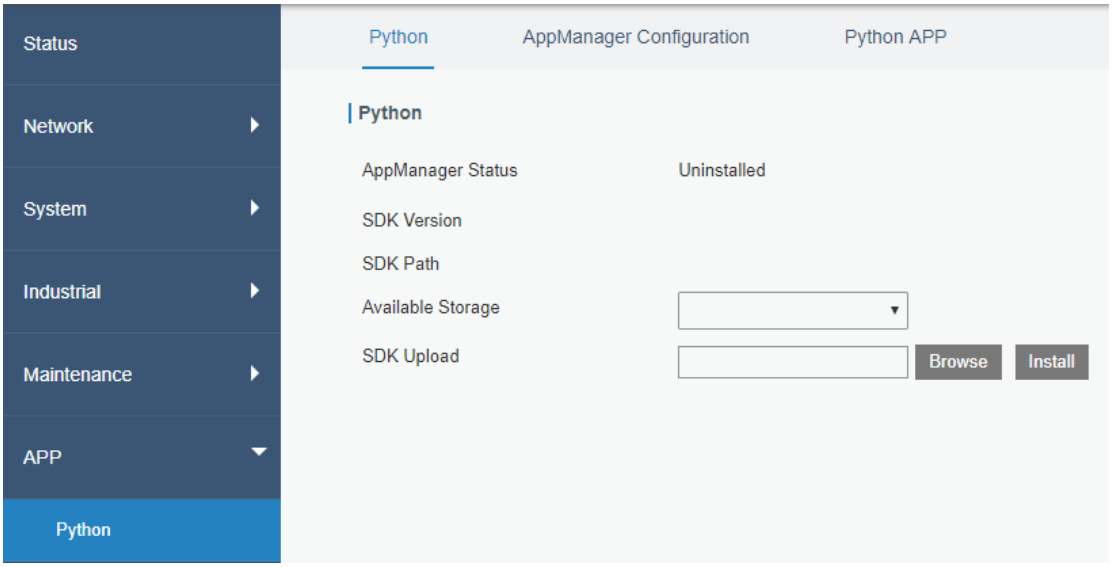
Schedule
Enable Reboot the router at a scheduled frequency.
Cycles Select the date and time to execute the schedule.

APP

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 is 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.

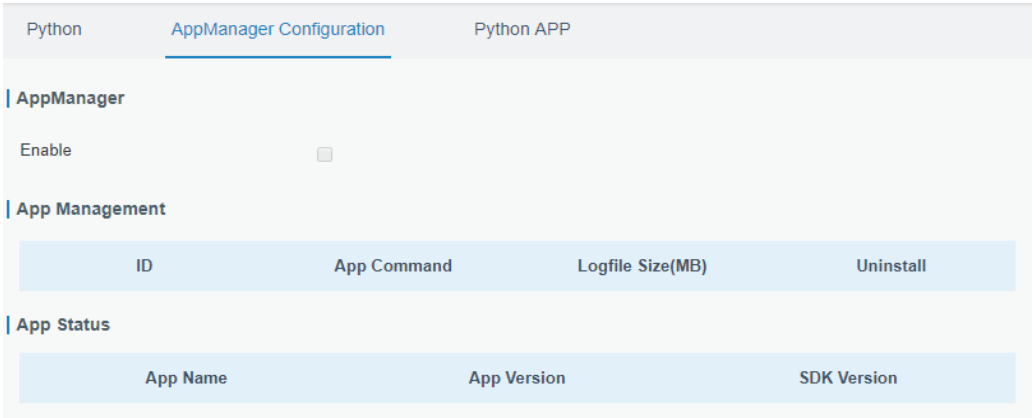
PYTHON

Micro SD card must be installed for Python App.



AppManager Status Show AppManager's running status, like "Uninstalled", "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.

APP MANAGER CONFIGURATION



Enable After enabling Python AppManager, user can click "View" button on the "Python" webpage to view the application status managed by AppManager.

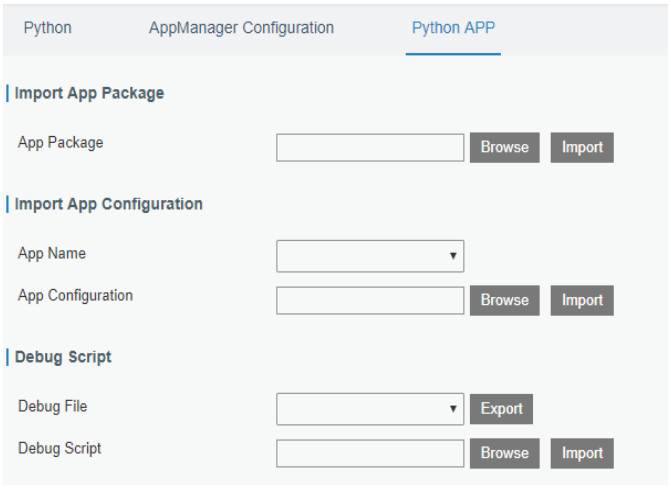
App Management

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.

PYTHON APP



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.

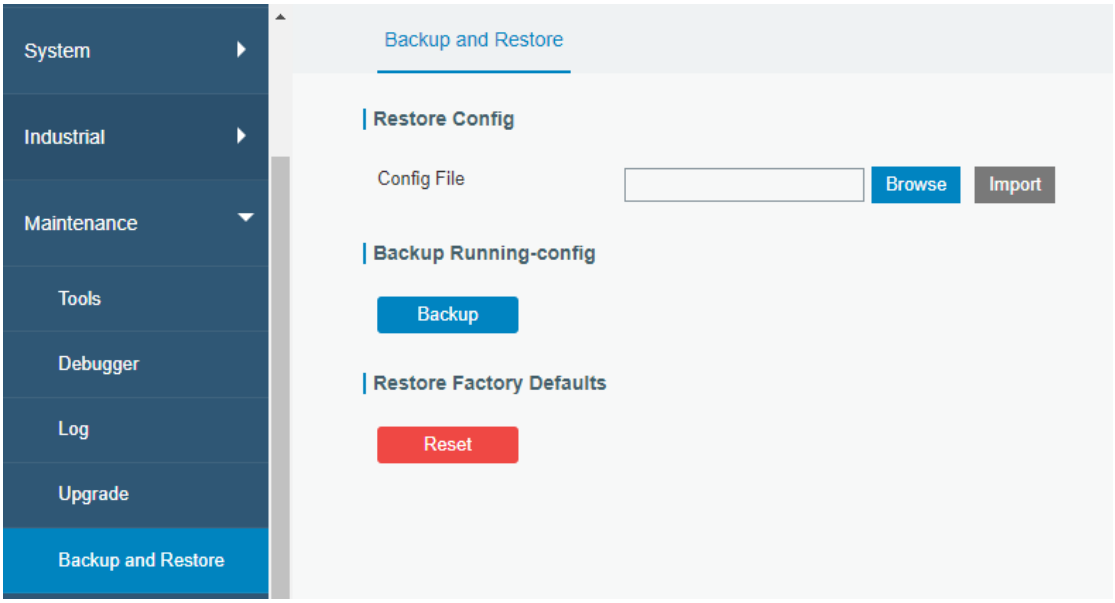
APPLICATION EXAMPLES

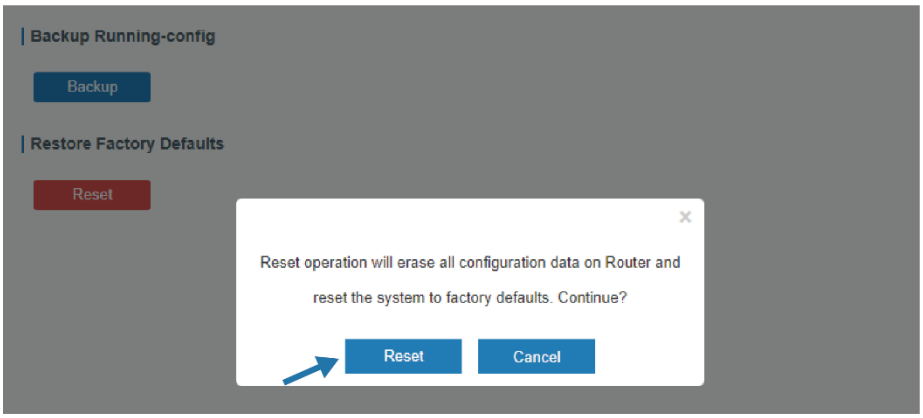
RESTORE FACTORY DEFAULTS

VIA WEB INTERFACE

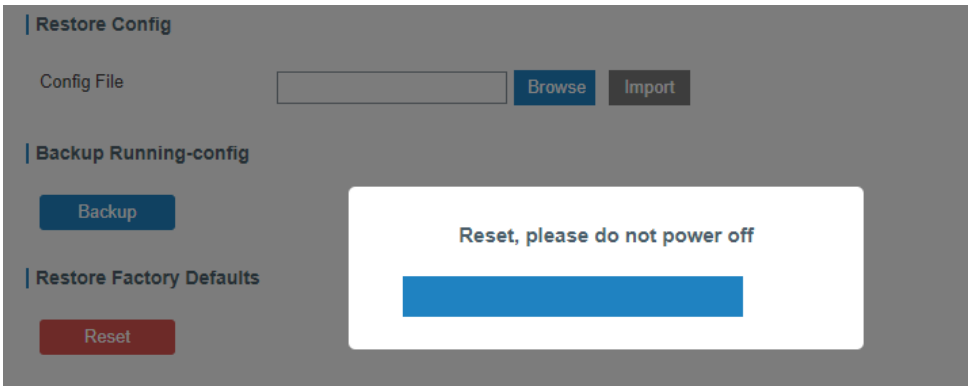
1. Log in web interface and go to “Maintenance > Backup and Restore.”
2. Click “Reset” button under the “Restore Factory Defaults.”

You will be asked to confirm if you would like to reset it to factory defaults. Then click “Reset” button.





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



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.

VIA HARDWARE

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

Blinking Press and hold the reset button for more than 5 seconds.

Static Green → Rapidly Blinking Release the button and wait.

Off → Blinking The router is now reset to factory defaults.

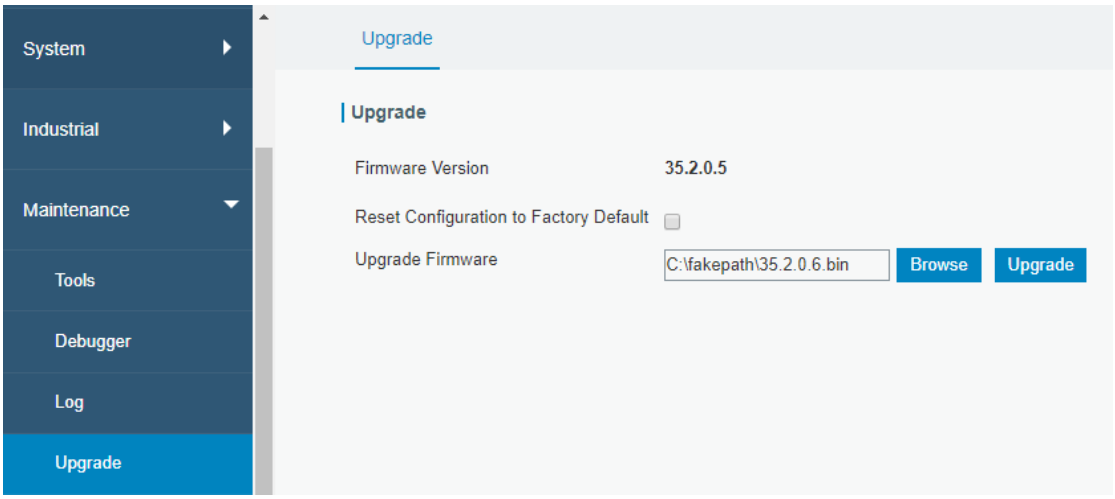
FIRMWARE UPGRADE

It is suggested that you contact SilverNet 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 is 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.



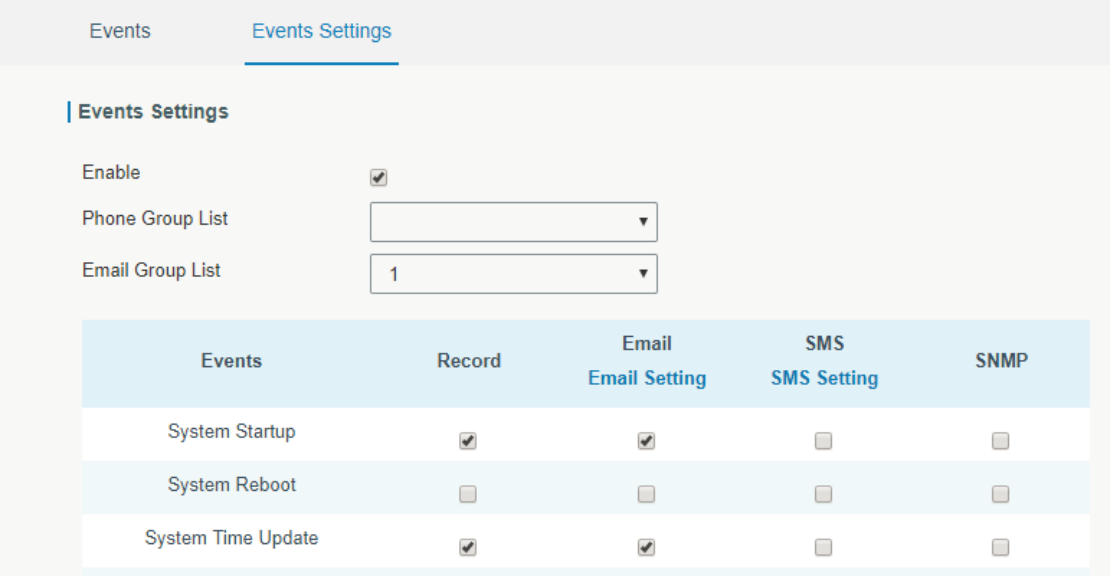
EVENTS APPLICATION EXAMPLE

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

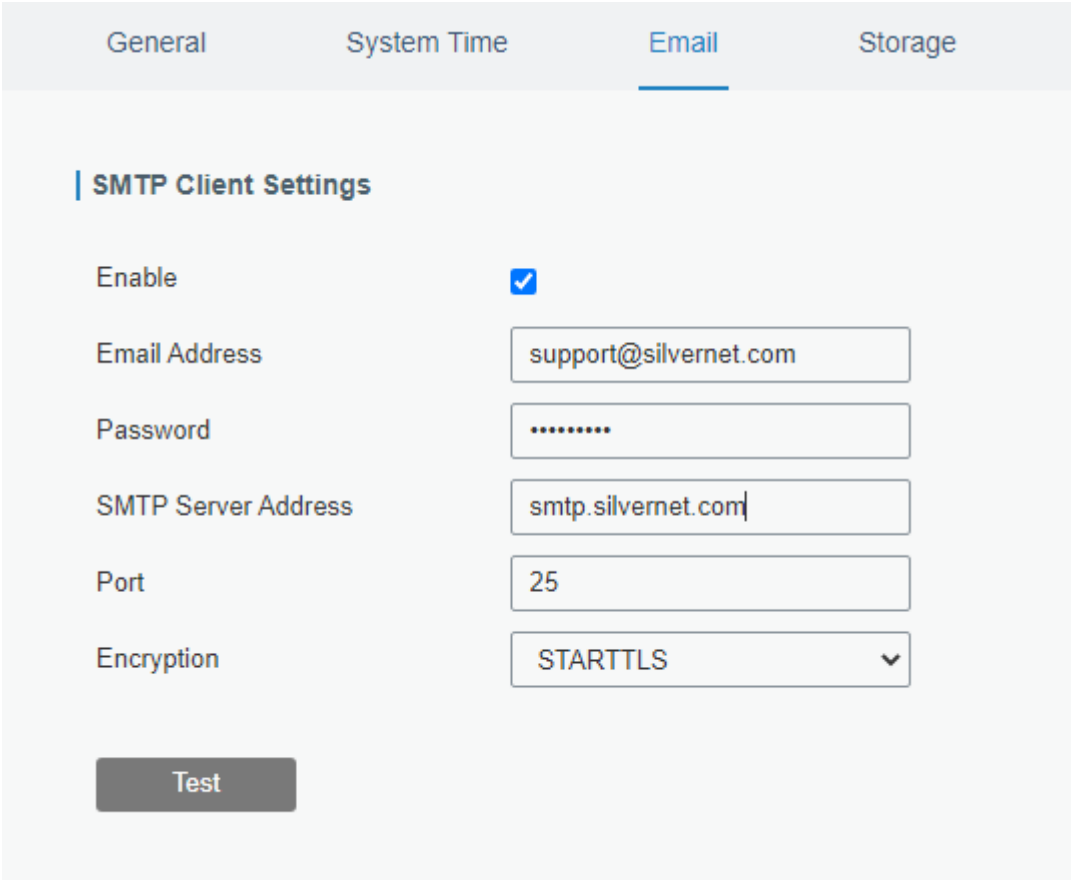
Events	Actions to make events occur (for test)
Router system start up.	Plug the power supply of the router.
Router system time update.	Set up system time manually.

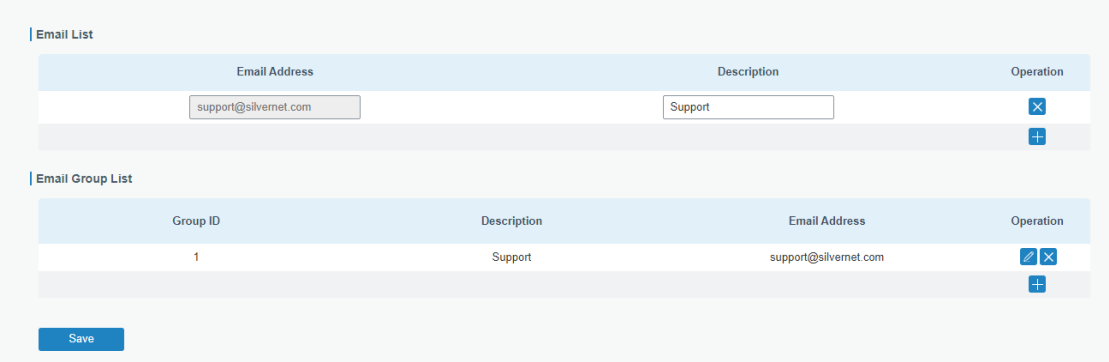
Configuration Steps

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



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.



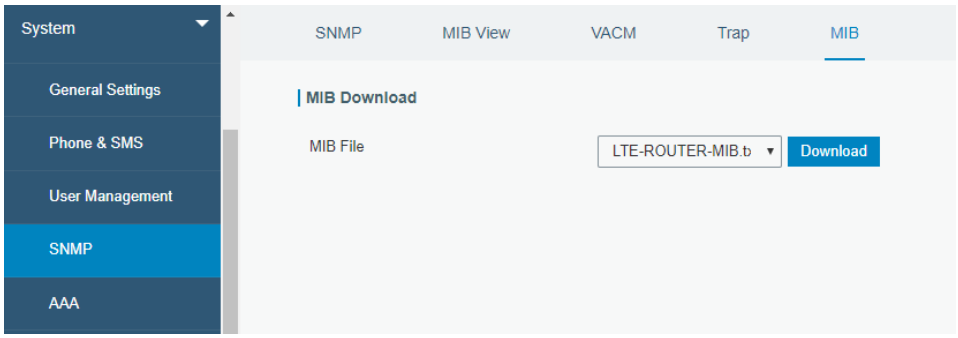


4. To test the functionality of Alarm, please take the corresponding actions listed above. It will send an alarm e-mail to you when the relevant event occurs. Refresh the web GUI, go to “Events > Events,” and you will find the events records.

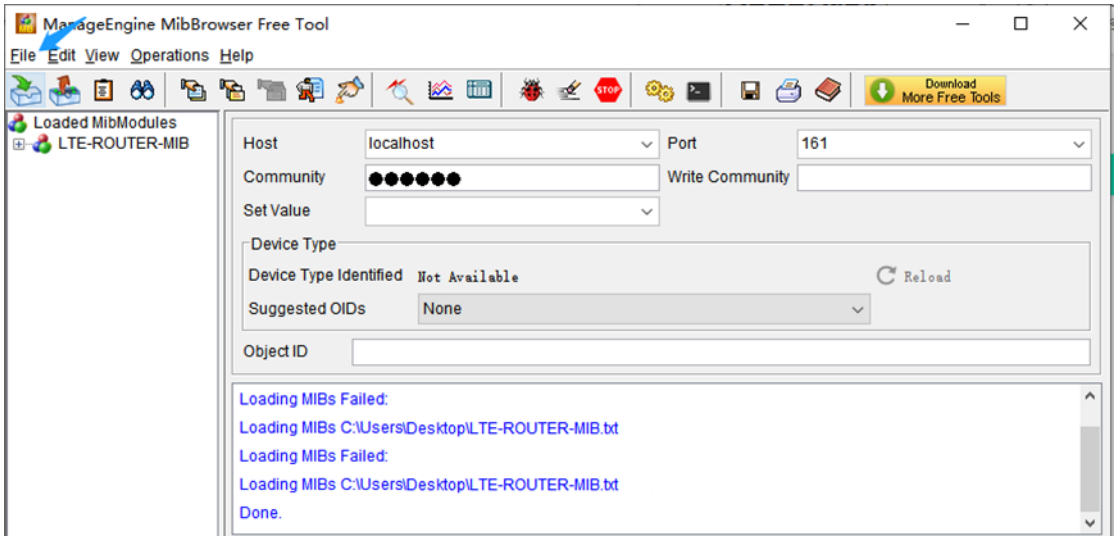
SNMP Application Example

Before you configure SNMP parameters, please download the relevant “MIB” file from the iSite’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.

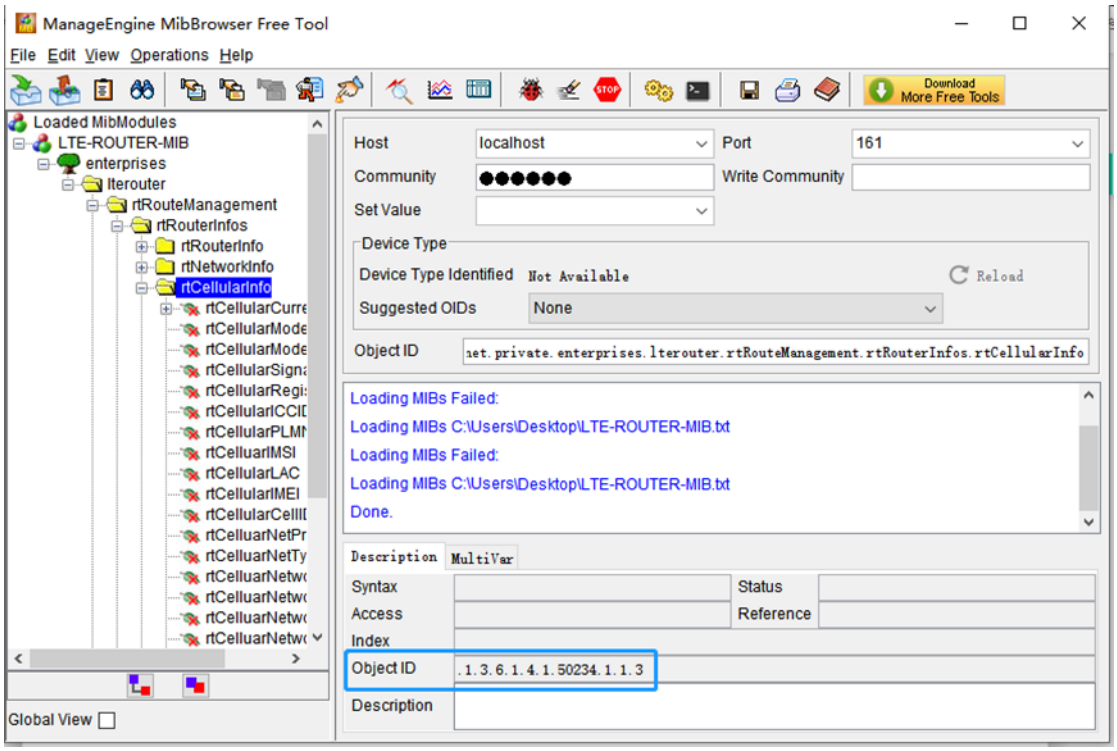
1. Go to “System > SNMP > MIB” and download the MIB file “LTE-ROUTER-MIB.txt” to PC.



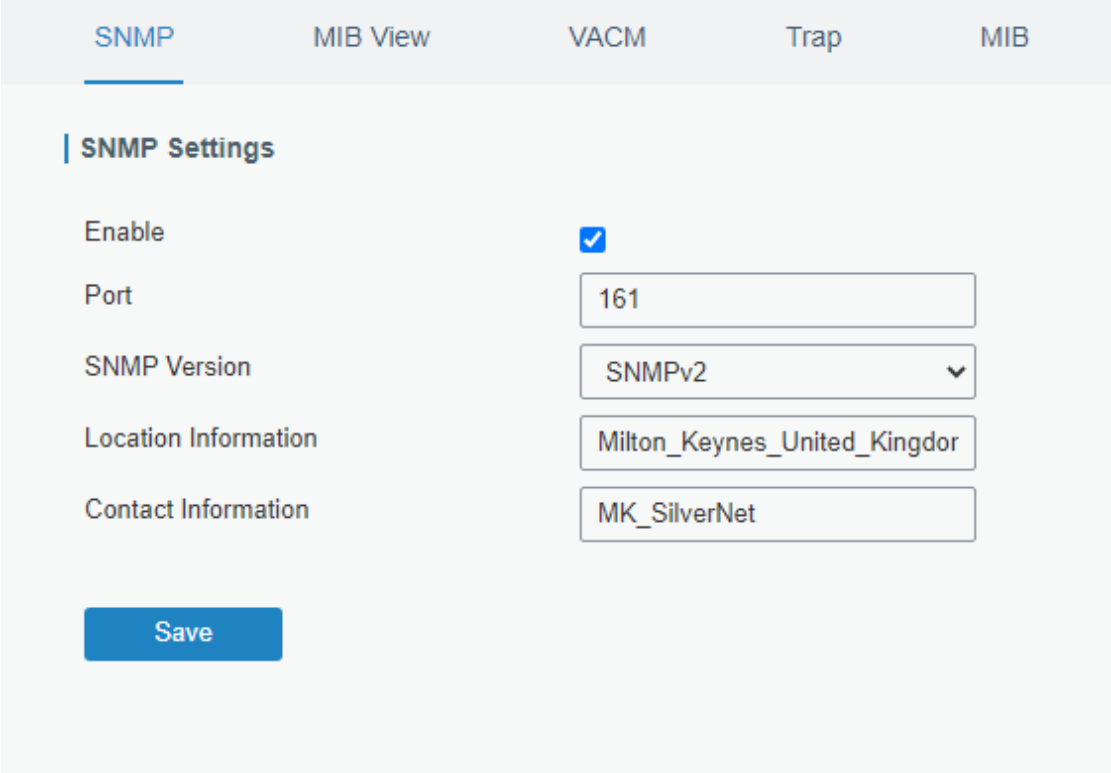
2. Start “ManageEngine MibBrowser Free Tool” on the PC. Click “File > Load MIB” on the menu bar. Then select “LTE-ROUTER-MIB.txt” file from PC and upload it to the software.



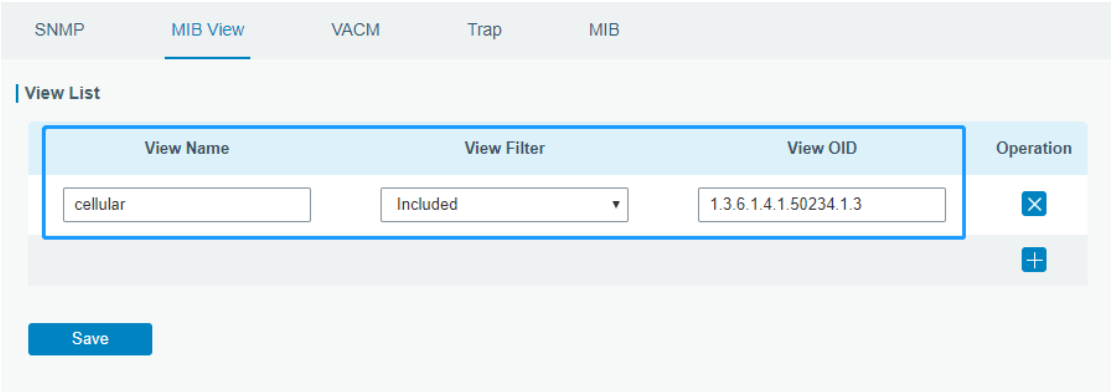
3. Click the “+” button beside “LTE-ROUTER-MIB,” which is under the “Loaded MibModules” menu and find “usCellularinfo.” And then you will see the OID of cellular info is “.1.3.6.1.4.1.50234”, which will be filled in the MIB View settings.



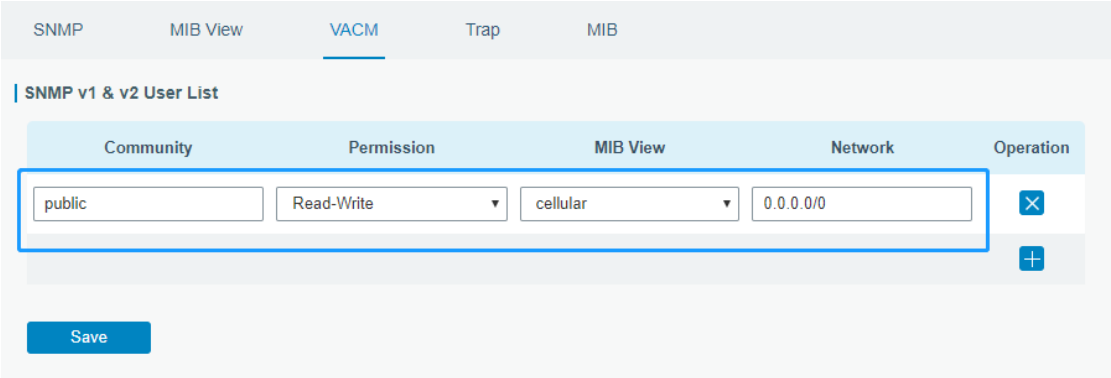
4. Go to “System > SNMP > SNMP” on the router’s WEB GUI. Check “Enable” option, then click “Save” button.



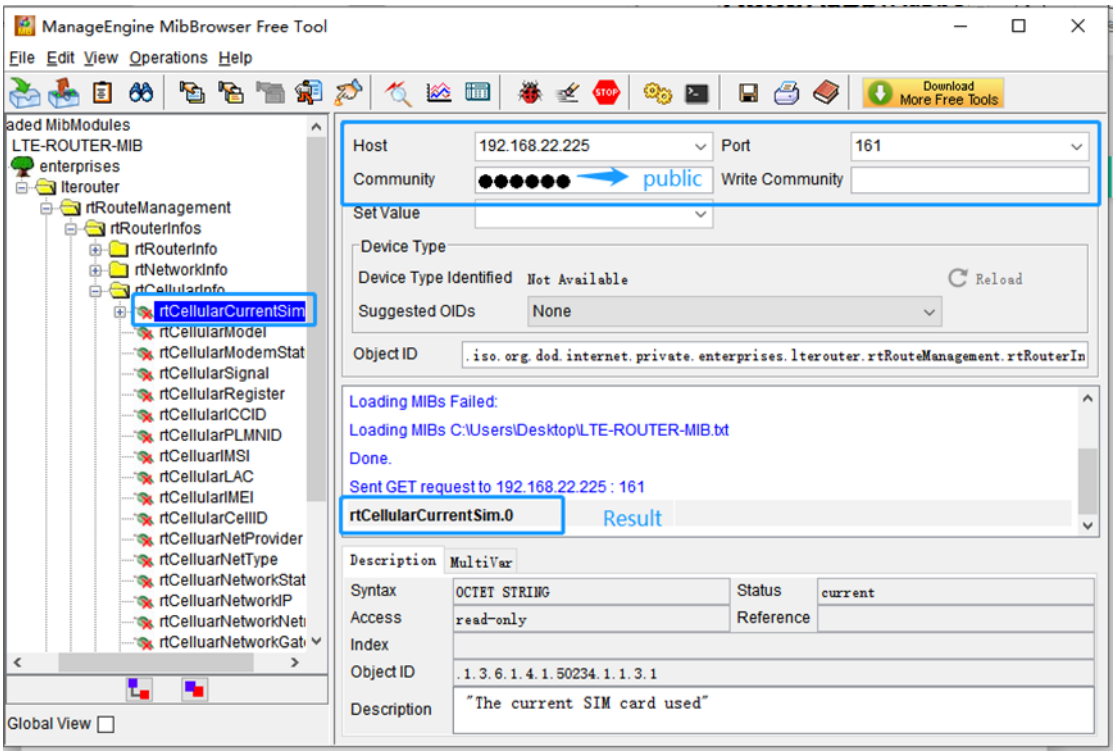
5. Go to “System > SNMP > MIB View.” Click to add a new MIB view and define the view to be accessed from the outside network. Then click “Save” button.



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



7. 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.



NETWORK CONNECTION

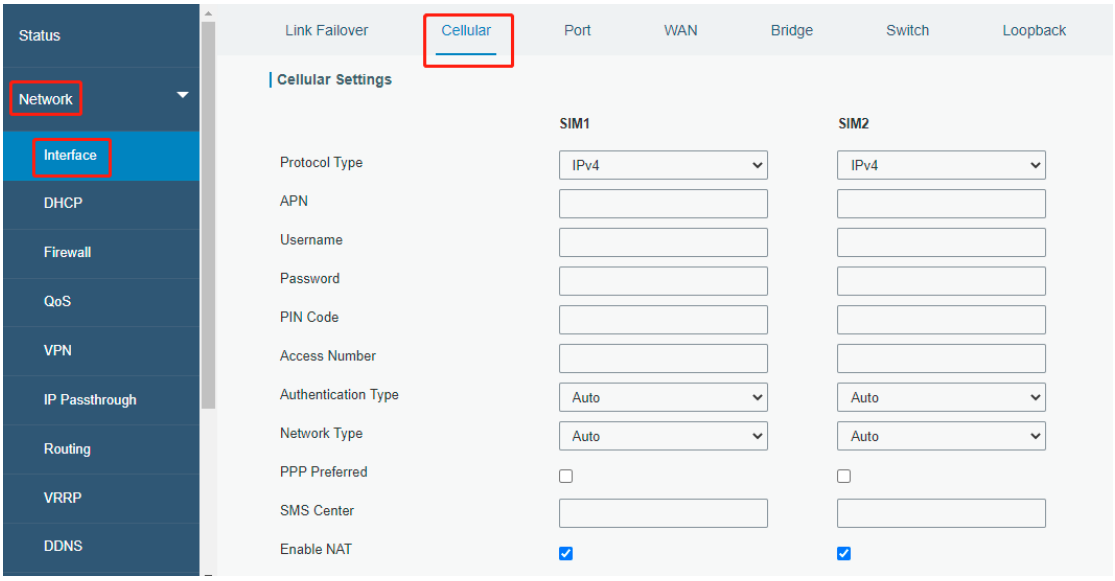
CELLULAR CONNECTION

The iSite 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.

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

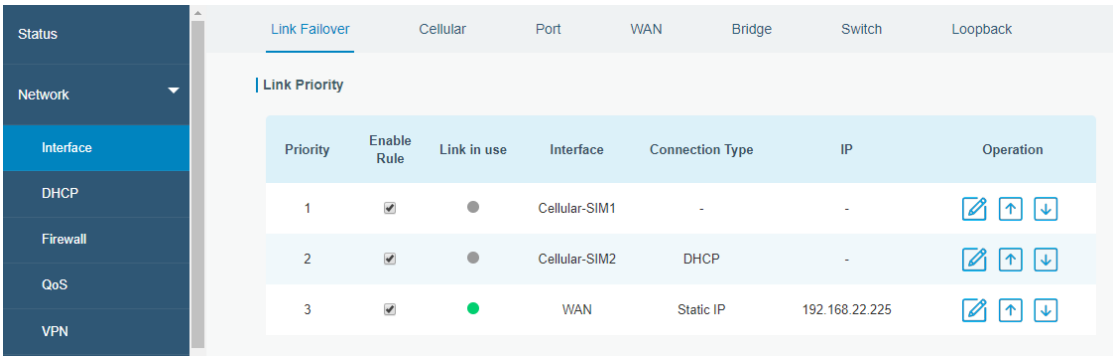
Configuration Steps

1. Go to “Network > Interface > Cellular > Cellular Setting” and configure the cellular info.

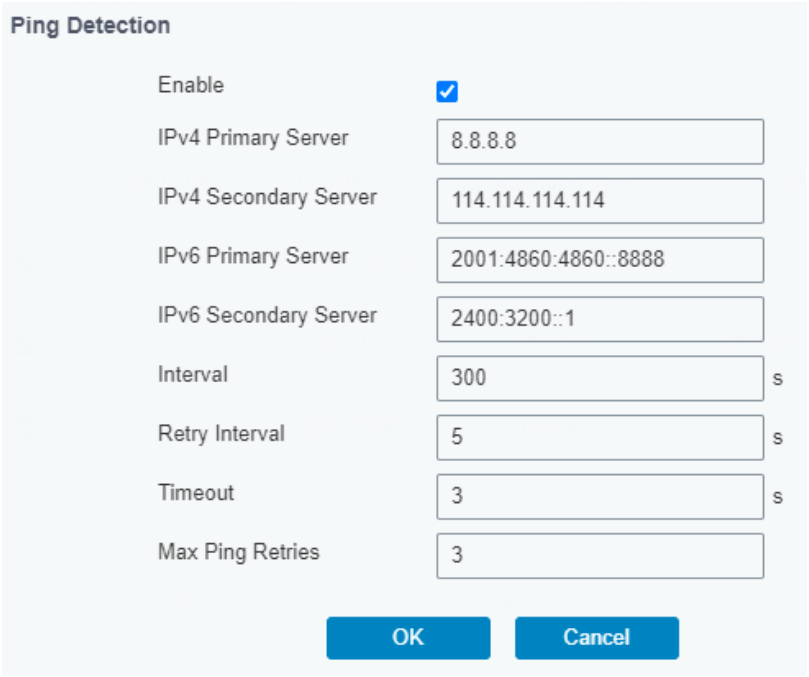


Click “Save” and “Apply” for configuration to take effect.

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

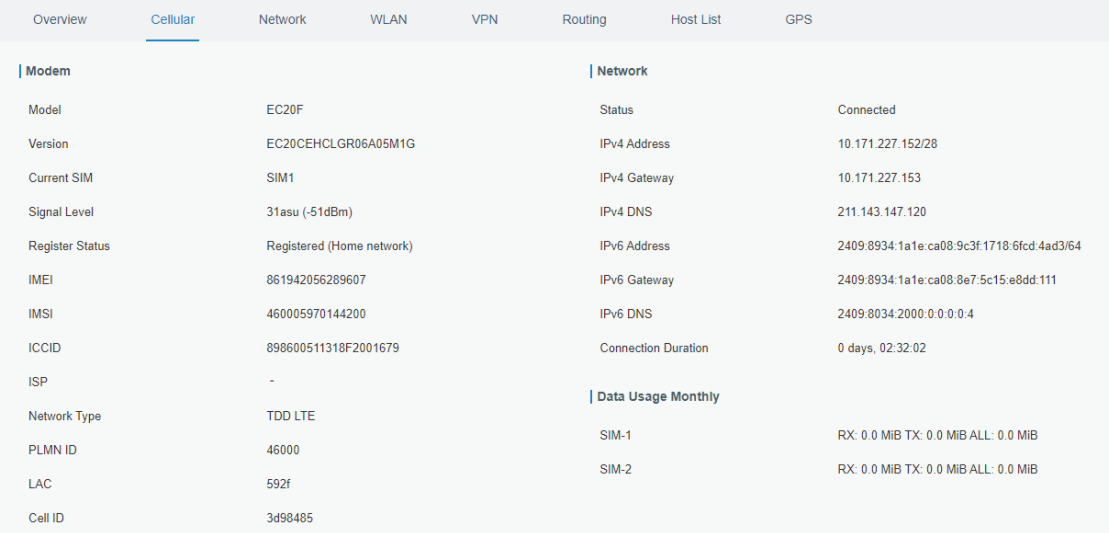


3. Click to configure ICMP ping detection information.



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 dialled up successfully.



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 iSite router.

ETHERNET WAN CONNECTION

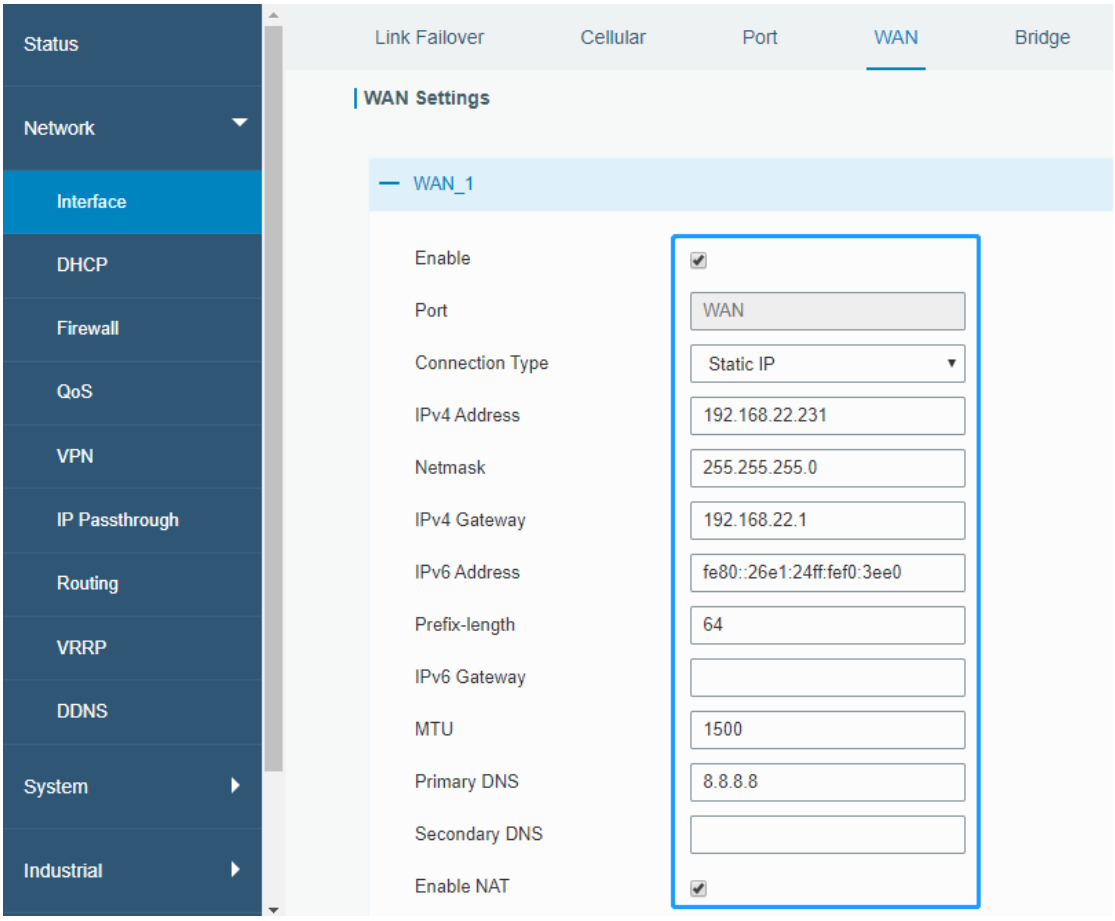
WAN port of the iSite is connected with Ethernet cable to get Internet access.

Configuration Steps

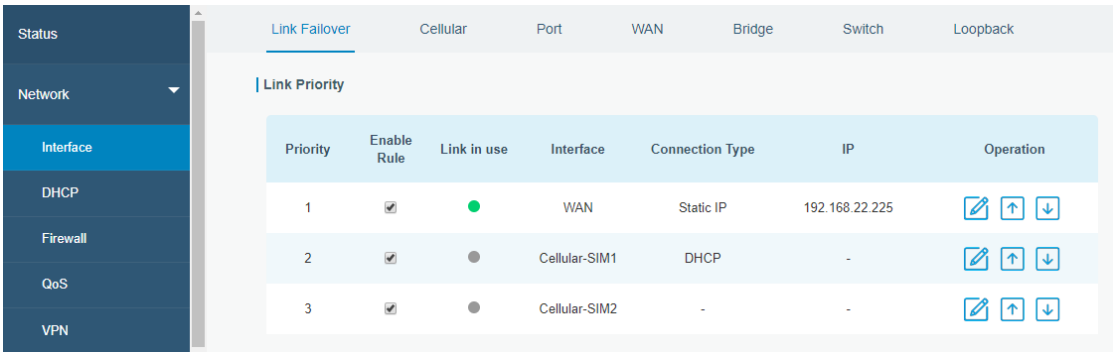
1. Go to “Network > Interface > WAN” to select connection type and configure WAN parameters. The following examples of static IP type, DHCP Client type, and PPPoE type are listed for your reference.

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.



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



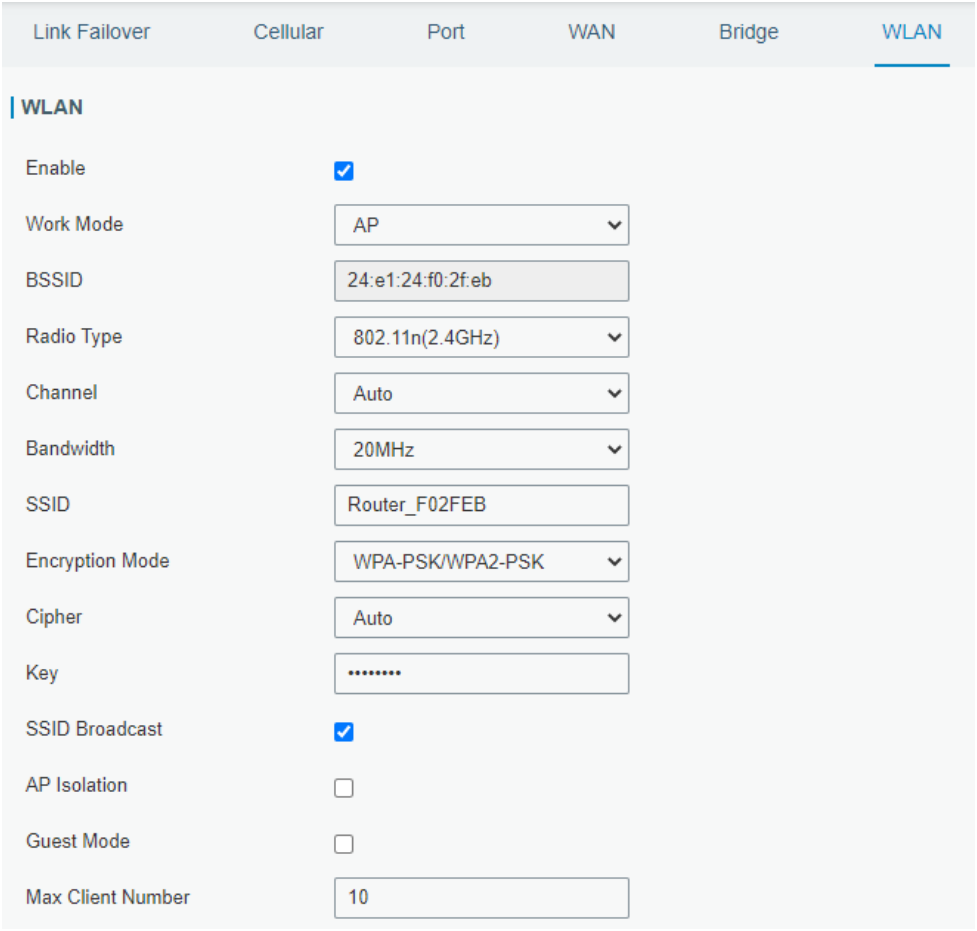
WI-FI APPLICATION EXAMPLE

AP MODE

Configure iSite as AP to allow connection from users or devices.

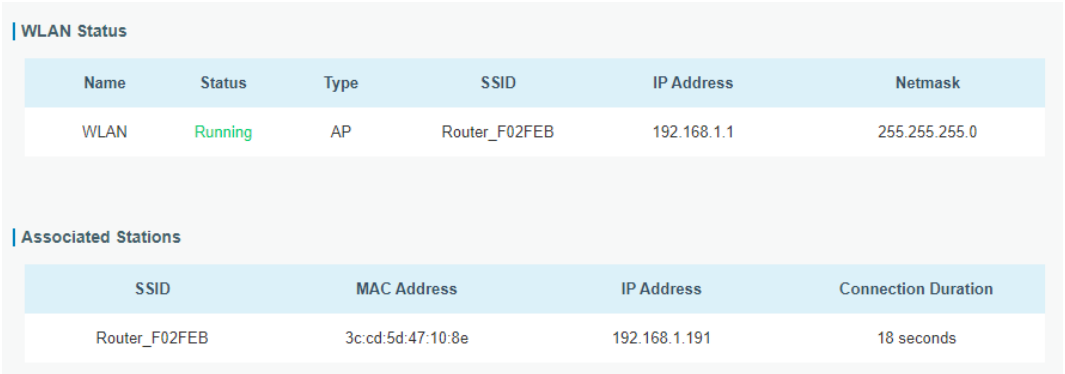
Configuration Steps

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



Click “Save” and “Apply” button after all configurations are done.

2. Use a smart phone to connect the access point of iSite. Go to “Status > WLAN,” and you can check the AP settings and information of the connected client/user.

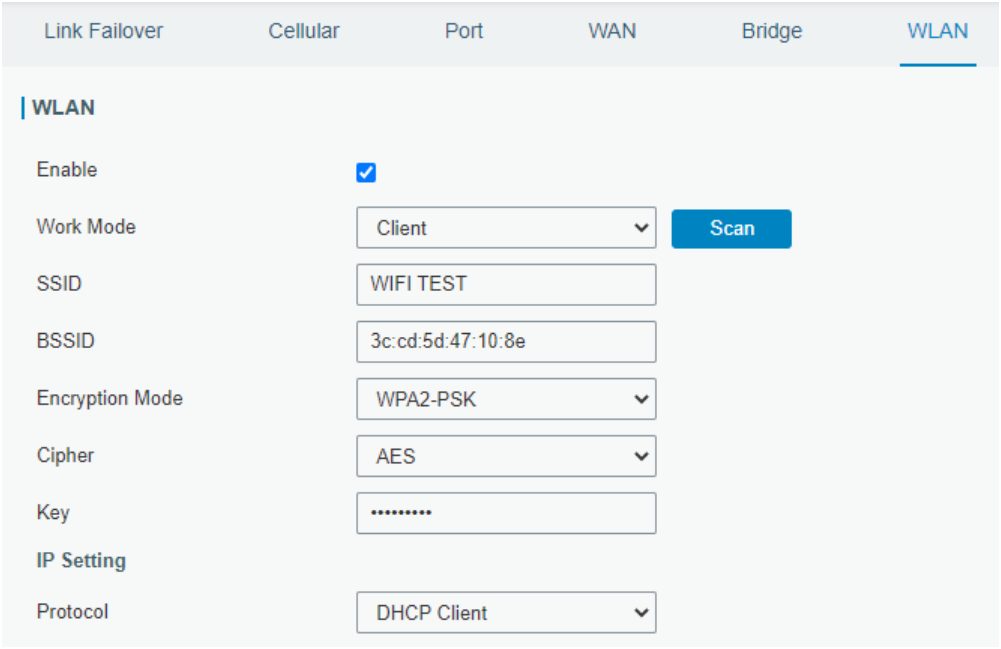


CLIENT MODE

Configure iSite as Wi-Fi client to connect to an access point to have Internet access.

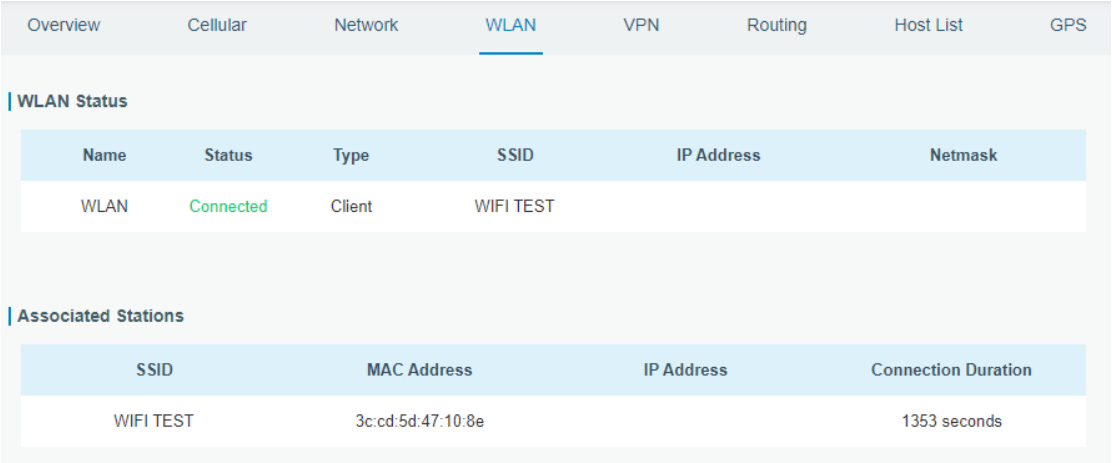
Configuration Steps

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



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.



VRRP APPLICATION EXAMPLE

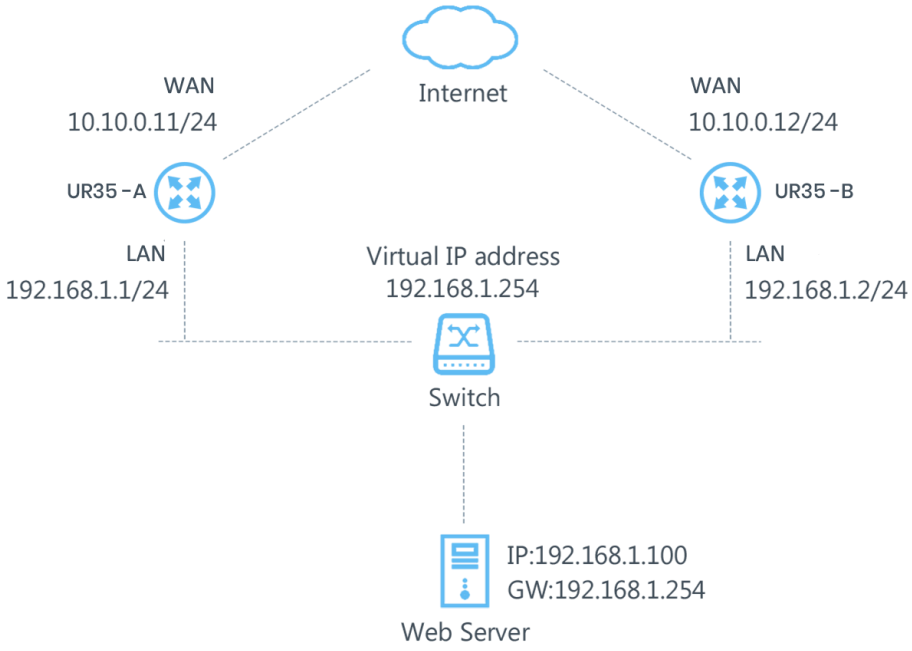
A Web server requires Internet access through the iSite router. To avoid data loss caused by router breakdown, two iSite routers can be deployed as VRRP backup group, so as to improve network reliability.

VRRP group:

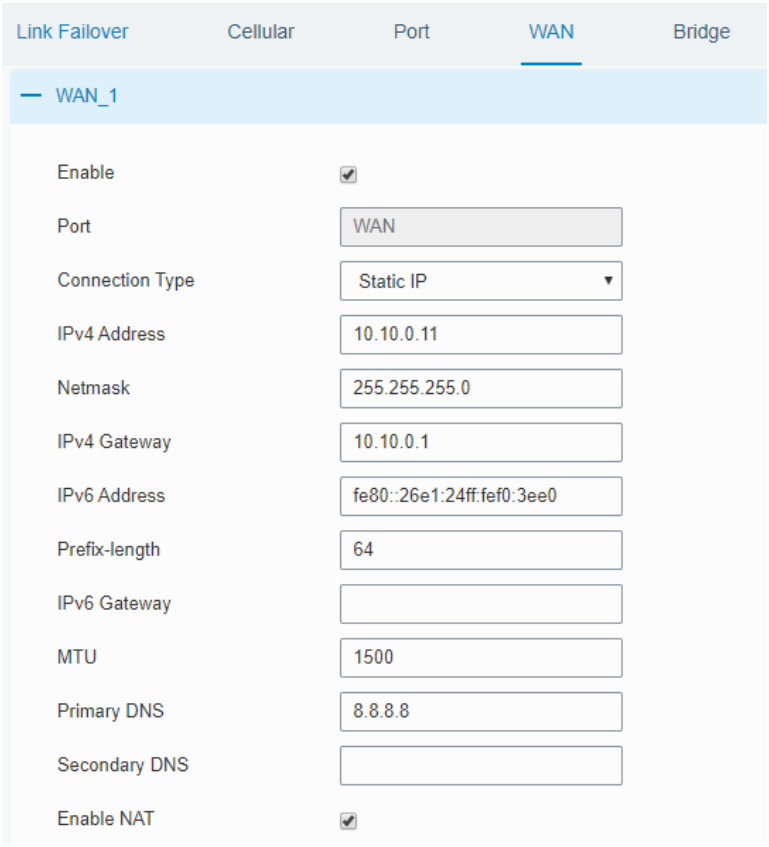
WAN ports of the iSite Router A and Router B are connected to the Internet via wired network. And LAN ports of them are connected to a switch.
Virtual IP is 192.168.1.254/24.

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

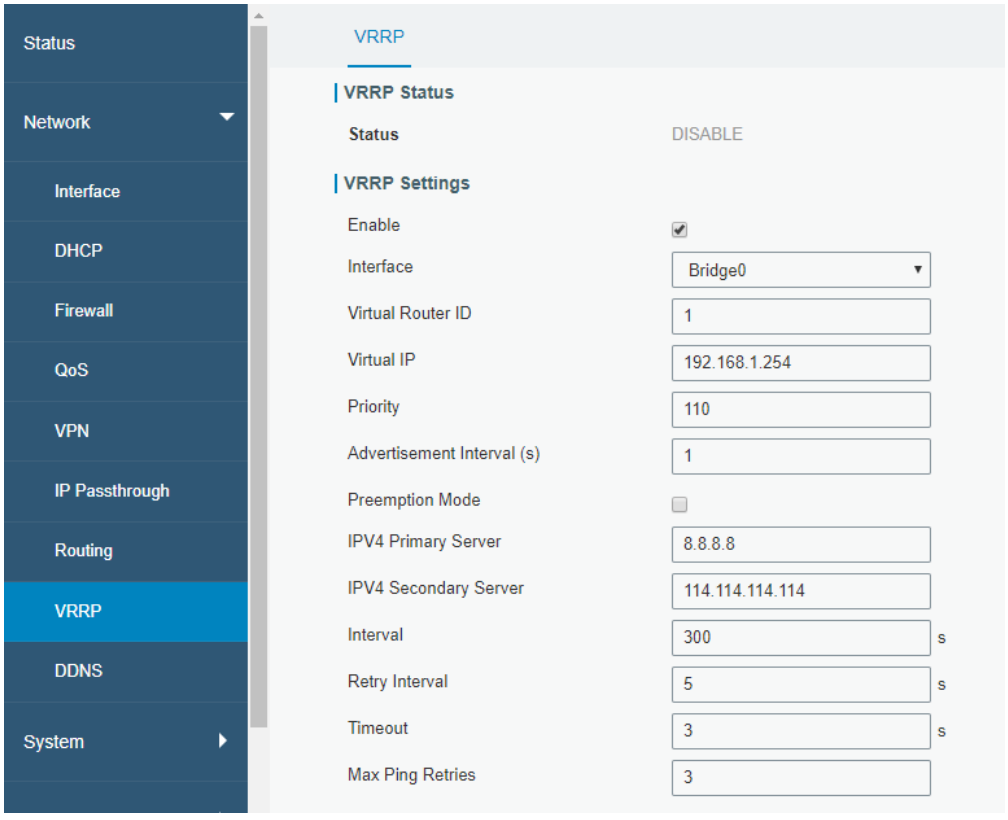
Refer to the topological below.



Configuration Steps
Router A Configuration
1. Go to “Network > Interface > WAN” and configure wired WAN connection as below.

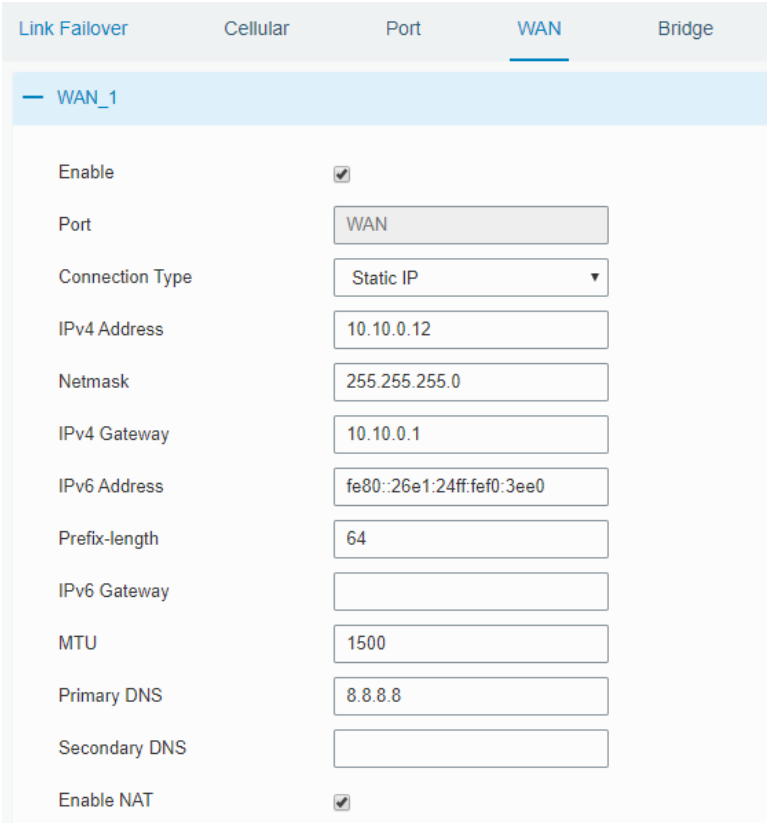


2. Go to “Network > VRRP > VRRP” and configure VRRP parameters as below.

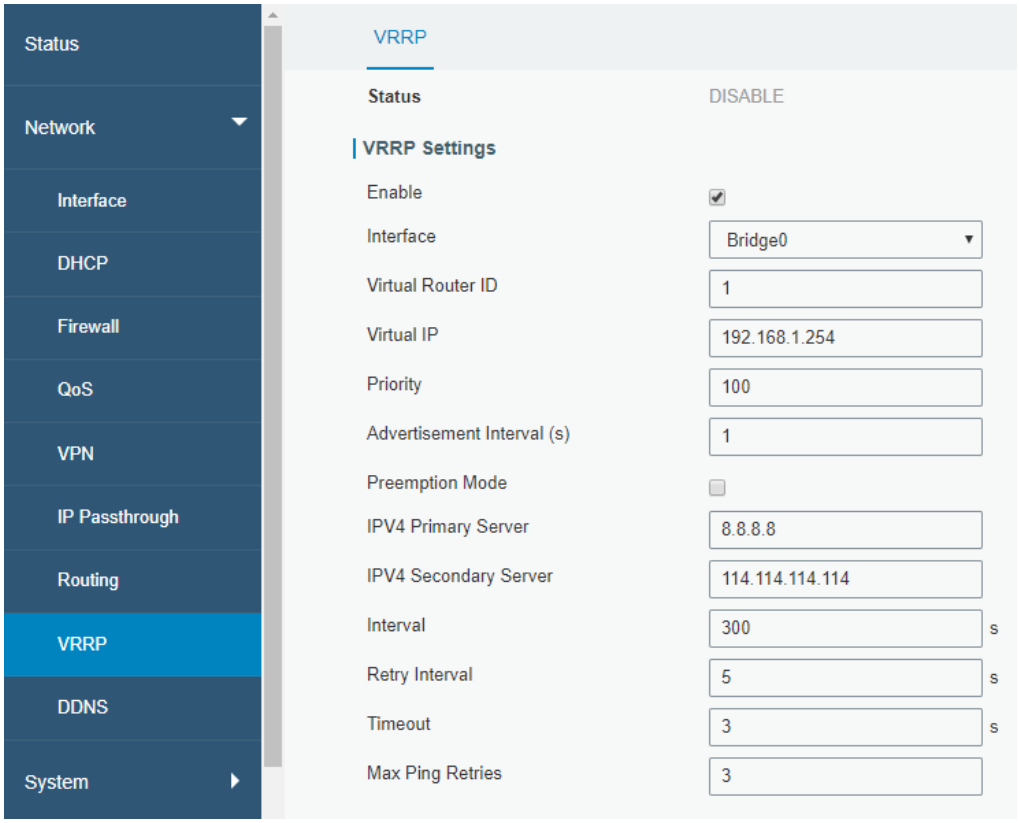


Router B Configuration

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



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



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

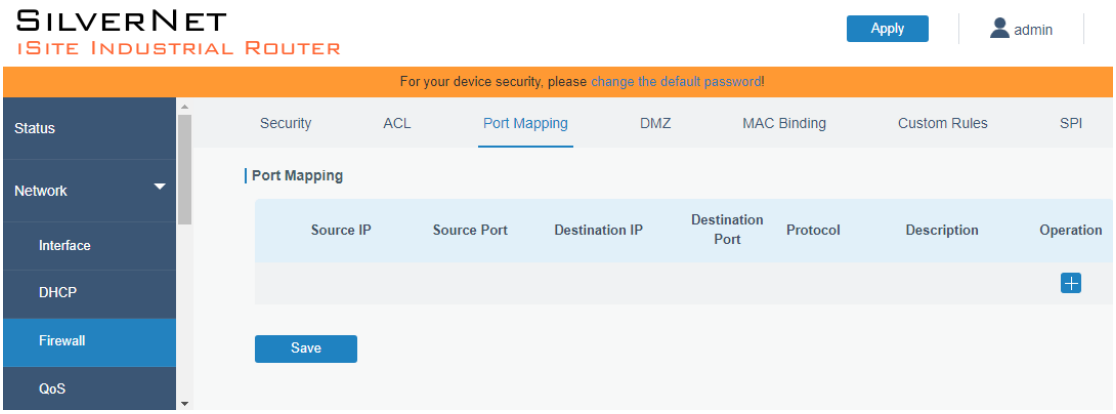
Result: normally, A is the master router, used as the default gateway. When the power of Router A is down or Router A suffers from failure, Router B will become the master router, used as the default gateway. With Preemption Mode enabled, Router A will be master and Router B will demote back to be the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

NAT Application Example

An iSite 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.



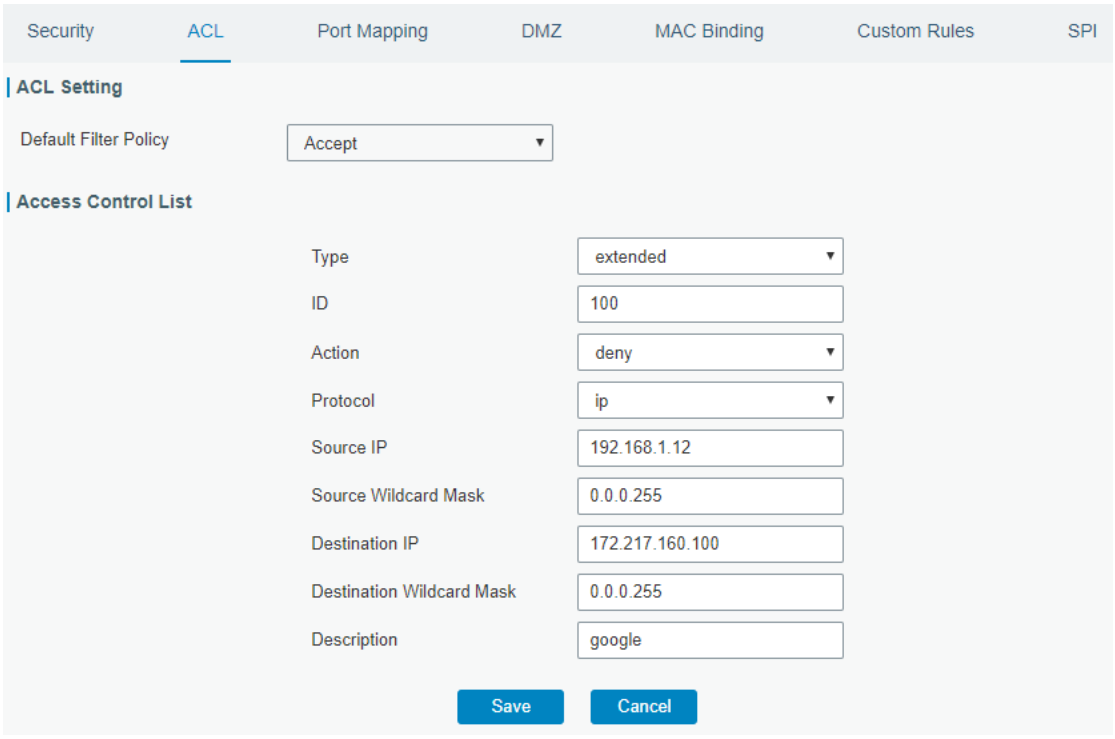
Click “Save” and “Apply” button.

Access Control Application Example

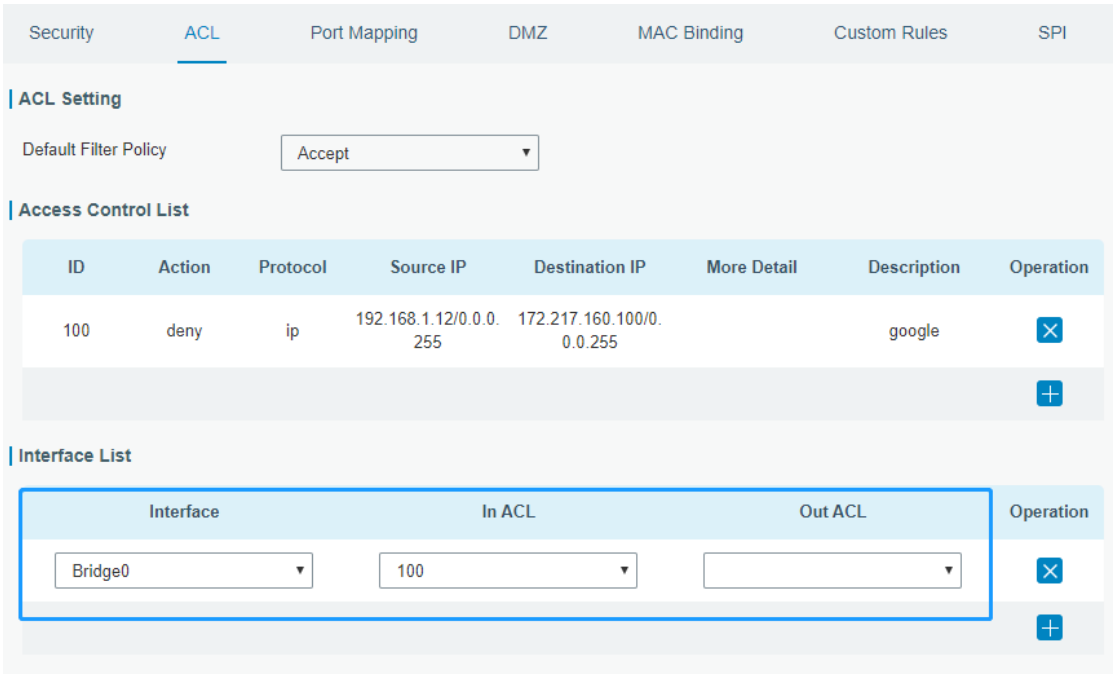
LAN port of the iSite is set with IP 192.168.1.0/24. Then configure the router to deny accessing to Google IP 172.217.160.100 from local device with IP 192.168.1.12.

Configuration Steps

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



2. Configure interface list. Then click “Save” and “Apply” button.



QoS Application Example

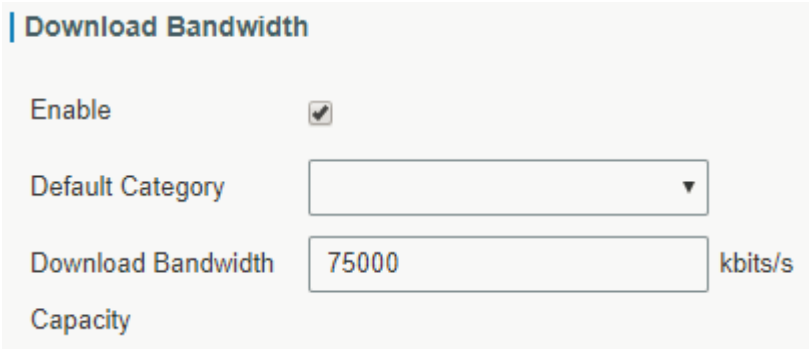
Configure the iSite router to distribute local preference to different FTP download channels. The total download bandwidth is 75000 kbps.

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

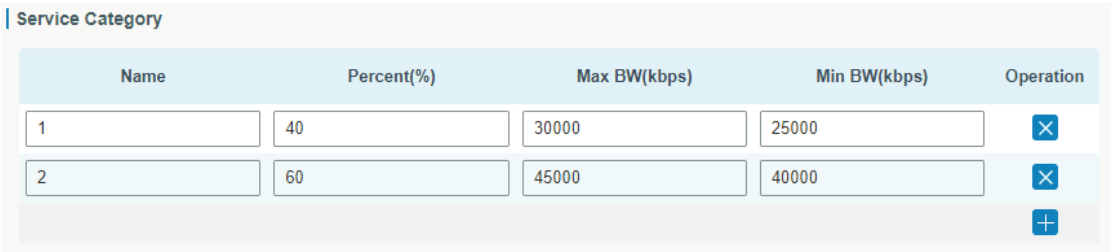
FTP Server IP & Port	Percent	Max Bandwidth(kbps)	Min Bandwidth(kbps)
110.21.24.98:21	40%	30000	25000
110.32.91.44:21	60%	45000	40000

Configuration Steps

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

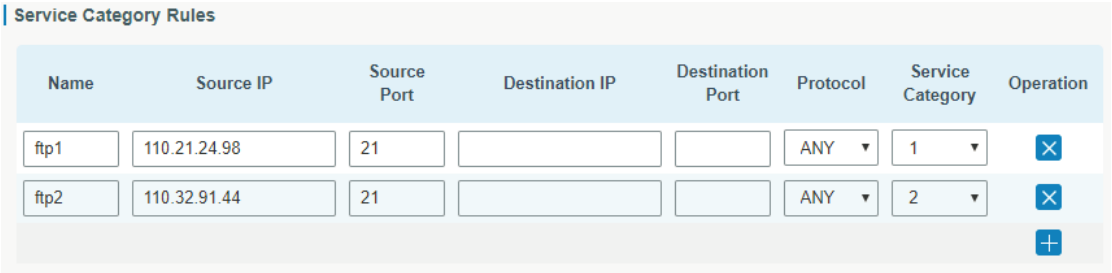


2. Please find “Service Category” option and click “ ” to set up service classes.



Note: the percentages must add up to 100%.

3. Please find “Service Category Rules” option and click “ ” to set up rules.



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

Click “Save” and “Apply” button.

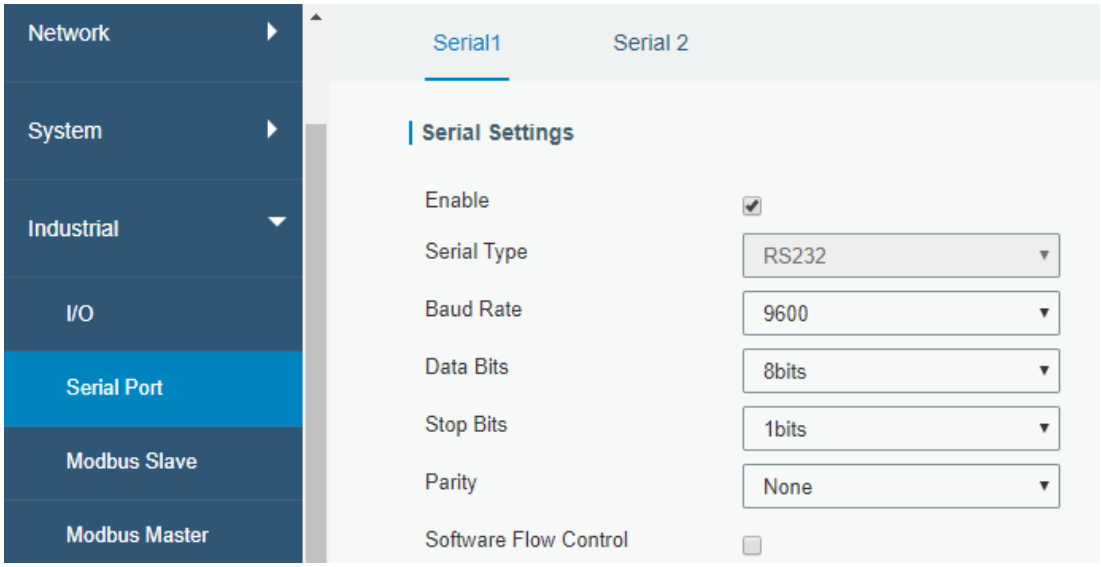
DTU APPLICATION EXAMPLE

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

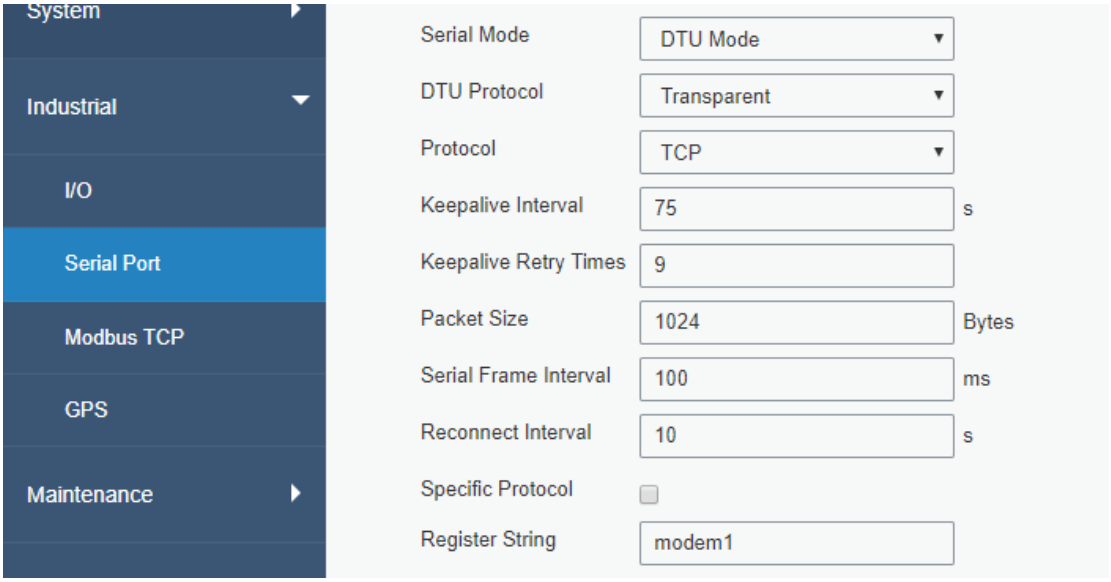
Serial Parameters of the PLC	
Baud Rate	9600
Data Bit	8
Stop Bit	1
Parity	None

Configuration Steps

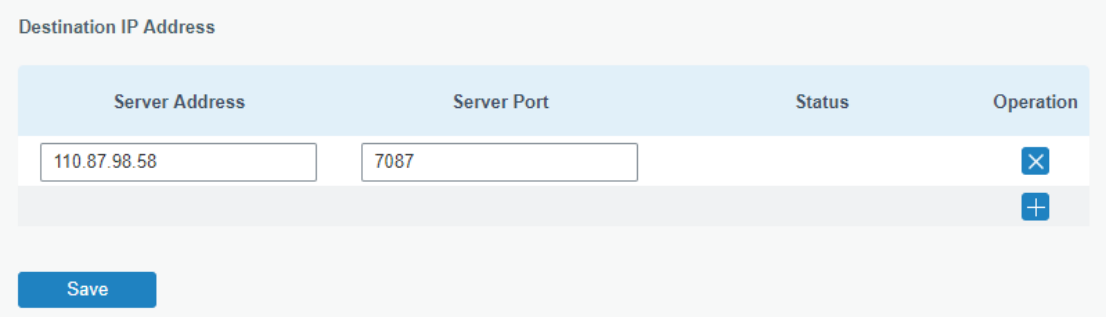
1. Go to “Industrial > Serial Port > Serial” and configure serial port parameters. The serial port parameter shall be kept in consistency with those of PLC, as shown in figure below.



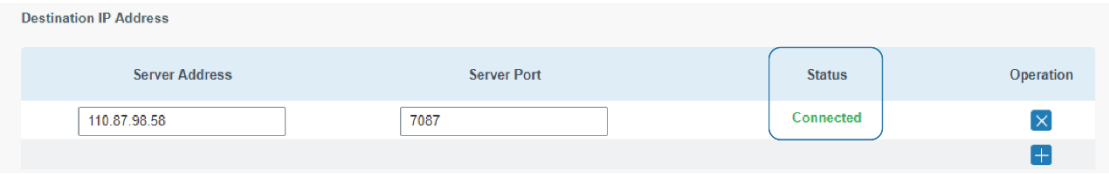
2. Configure Serial Mode as “DTU Mode.” The iSite is connected as client in “Transparent” protocol.



3. Configure TCP server IP and port.

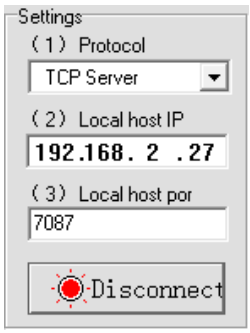


4. Once you complete all configurations, click “Save” and “Apply” button.



5. Start TCP server on PC.

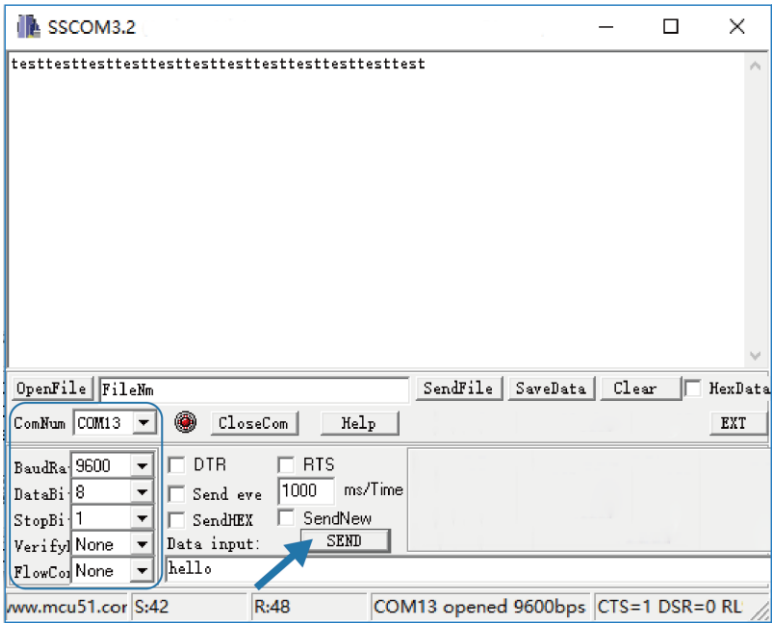
Take “Netassist” test software as example. Make sure port mapping is already done.



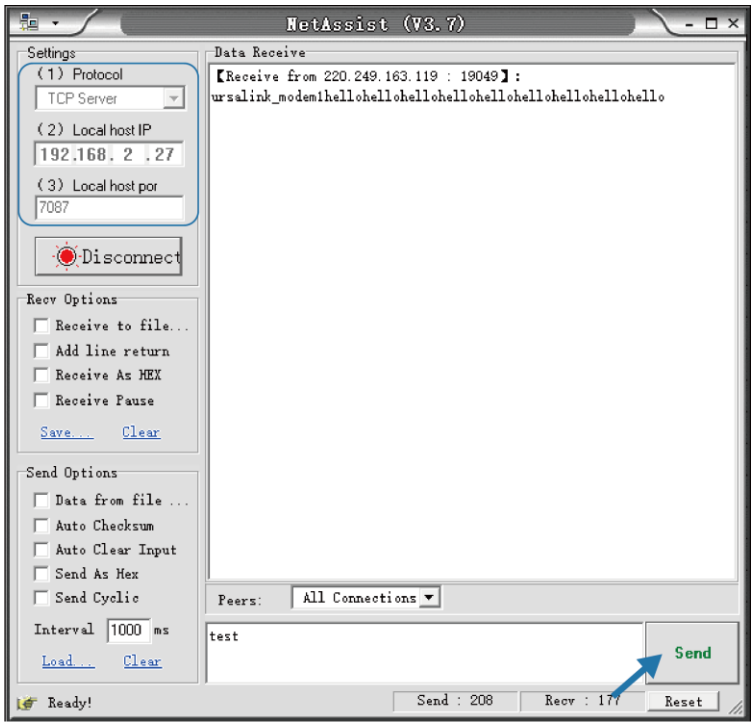
6. Connect the iSite to PC via RS232 for PLC simulation. Then start “sscom” software on the PC to test communication through serial port.

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

PC side



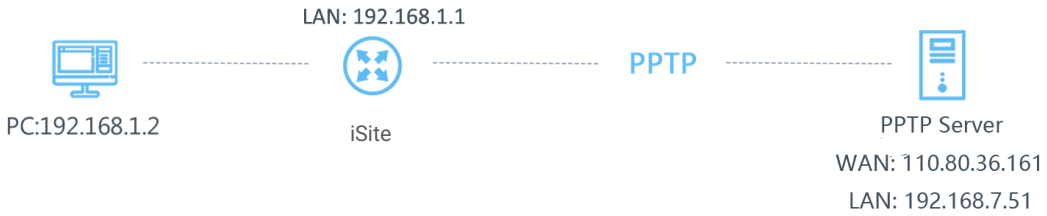
TCP server side



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

PPTP Application Example

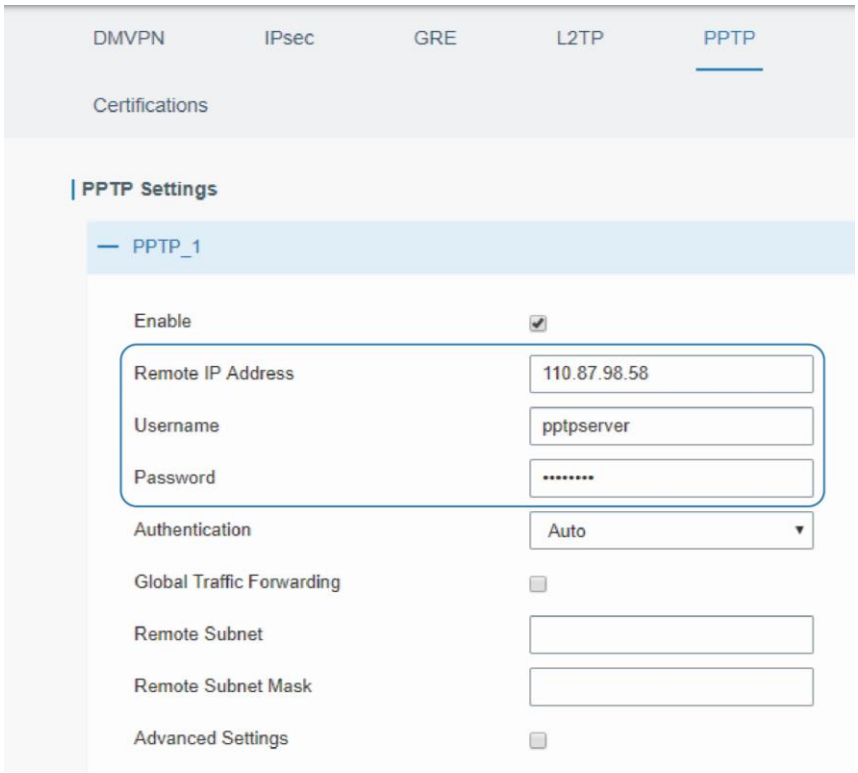
Configure the iSite as PPTP client to connect to a PPTP server in order to have data transferred securely. Refer to the following topological graph.



Configuration Steps

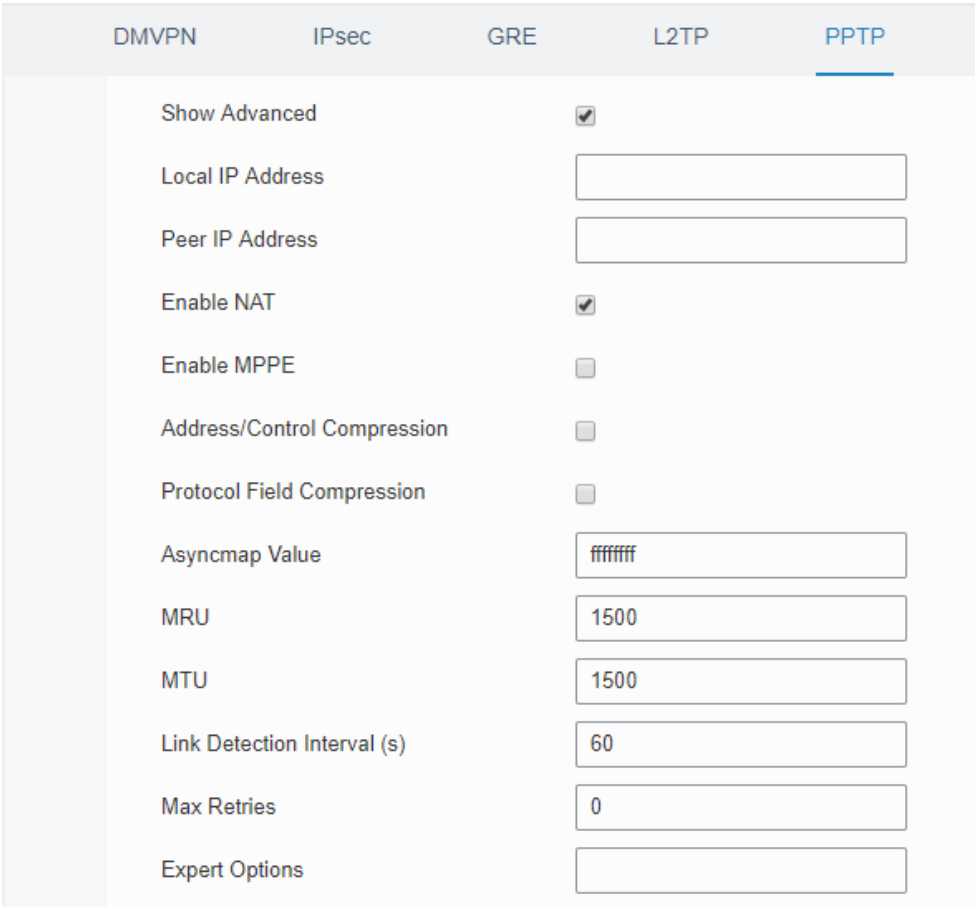
1. Go to “Network > VPN > PPTP,” configure PPTP server IP address, username and password provided by PPTP server.

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



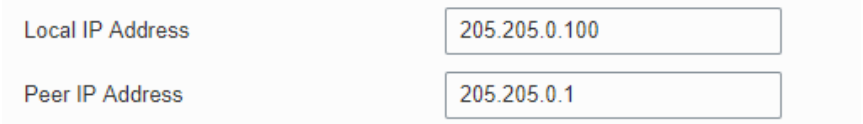
If you want to access peer subnet such as 192.168.3.0/24, you need to configure the subnet and mask to add the route.

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



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

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.



Otherwise PPTP server will assign tunnel IP randomly.

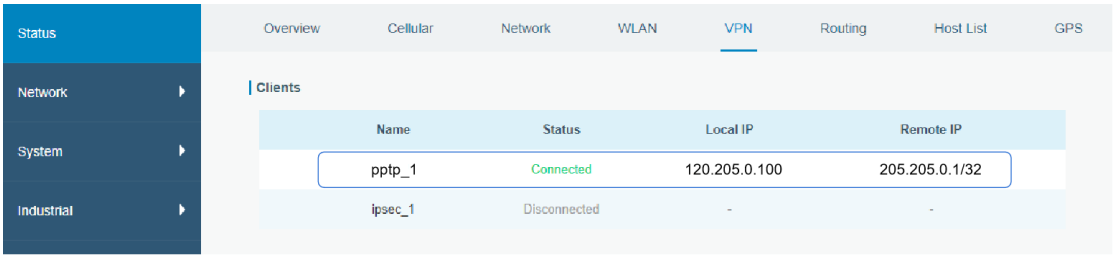
Click “Save” button when you complete all settings, and then the advanced settings will be hidden again. Then click “Apply” button to have the configurations take effect.

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.



DISCLAIMER

- SilverNet Limited does not accept liability for any loss or damage arising from the use of any information or particulars in this document or from any incorrect use of the product.
- All maintenance and service of the products must be authorised by SilverNet Limited or its designated distributors. SilverNet Limited does not accept any liability whatsoever for any loss or damage caused by service, maintenance, or repair by unauthorised personnel.
- Our Network equipment have a variety of uses in different industries and the customer must be satisfied that the system is suitable for their r own particular purposed. While SilverNet Limited can give an indication of possible uses of our Network equipment, it gives no express or implied warranty that the system will be suitable for any customer's particular needs.
- SilverNet Limited warranty is set out in its Standard Terms and Conditions of Sale and will only undertake repairs to our Network Equipment at its own premises. SilverNet Limited will not repair out Network Equipment already installed on a customer's site, nor will it be liable for costs associated with decommissioning and subsequent re-commissioning.
- All reasonable skill and care have been taken in the compiling of this document. There are no material facts or circumstances known to SilverNet Limited which are not disclosed in this document. Whilst every effort has been made to ensure accuracy of the information set out herein no warranty confirming such should be taken as having ben give (expressly or implied). SilverNet Limited can accept no responsibility for loss or damage occasioned by any person acting or refraining from cation as a result of the material in this document.

WARRANTY

The iSite comes with a 2-year warranty as standard. For full terms and conditions of warranty please go to **www.silvernet.com/terms-and-conditions/**

CONTACT SILVERNET

Email us at support@silvernet.com

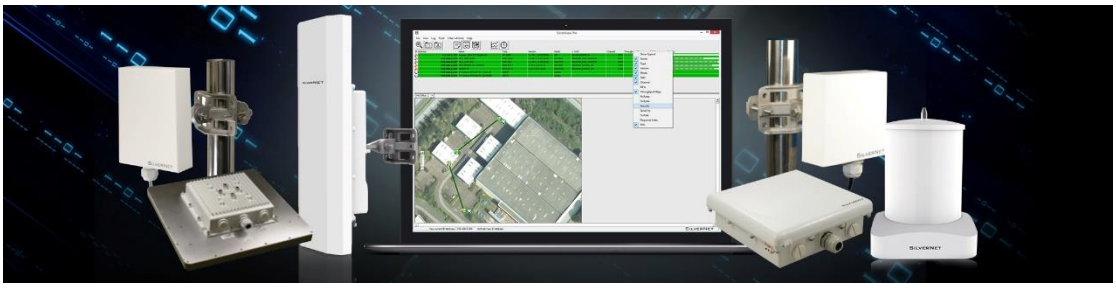
Call our support team on **08712233067**

www.silvernet.com

COPYRIGHT INFORMATION

OTHER SILVERNET PRODUCTS

PRO RANGE



INDUSTRIAL NETWORK TRANSMISSION

INTELLIGENT WI-FI SOLUTIONS

INDUSTRY LEADING TECHNICAL SUPPORT