DSR-211-Serie

Industrial LTE/HSPA+/UMTS/GSM-Router

Manual

AddSecure GmbH
Breite Straße 10
D-40670 Meerbusch

Phone: +49 (0)2159/693 75-0
Fax : +49 (0)2159/922 430 0
E-mail: info.digicomm@addsecure.com

Document Revision: 20-02

For further information regarding our products please visit us at www.addsecure.de

About This Document

This document provides hardware and software information of the DSR-211 Router, including introduction, installation, configuration and operation.

Copyright © 2024 AddSecure GmbH

Legal information

The contents of this document are provided “as is”. Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy and reliability or contents of this document. AddSecure reserves the right to revise this document or withdraw it at any time without prior notice.
Under no circumstances shall AddSecure be responsible for any loss of data or income or any special, incidental, and consequential or indirect damages howsoever caused.

More information about AddSecure can be found at the following Internet address: http://www.addsecure.de

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the router is used in a normal manner with a well-constructed network, the router should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. AddSecure accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the router, or for failure of the router to transmit or receive such data.

Safety Precautions

General

- The router generates radio frequency (RF) power. When using the router, care must be taken on safety issues related to RF interference as well as regulations of RF equipment.
- Do not use your router in aircraft, hospitals, petrol stations or in places where using cellular products is prohibited.
- Be sure that the router will not be interfering with nearby equipment. For example: pacemakers or medical equipment. The antenna of the router should be away from computers, office equipment, home appliance, etc.
- An external antenna must be connected to the router for proper operation. Only uses approved antenna with the router. Please contact authorized distributor on finding an approved antenna.
- Always keep the antenna with minimum safety distance of 20 cm or more from human body. Do not put the antenna inside metallic box, containers, etc.
- RF exposure statements
  1. For mobile devices without co-location (the transmitting antenna is installed or located more than 20cm away from the body of user and nearby person)
- 2. FCC RF Radiation Exposure Statement
    1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
    2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and human body.

Note: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Router may be used at this time.

Using the router in vehicle

- Check for any regulation or law authorizing the use of cellular devices in vehicle in your country before installing the router.

- The driver or operator of any vehicle should not operate the router while driving.
- Install the router by qualified personnel. Consult your vehicle distributor for any possible interference of electronic parts by the router.
- The router should be connected to the vehicle's supply system by using a fuse-protected terminal in the vehicle's fuse box.
- Be careful when the router is powered by the vehicle's main battery. The battery may be drained after extended period.

Protecting your router

To ensure error-free usage, please install and operate your router with care. Do remember the following:

- Do not expose the router to extreme conditions such as high humidity / rain, high temperature, direct sunlight, caustic / harsh chemicals, dust, or water.
- Do not try to disassemble or modify the router. There is no user serviceable part inside and the warranty would be void.
- Do not drop, hit or shake the router. Do not use the router under extreme vibrating conditions.
- Do not pull the antenna or power supply cable. Attach/detach by holding the connector.
- Connect the router only according to the instruction manual. Failure to do it will void the warranty.
- In case of problem, please contact authorized distributor.

Regulatory and Type Approval Information

Table 1: Directives

2011/65/EC	The European RoHS 2.0 2011/65/EU Directive was issued by the European parliament and the European Council on 1 July 2011 on the restriction of the use of certain Hazardous substances in electrical and electronic equipment.
2012/19/EU	The European WEEE 2012/19/EU Directive was issued by the European parliament and the European Council on 24 July 2012 on waste electrical and electronic equipment.
2013/56/EU	The European 2013/56/EU Directive is a battery Directive which published in the EU official gazette on 10 December 2013. The button battery used in this product conforms to the standard of 2013/56/EU directive.

Table 2: Toxic or hazardous substances or elements with defined concentration limits

Name of the part	Hazardous substances										
	(Pb)	(Hg)	(Cd)	(Cr (VI))	(PBB)	(PBDE)	(PBDE)	(DEHP)	(BBP)	(DBP)	(DIBP)
Metal Parts	o	o	o	o	o	o					
Circuit Modules	x	o	o	o	o	o					
Cables and Cable Assemblies	o	o	o	o	o	o					
Plastic and Polymeric parts	o	o	o	o	o	o					
o: Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006. x: Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part might exceed the limit requirement in SJ/T11363-2006.											

Content

Please note: This is a manual for DSR-211 Series. Please check which model you are using.

1 Product Overview

1.1 Key Features

DSR-211 is a rugged cellular router offering state-of-the-art mobile connectivity for machine to machine (M2M) applications.

- Supports WWAN1, WWAN2, Ethernet WAN, WLAN WAN link backup and ICMP detection
- Supports cold backup, warm backup and load balancing
- Wi-Fi supporting AP mode and Client mode (2.4 GHz/ 5.8 GHz), also supporting Captive Portal
- VPN tunnel - IPsec/ OpenVPN/ GRE/ PPTP/ L2TP/ DMVPN
- Supports DHCP server
- Supports 802.1 Q VLAN Trunk
- Supports APP importing
- Supports IP Pass-through
- Supports Modbus gateway (Modbus RTU/ ASCII to Modbus TCP) and Modbus Master
- Supports TCP Client/ Server, UDP and virtual serial port
- Supports SMS, Email, DO, SNMP trap and DigiLink output event
- Supports SDK (C/ Java/ Python), providing user with programmatic interface
- Supports DigiLink (a centralized M2M management platform for remote monitoring, configuration and firmware upgrade)
- Supports DigiVPN (a Cloud VPN Portal providing easy and secure remote access for PLCs and machines)
- Management via web user interface/ CLI/ SNMP/ DigiLink
- Firmware upgrading via web user interface/ CLI/ USB/ SMS/ DigiLink
- Auto reboot via SMS/ Timing
- Includes built-in real-time clock and watchdog

1.2 Packing Contents

Before installing your DSR-211 Router, verify the kit contents as following.
Note: The following pictures are for illustration purposes only, not based on their actual sizes.

Check your package to make sure it contains the following items:

- DSR-211 x 1 (model optional)
  More details about the antenna interface please refer to 1.3 Specifications section.

- 1x 3-pin 5mm male terminal block with lock for power supply

- 1x 7-pin pluggable terminal block with lock for serial port, I/O and console port

Note: If any of the above items is missing or damaged, please contact your AddSecure sales representative.

Optional accessories (can be purchased separately):

- 3G/4G SMA cellular antenna (Stubby antenna or Magnet antenna optional)

Stubby antenna

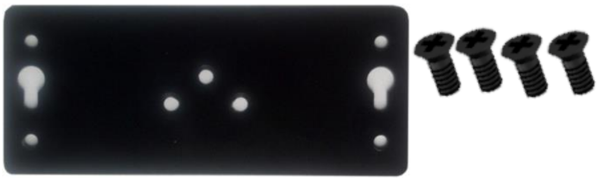
Magnet antenna

- RP-SMA WiFiantenne (Stubby antenna or Magnet antenna optional)

  Stubby antenna

  Magnet antenna

- Wall mounting kit



- 35 mm DIN rail mounting kit

- Ethernet cable x 1

- AC/DC Power Supply Adapter (12 VDC, 1.5A; EU, US, UK, AU plug optional)

1.3 Specifications

Cellular Interface

- Number of antennas: 2 (AUX + MAIN)
- Connector: SMA, female
- SIM: 2 (3.0 V & 1.8 V)
- Standards: GSM/GPRS/EDGE/WCDMA/HSDPA/HSUPA/HSPA+/DC HSPA+/TD SCDMA/CDMA (CDMA 1X/EVDO)/FDD LTE/TDD LTE

GSM: max DL/ UL = 9.6/ 2.7 Kbps
GPRS: max DL/ UL = 86 Kbps
EDGE: max DL/ UL = 236.8 Kbps
WCDMA/TD-SCDMA: max DL/UL = 2.8 Mbps/384 Kbps
EVDO: max DL/UL = 5.4 Mbps/ 14.7 Kbps
HSPA+: max DL/UL = 21/5.76 Mbps, fallback to 2G
DC HSPA+: max DL/UL = 42/5.76 Mbps, fallback to 2G
FDD LTE: max DL/UL = 100/50 Mbps, fallback to 2G/ 3G
TDD LTE: max DL/UL = 100/50 Mbps, fallback to 2G/ 3G

Ethernet Interface

- Number of ports: 2 x 10/100 Mbps, 2 x LAN or 1 x LAN + 1 x WAN
- Magnet isolation protection: 1.5 KV

WiFi Interface (Optional)

- Number of antennas: 1
- Connector: RP-SMA, male
- Standards: 802.11a/ b/ g/ n, supporting AP and Client mode
- Frequency bands: 2,4 GHz
  5 GHz
- Security: Open ,WPA, WPA2, WEP
- Encryption: AES, TKIP, WEP64
- Data speed: Up to 150 Mbps
- Receiving sensitivity: 1 M -97 dBm (< 8%PER)

(+/ - 1 dBm)	54 Mbps	-76.5 dBm (< 10%PER)
	MCS7 (20 MHz)	-72 dBm (< 10%PER)
	MCS7 (40 MHz)	-69 dBm (< 10%PER)

GPS & GLONASS Interface (Optional)

- Number of antennas: 1
- Connector: SMA, female with 50 ohms impedance
- Tracking sensitivity: GPS: greater than -148 dBm
  GLONASS: greater than -140 dBm
- Horizontal position accuracy: GPS: 2.5 m
  GLONASS: 4.0 m
- Protocol: NMEA-0183 V2.3

Serial Interface

- Number of ports: 1 x RS-232 + 1 x RS-485 or 2 x RS-232 or 2 x RS-485
- Connector: 3.5 mm terminal block with lock
- ESD protection: ±15 KV
- Parameters: 8E1, 8O1, 8N1, 8N2, 7E2, 7O2, 7N2, 7E1
- Baud rate: 300 bps to 230400 bps
- RS-232: TxD, RxD, RTS, CTS, GND
- RS-485: Data+ (A), Data- (B)

Digital Input / Digital Output

- Type : 2 x DI (dry contact) + 2 x DO (wet 4 x DI, 4 x DO, 3 x DI + 1 x DO or 3 x DO + 1 x DI
- Connector: 3.5 mm terminal block with lock
- Isolation: 3KVDCor 2KVrms
- Absolute maximum VDC: “ V+” +5 VDC(DI), 30 VDC(DO)
- Absolute maximum ADC: 300 mA
- Digital filtering time interval: software selectable

Others

- 1 x RST button
- 1 x Micro SD interface
- 1 x USB 2.0 host up to 480 Mbps
- 1 x CLI interface
- LED indicators - 1 x RUN, 1 x PPP, 1 x USR, 1 x RSSI, 1 x NET, 1 x SIM

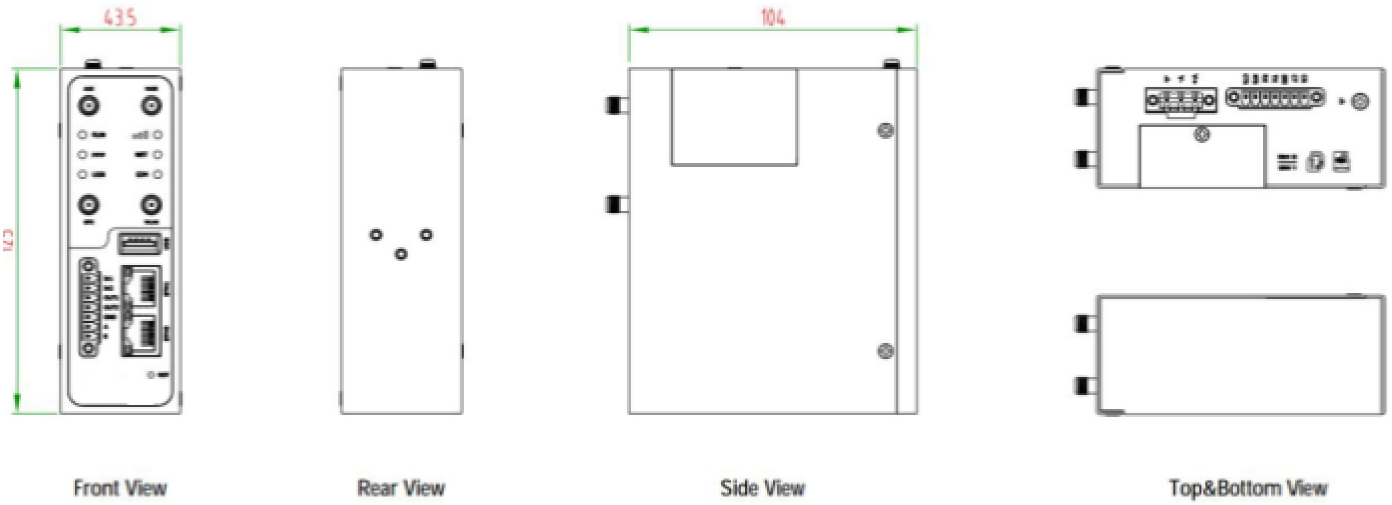
Power Supply and Consumption

- Connector : 3 pin 5 mm female socket with lock
- Input voltage: 9 to 60V DC
- Power consumption: Idle: 100 mA@12 V Data link: 400 mA (peak) @12 V

Physical Characteristics

- Housing & Weight: Metal, 570 g
- Ingress protection: IP30
- Dimension: 125 mm x 104 mm x 43,5 mm
- Installation: desktop, wall mounting or 35 mm DIN rail mounting

1.4 Dimensions



Front View

Rear View

Side View

Top&Bottom View

1.5 Warning

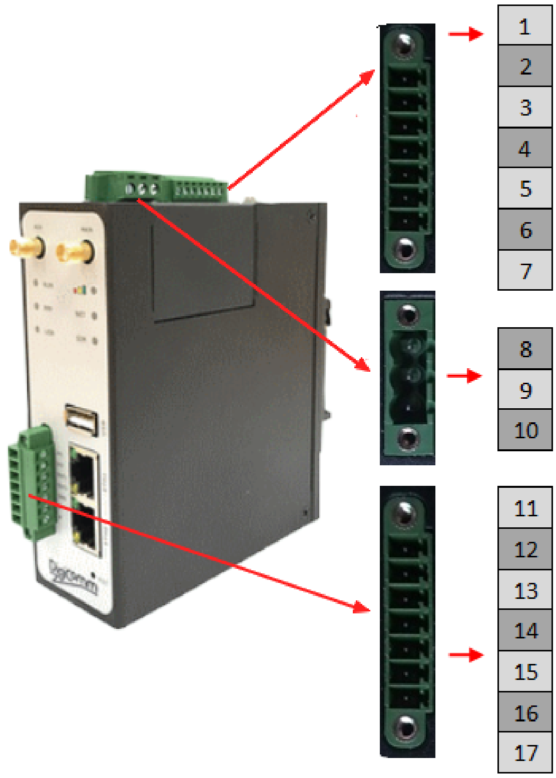
WARNING

EXPLOSION HAZAD. DO NOT REMOVE OR REPLACE WHILE CIRCUIT IS LIVE UNLESS THE AREA IS FREE OF IGNITIBLE CONCENTRATIONS.

Please check which model you are using. The Accessories can differ depending on device.

2. Hardware Installation

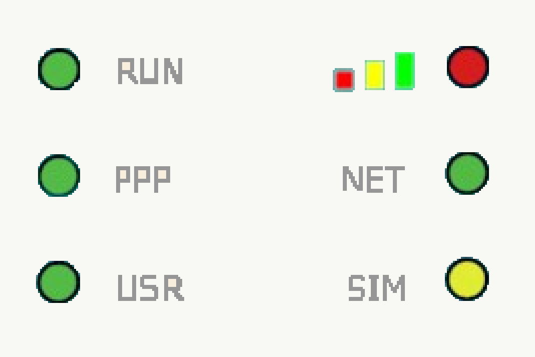
2.1 Pin Assignment

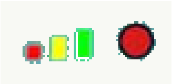


PIN	Debug	RS232	Direction
1	RXD		Device → DSR-211
2	TXD		DSR-211→ Device
3	GND	GND	
4		TXD	DSR-211→ Device
5		RXD	Device →DSR-211
6		RTS	DSR-211→ Device
7		CTS	Device →DSR-211

PIN	Power	Digital I/O	RS485	Direction
8	Positive			
9	Negative			
10	GND			
11		Input 1		DSR-211 – Device
12		Input 2		DSR-211← Device
13		Output 1		DSR-211 › Device
14		Output 2		DSR-211→ Device
15		GND		
16			Data+(A)	DSR-211→ Device
17			Data- (B)	DSR-211 → Device

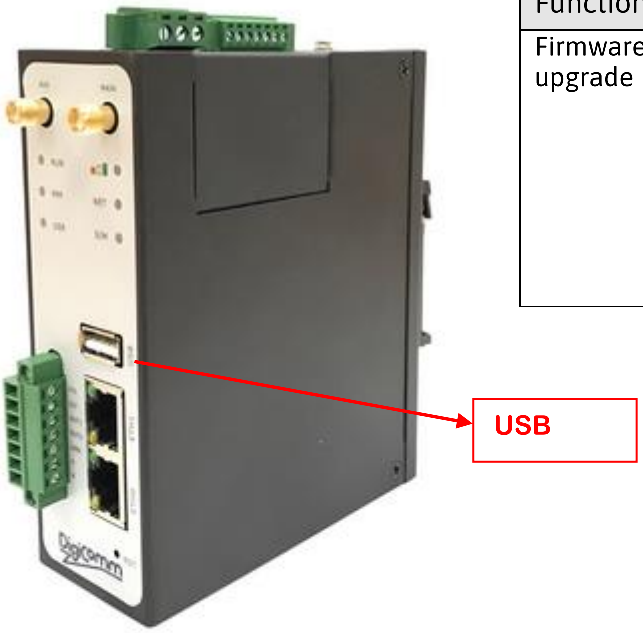
2.2 LED Indicators



Name	Color	Status	Description
RUN	Green	On, fast blinking (250 mSec blink time)	Router is powered on (the system is initializing)
		On, blinking (500 mSec blink time)	Router starts operating
		Off	Router is powered off
PPP	Green	On, solid	Link connection is working
		Off	Link connection is not working
USR-OpenVPN	Green	On, solid	OpenVPN connection is established
		Off	OpenVPN connection is not established
USR-IPsec	Green	On, solid	IPsec connection is established
		Off	IPsec connection is not established
USR-WiFi	Green	On, solid	Wi-Fi is enabled and working properly
		Off	Wi-Fi is disabled or not working properly
	Green	On, solid	High Signal strength (21-31) is available
	Yellow	On, solid	Medium Signal strength (11-20) is available
	Red	On, solid	Low Signal strength (1-10) is available
	--	Off	No signal
NET	Green	On, solid	Connection to 4G network is established
	Yellow	On, solid	Connection to 3G network is established
	Red	On, solid	Connection to 2G network is established
	--	Off	Connection to network is not established or establishing
SIM	Green	On, blinking	The router is using the backup card
		Off	The router is using the main card

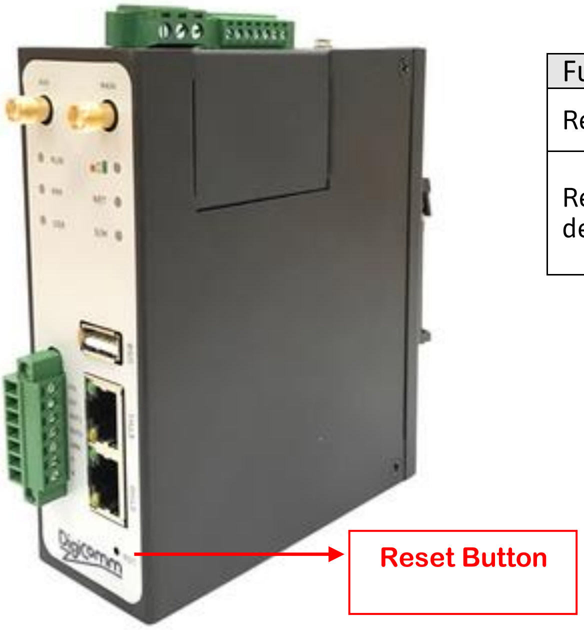
Note: You can choose the display type of USR LED. For more details, please refer to 3.30 Service > Advanced.

2.3 USB Interface



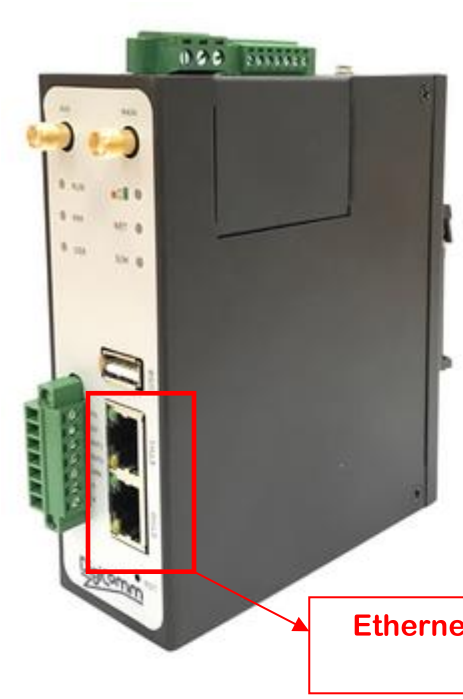
Function	Operation
Firmware upgrade	USB interface is used for batch firmware upgrading, but cannot be used for sending or receiving data from slave devices which connected to it. You can insert a USB storage device into the router's USB interface, such as a U disk or a hard disk. If there have a supported configuration file or a router firmware in this USB storage device, the router will automatically update the configuration file or the firmware. For more details, see 3.11 Interface > USB

2.4 Reset Button



Function	Operation
Reboot	Press and hold the RST button for at least 5 seconds under the operating status.
Restore to factory default setting	Wait for 5 seconds after powering up the router, press and hold the RST button until all six LEDs start blinking one by one, and release the button to return the router to factory defaults.

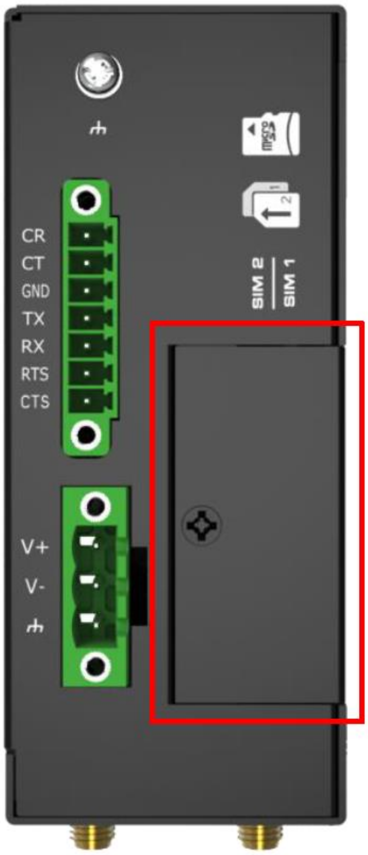
2.5 Ethernet Ports

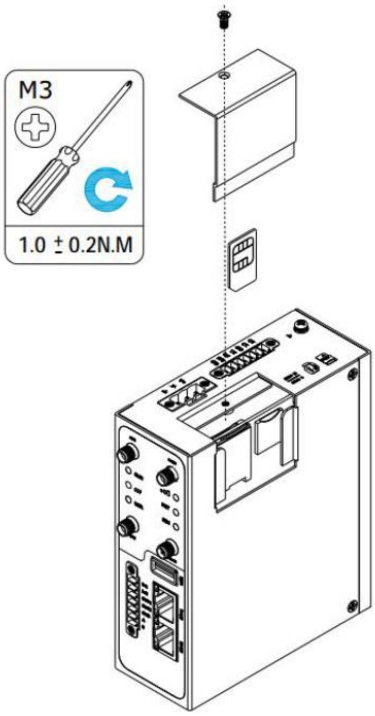


There are two Ethernet ports on DSR-211 Router, including ETH0 and ETH1. Each Ethernet port hast two LED indicators (refer to the left figure). The yellow one is Link Indicator, while the green one is speed Indicator. For details about status, see the table below.

Indicator	Status	Description
Speed Indicator	On, solid	100 Mbps mode
	Off	10 Mbps mode
Link Indicator	On, solid	Connection is established
	On, blinking	Data is being transferred
	Off	Connection is not established

2.6 Insert or remove SIM Card/ Micro SD Card





Insert or remove the SIM/Micro SD card as shown in the following steps.

- Insert SIM card/Micro SD card

1. Make sure router is powered off
2. To remove slot cover, loosen the screws associated with the cover by using a screwdriver and then find the SIM card slot/SD card slot.
3. To insert SIM card/Micro SD card, press the card with finger until you hear a click and then tighten the screws associated with the cover by using a screwdriver.
4. To put back the cover and tighten the screws associated with the cover by using a screwdriver.

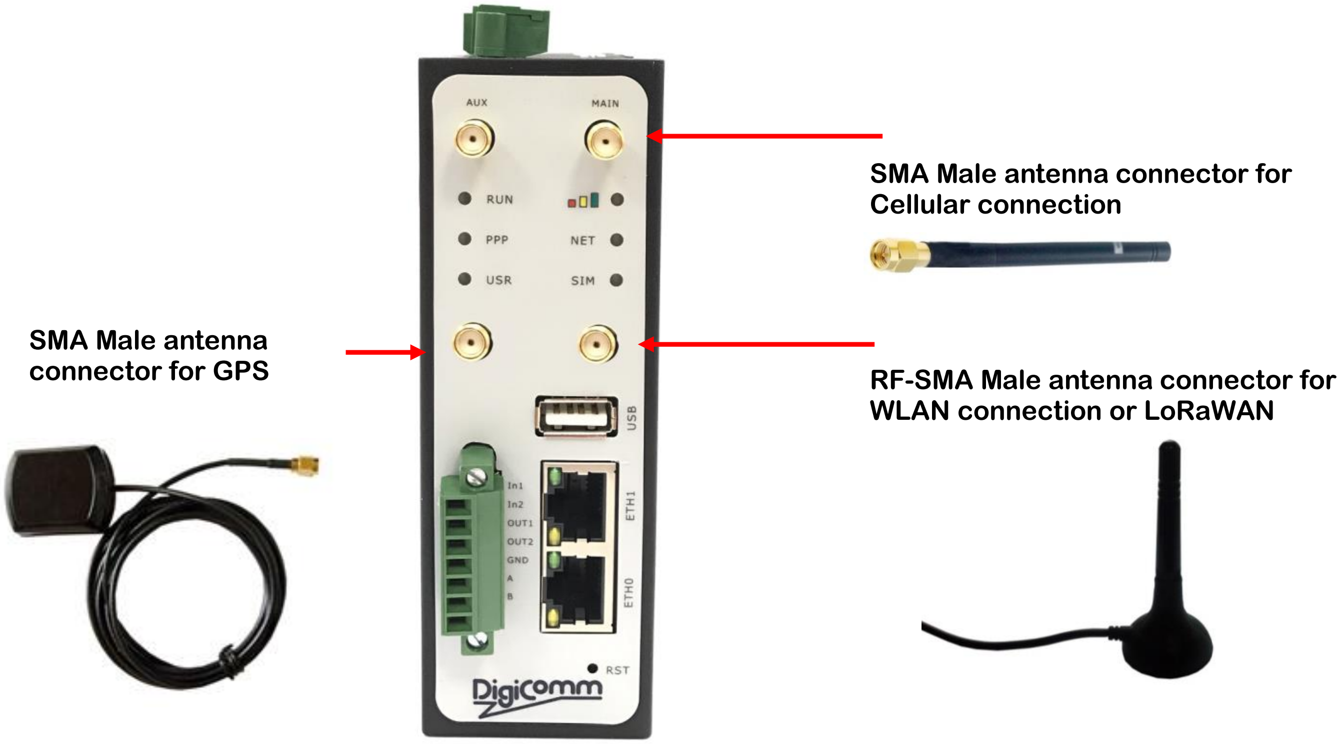
- Remove SIM card Micro SD card

1. Make sure router is powered off.
2. To remove slot cover, loosen the screws associated with the cover by using a screwdri ver and then find the SIM card slot/SD card slot.
3. To remove SIM card/Micro SD card, p ress the card with finger until it pops out and then take out the card.
4. To put back the cover and tighten the screws associated with the cover by using a screwdriver.

Note:
1. Recommended torque for inserting is 0.5 N.m, and the maximum allowed is 0.7 N.m.
2. Use the specific card when the device is working in extreme temperature (temperature exceeding 40°C), because the regular card for long-time working in harsh environment will be disconnected frequently.
3. Do not forget to twist the cover tightly to avoid being stolen.
4. Do not touch the metal of the card surface in case information in the card will loseor be destroyed.
5. Do not bend or scratch the card.
6. Keep the card away f rom electricity and magnetism.
7. Make sure router is powered off before inserting or removing the card.

2.7 Attach External Antenna (SMA Type)

Attach the SMA external antenna to the router’s connector and twist tightly. Make sure the antenna is within the correct frequency range provided by the ISP and with 50 Ohm impedance.
Note: Recommended torque for tightening is 0.35 N.m.

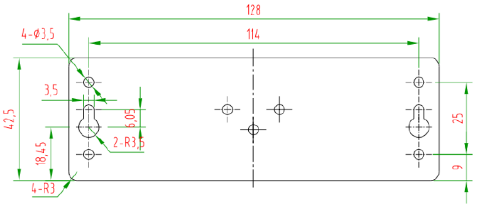

SMA Male antenna connector for Cellular connection
SMA Male antenna connector for GPS
RF-SMA Male antenna connector for WLAN connection or LoRaWAN
AUX
MAIN
RUN
PPP
NET
USR
SIM
USB
In1
In2
OUT1
OUT2
GND
A
B
ETH1
ETH0
RST
DigiComm

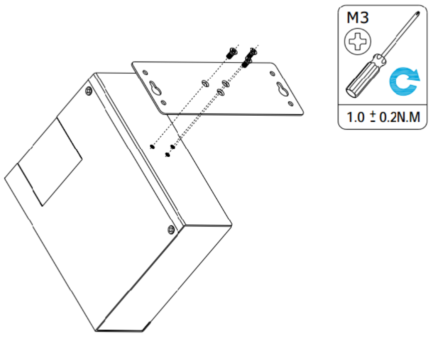
2.8 Mount the Router

The router can be placed on a desktop or mounted to a wall or a 35 mm DIN rail.

Note:
When used, the device needs a suitable environment.
1. If indoors, it needs to be provided an indoor enclosure.
2. If outdoors, it needs to be provided a rain proof enclosure.

Two methods for mounting the router
1. Wall mounting (measured in mm)

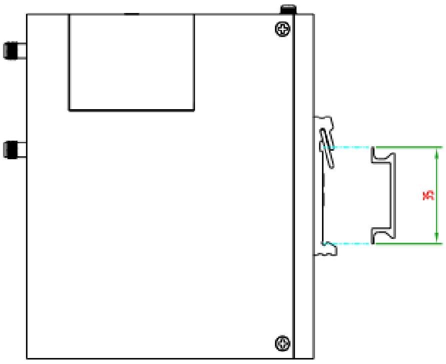


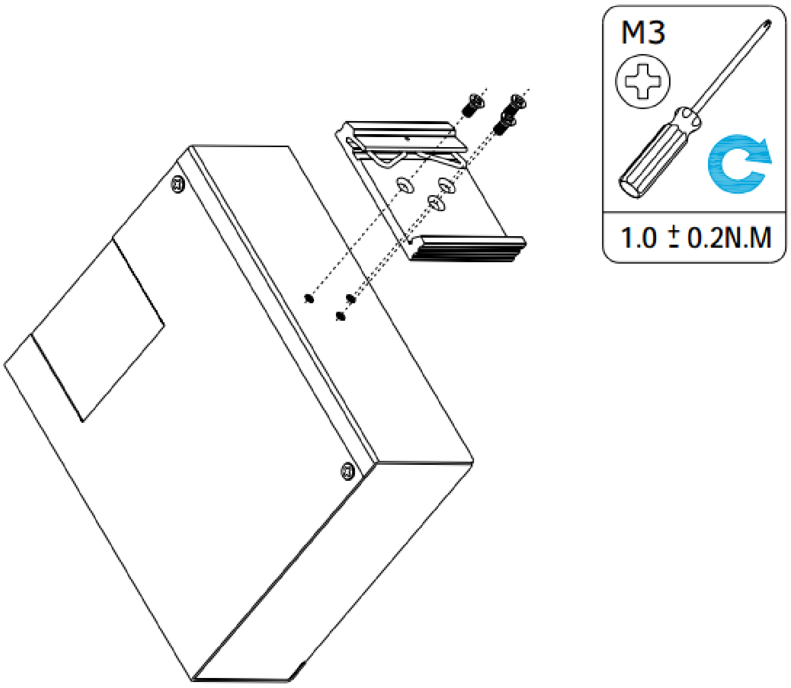


Use 3 pcs of M3*4 flat head screws to fix the wall mounting kit to the router, and then use 2 pcs of M3 drywall screws to mount the router associated with the wall mounting kit on the wall.

Note: Recommended torque for mounting is 1.0 N.m, and the maximum allowed is 1.2 N.m

2. DIN rail mounting (measured in mm)

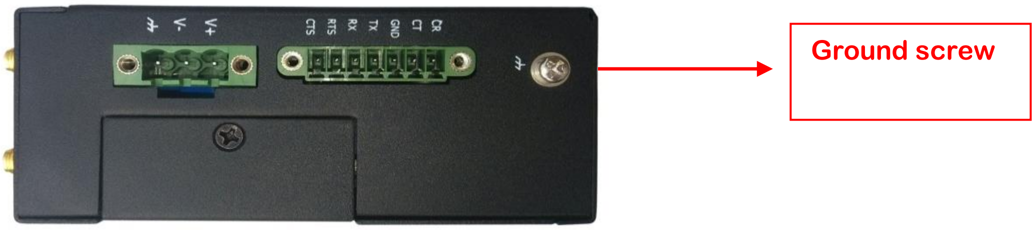




Use 3 pcs of M3*6 flat head screws to fix the DIN rail to the router, and then hang the DIN rail on the mounting bracket. It is necessary to choose a standard bracket.
Note: Recommended torque for mounting is 1.0 N.m, and the maximum allowed is 1.2 N.m.

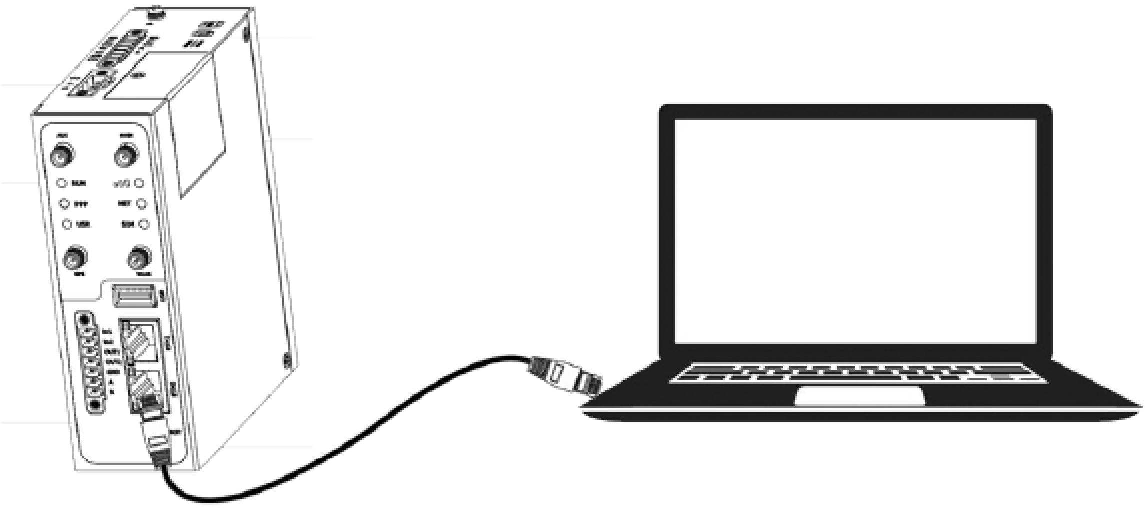
2.9 Ground the Router

Router grounding helps prevent the noise effect due to electromagnetic interference (EMI). Connect the router to the site ground wire by the ground screw before powering on.
Note: This product is appropriate to be mounted on a sound grounded device surface, such as a metal panel.

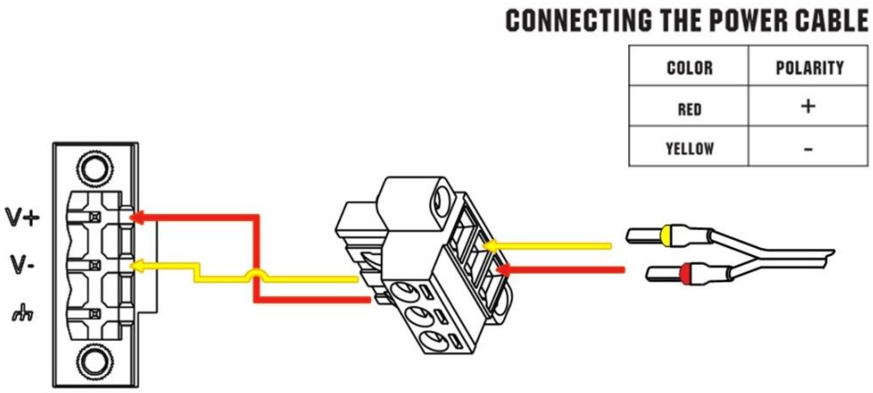


2.10 Connect the Router to a computer

Connect an Ethernet cable to the port marked ETH0 or ETH1 at the front of the DSR-211-L Router, and connect the other end of the cable to your computer



2.11 Power supply



CONNECTING THE POWER CABLE

COLOR	POLARITY
RED	+
YELLOW	-

DSR-211 Router supports reverse polarity protection, but always refers to the figure above to connect the power adapter correctly. There are two cables associated with the power adapter. Following to the color of the head, connect the cable marked red to the positive pole through a terminal block, and connect the yellow one to the negative in the same way. The last step is to plug the power adapter into your socket.
Note: The range of power voltage is 9 to 60V DC.

3. Initial Configuration

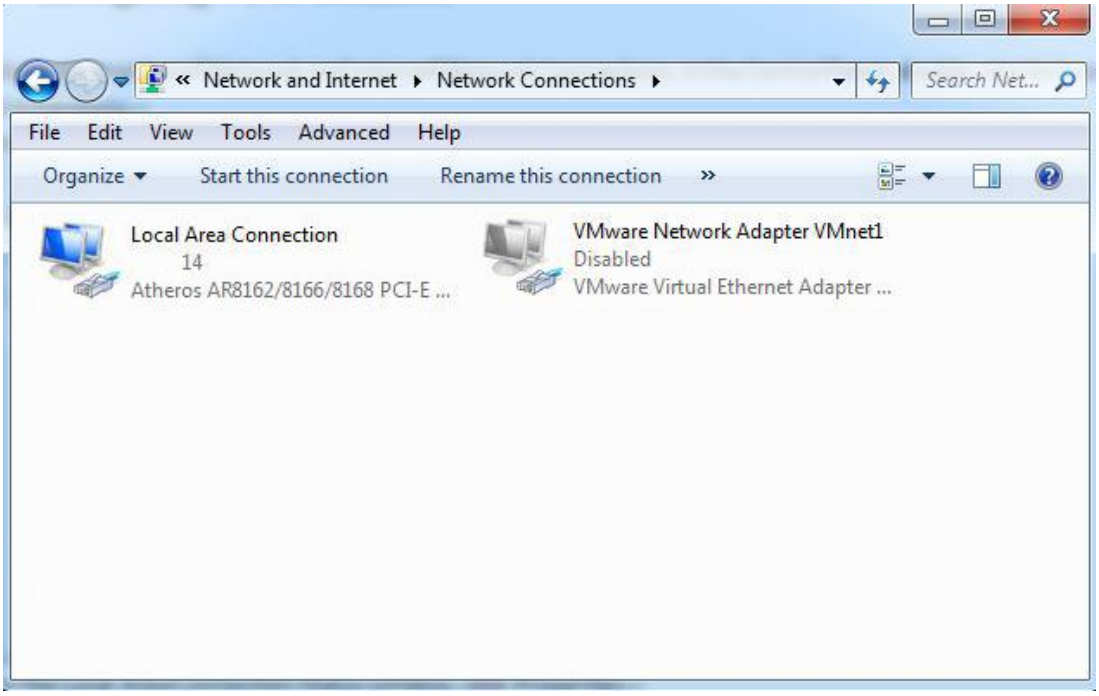
The router can be configured through your web browser that including IE8.0 or above, Chrome and Firefox, etc. a web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows98/ NT/ 2000/ XP/ Me/ Vista/ 7/ 8, etc. It provides an easy and user-friendly interface for configuration. There are various ways to connect the router, either through an external repeater/ hub or connect directly to your PC. However, make sure that your PC has an Ethernet interface properly installed prior to connecting the router. You must configure your PC to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. If you encounter any problems accessing the router web interface, it is advisable to uninstall your firewall program on your PC, as this tends to cause problems accessing the IP address of the router.

3.1 Configure the PC

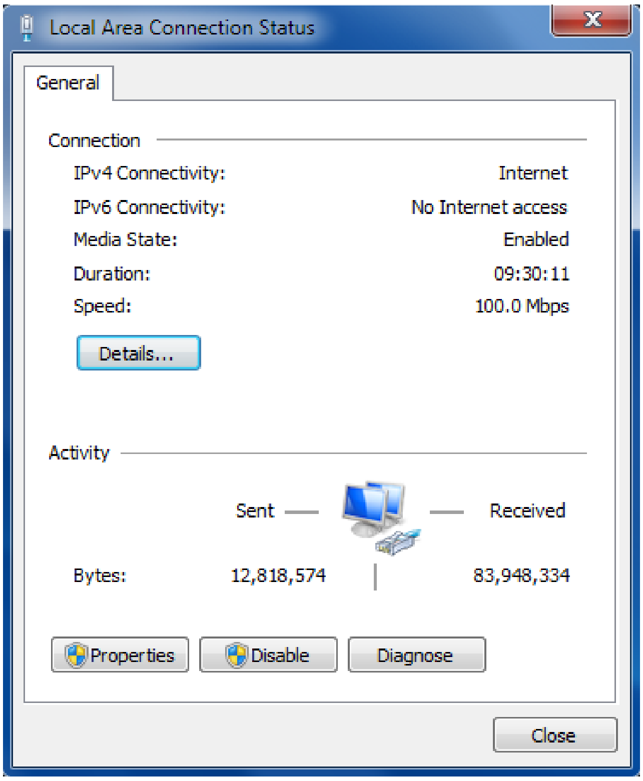
There are two methods to get IP address for the PC. One is to obtain an IP address automatically from “Local Area Connection”, and another is to configure a static IP address manually within the same subnet of the router. Please refer to the steps below.

Here take Windows 7 as example, and the configuration for windows system is similar.

1. Click Start > Control panel, double-click Network and Sharing Center, and then double-click Local Area Connection.


« Network and Internet ▸ Network Connections ▸
Search Net...
File Edit View Tools Advanced Help
Organize ▾ Start this connection Rename this connection »
Local Area Connection
14
Atheros AR8162/8166/8168 PCI-E ...
VMware Network Adapter VMnet1
Disabled
VMware Virtual Ethernet Adapter ...

2. Click Properties in the window of Local Area Connection Status.



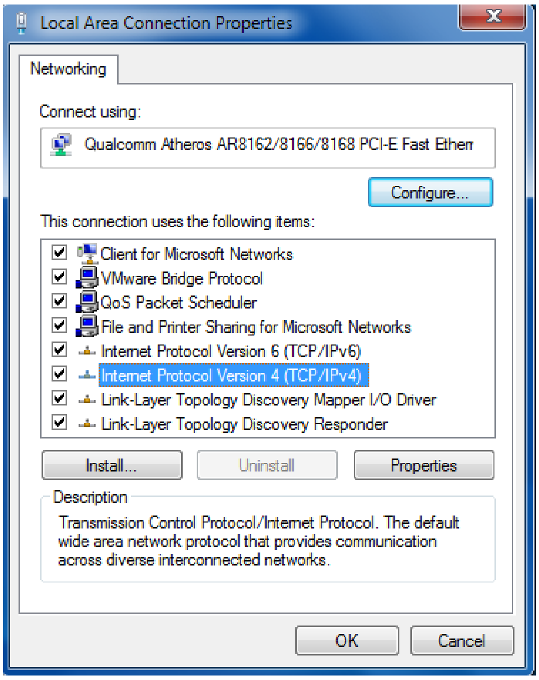
Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No Internet access
Media State:	Enabled
Duration:	09:30:11
Speed:	100.0 Mbps

Activity

	Sent	Received
Bytes:	12,818,574	83,948,334

3. Choose Internet Protocol Version 4 (TCP/ IPv4) and click Properties.



Connect using:

Qualcomm Atheros AR8162/8166/8168 PCI-E Fast Etherr

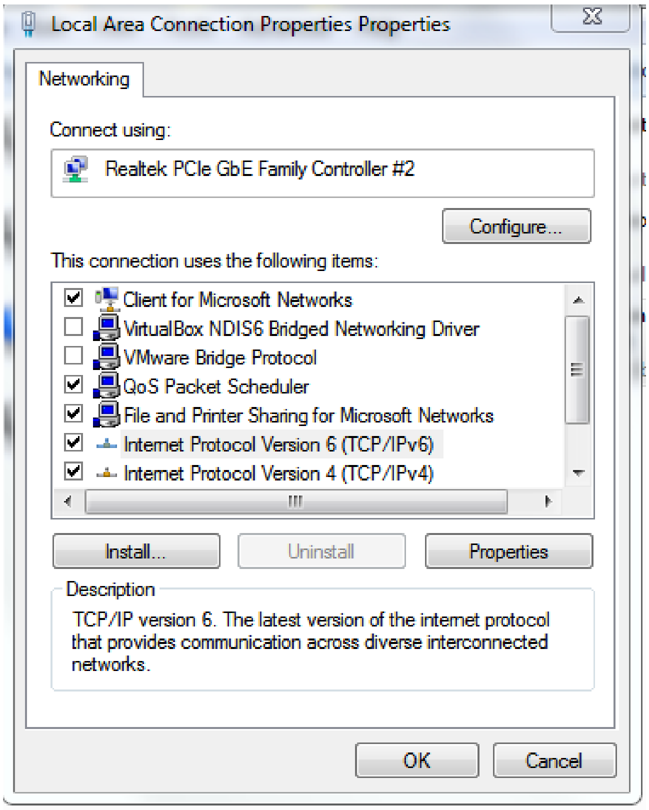
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ VMware Bridge Protocol
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Select Internet protocol version 6 (TCP/IPv6), and click Properties.



Connect using:

Realtek PCIe GbE Family Controller #2

This connection uses the following items:

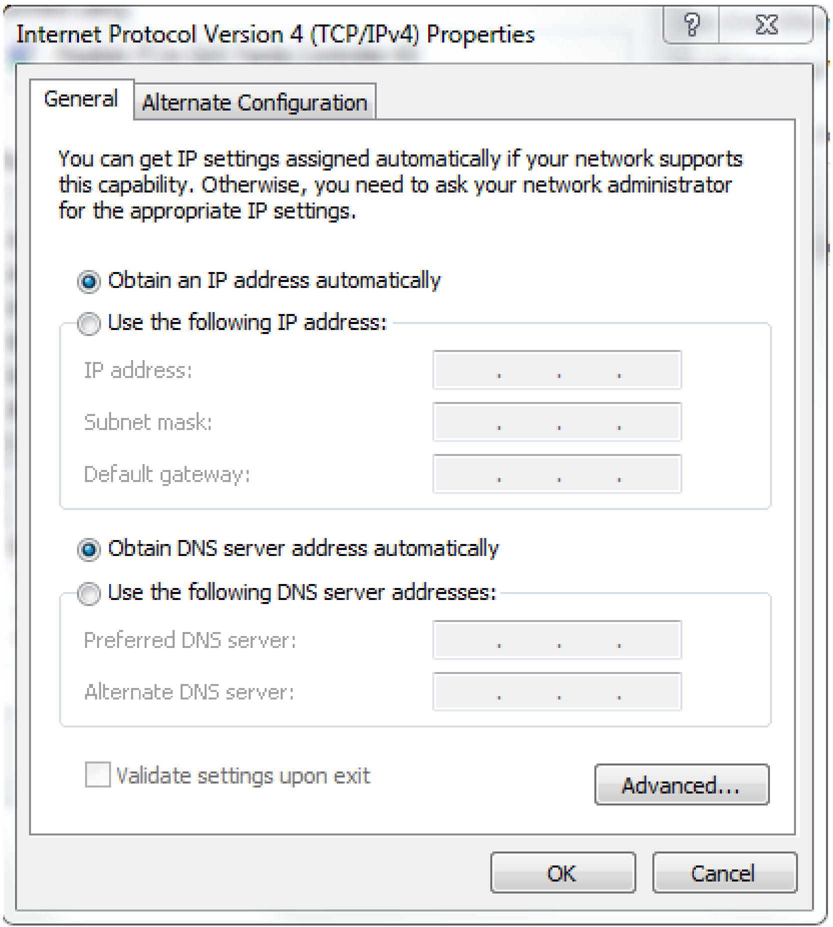
- ☑ Client for Microsoft Networks
- □ VirtualBox NDIS6 Bridged Networking Driver
- □ VMware Bridge Protocol
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

4. Two ways for configuring the IP address of PC

Obtain an IP address automatically:



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

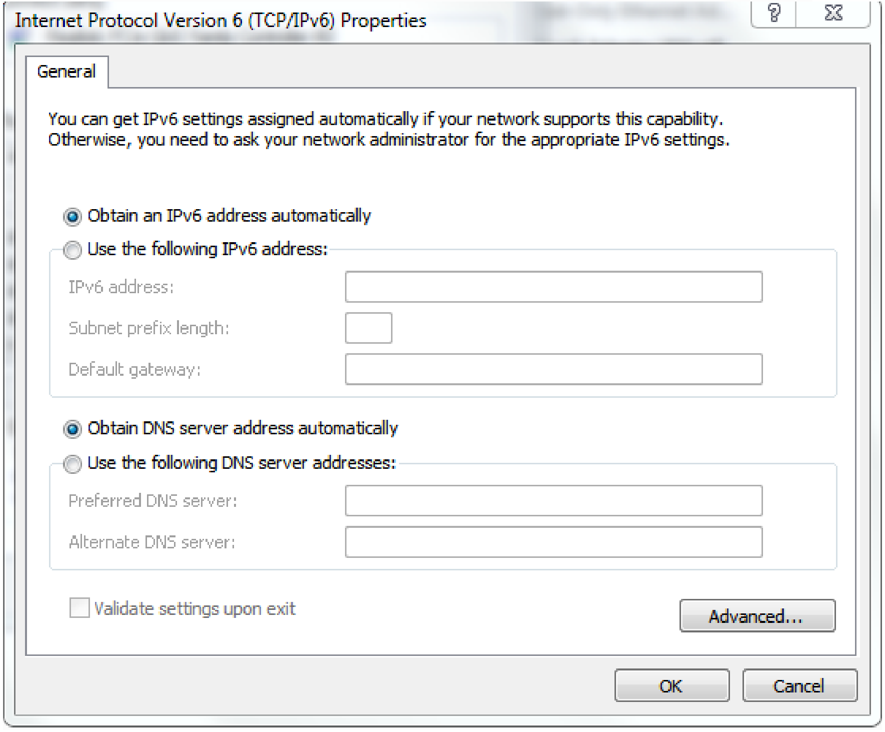
● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit



Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

● Obtain an IPv6 address automatically

○ Use the following IPv6 address:

IPv6 address:

Subnet prefix length:

Default gateway:

● Obtain DNS server address automatically

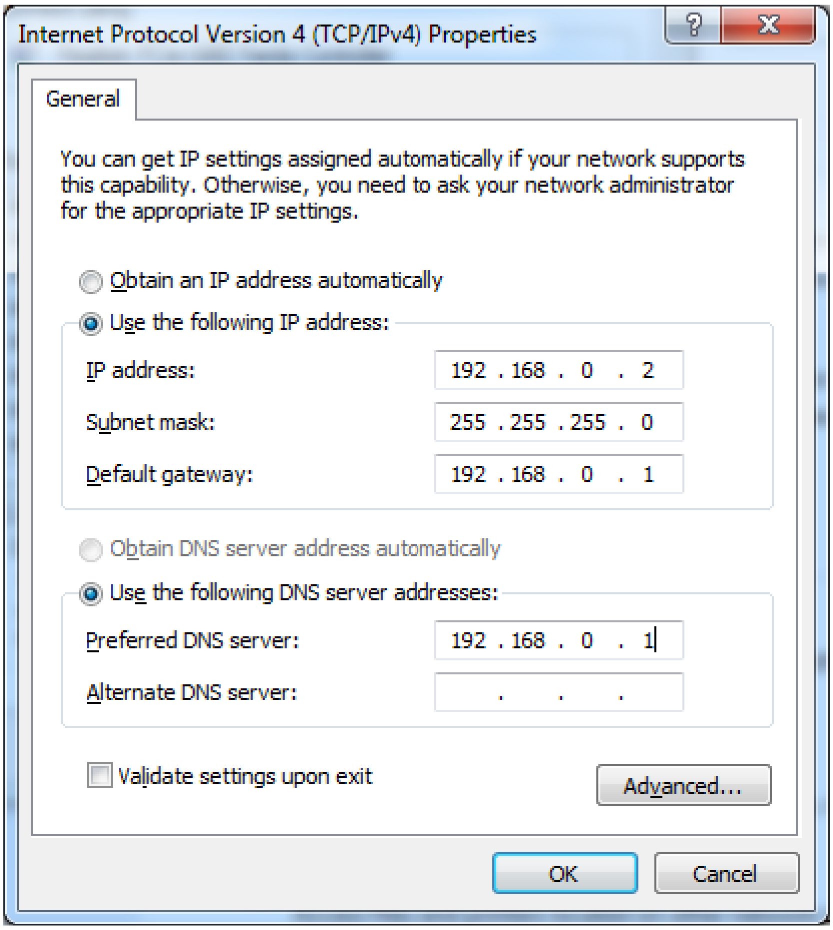
○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

Use the following IP address:
(Configured a static IP address manually within the same subnet of the router)



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

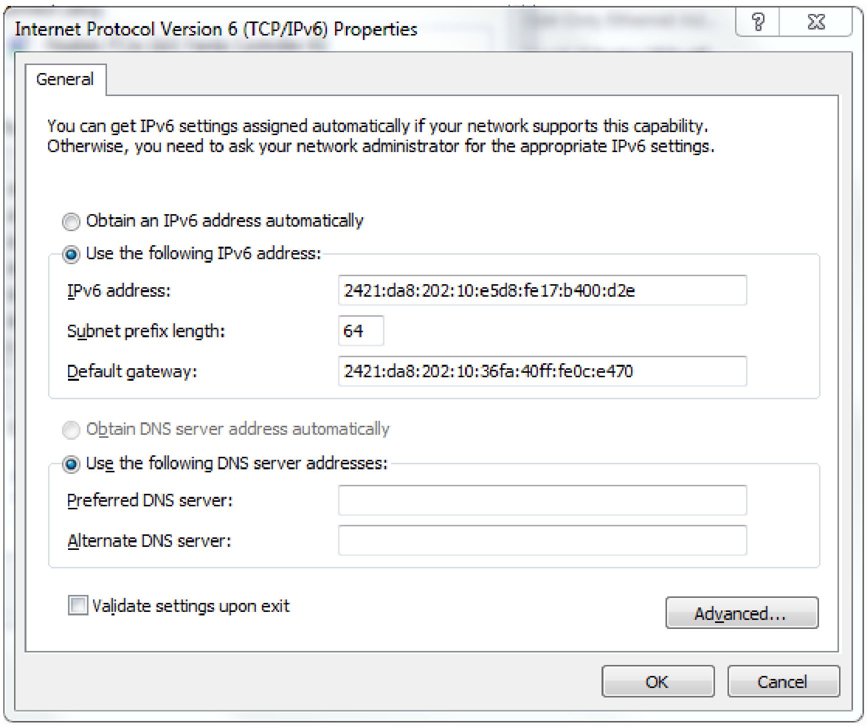
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 1

Alternate DNS server: . . .

□ Validate settings upon exit



Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

○ Obtain an IPv6 address automatically

● Use the following IPv6 address:

IPv6 address: 2421:da8:202:10:e5d8:fe17:b400:d2e

Subnet prefix length: 64

Default gateway: 2421:da8:202:10:36fa:40ff:fe0c:e470

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

5. Click OK to finish the configuration.

3.2 Factory Default Settings

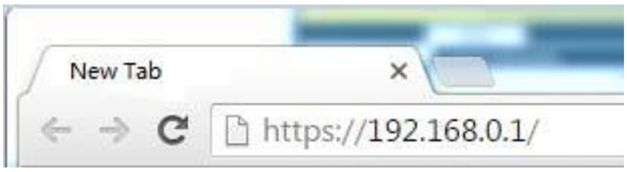
Before configuring your router, you need to know the following default settings.

Item	Description
Username	admin
Password	admin
Eth0	192.168.0.1/255.255.255.0, LAN mode
Eth1	192.168.0.1/255.255.255.0, LAN mode
DHCP Server	Enabled.

3.3 Log in the Router

To log in to the management page and view the configuration status of your router, please follow the steps below.

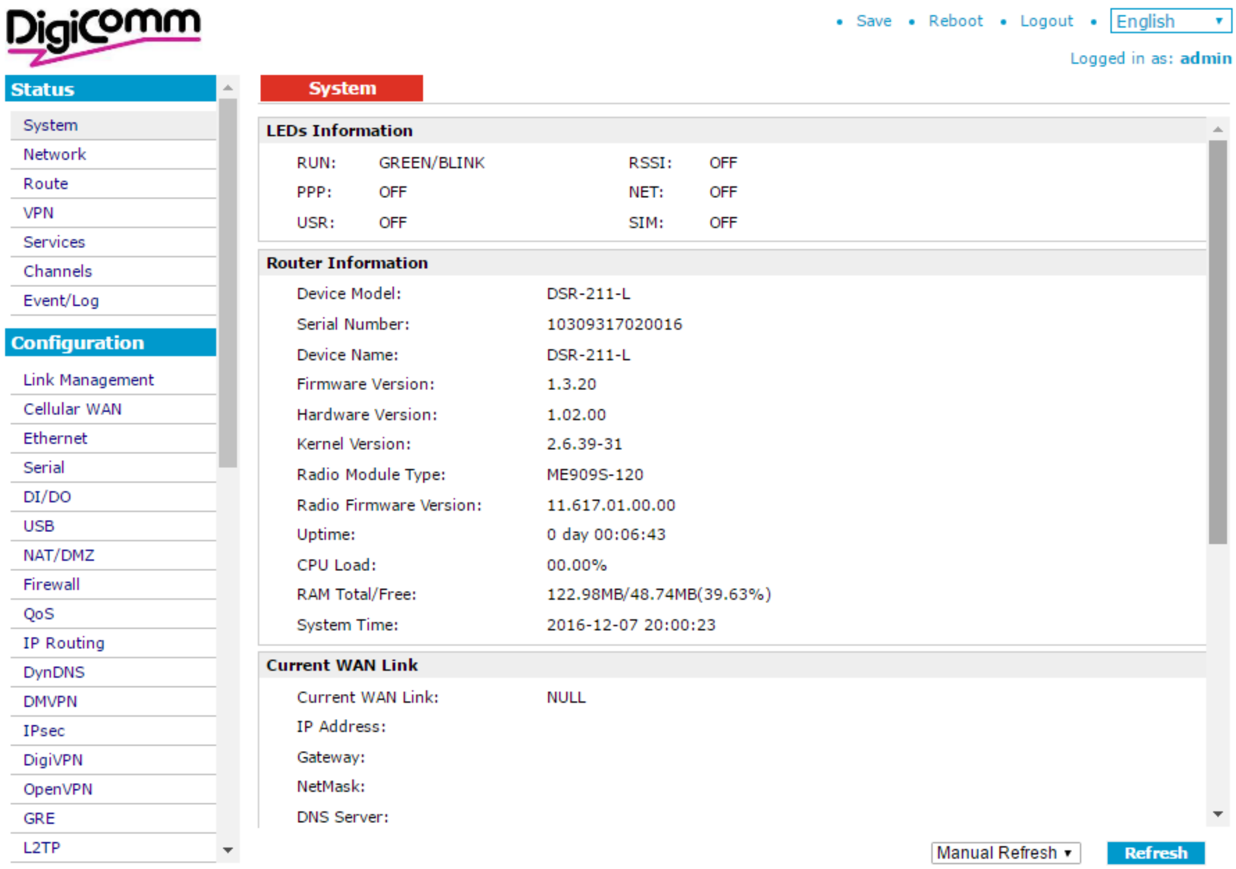
1. On your PC, open a web browser such as Internet Explorer, Google and Firefox, etc.
2. From your web browser, type the IP address of the router into the address bar and press enter.
   The default IP address of DSR-211 Router is 192.168.0.1, though the actual address may vary.



3. In the login page, enter the username and password, choose language and then click LOGIN. The default username and password : admin”.
   Note: If enter the wrong username or password over six times, the login web will be locked for 5 minutes.

3.4 Control Panel

After logging in, the home page of the DSR-211 Router’s web interface is displayed, for example.



LEDs Information

RUN:	GREEN/BLINK	RSSI:	OFF
PPP:	OFF	NET:	OFF
USR:	OFF	SIM:	OFF

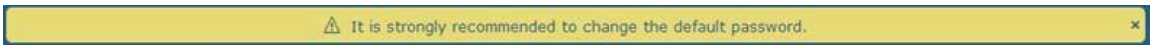
Router Information

Device Model:	DSR-211-L
Serial Number:	10309317020016
Device Name:	DSR-211-L
Firmware Version:	1.3.20
Hardware Version:	1.02.00
Kernel Version:	2.6.39-31
Radio Module Type:	ME909S-120
Radio Firmware Version:	11.617.01.00.00
Uptime:	0 day 00:06:43
CPU Load:	00.00%
RAM Total/Free:	122.98MB/48.74MB(39.63%)
System Time:	2016-12-07 20:00:23

Current WAN Link

Current WAN Link:	NULL
IP Address:	
Gateway:	
NetMask:	
DNS Server:	

From the home page, users can perform operations such as saving configuration, restarting the router, and logging out. Using the original password to log in the router, the page will pop up the following tab


⚠ It is strongly recommended to change the default password. ×

Click × to close the popup . It is strongly recommended for security purposes that you change the default username and/or password. To change your username and/or password, see 3.36 System > User Management

Control Panel		
Item	Description	Button
Save & Apply	Click to save the current configuration into router's flash and apply the modification on every configuration page, to make the modification taking effect.	Save & Apply
Reboot	Click to reboot the router. If the Reboot button is yellow, it means that some completed configurations will take effect only after reboot.	Reboot
Logout	Click to log the current user out safely. After logging out, it will switch to login page. Shut down web page directly without logout, the next one can login web on this browser without a password before timeout.	Logout
Submit	Click to save the modification on current configuration page.	Submit
Cancel	Click to cancel the modification on current configuration page.	Cancel

Note: The steps of how to modify configuration are as bellow:

1. Modify in one page;

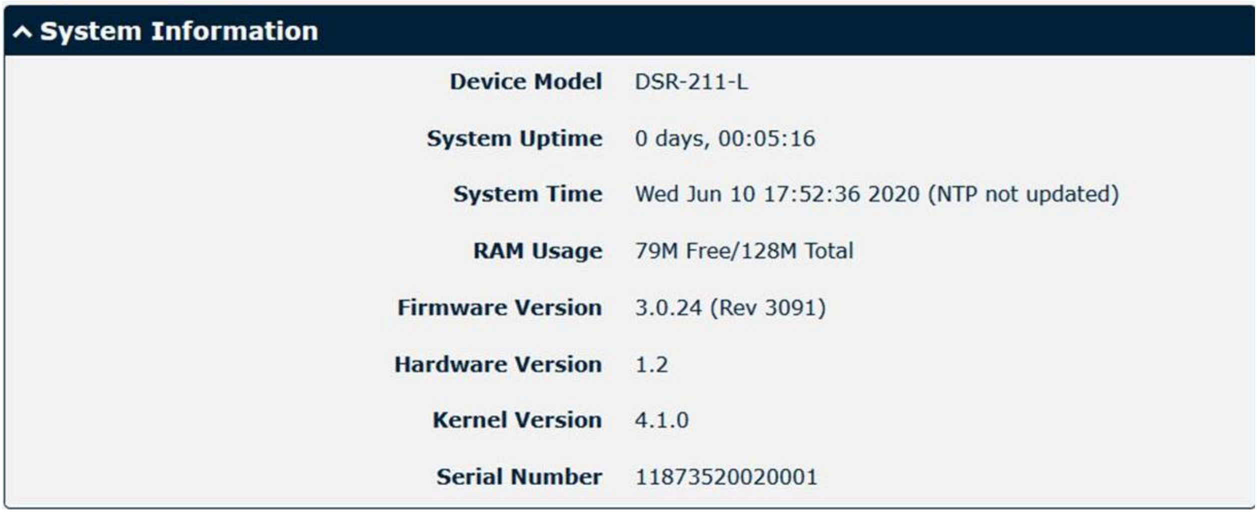
2. Click Submit under this page;

3. Modify in another page;
4. Click Submit under this page;
5. Complete all modification;
6. Click Save & Apply.

3.5 Status

This page allows you to view the System Information, Internet Status and LAN Status of your Router.

System Information

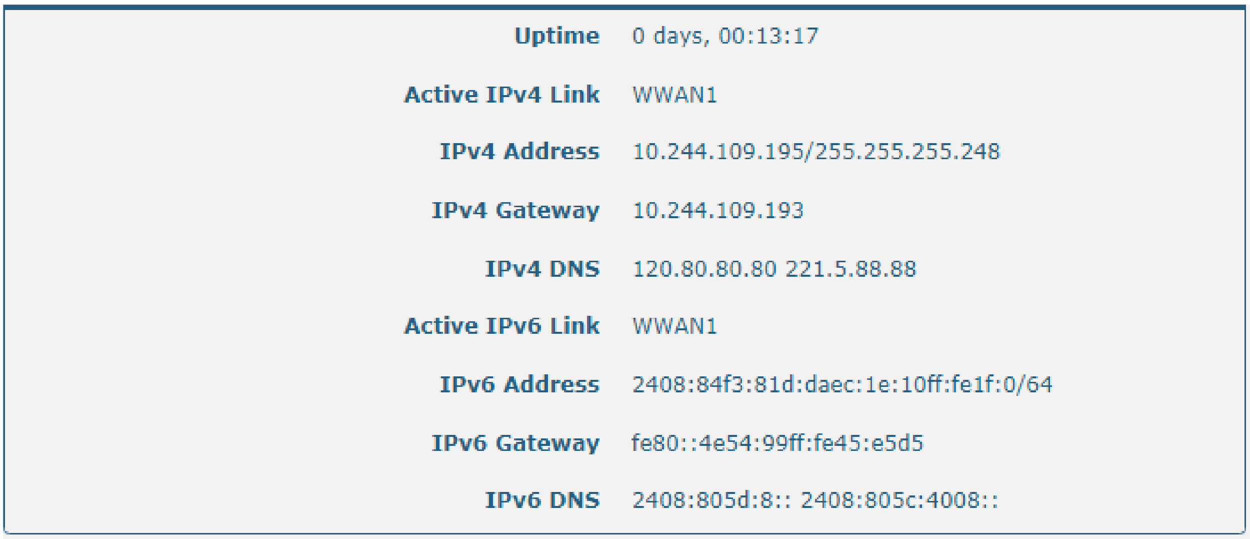


^ System Information

Device Model	DSR-211-L
System Uptime	0 days, 00:05:16
System Time	Wed Jun 10 17:52:36 2020 (NTP not updated)
RAM Usage	79M Free/128M Total
Firmware Version	3.0.24 (Rev 3091)
Hardware Version	1.2
Kernel Version	4.1.0
Serial Number	11873520020001

System information	
Item	Description
Device Model	Show the model name of your device
System Uptime	Show the current amount of time the router has been connected
System Time	Show the current system time
RAM Usage	Show the current RAM usage and total memory
Firmware Version	Show the firmware version running on the router
Hardware Version	Show the current hardware version
Kernel Version	Show the current kernel version
Serial Number	Show the serial number of your device

Internet Status



Uptime 0 days, 00:13:17

Active IPv4 Link WWAN1

IPv4 Address 10.244.109.195/255.255.255.248

IPv4 Gateway 10.244.109.193

IPv4 DNS 120.80.80.80 221.5.88.88

Active IPv6 Link WWAN1

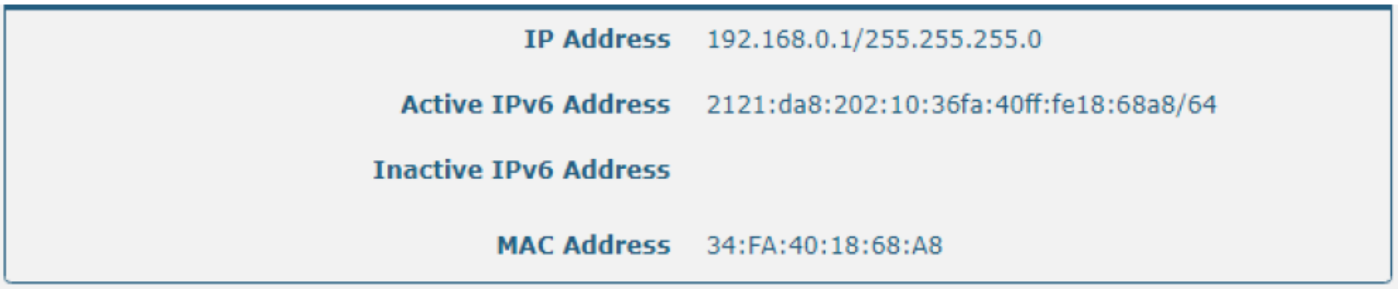
IPv6 Address 2408:84f3:81d:daec:1e:10ff:fe1f:0/64

IPv6 Gateway fe80::4e54:99ff:fe45:e5d5

IPv6 DNS 2408:805d:8:: 2408:805c:4008::

Internet Status	
Item	Description
Uptime	Show the current amount of time the link has been connected.
IPv4 Link Description	Show the currently online link: WWAN1, WWAN2, WAN or WLAN.
IPv4 Address	Show the IPv4 address of current link.
IPv4 Gateway	Show the IPv4 gateway of the current link.
IPv4 DNS	Show the current IPv4 DNS server.
IPv6 Link Description	Show the currently online link: WWAN1, WWAN2, WAN or WLAN.
IPv6 Address	Show the IPv6 address of current link.
IPv6 Gateway	Show the IPv6 gateway of the current link.
IPv6 DNS	Show the current IPv6 DNS server.

LAN Status



IP Address 192.168.0.1/255.255.255.0

Active IPv6 Address 2121:da8:202:10:36fa:40ff:fe18:68a8/64

Inactive IPv6 Address

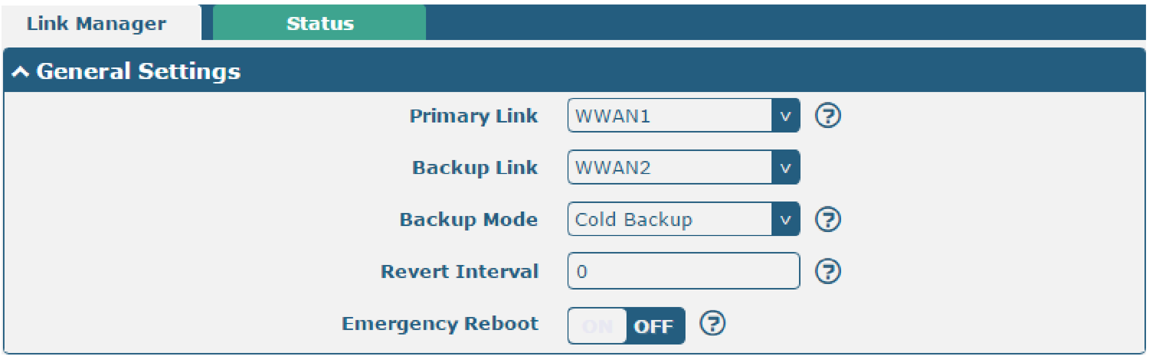
MAC Address 34:FA:40:18:68:A8

LAN Status	
Item	Description
IP Address	Show the IPv4 address and the Netmask of the router.
IPv6 Address	Shows the IPv6 address and prefix length obtained by the router along with the current backup link.
Inactive IPv6 Address	Shows the IPv6 address and prefix length obtained by the router along with the current online link.

MAC Address	Show the MAC address of the router.

3.6 Interface > Link Manager

This section allows you to setup the link connection.



Primary Link: WWAN1

Backup Link: WWAN2

Backup Mode: Cold Backup

Revert Interval: 0

Emergency Reboot: ON OFF

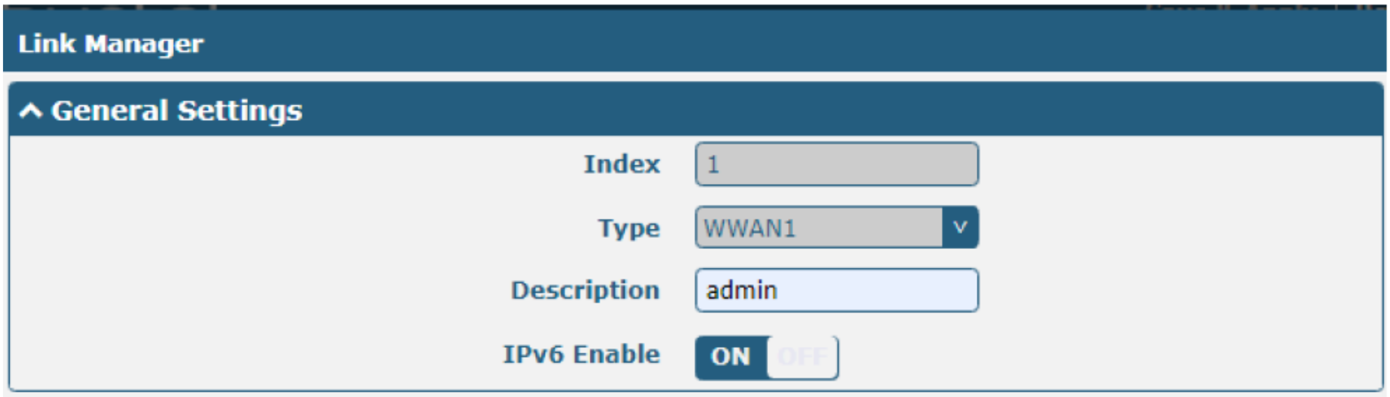
General Settings @ Link Manager		
Item	Description	Default
Primary Link	Select from “WWAN1” , “ WWAN2” , “ WAN” or “ WLAN” . WWAN1: Select to make SIM1 as the primary wireless link WWAN2: Select to make SIM2 as the primary wireless link WAN: Select to make WAN Ethernet port as the primary wired link Note: WAN link is available only if enable eth0 as WAN port in Interface > Ethernet > Ports > Port Settings. WLAN: Select to make WLAN as the primary wireless link Note: WLAN link is available only if enable Wi-Fi as Client mode, please refer to 3.10 Interface > Wi-Fi.	WWAN1
Backup Link	Select from “ None” , “ WWAN1” , “ WWAN2” , “ WAN” or “ WLAN” . None: Do not select any backup link WWAN1: Select to make SIM1 as backup wireless link WWAN2: Select to make SIM2 as backup wireless link WAN:Select to make WAN Ethernet port as the backup wired link Note: WAN link is available only if enable eth0 as WAN interface Interface > Ethernet > Ports > Port Settings. WLAN: Select to make WLAN as the backup wireless link Note: WLAN link is available only if enable Wi-Fi as Client mode, please refer to 3.10 Interface > Wi-Fi.	WWAN2
Backup Mode	Select from “Cold Backup”, “ Warm Backup” or “ Load Balancing” . Cold Backup: The inactive link is offline on standby Warm Backup: The inactive link is online on standby Note: Warm backup mode is not available for dual SIM backup. Load Balancing: Use two links simultaneously	Cold Backup
Revert Interval	Specify the number of minutes that elapses before the primary link is checked if a backup link is being used in cold backup mode. 0 means disable checking. Note: Revert interval is available only under the cold backup mode.	0
Emergency Reboot	Enable to reboot the whole system if no links available.	OFF

Note: Click ⓘ for help.

Link Settings allows you to configure the parameters of link connection, including WWAN1/ WWAN2, WAN and WLAN. It is recommended to enable Ping detection to keep the router always online. The Ping detection increases the reliability and also costs the data traffic.

Click ✎ on the right-most of WWAN1/ WWAN2 to enter the configuration window.

WWAN1/ WWAN2

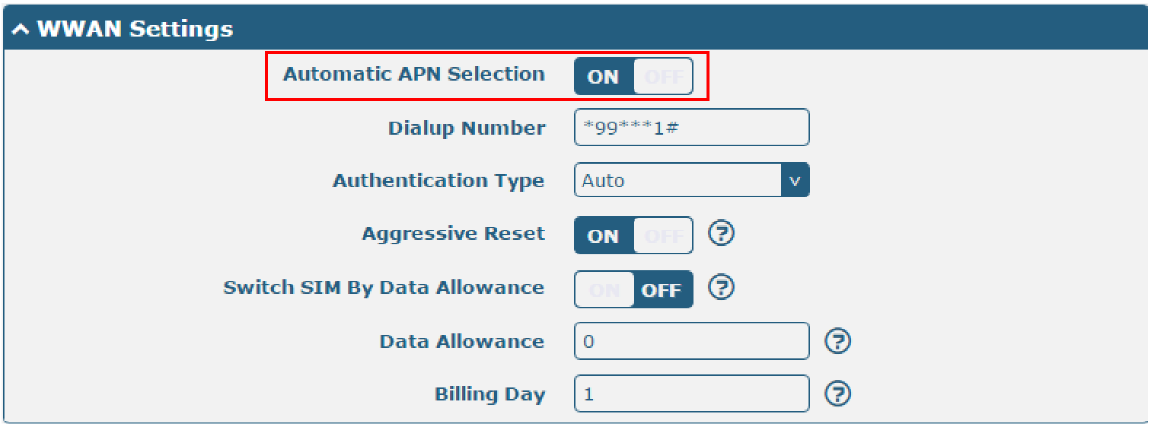


Link Manager

General Settings

Index	1
Type	WWAN1
Description	admin
IPv6 Enable	ON

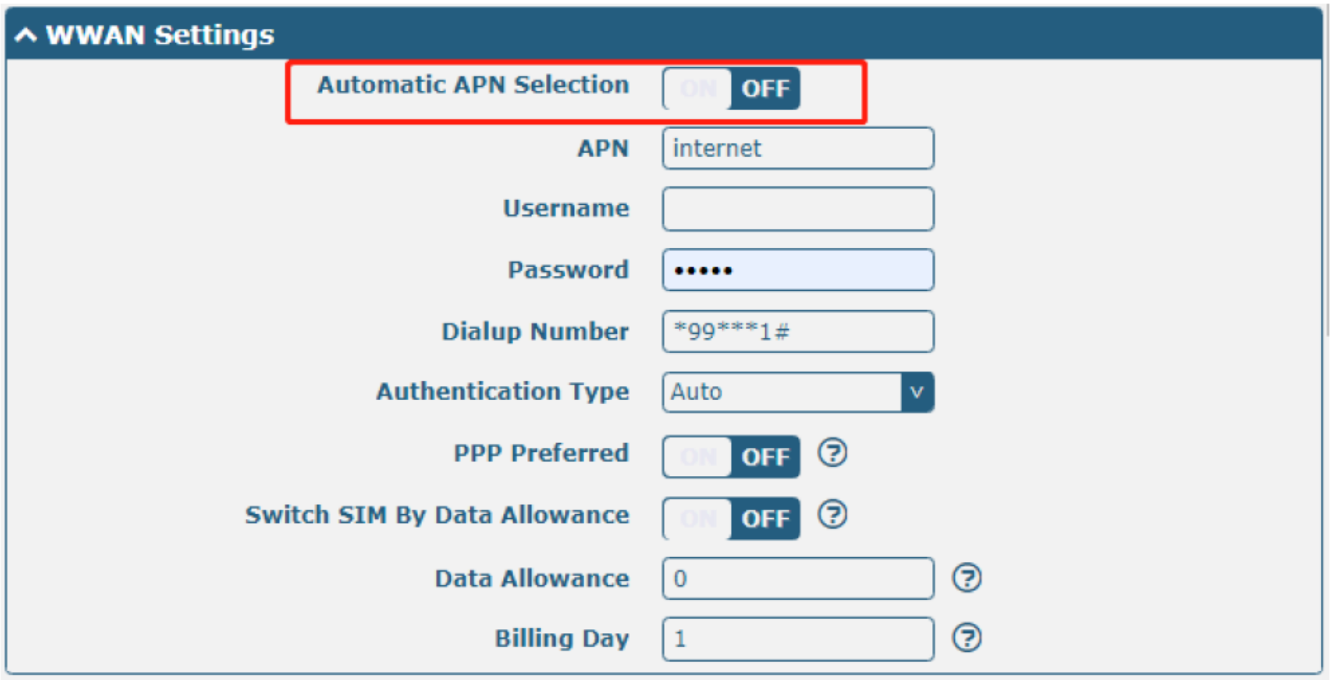
The window is displayed as below when enabling the “Automatic APN Selection” option.



WWAN Settings

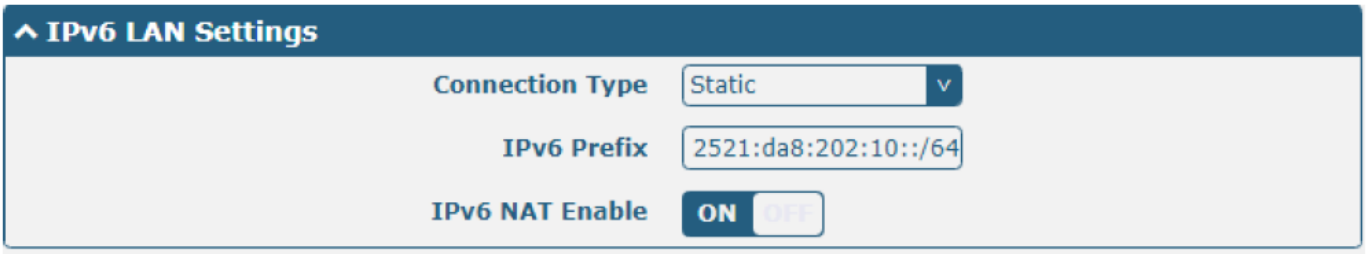
Automatic APN Selection	ON
Dialup Number	*99***1#
Authentication Type	Auto
Aggressive Reset	ON
Switch SIM By Data Allowance	OFF
Data Allowance	0
Billing Day	1

The window is displayed as below when disabling the “Automatic APN Selection” option.



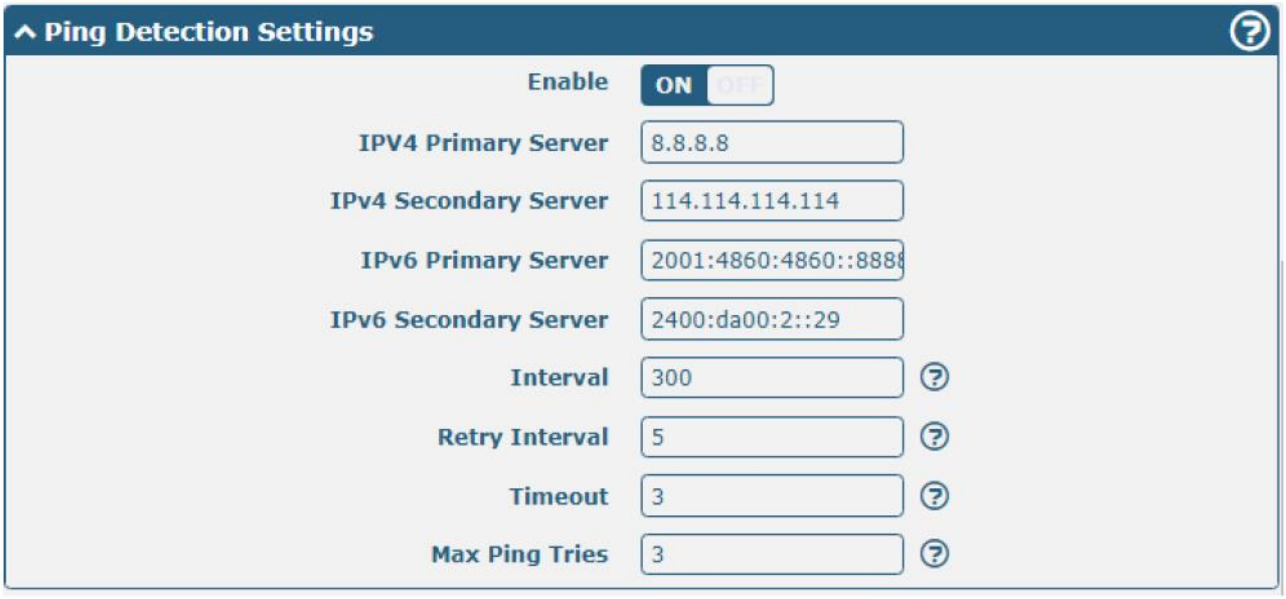
WWAN Settings

Automatic APN Selection	ON OFF
APN	internet
Username	
Password	•••••
Dialup Number	*99***1#
Authentication Type	Auto
PPP Preferred	ON OFF
Switch SIM By Data Allowance	ON OFF
Data Allowance	0
Billing Day	1



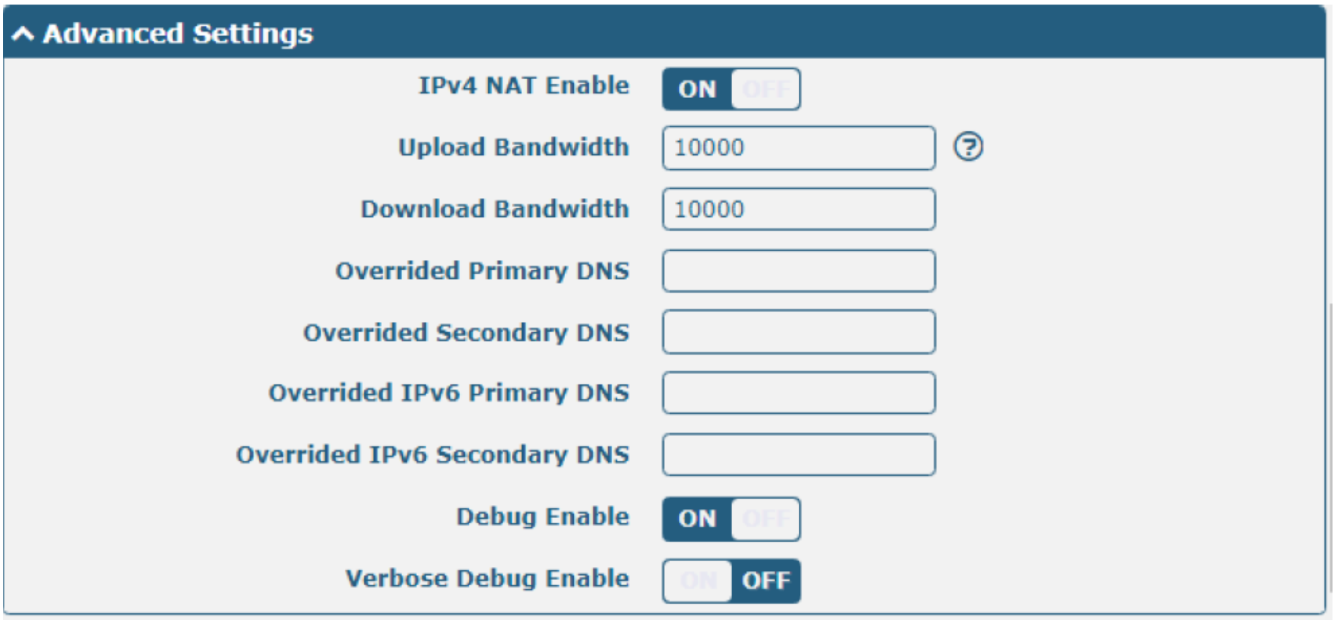
IPv6 LAN Settings

Connection Type	Static
IPv6 Prefix	2521:da8:202:10::/64
IPv6 NAT Enable	ON OFF



Ping Detection Settings

Enable	ON OFF
IPV4 Primary Server	8.8.8.8
IPv4 Secondary Server	114.114.114.114
IPv6 Primary Server	2001:4860:4860::888
IPv6 Secondary Server	2400:da00:2::29
Interval	300
Retry Interval	5
Timeout	3
Max Ping Tries	3



Advanced Settings

IPv4 NAT Enable: ON

Upload Bandwidth: 10000

Download Bandwidth: 10000

Overrided Primary DNS:

Overrided Secondary DNS:

Overrided IPv6 Primary DNS:

Overrided IPv6 Secondary DNS:

Debug Enable: ON

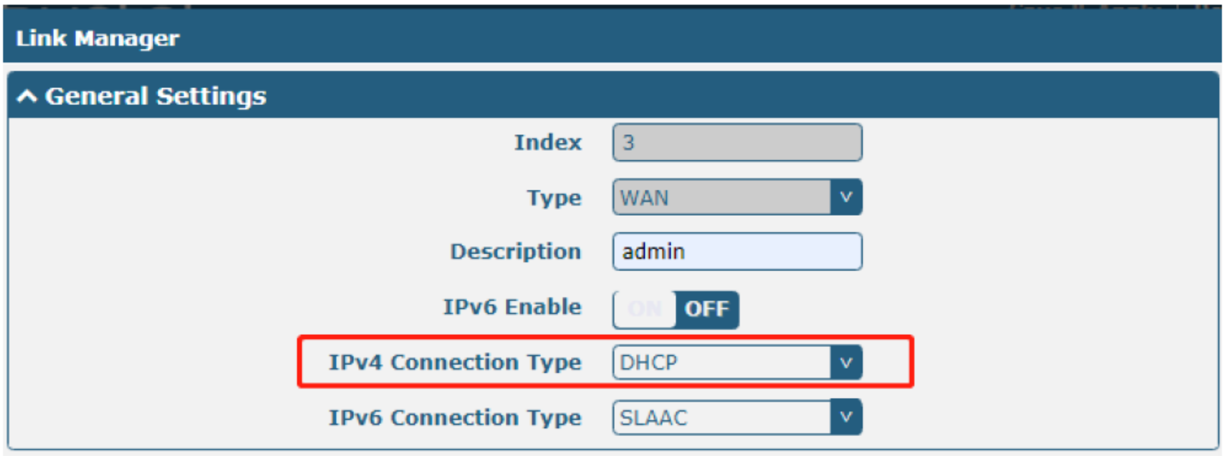
Verbose Debug Enable: OFF

Link Settings (WWAN)		
Item	Description	Default
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WWAN1
Description	Enter a description for this link.	Null
IPv6	Click the toggle button to enable / disable IPv6.	OFF
WWAN Settings		
Automatic APN Selection	Click the toggle button to enable/ disable the “Automatic APN Selection” option. After enabling, the device will recognize the access point name automatically. Alternatively, you can disable this option and manually add the access point name.	ON
APN	Enter the Access Point Name for cellular dial-up connection, provided by local ISP.	internet
Username	Enter the username for cellular dial-up connection, provided by local ISP.	Null
Password	Enter the password for cellular dial-up connection, provided by local ISP.	Null
Dialup Number	Enter the dialup number for cellular dial-up connection, provided by local ISP.	* 99* * * 1#
Authentication Type	Select from “ Auto” , “ PAP” or “ CHAP” as the local ISP required.	Auto
PPP Preferred	The PPP dial-up method is preferred.	OFF
Switch SIM By Data Allowance	Click the toggle button to enable/ disable this option. After enabling, it will switch to another SIM when the data limit reached. Note: Only used for dual SIM backup	OFF

Data Allowance	Set the monthly data traffic limitation. The system will record the data traffic statistics when data traffic limitation (MiB) is specified. The traffic record will be displayed in Interface > Link Manager > Status > WWAN Data Usage Statistics. 0 means disable data traffic record.	0
Billing Day	Specify the monthly billing day. The data traffic statistics will be recalculated from that day.	1
IPv6 LAN Settings		
Link Settings (WWAN)		
Connection Type	Select the link to assign an IPv6 prefix to the local area network.	Delegated
IPv6 prefix	Set the static IPv6 prefix assigned by the link to the LAN.	null
Enable IPv6 NAT	Set the link to enable IPv6 NAT.	OFF
Ping Detection Settings		
Enable	Click the toggle button to enable/ disable the ping detection mechanism, a keep-alive policy of DSR-200 Router.	ON
IPv4 Primary Server	Router will ping this primary address/ domain name to check that if the current IPv4 connectivity is active.	8.8.8.8
IPv4 Secondary Server	Router will ping this secondary address/ domain name to check that if the current connectivity is active.	114.114.114.114
IPv6 Primary Server	Router will ping this primary address/domain name to check that if the current IPv6 connectivity is active.	2001:4860:4860::8888
IPv6 Secondary Server	Router will ping this secondary address/domain name to check that if the current IPv6 connectivity is active.	2400:da00:2::29
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advanced Settings		
NAT Enable	Click the toggle button to enable/ disable the Network Address Translation option.	ON
Upload Bandwidth	Set the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Set the download bandwidth used for QoS, measured in kbps.	10000
Specify the Primary DNS server	Defines the primary IPv4 DNS server used by the link.	Null
Specify the Secondary DNS server	Defines the Secondary IPv4 DNS server used by the link.	Null
Specify the IPv6 Primary DNS server	Defines the primary IPv6 DNS server used by the link.	Null
Specify the IPv6 Secondary DNS server	Defines the Secondary IPv6 DNS server used by the link.	Null
Debug Enable	Click the toggle button to enable/ disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/ disable this option. Enable for verbose debugging information output.	OFF

WAN

Router will obtain IP automatically from DHCP server if choosing "DHCP" as IPv4 connection type. Router will obtain IPv6 prefix automatically from DHCP server if choosing „SLAAC" as IPv6 connection type The window is displayed as below.



Link Manager

General Settings

Index: 3

Type: WAN

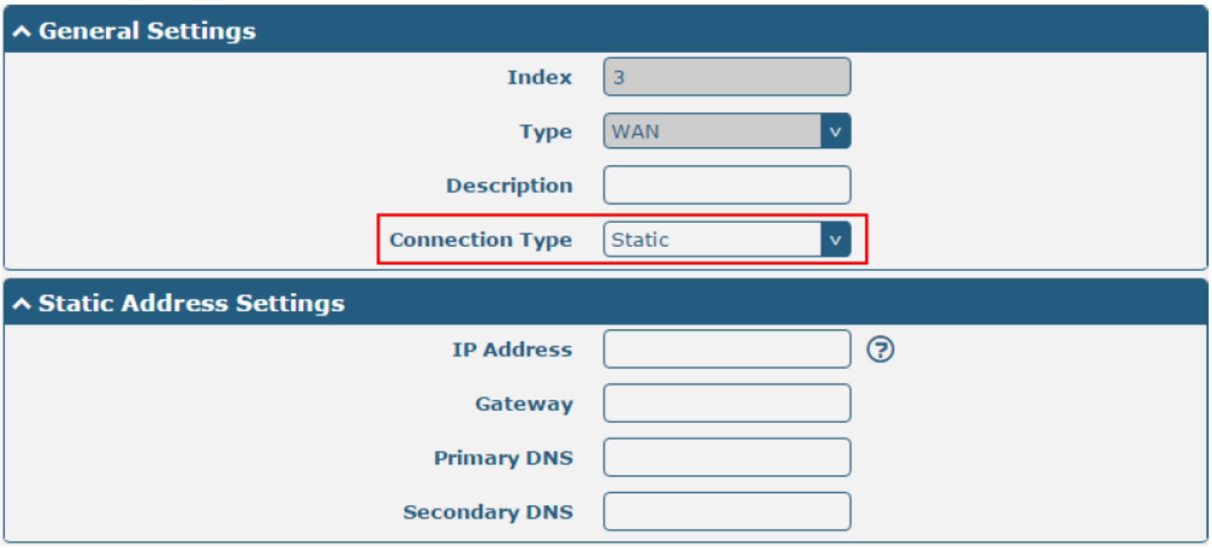
Description: admin

IPv6 Enable: ON OFF

IPv4 Connection Type: DHCP

IPv6 Connection Type: SLAAC

The window is displayed as below when choosing "Static"as the IPv4 connection type and IPv6 connection type.



General Settings

Index: 3

Type: WAN

Description:

Connection Type: Static

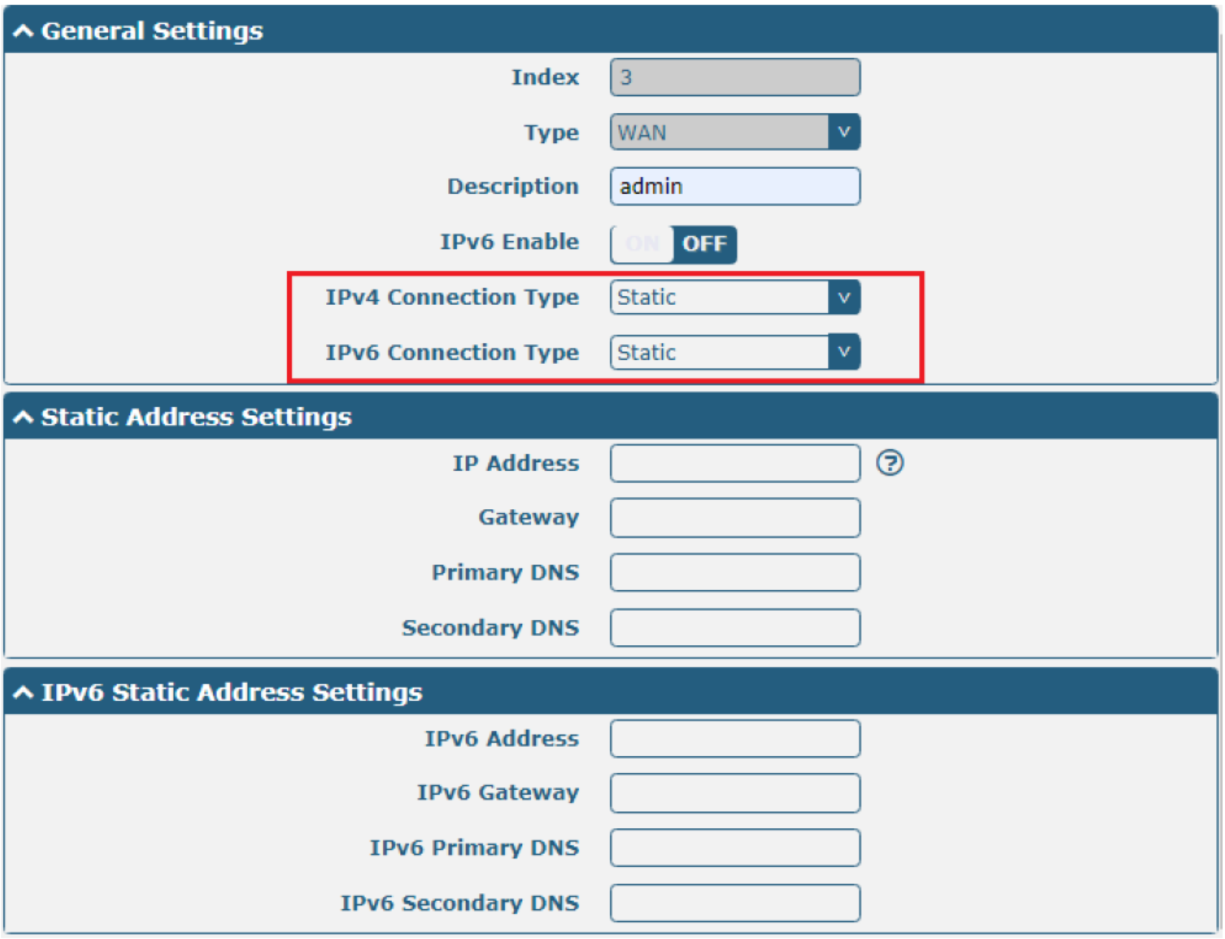
Static Address Settings

IP Address:

Gateway:

Primary DNS:

Secondary DNS:



General Settings

Index	3
Type	WAN
Description	admin
IPv6 Enable	ON OFF
IPv4 Connection Type	Static
IPv6 Connection Type	Static

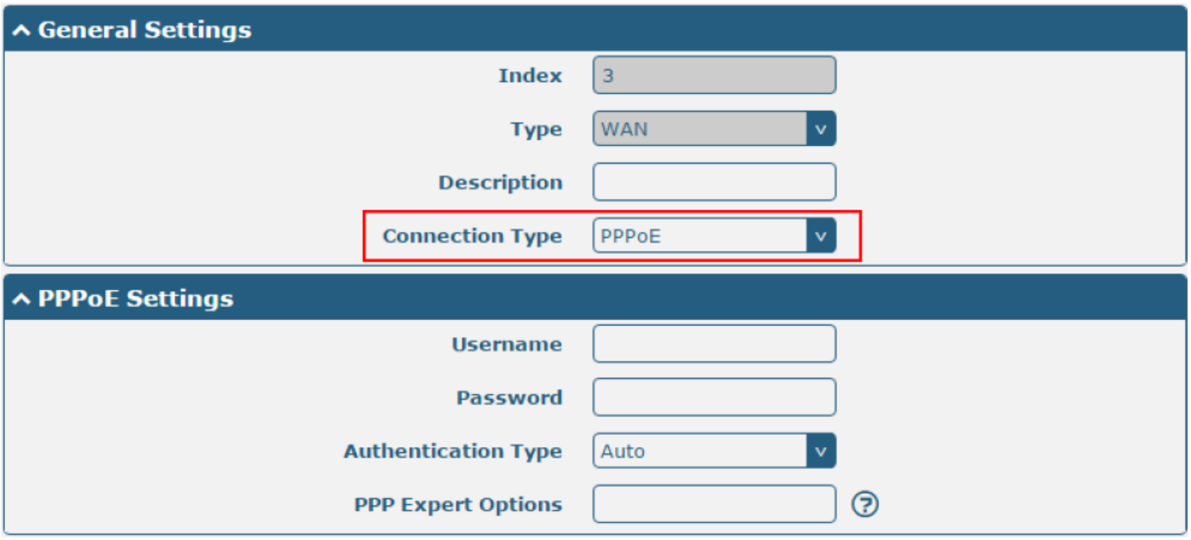
Static Address Settings

IP Address	
Gateway	
Primary DNS	
Secondary DNS	

IPv6 Static Address Settings

IPv6 Address	
IPv6 Gateway	
IPv6 Primary DNS	
IPv6 Secondary DNS	

The window is displayed as below when choosing “PPPoE”as the IPv4 connection type and IPv6 connection type.

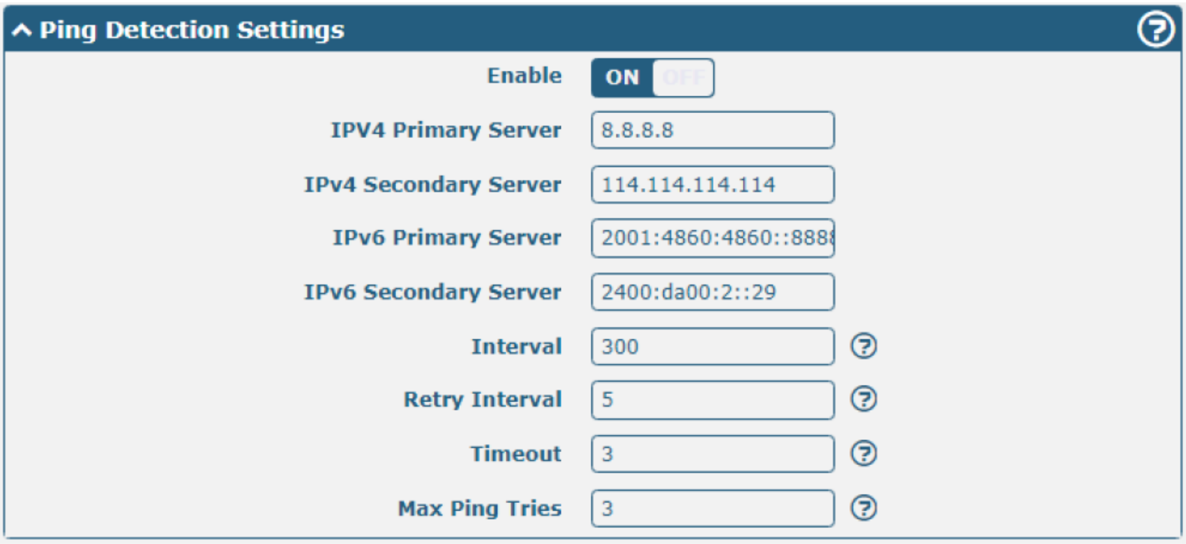


General Settings

Index	3
Type	WAN
Description	
Connection Type	PPPoE

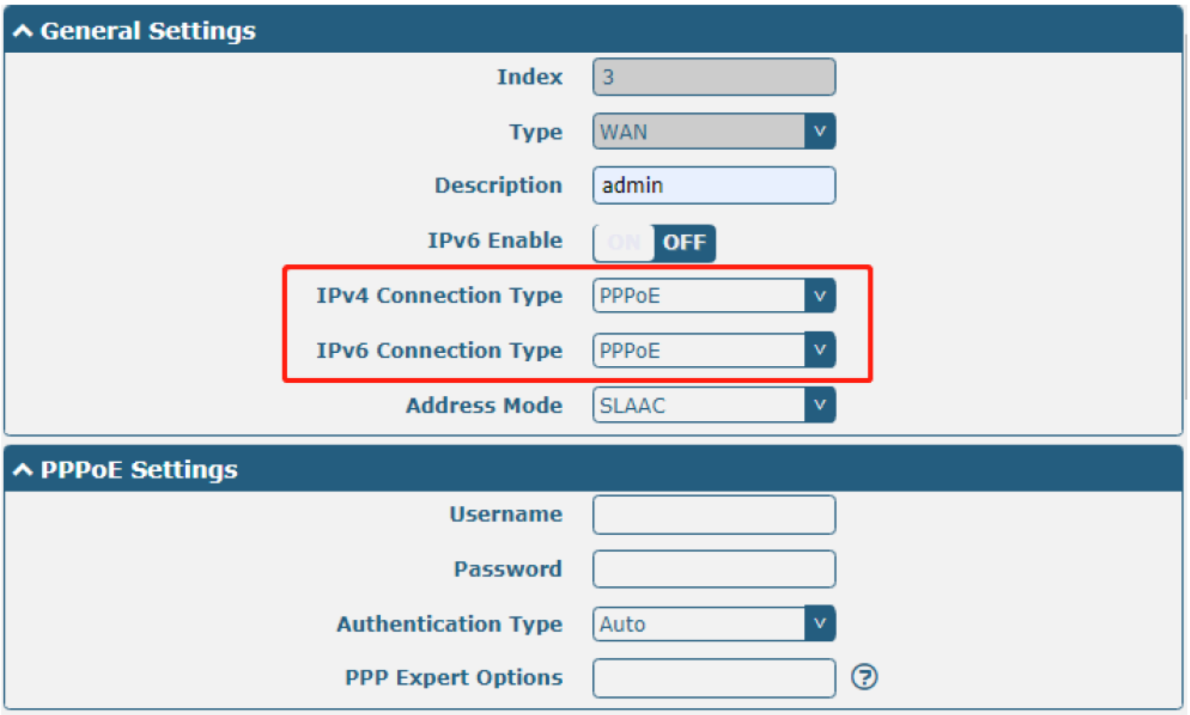
PPPoE Settings

Username	
Password	
Authentication Type	Auto
PPP Expert Options	



Ping Detection Settings

Enable	ON
IPV4 Primary Server	8.8.8.8
IPv4 Secondary Server	114.114.114.114
IPv6 Primary Server	2001:4860:4860::8888
IPv6 Secondary Server	2400:da00:2::29
Interval	300
Retry Interval	5
Timeout	3
Max Ping Tries	3

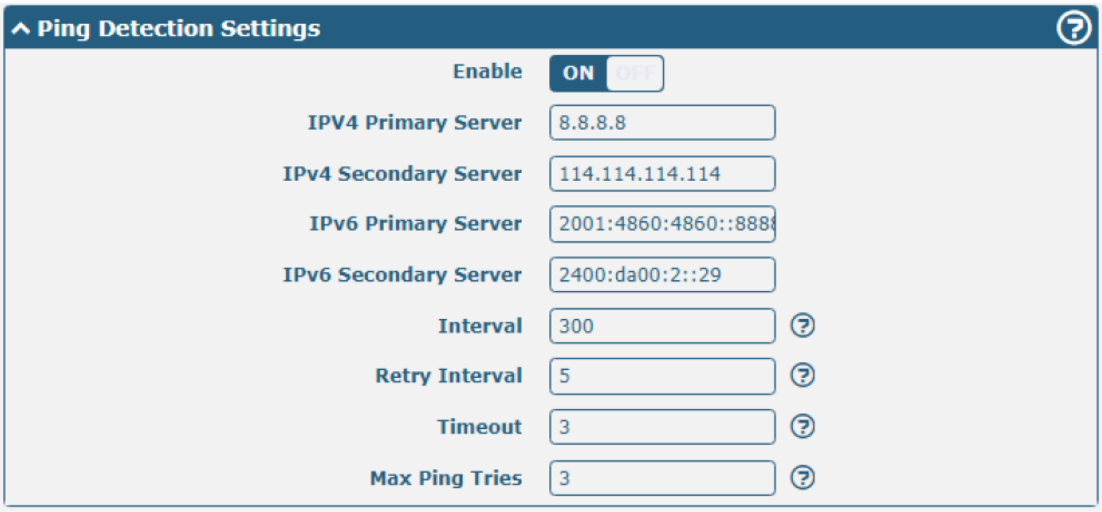


General Settings

Index	3
Type	WAN
Description	admin
IPv6 Enable	OFF
IPv4 Connection Type	PPPoE
IPv6 Connection Type	PPPoE
Address Mode	SLAAC

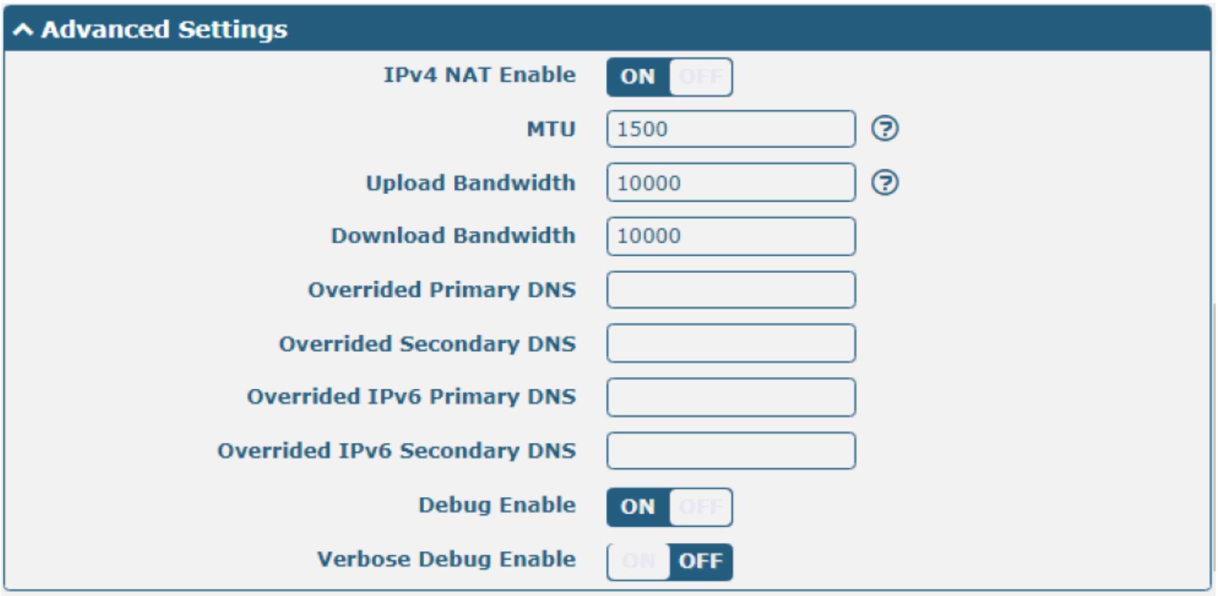
PPPoE Settings

Username	
Password	
Authentication Type	Auto
PPP Expert Options	



Ping Detection Settings

Enable	ON
IPV4 Primary Server	8.8.8.8
IPv4 Secondary Server	114.114.114.114
IPv6 Primary Server	2001:4860:4860::8888
IPv6 Secondary Server	2400:da00:2::29
Interval	300
Retry Interval	5
Timeout	3
Max Ping Tries	3



IPv4 NAT Enable: ON

MTU: 1500

Upload Bandwidth: 10000

Download Bandwidth: 10000

Overrided Primary DNS:

Overrided Secondary DNS:

Overrided IPv6 Primary DNS:

Overrided IPv6 Secondary DNS:

Debug Enable: ON

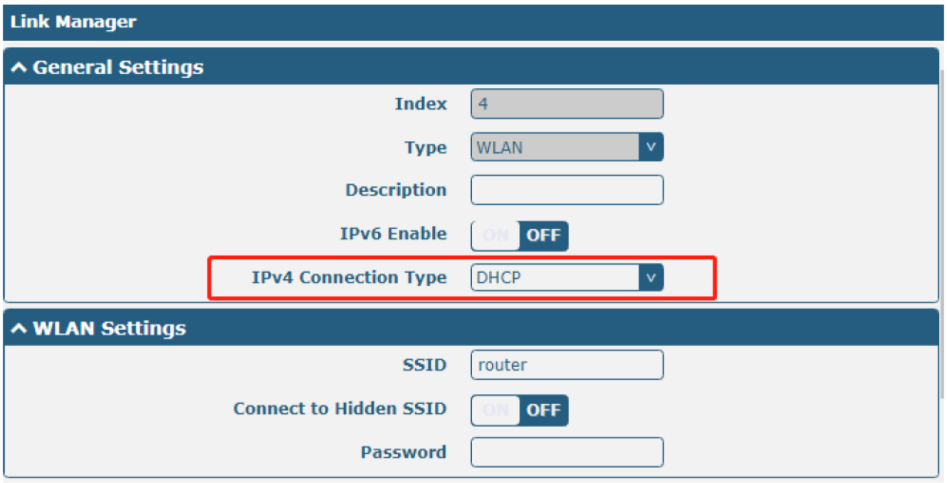
Verbose Debug Enable: OFF

Link Settings (WAN)		
Item	Description	Default
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WAN
Description	Enter a description for this link.	Null
Enable IPv6	Click the toggle button to enable / disable IPv6.	OFF
IPv4 connection type	Select from "DHCP", "Static IP" or "PPPoE".	DHCP
IPv6 connection type	Select from "SLAAC", "DHCPv6", "Static IP" or "PPPoE".	SLAAC
Address type	Select from "SLAAC"or "DHCPv6".	SLAAC
IPv4 Static Address Settings		
IP Address	Set the IP address with Netmask which can access the internet. IP address with Netmask, e.g. 192.168.1.1/ 24	Null
Gateway	Set the gateway of the IPv4 address in WAN port.	Null
Primary DNS	Set the primary DNS.	Null
Secondary DNS	Set the secondary DNS.	Null
IPv6 Static Address Settings		
IPv6 Address	Set the IPv6 address with Netmask which can access the internet. IP address with Netmask, e.g. 2521:da8:202:10::20/64	Null
Gateway	Set the gateway of the IPv6 address in WAN port.	Null
IPv6 Primary DNS	Set the primary IPv6 DNS server used by the link.	Null
IPv6 Secondary DNS	Set the secondary IPv6 DNS server used by the link.	Null
PPPoE Settings		
Username	Enter the username provided by your Internet Service Provider.	Null
Password	Enter the password provided by your Internet Service Provider.	Null
Authentication Type	Select from “ Auto” , “ PAP” or “ CHAP” as the local ISP required.	Auto

PPP Expert Options	Enter the PPP Expert options used for PPPoE dialup. You can enter some other PPP dial strings in this field. Each string can be separated by a semicolon.	Null
IPv6 LAN Settings		
Connection type	Select the link to assign IPv6 prefixes to the LAN.	Delegated
IPv6 Prefix	Sets the static IPv6 prefix assigned by the link to the LAN.	Null
Enabled IPv6 NAT	Set up links to enable IPv6 NAT.	OFF
Ping Detection Settings		
Enable	Click the toggle button to enable/ disable the ping detection mechanism, a keep-alive policy of DSR-211 Router.	ON
Primary Server	Router will ping this primary address/domain name to check that if the current IPv4 connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain name to check that if the current IPv4 connectivity is active.	114.114.114.114
IPv6 Primary Server	Router will ping this primary address/domain name to check that if the current IPv6 connectivity is active.	2001:4860:4860::8888
IPv6 Secondary Server	Router will ping this secondary address/domain name to check that if the current IPv6 connectivity is active.	2400:da00:2::29
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advanced Settings		
NAT Enable	Click the toggle button to enable/ disable the Network Address Translation option.	ON
MTU	Enter the Maximum Transmission Unit.	1500
Upload Bandwidth	Enter the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter the download bandwidth used for QoS, measured in kbps.	10000
Specify the Primary DNS server	Defines the primary IPv4 DNS server for the link.	Null
Specify the SecondaryDNS server	Defines the secondary IPv4 DNS server for the link.	Null
Specify the IPv6 Primary DNS server	Defines the primary IPv6 DNS server for the link.	Null
Specify the IPv6 Secondary DNS server	Defines the secondary IPv6 DNS server for the link.	Null
Debug Enable	Click the toggle button to enable/ disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/ disable this option. Enable for verbose debugging information output.	OFF

WLAN

Router will obtain IP automatically from the WLAN AP if choosing "DHCP" as the connection type. The specific parameter configuration of SSID is shown as below.



Link Manager

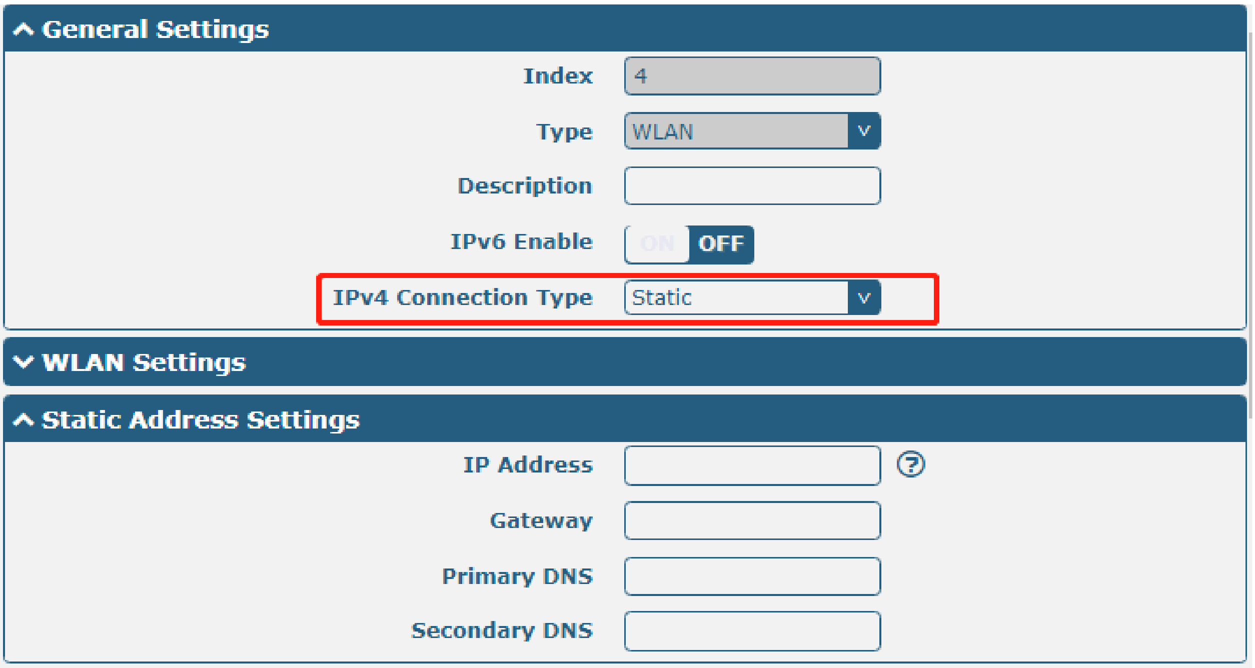
^ General Settings

Index	4
Type	WLAN
Description	
IPv6 Enable	ON OFF
IPv4 Connection Type	DHCP

^ WLAN Settings

SSID	router
Connect to Hidden SSID	ON OFF
Password	

The window is displayed as below when choosing "Static"as the IPv4 connection type.



^ General Settings

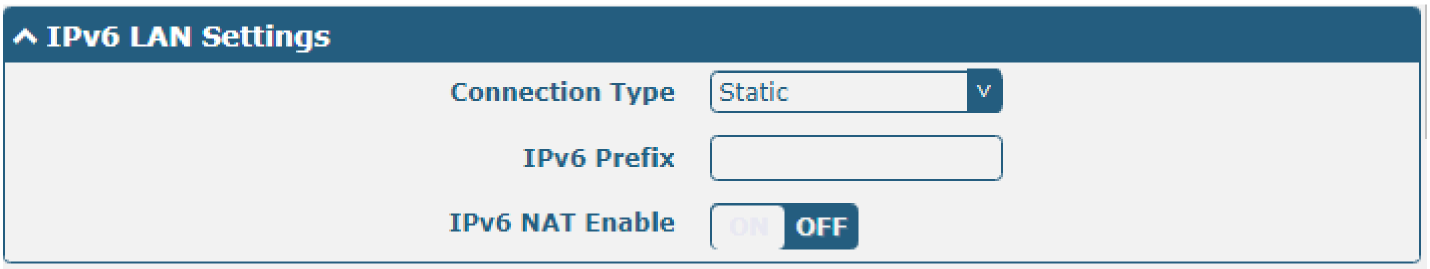
Index	4
Type	WLAN
Description	
IPv6 Enable	ON OFF
IPv4 Connection Type	Static

v WLAN Settings

^ Static Address Settings

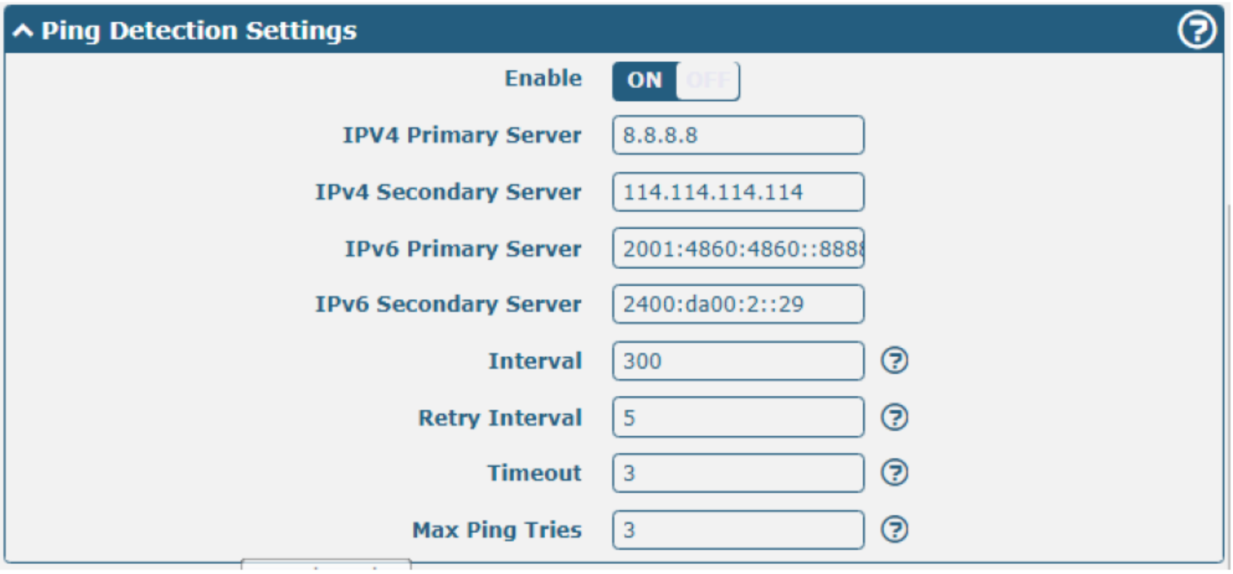
IP Address	
Gateway	
Primary DNS	
Secondary DNS	

DSR-211 does not support the PPPoE WLAN Connection Type.



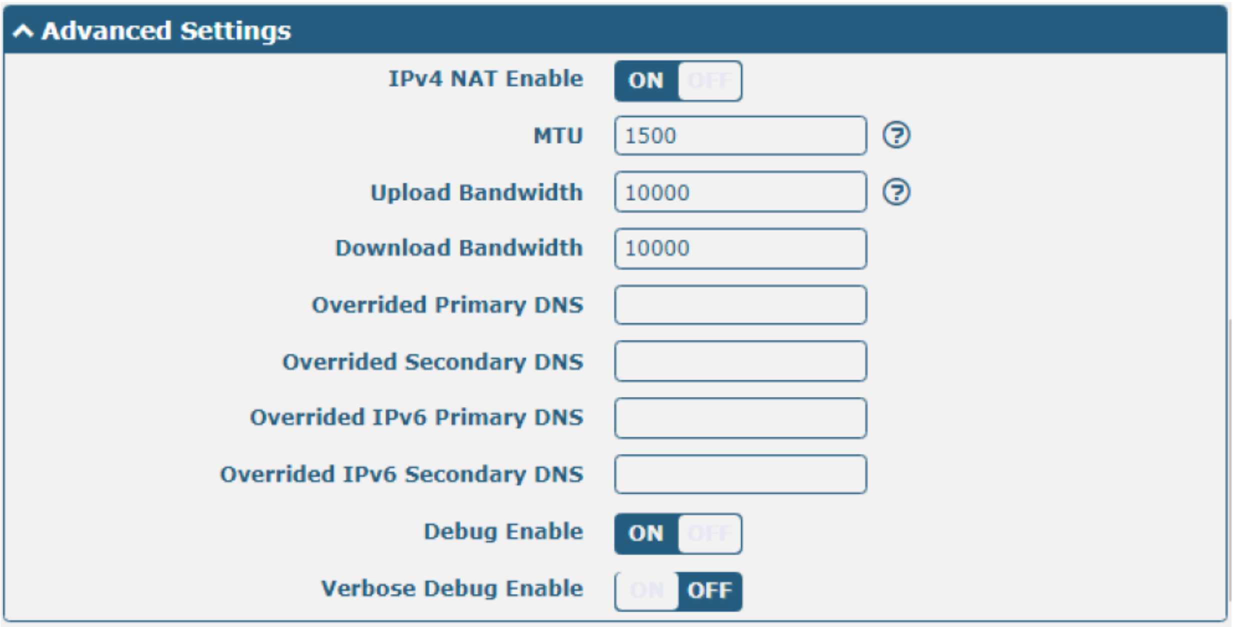
^ IPv6 LAN Settings

Connection Type	Static
IPv6 Prefix	
IPv6 NAT Enable	ON [✓ OFF]



^ Ping Detection Settings

Enable	[✓ ON] OFF
IPV4 Primary Server	8.8.8.8
IPv4 Secondary Server	114.114.114.114
IPv6 Primary Server	2001:4860:4860::888
IPv6 Secondary Server	2400:da00:2::29
Interval	300
Retry Interval	5
Timeout	3
Max Ping Tries	3



^ Advanced Settings

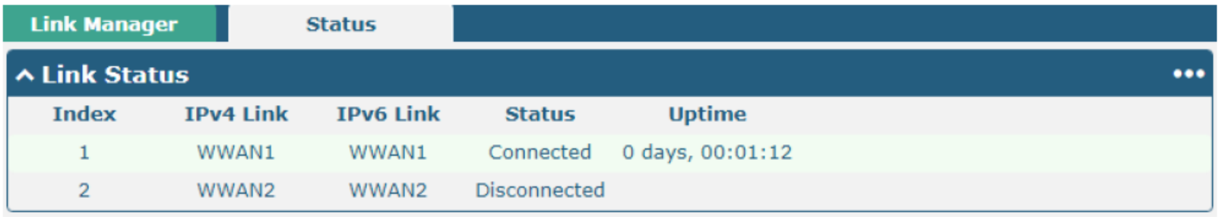
IPv4 NAT Enable	[✓ ON] OFF
MTU	1500
Upload Bandwidth	10000
Download Bandwidth	10000
Overrided Primary DNS	
Overrided Secondary DNS	
Overrided IPv6 Primary DNS	
Overrided IPv6 Secondary DNS	
Debug Enable	[✓ ON] OFF
Verbose Debug Enable	ON [✓ OFF]

Link Settings (WLAN)		
Item	Description	Default
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WLAN
Description	Enter a description for this link.	Null
Enable Ipv6	Click the toggle button to enable / disable IPv6.	OFF
IPv4 Connection Type	Select from “DHCP” or “ Static”.	DHCP
WLAN Settings		
SSID	Enter a 1-32 characters SSID which your router wants to connect. SSID (Service Set Identifier) is the name of your wireless network.	router
Connect to Hidden SSID	Click the toggle button to enable/ disable this option. When router works as Client mode and needs to connect any access point which has hidden SSID, you need to enable this option.	OFF
Password	Enter an 8-63 characters password of the access point which your router wants to connect.	Null
Static Address Settings		
IP Address	Enter the IPaddress with Netmask which can access the Internet, e.g. 192.168.1.1/ 24	Null
Gateway	Enter the IPaddress of Wi-Fi AP.	Null
Primary DNS	Set the primary DNS.	Null
Secondary DNS	Set the secondary DNS.	Null
IPv6 LAN Settings		
Connection type	Select the link to assign IPv6 prefixes to the LAN.	Delegated
IPv6 Prefix	Sets the static IPv6 prefix assigned by the link to the LAN.	Null
Enabled IPv6 NAT	Set up links to enable IPv6 NAT.	OFF
Ping Detection Settings		
Enable	Click the toggle button to enable/ disable the ping detection mechanism, a keepalive policy of DSR-211 Router.	ON
Primary Server	Router will ping this primary address/ domain name to check that if the current connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/ domain name to check that if the current connectivity is active.	114.114.114.114
IPv6 Primary Server	Router will ping this primary address/domain name to check that if the current IPv6 connectivity is active.	2001:4860:4860::88 8 8
IPv6 Secondary Server	Router will ping this secondary address/domain name to check that if the current IPv6 connectivity is active.	2400:da00:2::29
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3

Advance Settings		
NAT Enable	Click the toggle button to enable/ disable the Network Address Translation option.	ON
MTU	Enter the Maximum Transmission Unit.	1500
Upload Bandwidth	Enter the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter the download bandwidth used for QoS, measured in kbps.	10000
Specify the Primary DNS server	Defines the primary IPv4 DNS server for the link.	Null
Specify the Secondary DNS server	Defines the secondary IPv4 DNS server for the link.	Null
Specify the IPv6 Primary DNS server	Defines the primary IPv6 DNS server for the link.	Null
Specify the IPv6 Secondary DNS server	Defines the secondary IPv6 DNS server for the link.	Null
Debug Enable	Click the toggle button to enable/ disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/ disable this option. Enable for verbose debugging information output.	OFF

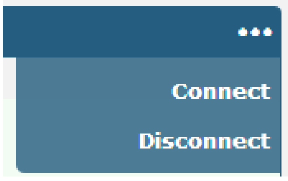
Status

This page allows you to view the status of link connection and clear the monthly data usage statistics.

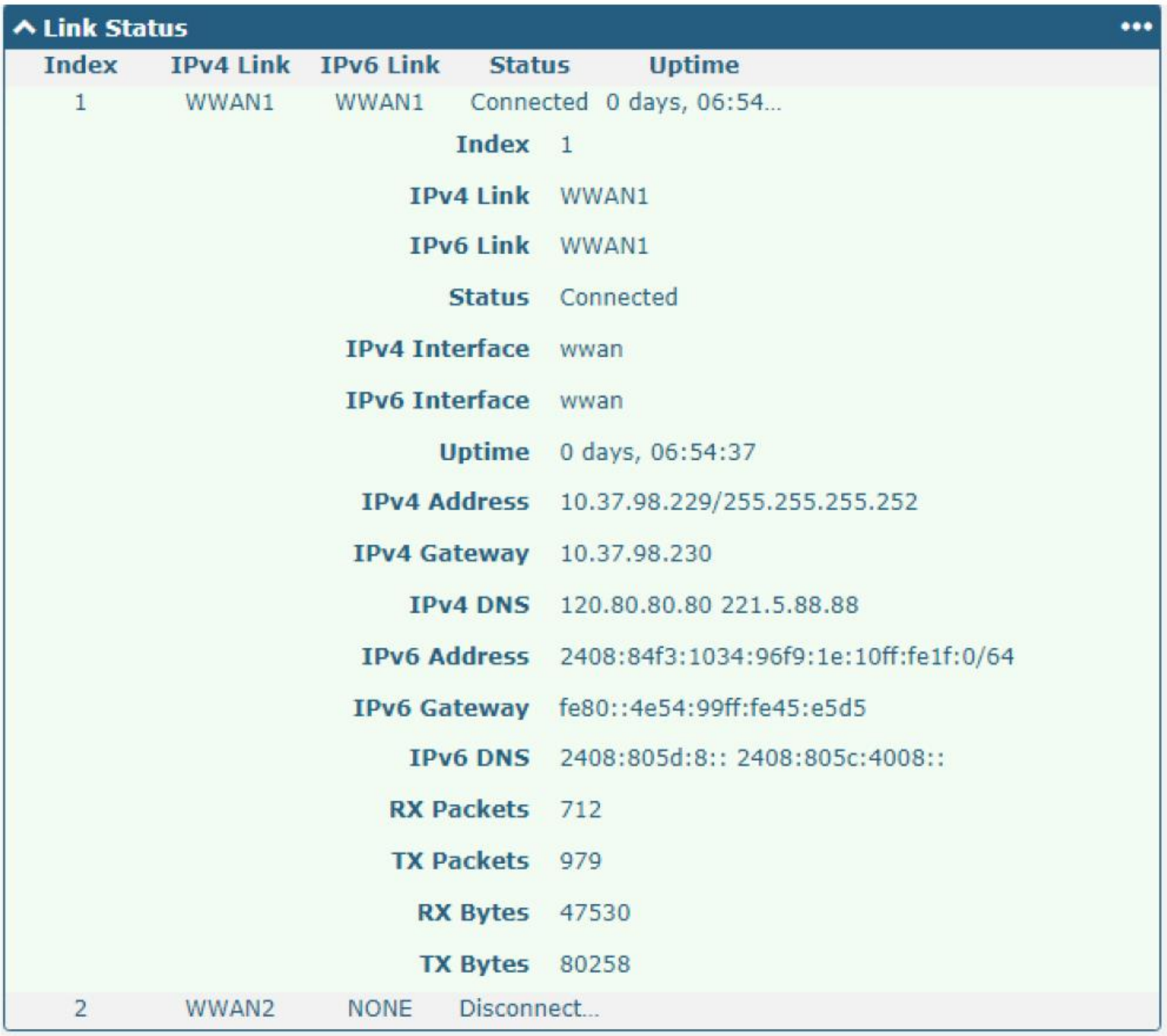


Index	IPv4 Link	IPv6 Link	Status	Uptime
1	WWAN1	WWAN1	Connected	0 days, 00:01:12
2	WWAN2	WWAN2	Disconnected	

Click the right-most button ••• to select the connection status of the current link.



Click the row of the link, and it will show the details information of the current link connection under the row.

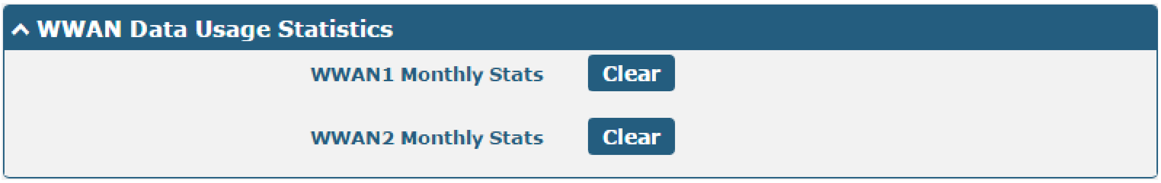


^ Link Status •••

Index	IPv4 Link	IPv6 Link	Status	Uptime
1	WWAN1	WWAN1	Connected	0 days, 06:54...

Index	1
IPv4 Link	WWAN1
IPv6 Link	WWAN1
Status	Connected
IPv4 Interface	wwan
IPv6 Interface	wwan
Uptime	0 days, 06:54:37
IPv4 Address	10.37.98.229/255.255.255.252
IPv4 Gateway	10.37.98.230
IPv4 DNS	120.80.80.80 221.5.88.88
IPv6 Address	2408:84f3:1034:96f9:1e:10ff:fe1f:0/64
IPv6 Gateway	fe80::4e54:99ff:fe45:e5d5
IPv6 DNS	2408:805d:8:: 2408:805c:4008::
RX Packets	712
TX Packets	979
RX Bytes	47530
TX Bytes	80258

Index	IPv4 Link	IPv6 Link	Status	Uptime
2	WWAN2	NONE	Disconnect...	



^ WWAN Data Usage Statistics

WWAN1 Monthly Stats	Clear
WWAN2 Monthly Stats	Clear

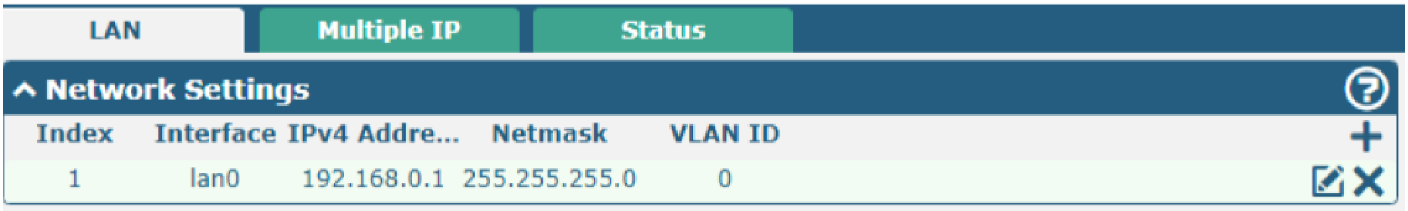
Click the Clear button to clear SIM1 or SIM2 monthly data traffic usage statistics. Data statistics will be displayed only if enable the Data Allowance function in Interface > Link Manager > Link Settings > WWAN Settings > Data Allowance.

3.7 Interface > LAN

This section allows you to set the related parameters for LAN port. There are two LAN ports on DSR-211 Router, including ETH0 and ETH1. The ETH0 and ETH1 can freely choose from lan0 and lan1, but at least one LAN port must be assigned as lan0. The default settings of ETH0 and ETH1 are lan0 and their default IP are 192.168.0.1/ 255.255.255.0.

LAN

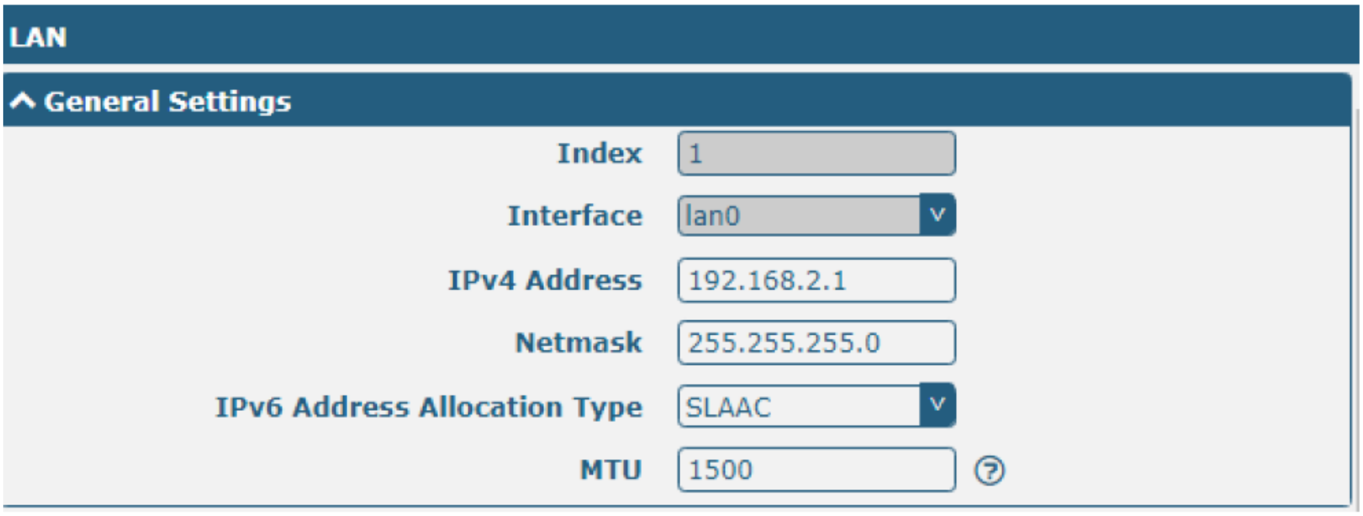
By default, there is a LAN port (lan0) in the list. To begin adding a new LAN port (lan1), please configure ETH0 or ETH1 as lan1 first in Ethernet > Ports > Port Settings. Otherwise, the operation will be prompted as "List is full".



Index	Interface	IPv4 Addre...	Netmask	VLAN ID
1	lan0	192.168.0.1	255.255.255.0	0

Note: Lan0 cannot be deleted.

You may click + to add a new LAN port, or click ✕ to delete the current LAN port. Now, click ✎ to edit the configuration of the LAN port.

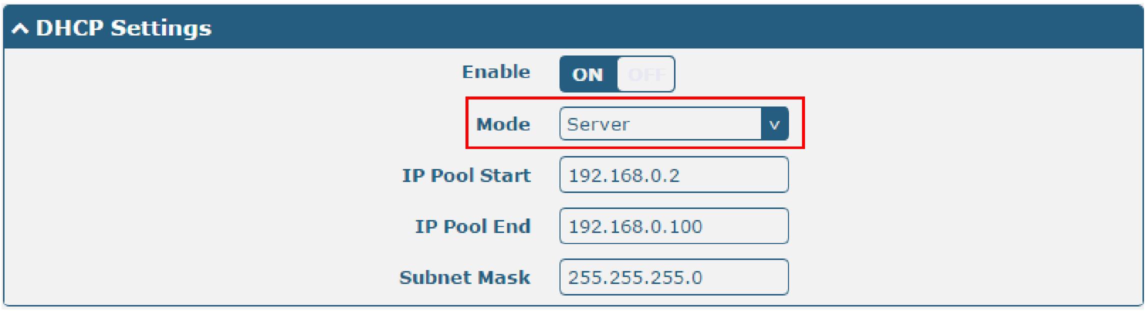


Index	1
Interface	lan0
IPv4 Address	192.168.2.1
Netmask	255.255.255.0
IPv6 Address Allocation Type	SLAAC
MTU	1500

General Settings		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Interface	Show the editing port. Lan1 is available only if it was selected by one of ETH 0 ETH 1 in Ethernet > Ports > Port Settings	--
IP Address	Set the IP address of the LAN port.	192.168.0.1
Netmask	Set the Netmask of the LAN port.	255.255.255.0
IPv6 Address AllocationType	Set the method of assigning IPv6 addresses on the LAN side.	SLAAC

MTU	Enter the Maximum Transmission Unit.	1500

The window is displayed as below when choosing “Server” as the mode.



^ DHCP Settings

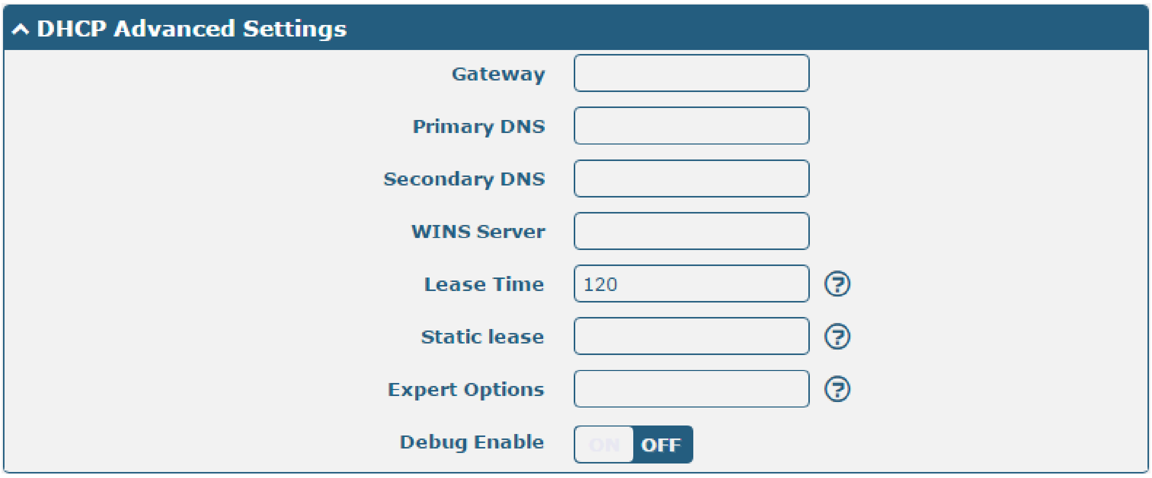
Enable: ON

Mode: Server

IP Pool Start: 192.168.0.2

IP Pool End: 192.168.0.100

Subnet Mask: 255.255.255.0



^ DHCP Advanced Settings

Gateway:

Primary DNS:

Secondary DNS:

WINS Server:

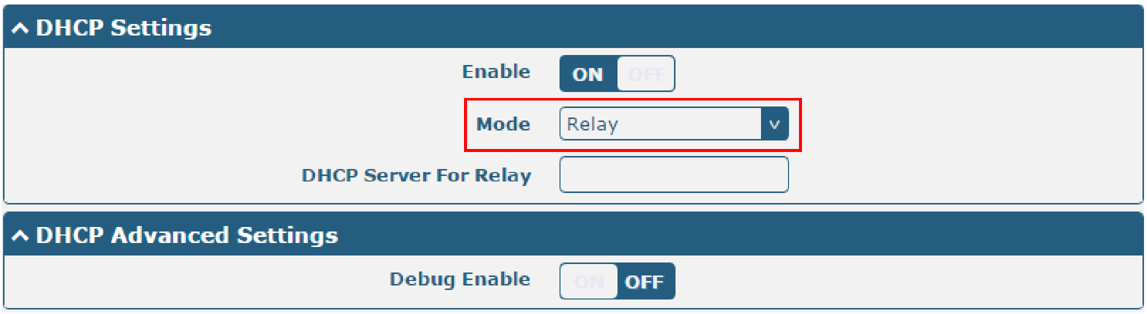
Lease Time: 120

Static lease:

Expert Options:

Debug Enable: OFF

The window is displayed as below when choosing “Relay” as the mode.



^ DHCP Settings

Enable: ON

Mode: Relay

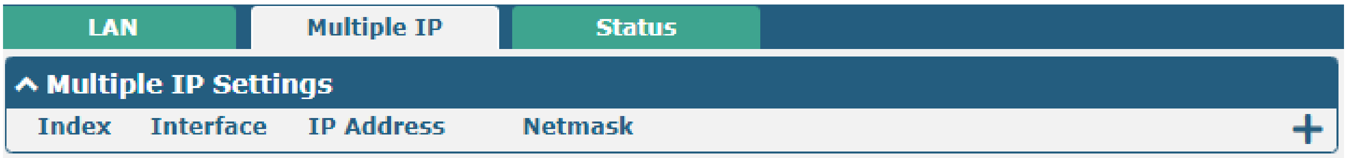
DHCP Server For Relay:

^ DHCP Advanced Settings

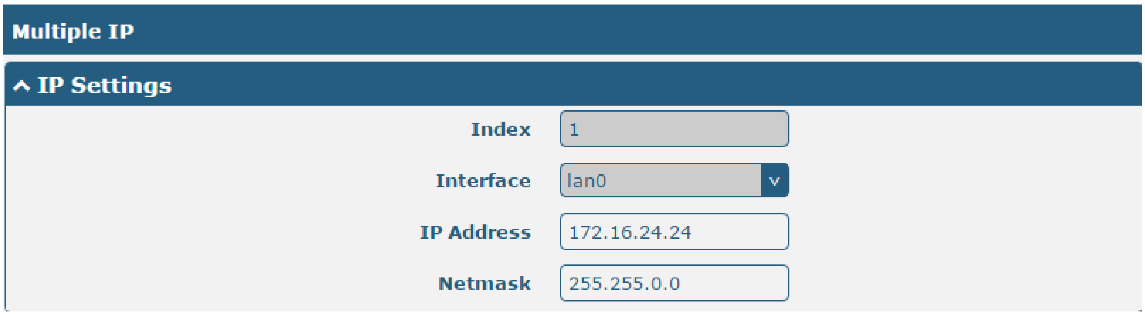
Debug Enable: OFF

LAN		
Item	Description	Default
DHCP Settings		
Enable	Click the toggle button to enable/ disable the DHCP function.	ON
Mode	Select from “Server” or “ Relay” . Server: Lease IP address to DHCPclients which have been connected to LAN port Relay: Router can be DHCP Relay, which will provide a relay tunnel to solve problem that DHCP Client and DHCP Server is not in a same subnet	Server
IP Pool Start	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.	192.168.0.2
IP Pool End	Define the end of the pool of IPaddresses which will be leased to DHCP clients.	192.168.0.100
Subnet Mask	Define the subnet mask of IP address obtained by DHCP clients from DHCPserver.	255.255.255.0
DHCP Server for Relay	Enter the IP address of DHCP relay server.	Null
DHCP Advanced Settings		
Gateway	Define the gateway assigned by the DHCP server to the clients, which must be on the same network segment with DHCP address pool.	Null
Primary DNS	Define the primary DNS server assigned by the DHCP server to the clients.	Null
Secondary DNS	Define the secondary DNS server assigned by the DHCP server to the clients.	Null
WINS Server	Define the Windows Internet Naming Service obtained by DHCP clients from DHCP sever.	Null
Lease Time	Set the lease time which the client can use the IP address obtained from DHCP server, measured in seconds.	120
Static lease	Bind a lease to correspond an IP address via a MAC address. format: mac,ip;mac,ip;..., e.g. FF:ED:CB:A0:98:01,192.168.0.200	Null
Expert Options	Enter some other options of DHCP server in this field. format: config-desc;config-desc, e.g. log dhcp;quiet-dhcp	Null
Debug Enable	Click the toggle button to enable/ disable this option. Enable for DHCP information output.	OFF

Multiple IP



You may click ➕ to add a multiple IP to the LAN port, or click ✕ to delete the multiple IP of the LAN port. Now, click ✎ to edit the multiple IP of the LAN port.



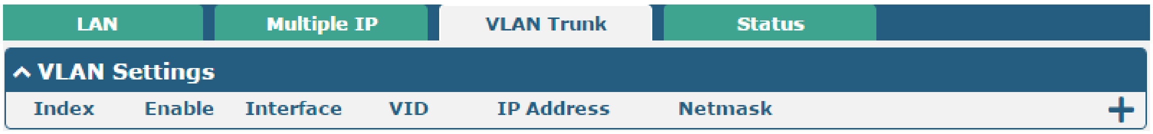
Multiple IP

^ IP Settings

Index	1
Interface	lan0
IP Address	172.16.24.24
Netmask	255.255.0.0

IP Settings		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Interface	Show the editing port, read only.	lan0
IP Address	Set the multiple IP address of the LAN port.	Null
Netmask	Set the multiple Netmask of the LAN port.	Null

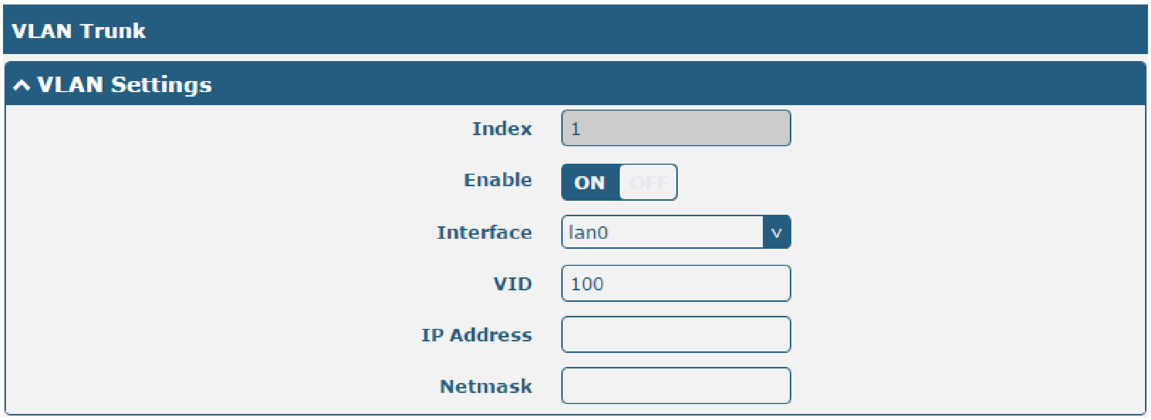
VLAN Trunk



^ VLAN Settings

Index	Enable	Interface	VID	IP Address	Netmask	➕

Click ➕ to add a VLAN. The maximum count is 8.



VLAN Trunk

^ VLAN Settings

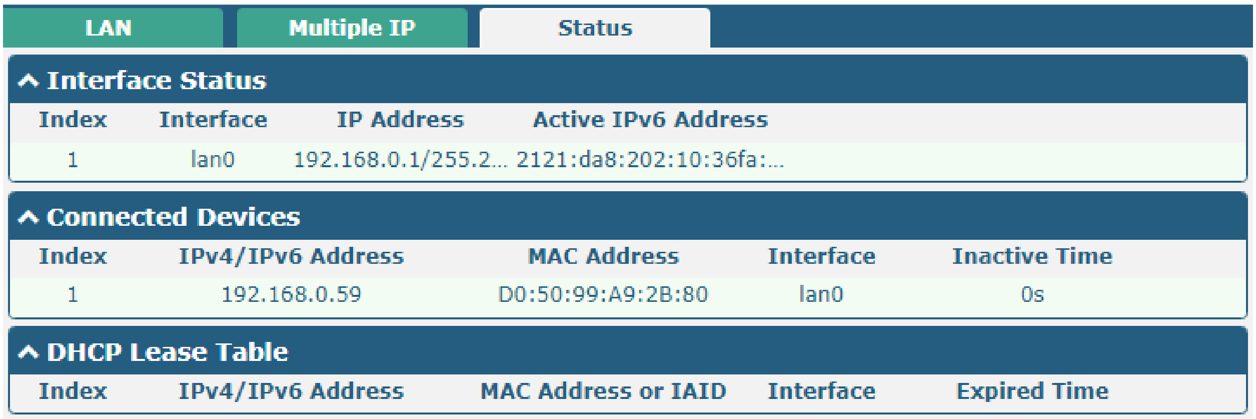
Index	1
Enable	ON OFF
Interface	lan0
VID	100
IP Address	
Netmask	

VLAN Trunk		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/ disable this VLAN. Enable to make router can encapsulate and de-encapsulate the VLAN tag.	ON

Interface	Choose the interface which wants to enable VLAN trunk function. Select from "lan0" or " lan1" depends on your ETH0 and ETH1's corresponding LAN port.	lan0
VID	Set the tag ID of VLAN and digits from 1 to 4094.	100
IP Address	Set the IP address of VLAN port.	Null
Netmask	Set the Netmask of VLAN port.	Null

Status

This section allows you to view the status of LAN connection.



^ Interface Status

Index	Interface	IP Address	Active IPv6 Address
1	lan0	192.168.0.1/255.2...	2121:da8:202:10:36fa:...

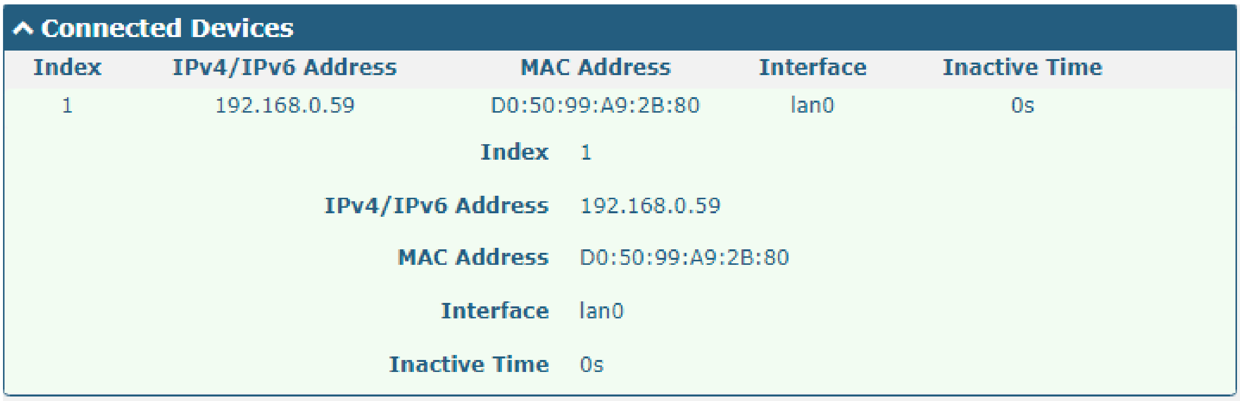
^ Connected Devices

Index	IPv4/IPv6 Address	MAC Address	Interface	Inactive Time
1	192.168.0.59	D0:50:99:A9:2B:80	lan0	0s

^ DHCP Lease Table

Index	IPv4/IPv6 Address	MAC Address or IAID	Interface	Expired Time

Click the row of status, the details status information will be display under the row. Please refer to the screenshot below.



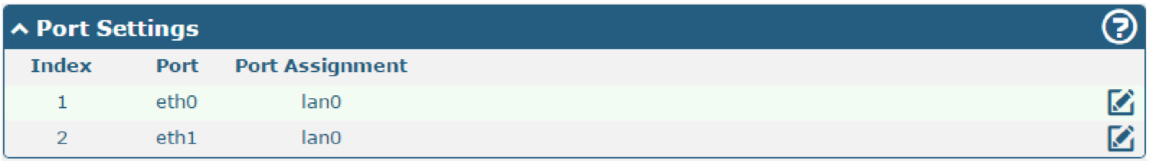
^ Connected Devices

Index	IPv4/IPv6 Address	MAC Address	Interface	Inactive Time
1	192.168.0.59	D0:50:99:A9:2B:80	lan0	0s

Index	1
IPv4/IPv6 Address	192.168.0.59
MAC Address	D0:50:99:A9:2B:80
Interface	lan0
Inactive Time	0s

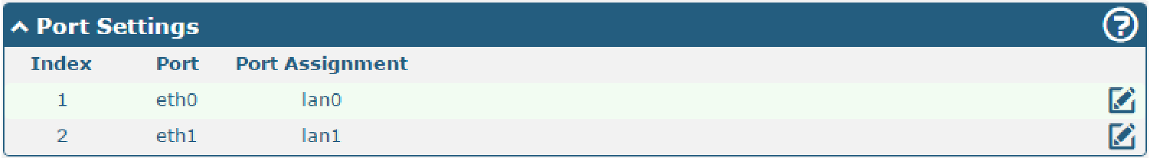
3.8 Interface > Ethernet

This section allows you to set the related parameters for Ethernet. There are two Ethernet ports on DSR-211 Router, including ETH0 and ETH1. The ETH0 on the router can be configured as either a WAN or a LAN port, while ETH1 can only be configured as a LAN port. By default, ETH0 and ETH1 are lan0, and their IP are 192.168.0.1/ 255.255.255.0. Since lan0 must be assigned to one port and WAN port must be assigned to the ETH0, there are four configurations. You can choose the appropriate configuration to fit your current needs. The specific port configurations are shown below.



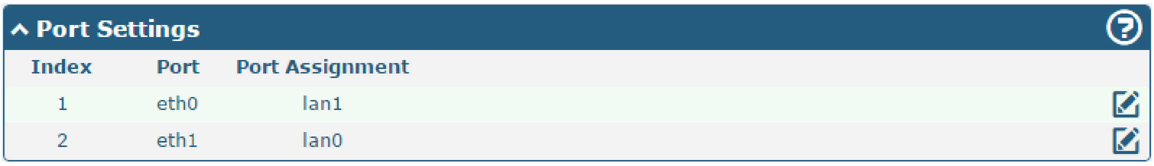
Port Settings

Index	Port	Port Assignment
1	eth0	lan0
2	eth1	lan0



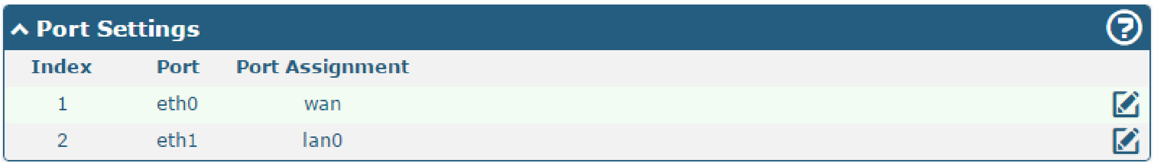
Port Settings

Index	Port	Port Assignment
1	eth0	lan0
2	eth1	lan1



Port Settings

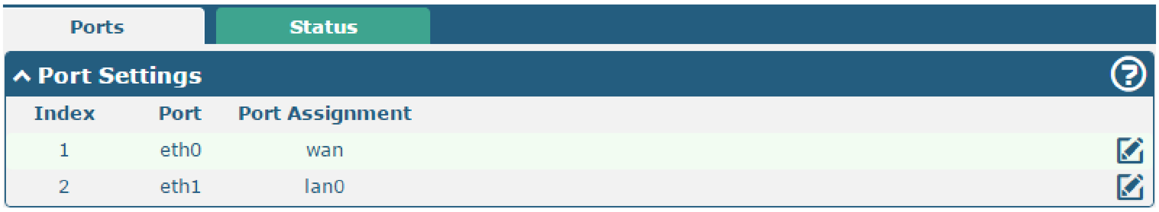
Index	Port	Port Assignment
1	eth0	lan1
2	eth1	lan0



Port Settings

Index	Port	Port Assignment
1	eth0	wan
2	eth1	lan0

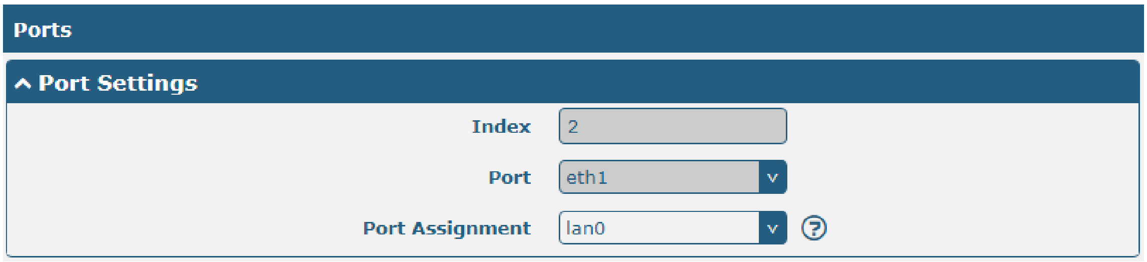
This section introduces you to set the parameters of the WAN port.



Port Settings

Index	Port	Port Assignment
1	eth0	wan
2	eth1	lan0

Click ✎ button of eth0 to configure its parameters. The port assignment can be changed by selecting from the drop down list.



Port Settings

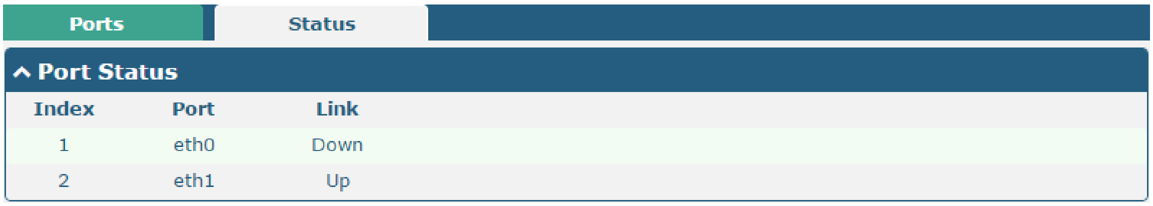
Index: 2

Port: eth1

Port Assignment: lan0

Port Settings		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Port	Show the editing port, read only.	--
Port Assignment	Choose the Ethernet port 's type, as a WAN port or a LAN port. When setting the port as a LAN port in Interface > LAN > LAN > Network Settings > General Settings, you can click the drop-down list to select from " lan0" or " lan1".	lan0

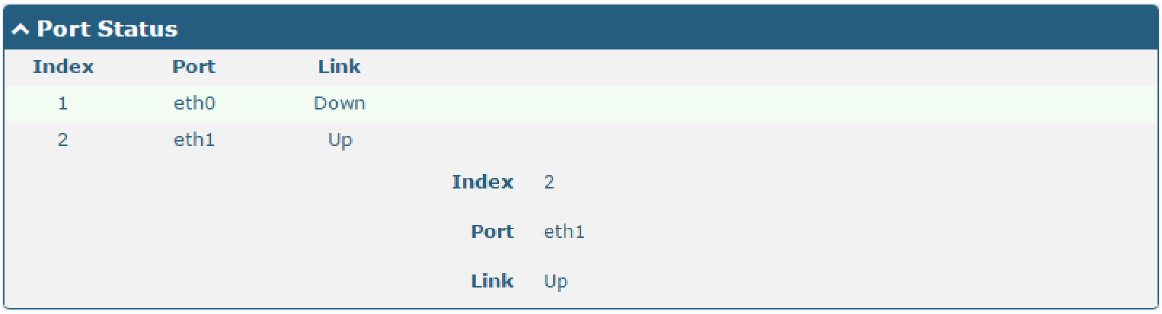
This column allows you to view the status of Ethernet port.



Port Status

Index	Port	Link
1	eth0	Down
2	eth1	Up

Click the row of status, the details status information will be display under the row. Please refer to the screenshot below.



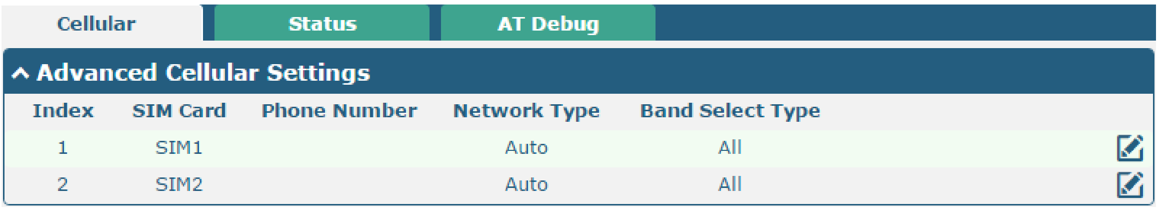
Port Status

Index	Port	Link
1	eth0	Down
2	eth1	Up

Index	2
Port	eth1
Link	Up

3.9 Interface > Cellular

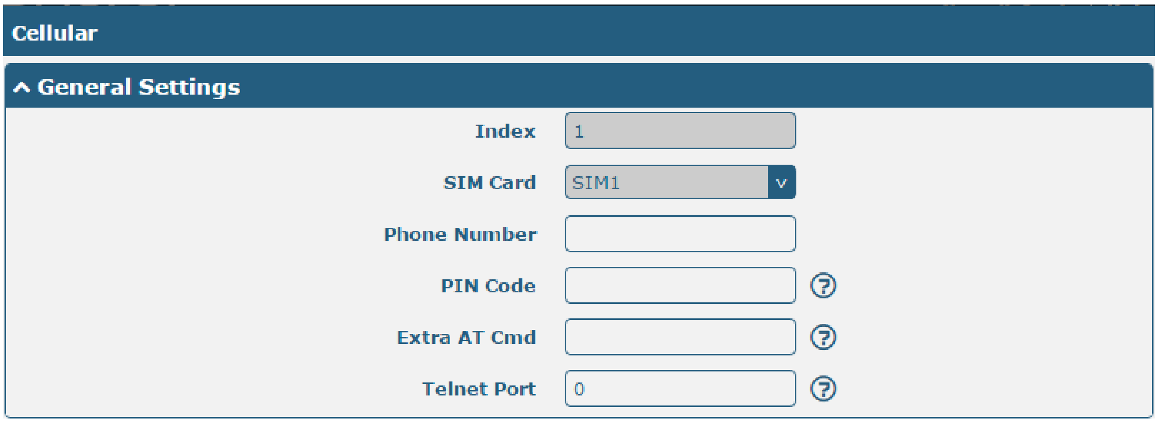
This section allows you to set the related parameters of Cellular. The DSR-211 Router has two SIM card slots, but do not support two SIM cards online simultaneously due to its single module design. If insert single SIM card at the first time, SIM1 slot and SIM2 slots are available.



Advanced Cellular Settings

Index	SIM Card	Phone Number	Network Type	Band Select Type	
1	SIM1		Auto	All	✎
2	SIM2		Auto	All	✎

Click ✎ of SIM 1 to edit the parameters.

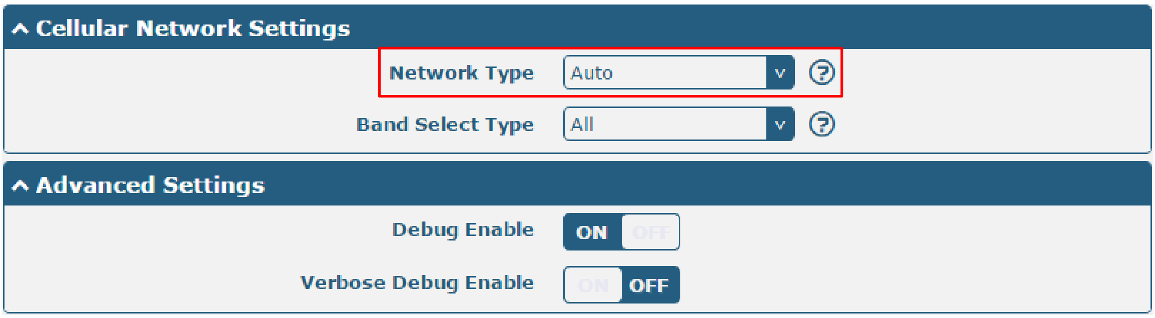


Cellular

General Settings

Index	1
SIM Card	SIM1
Phone Number	
PIN Code	
Extra AT Cmd	
Telnet Port	0

The window is displayed as below when choosing “Auto” as the network type.



^ Cellular Network Settings

Network Type: Auto

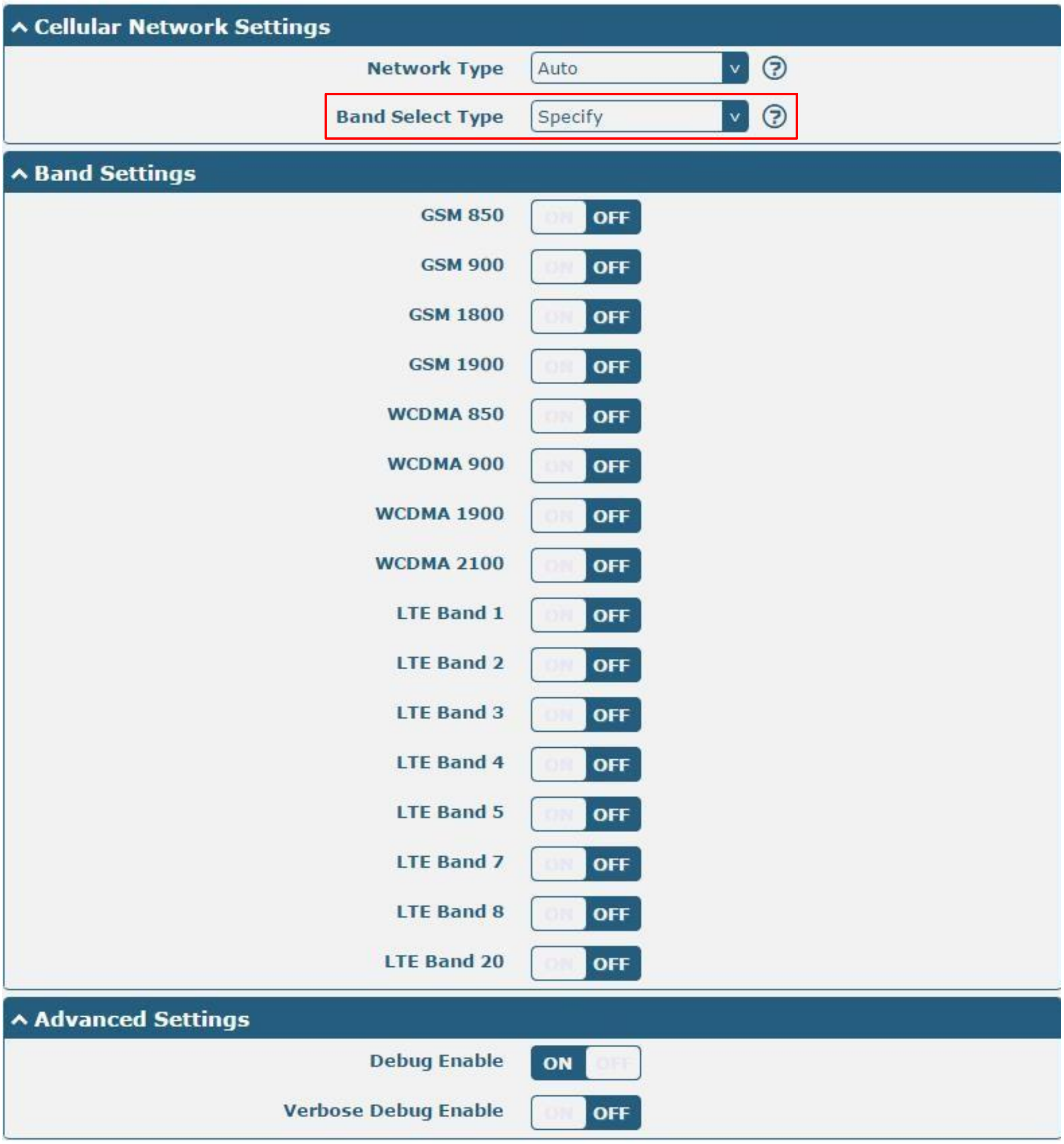
Band Select Type: All

^ Advanced Settings

Debug Enable: ON

Verbose Debug Enable: OFF

The window is displayed as below when choosing “Specify” as the band select type.



^ Cellular Network Settings

Network Type: Auto

Band Select Type: Specify

^ Band Settings

GSM 850: OFF

GSM 900: OFF

GSM 1800: OFF

GSM 1900: OFF

WCDMA 850: OFF

WCDMA 900: OFF

WCDMA 1900: OFF

WCDMA 2100: OFF

LTE Band 1: OFF

LTE Band 2: OFF

LTE Band 3: OFF

LTE Band 4: OFF

LTE Band 5: OFF

LTE Band 7: OFF

LTE Band 8: OFF

LTE Band 20: OFF

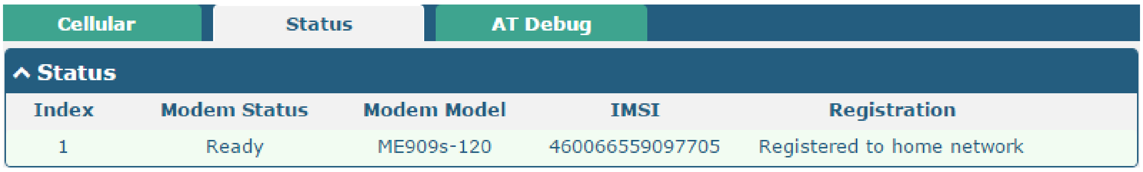
^ Advanced Settings

Debug Enable: ON

Verbose Debug Enable: OFF

Cellular		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
SIM Card	Set the currently editing SIM card.	SIM1
Phone Number	Enter the phone number of the SIM card.	Null
PIN Code	Enter a 4-8 characters PIN code used for unlocking the SIM.	Null
Extra AT Cmd	Enter the AT commands used for cellular initialization.	Null
Telnet Port	Specify the Port listening of telnet service, used for AT over Telnet.	0
Cellular Network Settings		
Network Type	Select from " Auto" , " 2G Only" , " 2G First" , " 3G Only" , " 3G First" , " 4G Only" , " 4G First" . Auto: Connect to the best signal network automatically 2G Only: Only the 2G network is connected 2G First: Connect to the 2G network preferentially 3G Only: Only the 3G network is connected 3G First: Connect to the 3G network preferentially 4G Only: Only the 4G network is connected 4G First: Connect to the 4G network preferentially	Auto
Band Select Type	Select from "All" or "Specify". You may choose certain bands if choosing "Specify".	All
Advanced Settings		
Debug Enable	Click the toggle button to enable/ disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/ disable this option. Enable for verbose debugging information output.	OFF

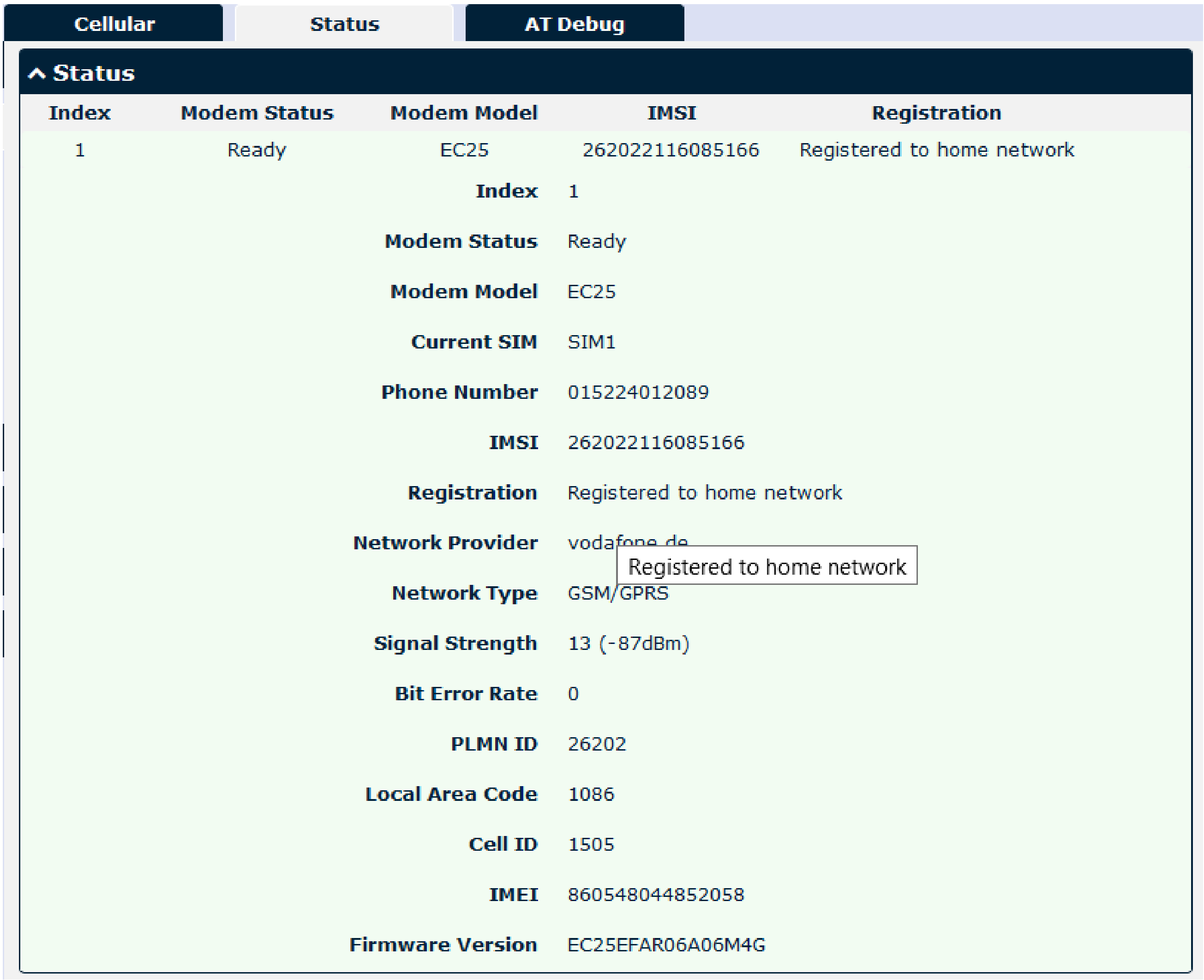
This section allows you to view the status of the cellular connection.



^ Status

Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	ME909s-120	460066559097705	Registered to home network

Click the row of status, the details status information will be displayed under the row.



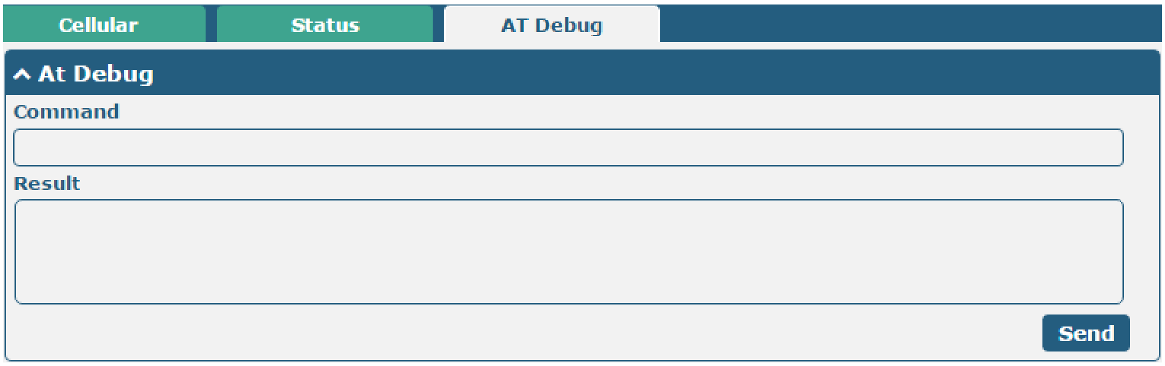
Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	EC25	262022116085166	Registered to home network

Index	1
Modem Status	Ready
Modem Model	EC25
Current SIM	SIM1
Phone Number	015224012089
IMSI	262022116085166
Registration	Registered to home network
Network Provider	vodafone.de
Network Type	GSM/GPRS
Signal Strength	13 (-87dBm)
Bit Error Rate	0
PLMN ID	26202
Local Area Code	1086
Cell ID	1505
IMEI	860548044852058
Firmware Version	EC25EFAR06A06M4G

Status	
Item	Description
Index	Indicate the ordinal of the list.
Modem Status	Show the status of the radio module.
Modem Model	Show the model of the radio module.
Current SIM	Show the SIM card that your router is using.
Phone Number	Show the phone number of the current SIM. Note: This option will be displayed if enter manually in Cellular > Advanced Cellular Settings > SIM1/SIM2 > General Settings > Phone Number
IMSI	Show the IMSI number of the current SIM.
ICCID	Show the ICCID number of the current SIM.
Registration	Show the current network status.
Network Provider	Show the name of Network Provider.
Network Type	Show the current network service type, e.g. GPRS.
Signal Strength	Show the signal strength detected by the mobile.
Registered band	Show the current frequency band.

RSRP	Show the reference signal received power.
RSRQ	Show the reference signal reception quality.
Bit Error Rate	Show the current bit error rate.
PLMN ID	Show the current PLMN ID.
Local Area Code	Show the current local area code used for identifying different area.
Cell ID	Show the current cell ID used for locating the router.
IMEI	Show the IMEI (International Mobile Equipment Identity) number of the radio module.
Firmware Version	Show the current firmware version of the radio module.

This page allows you to check the AT Debug.



AT Debug		
Item	Description	Default
Command	Enter the AT command that you want to send to cellular module in this text box.	Null
Result	Show the AT command responded by cellular module in this text box.	Null
Send	Click the button to send AT command.	--

3.10 Interface > Wi-Fi

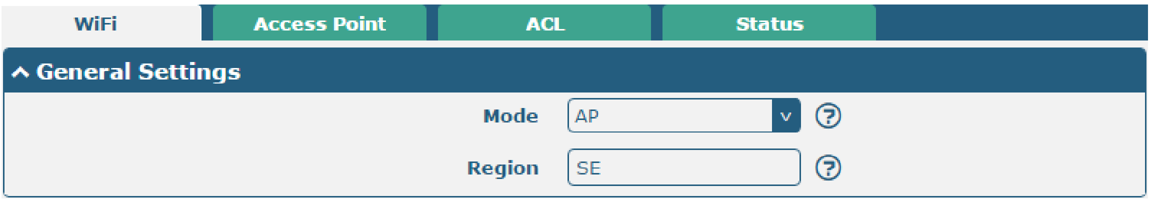
This section allows you to configure the parameters of two Wi-Fi modes. DSR-211 Router supports either Wi-Fi AP mode or Client mode, and default as AP mode.

Note: Need to reboot to make configuration take effect if switching the AP and Client mode.

Wi-Fi AP

Configure DSR-211 Router as Wi-Fi AP

Click Interface > Wi-Fi > Wi-Fi, select “AP” as the mode and click “Submit”.

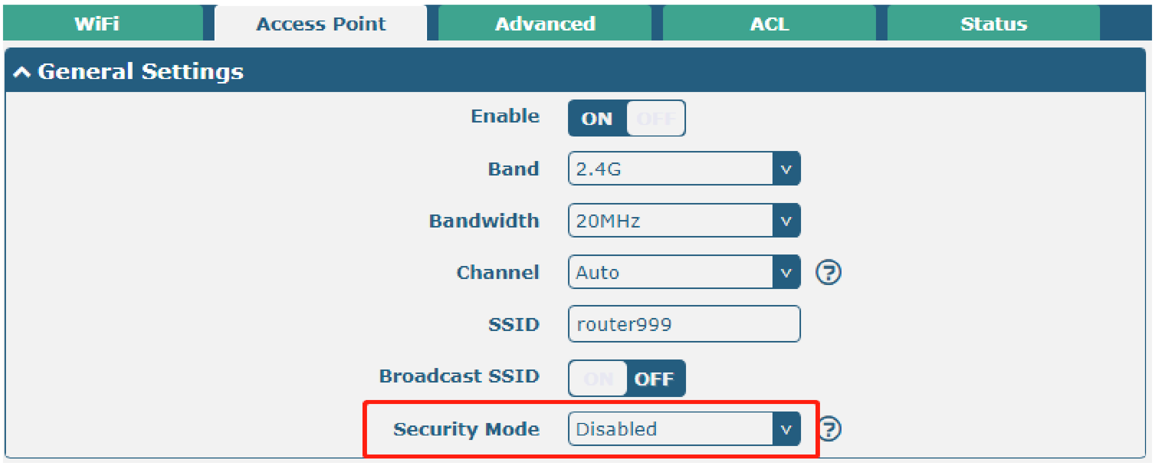


Mode: AP

Region: SE

Note: Please remember to click Save & Apply > Reboot after finish the configuration, so that the configuration can be took effect.

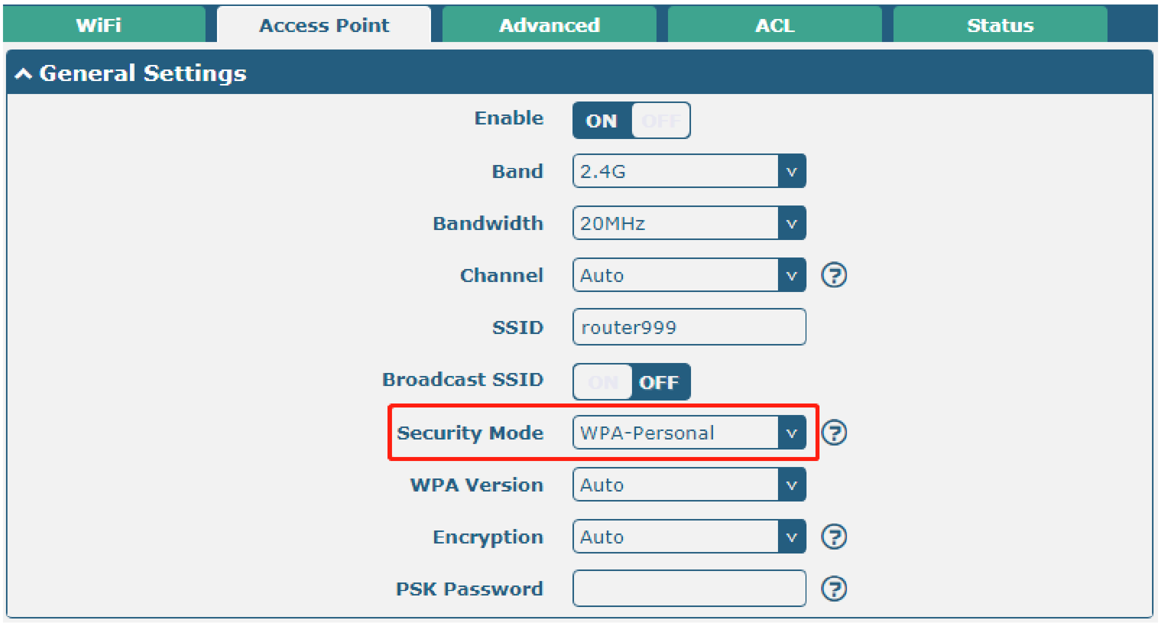
Click the Access Point column to configure the parameters of Wi-Fi AP.
By default, the security mode is set as “ Disabled”.



General Settings

Enable: ON
Band: 2.4G
Bandwidth: 20MHz
Channel: Auto
SSID: router999
Broadcast SSID: OFF
Security Mode: Disabled

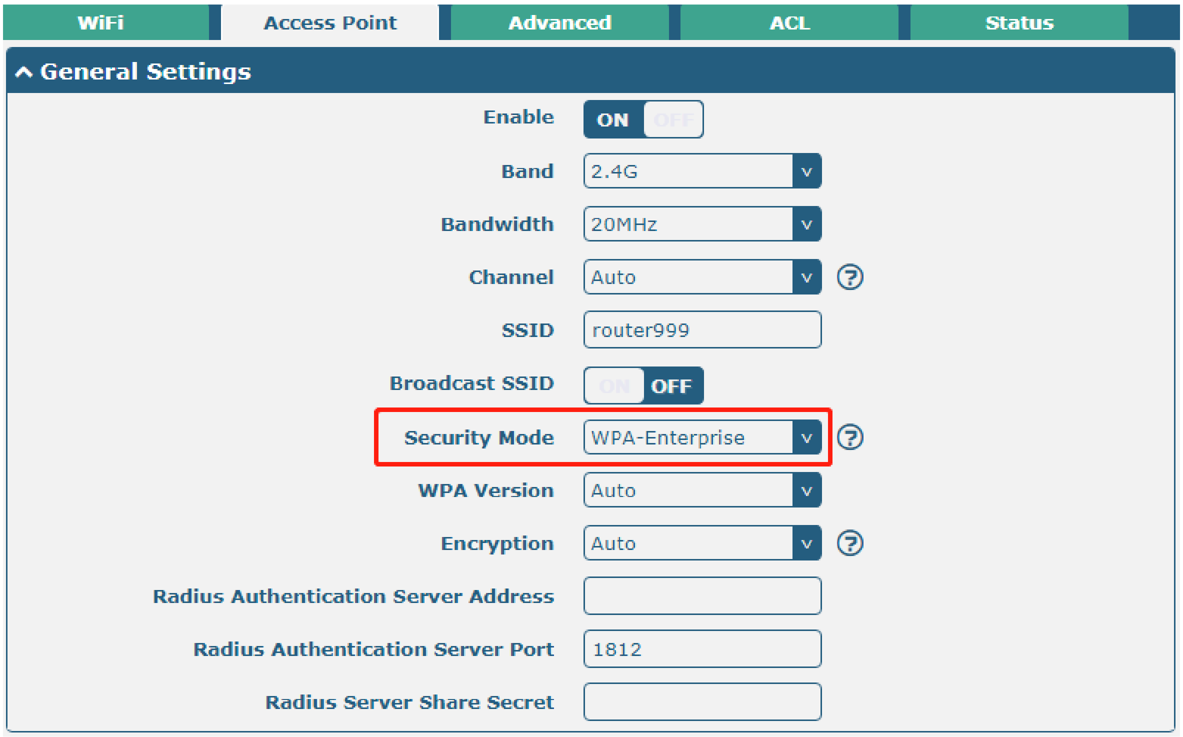
The window is displayed as below when setting “ WPA-Personal” as the security mode.



General Settings

Enable: ON
Band: 2.4G
Bandwidth: 20MHz
Channel: Auto
SSID: router999
Broadcast SSID: OFF
Security Mode: WPA-Personal
WPA Version: Auto
Encryption: Auto
PSK Password:

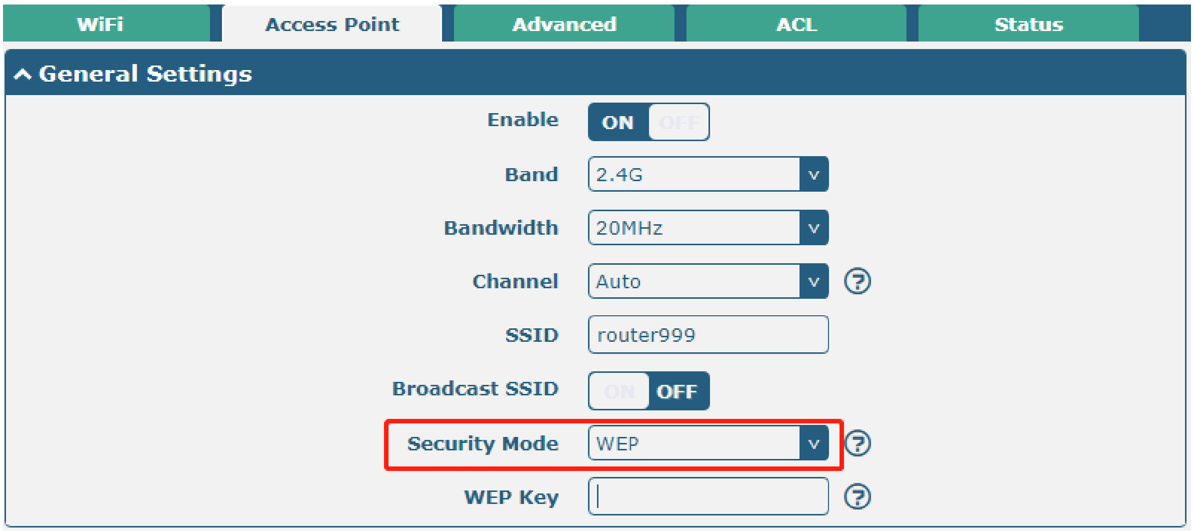
The window is displayed as below when setting “WEP-Enterprise” as the security mode.



General Settings

Enable: ON
Band: 2.4G
Bandwidth: 20MHz
Channel: Auto
SSID: router999
Broadcast SSID: OFF
Security Mode: WPA-Enterprise
WPA Version: Auto
Encryption: Auto
Radius Authentication Server Address:
Radius Authentication Server Port: 1812
Radius Server Share Secret:

When "WEP" is selected as the security mode, the window is displayed as follows:

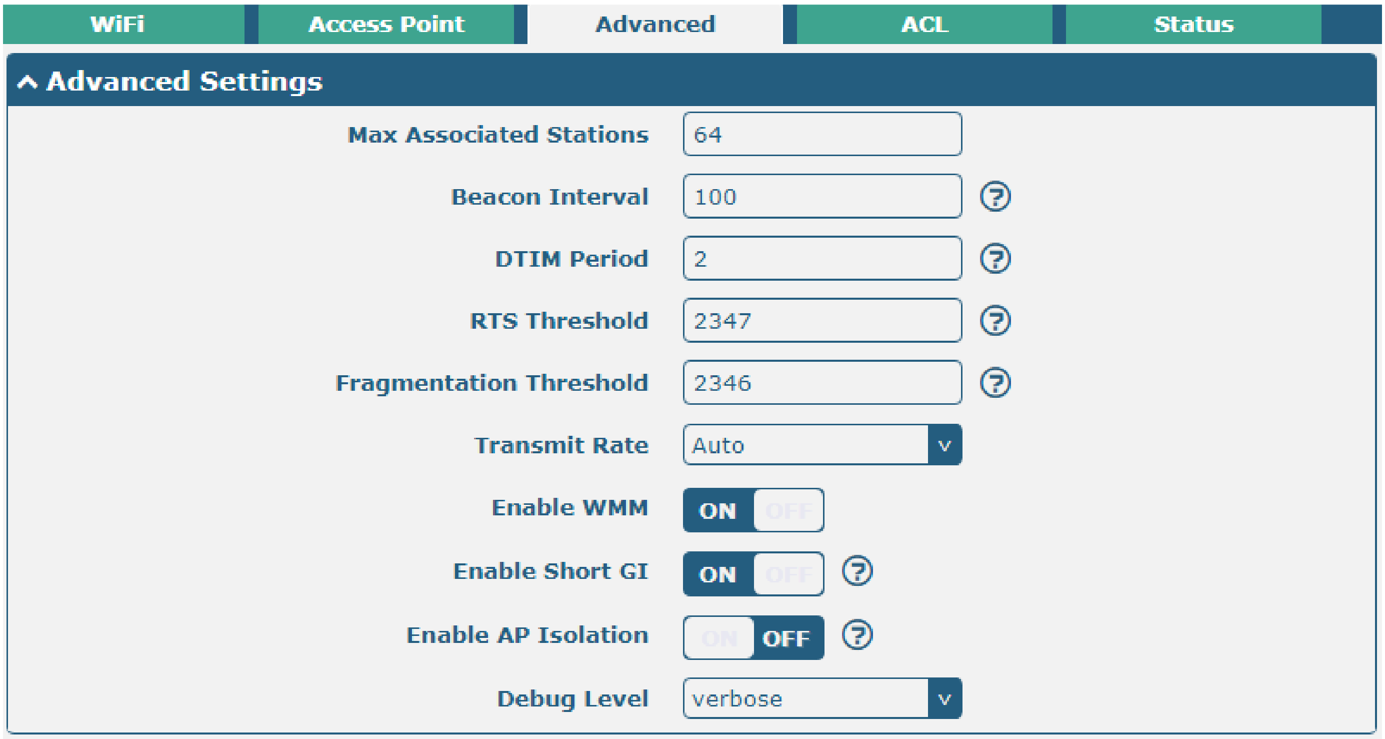


General Settings

Enable: ON
Band: 2.4G
Bandwidth: 20MHz
Channel: Auto
SSID: router999
Broadcast SSID: OFF
Security Mode: WEP
WEP Key:

General Settings @ Access Point		
Item	Description	Default
Enable	Click the toggle button to enable/ disable the Wi-Fi access point option.	OFF
Band	Choose from “2.4G” or “ 5G” .	2.4G
Bandwidth	Select from “20MHz” , “ 40MHz” . 40 MHz channel width provides twice the data rate available over a single 20 MHz channel.	20MHz
Channel	Select the frequency channel, including “ Auto” , “ 1” , “ 2” ......“ 13” . Auto: Router will scan all frequency channels until the best one is found 1~13: Router will be fixed to work with this channel Following are the frequency of 1~ 13 channel. 1: 2412 MHz 2: 2417 MHz 3: 2422 MHz 4: 2427 MHz 5: 2432 MHz 6: 2437 MHz 7: 2442 MHz 8: 2447 MHz 9: 2452 MHz 10: 2457 MHz 11: 2462 MHz 12: 2467 MHz 13: 2472 MHz	Auto
SSID	Enter the Service Set Identifier, the name of your wireless network. The SSID of a client and the SSID of the AP must be identical for the client and AP to be able to communicate with each other. Enter 1 to 32 characters.	router
Broadcast SSID	Click the toggle button to enable/ disable the SSID being broadcast. When enabled, the client can scan your SSID. When disabled, the client cannot scan your SSID. If you want to connect to the router AP, you need to manually enter the SSID of router AP at Wi-Fi client side.	ON
Security Mode	Select from “Disabled” , “ WPA-Personal” or “ WEP-Enterprise” . Disabled: User can access the Wi-Fi without the password when disable security Note: It is strongly recommended for security purposes that you do not choose this kind of mode. WPA-Personal: WiFi access protection, only one password can be provided for identity authentication. WEP-Enterprise: Wi-Fi secure network protection with RADIUS service. WEP: Wired Equivalent Privacy provides encryption for wireless device’s data transmission.	Disabled
WPA Version	Select from “Auto”, “ WPA” or “ WPA2” . Auto: Router will choose automatically the most suitable WPA version WPA2 is a stronger security feature than WPA	Auto

Encryption	Select from “Auto”, “ TKIP” or “ AES” . Auto: Router will choose automatically the most suitable encryption TKIP: Temporal Key Integrity Protocol (TKIP) encryption uses a wireless connection. TKIP encryption can be used for WPA-PSK and WPA with 802.1x authentication. Note: It's not recommended to use TKIP encryption in 802.11n mode. AES: AES encryption uses a wireless connection. AES can be used for WPA-PSK and WPA with 802.1x authentication. AES is a stronger encryption algorithm than TKIP.	Auto
PSK Password	Enter the Pre share key password. Enter 8 to 63 characters.	Null
Radius Authentication server address	Address used by the RADIUS server.	Null
Radius Authentication server port	Port used by the RADIUS server.	1812
Radius Authentication server shared key	A trusted connection is established between the RADIUS client and the RADIUS server, and the exchange of authentication messages is guaranteed by the shared key.	Null



Advanced Settings

Max Associated Stations: 64

Beacon Interval: 100

DTIM Period: 2

RTS Threshold: 2347

Fragmentation Threshold: 2346

Transmit Rate: Auto

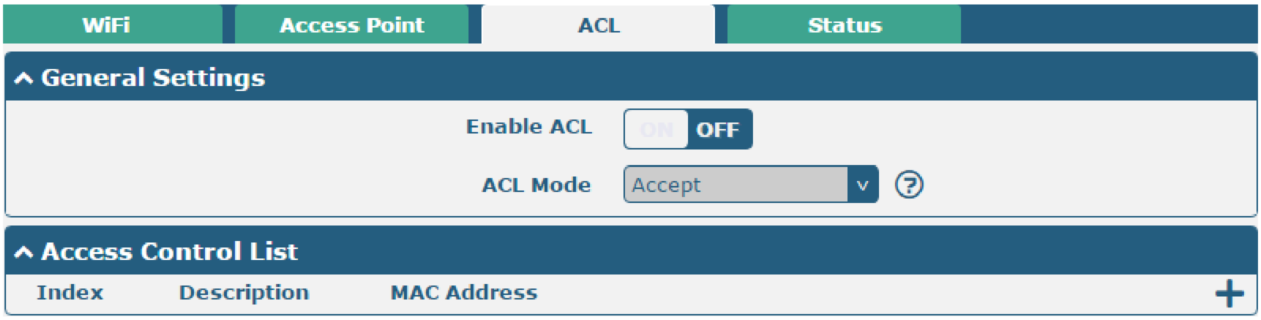
Enable WMM: ON

Enable Short GI: ON

Enable AP Isolation: OFF

Debug Level: verbose

Advanced Settings		
Item	Description	Default
Maximum number of access points	Set the maximum number of clients allowed to access the device AP. (Avalue of 0 means no limit)	64
Signal interval	Sets the signal interval for the device AP to broadcast Beacon messages, which is used to declare the existence of a wireless network.	100
DTIM cycle	Set the Delivery Traffic Indication Message period, that is, the period for delivering transmission instruction information. DTIM is used in the power saving mode. Device APs will multicast traffic based on this interval.	2
RTS / CTS threshold	Set the Request To Send threshold, that is, the request to send threshold. When the threshold is set to 2347, the device AP does not send detection signals before sending data; when the threshold is set to 0, the device AP must send detection signals before sending data.	2347
Fragmentation threshold	Set the packet threshold for WiFi AP packets. The recommended default is 2346.	2346
Transmission rate	Data transfer rates can be automated or specified by default. Select from "Auto", "1Mbps", "2Mbps", "5.5Mbps", "6Mbps", "11Mbps", "12Mbps", "18Mbps", "24Mbps", "36Mbps", "48Mbps", or “54Mbps	Auto
Enable WMM	Click the toggle button to enable/disable the WMM option.	ON
Enable Short GI	Click the toggle button to enable/disable the Short Guard Interval. It is the blank period between two symbols and provides buffer time for signal delay. Using a short guard interval can increase the data rate by 11%, but can also lead to higher packet error rates.	ON
Enable AP isolation	Click the switch button to enable/disable the AP isolation option. When enabled, isolate all connected wireless devices, which cannot be accessed directly through the WLAN.	OFF
Commissioning level	Select debug level. Select from "verbose," "debug," "info," "notice," "warning," or "none."	none



General Settings

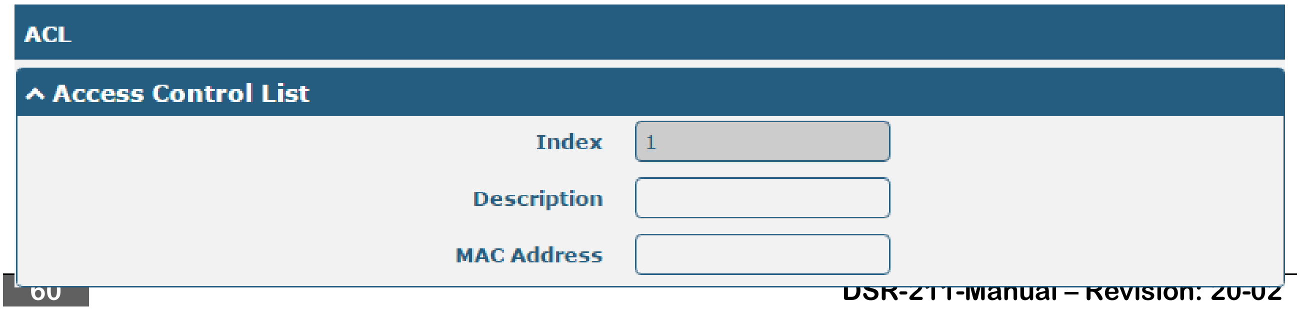
Enable ACL: ON OFF

ACL Mode: Accept

Access Control List

Index	Description	MAC Address

Click + to add a MAC address to the Access Control List. The maximum count for MAC address is 64.



ACL

Access Control List

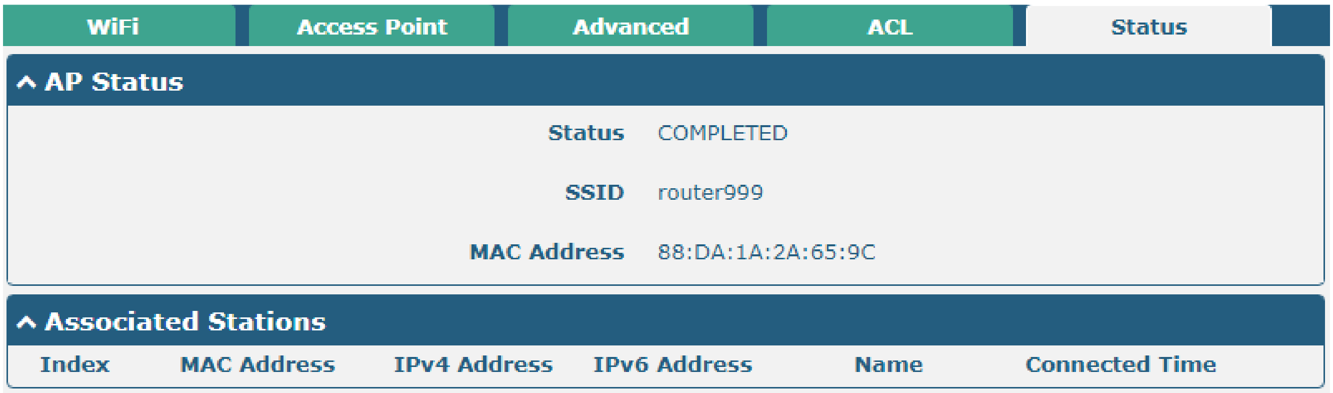
Index: 1

Description:

MAC Address:

ACL		
Item	Description	Default
General Settings		
Enable ACL	Click the toggle button to enable ACL (Access Control List) option.	OFF
ACL Mode	Select from “Accept” or “Deny”. Accept Only the packets fitting the entities of the “Access Control List ” can be allowed Deny: All the packets fitting the entities of the “Access Control List ” will be denied Note: Router can only allow or deny devices which are included in “Access Control List ” at one time.	Accept
Access Control List		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this access control list.	Null
MAC Address	Add a MAC address here.	Null

This section allows you to view the status of AP.



Status COMPLETED

SSID router999

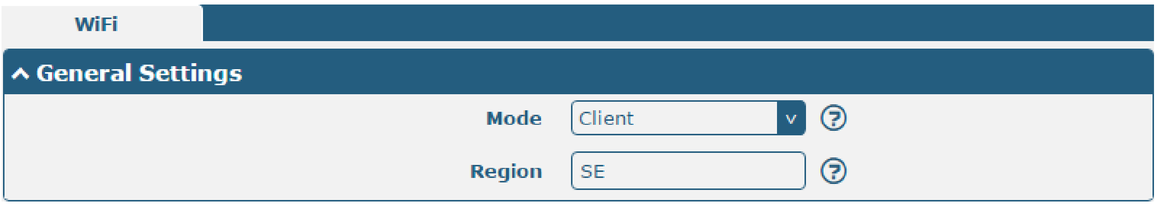
MAC Address 88:DA:1A:2A:65:9C

Index	MAC Address	IPv4 Address	IPv6 Address	Name	Connected Time

Note: The WiFi function is turned off by default on the router. If you need to use it, please turn on WiFi according to the following steps and configure the router as a WiFi client.

Wi-Fi Client

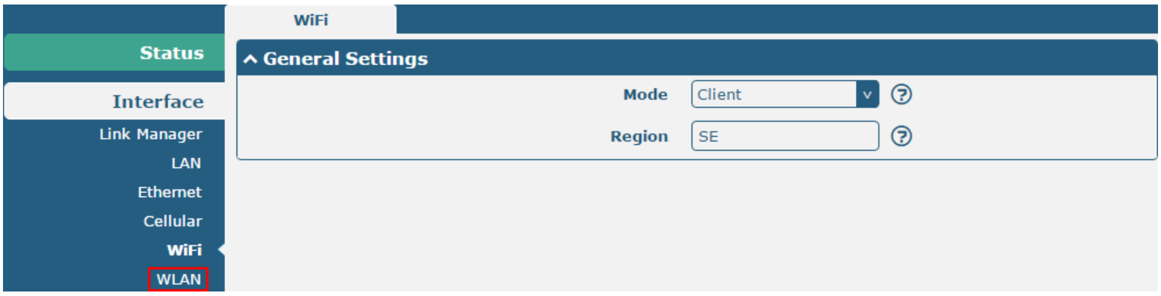
Configure DSR-211 as Wi-Fi client
Click Interface > Wi-Fi > Wi-Fi, select “Client ” as the mode and click “ Submit”> Save & Apply



Mode Client

Region SE

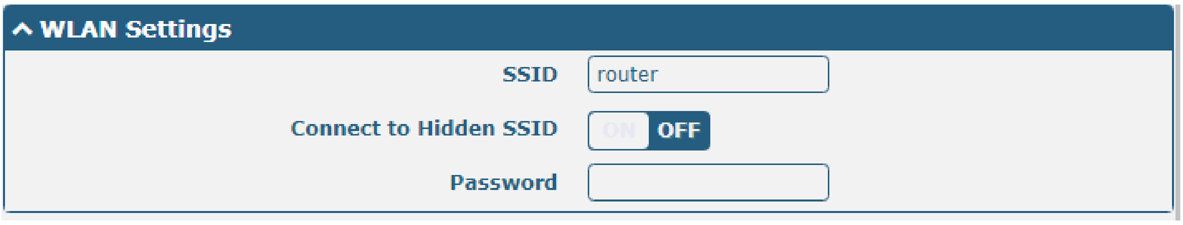
And then a " WLAN" column will appear under the Interface list.



Mode: Client

Region: SE

Click Interface > Link Manager > Link Settings, and click the edit button of WLAN, then configure the related parameters of WLAN.

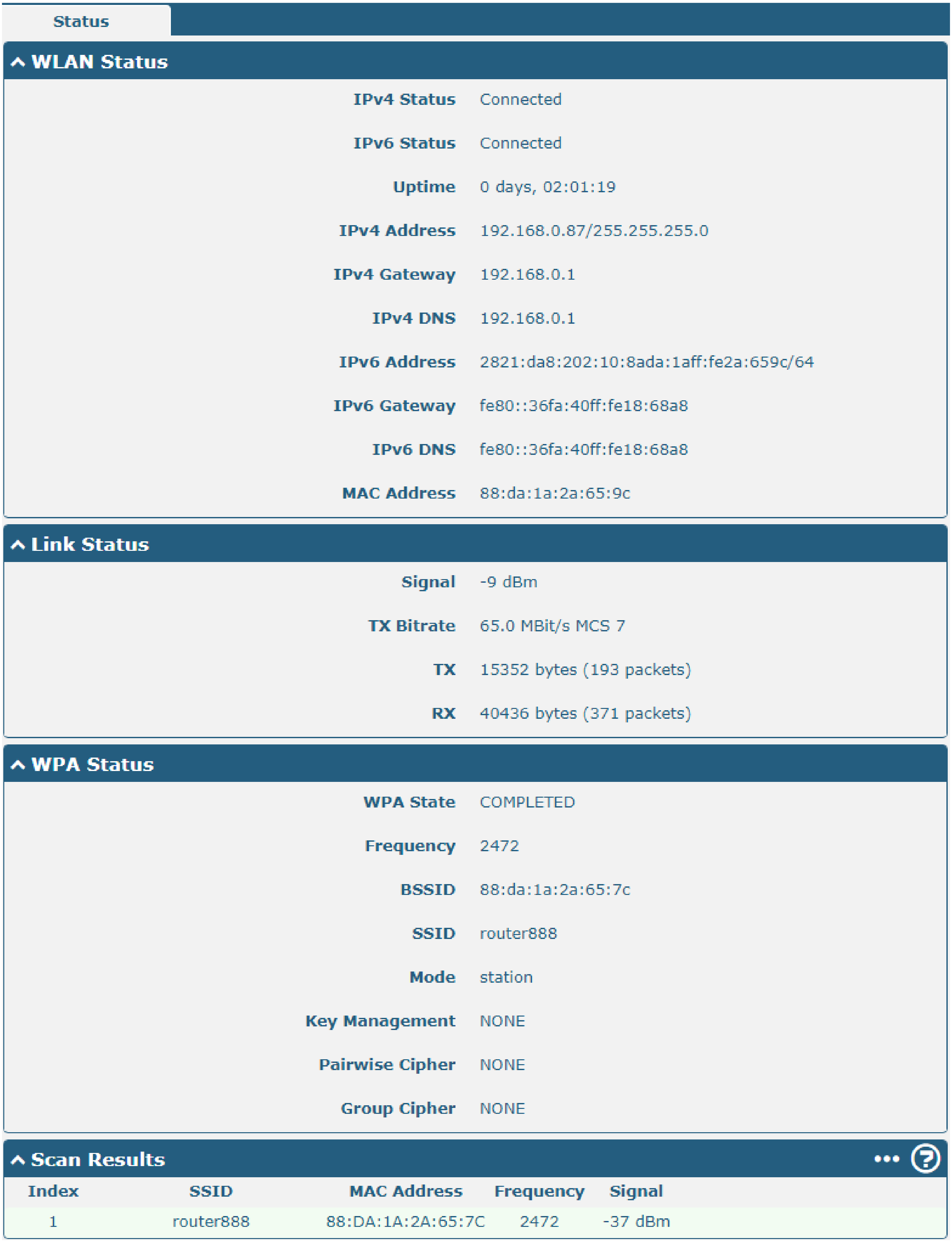


SSID: router

Connect to Hidden SSID: ON OFF

Password:

Click Interface > WLAN to configure the parameters of WiFi Client after setting the mode as Client. Please remember to click Save & Apply > Reboot after finish the configuration, so that the configuration can be took effect.



Status

WLAN Status

IPv4 Status	Connected
IPv6 Status	Connected
Uptime	0 days, 02:01:19
IPv4 Address	192.168.0.87/255.255.255.0
IPv4 Gateway	192.168.0.1
IPv4 DNS	192.168.0.1
IPv6 Address	2821:da8:202:10:8ada:1aff:fe2a:659c/64
IPv6 Gateway	fe80::36fa:40ff:fe18:68a8
IPv6 DNS	fe80::36fa:40ff:fe18:68a8
MAC Address	88:da:1a:2a:65:9c

Link Status

Signal	-9 dBm
TX Bitrate	65.0 MBit/s MCS 7
TX	15352 bytes (193 packets)
RX	40436 bytes (371 packets)

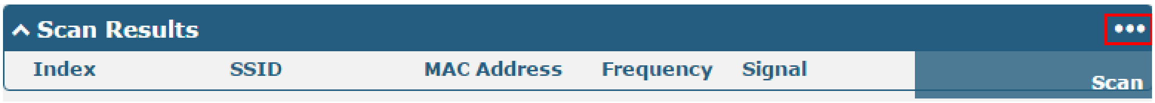
WPA Status

WPA State	COMPLETED
Frequency	2472
BSSID	88:da:1a:2a:65:7c
SSID	router888
Mode	station
Key Management	NONE
Pairwise Cipher	NONE
Group Cipher	NONE

Scan Results

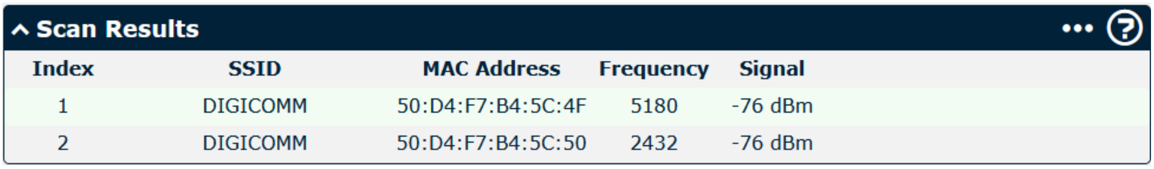
Index	SSID	MAC Address	Frequency	Signal
1	router888	88:DA:1A:2A:65:7C	2472	-37 dBm

This window allows you to scan for all the available SSIDs in your area and click one of those shown on the " Scan Results" list.



^ Scan Results

Index	SSID	MAC Address	Frequency	Signal

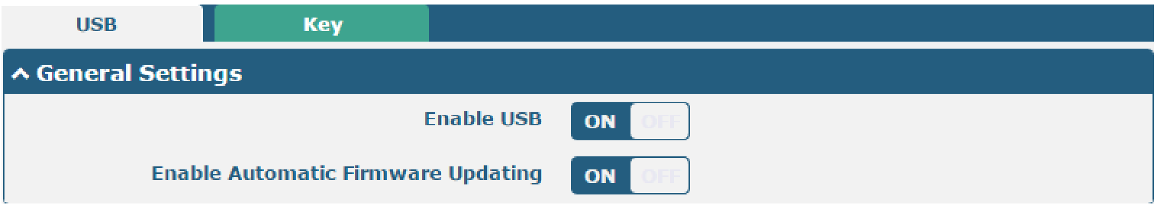


^ Scan Results

Index	SSID	MAC Address	Frequency	Signal
1	DIGICOMM	50:D4:F7:B4:5C:4F	5180	-76 dBm
2	DIGICOMM	50:D4:F7:B4:5C:50	2432	-76 dBm

3.11 Interface > USB

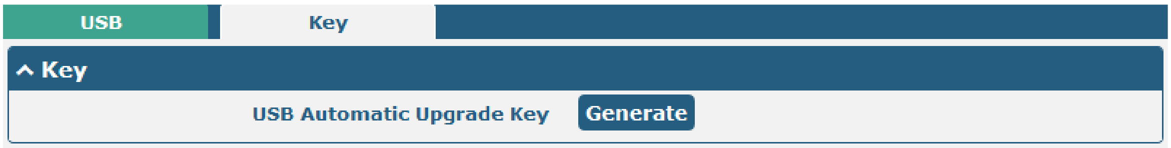
This section allows you to set the USB parameters. The USB interface of DSR-211 Router can be used for firmware upgrade and configuration upgrade.



^ General Settings

Enable USB: ON

Enable Automatic Firmware Updating: ON



^ Key

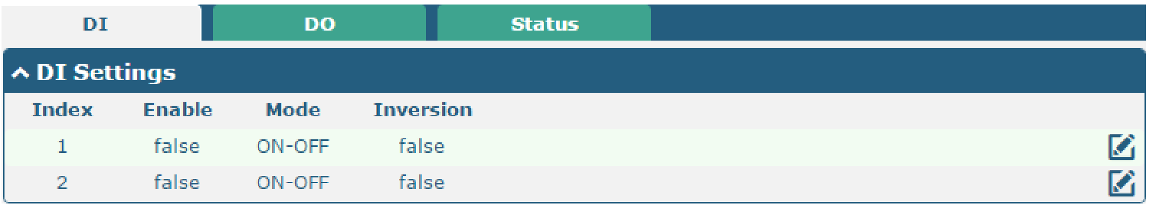
USB Automatic Upgrade Key: Generate

General Settings @ USB		
Item	Description	Default
Enable USB	Click the toggle button to enable/ disable the USB option.	ON
Enable Automatic Firmware Updating	Click the toggle button to enable/ disable this option. Enable to automatically update the firmware of DSR-211 when inserting a USB storage device with DSR-211 firmware.	ON
Key		
USB Automatic Update Key	Click Generate to generate a key. It is used to verify the key file in the U disk. If it is consistent, it can be upgraded.	--

3.12 Interface > DI / DO

This section allows you to set the DI/ DO parameters. Digital Input and Digital Output are the specific interfaces for DSR-211. The DI interface can be used for triggering alarm, while the DO can be used for controlling the slave device so as to realize real-time monitoring.

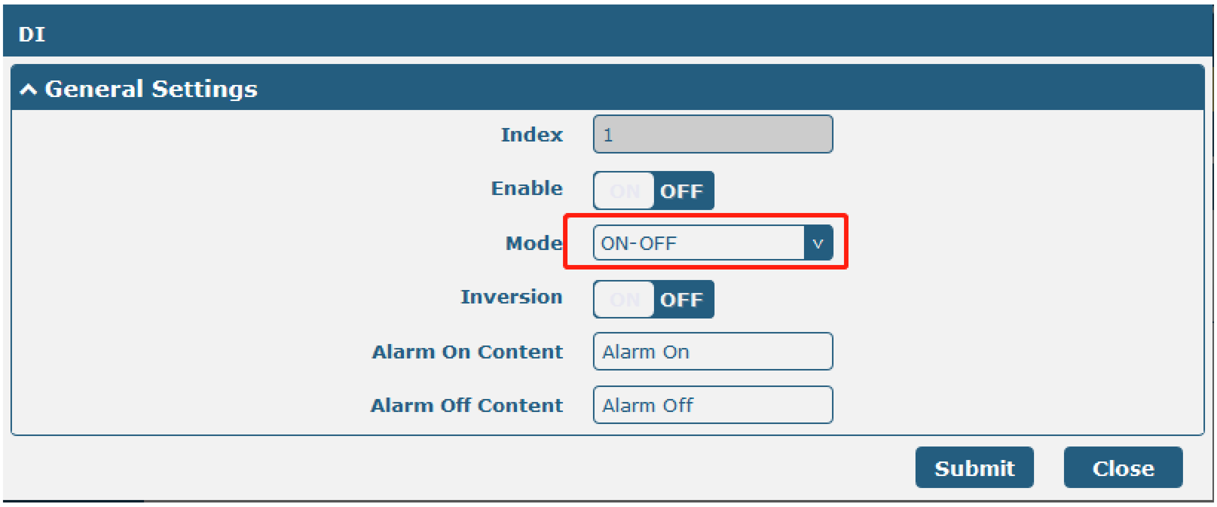
DI



DI Settings

Index	Enable	Mode	Inversion
1	false	ON-OFF	false
2	false	ON-OFF	false

Click the right-most ✎ button of index 1 as below. The default mode is “ ON-OFF”.

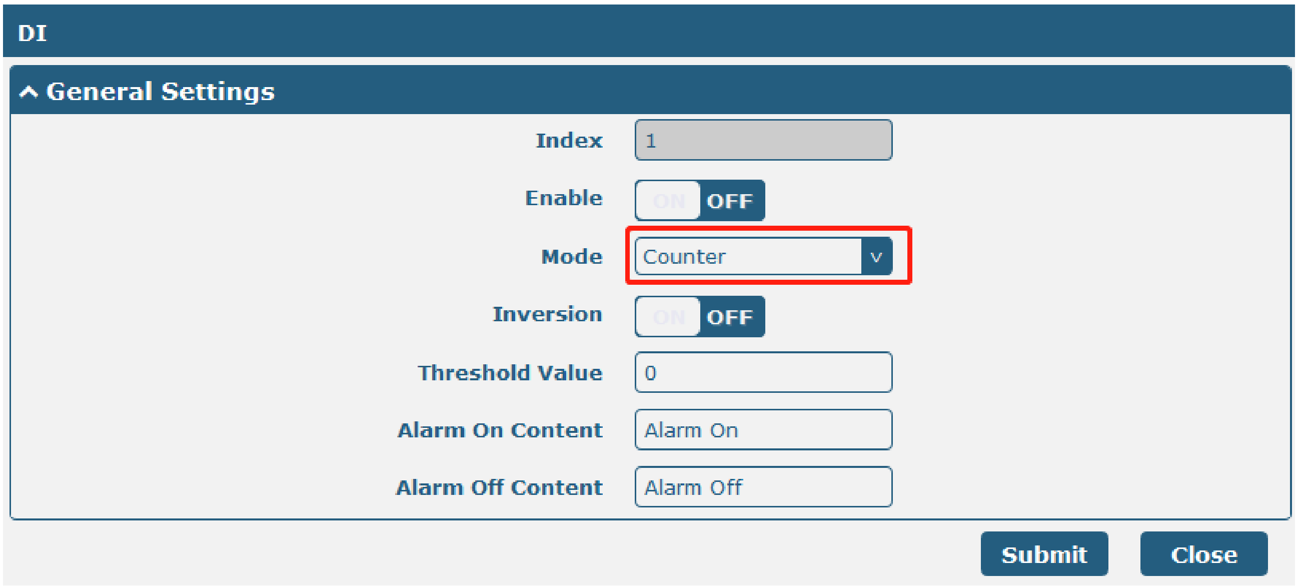


DI

General Settings

Index	1
Enable	ON OFF
Mode	ON-OFF
Inversion	ON OFF
Alarm On Content	Alarm On
Alarm Off Content	Alarm Off

The window is displayed as below when choosing “Counter” as the mode.



DI

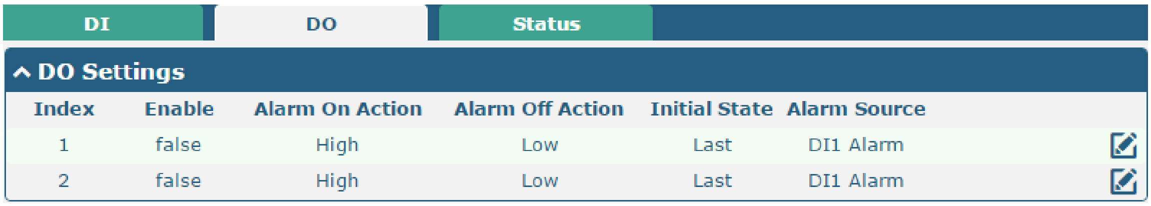
General Settings

Index	1
Enable	ON OFF
Mode	Counter
Inversion	ON OFF
Threshold Value	0
Alarm On Content	Alarm On
Alarm Off Content	Alarm Off

General Settings @ DI		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/ disable this DI.	OFF
Mode	Select from “ON-OFF” or “ Counter” . ON-OFF: DI interface support ON and OFF mode (high or low level electrical) trigger DI alarm. The mode default to ON, and OFF mode is available only when enabling the inversion feature ON—Under this mode, DI alarm status will be triggered to ON when DI interface open from GND or input a high level electrical (logic 1), on the contrary DI alarm status will be trigged to OFFwhen DI interface connect to GND or input a low level electrical (logic 0) OFF—Under this mode, DI alarm status will be triggered to ON when DI interface connect to GND or input a low level electrical (logic 0), on the contrary DI alarm status will be trigged to OFF when DI interface open from GND or input a high level electrical (logic 1) Counter: Event counter mode	ON-OFF
Inversion	Click the toggle button to enable/ disable this option. Enable to set DI mode as OFF mode.	OFF
Threshold Value	Set the threshold vale. It will trigger alarm when event counter reaches this figure. After triggering alarm, DI will keep counting but not trigger alarm again. Enter 0 to 65535 digits. (0=will not trigger alarm) Note: This option is only available when DI under the “ Counter” mode.	Null
Alarm On Content	When the alarm is on, show its content.	Alarm On
Alarm Off Content	When the alarm is off, show its content.	Alarm Off

Note: It defaults as high alarm, while turns to low alarm after enabling the “Inversion” button.

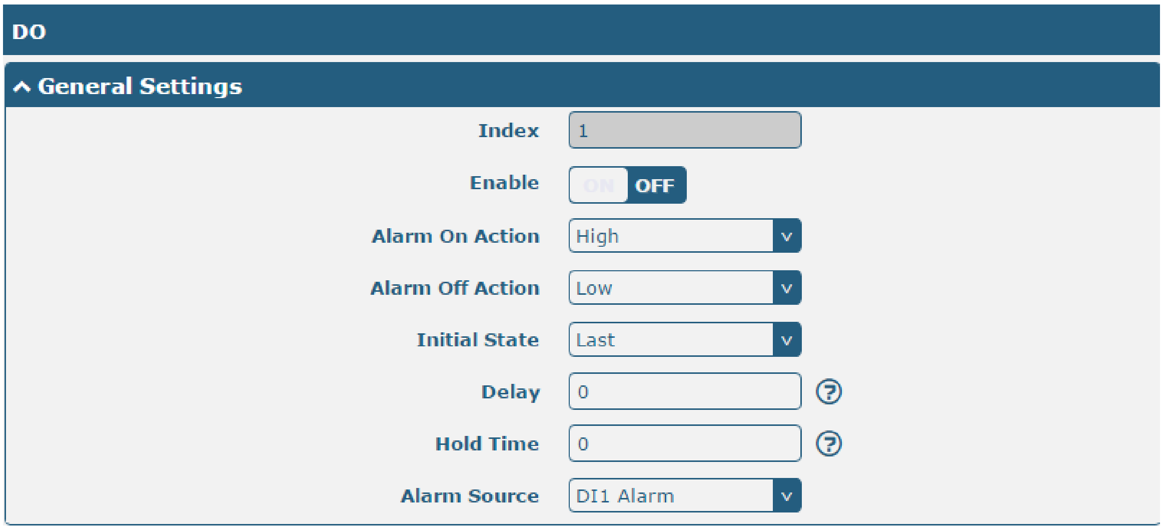
DO



^ DO Settings

Index	Enable	Alarm On Action	Alarm Off Action	Initial State	Alarm Source	
1	false	High	Low	Last	DI1 Alarm	✎
2	false	High	Low	Last	DI1 Alarm	✎

Click ✎ to enter the DO configuration window.

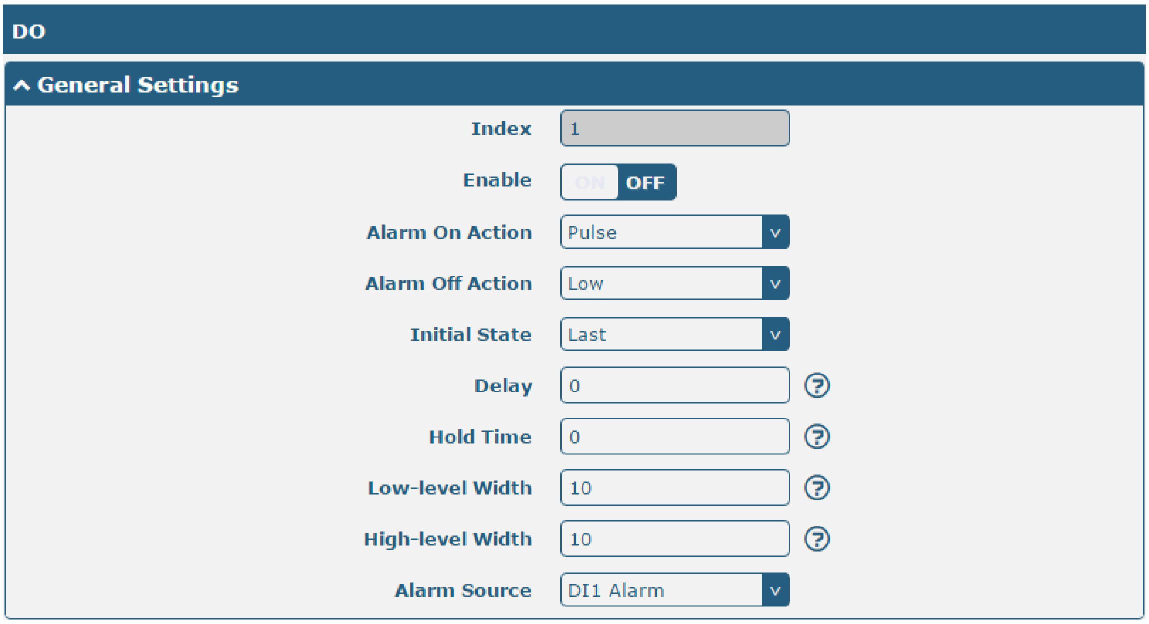


DO

General Settings

Index	1
Enable	ON OFF
Alarm On Action	High
Alarm Off Action	Low
Initial State	Last
Delay	0
Hold Time	0
Alarm Source	DI1 Alarm

The window is displayed as below when choosing “ Pulse” as the alarm on action.

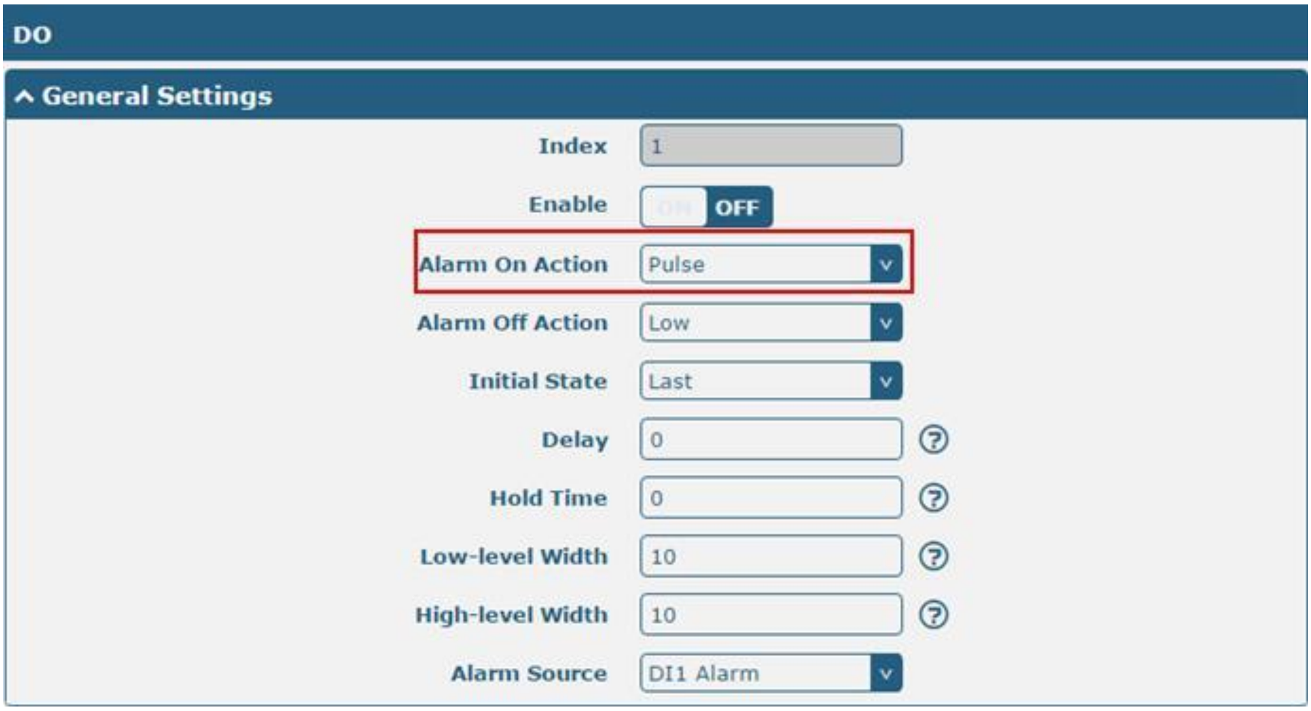


DO

General Settings

Index	1
Enable	ON OFF
Alarm On Action	Pulse
Alarm Off Action	Low
Initial State	Last
Delay	0
Hold Time	0
Low-level Width	10
High-level Width	10
Alarm Source	DI1 Alarm

The window is displayed as below when choosing "Pulse" as the alarm off action.



DO

General Settings

Index: 1

Enable: OFF

Alarm On Action: Pulse

Alarm Off Action: Low

Initial State: Last

Delay: 0

Hold Time: 0

Low-level Width: 10

High-level Width: 10

Alarm Source: DI1 Alarm

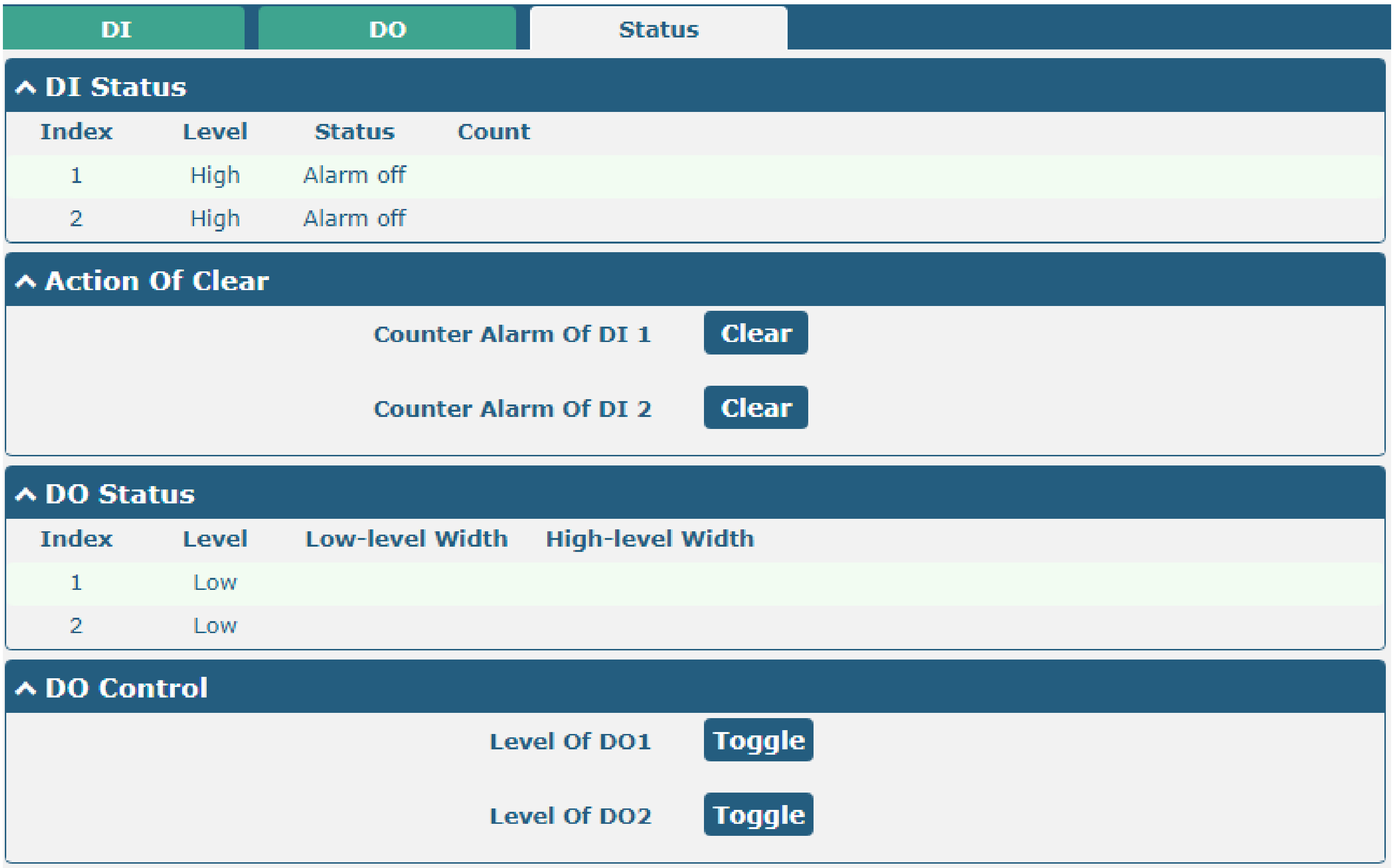
DO		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/ disable this DO.	OFF
Alarm On Action	Digital Output initiates when there is an alarm. Selected from " High", " Low" or " Pulse". High: a high electrical level output Low: a low electrical level output Pulse: Generates a square wave as specified in the pulse mode parameters when triggered	High
Alarm Off Action	Digital Output initiates when alarm removed. Selected from " High", " Low" or " Pulse". High: a high electrical level output Low: a low electrical level output Pulse: Generates a square wave as specified in the pulse mode parameters when triggered	Low
Initial State	Specify the Digital Output status when powered on. Selected from " Last ", " High" or" Low". Last: DO's status will consist with the status of last power off High: DO interface is in high electrical level Low: DO interface is in low electrical level	Low
Delay	Set the delay time for DO alarm start -up. The first pulse will be generated after a "Delay" . Enter from 0 to 30000ms. (0=generate pulse without delay)	0
Hold Time	Set the hold time of DO status (Alarm On Action/ Alarm Off Action). When the action time reach this specified time, DO will stop the action. Enter from 0 to 255 seconds. (0=keep on until the next action)	0

Low-level Width	Set the low-level width. It is available when enabling Pulse as " Alarm On Action/ Alarm Off Action" . In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The low level widths are specified here. Enter from 1 to 30000 ms.	10
High-level Width	Set the high-level width. It is available when enabling Pulse as " Alarm On Action/ Alarm Off Action" . In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The high level widths are specified here. Enter from 1 to 30000 ms.	10
Alarm Source	Digital Output initiates according to different alarm source. Selected from " DI1 Alarm", " DI2 Alarm". DI1/ DI2 Alarm: Digital Output triggers the related action when there is alarm from Digital Input.	DI1 Alarm

Status

This window allows you to view the status of DO and DI interface. It also can clear the counter alarm of DI in here.

Click Clear button to clear DI1 or DI2 monthly usage statistics info for counter alarm.



^ DI Status

Index	Level	Status	Count
1	High	Alarm off	
2	High	Alarm off	

^ Action Of Clear

Counter Alarm Of DI 1 Clear

Counter Alarm Of DI 2 Clear

^ DO Status

Index	Level	Low-level Width	High-level Width
1	Low		
2	Low		

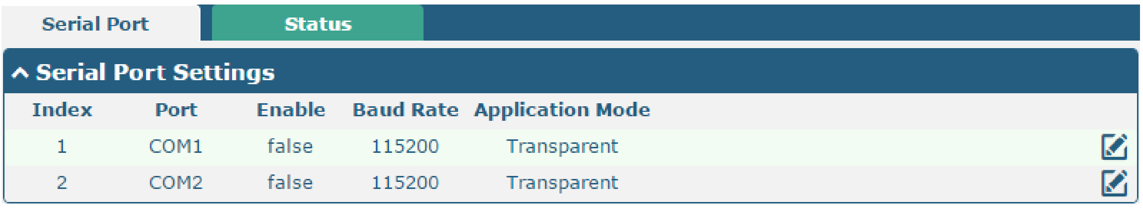
^ DO Control

Level Of DO1 Toggle

Level Of DO2 Toggle

3.13 Interface > Serial Port

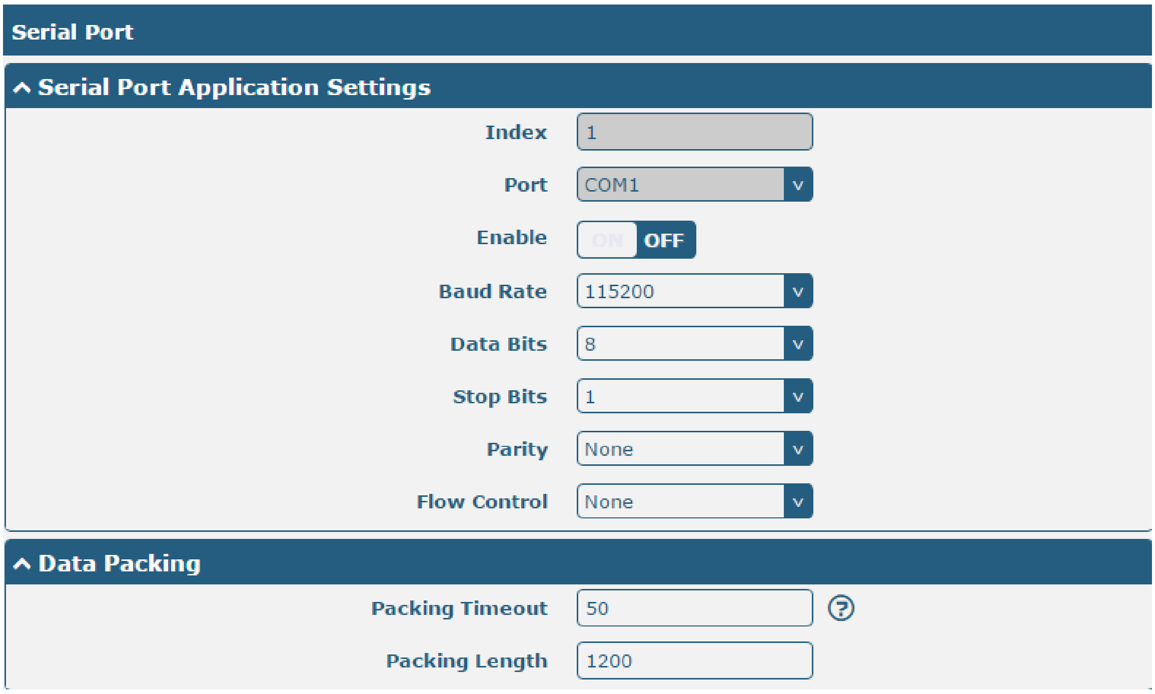
This section allows you to set the serial port parameters. DSR-211 Router supports one COM1 and one COM2, also can be configured as either two COM1 or two COM2.



Serial Port Settings

Index	Port	Enable	Baud Rate	Application Mode
1	COM1	false	115200	Transparent
2	COM2	false	115200	Transparent

Click the ✎ button on the most right of COM1, the pop-up window is as follows:



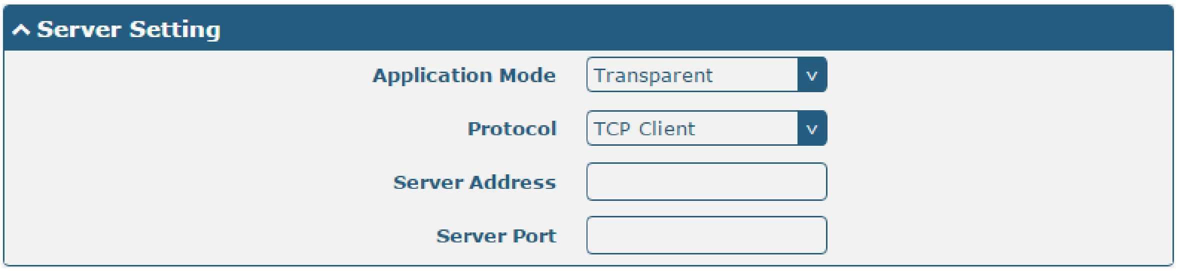
Serial Port

Serial Port Application Settings

Index	1
Port	COM1
Enable	OFF
Baud Rate	115200
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None

Data Packing

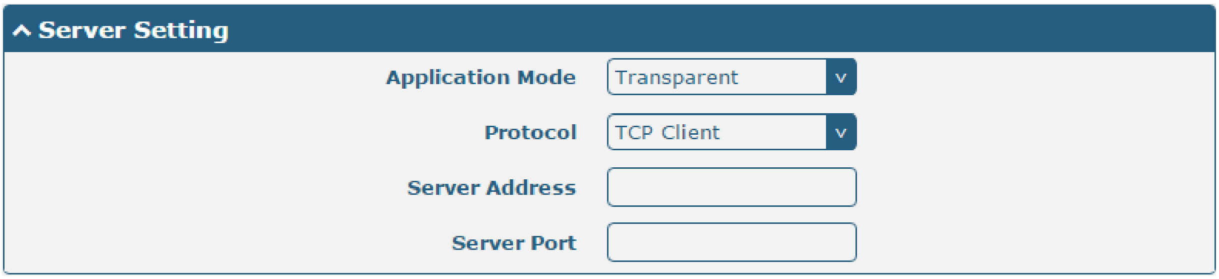
Packing Timeout	50
Packing Length	1200



Server Setting

Application Mode	Transparent
Protocol	TCP Client
Server Address	
Server Port	

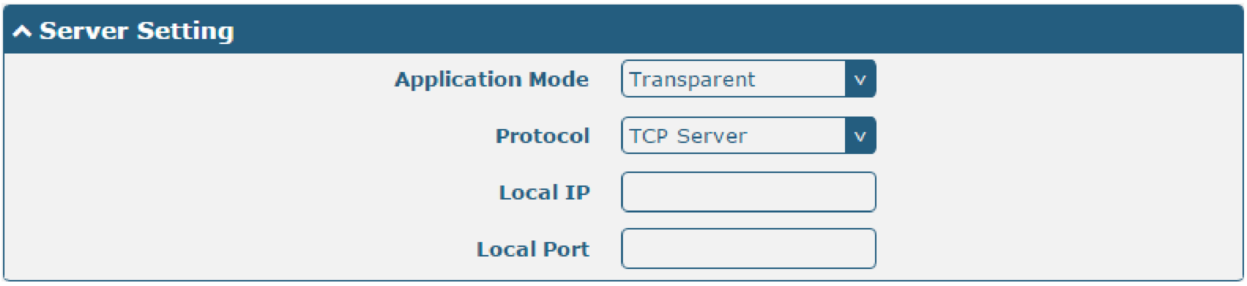
The window is displayed as below when choosing “ Transparent ” as the application mode and TCP Client as the Protocol



Server Setting

Application Mode	Transparent
Protocol	TCP Client
Server Address	
Server Port	

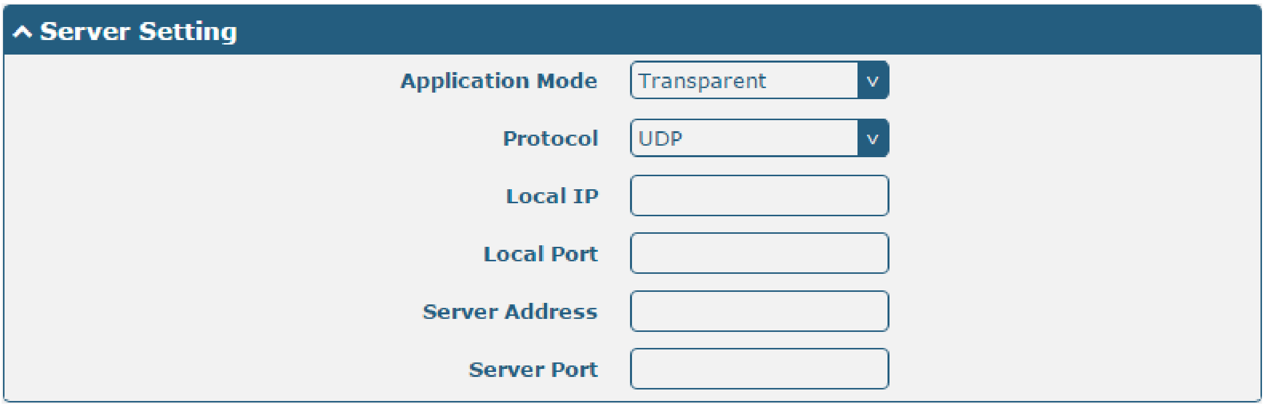
The window is displayed as below when choosing “Transparent ” as the application mode and TCP Server as the protocol.



^ Server Setting

Application Mode	Transparent
Protocol	TCP Server
Local IP	
Local Port	

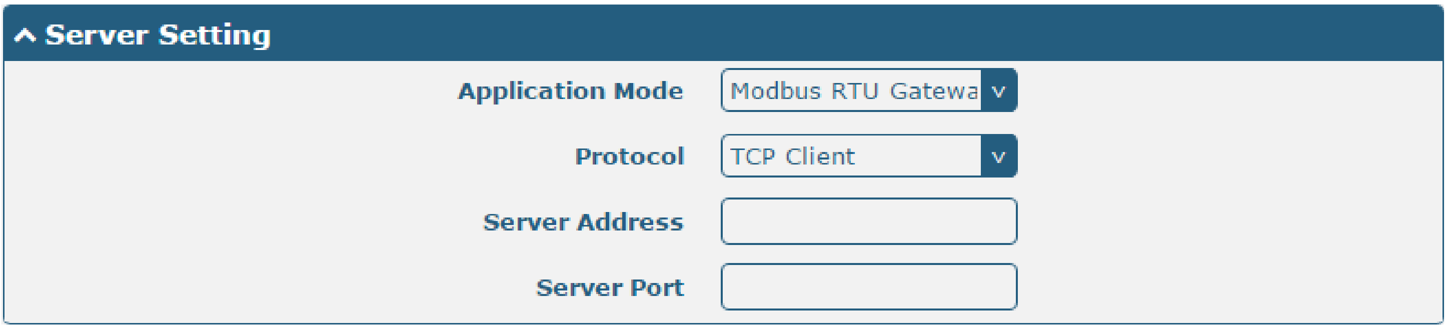
The window is displayed as below when choosing “Transparent ” as the application mode and UDP as the Protocol.



^ Server Setting

Application Mode	Transparent
Protocol	UDP
Local IP	
Local Port	
Server Address	
Server Port	

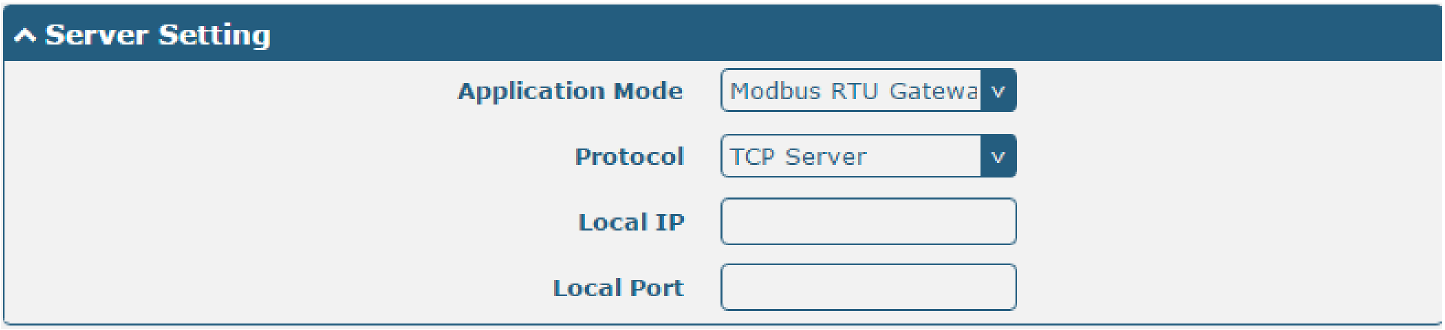
The window is displayed as below when choosing “ Modbus RTU Gateway ” as the application mode and TCP Client as the protocol



^ Server Setting

Application Mode	Modbus RTU Gatewa
Protocol	TCP Client
Server Address	
Server Port	

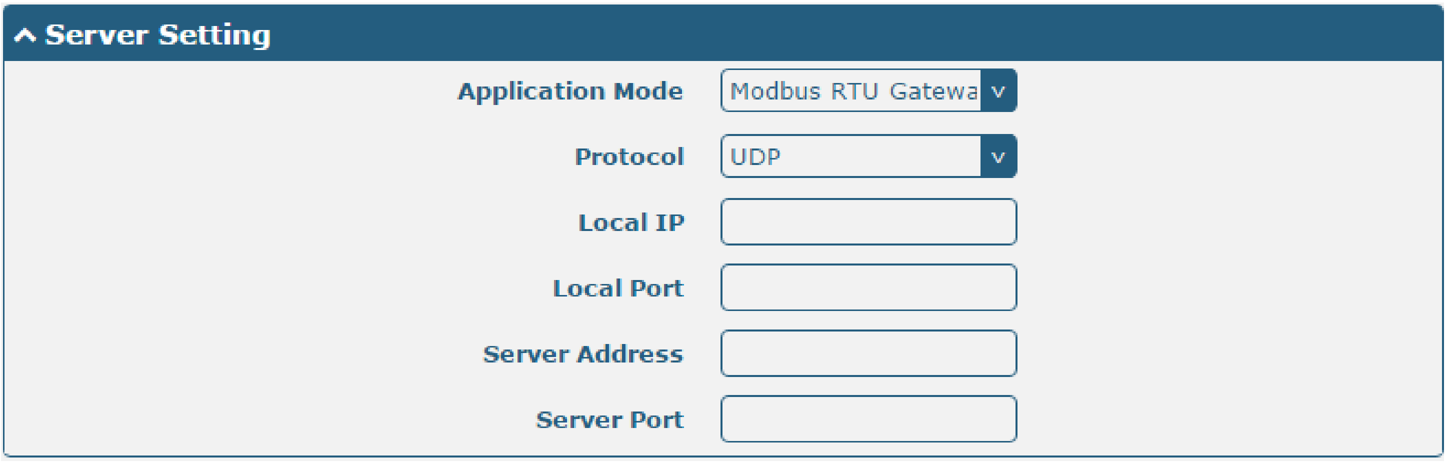
The window is displayed as below when choosing “Modbus RTU Gateway ” as the application mode and TCP Server as the protocol.



^ Server Setting

Application Mode	Modbus RTU Gatewa
Protocol	TCP Server
Local IP	
Local Port	

The window is displayed as below when choosing “Modbus RTU Gateway ” as the application mode and UDP as the protocol.



Server Setting

Application Mode: Modbus RTU Gatewa

Protocol: UDP

Local IP:

Local Port:

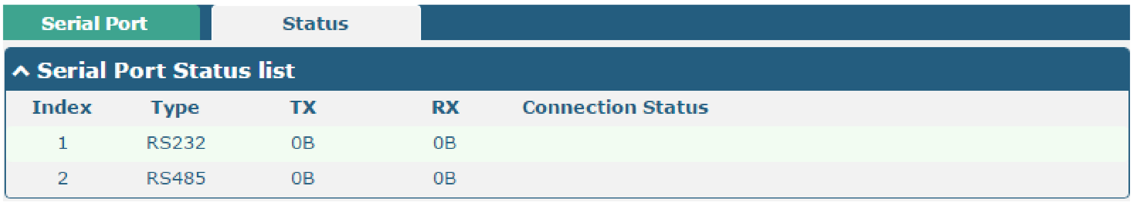
Server Address:

Server Port:

Serial Port		
Item	Description	Default
Serial Port Application Settings		
Index	Indicate the ordinal of the list.	--
Port	Show the current serial's name, read only.	--
Enable	Click the toggle button to enable/ disable this serial port. When the status is OFF, the serial port is not available.	OFF
Baud Rate	Select from " 300", " 600", " 1200", " 2400", " 4800", " 9600", " 19200", " 38400", " 57600" , " 115200" or " 230400".	115200
Data Bits	Select from " 7" or " 8".	8
Stop Bits	Select from " 1" or " 2".	1
Parity	Select from "None", "Odd" or "Even".	None
Flow control	Select from "None", "Software" or " Hardware".	None
Data Packing		
Packing Timeout	Set the packing timeout. The serial port will queue the data in the buffer and send the data to the Cellular WAN/ Ethernet WAN when it reaches the Interval Timeout in the field. Note: Data will also be sent as specified by the packet length even when data is not reaching the interval timeout in the field.	50
Packing Length	Set the packet length. The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When a packet length between 1 and 3000 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.	1200
Server Settings		
Application Mode	Select from Transparent or Modbus RTU Gateway • Transparent: Router will transmit the serial data transparently • Modbus RTU Gateway : Router will trans late the Modbus RTU data to Modbus TCP data and sent out, and vice versa	Transparent

Protocol	Select from TCP Client ””, TCP Server and UDP • TCP Client: Router works as TCP client, initiate TCP connection to TCP server. Server address supports both IP and domain name • TCP Server: Router works as TCP server, listening for connection request from TCP client • UDP: Router works as UDP client • Digilink: Router will automatically upload the serial data to Digilink	TCP Client
Serial Port Application Settings		
Index	Indicate the ordinal of the list.	--
	platform under the Digilink protocol. Digilink is a management platform from Digilink. This function only available when Router is connects to Digilink	
Server Address	Enter the address of server which will receive the data sent from router’s serial port. IP address or domain name will be available.	Null
Server Port	Enter the specified port of server which is used for receiving the serial data.	Null
Local IP @ Transparent	Enter router’s LAN IP which will forward to the internet port of router.	Null
Local Port @ Transparent	Enter the port of router’s LAN IP.	Null
Local IP @ Modbus	Enter the local IP of under Modbus mode.	Null
Local Port @ Modbus	Enter the local port of under Modbus mode.	Null

Click the “Status “column to view the current serial port type.



^ Serial Port Status list

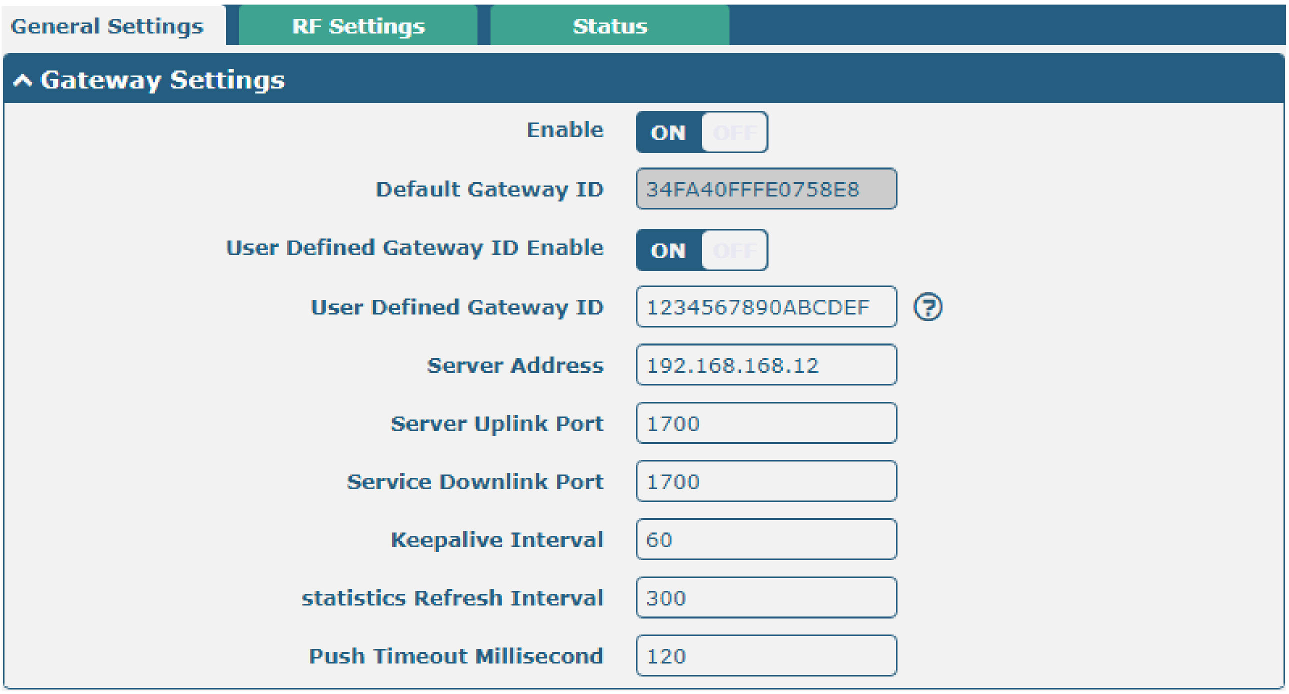
Index	Type	TX	RX	Connection Status
1	RS232	0B	0B	
2	RS485	0B	0B	

3.14 Interface > LoRa

This section allows you to set the LoRaWAN parameters.

General Settings

Click “General Settings > Gateway Settings” to configure your node parameters. Here takes an example as below.

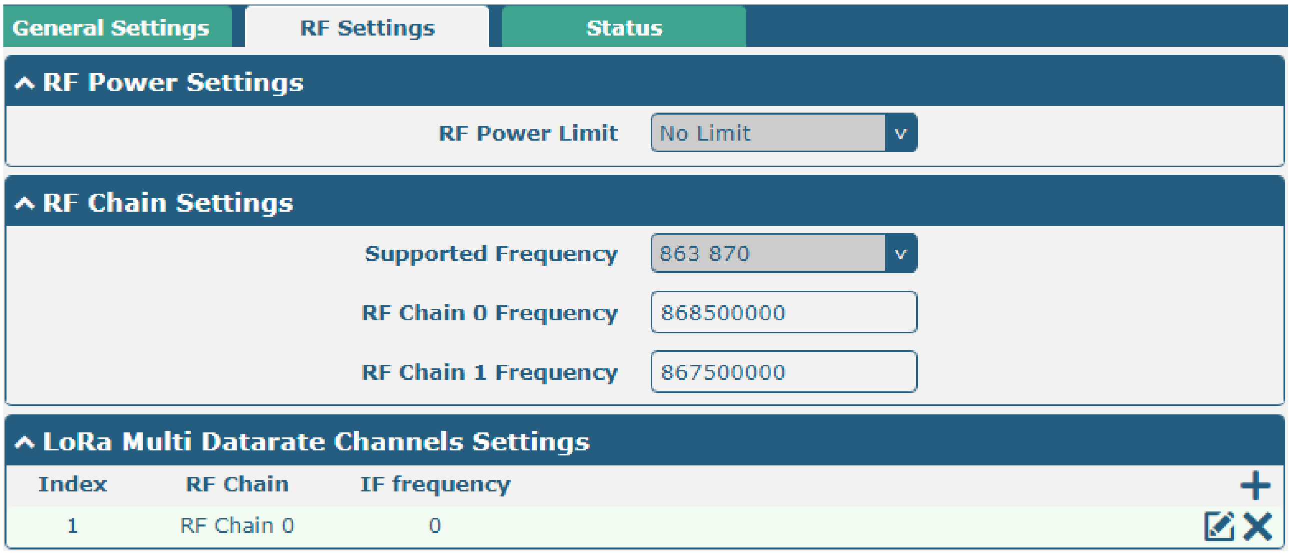


^ Gateway Settings

Enable	ON
Default Gateway ID	34FA40FFFE0758E8
User Defined Gateway ID Enable	ON
User Defined Gateway ID	1234567890ABCDEF
Server Address	192.168.168.12
Server Uplink Port	1700
Service Downlink Port	1700
Keepalive Interval	60
statistics Refresh Interval	300
Push Timeout Millisecond	120

Gateway Settings		
Item	Description	Default
Enable	Click the toggle button to enable/ disable the LoRaWAN forwarding of the gateway.	OFF
Default Gateway ID	Set the defaut gateway ID, or you could define the Gateway ID with a unique 64-bit sequence by yourself.	Null
User Defined Gateway ID Enable	Click the toggle button to enable/ disable this option.	OFF
User Defined Gateway ID	Enter your defined Gateway ID.	Null
Server Address	Enter the remote IP of LoRaWAN Server.	Null
Server Uplink Port	Enter the port oft the LoRaWAN Server to upload data.	Null
Service Downlink Port	Enther the port of the LoRaWAN Server to send data to your gateway.	Null
Keepalive Interval	Enter the interval of keepalive packet which is sent from gateway to LoRaWAN server to keep the connection stable and alive.	Null
Statistics Refresh Interval	Enter the interval to refresh the statistics status of your gateway.	Null
Push Timeout Millisecond	Enter the timeout to wait for the response from server after the gateway sends data of mode, measured in ms.	Null

RF Settings



^ RF Power Settings

RF Power Limit	No Limit

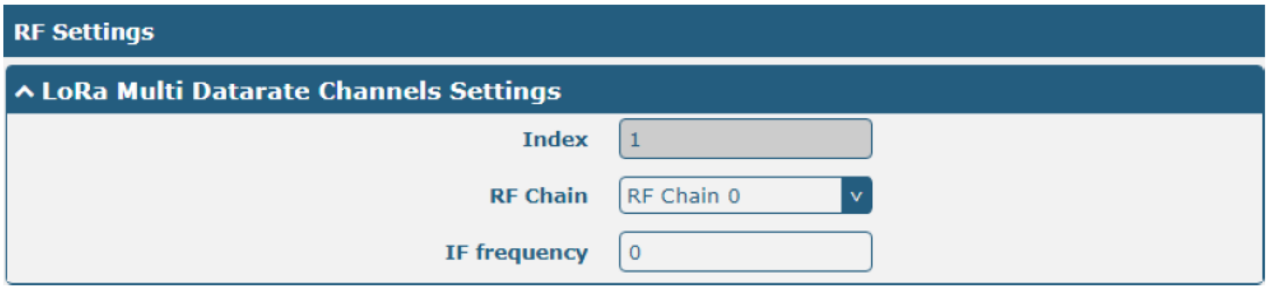
^ RF Chain Settings

Supported Frequency	863 870
RF Chain 0 Frequency	868500000
RF Chain 1 Frequency	867500000

^ LoRa Multi Datarate Channels Settings

Index	RF Chain	IF frequency
1	RF Chain 0	0

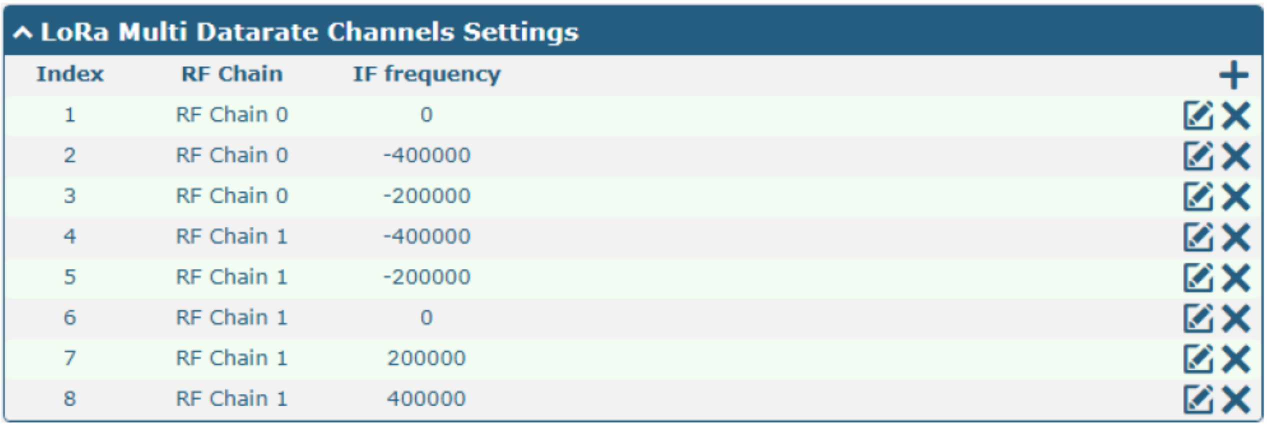
Click + to add a channel.The maximum count is 8.



RF Settings

^ LoRa Multi Datarate Channels Settings

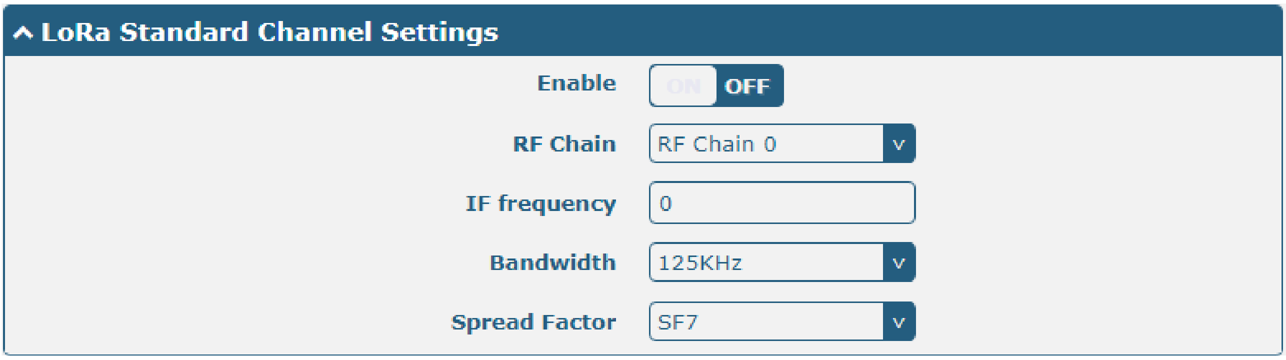
Index	1
RF Chain	RF Chain 0
IF frequency	0



^ LoRa Multi Datarate Channels Settings

Index	RF Chain	IF frequency
1	RF Chain 0	0
2	RF Chain 0	-400000
3	RF Chain 0	-200000
4	RF Chain 1	-400000
5	RF Chain 1	-200000
6	RF Chain 1	0
7	RF Chain 1	200000
8	RF Chain 1	400000

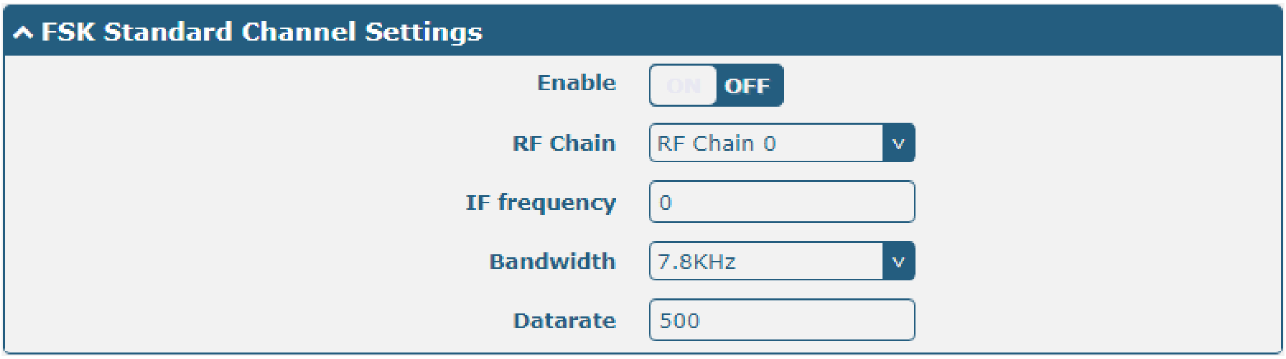
Use LoRa Standard channel to establish communication between nodes and gateway.



LoRa Standard Channel Settings

Enable	ON OFF
RF Chain	RF Chain 0
IF frequency	0
Bandwidth	125KHz
Spread Factor	SF7

Use FSK modulation instead of LoRa.



FSK Standard Channel Settings

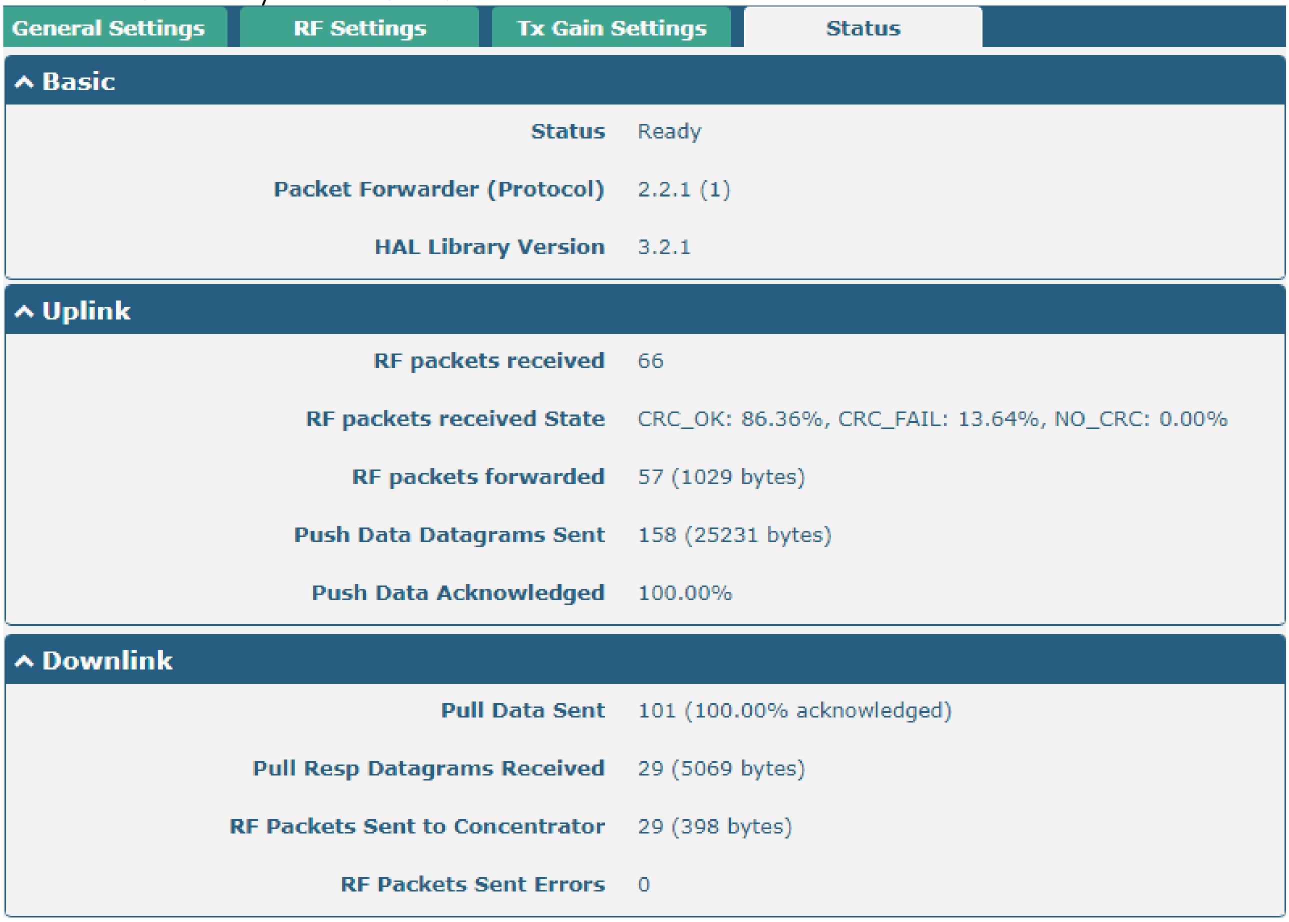
Enable	ON OFF
RF Chain	RF Chain 0
IF frequency	0
Bandwidth	7.8KHz
Datarate	500

RF Settings		
Item	Description	Default
RF Power Settings		
RF Power Limit	Used to indicate the maximum transmit power limit for current gateway. • No_Limit: Transmit power is not limited, depending on the transmit power value sent by the LoRaWAN server • EU_433: Maximum transmit power is limited to 10 dbm or less • EU_868_870: Maximum transmit power is limited to 14 dbm or less • CN_470_510: The maximum transmit power is limited to 17 dbm or less • US_902_928: Maximum transmit power is limited to 26dbm or less • AU_915_928: Maximum transmit power limit below 26dbm • AS_923: Maximum transmit power is limited to 14 dbm or less • KR_920_923: Maximum transmit power is limted to 23 dbm or less • Max_Power: Use the maximum transmit Power which is about 24.5dbm Note: The above options are not configurable and need to be set before delivery.	No Limit
RF Chain Settings		
Supported Frequency	Choose the supported frequency depending on the LoRaWAN module.	863870
RF Chain 0 Frequency	Enter the central frequency of radio transceiver 0 which supports transmitting and receiving.	Null

RF Chain 1 Frequency	Enter the center frequency of radio transceiver 1 which only supports receiving data from nodes.	Null
LoRa Multi Datarate Channels Settings		
Index	Indicate the ordinal of the list	--
RF Chain	Choose Chain 0 or Chain 1 as RF Chain.	RF Chain 0
IF frequency	Enter the IF frequency, measured in Hz. The offset between the central frequency of specific channel and the central frequency of chain is 0/1. Eg: RF Chain 0, IF frequency: -20000. It means the central frequency of this channel should be 868300000=868500000-200000.	0
LoRa Standard Channel Settings		
Enable	Click the toggle button to enable/disable this option.	OFF
RF Chain	Choose Chain 0 or Chain 1 as RF Chain.	Chain 0
RF Settings		
IF frequency	Enter the IF frequency valued from -500000 to 500000, and measured in Hz. The offset between the center frequency of specific channel and the center frequency of chain 0/1.	0
Bandwith	Choose the selectable bandwith, measured in KHz.	500KHz
Spread Factor	Enter the selectable spreading factor. The channel with large spreading factor corresponds to a low rate, while the small one corresponds to a high rate.	250000
FSK Standard Channel Settings		
Enable	Click the toggle button to enable/disable this option.	OFF
RF Chain	Choose Chain 0 or Chain 1 as RF Chain.	Chain 0
IF frequency	Enter the IF frequency valued from -500000 to 500000, and measured in Hz. The offset between the center frequency of specific channel and the center frequency of chain 0/1.	0
Bandwith	Choose the selectable bandwith, measured in KHz.	500KHz
Datarate	Enter the data rate valued from 500 to 250000 and measure in Bit.	250000

Status

Click “Status” to view your node status.



Basic

Status: Ready
Packet Forwarder (Protocol): 2.2.1 (1)
HAL Library Version: 3.2.1

Uplink

RF packets received: 66
RF packets received State: CRC_OK: 86.36%, CRC_FAIL: 13.64%, NO_CRC: 0.00%
RF packets forwarded: 57 (1029 bytes)
Push Data Datagrams Sent: 158 (25231 bytes)
Push Data Acknowledged: 100.00%

Downlink

Pull Data Sent: 101 (100.00% acknowledged)
Pull Resp Datagrams Received: 29 (5069 bytes)
RF Packets Sent to Concentrator: 29 (398 bytes)
RF Packets Sent Errors: 0

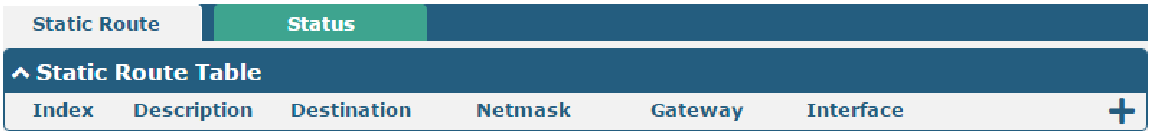
Status	
Item	Description
Basic	
Status	Show the LoRaWAN status of your gateway.
Packet Forwarder (Protocol)	Show the version of Packet forwarder.
HAL Library Version	Show the driver version of LoRaWAN chipset inside gateway.
Uplink	
RF packets received	Show the count of data packet from node to gateway.
RF packets received State	Show the RF packets receiving state. • CRC_OK: Percentage of CRC verification • CRC_Fail: Percentage of CRC failure • NO_CRC: Percentage of abnormal packets without CRC
RF packets forwarded	Packets that CRC verified are sent from gateway to server.
Push Data Datagrams Set	The total quantity of packets sent from gateway to server, including the RF packets forwarded and statistics packets.
Push Data Acknowledged	Percentage of acknowledged packets among Push Data Datagrams Sent:

Downlink	
Pull Data Sent	Show the number of keepalive packets sent to the server, and percentage of acknowledge packet regarding the keepalive packet from the server.
Pull Resp Datagrams Received	Show the packet counts and size that will be sent from server to gateway.
RF Packets Sent to Concentrator	Show the RF packet counts and size that will be sent from gateway to node.
RF Packets Sent Errors	Show the RF packet counts that fail to be sent from server to node.

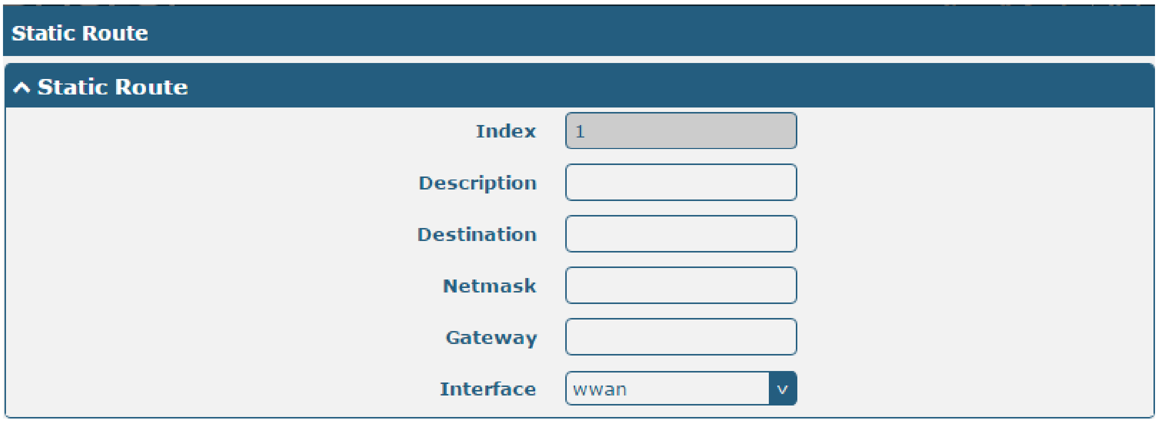
3.15 Network > Route

This section allows you to set the static route. Static route is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from a dynamic routing traffic. Route Information Protocol (RIP) is widely used in small network with stable use rate. Open Shortest Path First (OSPF) is made router within a single autonomous system and used in large network.

Static Route



Click + to add static route. The maximum count is 20.

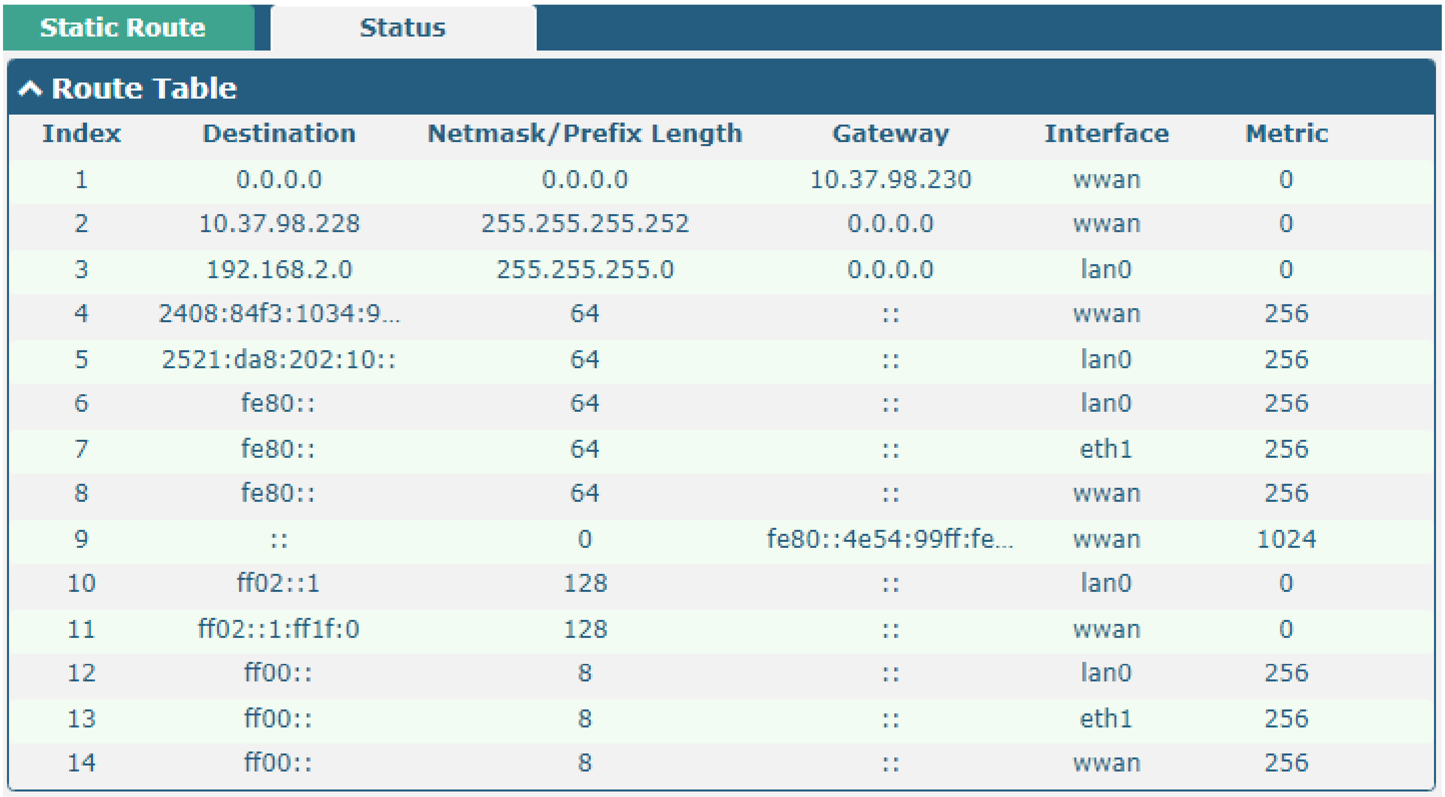


Index	1
Description	
Destination	
Netmask	
Gateway	
Interface	wwan

Static Route		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this route.	Null
Destination	Enter the IPaddress of destination host or destination network.	Null
Netmask/ IPv6 address Prefix Length	Enter the Netmask of destination host or destination network.	Null
Gateway	Define the gateway of the destination.	Null
Interface	Choose the corresponding port of the link that you want to configure.	wwan1

Status

This window allows you to view the status of route.



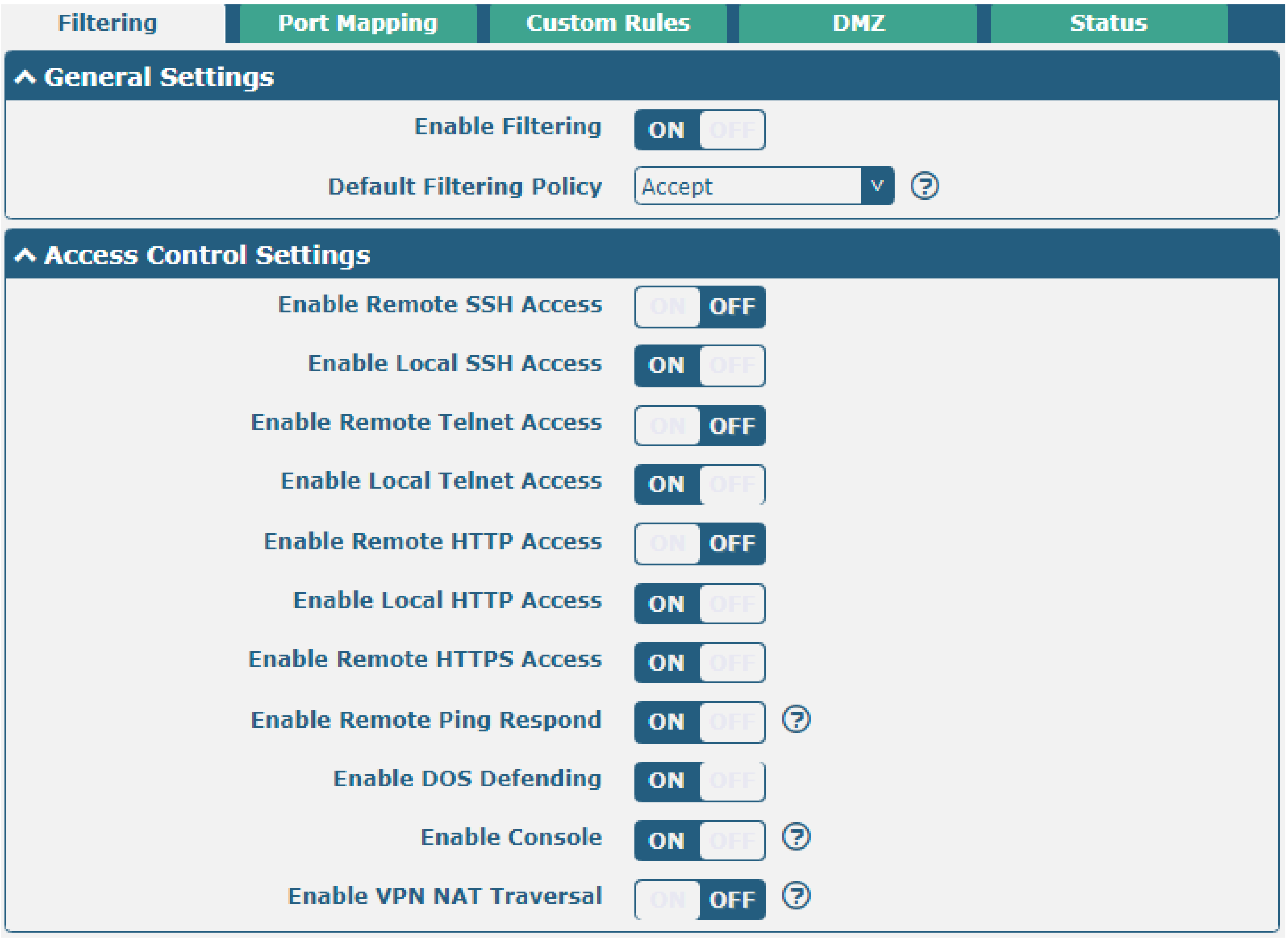
Index	Destination	Netmask/Prefix Length	Gateway	Interface	Metric
1	0.0.0.0	0.0.0.0	10.37.98.230	wwan	0
2	10.37.98.228	255.255.255.252	0.0.0.0	wwan	0
3	192.168.2.0	255.255.255.0	0.0.0.0	lan0	0
4	2408:84f3:1034:9...	64	::	wwan	256
5	2521:da8:202:10::	64	::	lan0	256
6	fe80::	64	::	lan0	256
7	fe80::	64	::	eth1	256
8	fe80::	64	::	wwan	256
9	::	0	fe80::4e54:99ff:fe...	wwan	1024
10	ff02::1	128	::	lan0	0
11	ff02::1:ff1f:0	128	::	wwan	0
12	ff00::	8	::	lan0	256
13	ff00::	8	::	eth1	256
14	ff00::	8	::	wwan	256

3.16 Network > Firewall

This section allows you to set the firewall and its related parameters, including Filtering, Port Mapping and DMZ.

Filtering

The filtering rules can be used to either accept or block certain users or ports from accessing your router.

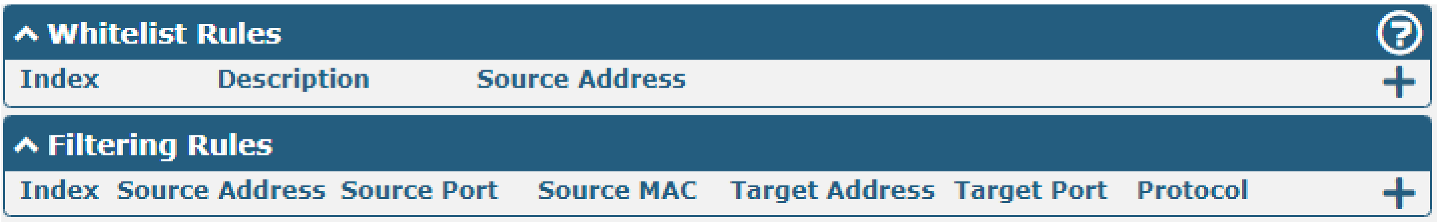


General Settings

Enable Filtering	ON
Default Filtering Policy	Accept

Access Control Settings

Enable Remote SSH Access	OFF
Enable Local SSH Access	ON
Enable Remote Telnet Access	OFF
Enable Local Telnet Access	ON
Enable Remote HTTP Access	OFF
Enable Local HTTP Access	ON
Enable Remote HTTPS Access	ON
Enable Remote Ping Respond	ON
Enable DOS Defending	ON
Enable Console	ON
Enable VPN NAT Traversal	OFF

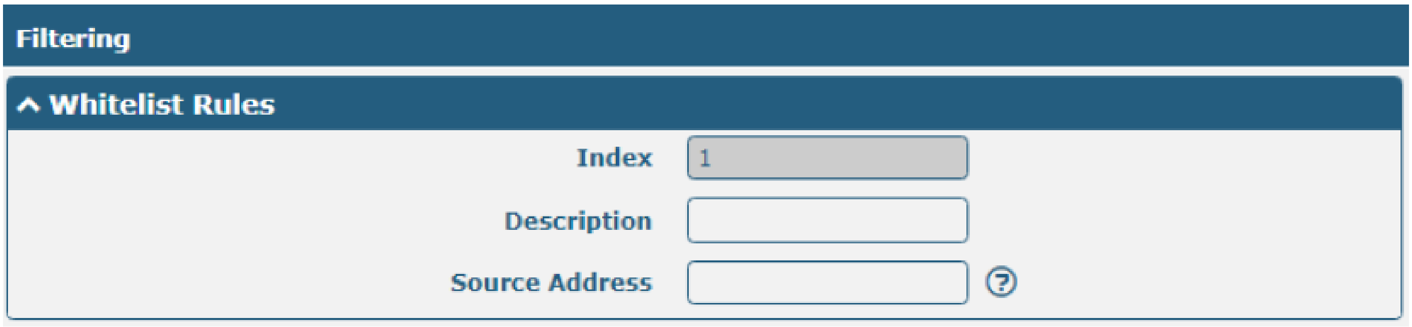

Whitelist Rules

Index	Description	Source Address

Filtering Rules

Index	Source Address	Source Port	Source MAC	Target Address	Target Port	Protocol

Click + to add whitelist:

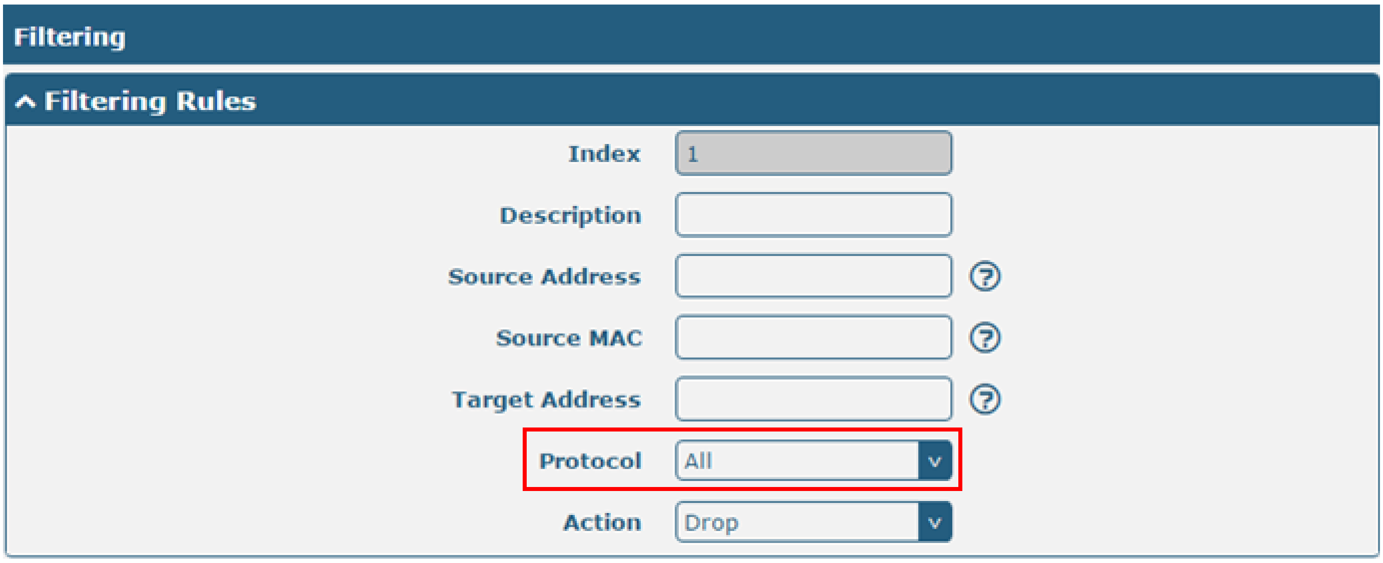


Filtering

Whitelist Rules

Index	1
Description	
Source Address	

Click + to add filtering rule , the maximum count is 50. The window is displayed as below when defaulting „All“ or choosing “ ICMP v6 ” or “ICMPv6” as the protocol. Here take „All“ as an example.

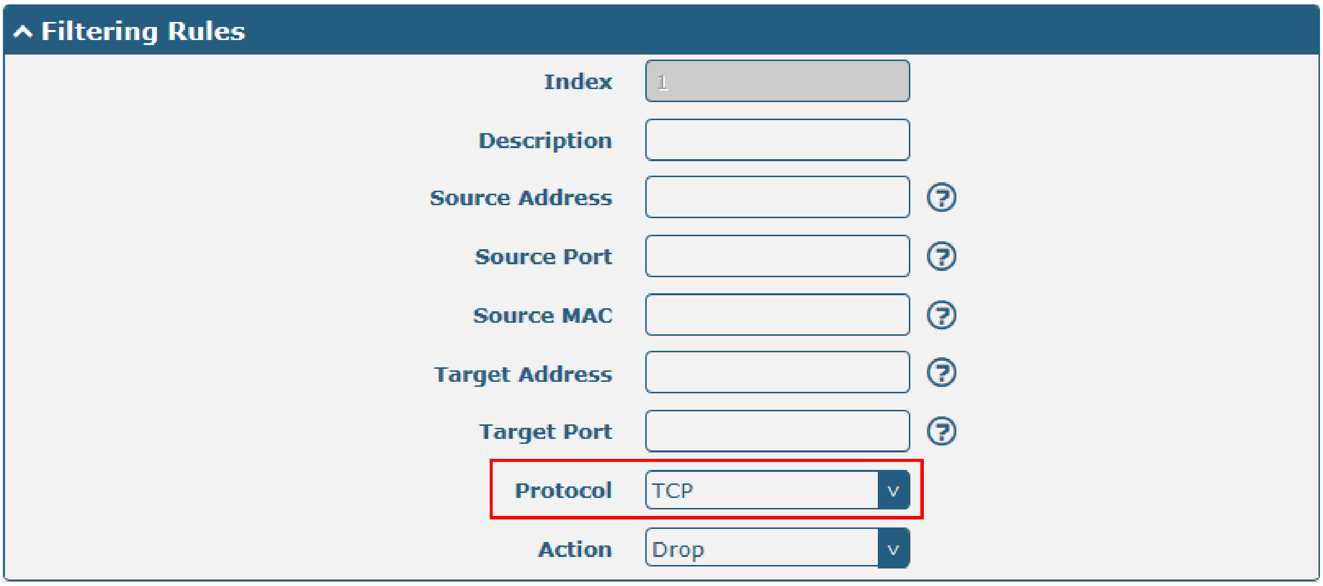


Filtering

Filtering Rules

Index	1
Description	
Source Address	
Source MAC	
Target Address	
Protocol	All
Action	Drop

The window is displayed as below when choosing “TCP”, “UDP”or “TCP-UDP” as the protocol. Here take “TCP”as an example.



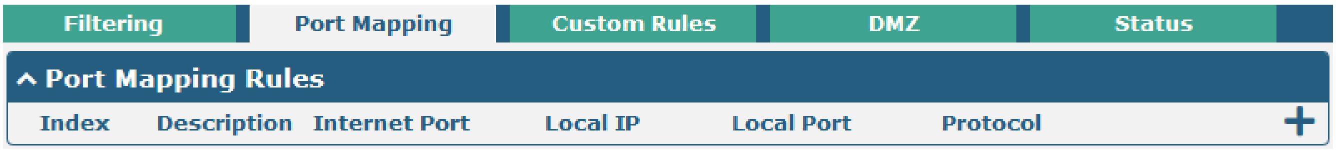
Filtering Rules

Index	1
Description	
Source Address	
Source Port	
Source MAC	
Target Address	
Target Port	
Protocol	TCP
Action	Drop

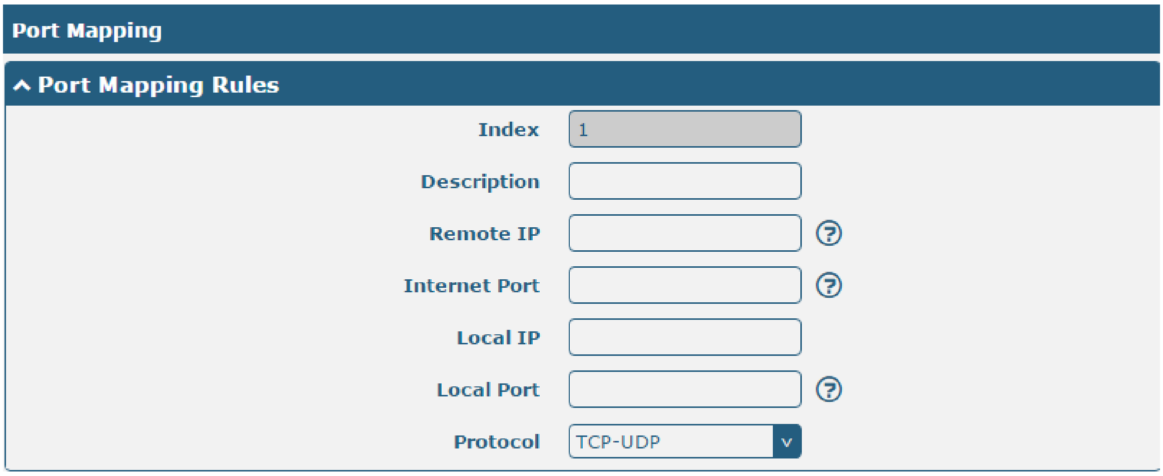
Filtering		
Item	Description	Default
General Settings		
Enable Filtering	Click the toggle button to enable/ disable the filtering option.	ON
Default Filtering Policy	Select from "Accept" or "Drop" . Cannot be changed when filtering rules table is not empty. Accept: Router will accept all the connecting requests except the hosts which fit the drop filter list Drop: Router will drop all the connecting requests except the hosts which fit the accept filter list	Accept
Access Control Settings		
Enable Remote SSH Access	Click the toggle button to enable/ disable this option. When enabled, the Internet user can access the router remotely via SSH.	OFF
Enable Local SSH Access	Click the toggle button to enable/ disable this option. When enabled, the LAN user can access the router locally via SSH.	ON
Enable Remote Telnet Access	Click the toggle button to enable/ disable this option. When enabled, the Internet user can access the router remotely via Telnet.	OFF
Enable Local Telnet Access	Click the toggle button to enable/ disable this option. When enabled, the LAN user can access the router locally via Telnet.	ON
Enable Remote HTTP Access	Click the toggle button to enable/ disable this option. When enabled, the Internet user can access the router remotely via HTTP.	OFF
Enable Local HTTP Access	Click the toggle button to enable/ disable this option. When enabled, the LAN user can access the router locally via HTTP.	ON
Enable Remote HTTPS Access	Click the toggle button to enable/ disable this option. When enabled, the Internet user can access the router remotely via HTTPS.	ON

Enable Remote Ping Respond	Click the toggle button to enable/ disable this option. When enabled, the router will reply to the Ping requests from other hosts on the Internet.	ON
Enable DOS Defending	Click the toggle button to enable/ disable this option. When enabled, the router will defend the DOS. Dos attack is an attempt to make a machine or network resource unavailable to its intended users.	ON
Enable Console	Click the toggle button to enable/disable this option.	ON
Enable vpn nat traversal	Click the toggle button to enable / disable this option. When enabled, enable NAT traversal for GRE / L2TP / PPTP VPN packets.	OFF
whitelist		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this whitelist.	Null
Source Address	Defines if access is allowed from one or a range of IP addresses which are defined by Source IP Address, or every IP addresses.	Null
Filtering Rules		
Item	Indicate the ordinal of the list.	-
Description	Enter a description for this filtering rule	Null
Source Address	Defines if access is allowed from one or a range of IP addresses which are defined by Source IP Address, or every IP addresses.	Null
Source Port	Specify an access originator and enter its source port.	Null
Source MAC	Enter the MAC address of the defined source IP address.	Null
Target Address	Defines if access is allowed to one or a range of IP addresses which are defined by Target IP Address, or every IP addresses.	Null
Target Port	Enter the target port which the access originator wants to access.	Null
Protocol	Select from “All”, “TCP”, “UDP”, “ICMP” or “TCP-UDP”. Note: It is recommended that you choose “All” if you don’t know which protocol of your application to use.	All
Filtering		
Action	Select from “Accept” or “Drop”. • Accept: When Default Filtering Policy is drop, router will drop all the connecting requests except the hosts which fit this accept filtering list • Drop: When Default Filtering Policy is accept, router will accept all the connecting requests except the hosts which fit this drop filtering list	Drop

Port Mapping



Click + to add port mapping rules. The maximum rule count is 40.

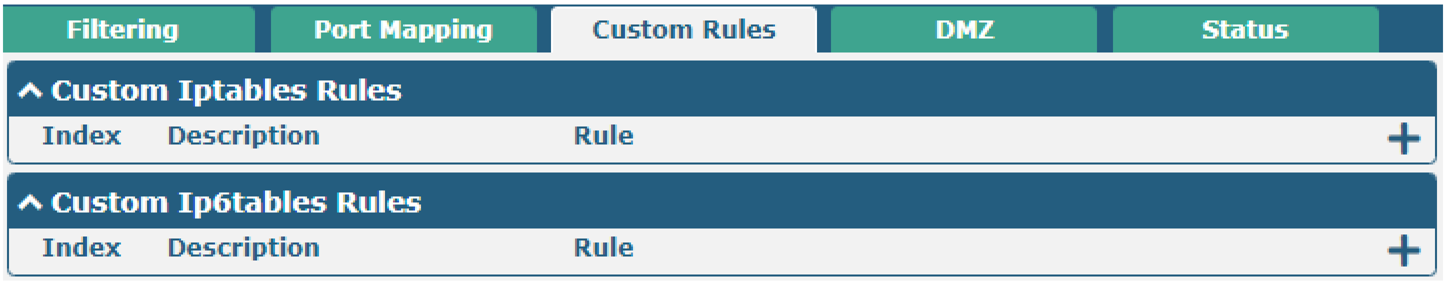


Index	1
Description	
Remote IP	
Internet Port	
Local IP	
Local Port	
Protocol	TCP-UDP

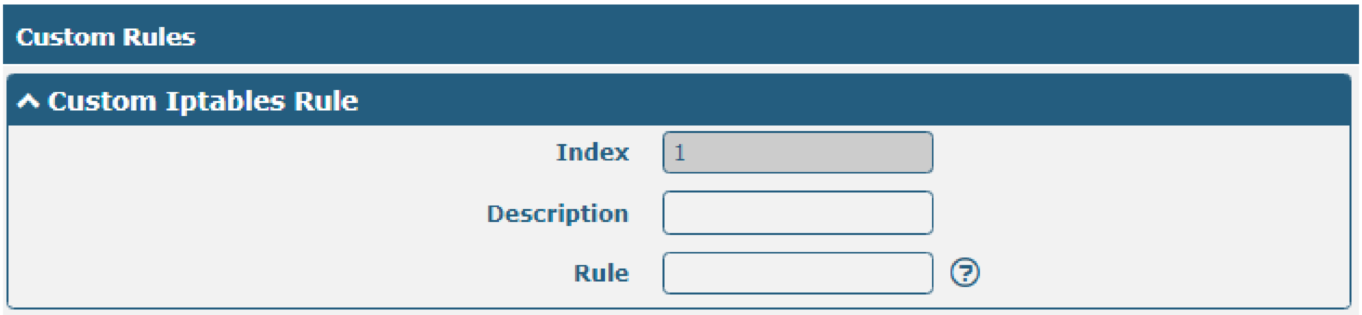
Port Mapping Rules		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this port mapping.	Null
Remote IP	Specify the host or network which can access to the local IP address. Empty means unlimited. e.g. 10.10.10.10/ 255.255.255.255 or 192.168.1.0/ 24	Null
Internet Port	Set the internet port of router which can be accessed by other hosts from internet.	Null
Local IP	Enter router's LAN IP which will forward to the internet port of router.	Null
Local Port	Enter the port of router's LAN IP.	Null
Protocol	Select from " TCP" , " UDP" or " TCP-UDP" as your application required.	TCP-UDP

Custom Rules

Custom rules, that is, rules that you define yourself. Click Network> Firewall> Custom Rule and is displayed as follows:



Click + to add to add an IPv4 or IPv6 custom rule, the window is displayed as follows (take "IPv4" as an example):



Custom Rules

^ Custom Iptables Rule

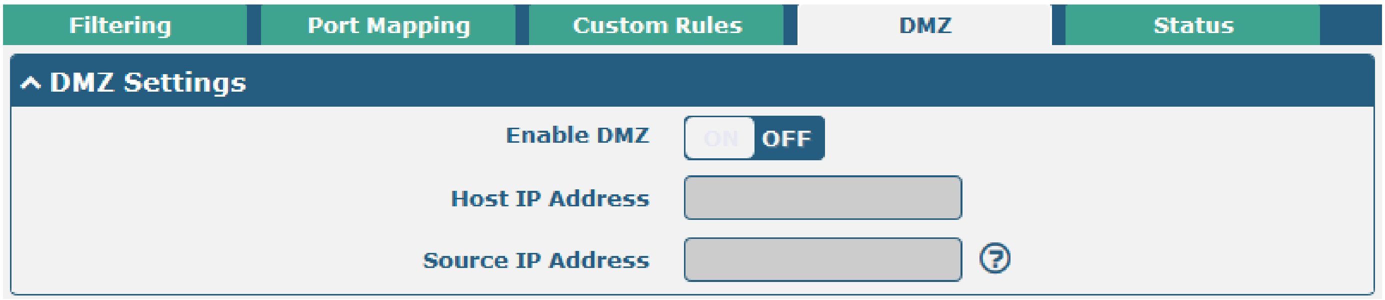
Index: 1

Description:

Rule:

Custom Ip tables Rule		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter the description of the rule.	Null
Rule	Specify one Ip tables rule.	Null

DMZ



^ DMZ Settings

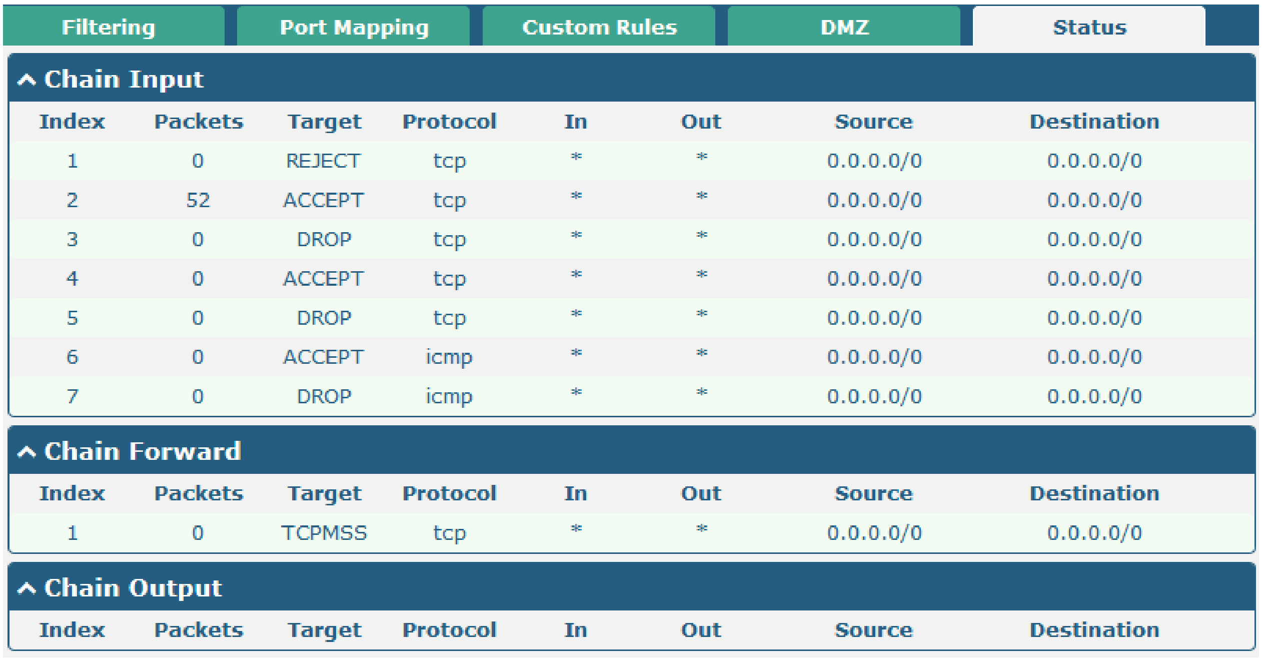
Enable DMZ: ON OFF

Host IP Address:

Source IP Address:

DMZ Settings		
Item	Description	Default
Enable DMZ	Click the toggle button to enable/ disable DMZ. DMZ host is a host on the internal network that has all ports exposed, except those ports otherwise forwarded.	OFF
Host IP Address	Enter the IP address of the DMZ host on your internal network.	Null
Source IP Address	Set the address which can talk to the DMZ host. 0.0.0.0 means for any addresses.	Null

Status



^ Chain Input

Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	REJECT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
2	52	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
3	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
4	0	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
5	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
6	0	ACCEPT	icmp	*	*	0.0.0.0/0	0.0.0.0/0
7	0	DROP	icmp	*	*	0.0.0.0/0	0.0.0.0/0

^ Chain Forward

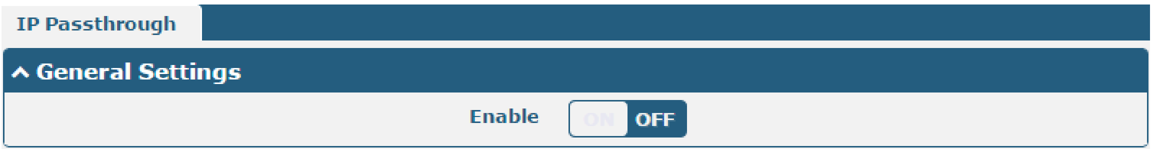
Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	TCPMSS	tcp	*	*	0.0.0.0/0	0.0.0.0/0

^ Chain Output

Index	Packets	Target	Protocol	In	Out	Source	Destination

3.17 Network > IP Passtrough

Click Network > IP Passthrough > IP Passthrough to enable or disable the IP Pass-through option.



^ General Settings

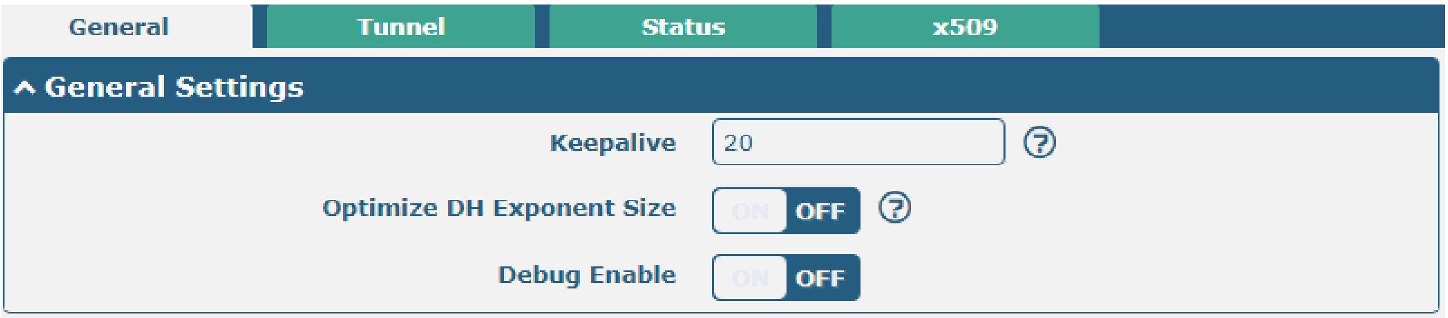
Enable: ON [✓ OFF]

If router enables the IP Pass-through, the terminal device (such as PC) will enable the DHCP Client mode and connect to LAN port of the router; and after the router dial up successfully, the PC will automatically obtain the IP address and DNS server address which assigned by ISP.

3.18 VPN > IPsec

IPsec (Internet Protocol Security) is a protocol built on the Internet protocol layer that enables two hosts to communicate in a secure manner. IPsec is the direction of secure networking. It provides active protection from end to end security to prevent attacks from private networks and the Internet.

Click Virtual Private Network> IPsec> General to set IPsec parameters.



^ General Settings

Keepalive: 20

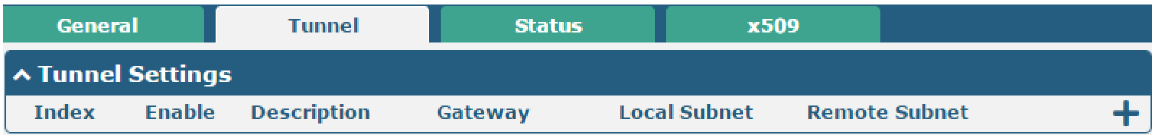
Optimize DH Exponent Size: ON [✓ OFF]

Debug Enable: ON [✓ OFF]

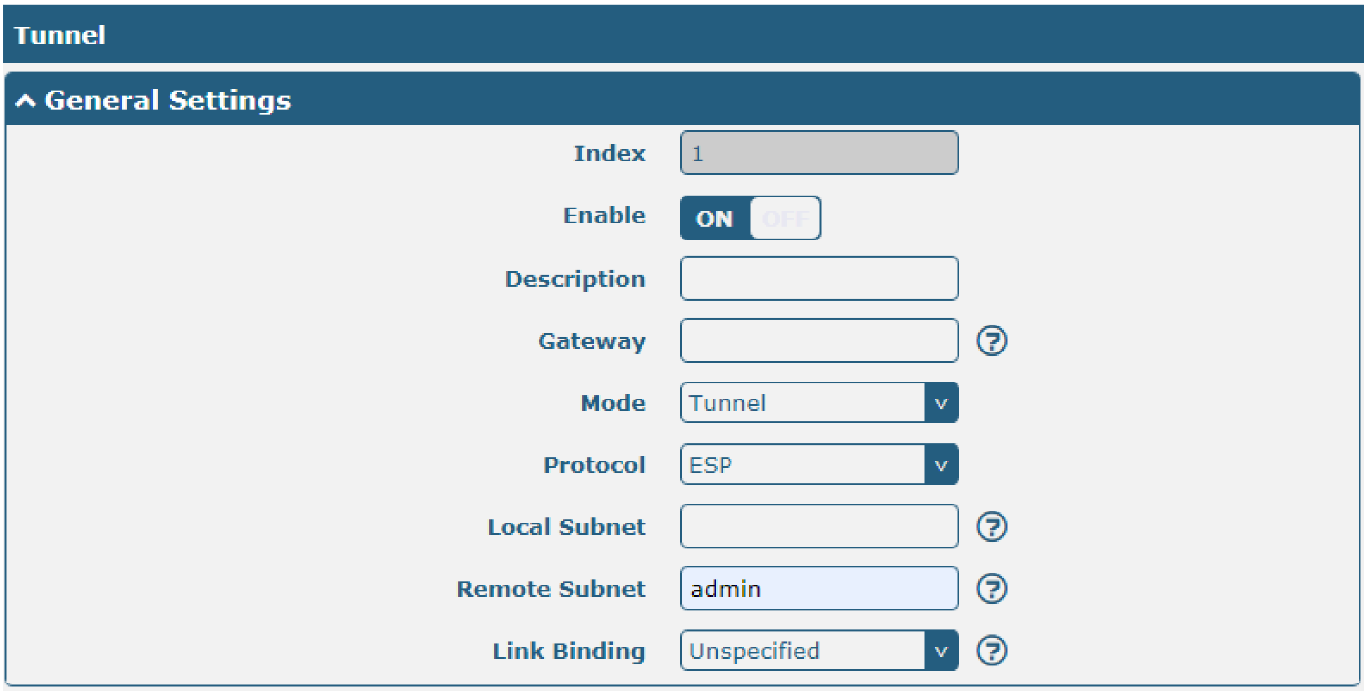
General

General Settings @ General		
Item	Description	Default
Survival time	Set the survival time in seconds. The router sends keep-alive packets to a NAT (Network Address Translation) server at regular intervals to prevent the records on the NAT table from disappearing.	20
Optimize DH index size	Click the toggle button to enable / disable this option. When enabled, when using dhgroup17 or dhgroup18, it helps to shorten the time to generate dh keys.	OFF
Debug Enable	Click the toggle button to enable/disable this option. Enable for IPsec VPN information output to the debug port	OFF

Tunnel



Click + to add tunnel settings. The maximum count is 3.


Tunnel

General Settings

Index: 1

Enable: ON OFF

Description:

Gateway:

Mode: Tunnel

Protocol: ESP

Local Subnet:

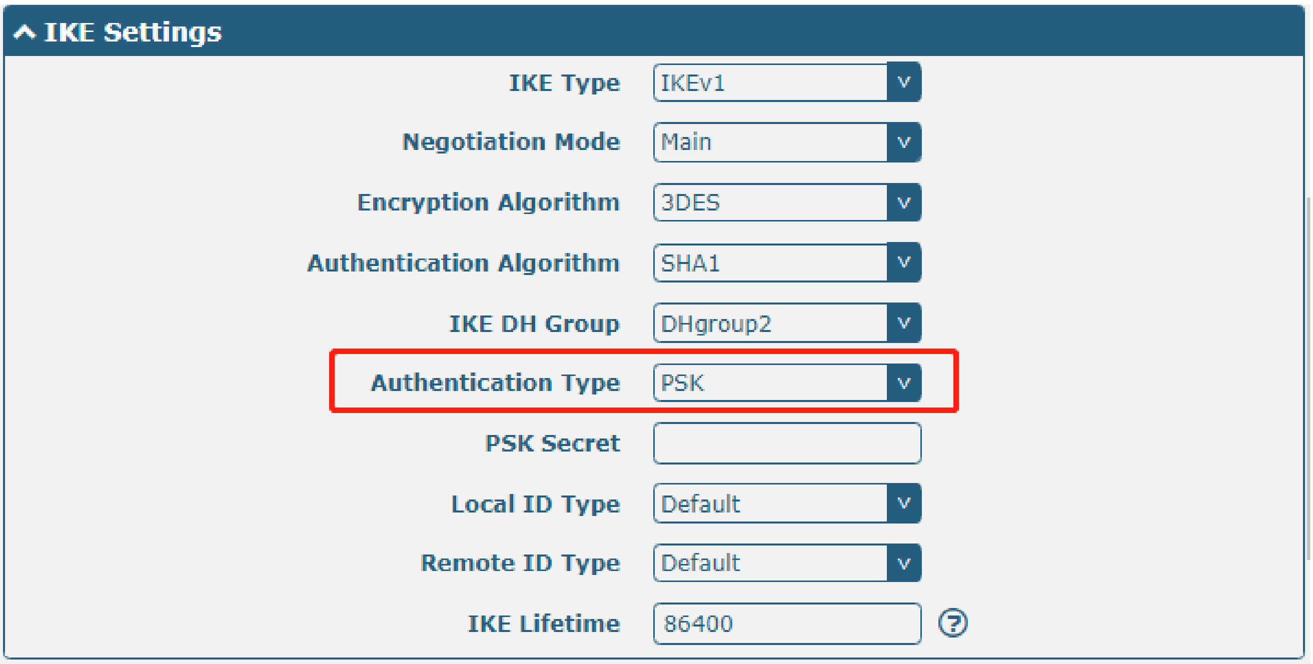
Remote Subnet: admin

Link Binding: Unspecified

General Settings @ Tunnel		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/ disable this IPsec tunnel.	ON
Description	Enter a description for this IPsec tunnel.	Null
Gateway	Enter the address of remote side IPsec VPN server. 0.0.0.0 represents for any address.	Null

Mode	Select from “ Tunnel” and “ Transport” . • Tunnel: Commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it • Transport: Used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host-for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination	Tunnel
Protocol	Select the security protocols from “ESP” and “ AH” . ESP: Use the ESP protocol AH: Use the AH protocol	ESP
Local Subnet	Enter the local subnet’s address with mask protected by IPsec, e.g. 192.168.1.0/ 24	Null
Remote Subnet	Enter the remote subnet’s address with mask protected by IPsec, e.g. 10.8.0.0/ 24	Null
Link binding	Select from WWAN1, WWAN2, WAN, or WLAN.	Not bound

The window is displayed as below when choosing " PSK" as the authentication type.



IKE Settings

IKE Type: IKEv1

Negotiation Mode: Main

Encryption Algorithm: 3DES

Authentication Algorithm: SHA1

IKE DH Group: DHgroup2

Authentication Type: PSK

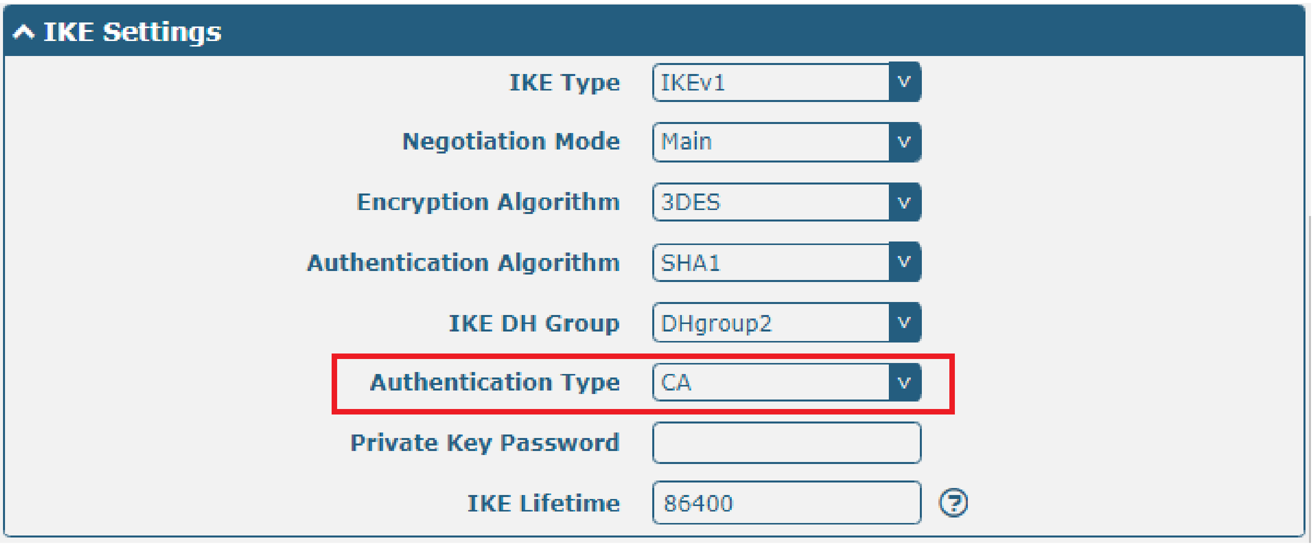
PSK Secret:

Local ID Type: Default

Remote ID Type: Default

IKE Lifetime: 86400

The window is displayed as below when choosing " CA" as the authentication type.



IKE Settings

IKE Type: IKEv1

Negotiation Mode: Main

Encryption Algorithm: 3DES

Authentication Algorithm: SHA1

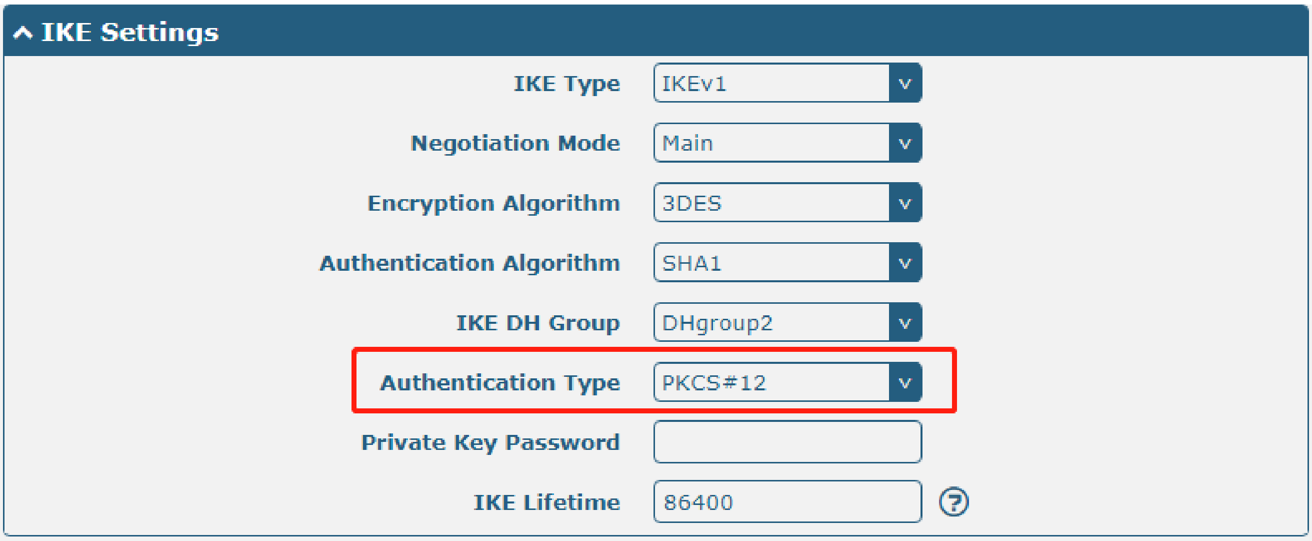
IKE DH Group: DHgroup2

Authentication Type: CA

Private Key Password:

IKE Lifetime: 86400

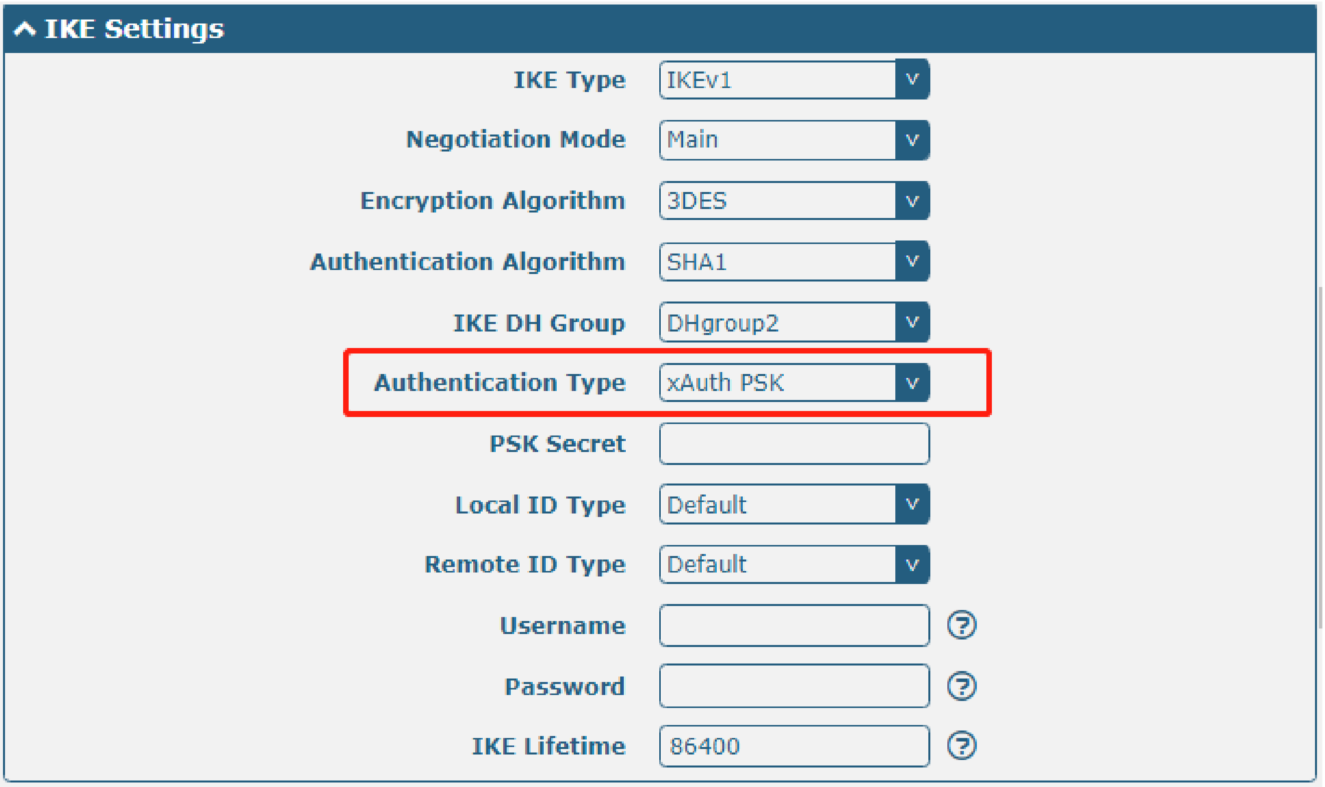
The window is displayed as below when choosing “PKCS#12”as the authentication type.



IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	PKCS#12
Private Key Password	
IKE Lifetime	86400

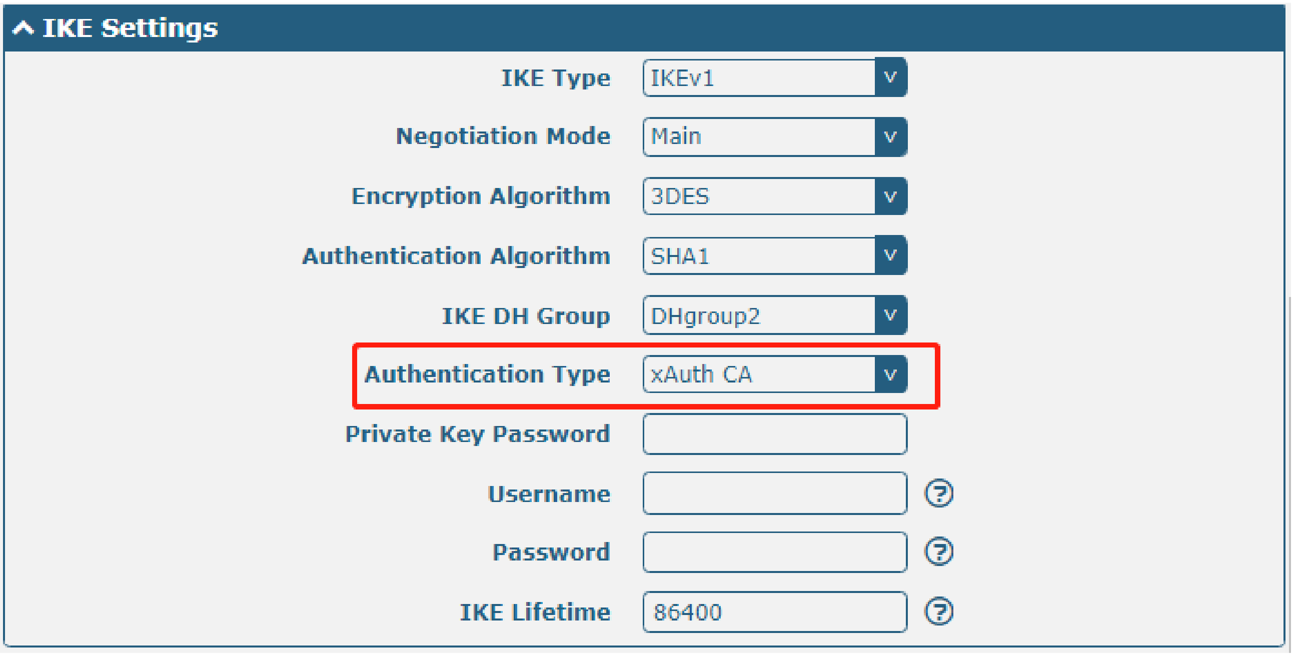
The window is displayed as below when choosing “ xAuth PSK” as the authentication type.



IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	xAuth PSK
PSK Secret	
Local ID Type	Default
Remote ID Type	Default
Username	
Password	
IKE Lifetime	86400

The window is displayed as below when choosing " xAuth CA" as the authentication type.



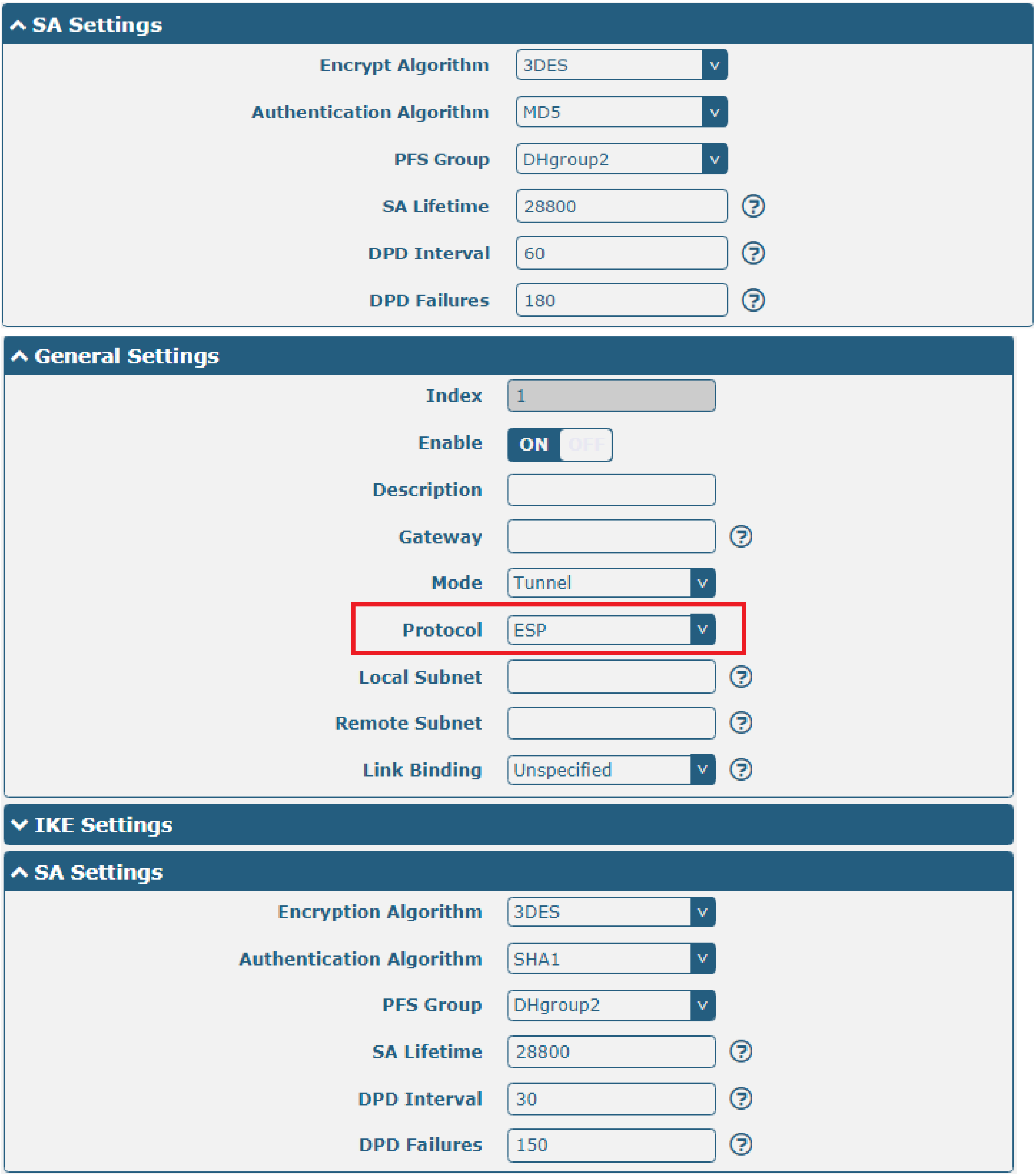
^ IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	xAuth CA
Private Key Password	
Username	
Password	
IKE Lifetime	86400

IKE Settings		
Item	Description	Default
IKE Type	Select from IKE v1 and IKE v2.	IKE v1
Negotiation Mode	Select from "Main" and "Aggressive" for the IKE negotiation mode in phase 1. If the IP address of one end of an IPsec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.	Main
Authentication Algorithm	Select from "MD5", "SHA1", "SHA2 256" or "SHA2 512" to be used in IKE negotiation.	SHA1
Encryption Algorithm	Select from "3DES", "AES128", "AES192" and "AES256"to be used in IKE negotiation. • 3DES: Use 168-bit 3DES encryption algorithm in CBC mode • AES128: Use 128-bit AES encryption algorithm in CBC mode • AES256: Use 256-bit AES encryption algorithm in CBC mode	3DES
IKE DH Group	Select DH packets for IKE (Network Key Exchange) negotiation. Select from "DHgroup1", "DHgroup2", "DHgroup5", "DHgroup14", "DHgroup15", "DHgroup16", "DHgroup17" or "DHgroup18" to be used in key negotiation phase 1.	PSK
Authentication Type	Select from "PSK", "CA", "PKCS#12", "xAuth PSK" and "xAuth CA" to be used in IKE negotiation. • PSK: Pre-shared Key • CA: Certification Authority • xAuth: Extended Authentication to AAA server	PSK

IKE Settings		
Item	Description	Default
PSK Secret	Enter the pre-shared key.	Null
Local ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation. • Default: Uses an IP address as the ID in IKE negotiation • FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.AddSecure.com. • User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign "@" for the local security gateway, e.g., test@AddSecure.com.	Default
Remote ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation. • Default: Uses an IP address as the ID in IKE negotiation • FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.AddSecure.com. • User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign "@" for the local security gateway, e.g., test@AddSecure.de	Default
Private Key Password	Enter the private key under the " CA" and " xAuth CA" authentication types.	Null
Username	Enter the username used for the " xAuth PSK" and " xAuth CA" authentication types.	Null
Password	Enter the password used for the " xAuth PSK" and " xAuth CA" authentication types.	Null
IKE Lifetime	Set the lifetime in IKE negotiation. Before an SA expires, IKE negotiates a new SA. As soon as the new SA is set up, it takes effect immediately and the old one will be cleared automatically when it expires.	86400

If click VPN > IPsec > Tunnel > General Settings, and choose ESP as protocol. The specific parameter configuration is shown as below.



SA Settings

Encrypt Algorithm	3DES
Authentication Algorithm	MD5
PFS Group	DHgroup2
SA Lifetime	28800
DPD Interval	60
DPD Failures	180

General Settings

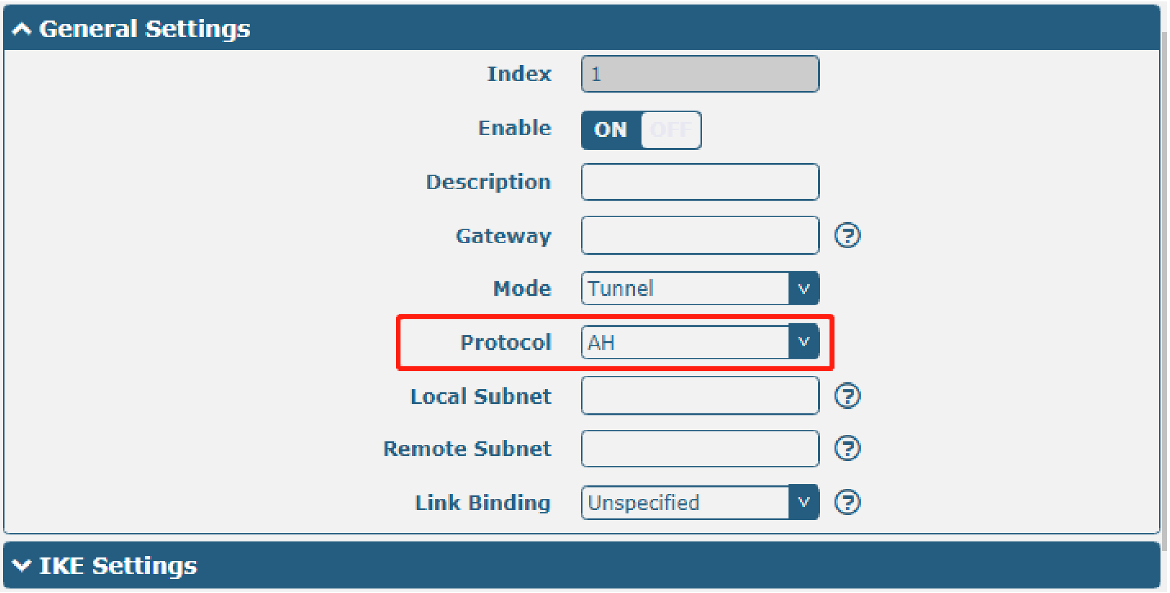
Index	1
Enable	ON
Description	
Gateway	
Mode	Tunnel
Protocol	ESP
Local Subnet	
Remote Subnet	
Link Binding	Unspecified

IKE Settings

SA Settings

Encryption Algorithm	3DES
Authentication Algorithm	SHA1
PFS Group	DHgroup2
SA Lifetime	28800
DPD Interval	30
DPD Failures	150

If choose AH as protocol, the window of SA Settings is displayed as below.



General Settings

Index: 1

Enable: ON

Description:

Gateway:

Mode: Tunnel

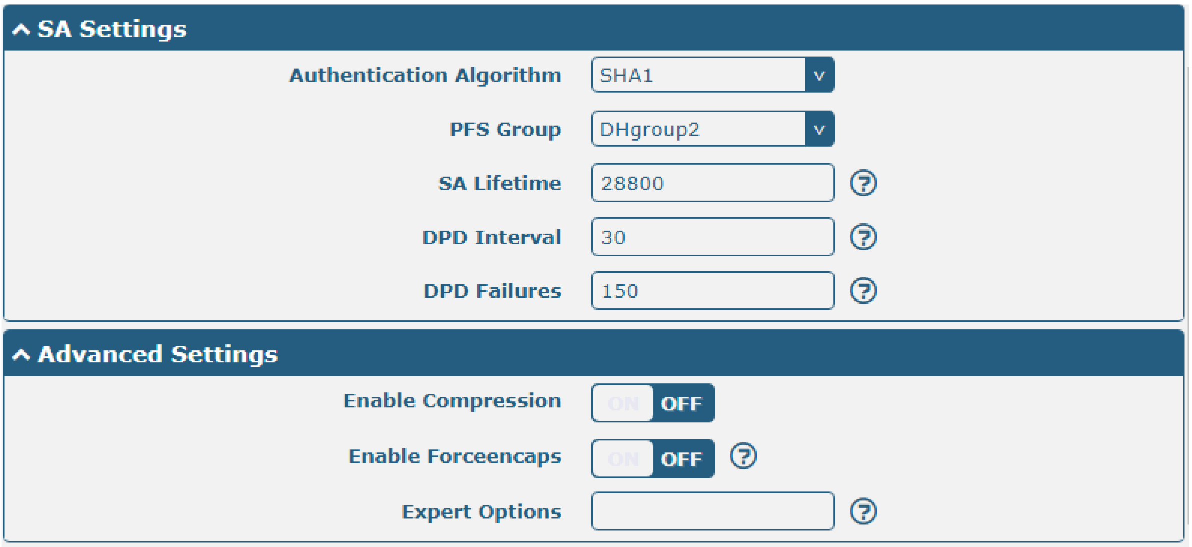
Protocol: AH

Local Subnet:

Remote Subnet:

Link Binding: Unspecified

IKE Settings



SA Settings

Authentication Algorithm: SHA1

PFS Group: DHgroup2

SA Lifetime: 28800

DPD Interval: 30

DPD Failures: 150

Advanced Settings

Enable Compression: OFF

Enable Forceencaps: OFF

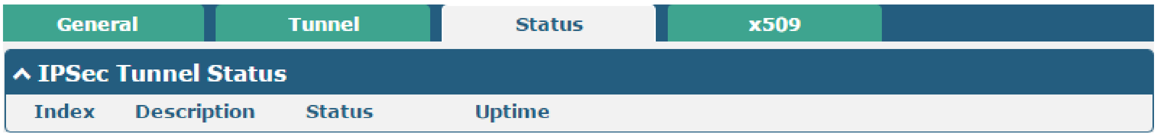
Expert Options:

SA Settings		
Item	Description	Default
Encrypt Algorithm	Select from “ 3DES” , “ AES128” or “ AES256” when you select “ ESP” in “ Protocol” . Higher security means more complex implementation and lower speed. DESis enough to meet general requirements. Use 3DESwhen high confidentiality and security are required.	3DES
Authentication Algorithm	Select from “MD5”, “ SHA1” , “ SHA2 256” or “ SHA2 512” to be used in SA negotiation.	MD5
PFS Group	Select from “PFS（N/A）”,“DHgroup1”, “DHgroup2”, “DHgroup5”, “DHgroup14”, “DHgroup15”, “DHgroup16”, “DHgroup17” or “DHgroup18” to be used in SA negotiation.	DHgroup2
SA Lifetime	Set the IPsec SA lifetime. When negotiating to set up IPsec SAs, IKEuses the smaller one between the lifetime set locally and the lifetime proposed by the peer.	28800

DPD Interval	Set the interval after which DPD is triggered if no IPsec protected packets is received from the peer. DPD is a Dead peer detection. DPD irregularly detects dead IKEpeers. When the local end sends an IPsec packet, DPD checks the time the last IPsec packet was received from the peer. If the time exceeds the DPD interval, it sends a DPD hello to the peer. If the local end receives no DPD acknowledgment within the DPD packet retransmission interval, it retransmits the DPD hello. If the local end still receives no DPD acknowledgment after having made the maximum number of retransmission attempts, it considers the peer already dead, and clears the IKESA and the IPsec SAs based on the IKE SA.	60
DPD Failures	Set the timeout of DPD (Dead Peer Detection) packets.	180
Advanced Settings		
Enable Compression	Click the toggle button to enable/ disable this option. Enable to compress the inner headers of IP packets.	OFF
Enable Forced Encapsulation	Click the toggle button to enable / disable this option. After it is enabled, even if no NAT condition is detected, the UDP encapsulation of esp packets is forced. This may help overcome restrictive firewalls.	OFF
Expert Options	Add more PPP configuration options here, format: config-desc;config-desc, e.g. protostack=netkey;plutodebug=none	Null

Status

This section allows you to view the status of the IPsec tunnel.

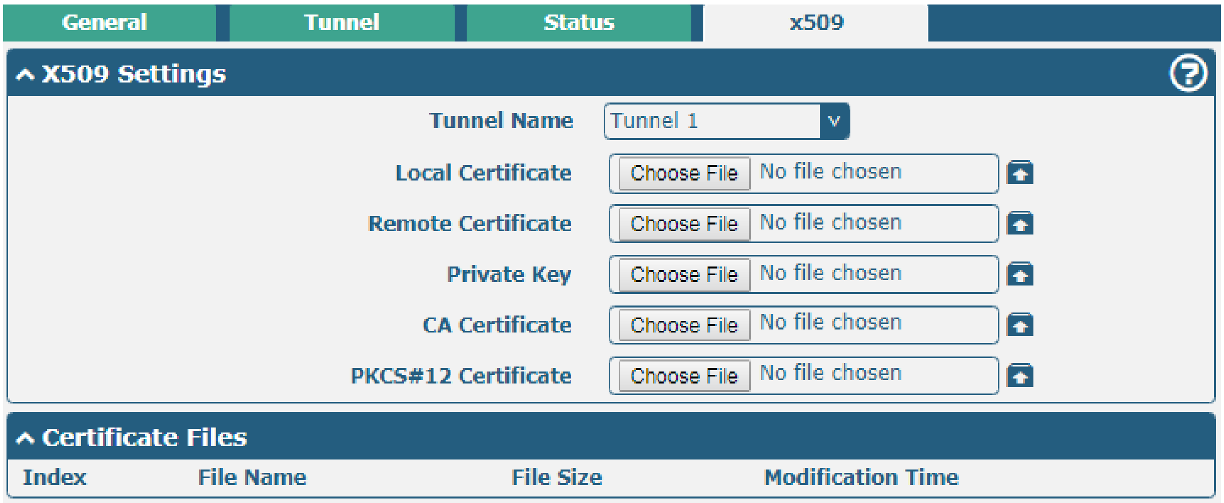


^ IPSec Tunnel Status

Index	Description	Status	Uptime

x509

User can upload the X509 certificates for the IPsec tunnel in this section.



^ X509 Settings

Tunnel Name: Tunnel 1

Local Certificate: No file chosen

Remote Certificate: No file chosen

Private Key: No file chosen

CA Certificate: No file chosen

PKCS#12 Certificate: No file chosen

^ Certificate Files

Index	File Name	File Size	Modification Time

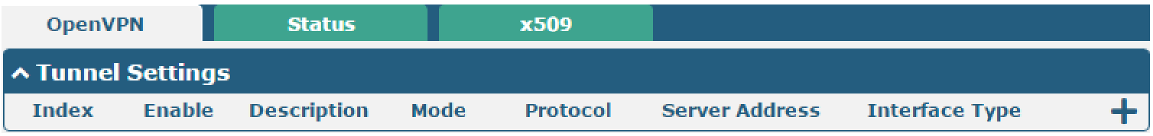
x509		
Item	Description	Default
X509 Settings		
Tunnel Name	Choose a valid tunnel.	Tunnel 1
Local Certificate	Click on “Choose File” to upload a local certificate file from your computer, and then import this file into your router. The correct file format is displayed as follows: @ca.crt @remote.crt @local.crt @private.key @crl.pem	Null
Remote Certificate	Click on “Choose File” to upload a remote certificate file from your computer, and then import this file into your router.	Null
Private Key	Select the correct private key file to import into the router	Null
Root certificate	Select the root certificate file to import into the router.	--
PKCS # 12 certificate	Select the PKCS # 12 certificate file to import into the router.	--
Certificate Files		
Index	Indicate the ordinal of the list.	--

File Name	Show the imported certificate’s name.	Null
File Size	Show the size of the certificate file.	Null
Modification Time	Show the timestamp of that the last time to modify the certificate file.	Null

3.19 VPN > Open VPN

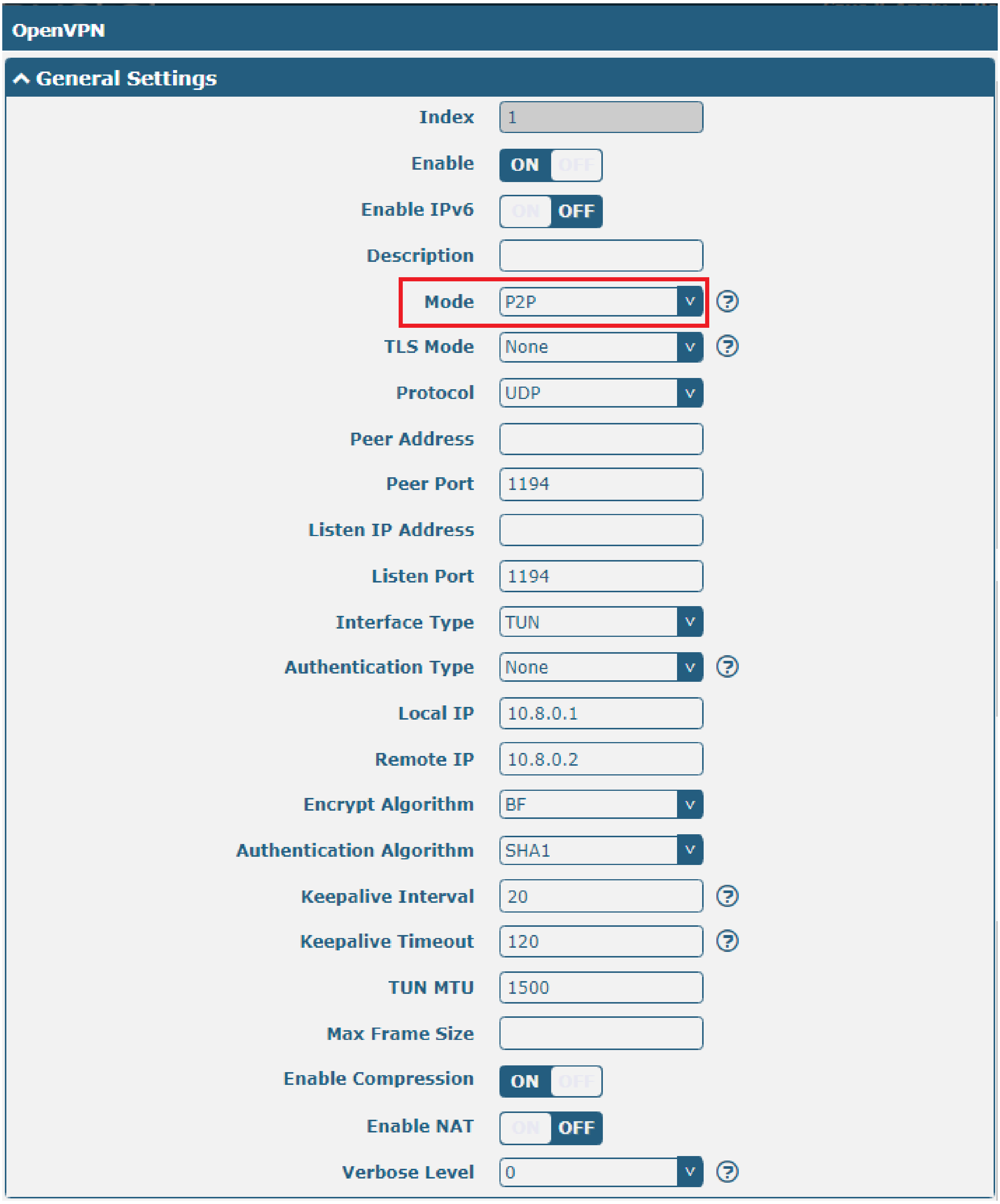
This section allows you to set the OpenVPN and the related parameters. OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. Router supports point-to-point and point-to-points connections.

OpenVPN



Index	Enable	Description	Mode	Protocol	Server Address	Interface Type

Click + to add tunnel settings. The maximum count is 3. The window is displayed as below when choosing “None” as the authentication type. By default, the mode is “P2P ”.

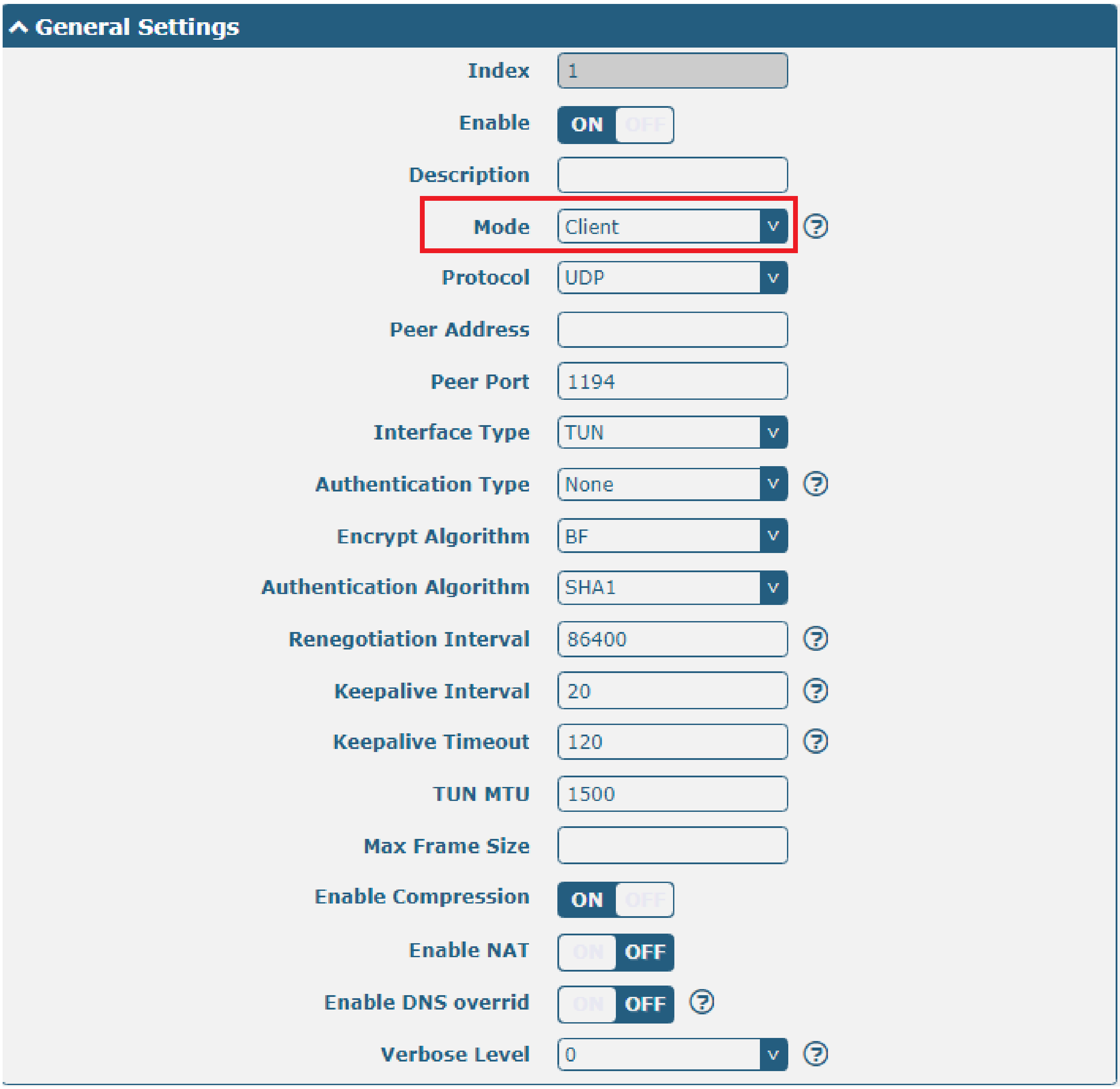


OpenVPN

General Settings

Index	1
Enable	[✓ ON] OFF
Enable IPv6	ON [✓ OFF]
Description	
Mode	P2P
TLS Mode	None
Protocol	UDP
Peer Address	
Peer Port	1194
Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	None
Local IP	10.8.0.1
Remote IP	10.8.0.2
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	[✓ ON] OFF
Enable NAT	ON [✓ OFF]
Verbose Level	0

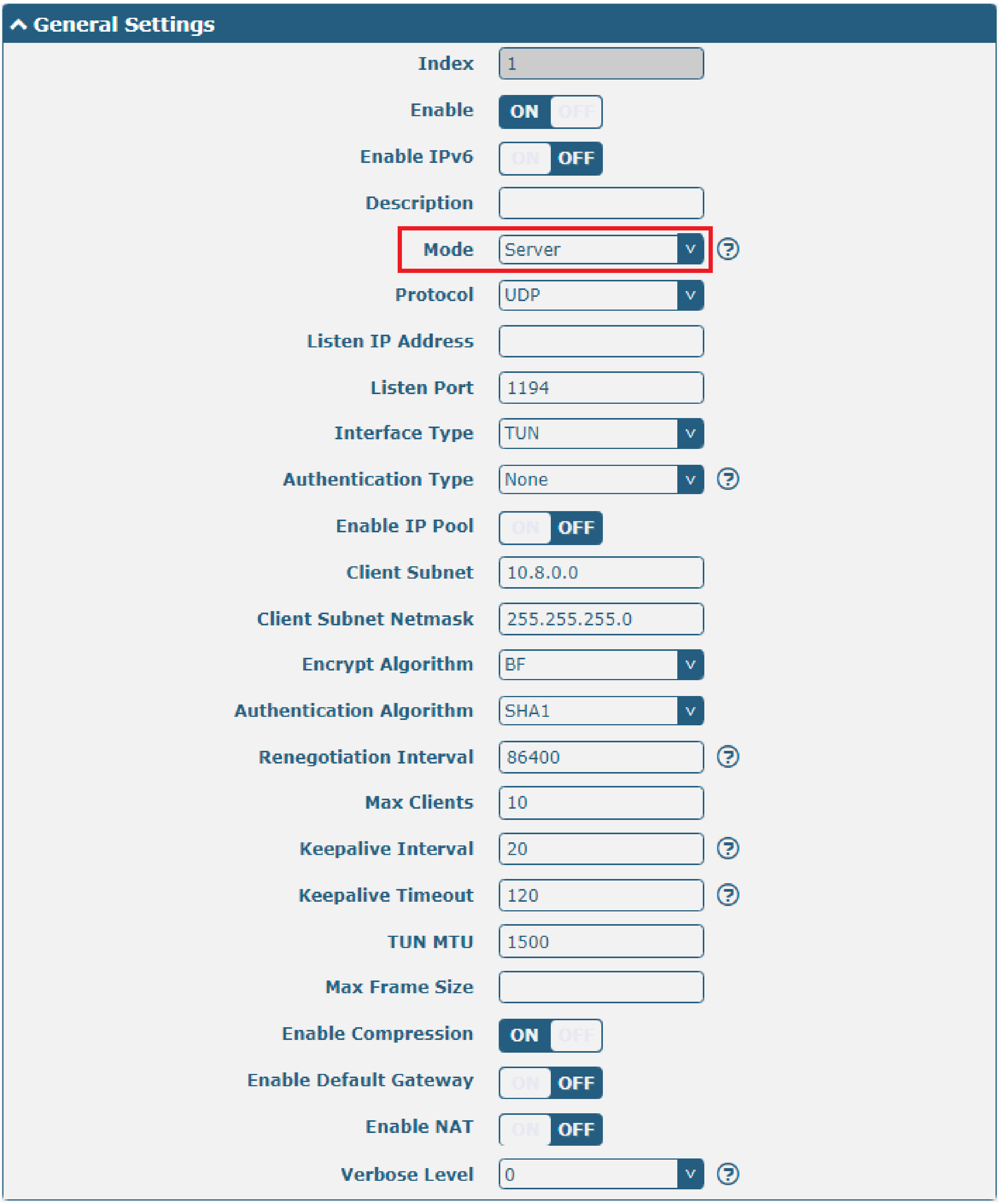
The window is displayed as below when choosing “Client” as the mode.



General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Peer Address	
Peer Port	1194
Interface Type	TUN
Authentication Type	None
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON
Enable NAT	OFF
Enable DNS overrid	OFF
Verbose Level	0

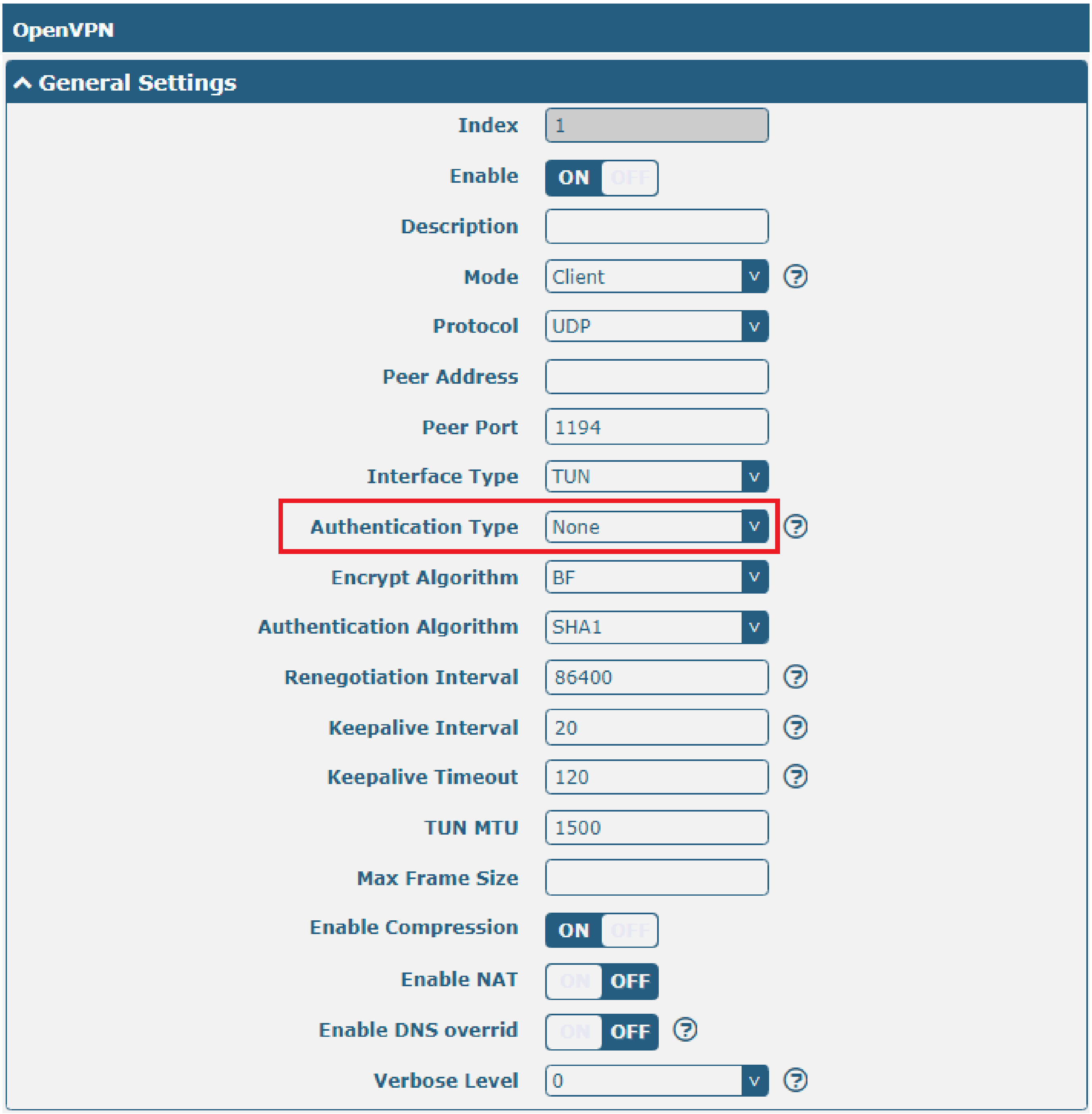
The window is displayed as below when choosing “Server” as the mode



General Settings

Index	1
Enable	ON
Enable IPv6	OFF
Description	
Mode	Server
Protocol	UDP
Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	None
Enable IP Pool	OFF
Client Subnet	10.8.0.0
Client Subnet Netmask	255.255.255.0
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Renegotiation Interval	86400
Max Clients	10
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON
Enable Default Gateway	OFF
Enable NAT	OFF
Verbose Level	0

The window is displayed as below when choosing “None” as the authentication type

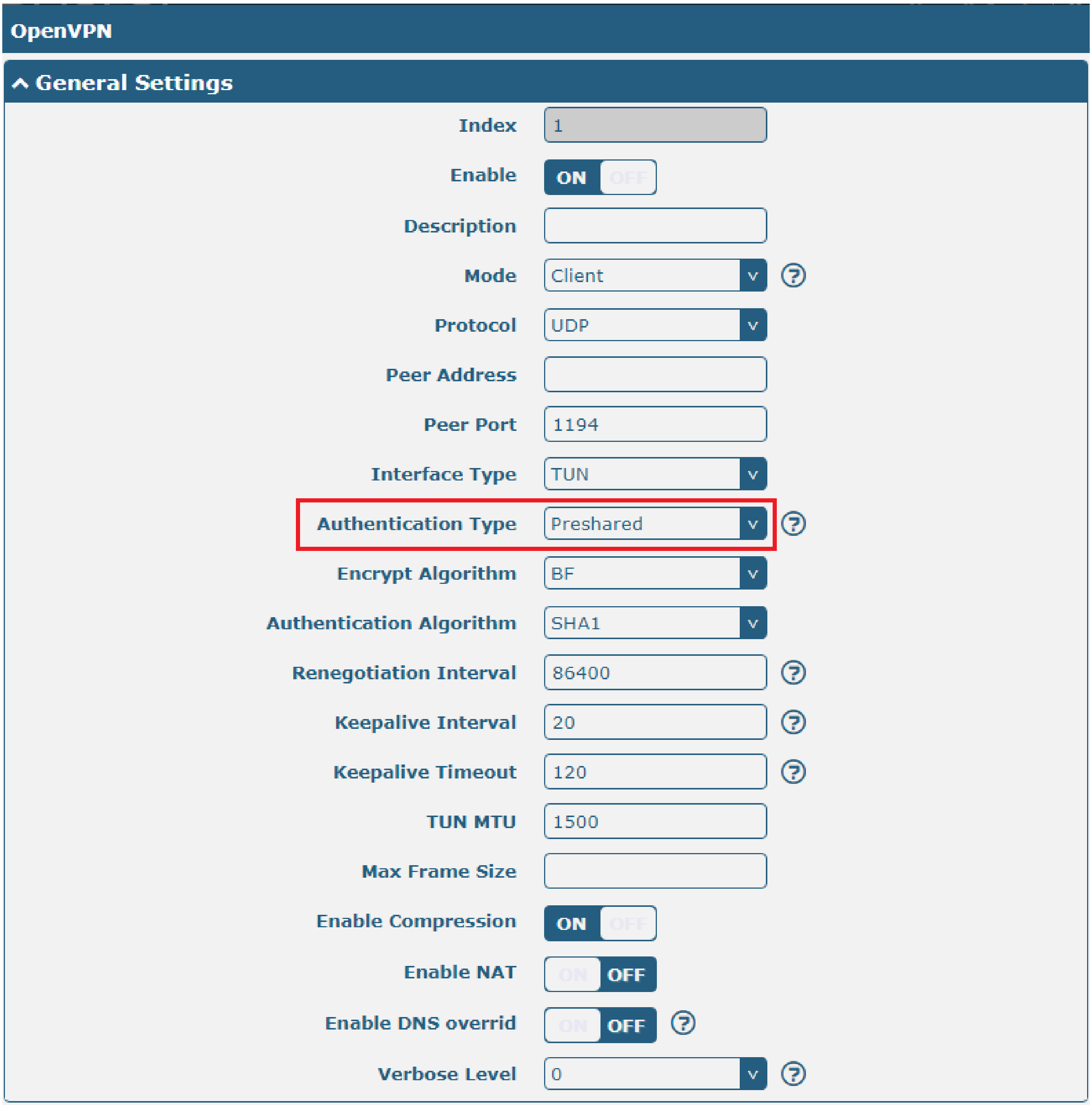


OpenVPN

General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Peer Address	
Peer Port	1194
Interface Type	TUN
Authentication Type	None
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON
Enable NAT	OFF
Enable DNS overrid	OFF
Verbose Level	0

The window is displayed as below when choosing “Preshared” as the authentication type.

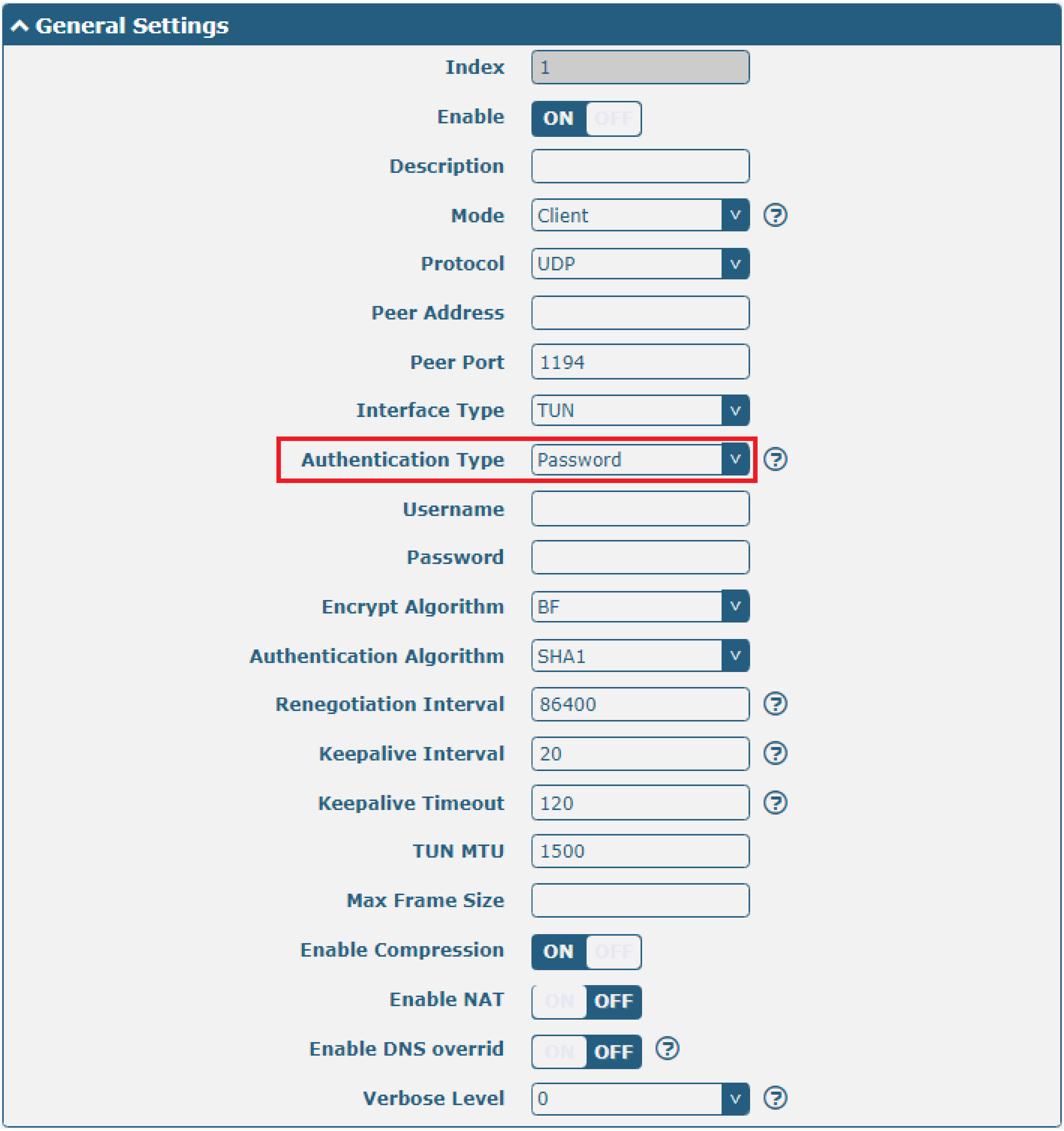


OpenVPN

General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Peer Address	
Peer Port	1194
Interface Type	TUN
Authentication Type	Preshared
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON
Enable NAT	OFF
Enable DNS overrid	OFF
Verbose Level	0

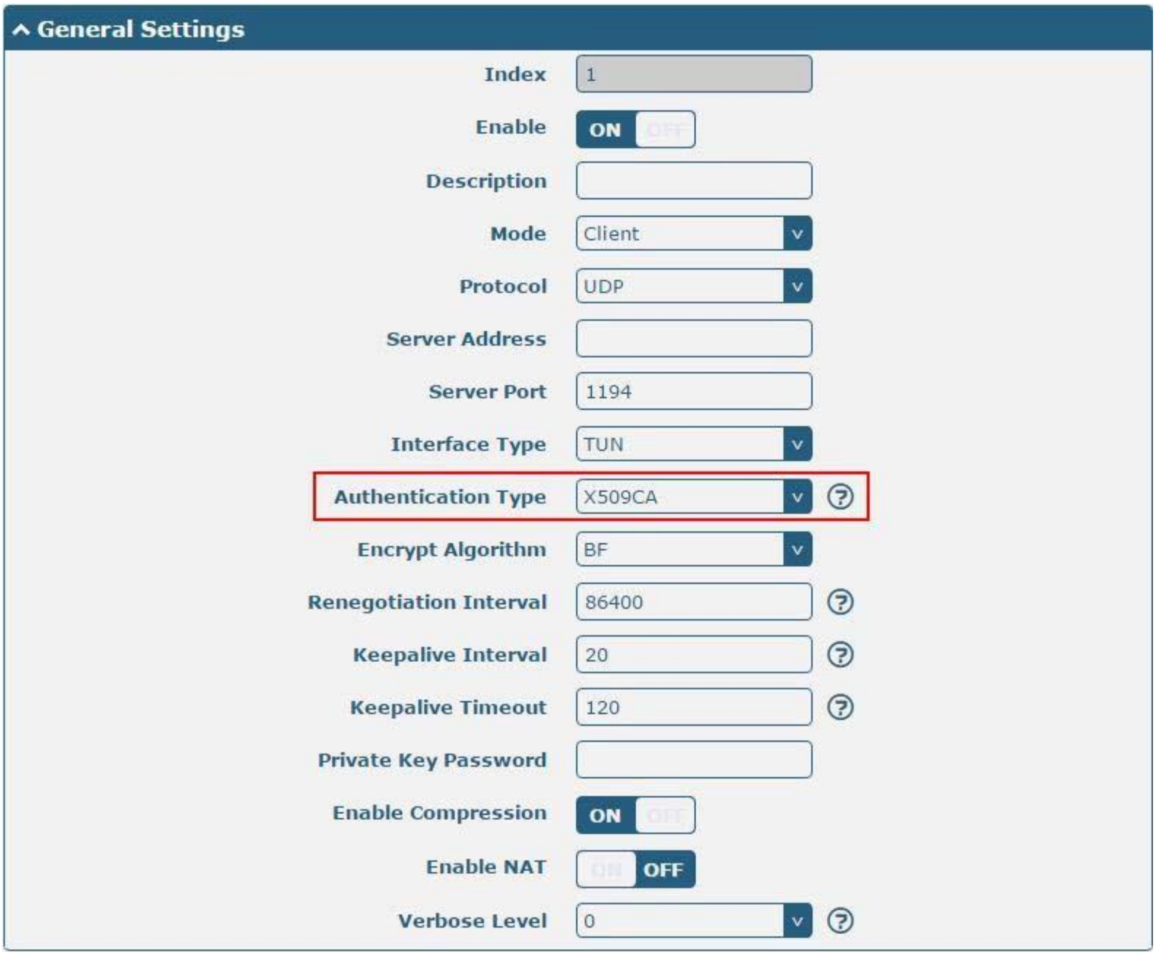
The window is displayed as below when choosing “Password ” as the authentication.



General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Peer Address	
Peer Port	1194
Interface Type	TUN
Authentication Type	Password
Username	
Password	
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON
Enable NAT	OFF
Enable DNS overrid	OFF
Verbose Level	0

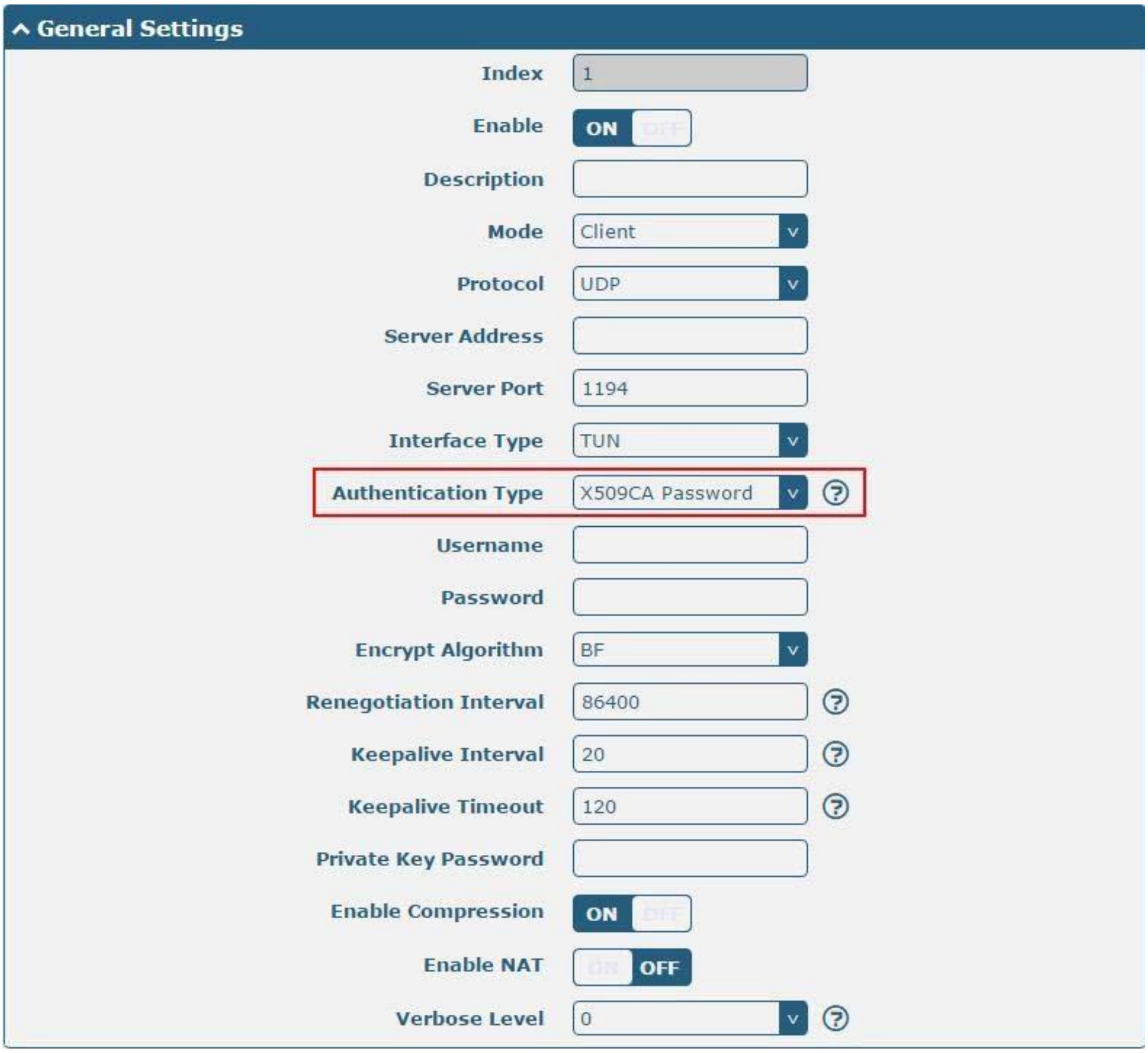
The window is displayed as below when choosing “ X509CA” as the authentication type.



General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	X509CA
Encrypt Algorithm	BF
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
Private Key Password	
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

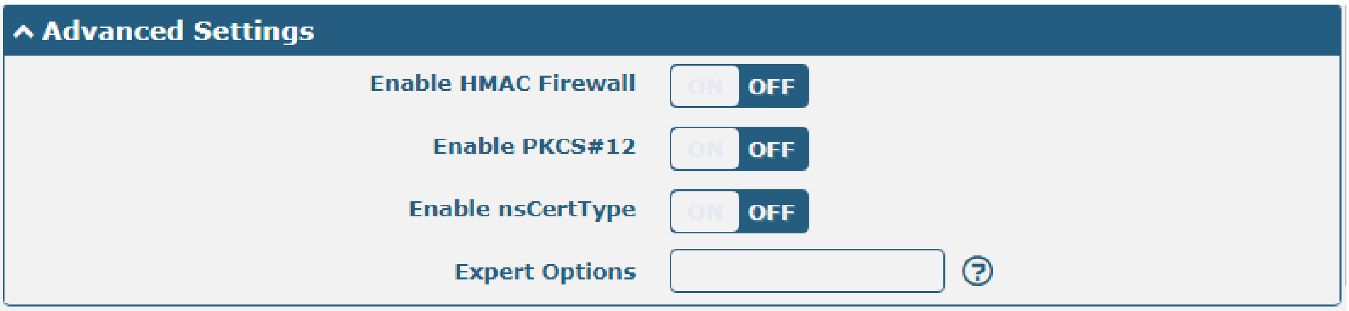
The window is displayed as below when choosing " X509CA Password" as the authentication type.



General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	X509CA Password
Username	
Password	
Encrypt Algorithm	BF
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
Private Key Password	
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

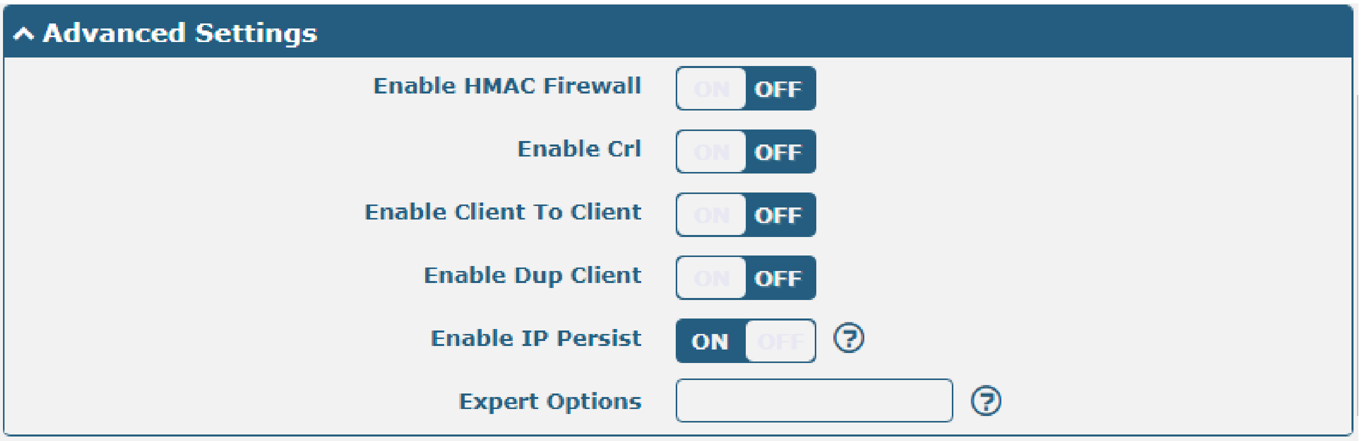
The window is displayed as below when choosing "Client" as the mode



Advanced Settings

Enable HMAC Firewall	OFF
Enable PKCS#12	OFF
Enable nsCertType	OFF
Expert Options	

The window is displayed as below when choosing"Server" as the mode



^ Advanced Settings

Enable HMAC Firewall: ON OFF

Enable Crl: ON OFF

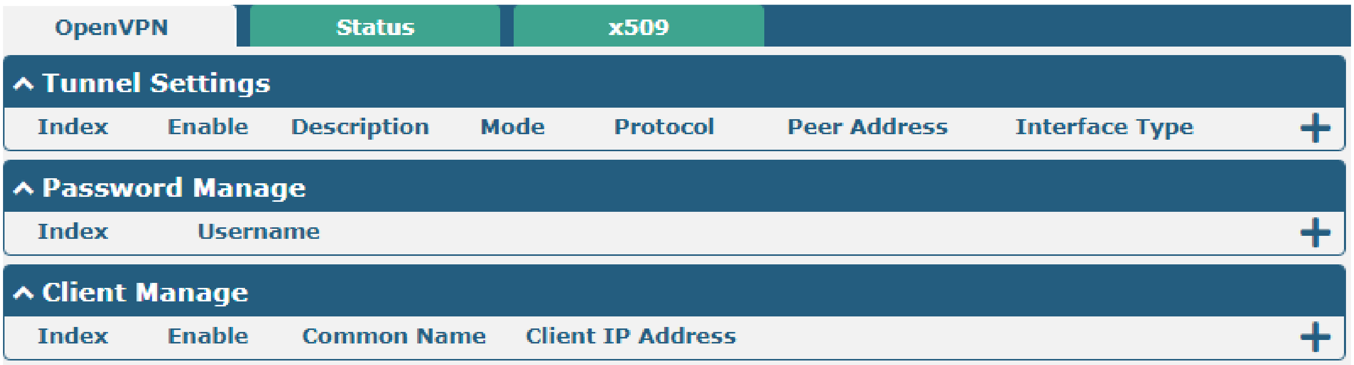
Enable Client To Client: ON OFF

Enable Dup Client: ON OFF

Enable IP Persist: ON OFF

Expert Options:

The window of "Virtual Private Network> OpenVPN> OpenVPN" is displayed as below when choosing “Server” as the mode and choosing “X509CA Password” as the authentication type .



^ Tunnel Settings

Index	Enable	Description	Mode	Protocol	Peer Address	Interface Type

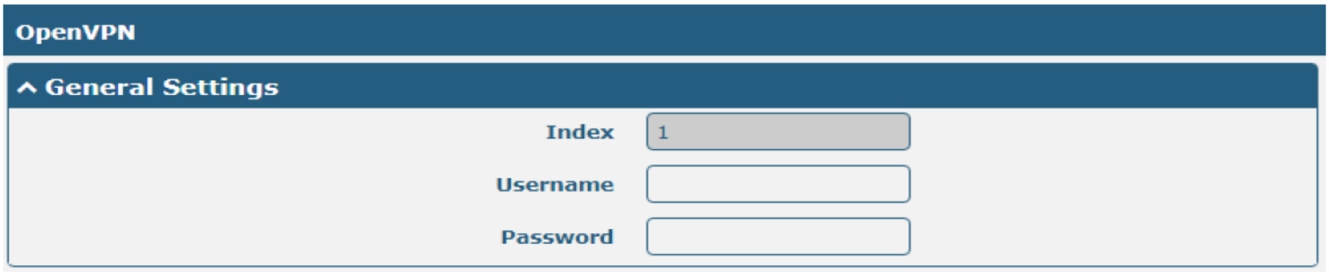
^ Password Manage

Index	Username

^ Client Manage

Index	Enable	Common Name	Client IP Address

Click User Password Management + to add username and password, as shown below:



OpenVPN

^ General Settings

Index: 1

Username:

Password:

Click Client Management + to add Client information, as shown below:

General Settings @ OpenVPN		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/ disable this OpenVPN tunnel.	ON
Enable IPv6	Click the toggle button to enable/disable this OpenVPN tunnel to use IPv6.	OFF
Description	Enter a description for this OpenVPN tunnel.	Null
Mode	Select from “P2P”, “Client” or “Server”.	Client
TLS Mode	Select from “None”, “Client” or “Server”.	None
Protocol	Select from “UDP”, “TCP-Client” or “TCP-Server”.	UDP

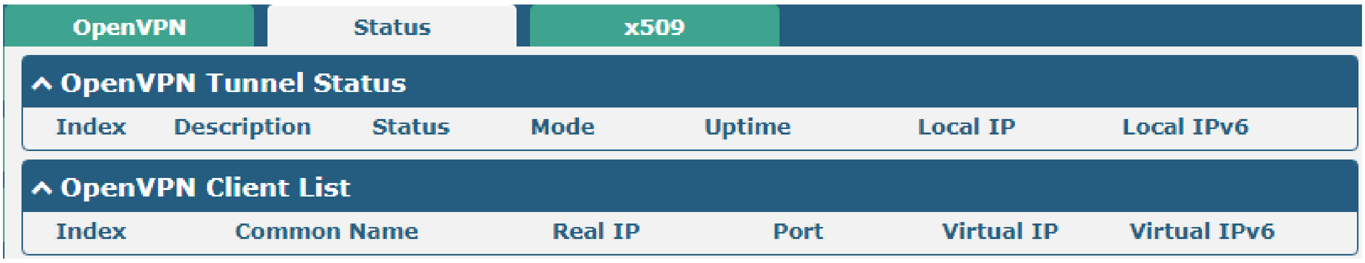
Server Address	Enter the end-to-end IP address or the domain of the remote OpenVPN server.	Null
Server Port	Enter the end-to-end listener port or the listener port of the OpenVPN server.	1194
Listening address	Local server address.	Null
Listening port	Local server port.	1194
Interface Type	Select from “TUN”, “TAP” which are two different kinds of device interface for OpenVPN. The difference between TUN and TAP device is that a TUN device is a point-to-point virtual device on network while a TAP device is a virtual device on Ethernet.	TUN
Authentication Type	Select from “None”, “Preshared”, “Password”, “X509CA” and “X509CA Password”. Note: “None” and “Preshared” authentication type are only working with P2P mode.	None
Enable IP Address pool	Click the toggle button to enable / disable the IP address pool allocation function.	OFF
Starting Address	Defines the beginning of an IP address pool that assigns addresses to OpenVPN clients.	10.8.0.5
End Address	Defines the end of the IP address pool for assigning addresses to OpenVPN clients.	10.8.0.254
Client Network	Enter the client network IP.	10.8.0.0
Client Netmask	Enter the client netmask.	255.255.255.0
Username	Enter the username used for “ Password” or “ X509CA Password” authentication type.	Null
Password	Enter the password used for “ Password” or “ X509CA Password” authentication type.	Null
Local IP	Enter the local virtual IP.	10.8.0.1
Remote IP	Enter the remote virtual IP.	10.8.0.2
Encrypt Algorithm	Select from “ BF” , “ DES”, “ DES-EDE3”, “ AES128” , “ AES192” and“ AES256” . • BF: Use 128-bit BF encryption algorithm in CBCmode • DES: Use 64-bit DESencryption algorithm in CBCmode • DES-EDE3: Use 192-bit 3DESencryption algorithm in CBCmode • AES128: Use 128-bit AESencryption algorithm in CBCmode • AES192: Use 192-bit AESencryption lgorithm in CBCmode • AES256: Use 256-bit AESencryption algorithm in CBCmode	BF
Renegotiation Interval	Set the renegotiation interval. If connection failed, OpenVPN will renegotiate when the renegotiation interval reached.	86400
Maximum number of clients	Set the maximum number of clients allowed to access the OpenVPN	10
Keepalive Interval	Set keepalive (ping) interval to check if the tunnel is active.	20
Keepalive Timeout	Set the keepalive timeout. Trigger OpenVPN restart after n seconds pass without reception of a ping or other packet from remote.	120

MTU	Set the maximum transmission unit.	1500
Data Sharding	Set the maximum frame length.	Null
Private Key Password	Enter the private key password under the “X509CA” and “X509CA Password” authentication type.	Null
Enable Compression	Click the toggle button to enable/ disable this option. Enable to compress the data stream of the header.	ON
Enable Default Gateway	Standalone switch button to enable / disable the default gateway function. After enabling, push the local tunnel address as the default gateway of the peer device.	OFF
Enable NAT	Click the toggle button to enable/ disable the NAT option. When enabled, the source IP address of host behind router will be disguised before accessing the remote OpenVPN client.	OFF
Receive DNS Push	Standalone switch button to enable / disable receiving DNS push function. After it is enabled, it is allowed to receive DNS information pushed by the peer.	OFF
Verbose Level	Select the level of the output log and values from 0 to 11. 0: No output except fatal errors 1~4: Normal usage range 5: Output Rand W characters to the console for each packet read and write 6~11: Debug info range	0
Advanced Settings @ OpenVPN		
Enable HMAC Firewall	Click the toggle button to enable/ disable this option. Add an additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks.	OFF
Enable PKCS#12	Click the toggle button to enable/ disable the PKCS#12 certificate. It is an exchange of digital certificate encryption standard, used to describe personal identity information.	OFF
Enable nsCertType	Click the toggle button to enable/ disable nsCertType. Require that peer certificate was signed with an explicit nsCertType designation of "server".	OFF
Enable Crl	Click the toggle button to enable / disable the option. When enabled, client certificates can be revoked.	OFF
Enable client to client	Click the toggle button to enable / disable the option. When enabled, clients can communicate with each other.	OFF
Enable Dup Client	Click the toggle button to enable / disable the option. After being enabled, the tunnel IPs obtained by multiple clients are different, and the tunnel IP of the client and the tunnel IP of the server are interoperable.	OFF
Enable IP address hold	Click the toggle button to enable / disable the option. When enabled, the IP in the address pool is obtained automatically.	ON
Expert Options	Enter some other options of OpenVPN in this field. Each expression can be separated by a ‘;’.	Null
Advanced Settings @ User Password Management		
Username	Custom tunnel connection username.	Null

Password	Custom tunnel connection password.	Null
	Advanced Settings @ Client Management	
Enable	Click the toggle button to enable / disable this option. When enabled, the client IP address can be managed.	OFF
Common Name	Set the certificate name.	Null
Client IP Address	Set a fixed client virtual IP.	Null

Status

This section allows you to view the status of the OpenVPN tunnel.



^ OpenVPN Tunnel Status

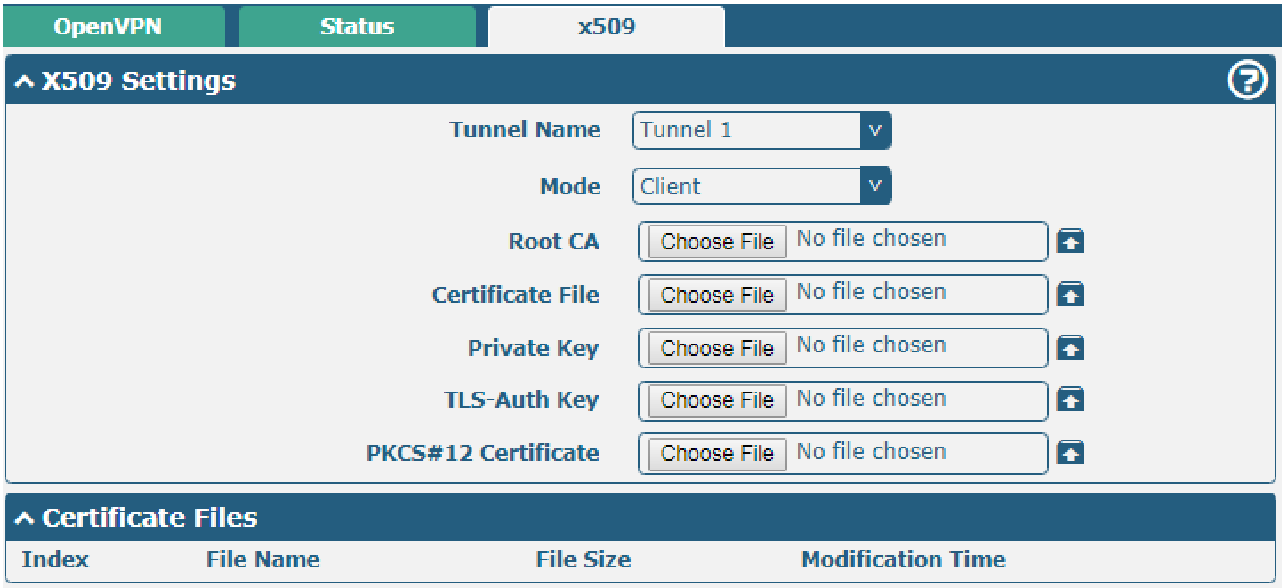
Index	Description	Status	Mode	Uptime	Local IP	Local IPv6

^ OpenVPN Client List

Index	Common Name	Real IP	Port	Virtual IP	Virtual IPv6

x509

User can upload the X509 certificates for the OpenVPN in this section.



^ X509 Settings

Tunnel Name: Tunnel 1

Mode: Client

Root CA: No file chosen

Certificate File: No file chosen

Private Key: No file chosen

TLS-Auth Key: No file chosen

PKCS#12 Certificate: No file chosen

^ Certificate Files

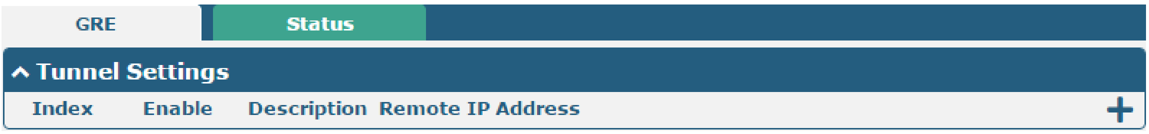
Index	File Name	File Size	Modification Time

x509		
Item	Description	Default
X509 Settings		
Tunnel Name	Choose a valid tunnel. Select from "Tunnel 1", "Tunnel 2", "Tunnel 3", "Tunnel 4", "Tunnel 5" or "Tunnel 6".	Tunnel 1
Tunnel Mode	Select from "P2P Mode", "Client Mode" or "Server Mode"	Client mode
Root certificate	Select the root certificate file to import into the router.	--
Certificate File	Click on “Choose File” to upload certificate file into the router.	--
Private Key	Click on “Choose File” to upload private key into the router.	--
TLS Auth Key	Click on “Choose File” to upload TLS-AutH key into the router.	--
PKCS#12 Certificate	Click on “Choose File” to upload PKCS#12 Certificate into the router.	--
Certificate Files		
Index	Indicate the ordinal of the list.	--
Filename	Show the imported certificate’s name.	Null
File Size	Show the size of the certificate file.	Null
Modification Time	Show the timestamp of that the last time to modify the certificate file.	Null

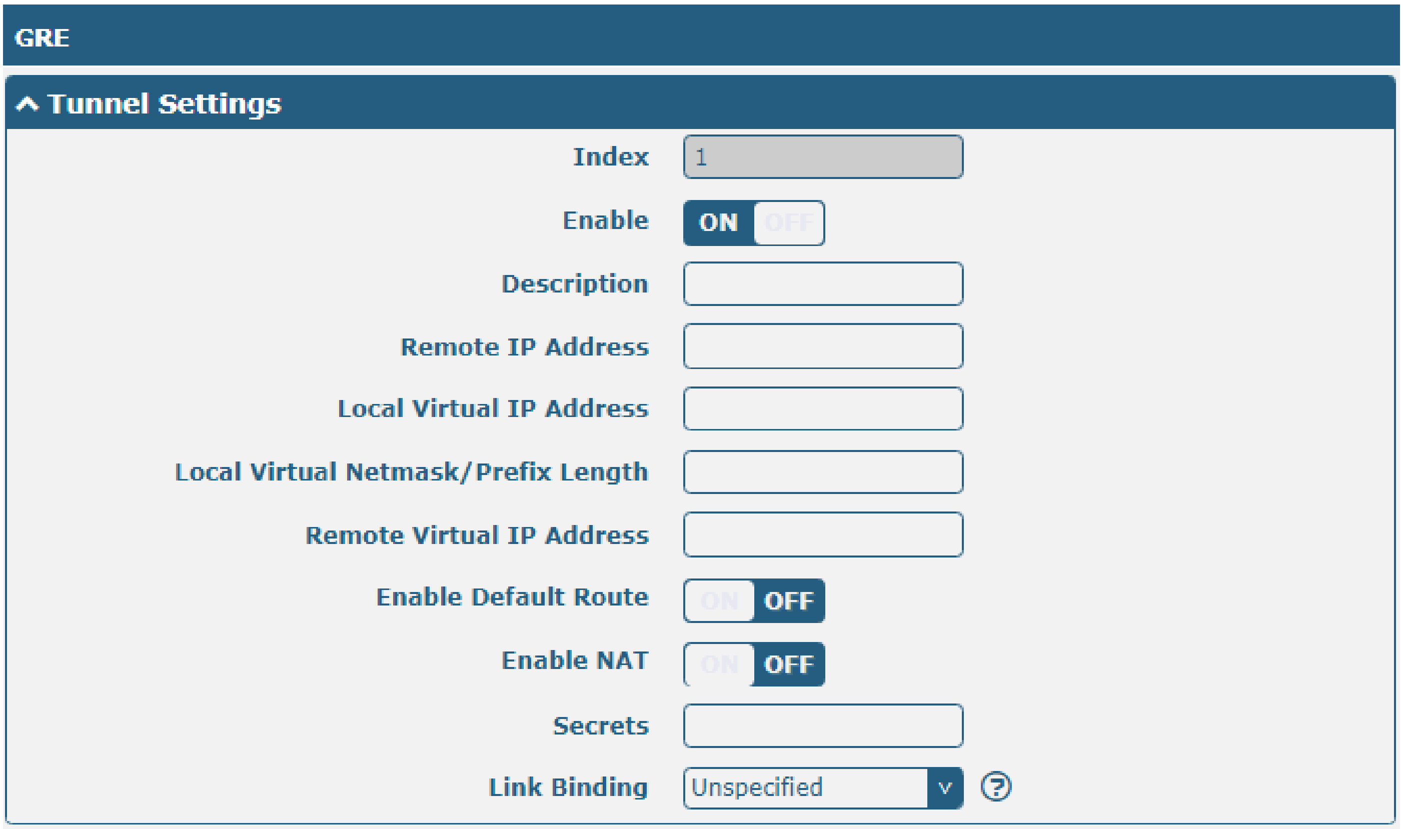
3.20 VPN > GRE

This section allows you to set the GRE and the related parameters. Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network.

GRE



Click + to add tunnel settings. The maximum count is 3.



GRE

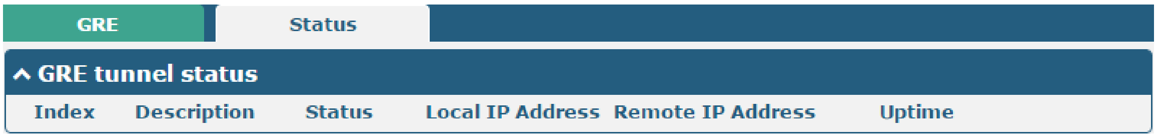
Tunnel Settings

Index	1
Enable	ON
Description	
Remote IP Address	
Local Virtual IP Address	
Local Virtual Netmask/Prefix Length	
Remote Virtual IP Address	
Enable Default Route	OFF
Enable NAT	OFF
Secrets	
Link Binding	Unspecified

Tunnel Settings @ GRE		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/ disable this GRE tunnel.	ON
Description	Enter a description for this GRE tunnel.	Null
Remote IP Address	Set the remote real IP address of the GRE tunnel.	Null
Local Virtual IP Address	Set the local virtual IP address of the GRE tunnel.	Null
Local Virtual Netmask	Set the local virtual Netmask of the GRE tunnel.	Null
Remote Virtual IP Address / IPv6 prefix length	Set the remote virtual IP Address of the GRE tunnel.	Null
Enable Default Route	Click the toggle button to enable/ disable this option. When enabled, all the traffics of DSR-211 Router will go through the GRE VPN.	OFF
Enable NAT	Click the toggle button to enable/ disable this option. This option must be enabled when router under NAT environment.	Disable
Secrets	Set the key of the GRE tunnel.	Null
Link Binding	Select from "WWAN1", "WWAN2", "WAN", or "WLAN".	Not bound

Status

This section allows you to view the status of GRE tunnel.

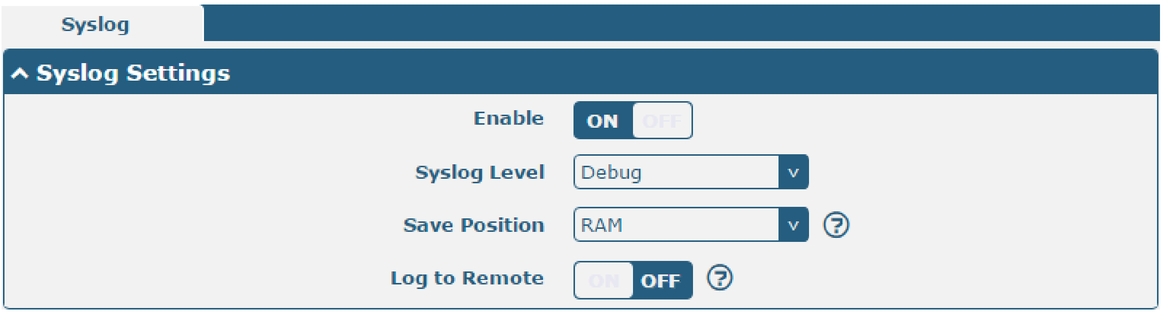


GRE tunnel status

Index	Description	Status	Local IP Address	Remote IP Address	Uptime

3.21 Services > Syslog

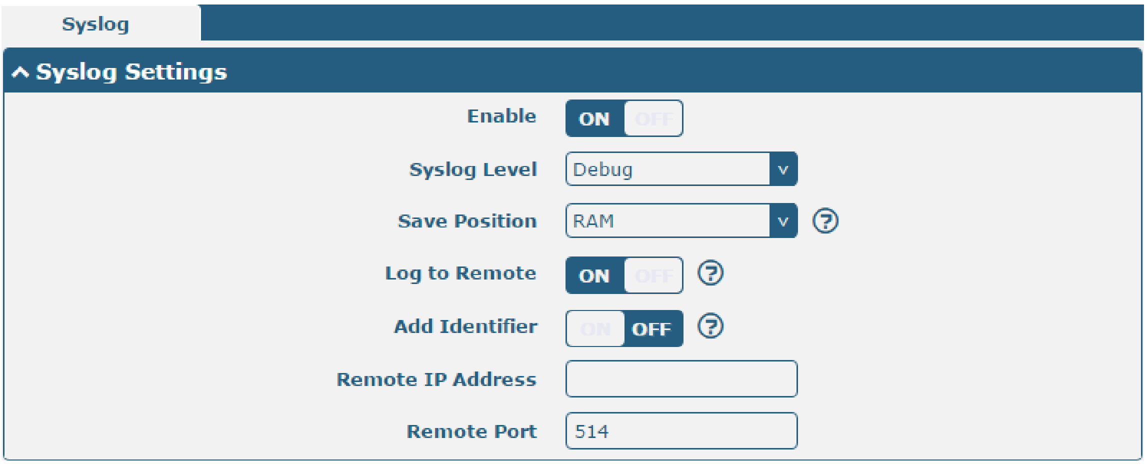
This section allows you to set the syslog parameters. The system log of DSR-211 Router can be saved in the local, also supports to be sent to remote log server and specified application debugging. By default, the “Log to Remote” option is disabled.



Syslog Settings

Enable	ON
Syslog Level	Debug
Save Position	RAM
Log to Remote	OFF

The window is displayed as below when enabling the “Log to Remote” option.



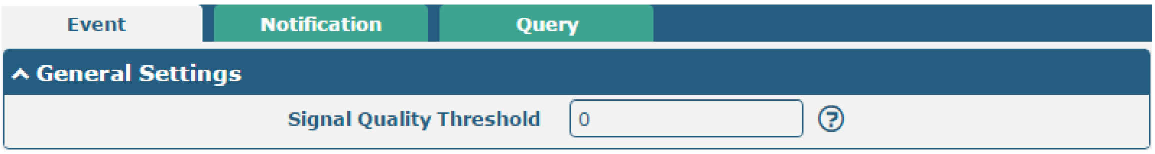
Syslog Settings

Enable	ON
Syslog Level	Debug
Save Position	RAM
Log to Remote	ON
Add Identifier	OFF
Remote IP Address	
Remote Port	514

Syslog Settings		
Item	Description	Default
Enable	Click the toggle button to enable/ disable the Syslog settings option.	OFF
Syslog Level	Select from "Debug", "Info", " Notice" , " Warning" or " Error" , which from low to high. The lower level will output more syslog in detail.	Debug
Save Position	Select the save position from " RAM" , " NVM" or " Console" . Choose "RAM" , the data will be cleared after reboot. Note: It's not recommended that saving syslog to NVM (Non-Volatile Memory) for a long time.	RAM
Log to Remote	Click the toggle button to enable/ disable this option. Enable to allow router sending syslog to the remote syslog server. You need to enter the IPand Port of the syslog server.	OFF
Add Identifier	Click the toggle button to enable/ disable this option. When enabled, you can add serial number to syslog message which used for loading Syslog to DigiLink.	OFF
Remote IP Address	Enter the IP address of syslog server when enabling the " Log to Remote" option.	Null
Remote Port	Enter the port of syslog server when enabling the " Log to Remote" option.	514

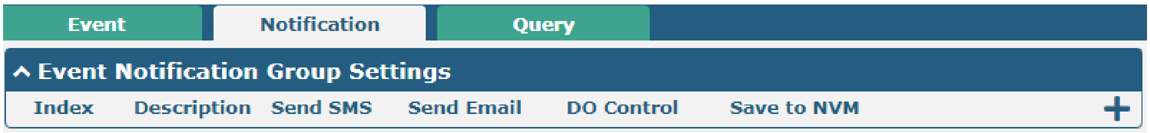
3.22 Services > Event

This section allows you to set the event parameters. Event feature provides an ability to send alerts by SMS or Email when certain system events occur.



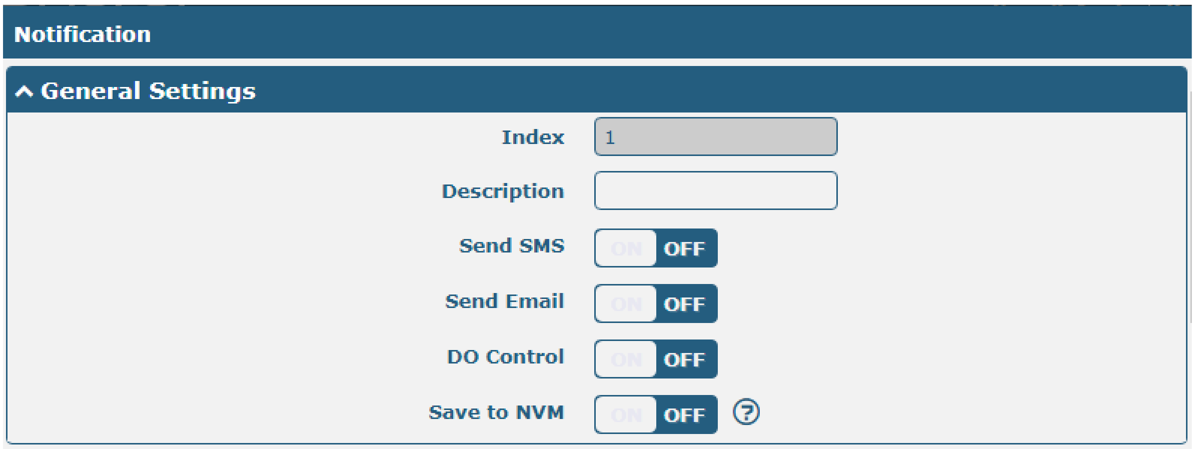
Signal Quality Threshold: 0

General Settings @ Event		
Item	Description	Default
Signal Quality Threshold	Set the threshold for signal quality. Router will generate a log event when the actual threshold is less than the specified threshold. 0 means disable this option.	0



Index	Description	Send SMS	Send Email	DO Control	Save to NVM

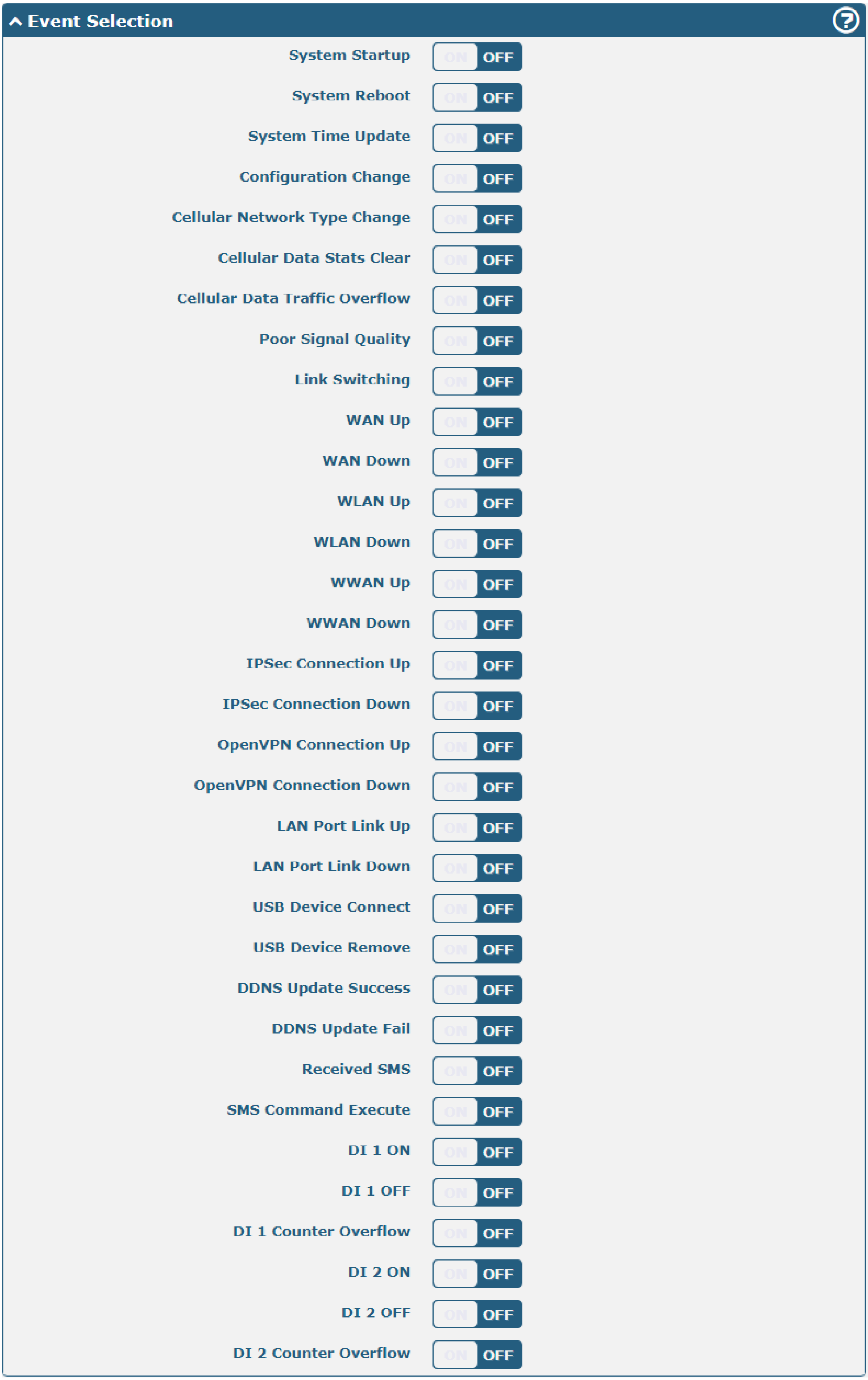
Click + button to add Event parameters.



Notification

General Settings

Index	1
Description	
Send SMS	ON OFF
Send Email	ON OFF
DO Control	ON OFF
Save to NVM	ON OFF ?

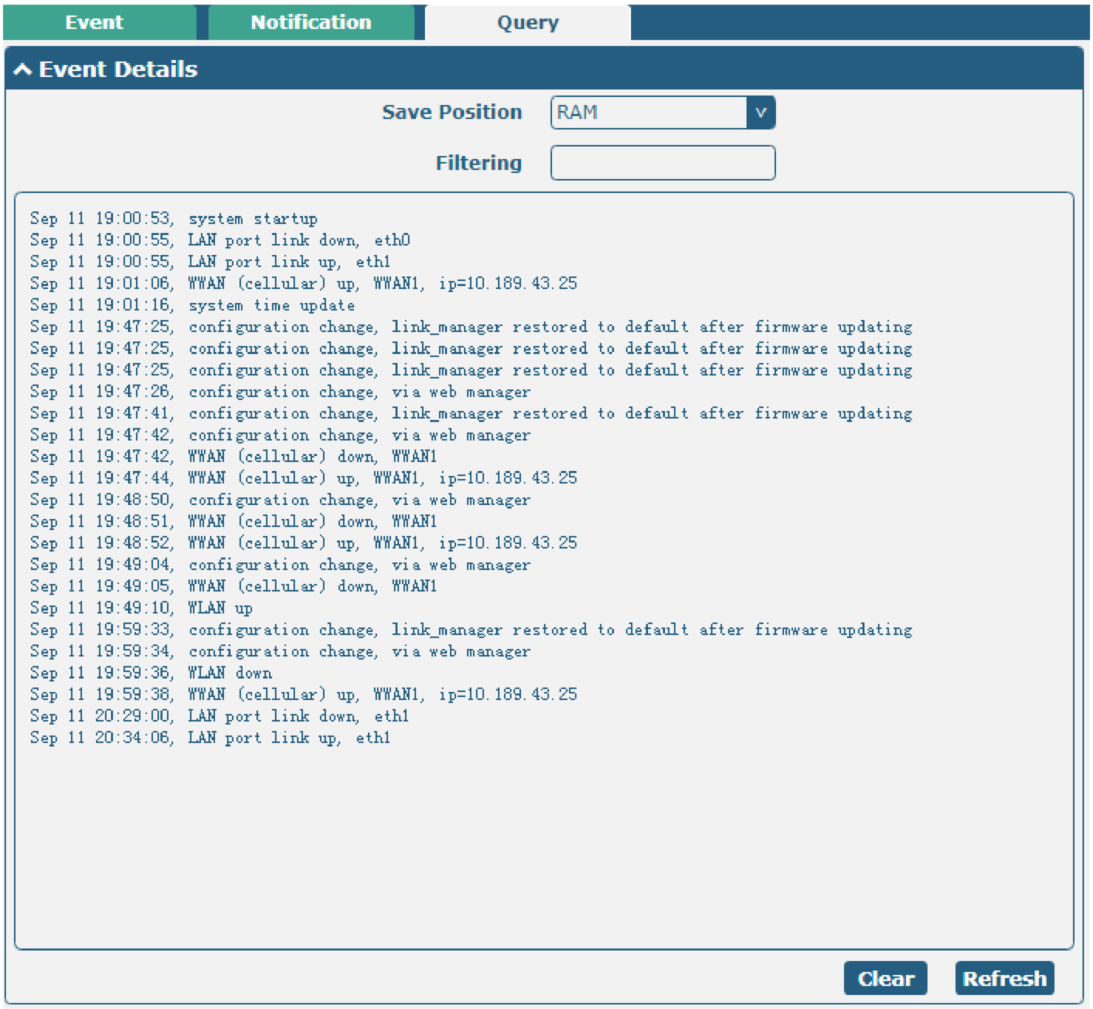


Event Selection

System Startup	OFF
System Reboot	OFF
System Time Update	OFF
Configuration Change	OFF
Cellular Network Type Change	OFF
Cellular Data Stats Clear	OFF
Cellular Data Traffic Overflow	OFF
Poor Signal Quality	OFF
Link Switching	OFF
WAN Up	OFF
WAN Down	OFF
WLAN Up	OFF
WLAN Down	OFF
WWAN Up	OFF
WWAN Down	OFF
IPSec Connection Up	OFF
IPSec Connection Down	OFF
OpenVPN Connection Up	OFF
OpenVPN Connection Down	OFF
LAN Port Link Up	OFF
LAN Port Link Down	OFF
USB Device Connect	OFF
USB Device Remove	OFF
DDNS Update Success	OFF
DDNS Update Fail	OFF
Received SMS	OFF
SMS Command Execute	OFF
DI 1 ON	OFF
DI 1 OFF	OFF
DI 1 Counter Overflow	OFF
DI 2 ON	OFF
DI 2 OFF	OFF
DI 2 Counter Overflow	OFF

General Settings @ Notification		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this group.	Null
Sent SMS	Click the toggle button to enable/ disable this option. When enabled, the router will send notification to the specified phone numbers via SMSif event occurs. Set the related phone number in 3.24 Services > Email", and use ';'to separate each number.	OFF
Send Email	Click the toggle button to enable/ disable this option. When enabled, the router will send notification to the specified email box via Email if event occurs. Set the related email address in " 3.24 Services > Email".	OFF
DO Control	Click the toggle button to enable / disable this option. After it is turned on, the event router will send it to the corresponding DO in the form of Low / High level.	OFF
Save to NVM	Click the toggle button to enable/ disable this option. Enable to save event to nonvolatile memory.	OFF

In the following window you can query various types of events record. Click Refresh to query filtered events while click Clear r the event records in the window.



Save Position: RAM

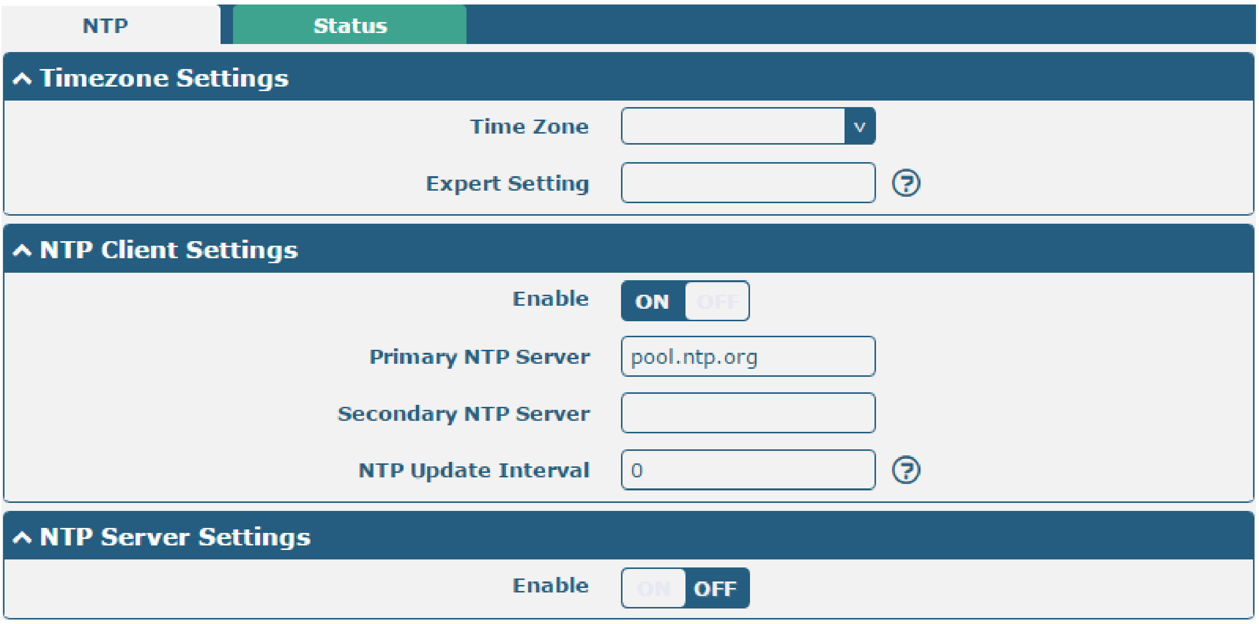
Filtering:

```
Sep 11 19:00:53, system startup
Sep 11 19:00:55, LAN port link down, eth0
Sep 11 19:00:55, LAN port link up, eth1
Sep 11 19:01:06, WWAN (cellular) up, WWAN1, ip=10.189.43.25
Sep 11 19:01:16, system time update
Sep 11 19:47:25, configuration change, link_manager restored to default after firmware updating
Sep 11 19:47:25, configuration change, link_manager restored to default after firmware updating
Sep 11 19:47:25, configuration change, link_manager restored to default after firmware updating
Sep 11 19:47:26, configuration change, via web manager
Sep 11 19:47:41, configuration change, link_manager restored to default after firmware updating
Sep 11 19:47:42, configuration change, via web manager
Sep 11 19:47:42, WWAN (cellular) down, WWAN1
Sep 11 19:47:44, WWAN (cellular) up, WWAN1, ip=10.189.43.25
Sep 11 19:48:50, configuration change, via web manager
Sep 11 19:48:51, WWAN (cellular) down, WWAN1
Sep 11 19:48:52, WWAN (cellular) up, WWAN1, ip=10.189.43.25
Sep 11 19:49:04, configuration change, via web manager
Sep 11 19:49:05, WWAN (cellular) down, WWAN1
Sep 11 19:49:10, WLAN up
Sep 11 19:59:33, configuration change, link_manager restored to default after firmware updating
Sep 11 19:59:34, configuration change, via web manager
Sep 11 19:59:36, WLAN down
Sep 11 19:59:38, WWAN (cellular) up, WWAN1, ip=10.189.43.25
Sep 11 20:29:00, LAN port link down, eth1
Sep 11 20:34:06, LAN port link up, eth1
```

Event Details		
Item	Description	Default
Save Position	Select the events' save position from "RAM" or "NVM" . RAM: Random-access memory NVM: Non-Volatile Memory	RAM
Filter Message	Event will be filtered according to the Filter Message that the user set. Click the "Refresh" button, the filtered event will be displayed in the follow box. Use "&" to separate more than one filter message, such as message1& message2.	Null

3.23 Services > NTP

This section allows you to set the related NTP (Network Time Protocol) parameters, including Time zone, NTP Client and NTP Server.



^ Timezone Settings

Time Zone

Expert Setting

^ NTP Client Settings

Enable: ON

Primary NTP Server: pool.ntp.org

Secondary NTP Server

NTP Update Interval: 0

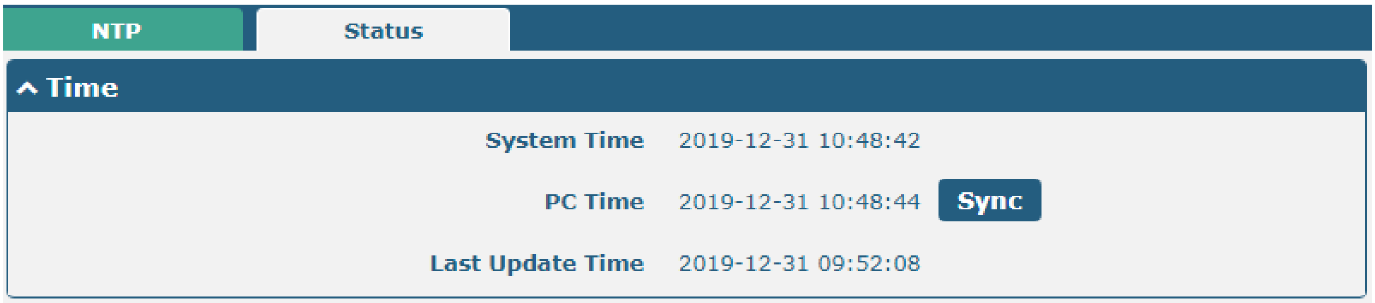
^ NTP Server Settings

Enable: OFF

NTP		
Item	Description	Default
Timezone Settings		
Time Zone	Click the drop down list to select the time zone you are in.	MEZ+08:00
Expert Setting	Specify the time zone with Daylight Saving Time in TZ environment variable format. The Time Zone option will be ignored in this case.	Null
NTP Client Settings		
Enable	Click the toggle button to enable/ disable this option. Enable to synchronize time with the NTP server.	ON
Primary NTP Server	Enter primary NTP Server's IP address or domain name.	pool.ntp.org
Secondary NTP Server	Enter secondary NTP Server's IP address or domain name.	Null

NTP Update interval	Enter the interval (minutes) which NTP client synchronize the time from NTP server. Minutes wait for next update, and 0 means update only once.	0
NTP Server Settings		
Enable	Click the toggle button to enable the NTP server option.	OFF

This window allows you to view the current time of router and also synchronize the router time. Click Sync button to synchronize the router time with PC's.



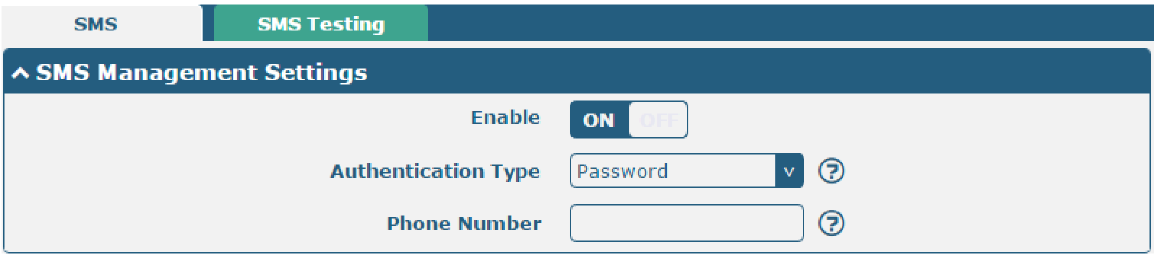
System Time 2019-12-31 10:48:42

PC Time 2019-12-31 10:48:44

Last Update Time 2019-12-31 09:52:08

3.24 Services > SMS

This section allows you to set SMS parameters. DSR-211 Router supports SMS management, and user can control and configure their routers by sending SMS. For more details about SMS control, refer to 4.2.2 SMS Remote Control.



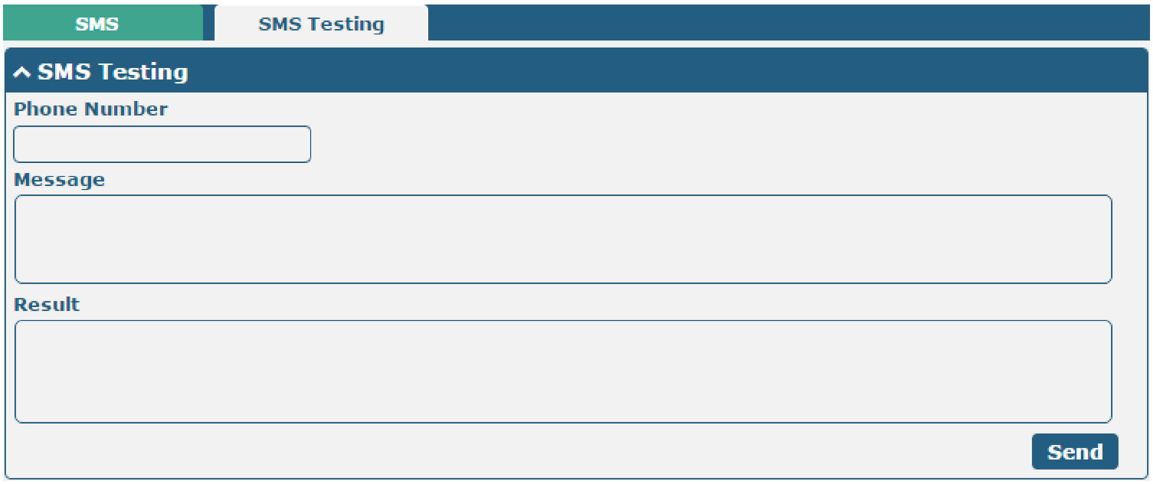
Enable ON OFF

Authentication Type Password

Phone Number

SMS Management Settings		
Item	Description	Default
Enable	Click the toggle button to enable/ disable the SMS Management option. Note: If this option is disabled, the SMS configuration is invalid.	ON
Authentication Type	Select Authentication Type from "Password" , " Phonenum" or " Both" . • Password: Use the same username and password as WEB manager for authentication. For example, the format of the SMS should be "username: password; cmd1; cmd2; …" Note: Set the WEB manager password in System > User Management section. • Phonenum: Use the Phone number for authenticating, and user should set the Phone Number that is allowed for SMS management. The format of the SMS should be " cmd1; cmd2; • Both: Use both the "Password" and " Phonenum" for authentication. User should set the Phone Number that is allowed for SMS management. The format of the SMS should be " username: password; cmd1; cmd2; …"	Password
Phone Number	Set the phone number used for SMS management, and use '; 'to separate each number. Note: It can be null when choose "Password" as the authentication type.	Null

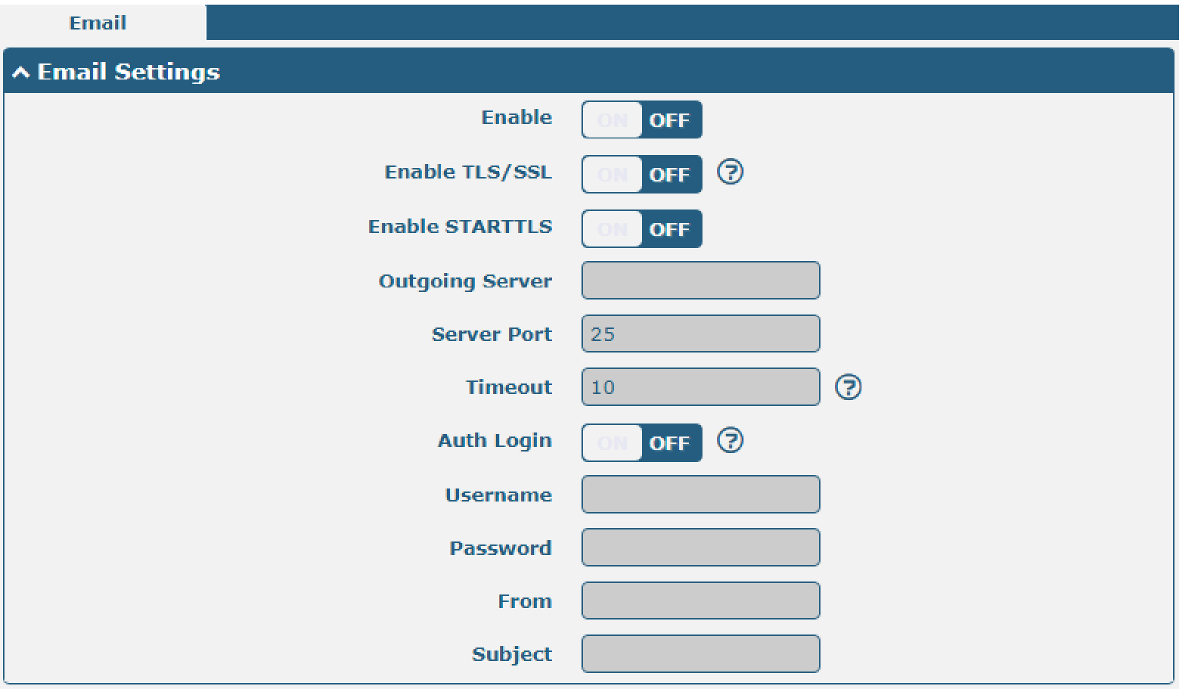
User can test the current SMS service whether it is available in this section.



SMS Testing		
Item	Description	Default
Phone Number	Enter the specified phone number which can receive the SMS from router.	Null
Message	Enter the message that router will send it to the specified phone number.	Null
Result	The result of the SMStest will be displayed in the result box.	Null
Send	Click the button to send the test message.	--

3.25 Services > Email

Email function supports to send the event notifications to the specified recipient by ways of email.



Email

Email Settings

Enable: ON OFF

Enable TLS/SSL: ON OFF

Enable STARTTLS: ON OFF

Outgoing Server:

Server Port: 25

Timeout: 10

Auth Login: ON OFF

Username:

Password:

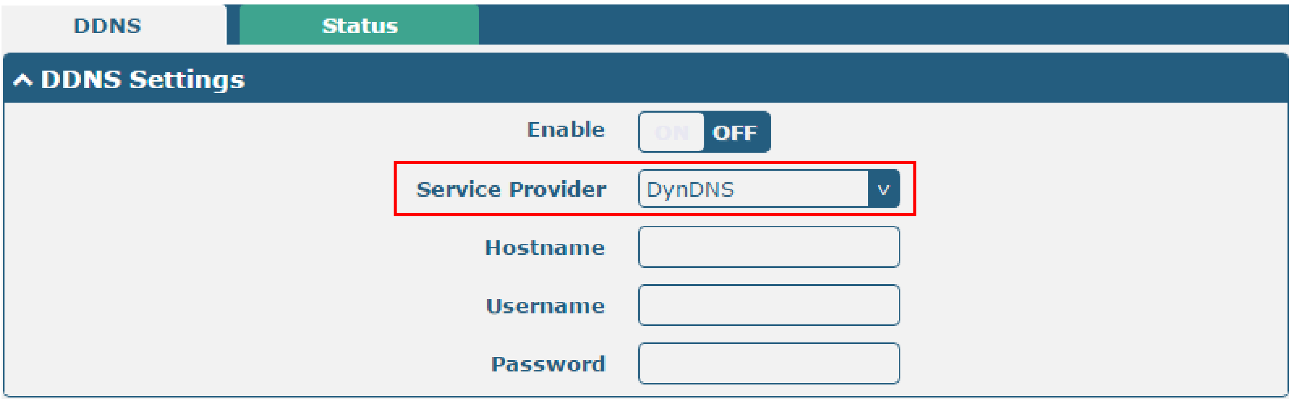
From:

Subject:

Email Settings		
Item	Description	Default
Enable	Click the toggle button to enable/ disable the Email option.	OFF
Enable TLS/ SSL	Click the toggle button to enable/ disable the TLS/ SSL option.	OFF
Enable STARTTLS	Click the toggle button to enable / disable STARTTLS encryption.	OFF
Outgoing server	Enter the SMTP server IP Address or domain name.	Null
Server port	Enter the SMTP server port.	25
Timeout	Set the max time for sending email to SMTP server. When the server doesn't receive the email over this time, it will try to resend.	10
Auth Login	If the mail server supports AUTH login, you must enable this button and set a username and password.	OFF
Username	Enter the username which has been registered from SMTP server.	Null
Password	Enter the password of the username above.	Null
From	Enter the source address of the email.	Null
Subject	Enter the subject of this email.	Null

3.26 Services > DDNS

This section allows you to set the DDNS parameters. The Dynamic DNS function allows you to alias a dynamic IP address to a static domain name, allows you whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP. The service provider defaults to " DynDNS", as shown below.



Enable ON OFF

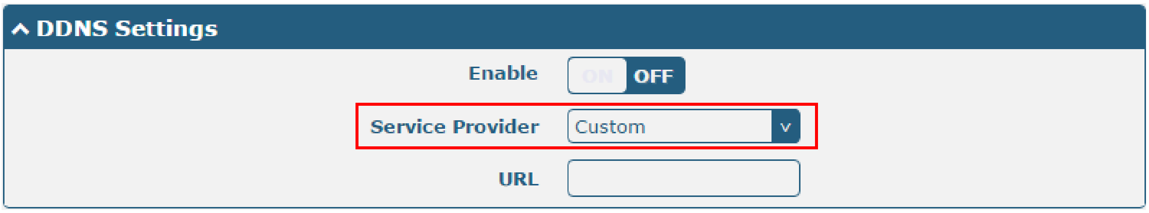
Service Provider DynDNS

Hostname

Username

Password

When "Custom" service provider chosen, the window is displayed as below.



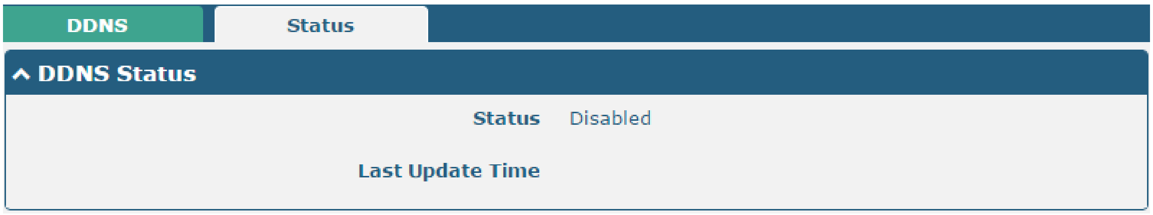
Enable ON OFF

Service Provider Custom

URL

DDNS Settings		
Item	Description	Default
Enable	Click the toggle button to enable/ disable the DDNS option.	OFF
Service Provider	Select the DDNS service from " DynDNS" , " NO-IP" or " 3322" Note: the DDNS service only can be used after registered by Corresponding service provider.	DynDNS
Hostname	Enter the hostname provided by the DDNS server.	Null
Username	Enter the username provided by the DDNS server.	Null
Password	Enter the password provided by the DDNS server.	Null
URL	Enter the URL customized by user.	Null

Click "Status"bar to view the status of the DDNS.



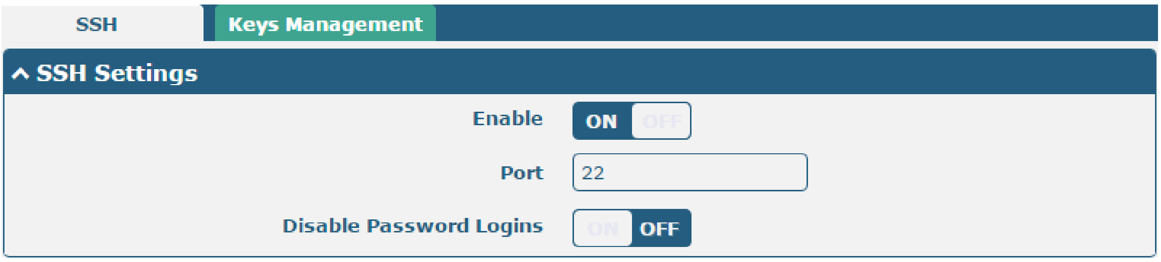
Status Disabled

Last Update Time

DDNS Status	
Item	Description
Status	Display the current status of the DDNS.
Last Update Time	Display the date and time for the DDNS was last updated successfully.

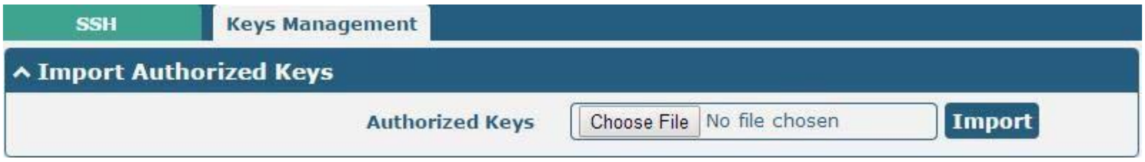
3.27 Services > SSH

DSR-211 Router supports SSH password access and secret -key access.



Enable: ON
Port: 22
Disable Password Logins: OFF

SSH Settings		
Item	Description	Default
Enable	Click the toggle button to enable/ disable this option. When enabled, you can access DSR-211 Router via SSH.	OFF
Port	Set the port of the SSH access.	22
Disable Password Logins	Click the toggle button to enable/ disable this option. When enabled, you cannot use username and password to access the router via SSH. In this case, only the key can be used for login.	OFF

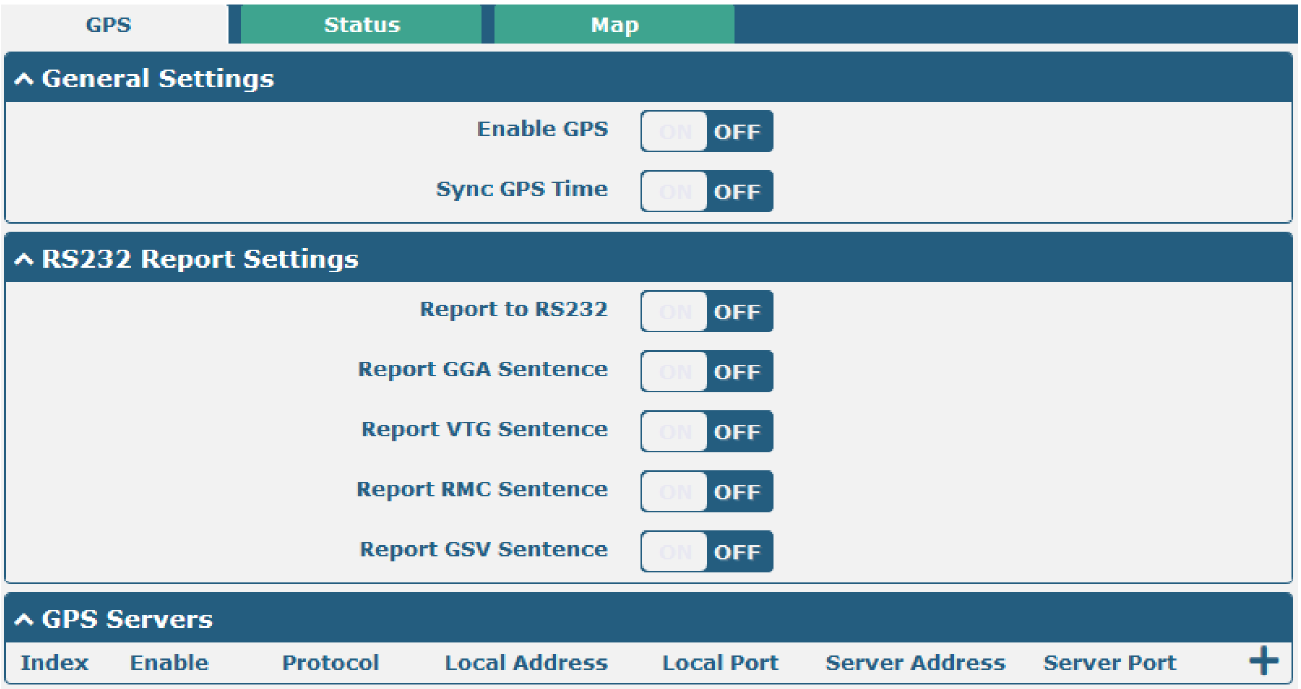


Authorized Keys: No file chosen

Keys Management	
Item	Description
Authorized Keys	Click on “Choose File” to locate an authorized key from your computer, and then click “Import” to import this key into your router. Note: This option is valid when enabling the password logins option.

3.28 Services > GPS

This section allows you to set the GPS setting parameters.



^ General Settings

Enable GPS: OFF

Sync GPS Time: OFF

^ RS232 Report Settings

Report to RS232: OFF

Report GGA Sentence: OFF

Report VTG Sentence: OFF

Report RMC Sentence: OFF

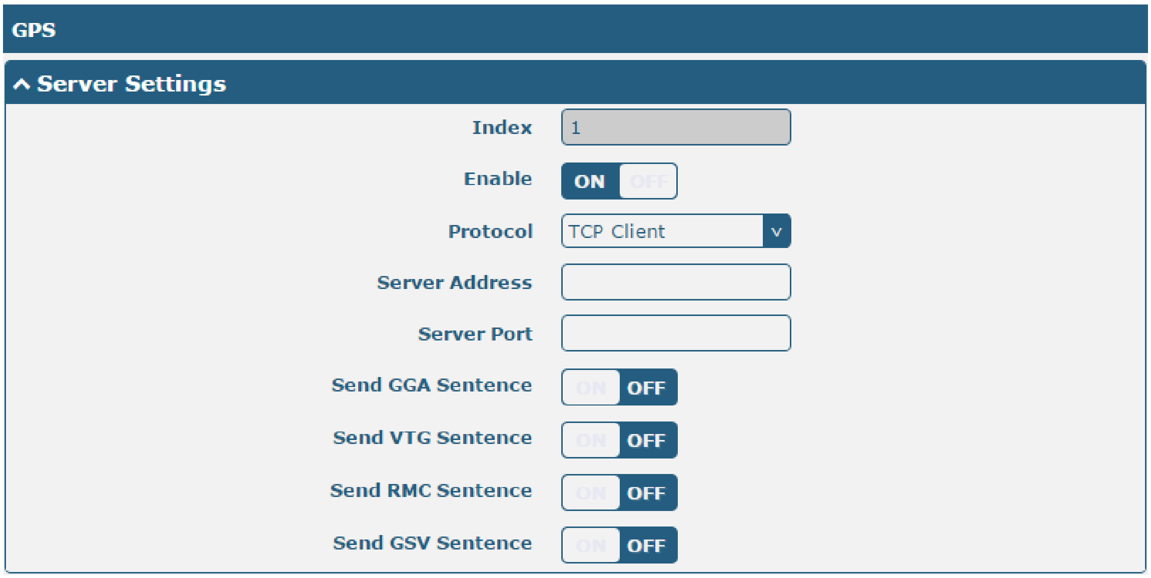
Report GSV Sentence: OFF

^ GPS Servers

Index	Enable	Protocol	Local Address	Local Port	Server Address	Server Port	+

General Settings @ GPS		
Item	Description	Default
Enable GPS	Click the toggle button to enable/ disable the GPS option.	OFF
Sync GPS Time	Click the toggle button to synchronize GPS time.	OFF
RS 232 Report Settings		
Report to RS232	Click the toggle button to report to RS232.	OFF
Report GGA Sentence	Click the toggle button to report GGA sentence.	OFF
Report VTG Sentence	Click the toggle button to report VTG sentence.	OFF
Report RMC Sentence	Click the toggle button to report RMC sentence.	OFF
Report GSV Sentence	Click the toggle button to report GSV sentence.	OFF

The window is displayed as below when choosing “TCP Client ” as the protocol.



GPS

Server Settings

Index: 1

Enable: ON

Protocol: TCP Client

Server Address:

Server Port:

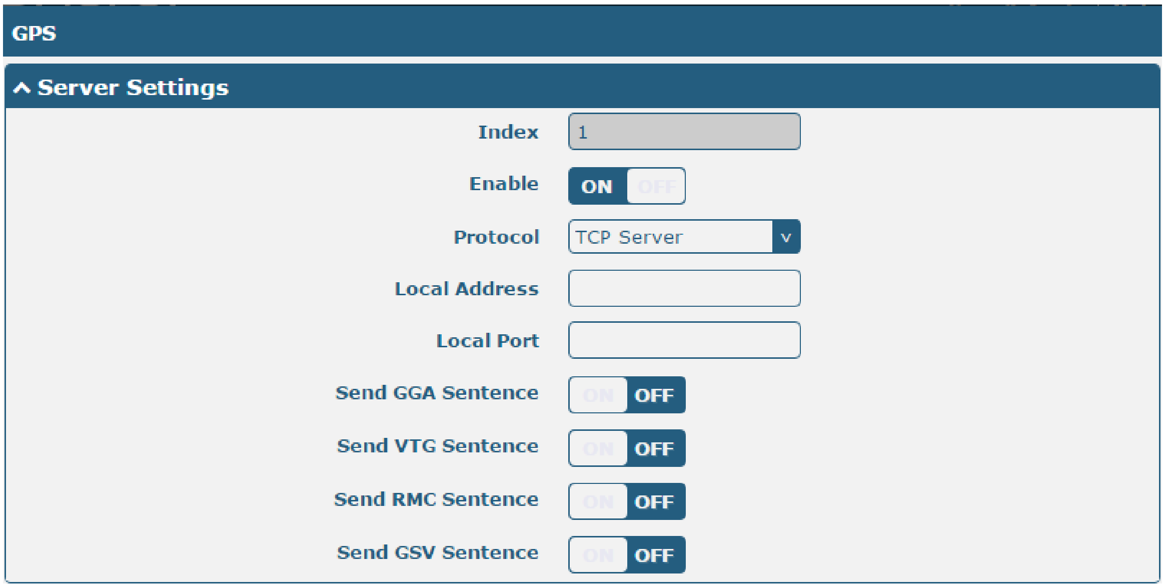
Send GGA Sentence: OFF

Send VTG Sentence: OFF

Send RMC Sentence: OFF

Send GSV Sentence: OFF

The window is displayed as below when choosing “TCP Server” as the protocol.



GPS

Server Settings

Index: 1

Enable: ON

Protocol: TCP Server

Local Address:

Local Port:

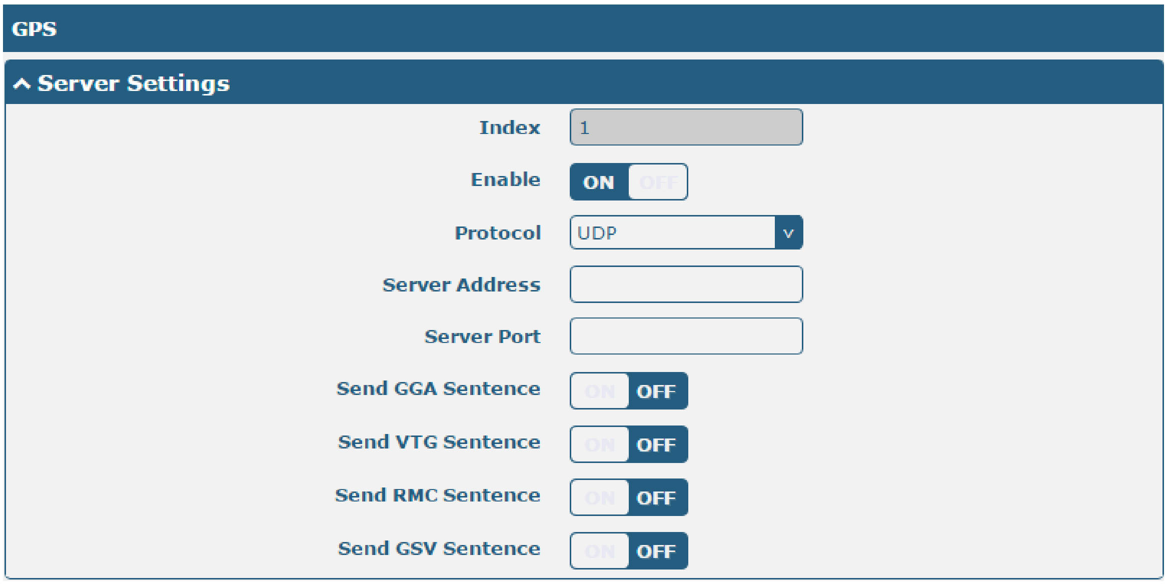
Send GGA Sentence: OFF

Send VTG Sentence: OFF

Send RMC Sentence: OFF

Send GSV Sentence: OFF

The window is displayed as below when choosing “UDP” as the protocol.



GPS

Server Settings

Index: 1

Enable: ON

Protocol: UDP

Server Address:

Server Port:

Send GGA Sentence: OFF

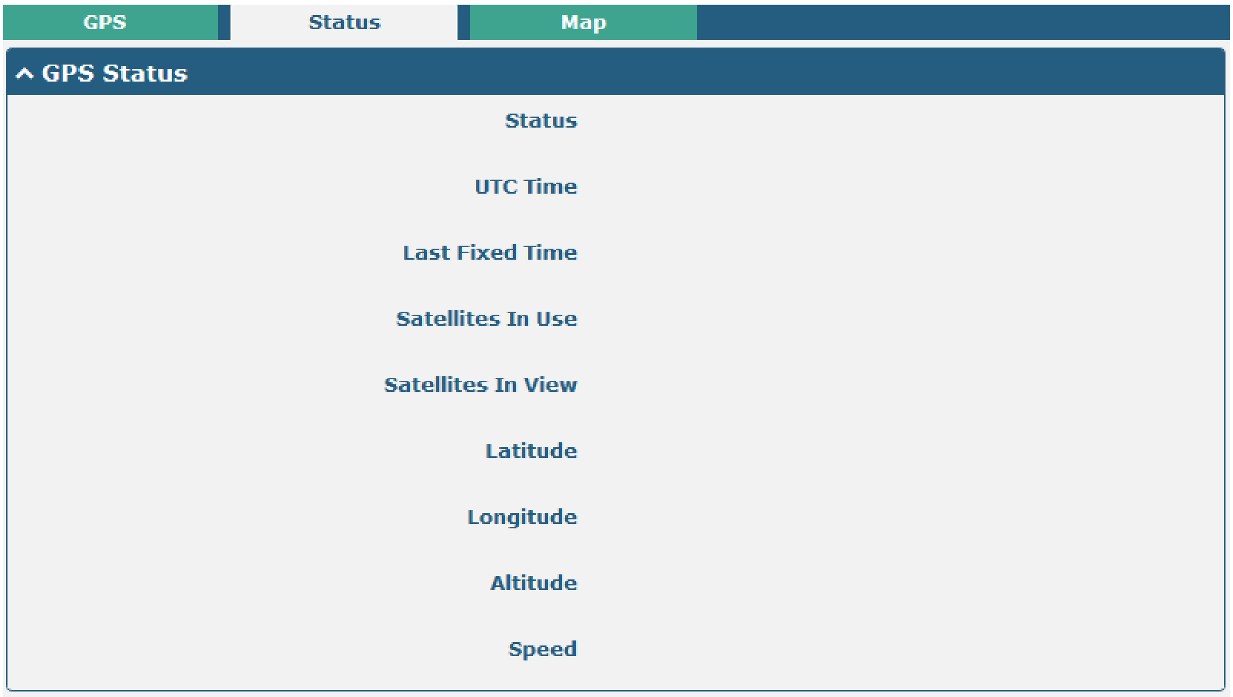
Send VTG Sentence: OFF

Send RMC Sentence: OFF

Send GSV Sentence: OFF

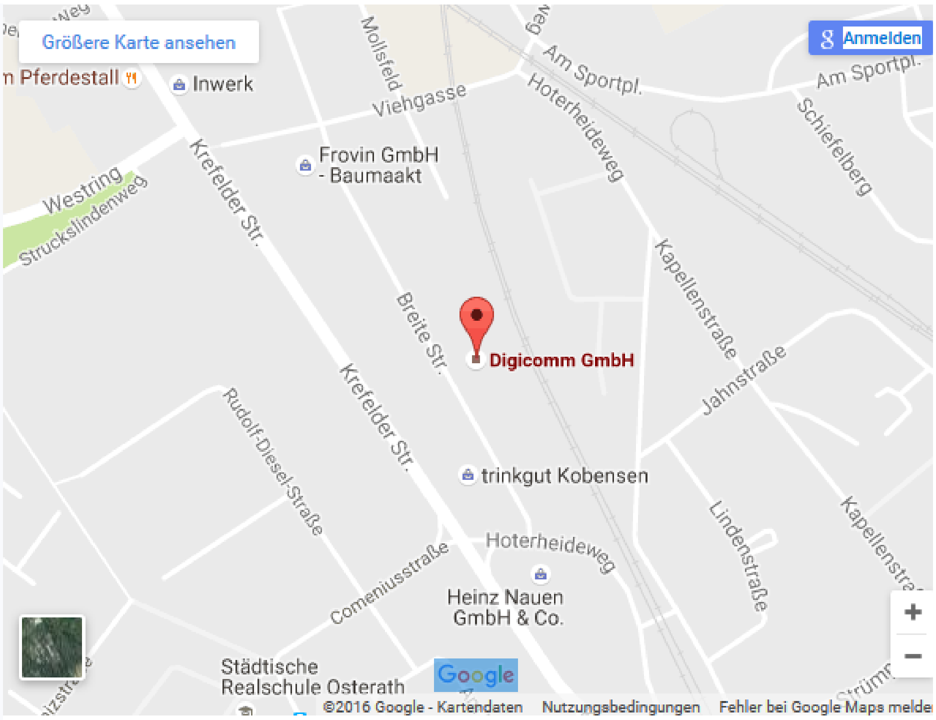
Server Settings		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/ disable the GPS server settings.	ON
Protocol	Select from " TCP Client" , " TCP Server" or " UDP" .	TCP Client
Server Address @TCP Client	Set the address of the TCP Client.	Null
Server Port @TCP Client	Set the port of the remote TCP Server.	Null
Local Address	Set the local address when the router set as a TCP Server.	Null
Local Port	Set the local port when the router set as a TCP Server.	Null
Server Address @ UDP	Set the address of the TCPServer.	Null
Server Port @ UDP	Set the port of the remote TCP Server.	Null
Send GGA Sentence	Send GGA information in NMEA format.	OFF
Send VTG Sentence	Send VTG information in NMEA format.	OFF
Send RMCSentence	Send RMC information in NMEA format.	OFF
Send GSV Sentence	Send GSV information in NMEA format.	OFF

Click the Status column to view the status of the GPS.



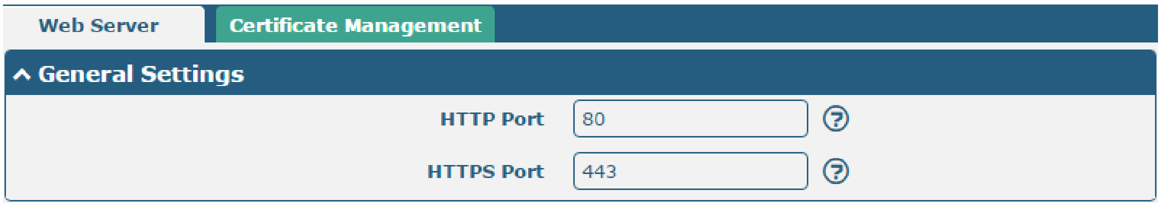
GPS Status	
Item	Description
Status	Show the GPS Status. GPS status includes: “ NO Fix” , “ 2D Fix” and “ 3D Fix” .
UTC Time	Show the UTC of satellites, which is world unified time, not local time.
Last Fixed Time	Show the last positioning time.
Satellites In Use	Show the satellite quantity in use.
Satellite In View	Show the satellite quantity in view.
Latitude	Show the latitude status of router.
Longitude	Show the longitude status of router.
Altitude	Show the altitude status of router.
Speed	Show the horizontal speed of router.

Click the Map column to view the current location of the router.



3.29 Services > Web Server

This section allows you to modify the parameters of Web Server.

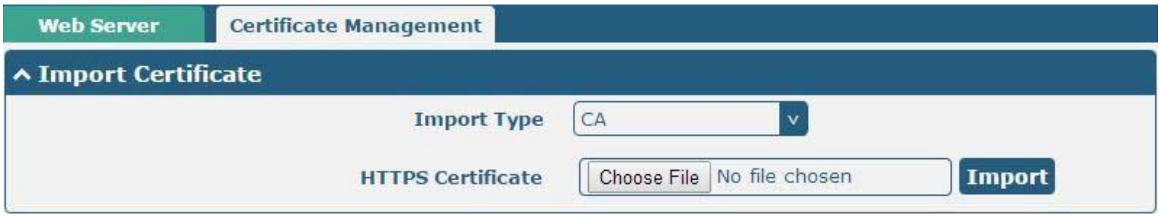


HTTP Port 80

HTTPS Port 443

Basic @ Web Server		
Item	Description	Default
HTTP Port	Enter the HTTP port number you want to change in router's Web Server. On a Web server, port 80 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTP Port number except 80, only adding that port number then you can login router's Web Server.	80
HTTPS Port	Enter the HTTPS port number you want to change in router's Web Server. On a Web server, port 443 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTPS Port number except 443, only adding that port number then you can login DSR-211's Web Server. Note: HTTPS is more secure than HTTP. In many cases, clients may be exchanging confidential information with a server, which needs to be secured in order to prevent unauthorized access. For this reason, HTTP was developed by Netscape corporation to allow authorization and secured transactions.	443

This section allows you to import the certificate file into the route.



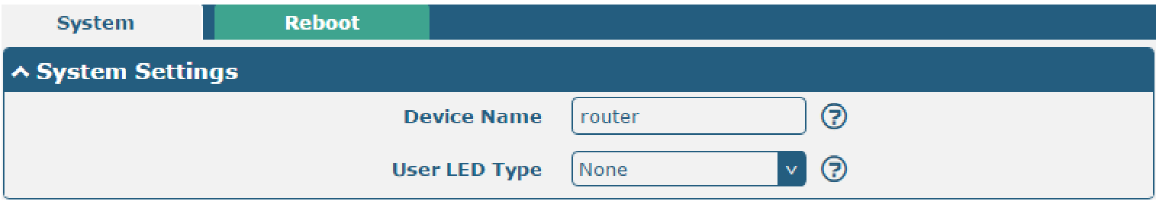
Import Type: CA

HTTPS Certificate: Choose File No file chosen

Certificate Management		
Item	Description	Default
Import Type	Select from "CA" and "Private Key" . CA: a digital certificate issued by CA center Private Key: a private key file	CA
HTTPS Certificate	Click on "Choose File" to locate the certificate file from your computer, and then click " Import" to import this file into your router.	--

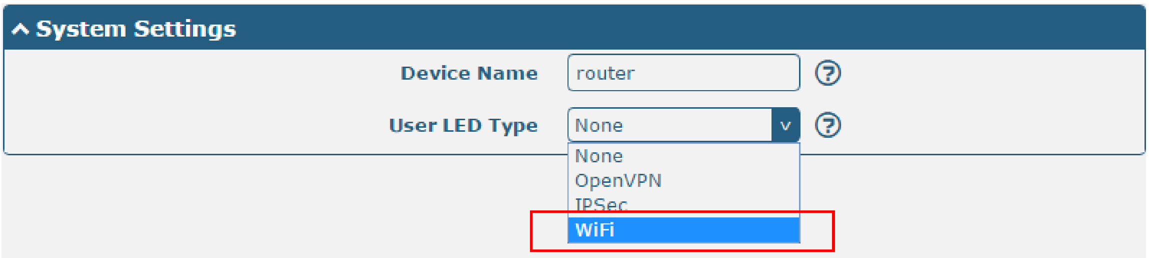
3.30 Services > Advanced

This section allows you to set the Advanced and parameters.



Device Name: router

User LED Type: None

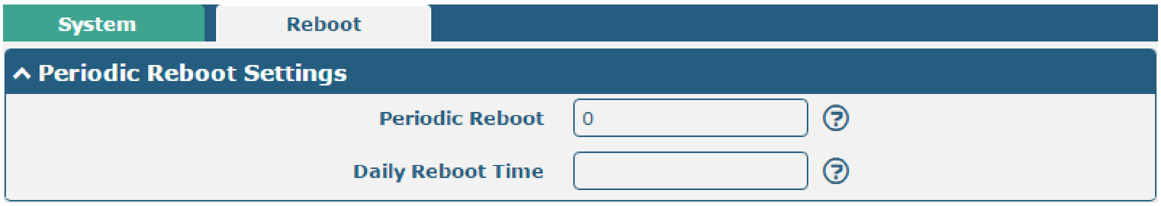


System Settings

Device Name: router

User LED Type: None

System Settings		
Item	Description	Default
Device Name	Set the device name to distinguish different devices you have installed; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and * .	router
User LED Type	Specify the display type of your USR LED. Select from " None", " OpenVPN" , " IPsec" or "WiFi". • None: Meaningless indication, and the LED is off • OpenVPN: USR indicator showing the OpenVPN status • IPsec: USR indicator showing the IPsec status • WiFi: USR indicator showing the WiFi status Note: For more details about USR indicator, see "2.2 LED Indicators".	None



Periodic Reboot Settings

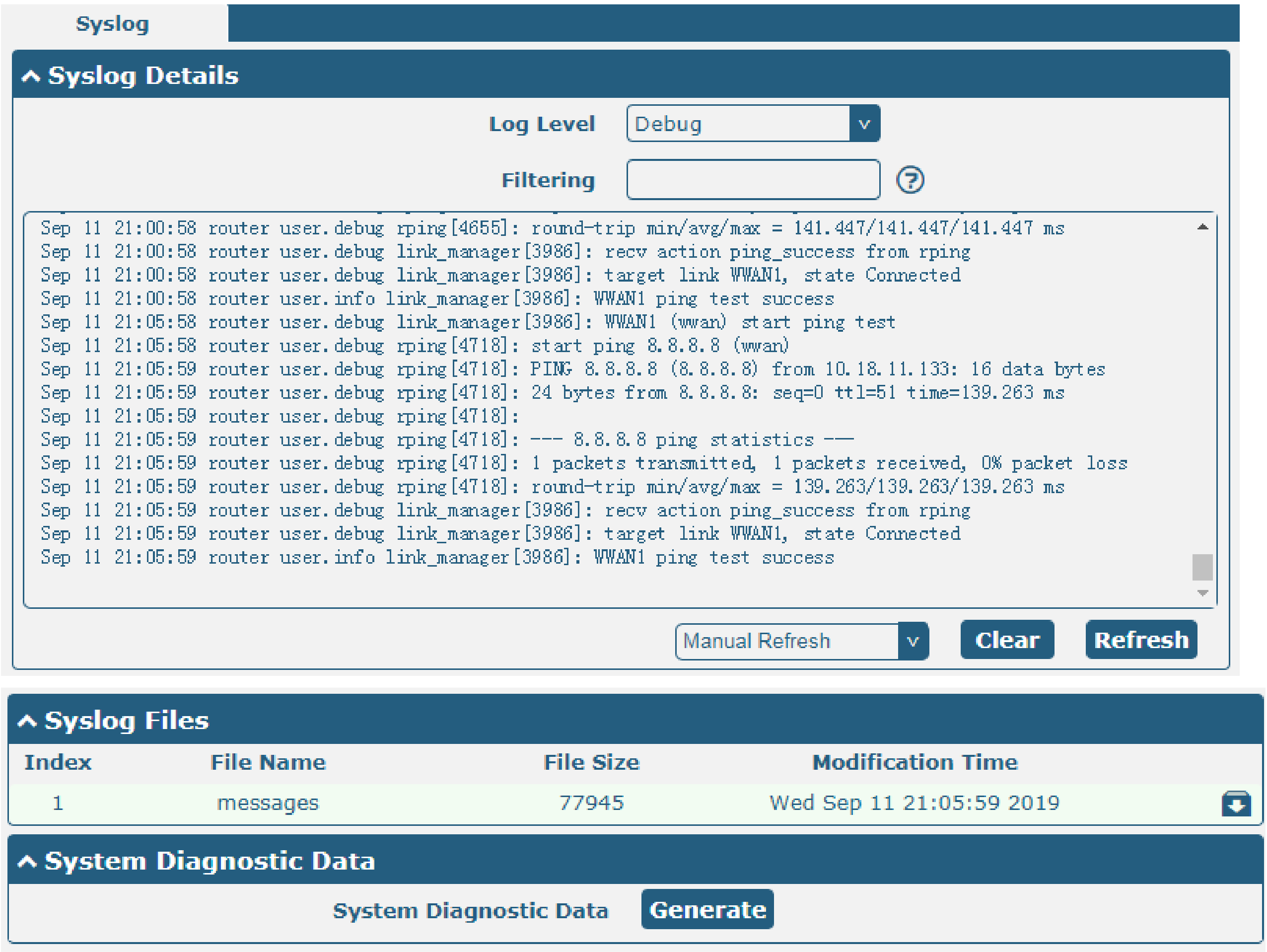
Periodic Reboot: 0

Daily Reboot Time:

Reboot		
Item	Description	Default
Periodic Reboot	Set the reboot period of the router. 0 means disable.	0
Daily Reboot Time	Set the daily reboot time of the router, you should follow the format as HH: MM, in 24h time frame, otherwise the data will be invalid. Leave it empty means disable.	Null

3.31 System > Debug

This section allows you to check and download the syslog details.



Log Level: Debug

Filtering:

```
Sep 11 21:00:58 router user.debug rping[4655]: round-trip min/avg/max = 141.447/141.447/141.447 ms
Sep 11 21:00:58 router user.debug link_manager[3986]: recv action ping_success from rping
Sep 11 21:00:58 router user.debug link_manager[3986]: target link WWAN1, state Connected
Sep 11 21:00:58 router user.info link_manager[3986]: WWAN1 ping test success
Sep 11 21:05:58 router user.debug link_manager[3986]: WWAN1 (wwan) start ping test
Sep 11 21:05:58 router user.debug rping[4718]: start ping 8.8.8.8 (wwan)
Sep 11 21:05:59 router user.debug rping[4718]: PING 8.8.8.8 (8.8.8.8) from 10.18.11.133: 16 data bytes
Sep 11 21:05:59 router user.debug rping[4718]: 24 bytes from 8.8.8.8: seq=0 ttl=51 time=139.263 ms
Sep 11 21:05:59 router user.debug rping[4718]:
Sep 11 21:05:59 router user.debug rping[4718]: --- 8.8.8.8 ping statistics ---
Sep 11 21:05:59 router user.debug rping[4718]: 1 packets transmitted, 1 packets received, 0% packet loss
Sep 11 21:05:59 router user.debug rping[4718]: round-trip min/avg/max = 139.263/139.263/139.263 ms
Sep 11 21:05:59 router user.debug link_manager[3986]: recv action ping_success from rping
Sep 11 21:05:59 router user.debug link_manager[3986]: target link WWAN1, state Connected
Sep 11 21:05:59 router user.info link_manager[3986]: WWAN1 ping test success
```

Index	File Name	File Size	Modification Time
1	messages	77945	Wed Sep 11 21:05:59 2019

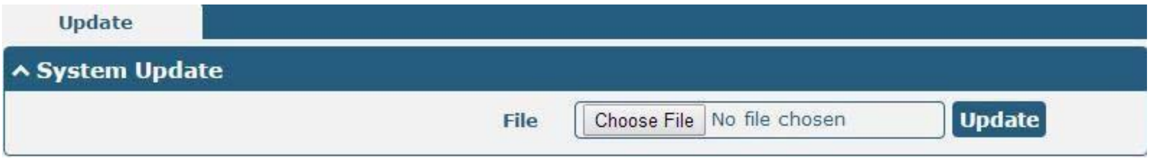
System Diagnostic Data: Generate

Syslog		
Item	Description	Default
Syslog Details		
Log Level	Select from " Debug", " Info", " Notice" , " Warn", " Error" which from low to high. The lower level will output more syslog in detail.	Debug
Filtering	Enter the filtering message based on the keywords. Use " &" to separate more than one filter message, such as "keyword1&keyword2".	Null
Refresh	Select from " Manual Refresh" , " 5 Seconds" , " 10 Seconds" , " 20 Seconds" or " 30 Seconds". You can select these intervals to refresh the log information displayed in the follow box. If selecting "manual refresh", you should click the refresh button to refresh the syslog.	Manual Refresh
Clear	Click the button to clear the syslog.	--
Refresh	Click the button to refresh the syslog.	--
Syslog Files		
Syslog Files List	It can show at most 5 syslog files in the list, the files' name range from message 0 to message 4. And the newest syslog file will be placed on the top of the list.	/
System Diagnoging Data		
Generate	Click to generate the syslog diagnosing file.	/
Download	Click to download the generated system diagnostic data.	/

3.32 System > Update

This section allows you to upgrade the firmware of your DSR-211. Click System > Update > System Update, and click on “Choose File” to locate the firmware file to be used for the upgrade. Once the latest firmware has been chosen, click Update to start the upgrade process. The upgrade process may take several minutes. Do not turn off your Router during the firmware upgrade process.

Note: To access the latest firmware file, please contact your technical support engineer



Update		
Item	Description	Default
System Update	Click Choose File button to select the correct firmware in your PC, and then click Update button to update. After updating successfully, you need to click “ save and apply” , and then reboot the router to take effect.	Null

3.33 System> App Center

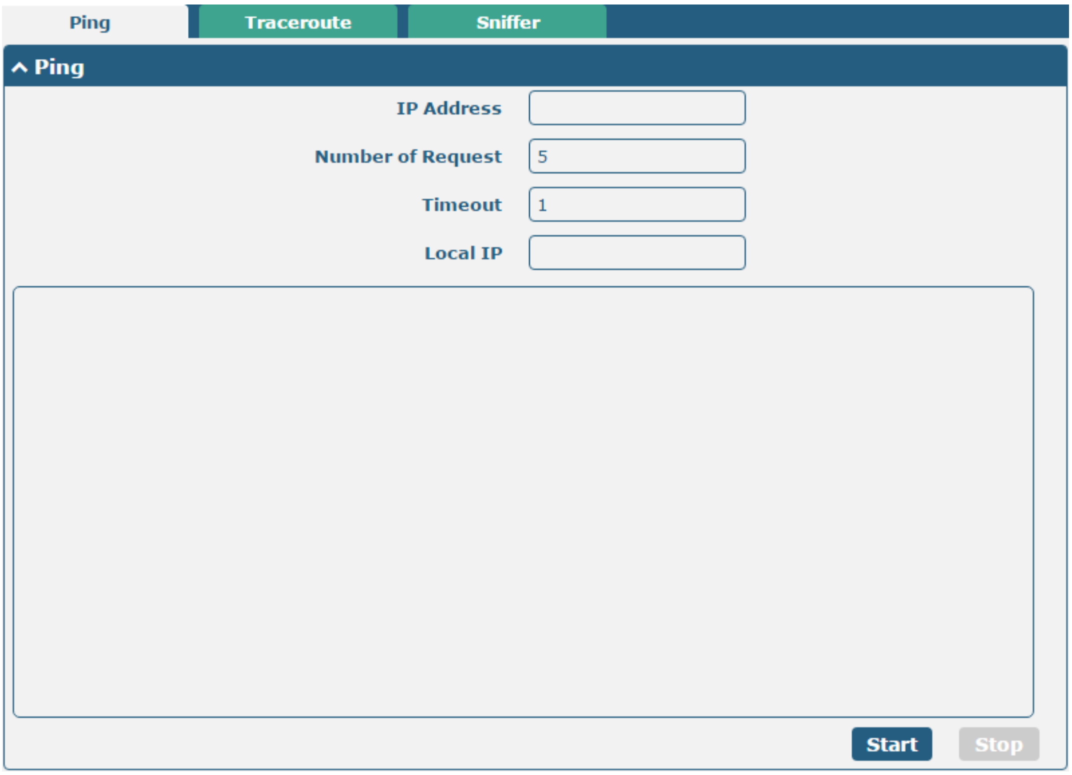
This section allows you to add some required or customized applications to the router. Import and install your applications to the APP Center, and reboot the device according to the system prompts. Each installed application will be displayed under the “Services” menu, while other applications related to VPN will be displayed under the “ VPN” menu.

Note: After importing the applications to the router, the page display may have a slight delay due to the browser cache. It is recommended that you clear the browser cache first and log in the router again.

App Center		
Item	Description	Default
App Install		
File	Click on “ Choose File” to locate the App file from your computer, and then click Install to import this file into your router. Note: File format should be xxx.rpk, e.g. DSR-211-Digilink-1.0.0.rpk.	--
Installed Apps		
Index	Indicate the ordinal of the list.	--
Name	Show the name of the App.	Null
Version	Show the version of the App.	Null
Status	Show the status of the App.	Null
Description	Show the description for this App.	Null

3.34 System > Tools

This section provides users three tools: Ping, Traceroute and Sniffer.



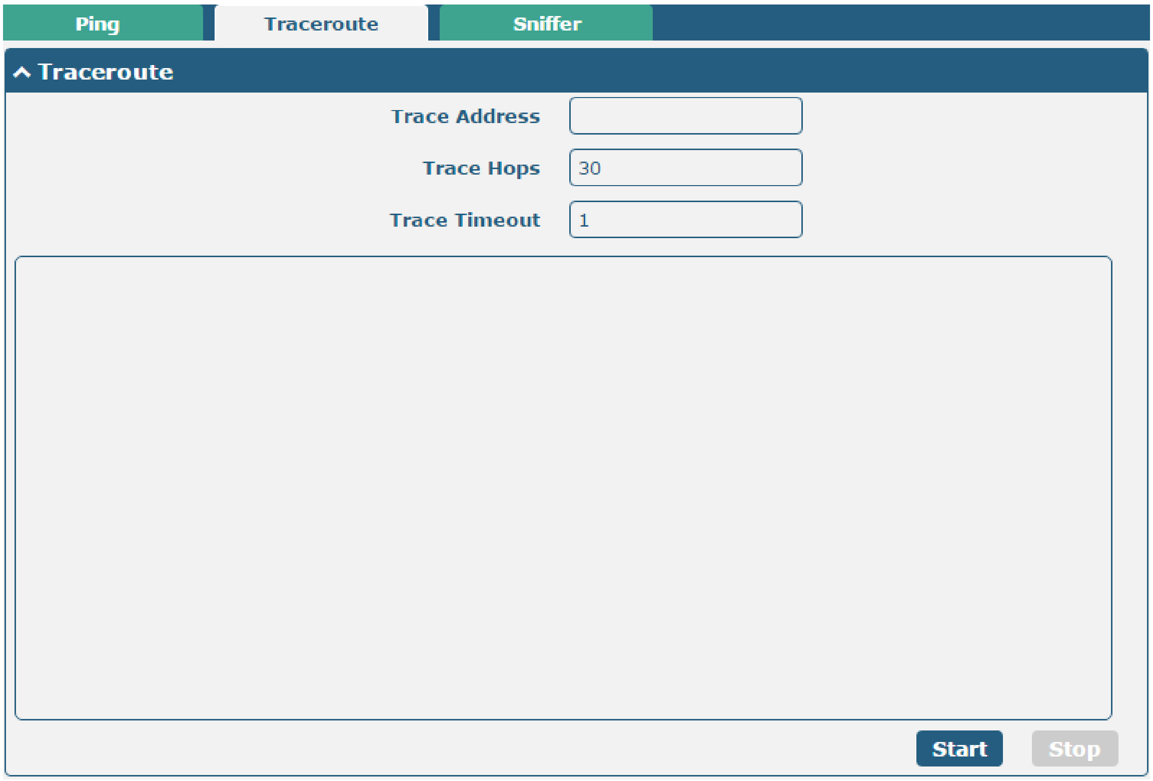
IP Address

Number of Request: 5

Timeout: 1

Local IP

Ping		
Item	Description	Default
IP address	Enter the ping's destination IP address or destination domain.	Null
Number of Requests	Specify the number of ping requests.	5
Timeout	Specify the timeout of ping request.	1
Local IP	Specify the local IP from cellular WAN, Ethernet WAN or Ethernet LAN. Null stands for selecting local IP address from these three automatically.	Null
Start	Click this button to start ping request, and the log will be displayed in the follow box.	Null
Stop	Click this button to stop ping request.	--

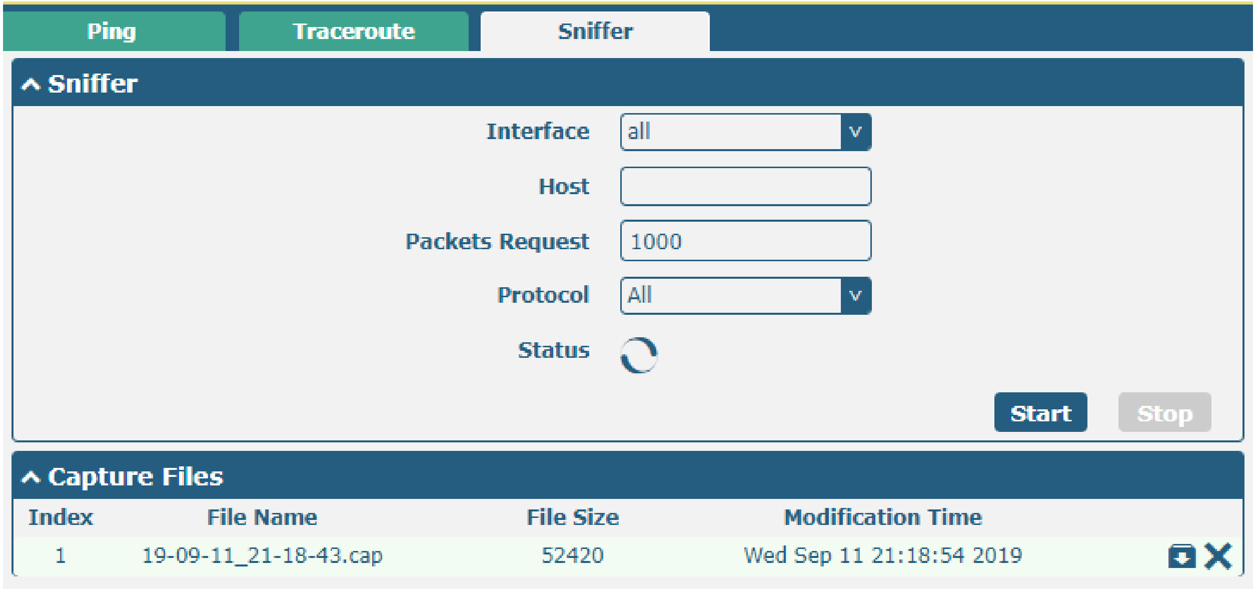


Trace Address:

Trace Hops: 30

Trace Timeout: 1

Traceroute		
Item	Description	Default
Trace Address	Enter the trace's destination IP address or destination domain.	Null
Trace Hops	Specify the max trace hops. Router will stop tracing if the trace hops has met max value no matter the destination has been reached or not.	30
Trace Timeout	Specify the timeout of Traceroute request.	1
Start	Click this button to start Traceroute request , and the log will be displayed in the follow box.	--
Stop	Click this button to stop Traceroute request.	--



Interface: all

Host:

Packets Request: 1000

Protocol: All

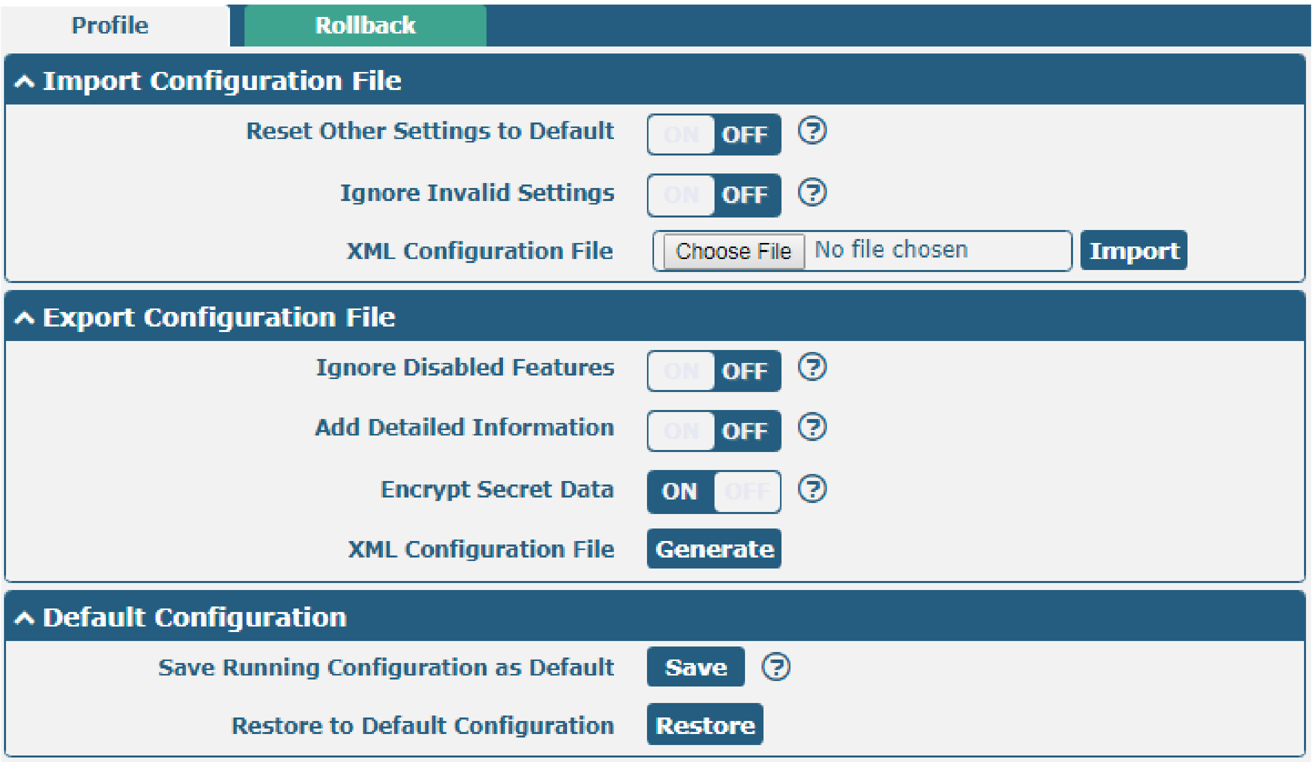
Status

Index	File Name	File Size	Modification Time
1	19-09-11_21-18-43.cap	52420	Wed Sep 11 21:18:54 2019

Sniffer		
Item	Description	Default
Interface	Choose the interface according to your Ethernet configuration.	All
Host	Filter the packet that contain the specify IP address.	Null
Packets Request	Set the packet number that the router can sniffer at a time.	1000
Protocol	Select from “ All” , “ IP” , “ TCP” , “ UDP” and “ ARP” .	All
Port	Set the port number for TCPor UDP that is used in sniffer.	Null
Status	Show the current status of sniffer.	Null
Start	Click this button to start the sniffer.	--
Stop	Click this button to stop the sniffer. Once you click this button, a new log file will be displayed in the following List.	--
Capture Files	Every times of sniffer log will be saved automatically as a new file. You can find the file from this Sniffer Traffic Data List and click ⬇to download the log, click to delete the lo✕file. It can cache a maximum of 5 files.	Null

3.35 System > Profile

This section allows you to import or export the configuration file, and restore the router to factory default setting.



Profile | Rollback

^ Import Configuration File

Reset Other Settings to Default: ON **OFF** ?

Ignore Invalid Settings: ON **OFF** ?

XML Configuration File: Choose File No file chosen Import

^ Export Configuration File

Ignore Disabled Features: ON **OFF** ?

Add Detailed Information: ON **OFF** ?

Encrypt Secret Data: **ON** OFF ?

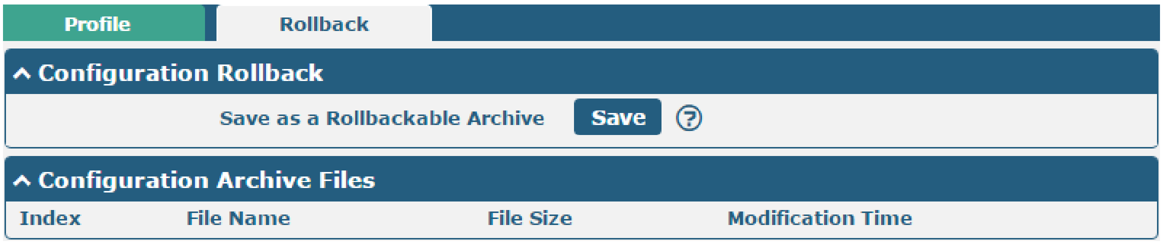
XML Configuration File: Generate

^ Default Configuration

Save Running Configuration as Default: Save ?

Restore to Default Configuration: Restore

Profile		
Item	Description	Default
Import Configuration File		
Reset Other Settings to Default	Click the toggle button as " ON" to return other parameters to default settings.	OFF
Ignore Invalid Settings	Click the toggle button as " OFF" to ignore invalid settings.	OFF
XML Configuration File	Click on Choose File to locate the XML configuration file from your computer, and then click Import to import this file into your router.	--
Export Configuration File		
Ignore Disabled Features	Click the toggle button as " OFF" to ignore the disabled features.	OFF
Add Detailed Information	Click the toggle button as " On" to add detailed information.	OFF
Encrypt Secret Data	Click the toggle button as " ON" to encrypt the secret data.	OFF
XML Configuration File	Click Generate button to generate the XML configuration file.	--
Default Configuration		
Save Running Configuration as Default	Click Save to save the current running parameters as default configuration.	--
Restore to Default Configuration	Click Restore button to restore the factory defaults.	--

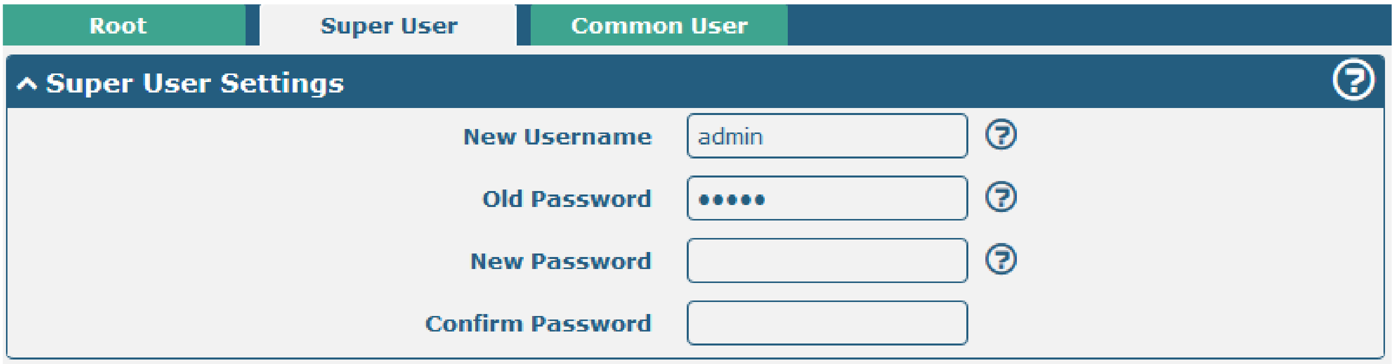


Index | File Name | File Size | Modification Time

Rollback		
Item	Description	Default
Configuration Rollback		
Save as a Rollbackable Archive	Create a save point manually. Additionally, the system will create a save point every day automatically if configuration changes.	--
Configuration Archive Files		
Configuration Archive Files	View the related information about configuration archive files, including name, size and modification time.	--

3.36 System > User Management

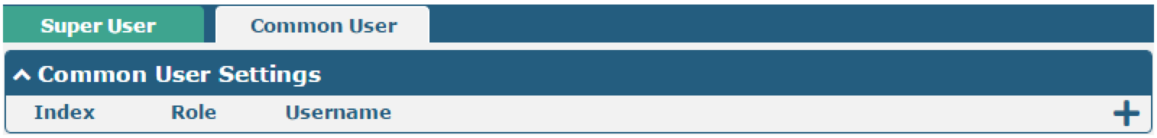
One router has only one super user who has the highest authority to modify, add and manage other common users.



Super User Settings

New Username	admin
Old Password	•••••
New Password	
Confirm Password	

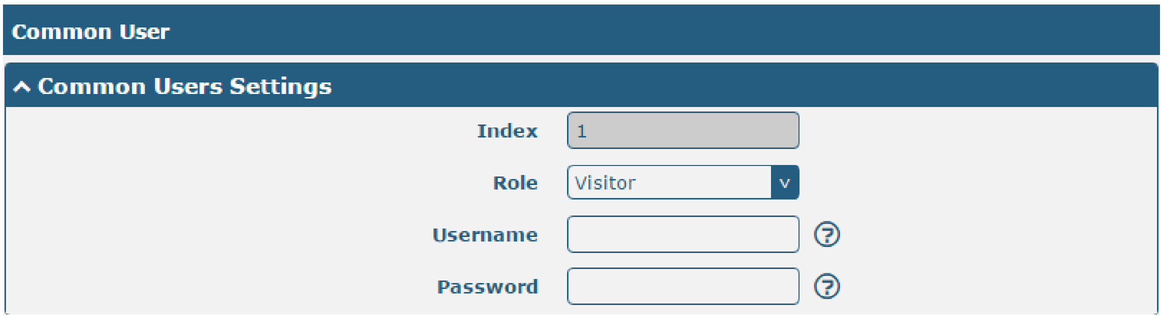
Super User Settings		
Item	Description	Default
New Username	Enter a new username you want to create; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and * .	Null
Old Password	Enter the old password of your router. The default is " admin" .	Null
New Password	Enter a new password you want to create; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and * .	Null
Confirm Password	Enter the new password again to confirm.	Null



Common User Settings

Index	Role	Username

Click + button to add a new common user. The maximum rule count is 5.



Common User

Common Users Settings

Index	1
Role	Visitor
Username	
Password	

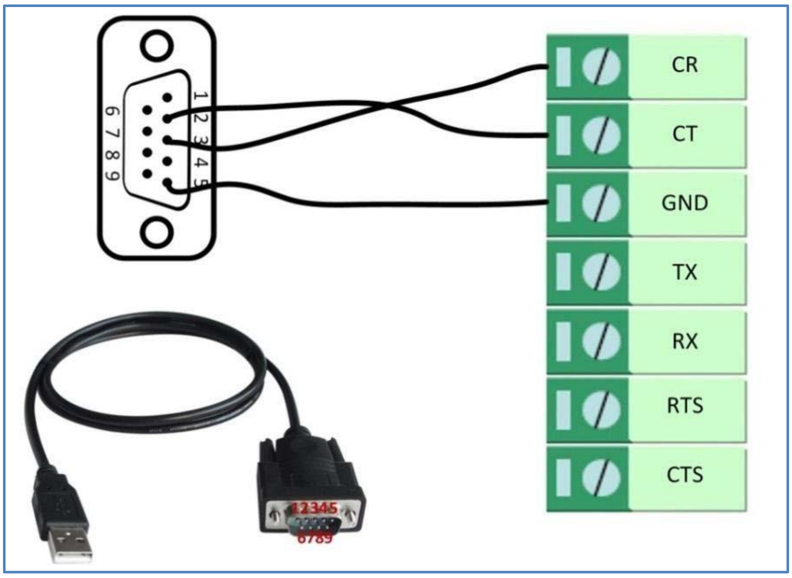
Common User Settings		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Role	Select from " Visitor" and " Editor" . Visitor: Users only can view the configuration of router under this level Editor: Users can view and set the configuration of router under this level	Visitor
Username	Set the Username; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and * .	Null
Password	Set the password which at least contains 5 characters; valid characters are a-z, A-Z,0-9, @, ., -, #, $, and * .	Null

4. Configuration Examples

4.1 Interface

4.1.1 Console Port

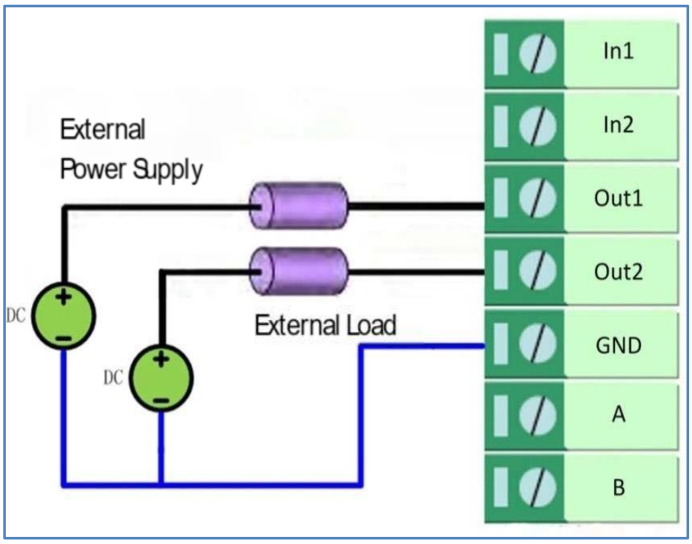
You can use the console port to manage the Router via CLI commands, please refer to Chapter 5 Introductions for CLI.



4.1.2 Digital Input

DSR-211 supports digital input with dry contact. Please check the connector interface of the Router, you can easily find a mark “V”- at one pin of the power connector.
Note: Do not connect In1/In2 directly and do not slide the switch to the port marked “GND” on the Terminal block. Otherwise, the DI cannot work properly.

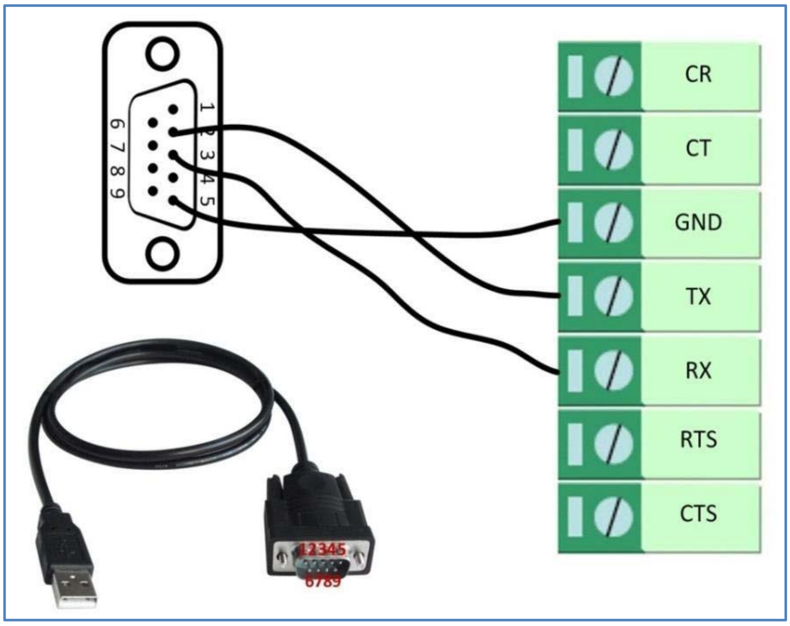
4.1.3 Digital Output



DSR-211 supports digital output with wet contact. Please refer to the right side figure to connect the negative pole of the power to the port marked “GND”. The maximum output voltage, output current and output power of DO is 30V DC, 0,3 A and 0,3 W respectively. It means that the voltage difference between Out1, Out2 and GND cannot exceed to 30 V DC, and the current value through Out 1 and Out 2 cannot exceed to 300 mA while the output power dissipated by Out 1 and Out 2 cannot exceed to 0,3 W. Otherwise, the DO will be damaged.

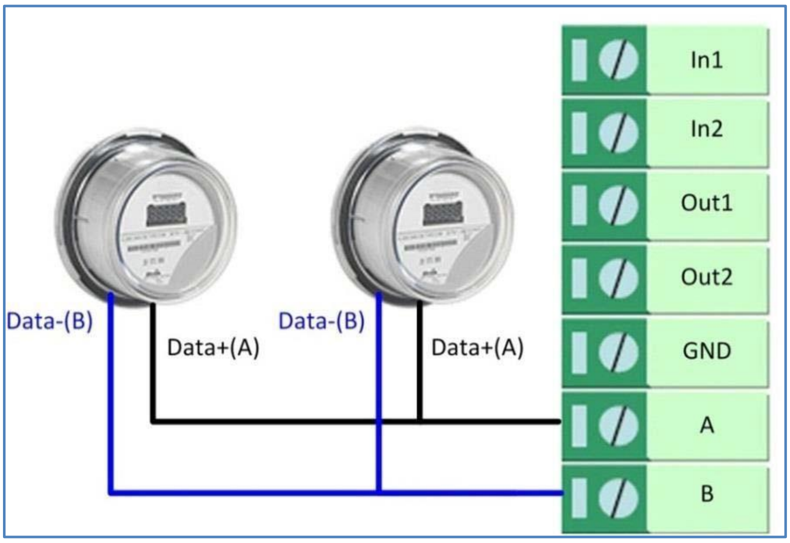
4.1.4 RS-232

DSR-211 support one RS-232 for serial data communication. Please refer to the connection diagram at the right side.



4.1.5 RS-485

DSR-211 supports one RS-485 for serial data communication. Please refer to the connection diagram at the right side.

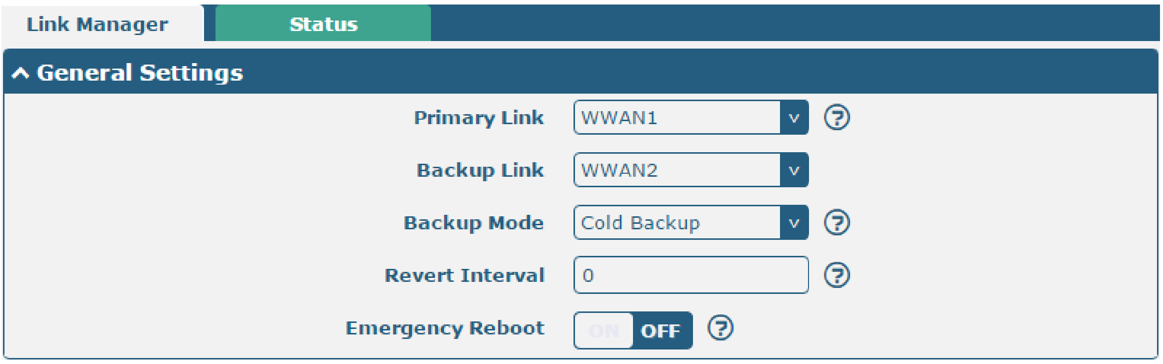


4.2 Cellular

4.2.1 Cellular Dial-Up

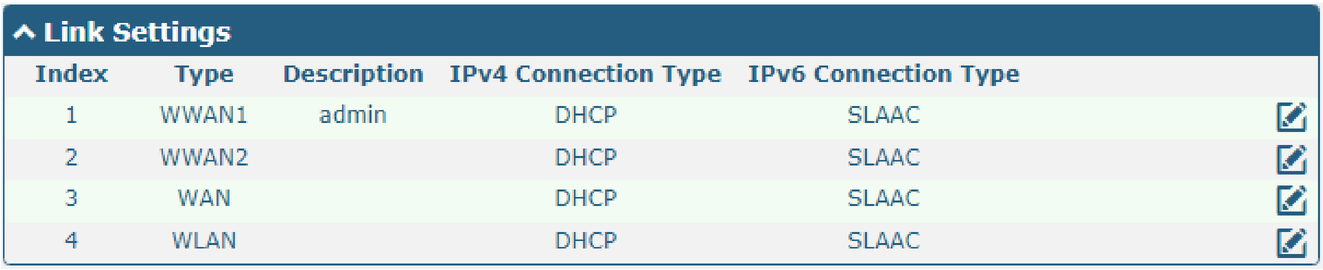
This section shows you how to configure the primary and backup SIM card for Cellular Dial-up. Connect the router correctly and insert two SIM, then open the configuration page. Under the homepage menu, click Interface > Link Manager > General Settings, choose “ WWAN1” as the primary link, “ WWAN2” as the backup link and “ Cold Backup” as the backup mode as the backup mode, then click Submit

Note: All data will be transferred via WWAN1 when choose WWAN1 as the primary link and set backup mode as cold backup. At the same time, WWAN2 is always offline as a backup link. All data transmission will be switched to WWAN2 when the WWAN1 is disconnected.



General Settings

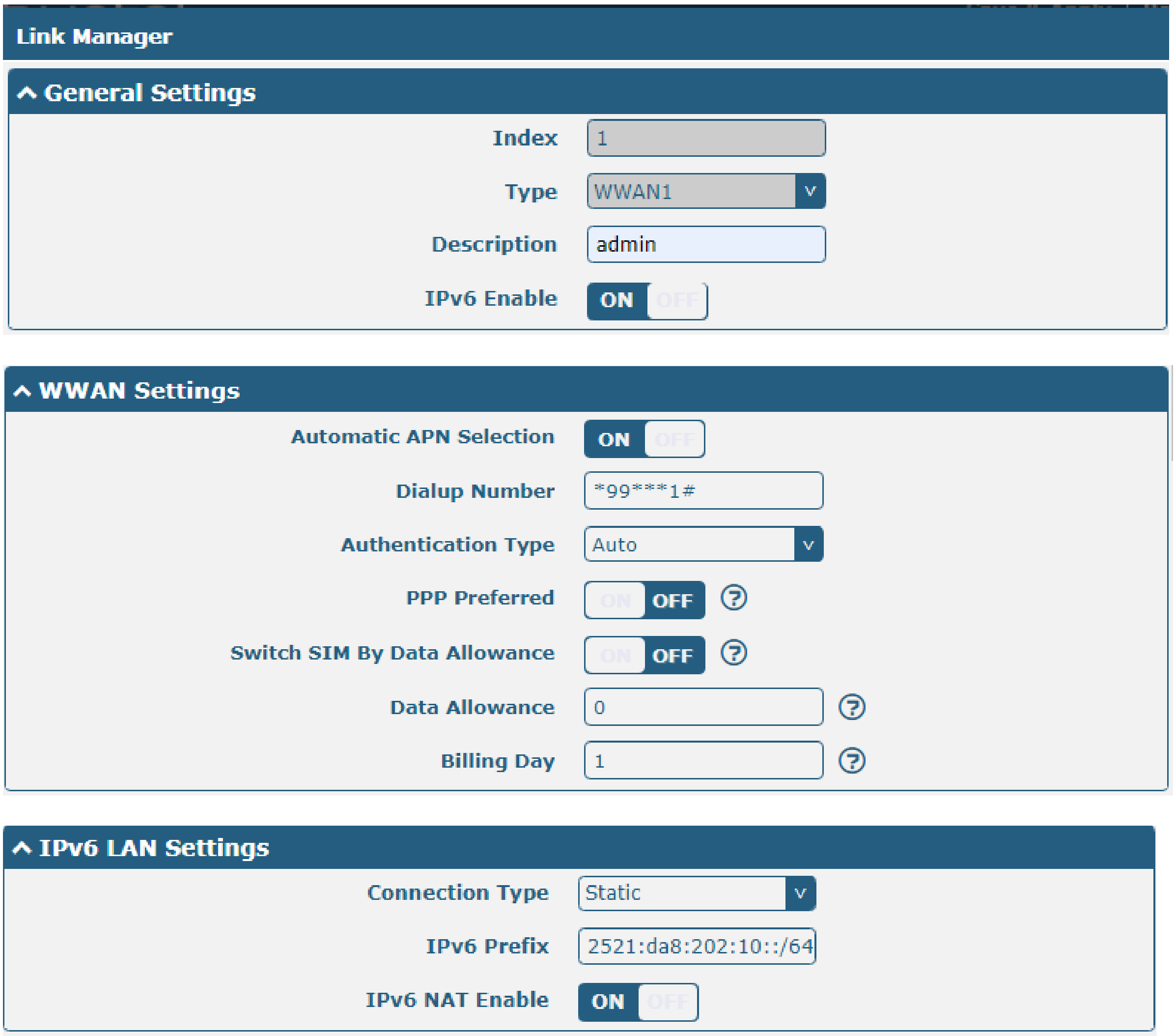
Primary Link	WWAN1
Backup Link	WWAN2
Backup Mode	Cold Backup
Revert Interval	0
Emergency Reboot	ON OFF



^ Link Settings

Index	Type	Description	IPv4 Connection Type	IPv6 Connection Type	
1	WWAN1	admin	DHCP	SLAAC	✎
2	WWAN2		DHCP	SLAAC	✎
3	WAN		DHCP	SLAAC	✎
4	WLAN		DHCP	SLAAC	✎

Click the ✎ button of WWAN1 to set its parameters according to the current ISP.



Link Manager

^ General Settings

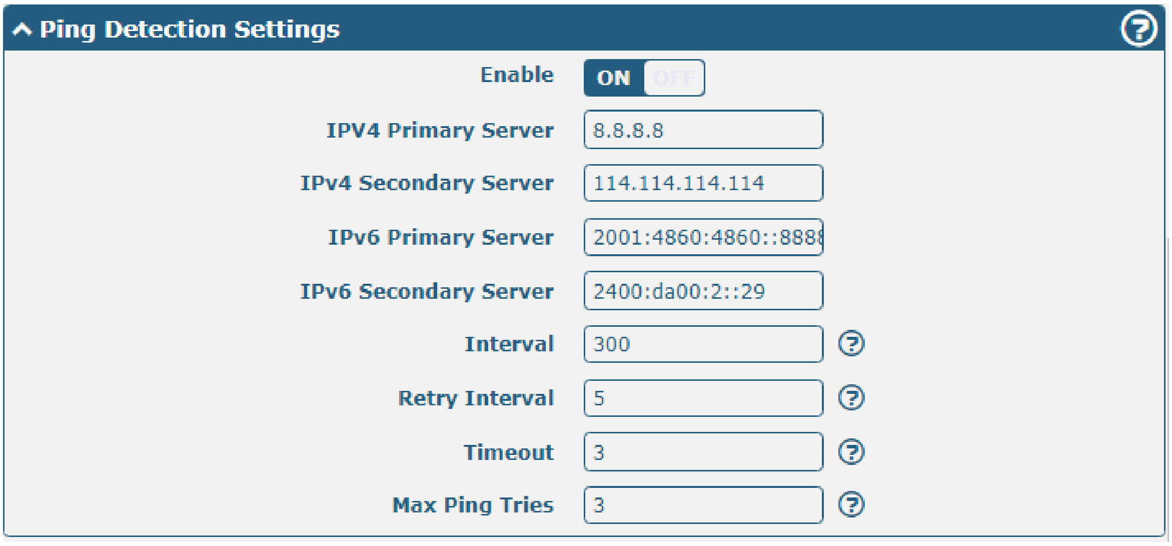
Index	1
Type	WWAN1
Description	admin
IPv6 Enable	ON

^ WWAN Settings

Automatic APN Selection	ON
Dialup Number	*99***1#
Authentication Type	Auto
PPP Preferred	OFF
Switch SIM By Data Allowance	OFF
Data Allowance	0
Billing Day	1

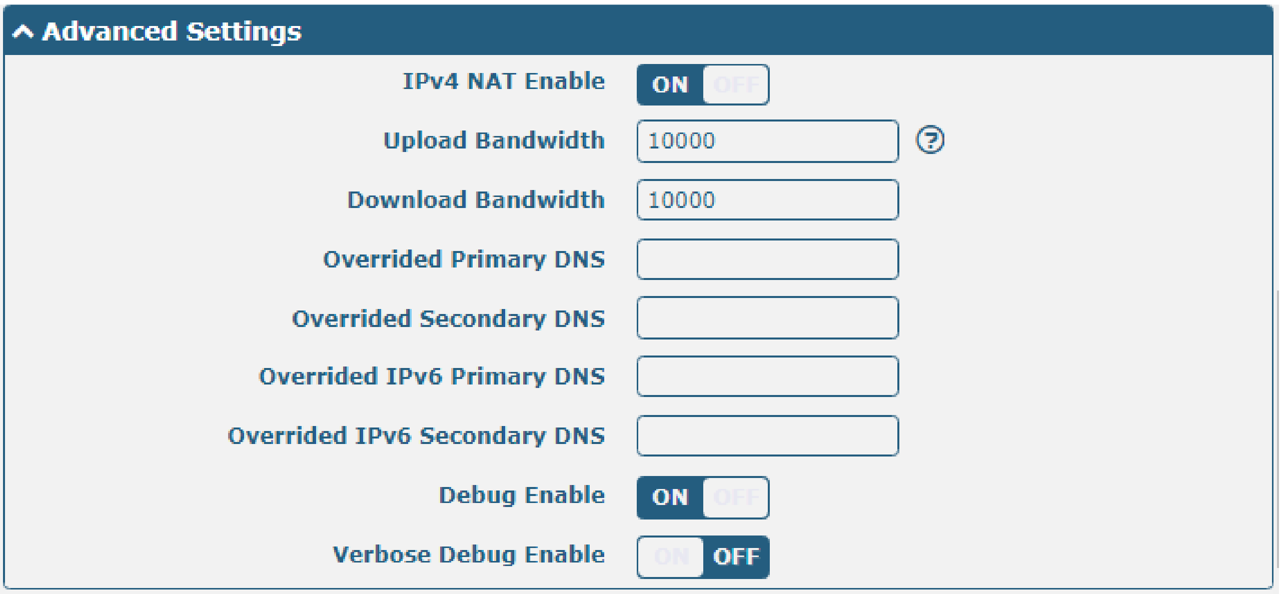
^ IPv6 LAN Settings

Connection Type	Static
IPv6 Prefix	2521:da8:202:10::/64
IPv6 NAT Enable	ON



Ping Detection Settings

Enable	ON
IPV4 Primary Server	8.8.8.8
IPv4 Secondary Server	114.114.114.114
IPv6 Primary Server	2001:4860:4860::8888
IPv6 Secondary Server	2400:da00:2::29
Interval	300
Retry Interval	5
Timeout	3
Max Ping Tries	3

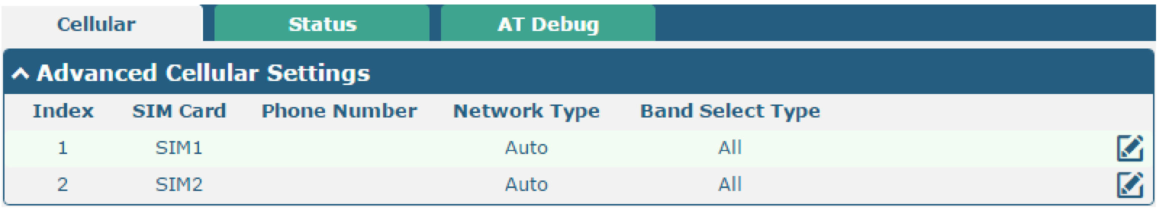


Advanced Settings

IPv4 NAT Enable	ON
Upload Bandwidth	10000
Download Bandwidth	10000
Overrided Primary DNS	
Overrided Secondary DNS	
Overrided IPv6 Primary DNS	
Overrided IPv6 Secondary DNS	
Debug Enable	ON
Verbose Debug Enable	OFF

When finished, click Submit > Save & Apply for the configuration to take effect.

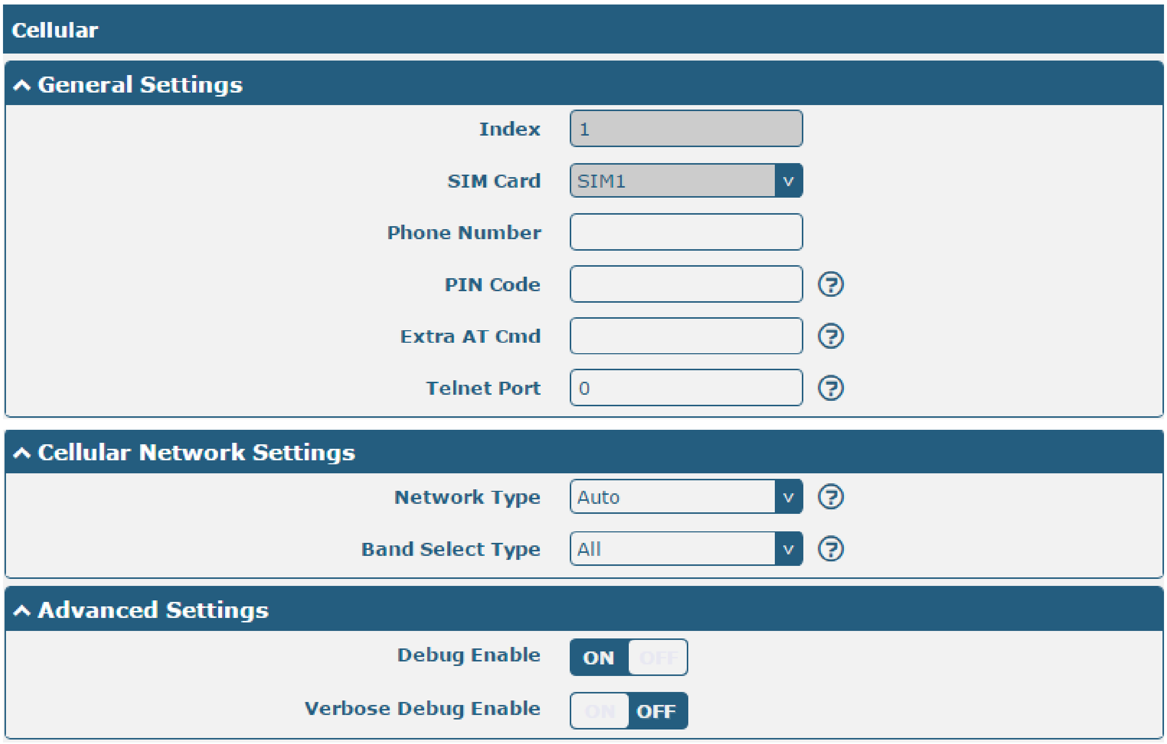
The window is displayed below by clicking Interface > Cellular > Advanced Cellular Settings.



Advanced Cellular Settings

Index	SIM Card	Phone Number	Network Type	Band Select Type
1	SIM1		Auto	All
2	SIM2		Auto	All

Click the edit button of SIM1 to set its parameters according to your application request.



Cellular

General Settings

Index	1
SIM Card	SIM1
Phone Number	
PIN Code	
Extra AT Cmd	
Telnet Port	0

Cellular Network Settings

Network Type	Auto
Band Select Type	All

Advanced Settings

Debug Enable	ON
Verbose Debug Enable	OFF

When finished, click Submit > Save & Apply for the configuration to take effect.

4.2.2 SMS Remote Control

DSR-211 supports remote control via SMS. You can use the following commands to get the status of DSR-211, and set all the parameters of DSR-211. There are three authentication types for SMS control. You can select from “ Password”, “ Phonenum” or “ Both”.

A SMS command has the following structure:

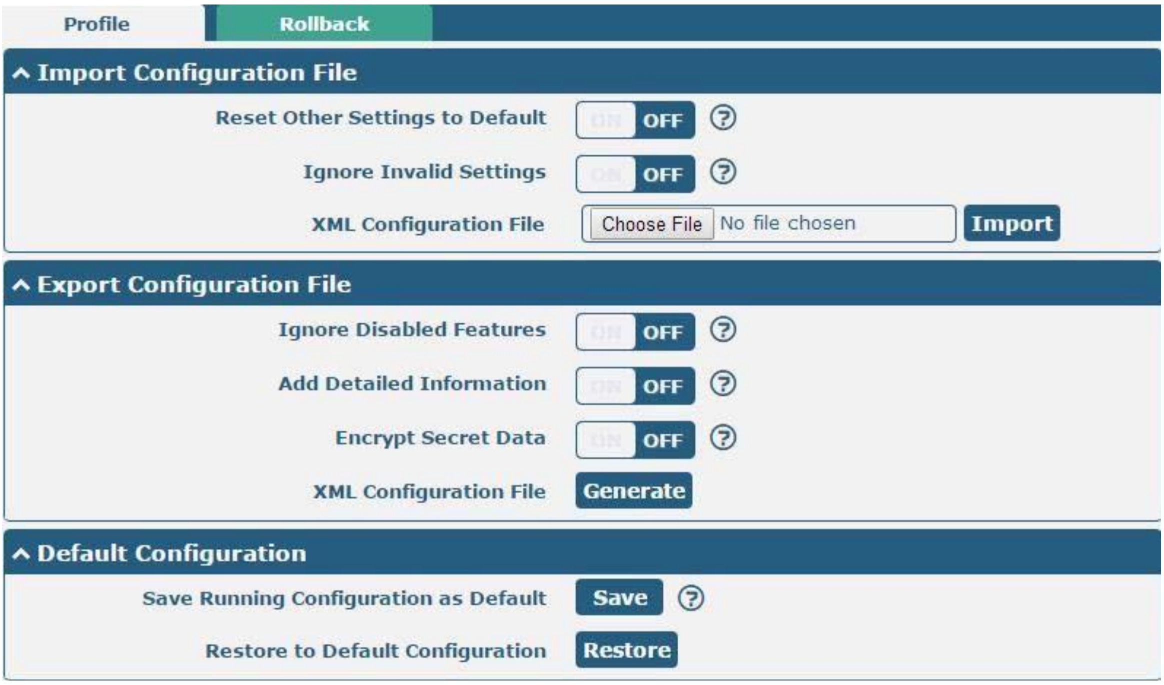
1. Password mode—Username Password;cmd1;cmd2;cmd3; …cmdn (available for every phone number).
2. Phonenum mode- Password;cmd1; cmd2; cmd3; …cmdn (available when the SMS was sent from the phone number which had been added in DSR-211’s phone group).
3. Both mode—Username: Password;cmd1;cmd2;cmd3; …cmdn (available when the SMS was sent from the phone number which had been added in DSR-211’s phone group).

SMS command Explanation:

1. User name and Password: use the same username and password as WEB manager for authentication.
2. cmd1, cmd2, cmd3 to Cmdn, the command format is the same as the CLI command, more details about CLI cmd please refer to Chapter 5 Introductions for CLI.

Note: Download the configure XML file from the configured web browser. The format of SMS control command can refer to the data of the XML file.

Go to System > Profile > Export Configuration File, click Generate to generate the XML file and click Export to export the XML file.



Import Configuration File

Reset Other Settings to Default: OFF

Ignore Invalid Settings: OFF

XML Configuration File: Choose File No file chosen Import

Export Configuration File

Ignore Disabled Features: OFF

Add Detailed Information: OFF

Encrypt Secret Data: OFF

XML Configuration File: Generate

Default Configuration

Save Running Configuration as Default: Save

Restore to Default Configuration: Restore

XML command:

```
<lan >
<network max_entry_num="2" >
<id > 1</id >
<interface > lan0</interface >
<ip > 172.16.24.24</ip >
<netmask > 255.255.0.0</netmask >
<mtu > 1500</mtu >
```

SMS cmd:

```
set lan network 1 interface lan0 set
lan network 1 ip 172.16.24.24
set lan network 1 netmask 255.255.0.0 set
lan network 1 mtu 1500
```

3. The semicolon character (‘;’) is used to separate more than one command packed in a single SMS.
4. E.g.

admin:admin;status system

In this command, username is “ admin”, password is “ admin”, and the function of the command is to get the system status.

SMS received:

hardware_version = 1.2

```
firmware_version = "3.0.0"
kernel_version = 4.1.0
device_model = DSR-211
serial_number = 201612221052
uptime = "0 days, 00:39:31"
system_time = "Mon Feb 27 09:52:52 2017 admin:
admin;reboot
```

In this command, username is “ admin”, password is “ admin”, and the command is to reboot the Router.

SMS received:

```
OK
```

```
admin:admin;set firewall remote_ssh_access false;set firewall remote_telnet _access false
```

In this command, username is “ admin”, password is “ admin”, and the command is to disable the remote_ssh and remote_telnet access.

SMS received

```
OK
OK
```

```
admin:admin; set lan net work 1 interface lan0;set lan network 1 ip 172.16.24.24; set lan network 1 netmask
255.255.0.0;set lan network 1 mtu 1500
```

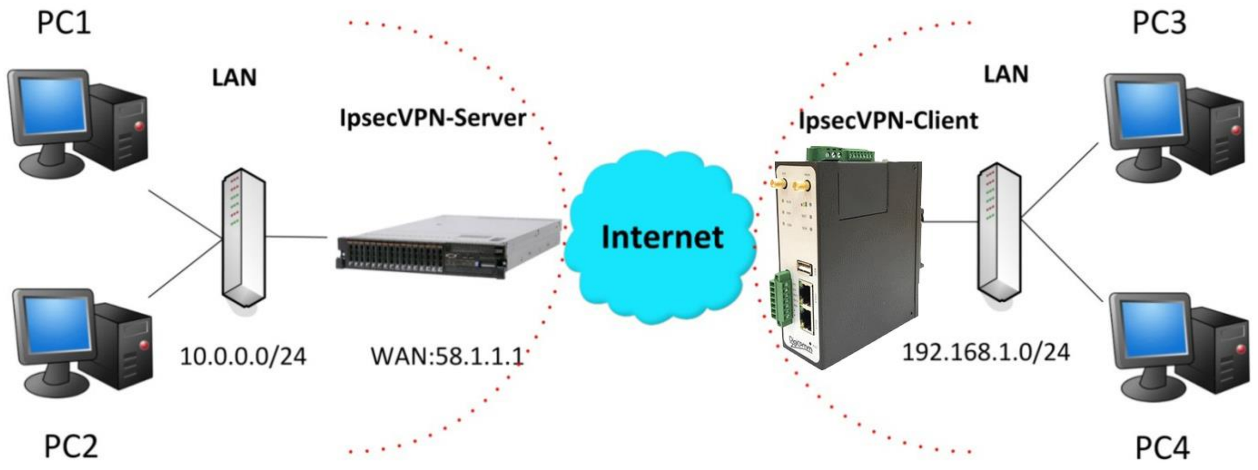
In this command, username is “ admin”, password is “ admin”, and the commands is to configure the LAN parameter.

SMS received: OK

```
OK
OK
OK
```

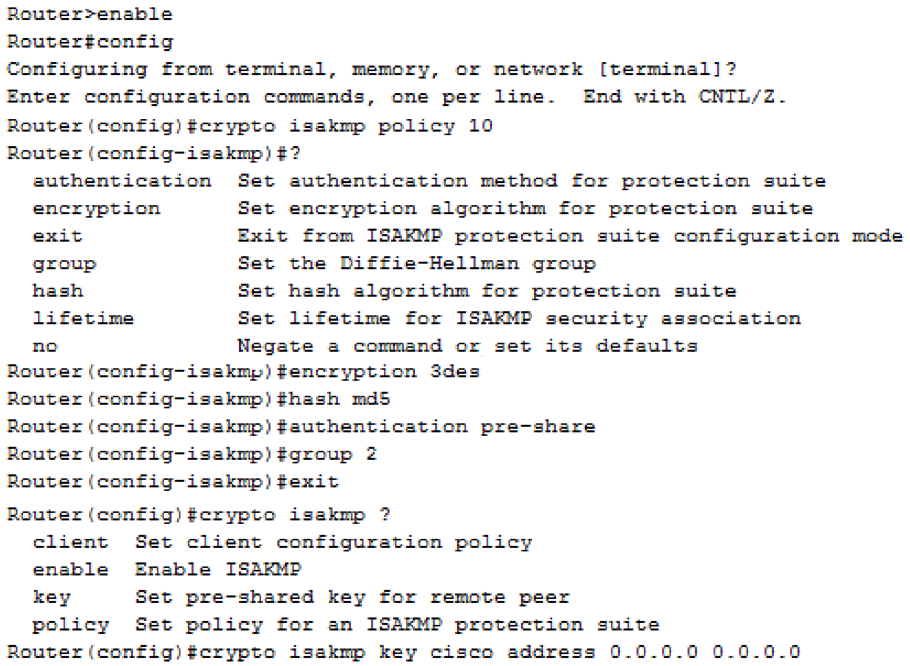
4.3 Network

4.3.1 IPsec VPN

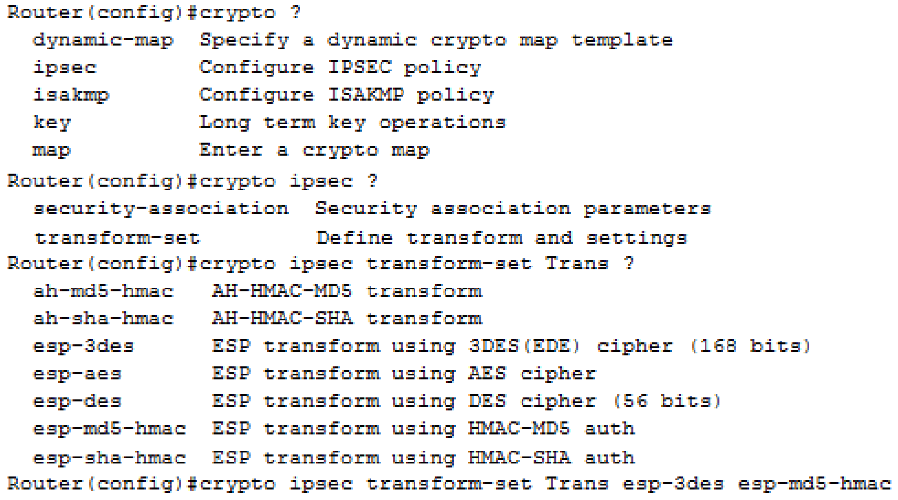


The configuration of server and client is as follows.

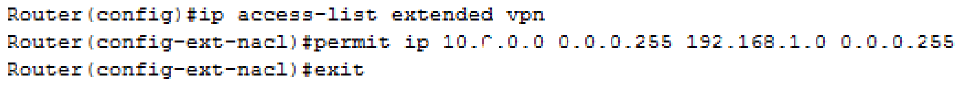
IPsecVPN_Server:
Cisco 2811:



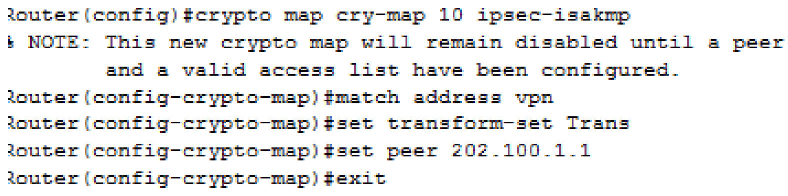
```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp ?
  client  Set client configuration policy
  enable  Enable ISAKMP
  key     Set pre-shared key for remote peer
  policy  Set policy for an ISAKMP protection suite
Router(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0
```



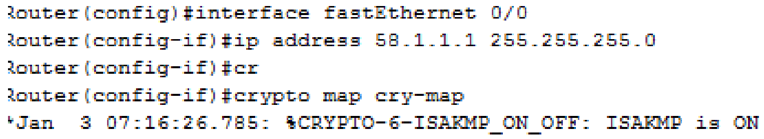
```
Router(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
Router(config)#crypto ipsec ?
  security-association  Security association parameters
  transform-set         Define transform and settings
Router(config)#crypto ipsec transform-set Trans ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-sha-hmac  ESP transform using HMAC-SHA auth
Router(config)#crypto ipsec transform-set Trans esp-3des esp-md5-hmac
```



```
Router(config)#ip access-list extended vpn
Router(config-ext-nacl)#permit ip 10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config-ext-nacl)#exit
```



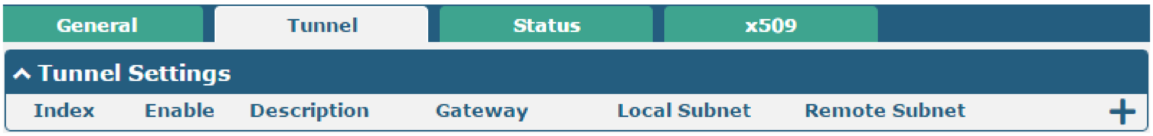
```
Router(config)#crypto map cry-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#match address vpn
Router(config-crypto-map)#set transform-set Trans
Router(config-crypto-map)#set peer 202.100.1.1
Router(config-crypto-map)#exit
```



```
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 58.1.1.1 255.255.255.0
Router(config-if)#cr
Router(config-if)#crypto map cry-map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

IPsec VPN_CLIENT:

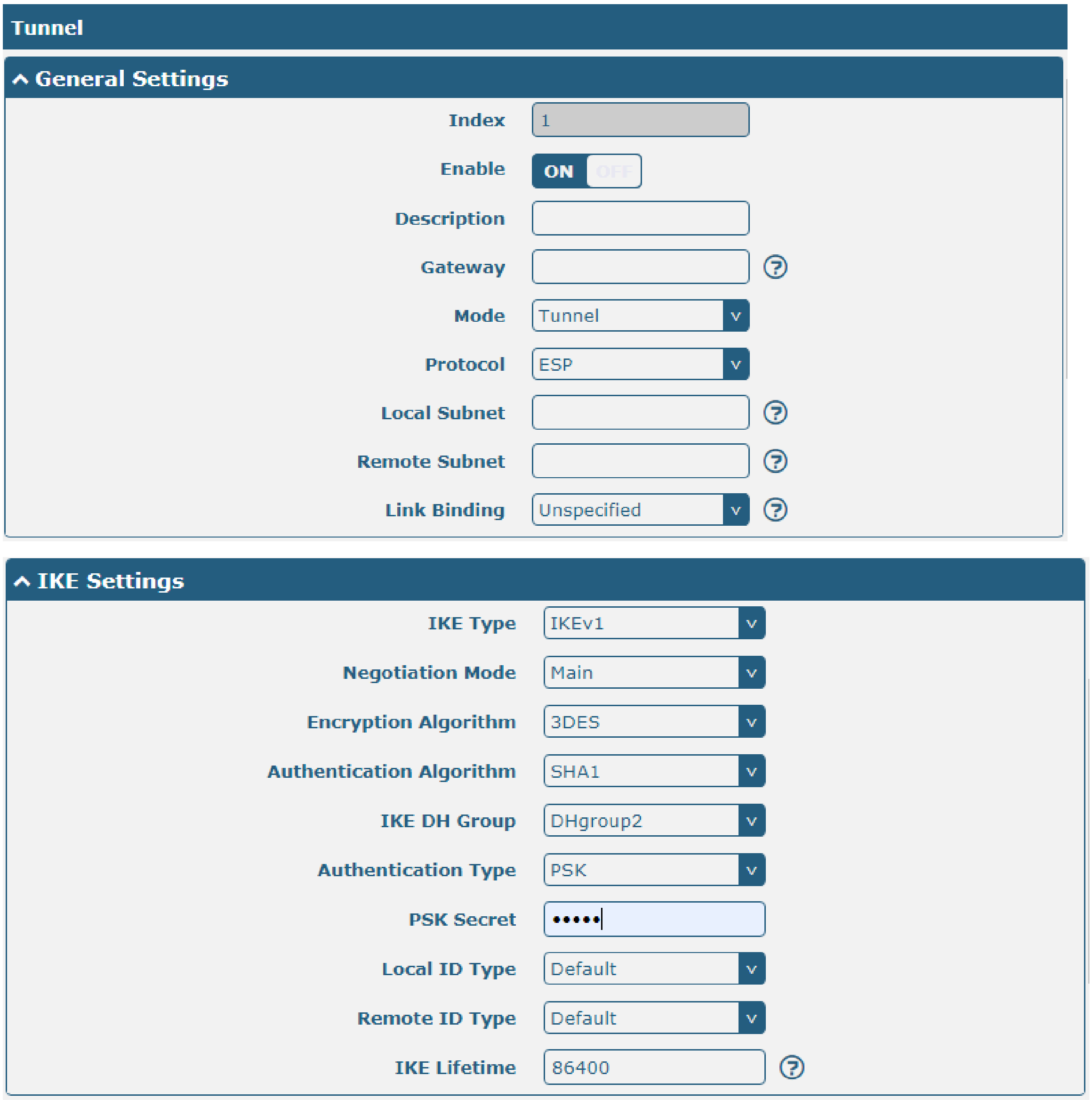
The window is displayed as below by clicking VPN > IPsec > Tunnel.



Tunnel Settings

Index	Enable	Description	Gateway	Local Subnet	Remote Subnet

Click + button and set the parameters of IPsec Client as below.

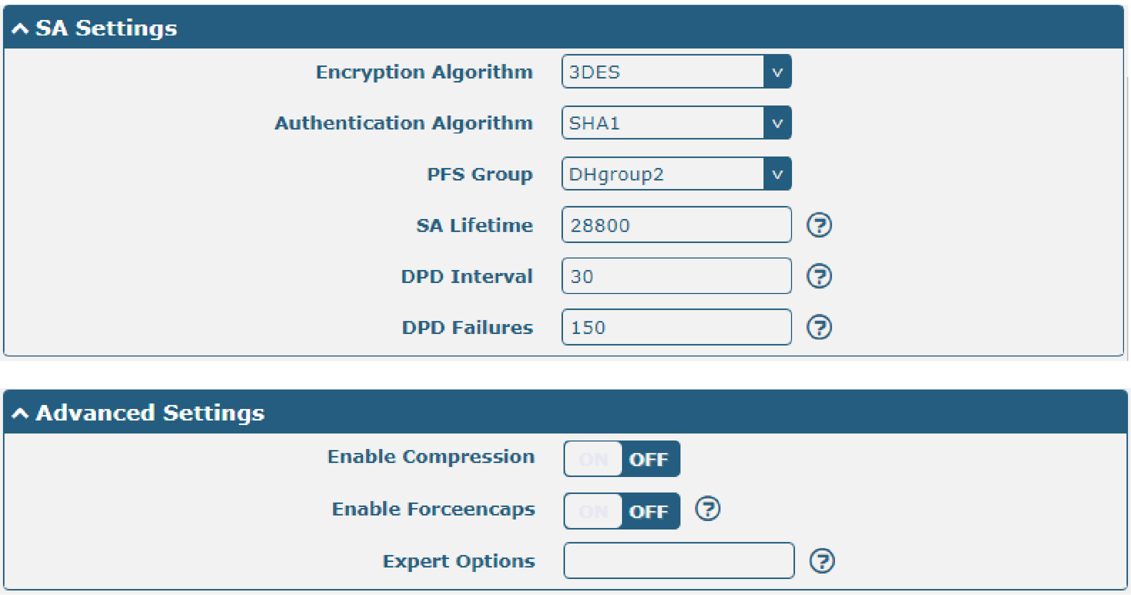

Tunnel

General Settings

Index	1
Enable	ON
Description	
Gateway	
Mode	Tunnel
Protocol	ESP
Local Subnet	
Remote Subnet	
Link Binding	Unspecified

IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	PSK
PSK Secret	•••••
Local ID Type	Default
Remote ID Type	Default
IKE Lifetime	86400

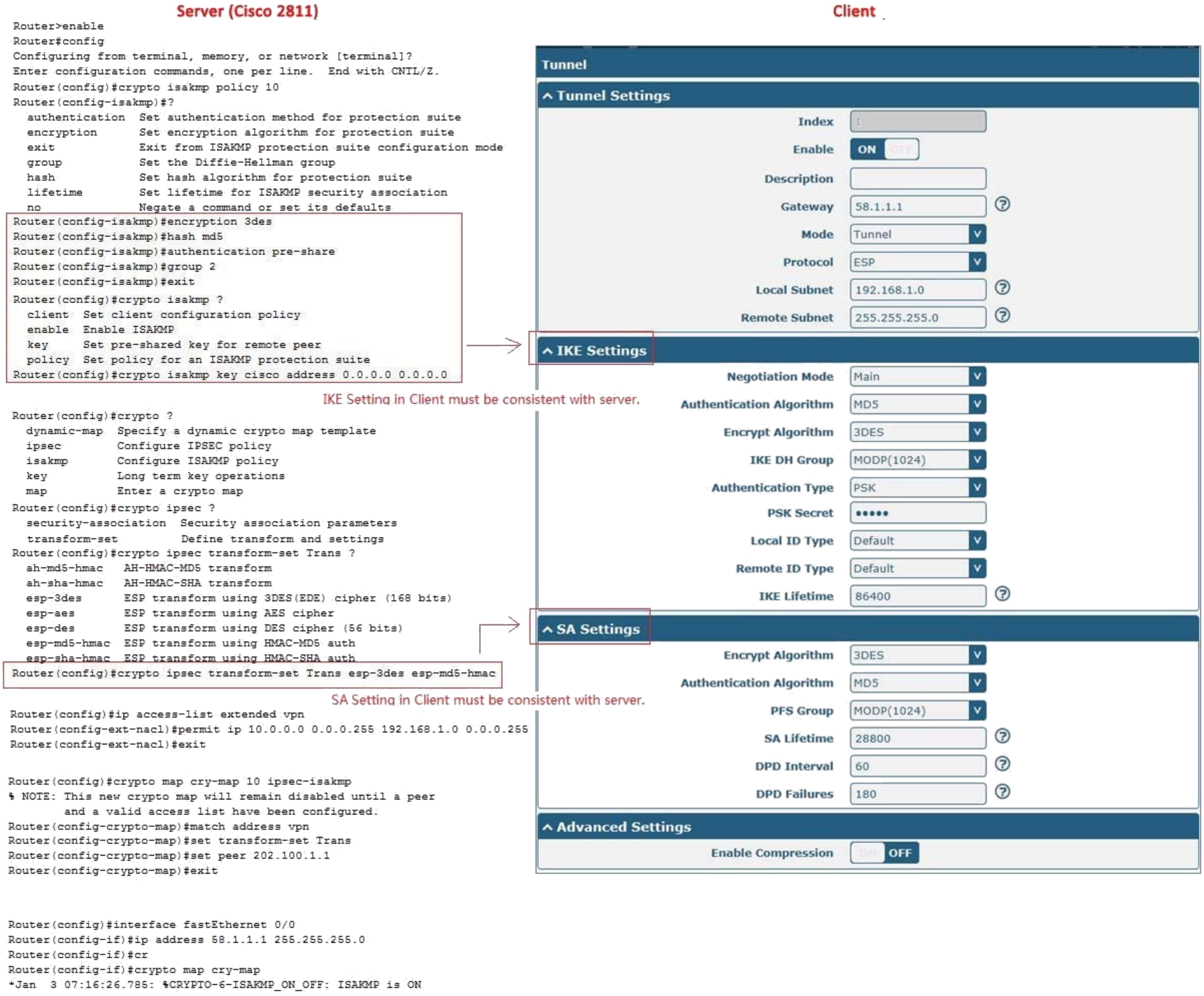


^ SA Settings

Encryption Algorithm	3DES
Authentication Algorithm	SHA1
PFS Group	DHgroup2
SA Lifetime	28800
DPD Interval	30
DPD Failures	150

^ Advanced Settings

Enable Compression	ON OFF
Enable Forceencaps	ON OFF
Expert Options	



Server (Cisco 2811)

```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp ?
  client  Set client configuration policy
  enable  Enable ISAKMP
  key     Set pre-shared key for remote peer
  policy  Set policy for an ISAKMP protection suite
Router(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0
```

IKE Setting in Client must be consistent with server.

```
Router(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
Router(config)#crypto ipsec ?
  security-association  Security association parameters
  transform-set         Define transform and settings
Router(config)#crypto ipsec transform-set Trans ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-sha-hmac  ESP transform using HMAC-SHA auth
Router(config)#crypto ipsec transform-set Trans esp-3des esp-md5-hmac
```

SA Setting in Client must be consistent with server.

```
Router(config)#ip access-list extended vpn
Router(config-ext-nacl)#permit ip 10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config-ext-nacl)#exit


Router(config)#crypto map cry-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#match address vpn
Router(config-crypto-map)#set transform-set Trans
Router(config-crypto-map)#set peer 202.100.1.1
Router(config-crypto-map)#exit



Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 58.1.1.1 255.255.255.0
Router(config-if)#cr
Router(config-if)#crypto map cry-map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Client

Tunnel

^ Tunnel Settings

Index	1
Enable	ON OFF
Description	
Gateway	58.1.1.1
Mode	Tunnel
Protocol	ESP
Local Subnet	192.168.1.0
Remote Subnet	255.255.255.0

^ IKE Settings

Negotiation Mode	Main
Authentication Algorithm	MD5
Encrypt Algorithm	3DES
IKE DH Group	MODP(1024)
Authentication Type	PSK
PSK Secret	•••••
Local ID Type	Default
Remote ID Type	Default
IKE Lifetime	86400

^ SA Settings

Encrypt Algorithm	3DES
Authentication Algorithm	MD5
PFS Group	MODP(1024)
SA Lifetime	28800
DPD Interval	60
DPD Failures	180

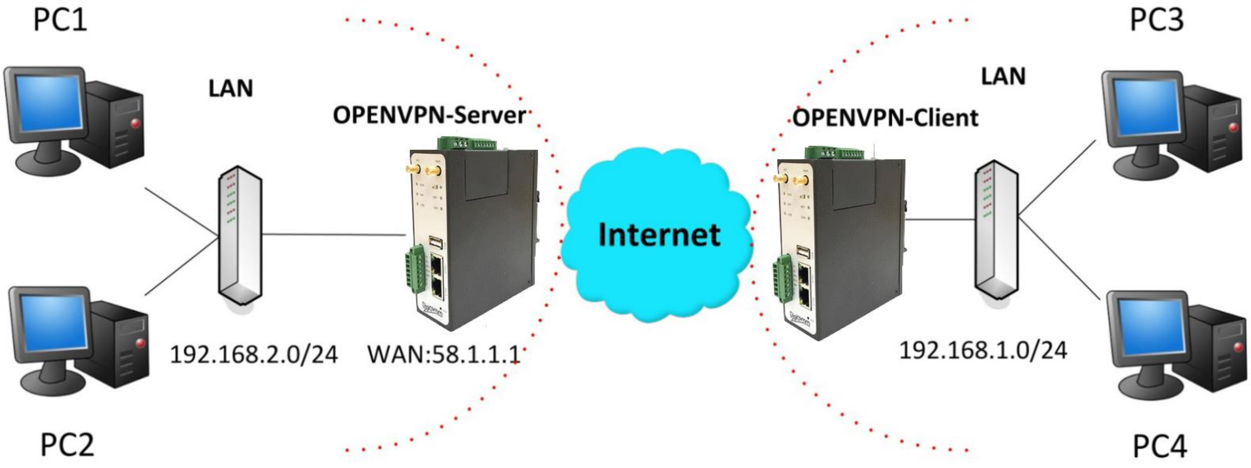
^ Advanced Settings

Enable Compression	ON OFF

When finished, click Submit > Save & Apply for the configuration to take effect. The comparison between server and client is as below.

4.3.2 OpenVPN

OpenVPN supports two modes, including Client and P2P. Here takes P2P as an example.



The configuration of two points is as follows.

OPENVPN_Server

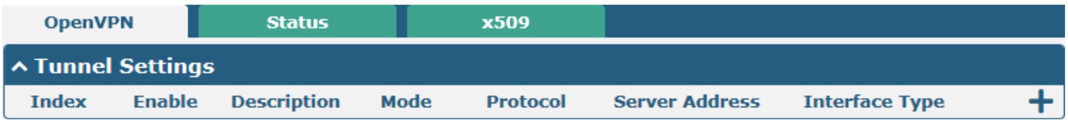
Generate relevant OpenVPN certificate on the server side firstly, and refer to the following commands to configuration the Server:

```
local 202.96.1.100
mode server
port 1194
proto udp
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert Server01.crt
key Server01.key
dh dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.3.0 255.255.255.0"
client-config-dir ccd
route 192.168.1.0 255.255.255.0
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

Note: For more configuration details, please contact your technical support engineer

OpenVPN_Client:

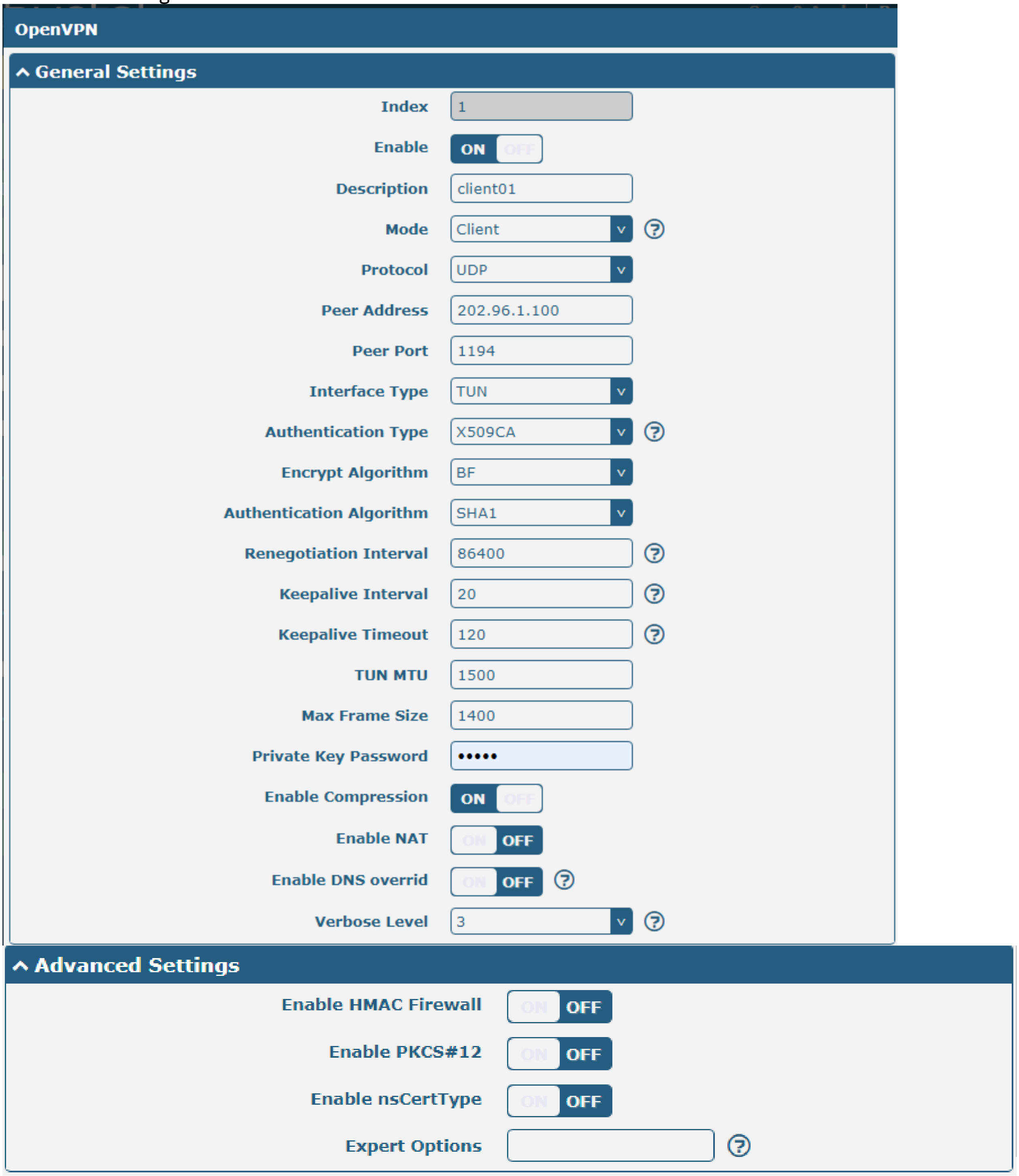
Click VPN > OpenVPN > OpenVPN as below.



Tunnel Settings

Index	Enable	Description	Mode	Protocol	Server Address	Interface Type	+

Click + to configure the Client01 as below.



OpenVPN

General Settings

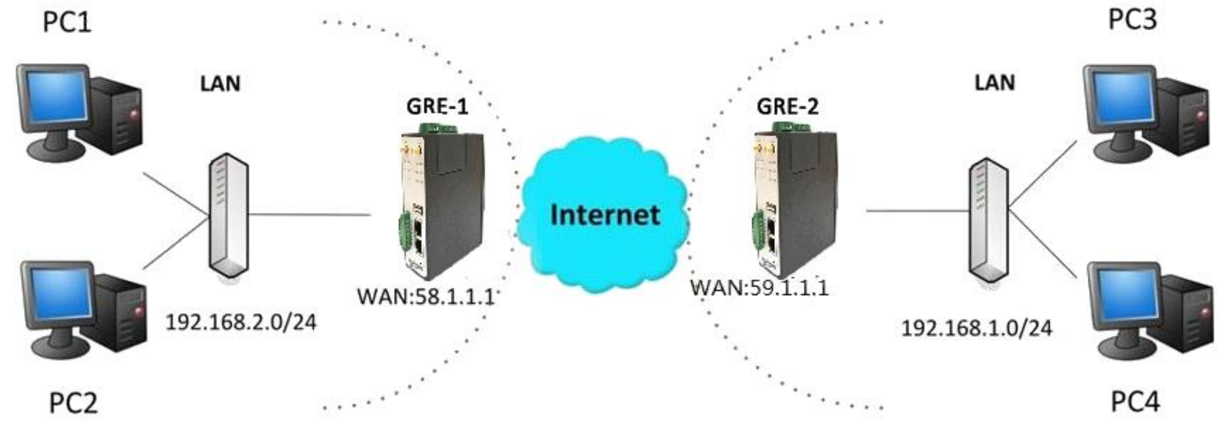
Index	1
Enable	ON
Description	client01
Mode	Client
Protocol	UDP
Peer Address	202.96.1.100
Peer Port	1194
Interface Type	TUN
Authentication Type	X509CA
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	1400
Private Key Password	•••••
Enable Compression	ON
Enable NAT	OFF
Enable DNS overrid	OFF
Verbose Level	3

Advanced Settings

Enable HMAC Firewall	OFF
Enable PKCS#12	OFF
Enable nsCertType	OFF
Expert Options	

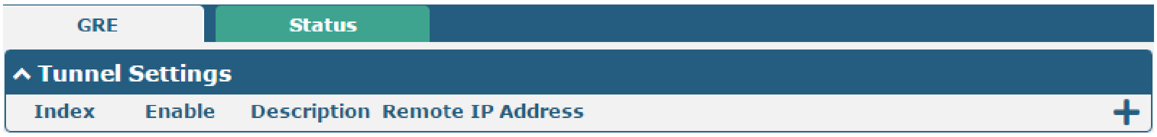
When finished, click Submit > Save & Applyfor the configuration to take effect.

4.3.3 GRE VPN



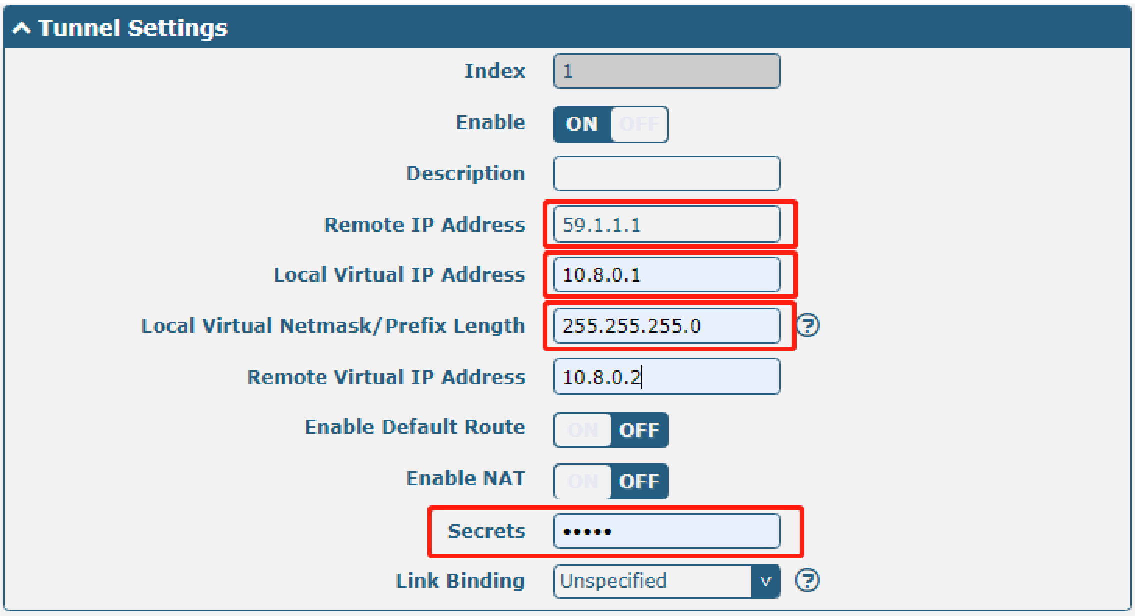
The configuration of two points is as follows.

The window is displayed as below by clicking VPN > GRE> GRE.



GRE-1

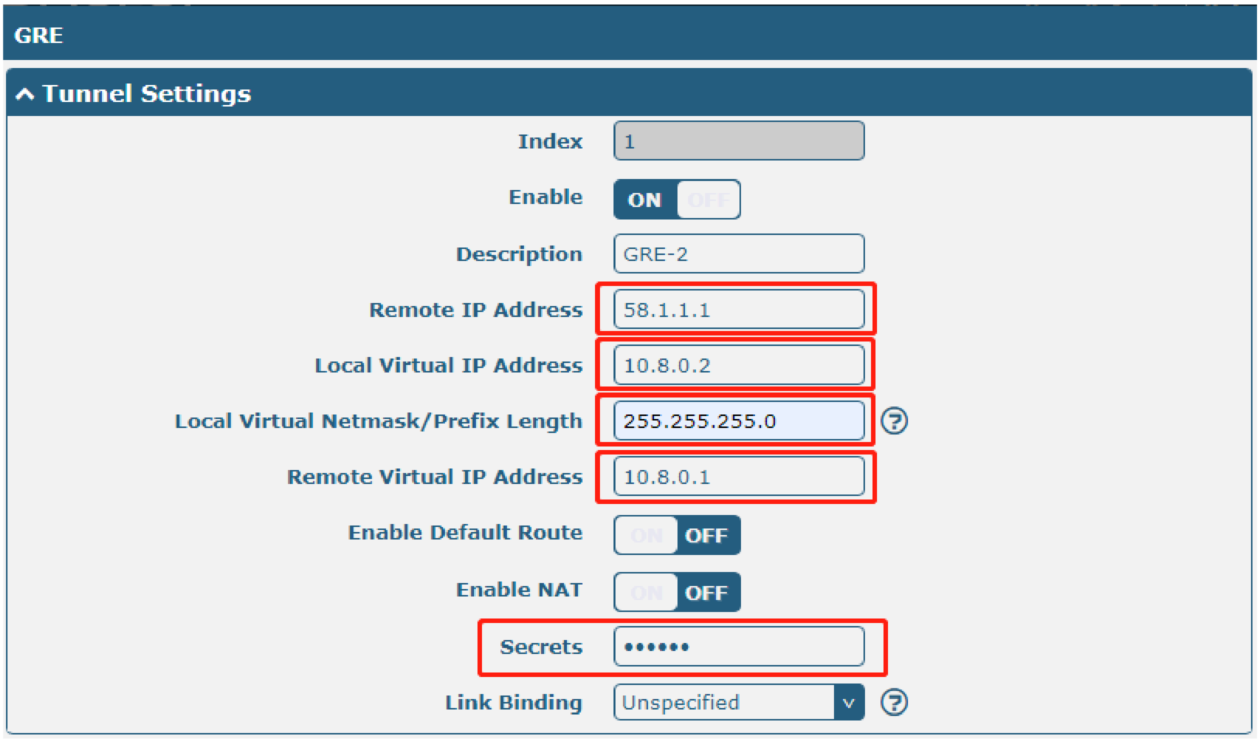
Click + button and set the parameters of GRE-1 as below



^ Tunnel Settings

Index	1
Enable	ON
Description	
Remote IP Address	59.1.1.1
Local Virtual IP Address	10.8.0.1
Local Virtual Netmask/Prefix Length	255.255.255.0
Remote Virtual IP Address	10.8.0.2
Enable Default Route	OFF
Enable NAT	OFF
Secrets	•••••
Link Binding	Unspecified

When finished, click Submit > Save & Apply for the configuration to take effect.



GRE

^ Tunnel Settings

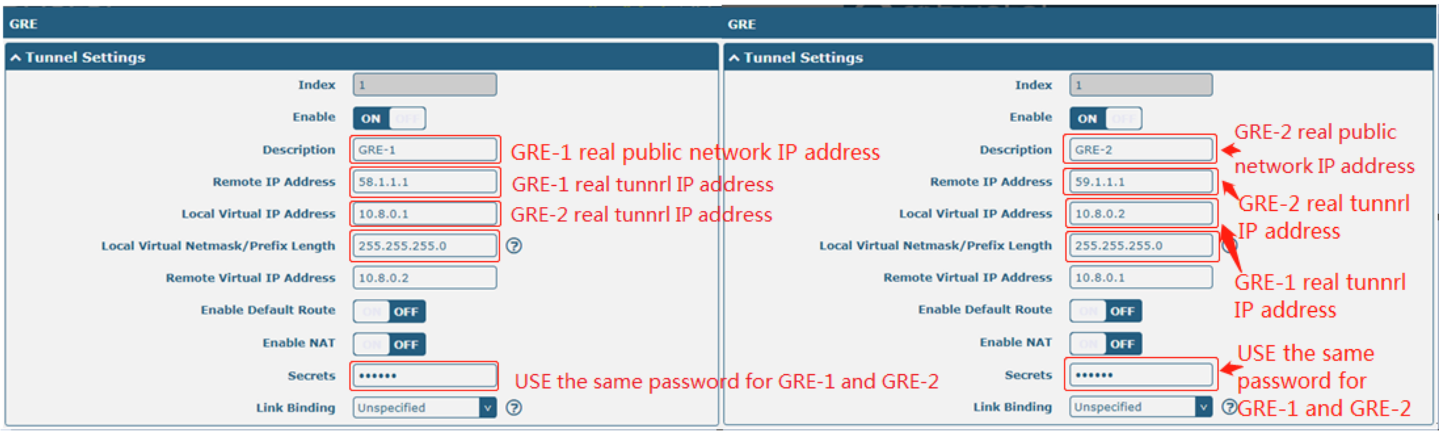
Index	1
Enable	ON
Description	GRE-2
Remote IP Address	58.1.1.1
Local Virtual IP Address	10.8.0.2
Local Virtual Netmask/Prefix Length	255.255.255.0
Remote Virtual IP Address	10.8.0.1
Enable Default Route	OFF
Enable NAT	OFF
Secrets	••••••
Link Binding	Unspecified

GRE-2:

Click + button and set the parameters of GRE-1 as below.

When finished, click Submit > Save & Apply for the configuration to take effect.

The comparison between GRE-1 and GRE-2 is as below.



GRE

Tunnel Settings

Index	1	1
Enable	ON	ON
Description	GRE-1	GRE-2
Remote IP Address	58.1.1.1	59.1.1.1
Local Virtual IP Address	10.8.0.1	10.8.0.2
Local Virtual Netmask/Prefix Length	255.255.255.0	255.255.255.0
Remote Virtual IP Address	10.8.0.2	10.8.0.1
Enable Default Route	OFF	OFF
Enable NAT	OFF	OFF
Secrets	••••••	••••••
Link Binding	Unspecified	Unspecified

GRE-1 real public network IP address

GRE-1 real tunnrl IP address

GRE-2 real tunnrl IP address

USE the same password for GRE-1 and GRE-2

GRE-2 real public network IP address

GRE-2 real tunnrl IP address

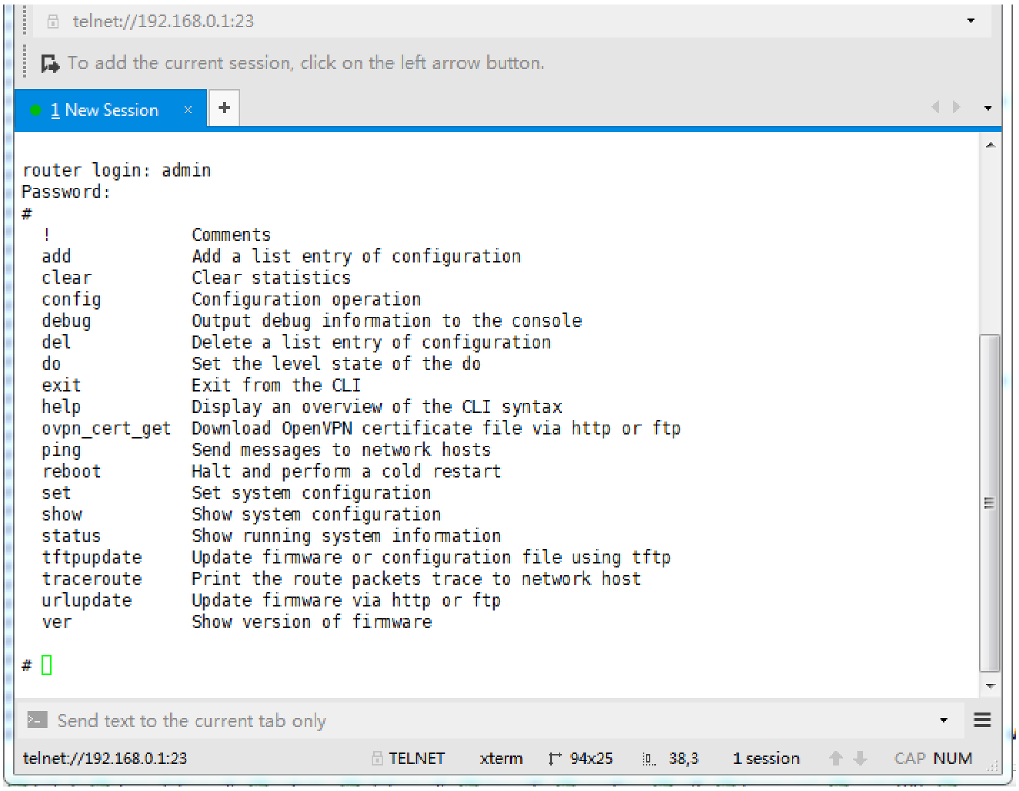
GRE-1 real tunnrl IP address

USE the same password for GRE-1 and GRE-2

5 Introductions for CLI

5.1 What Is CLI

The DRS-211 command-line interface (CLI) is a software interface providing another way to set the parameters of equipment from the SSH or through a telnet network connection.



```
router login: admin
Password:
#
  !             Comments
  add           Add a list entry of configuration
  clear         Clear statistics
  config        Configuration operation
  debug         Output debug information to the console
  del           Delete a list entry of configuration
  do            Set the level state of the do
  exit          Exit from the CLI
  help          Display an overview of the CLI syntax
  ovpn_cert_get Download OpenVPN certificate file via http or ftp
  ping          Send messages to network hosts
  reboot        Halt and perform a cold restart
  set           Set system configuration
  show          Show system configuration
  status        Show running system information
  tftpupdate    Update firmware or configuration file using tftp
  traceroute    Print the route packets trace to network host
  urlupdate     Update firmware via http or ftp
  ver           Show version of firmware

#
```

Route login:

Router login: admin

Password: admin

#

CLI commands:

```
    # ? (Note: the '?' won't display on the page.)
!                  Comments
add                Add a list entry of configuration
clear              Clear statistics
config             Configuration operation
debug              Output debug information to the console del
                   Delete a list entry of configuration
exit               Exit from the CLI
help               Display an overview of the CLI syntax
ovpn_cert_get  Download OpenVPN certificate file via http or ftp
ping               Send messages to network hosts reboot
                   Halt and perform a cold restart
route              Static route modify dynamically, this setting will not be saved set
                   Set system configuration
show               Show system configuration
status             Show running system information
tftpupdate         Update firmware using tftp
traceroute         Print the route packets trace to network
urlupdate          Update firmware using http or ftp
ver                Show version of firmware
```

5.2 How to configure the CLI

Following is a table about the description of help and the error should be encountered in the configuring program.

Commands / tips	Description
?	Typing a question mark " ?" will show you the help information. eg. # config (Press?) config Configuration operation #config Press (spacebar+?) commit Save the configuration changes and take effect changed configuration save_and_apply Save the configuration changes and take effect changed configuration loaddefault Restore Factory Configuration
Ctrl+c	Press these two keys at the same time, except its "copy" function but also can be used for "break" out of the setting program.
Syntax error: The command is not completed	Command is not completed.
Tick space key+ Tab key	It can help you finish your command. Example: # config (tick Enter key) Syntax error: The command is not completed # config (tick space key+ Tab key) commit save_and_apply loaddefault

# config commit # config save_and_apply /	When your setting finished, you should enter those commands to make your setting take effect on the device. Note: Commit and save_and_apply plays the same role.

5.3 Commands Reference

Commands	Syntax	Description
Debug	Debug parameters	Turn on or turn off debug function
Show	Show parameters	Show current configuration of each function , if we need to see all please using “ show running ”
Set	Set parameters Add parameters	All the function parameters are set by commands set and add, the difference is that set is for the single parameter and add is for the list parameter
Add		

Note: Download the config.XML file from the configured web browser. The command format can refer to the config.XML file format.

5.4 Quick Start with Configuration Examples

The best and quickest way to master CLI is firstly to view all features from the webpage and then read all CLI commands at a time, finally learn to configure it with some reference examples.

Example 1: Show current version

```
# status system
hardware_version = 1.2
firmware_version = "3.0.0" (
kernel_version = 4.1.0
device_model = DSR-211
serial_number = 201612221052
uptime = "0 days, 00:40:31"
system_time = " Feb 27 09:52:52 2019“
```

Example 2: Update firmware via tftp

```
# tftpupdate (space+?)
firmware          New firmware
# tftpupdate firmware (space+?)
 String   Firmware name
# tftpupdate firmware DSR-211-firmware-sysupgrade-unknown.bin host 192.168.100.99 / / enter a new firmware name
Downloading
DSR-211-firmware-s 100%| * * * * * *** *** * * * *** ** **** * *** *** * |  5018k   0:00:00 ETA
Flashing
Checking 100%
Decrypting 100%
Flashing 100%
Verifying 100% Verfify Success
upgrade success           / / update success
# config save_and_apply
```

```
OK      / / save and apply current configuration, make you configuration effect
```

Example 3: Set link-manager

```
# set
# set
at_over_telnet          AT Over Telnet
cellular        Cellular
ddns                    Dynamic DNS
ethernet                Ethernet
event                   Event Management
firewall        Firewall
gre                     GRE
ipsec     I             Psec
lan                     Local Area Network
link_manager            Link Manager
ntp                     NTP
openvpn                 OpenVPN
reboot                  Automatic Reboot
DigiLink                DigiLink
route                   Route
sms                     SMS
snmp                    SNMP agent
ssh                     SSH
syslog                  Syslog
system                  System
user_management         User Management
vrrp                    VRRP
web_server              Web Server
# set link_manager
primary_link            Primary Link
backup_link             Backup Link
backup_mode             Backup Mode
emergency_reboot        Emergency Reboot
link                    Link Settings
# set link_manager primary_link (space+?)
Enum    Primary Link (wwan1/ wwan2/ wan)
# set link_manager primary_link wwan1/ / select " wwan1" as primary_link
OK                                                / / setting succeed
# set link_manager link 1
type                    Type
desc                    Description
connection_type         ConnectionType
wwan                    WWAN Settings
static_addr             Static Address Settings
pppoe                   PPPoE Settings
ping                    Ping Settings
mtu                     MTU
dns1_overrided Overrided Primary DNS
dns2_overrided Overrided Secondary DNS
# set link_manager link 1 type wwan1
OK
# set link_manager link 1 wwan
auto_apn                Automatic APN Selection apn    APN
username                Username
password                Password
dialup_number Dialup Number
auth_type               Authentication Type
aggressive_reset        Aggressive Reset
switch_by_data_allowance        Switch SIM By Data Allowance
data_allowance          Data Allowance
```

```
billing_day                  Billing Day
# set link_manager link 1 wwan switch_by_data_allowance true
OK
#
# set link_manager link 1 wwan data_allowance 100      / / open cellular switch_by_data_traffic
OK                                                             / / setting succeed
# set link_manager link 1 wwan billing_day 1                / / setting specifies the day of month for billing
OK                                                             / / setting succeed
...
# config save_and_apply
OK                                        / / save and apply current configuration, make you configuration effect
```

Example 4: Set Ethernet

```
# set Ethernet port_setting 2 port_assignment lan0                        //Set Table 2 (eth1) to lan0
OK
# config save_and_apply                                                   //setting succeed
OK
```

Example 5: Set LAN IP address

```
# show lan all
network {
id = 1
interface = lan0
ip = 192.168.0.1
netmask = 255.255.255.0
mtu = 1500
dhcp {
          enable = true
          mode = server relay_server = ""
          pool_start = 192.168.0.2
          pool_end = 192.168.0.100
         netmask = 255.255.255.0
          gateway = ""
          primary_dns = ""
          secondary_dns = ""
          wins_server = ""
          lease_time = 120
          expert_options = ""
          debug_enable = false
        }
  }
  multi_ip {
        id = 1
        interface = lan0
        ip = 172.16.24.24 netmask
        = 255.255.0.0
  }
  #
  # set lan
     network         Network Settings
```

```
    multi_ip        Multiple IP Address Settings vlan
                    VLAN
# set lan network 1(space+?)
    interface       Interface
    ip              IP Address
    netmask         Netmask mtu
                    MTU
    dhcp            DHCP Settings
# set lan network 1 interface lan0
OK
# set lan network 1 ip 172.16.99.22                  / / set IP address for lan
OK                                                   / / setting succeed
# set lan network 1 netmask 255.255.0.0
OK
#
...
# config save_and_apply
OK                                           / / save and apply current configuration, make you configuration effect
```

Example 6: CLI for setting Cellular

```
  # show cellular all
  sim {
id = 1
card = sim1
phone_number = ""
extra_at_cmd = ""
network_type = auto
band_select_type = all
band_gsm_850 = false
band_gsm_900 = false
band_gsm_1800 = false
band_gsm_1900 = false
band_wcdma_850 = false
band_wcdma_900 = false
band_wcdma_1900 = false
band_wcdma_2100 = false
band_lte_800 = false band_lte_850 =
false band_lte_900 = false
band_lte_1800 = false
band_lte_1900 = false
band_lte_2100 = false
band_lte_2600 = false
band_lte_1700 = false band_lte_700
= false band_tdd_lte_2600 = false
band_tdd_lte_1900 = false
band_tdd_lte_2300 = false
band_tdd_lte_2500 = false

}
sim {
```

```
id = 2
card = sim2
phone_number =
extra_at_cmd = ""
network_type = auto band_select_type
= all band_gsm_850 = false
band_gsm_900 = false band_gsm_1800
= false band_gsm_1900 = false
band_wcdma_850 = false
band_wcdma_900= false
band_wcdma_1900 = false
band_wcdma_2100 = false
band_lte_800 = false
band_lte_850 = false
band_lte_900 = false
band_lte_1800 = false
band_lte_1900 = false
band_lte_2100 = false
band_lte_2600 = false
band_lte_1700 = false
band_lte_700 = false
band_tdd_lte_2600 = false
band_tdd_lte_1900 = false
band_tdd_lte_2300 = false
band_tdd_lte_2500 =false
  }
  # set(space+?)
  at_over_telnet    cellular        ddns            dhcp            dns
  event             firewall        ipsec           lan             link_manager
  ntp               openvpn         reboot          route           serial_port
  sms               snmp            syslog          system          user_management vrrp
  # set cellular(space+?)
    sim    SIM Settings
  # set cellular sim(space+?)
  Integer       Index (1..2)

  # set cellular sim 1(space+?)
    card                   SIM Card
    phone_number           Phone Number
    extra_at_cmd           Extra AT Cmd
    network_type           Network Type
    band_select_type       Band Select Type
    band_gsm_850           GSM 850
    band_gsm_900           GSM 900
    band_gsm_1800          GSM 1800
    band_gsm_1900          GSM 1900
    band_wcdma_850         WCDMA 850
    band_wcdma_900         WCDMA 900
    band_wcdma_1900        WCDMA 1900
    band_wcdma_2100        WCDMA 2100
    band_lte_800           LTE800 (band 20)
    band_lte_850           LTE850 (band 5)
    band_lte_900           LTE900 (band 8)
    band_lte_1800          LTE1800 (band 3)
    band_lte_1900          LTE1900 (band 2)
    band_lte_2100          LTE2100 (band 1)
    band_lte_2600          LTE2600 (band 7)
    band_lte_1700          LTE1700 (band 4)
    band_lte_700           LTE700 (band 17)
    band_tdd_lte_2600      TDD LTE2600 (band 38)
    band_tdd_lte_1900      TDD LTE1900 (band 39)
    band_tdd_lte_2300      TDD LTE2300 (band 40)
    band_tdd_lte_2500      TDD LTE2500 (band 41)
# set cellular sim 1 phone_number 18620435279
OK
…
# config save_and_apply
OK                                          / / save and apply current configuration, make you configuration effect
```

6 Glossary

Abbr.	Description
AC	Alternating Current
APN	Access Point Name
ASCII	American Standard Code for Information Interchange
CE	Conformité Européene (European Conformity)
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface for batch scripting
CSD	Circuit Switched Data
CTS	Clear to Send
dB	Decibel
dBi	Decibel Relative to an Isotropic radiator
DC	Direct Current
DCD	Data Carrier Detect
DCE	Data Communication Equipment (typically modems)
DCS 1800	Digital Cellular System, also referred to as PCN
DI	Digital Input
DO	Digital Output
DSR	Data Set Ready
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi-frequency
DTR	Data Terminal Ready
EDGE	Enhanced Data rates for Global Evolution of GSM and IS-136
EMC	Electromagnetic Compatibility
EMI	Electro-Magnetic Interference
ESD	Electrostatic Discharges
ETSI	European Telecommunications Standards Institute
EVDO	Evolution-Data Optimized
FDD LTE	Frequency Division Duplexing Long Term Evolution
GND	Ground
GPRS	General Packet Radio Service
GRE	generic route encapsulation
GSM	Global System for Mobile Communications
HSPA	High Speed Packet Access
ID	identification data
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPsec	Internet Protocol Security
kbps	kbits per second

Abbr.	Description
L2TP	Layer 2 Tunneling Protocol
LAN	local area network
LED	Light Emitting Diode
M2M	Machine to Machine
MAX	Maximum
Min	Minimum
MO	Mobile Originated
MS	Mobile Station
MT	Mobile Terminated
OpenVPN	Open Virtual Private Network
PAP	Password Authentication Protocol
PC	Personal Computer
PCN	Personal Communications Network, also referred to as DCS1800
PCS	Personal Communication System, also referred to as GSM 1900
PDU	Protocol Data Unit
PIN	Personal Identity Number
PLCs	Program Logic Control System
PPP	Point-to-point Protocol
PPTP	Point to Point Tunneling Protocol
PSU	Power Supply Unit
PUK	Personal Unblocking Key
R&TTE	Radio and Telecommunication Terminal Equipment
RF	Radio Frequency
RTC	Real Time Clock
RTS	Request to Send
RTU	Remote Terminal Unit
Rx	Receive Direction
SDK	Software Development Kit
SIM	subscriber identification module
SMA antenna	Stubby antenna or Magnet antenna
SMS	Short Message Service
SNMP	Simple Network Management Protocol
TCP/ IP	Transmission Control Protocol / Internet Protocol
TE	Terminal Equipment, also referred to as DTE
Tx	Transmit Direction
UART	Universal Asynchronous Receiver-transmitter
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
USSD	Unstructured Supplementary Service Data
VDC	Volts Direct current
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSWR	Voltage Stationary Wave Ratio
WAN	Wide Area Network

Sie brauchen technische Unterstützung?

Unser Support-Team hilft Ihnen gerne weiter:

Support@digicomm.de

(02159) 693-75-50