AirGate 4G

INSTRUCTION MANUAL V1.0x B

We Measure, We Control, We Record

07661-19-12560

1 SAFETY ALERTS

The symbols below are used throughout this manual to draw the user's attention to important information regarding safety and use of the device.

⚠	⚡	
CAUTION Read the manual fully before installing and operating the device.	**CAUTION OR HAZARD** Risk of electric shock.	**ATTENTION** Material sensitive to static charge. Check precautions before handling.

Safety recommendations must be followed to ensure user safety and to prevent damage to the device or system. If the device is used in a manner other than that specified in this manual, the safety protections may not be effective.

1.1 INTERFERENCE ISSUES

Avoid possible radio frequency (RF) interference by following these guidelines:

- The use of cellular telephones or devices in aircraft is illegal. Use in aircraft may endanger operation and disrupt the cellular network. Failure to observe this restriction may result in suspension or denial of cellular services to the offender, legal action, or both.
- Do not operate in the vicinity of gasoline or diesel fuel pumps unless use has been approved or authorized.
- Do not operate in locations where medical equipment that the device could interfere with may be in use.
- Do not operate in fuel depots, chemical plants, or blasting areas unless use has been approved and authorized.
- Use care if operating in the vicinity of protected personal medical devices, i.e., hearing aids and pacemakers.
- Operation in the presence of other electronic equipment may cause interference if equipment is incorrectly protected. Follow recommendations for installation from equipment manufacturers.

2 INTRODUCTION

AirGate 4G has a unique and flexible platform that allows remote access to industrial automation networks. This device enables wireless data connectivity over public and private cellular networks with 2G/3G/4G technology and access to legacy network with Modbus RTU over RS485 networks and several protocols over TCP/IP and RS232.

AirGate 4G has two SIM cards inputs, allowing the use of up to two cellular network operators (one of them acting as failover), two LAN ports (one port that can be used as both LAN and WAN - for fixed Internet with mobile failover) and two digital inputs and two digital outputs for alarm applications. **AirGate 4G Wi-Fi** model has a Wi-Fi 802.11 b/g/n interface for access point with equipment that has Wi-Fi connectivity.

The device supports 9 to 48 VDC supply voltage and has a reverse polarity protection mechanism for added reliability. It is an advanced choice for M2M wireless applications with reliable data transmission capabilities.

2.1 FEATURES AND BENEFITS

INDUSTRIAL INTERNET ACCESS

- Wireless mobile broadband 2G / 3G / 4G connection
- Remote access to SCADA system for industrial automation
- Reduce high costs for on-site maintenance

DESIGNED FOR INDUSTRIAL USAGE

- Power input range 9 to 48 VDC
- Industrial designed for harsh environment
- Compact metal casing for easy mounting

SECURE AND RELIABLE REMOTE CONNECTION

- Connection manager ensure seamless communication
- Support multiple VPN tunnels for data encryption
- Firewall prevents unsafe and unauthorized access

EASY TO USE AND EASY TO MAINTAIN

- User-friendly web interface for human interaction
- Easy configuration for deployment
- Support 3rd party remote management cloud

2.2 MECHANICAL SPECIFICATIONS

AirGate 4G has the following dimensions: 106 mm x 106 mm x 40 mm (excluding antenna).

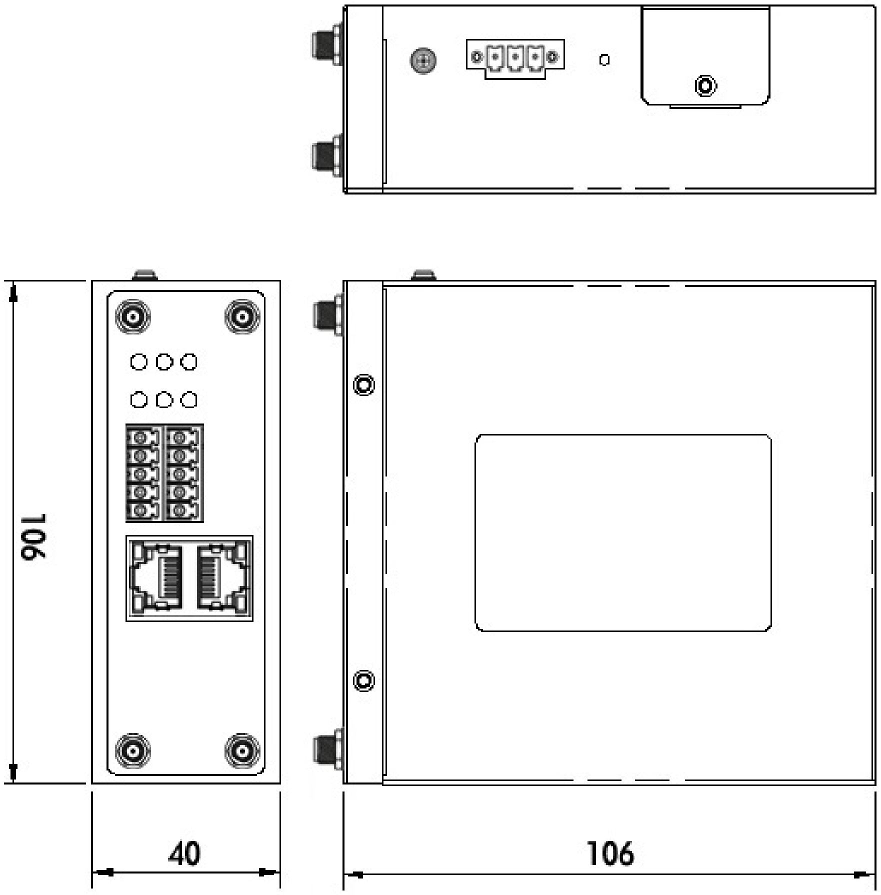


Figure 1 - **AirGate 4G** Dimension

2.3 PACKAGE CHECKLIST

AirGate 4G package contains:

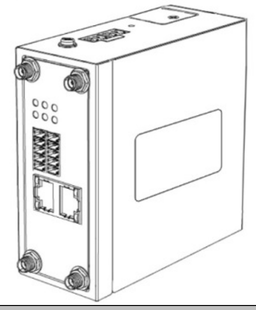
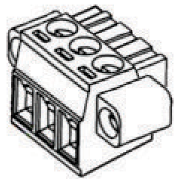
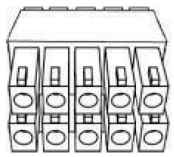
			
AirGate 4G or AirGate 4G Wi-Fi	**1 Power Supply Connector**	**1 Connector for serial ports and digital inputs and outputs**	**1 Ethernet Cable**

Table 1 – Required Items 1

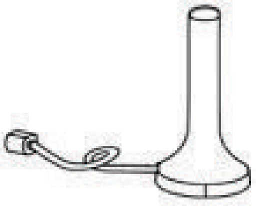
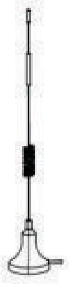
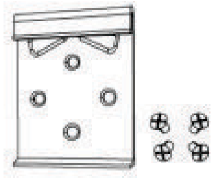
		
1 Cellular Antenna	**2 Wi-Fi Antennas (for AirGate 4G Wi-Fi)**	**1 DIN Rail mounting kit**

Table 2 – Required Items 2

AirGate 4G contains the following optional accessory items:

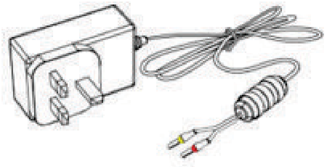
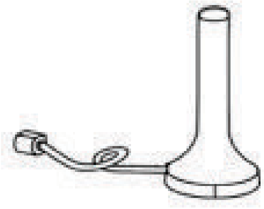
	
Power Supply	**Cellular Antenna**

Table 3 – Optional items

3 INSTALLATION

3.1 DEVICE OVERVIEW

3.1.1 FRONT PANEL

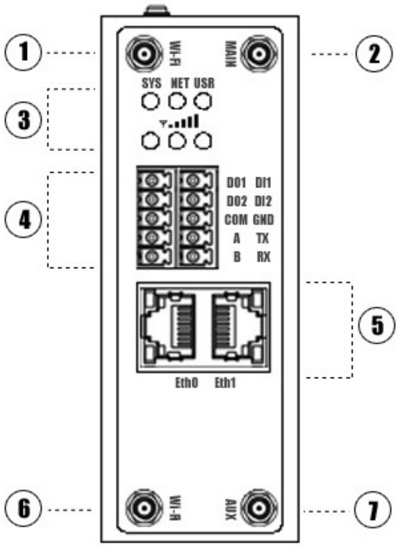


Figure 2 – Front panel

In the front panel, **AirGate 4G** has the following items:

1. Wi-Fi antenna connector (**AirGate 4G Wi-Fi** model);
2. MAIN cellular antenna connector;
3. LED indicator;
4. Serial ports and digital inputs and digital outputs (DIDO) connector;
5. Ethernet port;
6. Wi-Fi antenna connector (**AirGate 4G Wi-Fi** model);
7. AUX cellular antenna connector.

3.1.2 LEFT SIDE PANEL

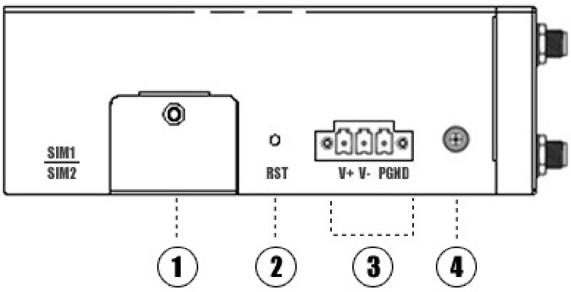


Figure 3 – Left site

In the left side panel, **AirGate 4G** has the following items:

1. SIM card slot;
2. Reset button;
3. Power connector;
4. Grounding stud.

3.2 LED INDICATOR

NAME	COLOR	STATUS	DESCRIPTION
SYS	Green	Slow blinking (500 ms duration)	System booting.
		Fast blinking	Operating normally.
		Off	Power is off.
NET	Green	On	Register to highest priority network service (depend on Radio, e.g. Radio support LTE as Highest priority network).
		Fast blinking (500 ms duration)	Register to non-highest priority network service (depend on Radio, e.g. Radio support LTE as Highest priority network, then WCDMA and GPRS is non-highest priority network).
		Off	Register failed.
USR: SIM	Green	On	Router is trying cellular connection with SIM1.
		Fast blinking (250 ms duration)	Router is trying cellular connection with SIM2.
		Off	No SIM detected.
USR: Wi-Fi	Green	On	Wi-Fi is enable but without data transmission.
		Blinking	Wi-Fi is enabled and transmitting data.
		Off	Wi-Fi is disabled or failed to boot.
Signal Strength Indicator 📶	Green	On / 3 LED light up	Signal strength (21-31) is high.
		On / 2 LED light up	Signal strength (11-20) is medium.
		On / 1 LED light up	Signal strength (1-10) is low.
		Off	No signal.

Table 4 – LED indicator

3.3 ETHERNET PORT INDICATOR

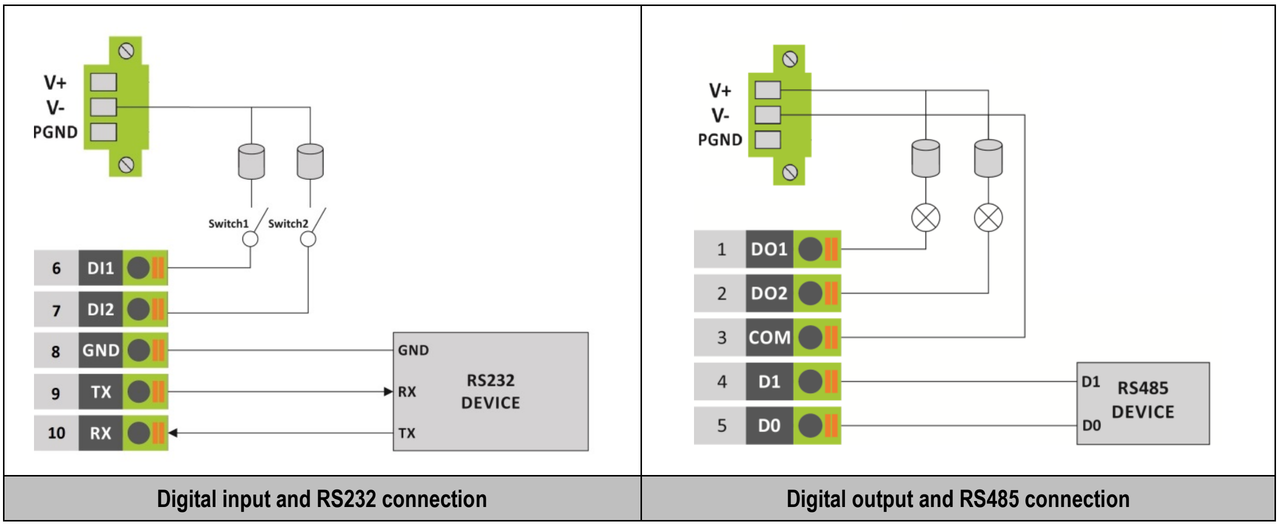
NAME	COLOR	STATUS	DESCRIPTION
Link indicator	Green	On	Connection is established.
		Blinking	Data is being transmitted.
		Off	Connection is not established.
	Yellow	Not used for this device model.	

Table 5 – Ethernet port indicator

3.4 CONNECTOR PIN DEFINITION

3.4.1 SERIAL PORTS & DIDO

Figure 4 shows the RS232, the RS485, and the DIDO connections:

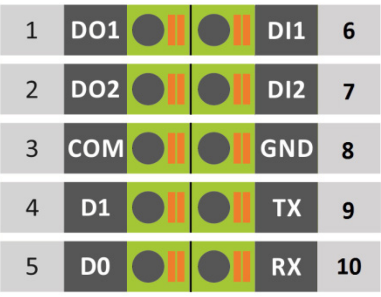


Digital input and RS232 connection

Digital output and RS485 connection

Figure 4 - **AirGate 4G** connections

Table 6 shows the connector pins numbering:



PIN	RS232	RS485	DI	DO	DIRECTION
1	--	--	--	DO1	Router ⟶ Device
2	--	--	--	DO2	Router ⟶ Device
3	--	--	--	COM	--
4	--	D1	--	--	Router ⟷ Device
5	--	D0	--	--	Router ⟷ Device
6	--	--	DI1	--	Router ⟵ Device
7	--	--	DI2	--	Router ⟵ Device
8	GND	--	--	--	--
9	TX	--	--	--	Router ⟶ Device
10	RX	--	--	--	Router ⟵ Device

Table 6 – Serial ports & DIDO

Table 7 shows the RS485 signals:

D1	D	D+	B	Bidirectional line of data.	Terminal 4
D0	$\overline{D}$	D-	C	Inverted bidirectional line of data.	Terminal 5
C				Optional link that improves communication performance.	Terminal 8
GND					

Table 7 - RS485 signals

3.4.2 POWER INPUT

Figure 5 shows the power input connections:

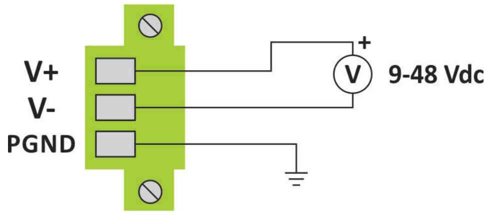


Figure 5 – Power input

PIN	DESCRIPTION
V+	Positive
V-	Negative
PGND	GND

Table 8 – Power input

3.5 RESET BUTTON

FUNCTION	ACTION
Reboot	Press the RST button for up to 3 seconds while device is operating.
Factory reset	Press the RST button until all LEDs flash. After that, you must manually restart the device.

Table 9 – Reset button

3.6 SIM CARD

To insert or remove a SIM card in **AirGate 4G**, you must do the following:

1. Ensure that the device is not being electrically powered;
2. Use a Phillips screwdriver to remove the protective cover from the device;
3. Insert the SIM card into the SIM socket;
4. Replace the protective cover.

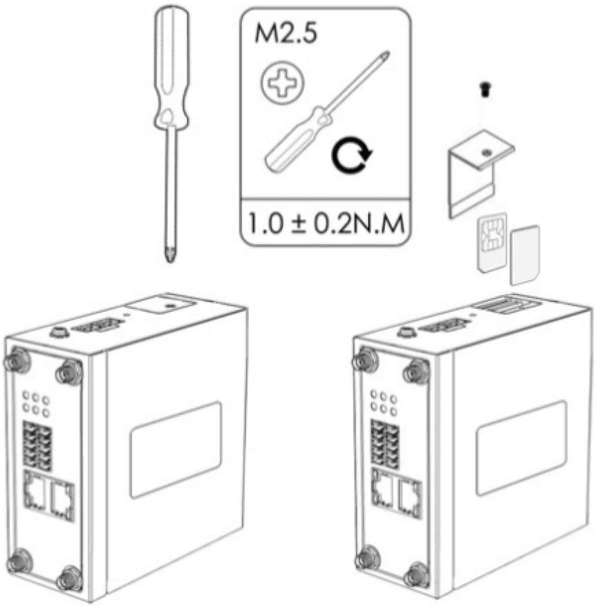


Figure 6 - Inserting SIM card

3.7 ANTENNAS

3.7.1 AIRGATE 4G

AirGate 4G supports two antennas: one on the MAIN connector and one on the AUX connector.

The MAIN connector is used to receive and transmit data via cellular antenna. The AUX connector is used to improve signal strength and depends on using an antenna on the MAIN connector to work.

How to connect the cellular antenna to the MAIN and AUX connectors of the device:

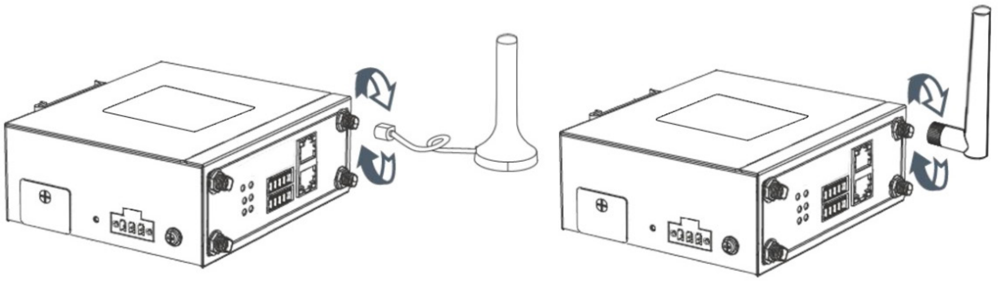


Figure 7 – Cellular antenna

3.7.2 AIRGATE 4G WI-FI

AirGate 4G Wi-Fi supports four antennas: two on Wi-Fi connectors for Wi-Fi functionality, one on MAIN connector and one on AUX connector, both for cellular connection.

Wi-Fi connectors are used to receive and transmit data wirelessly and their antennas should always be used together. The MAIN connector is used to receive and transmit data via cellular antenna. The AUX connector, in turn, is used to improve signal strength and depends on using an antenna on the MAIN connector to work.

How to connect the Wi-Fi antenna to the Wi-Fi connector of the device:

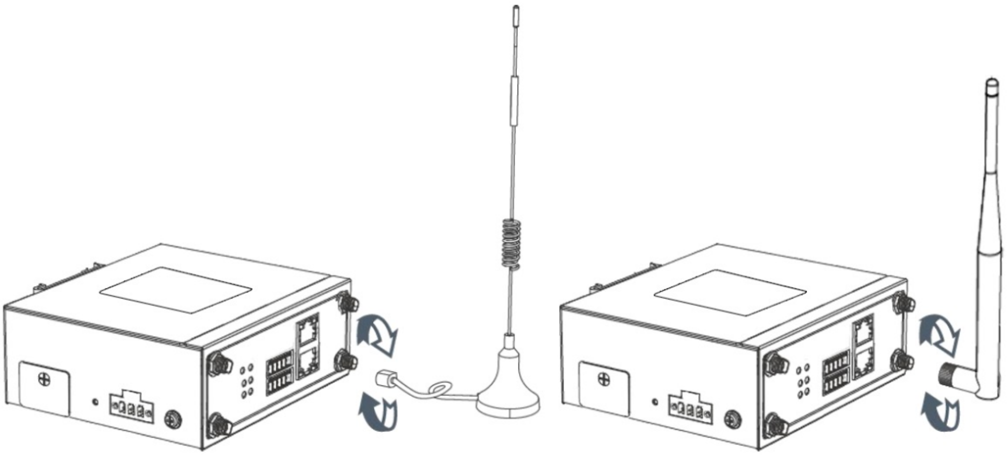


Figure 8 – Wi-Fi antenna

3.8 DIN RAIL

To mount the DIN rail kit, you must do the following:

1. Use four M3x6 flat head Phillips screws to fix the DIN rail kit to the device;
2. Insert the handle of the DIN rail bracket;
3. Press the device into the DIN rail until the bracket snaps into place.

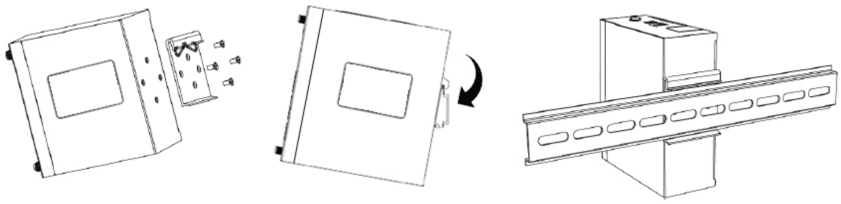


Figure 9 – DIN rail mounting

3.9 PROTECTIVE GROUNDING INSTALLATION

To install the grounding protection, you must do the following:

1. Remove the grounding screw;
2. Connect the grounding wire ring of the housing to the grounding pin;
3. Tighten the bolt screw.

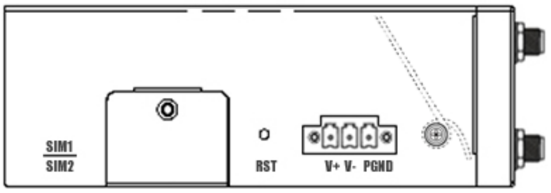


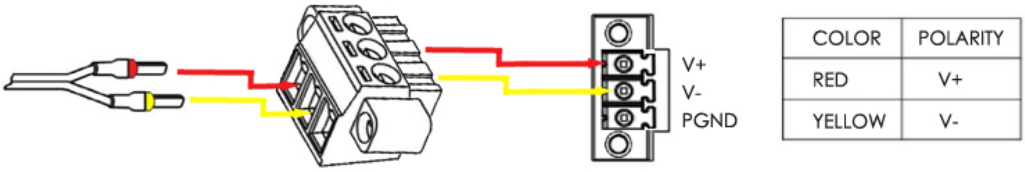
Figure 10 – Protective grounding

It is recommended that the device be grounded when installed.

3.10 POWER SUPPLY INSTALLATION

To install the power supply, you must do the following:

1. Remove the pluggable connector from the device;
2. Then loosen the screws for the locking flanges as needed;
3. Connect the wires of the power supply to the terminals.



COLOR	POLARITY
RED	V+
YELLOW	V-

Figure 11 – Power supply installation

3.11 TURN ON THE DEVICE

To turn the device, you must do the following:

1. Connect one end of the Ethernet cable to the device's LAN port and the other end to the computer's LAN port;
2. Connect the AC source to a power source;
3. The device is ready for use when the SYS LED is flashing.

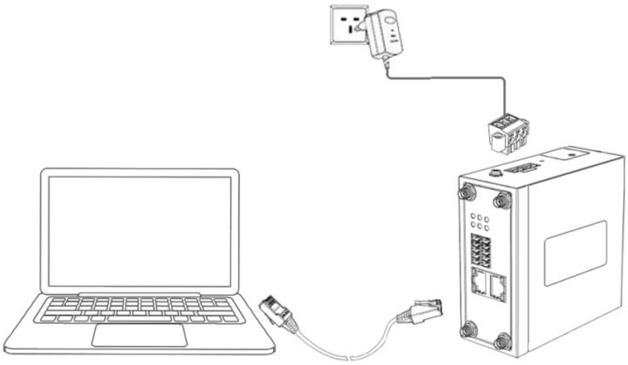


Figure 12 – Turning on the device

4 ACCESS TO WEB PAGE

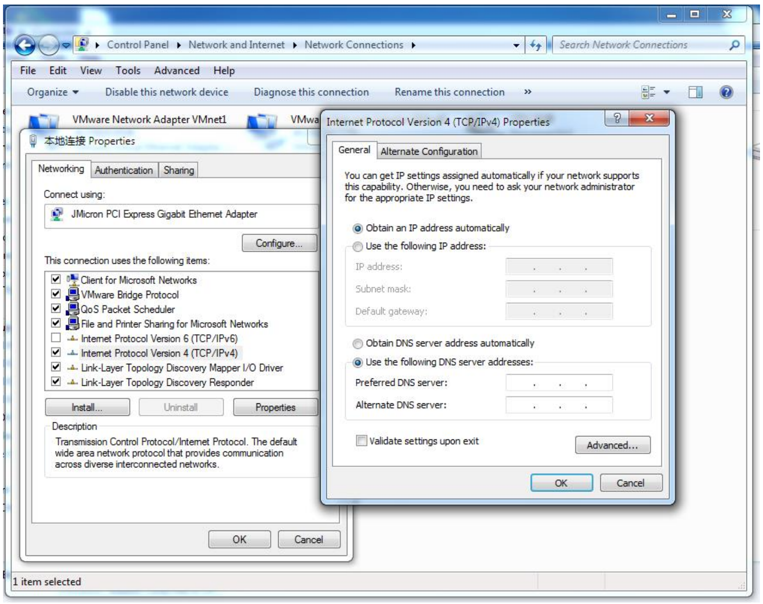
4.1 PC CONFIGURATION

AirGate 4G has a DHCP server that will automatically assign an IP address to the user's computer. In some cases, it will be necessary to change the computer's network settings to accept the router's IP address. You can also manually configure the IP address.

The sections below provide information on setting up an IP for **AirGate 4G** and how to make the first access to the device's web interface.

4.1.1 SET AN IP ADDRESS AUTOMATICALLY

You can set the device to automatically obtain an IP by following these steps:



Control Panel ▸ Network and Internet ▸ Network Connections ▸

本地连接 Properties

Networking | Authentication | Sharing

Connect using:

JMicron PCI Express Gigabit Ethernet Adapter

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.

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

1 item selected

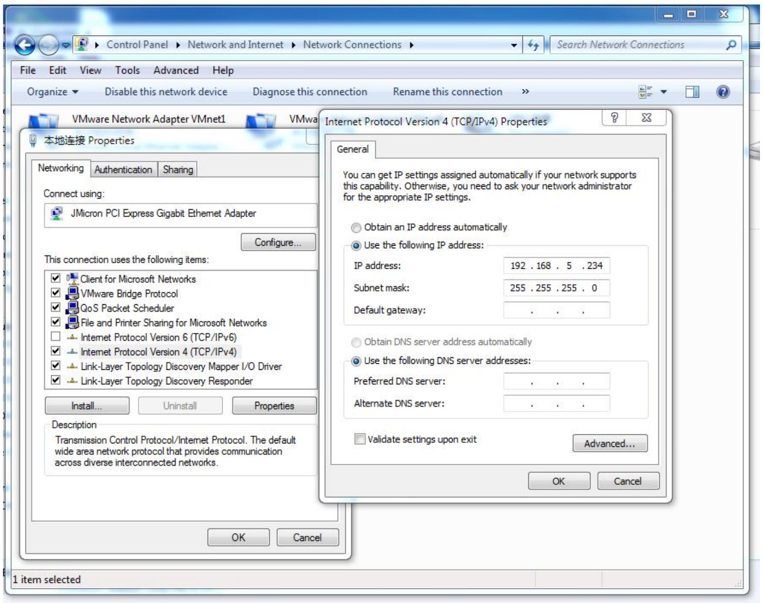
Figure 13 – Set an IP address automatically

Select **Start » Control Panel » Network Connections**. Right click **Local Area Connection** and select **Properties** to open the configuration dialog box for Local Area Connection. Select **Internet Protocol (TCP/IP)** and click **Properties** to open the TCP/IP configuration window.

On the General tab, select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Click **OK** to complete TCP/IP configuration.

4.1.2 SET AN STATIC IP ADDRESS

You can set your device to manually obtain an IP by following these steps:



Control Panel ▸ Network and Internet ▸ Network Connections ▸

本地连接 Properties

Networking | Authentication | Sharing

Connect using:

JMicron PCI Express Gigabit Ethernet Adapter

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.

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 . 5 . 234
  - Subnet mask: 255 . 255 . 255 . 0
  - Default gateway: . . .
- ○ Obtain DNS server address automatically
- ● Use the following DNS server addresses:
  - Preferred DNS server: . . .
  - Alternate DNS server: . . .
- ☐ Validate settings upon exit

1 item selected

Figure 14 – Set a static IP address

Click **Use the following IP address** to assign a static IP manually within the same subnet of the router.

Default Gateway and **DNS Server** are not necessary if PC not routing all traffic go through router.

4.2 FACTORY DEFAULT SETTINGS

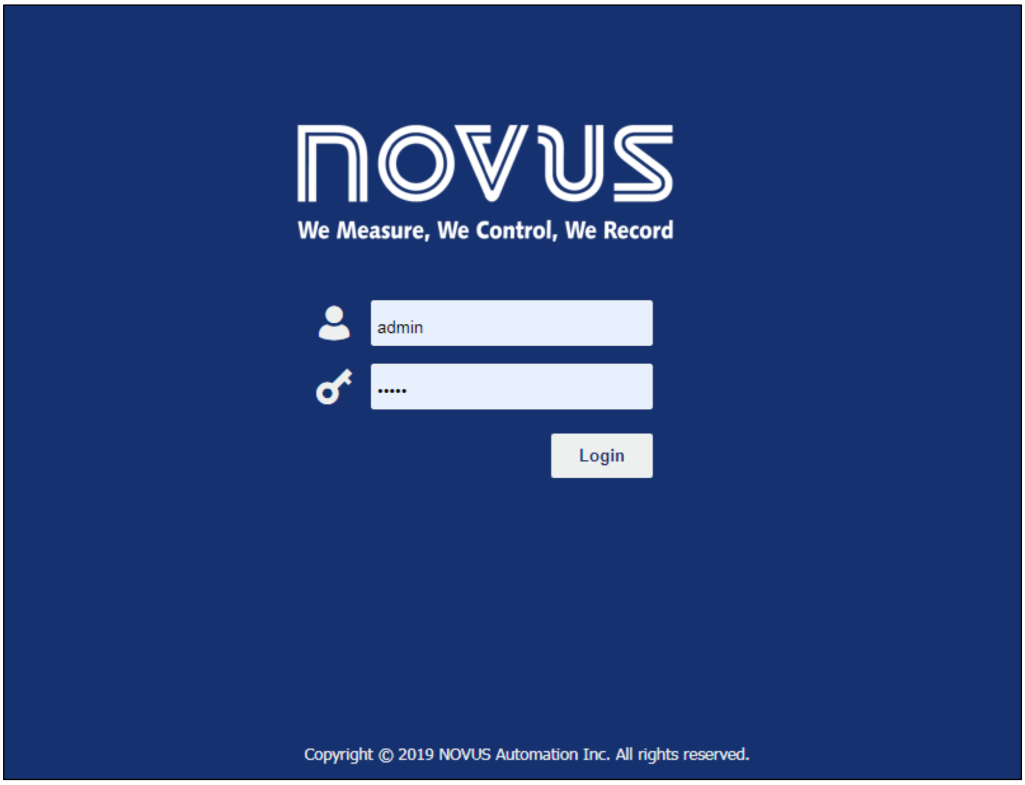
AirGate 4G can be set up via a web page. The Graphical User Interface (GUI), presented in the LOGIN TO WEB PAGE section, allows you to manage and configure the device. During the first router configuration, the following default settings should be used:

- Username: **admin**
- Password: **admin**
- LAN IP Address: **192.168.5.1** (Eth0 ~ Eth1 as LAN mode)
- DHCP Server: **Enabled**

4.3 LOGIN TO WEB PAGE

To access **AirGate 4G** setup page, you must open a web browser on your computer (Google Chrome or Internet Explorer are recommended) and enter IP 192.168.5.1 in the address bar.

After that, just use the same username and password (admin / admin) to access device settings.



admin

•••••

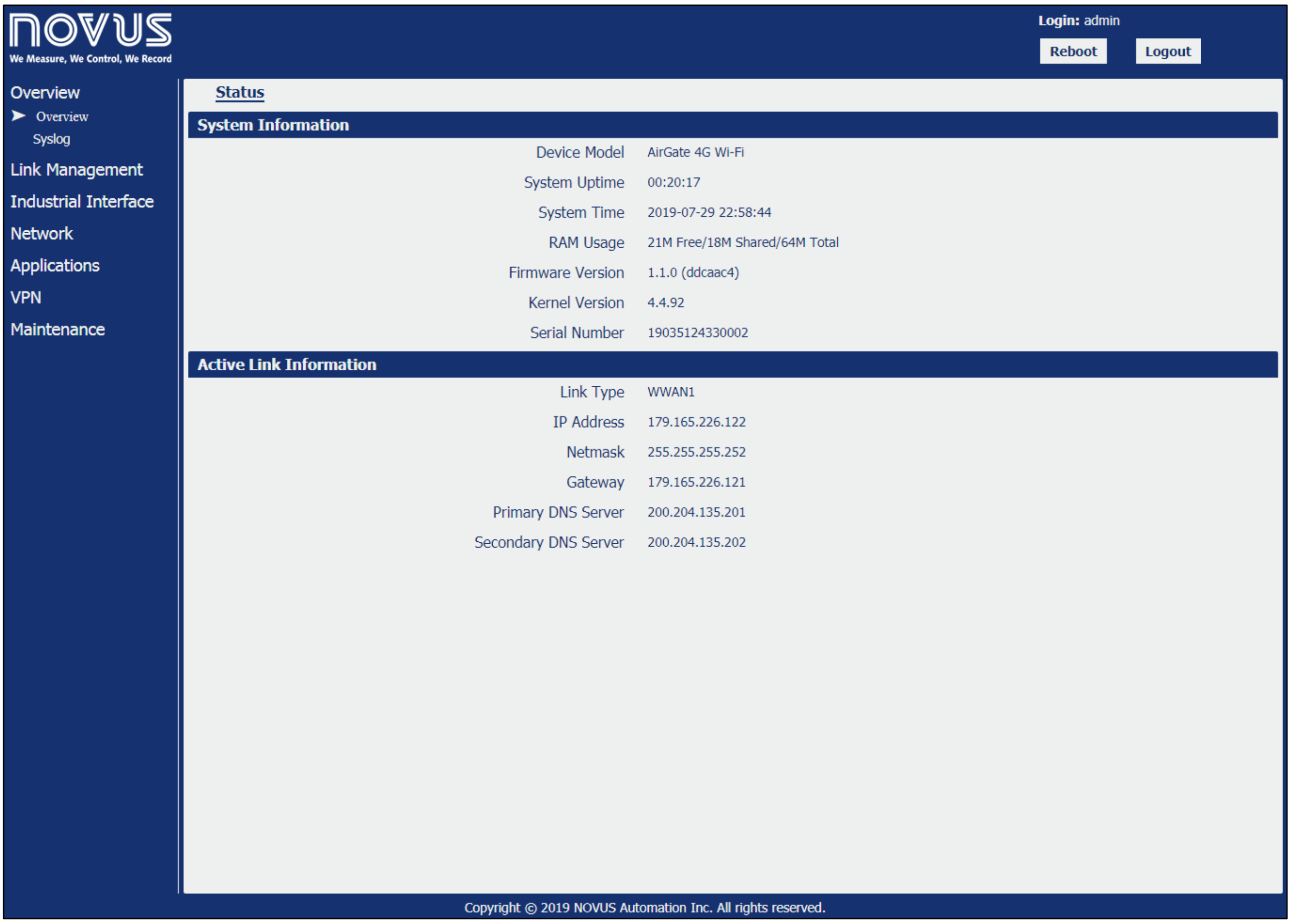
Copyright © 2019 NOVUS Automation Inc. All rights reserved.

Figure 15 - Login to Web page

5 WEB INTERFACE

5.1 WEB INTERFACE

AirGate 4G router Web interface is divided into two sections: In the left pane is the main navigation menu and on the right is the content area for each page.



System Information

Device Model	AirGate 4G Wi-Fi
System Uptime	00:20:17
System Time	2019-07-29 22:58:44
RAM Usage	21M Free/18M Shared/64M Total
Firmware Version	1.1.0 (ddcaac4)
Kernel Version	4.4.92
Serial Number	19035124330002

Active Link Information

Link Type	WWAN1
IP Address	179.165.226.122
Netmask	255.255.255.252
Gateway	179.165.226.121
Primary DNS Server	200.204.135.201
Secondary DNS Server	200.204.135.202

Copyright © 2019 NOVUS Automation Inc. All rights reserved.

Figure 16 – Home page

The navigation menu may contain fewer sections than shown here depending on which options are installed in your device.

5.1.1 WEB PAGE BUTTONS

The **AirGate 4G** configuration page contains the following buttons:

Figure 17 - Reboot and Logout buttons

- **Reboot:** Allows you to reboot the router.
- **Logout:** Allows you to logout the page.

Figure 18 - Save and Apply buttons

- **Save:** Allows you to save the settings applied to the current page.
- **Apply:** Allows you to apply the changes immediately made to the current page.

Figure 19 – Close button

- **Close:** Allows you to exit without changing the configuration on the current page.

5.2 OVERVIEW

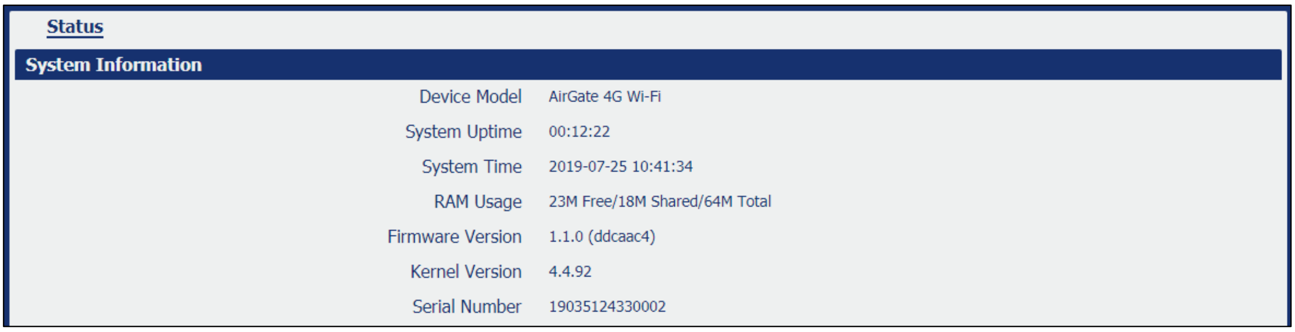
This section displays general information about the device and the system log files obtained by it.

5.2.1 STATUS

This tab allows displays information about the system and the current **AirGate 4G** connection.

5.2.1.1 SYSTEM INFORMATION

This parameter group displays information about the system. With the exception of the time format, which supports time zone setting (see section SYSTEM → GENERAL), none of them are configurable.



Status

System Information

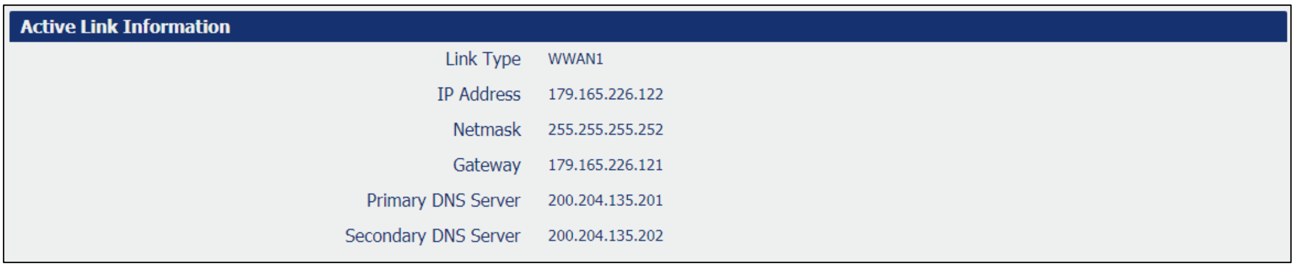
Device Model	AirGate 4G Wi-Fi
System Uptime	00:12:22
System Time	2019-07-25 10:41:34
RAM Usage	23M Free/18M Shared/64M Total
Firmware Version	1.1.0 (ddcaac4)
Kernel Version	4.4.92
Serial Number	19035124330002

Figure 20 – System information

- **Device Module:** Displays the model name of router.
- **System Uptime:** Displays the duration the system has been up in hours, minutes and seconds.
- **System Time:** Displays the current date and time.
- **RAM Usage:** Displays the RAM capacity and the available RAM memory.
- **Firmware Version:** Displays the current firmware version of router.
- **Kernel Version:** Displays the current kernel version of router.
- **Serial Number:** Display the serial number of router.

5.2.1.2 ACTIVE LINK INFORMATION

This parameter group provides information about the active **AirGate 4G** connection, which can be configured throughout the next chapters.



Active Link Information

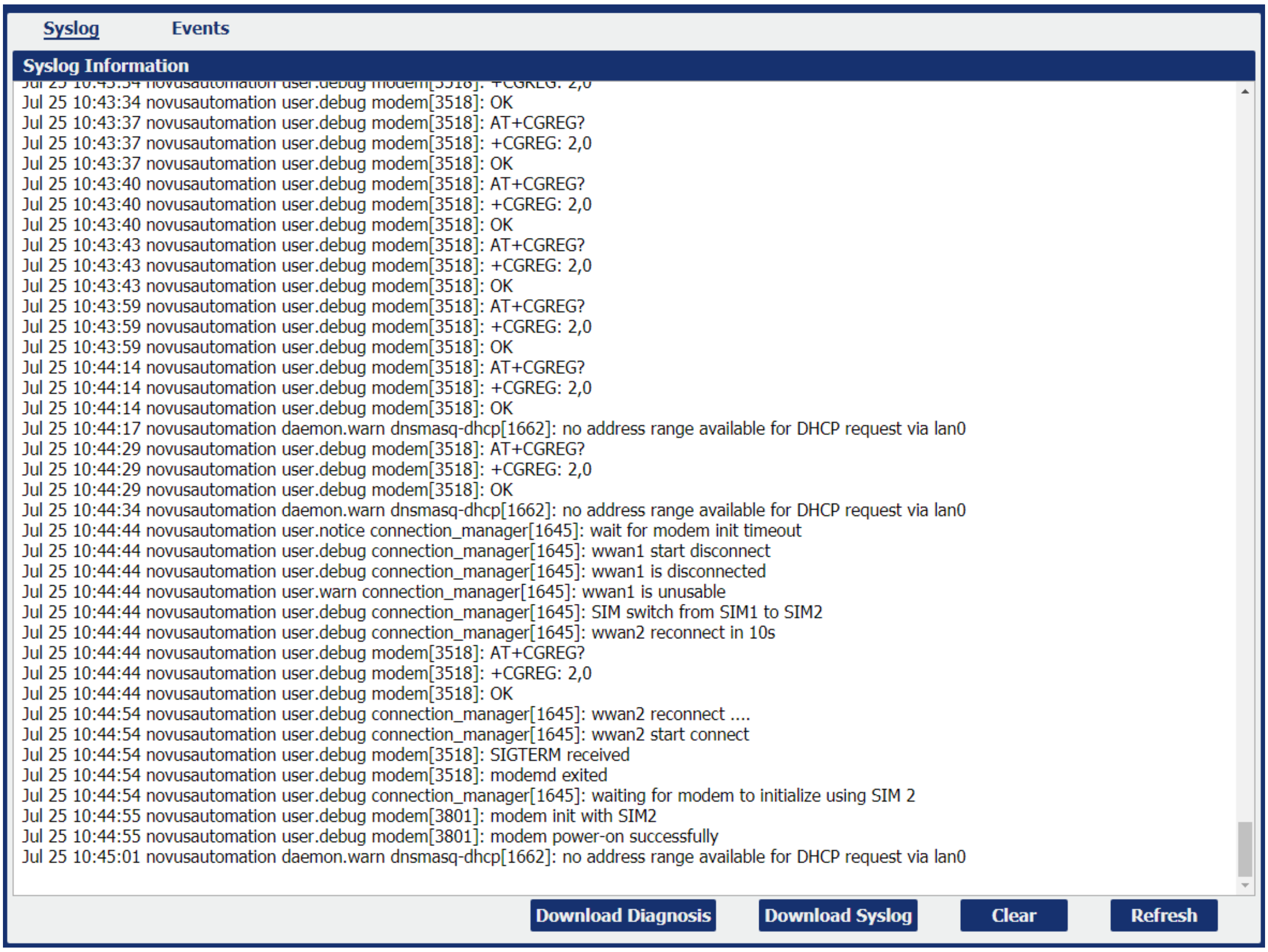
Link Type	WWAN1
IP Address	179.165.226.122
Netmask	255.255.255.252
Gateway	179.165.226.121
Primary DNS Server	200.204.135.201
Secondary DNS Server	200.204.135.202

Figure 21 – Active link information

- **Link Type:** Displays the current interface for Internet access.
- **IP Address:** Displays the IP address assigned to this interface.
- **Netmask:** Displays the subnet mask of this interface.
- **Gateway:** Displays the gateway of this interface.
- **Primary DNS Server:** Displays the primary DNS server of this interface.
- **Secondary DNS Server:** Displays the secondary DNS server of this interface.

5.2.2 SYSLOG

This feature allows you to view device system log data.



```
Jul 25 10:43:34 novusautomation user.debug modem[3518]: +CGREG: 2,0
Jul 25 10:43:34 novusautomation user.debug modem[3518]: OK
Jul 25 10:43:37 novusautomation user.debug modem[3518]: AT+CGREG?
Jul 25 10:43:37 novusautomation user.debug modem[3518]: +CGREG: 2,0
Jul 25 10:43:37 novusautomation user.debug modem[3518]: OK
Jul 25 10:43:40 novusautomation user.debug modem[3518]: AT+CGREG?
Jul 25 10:43:40 novusautomation user.debug modem[3518]: +CGREG: 2,0
Jul 25 10:43:40 novusautomation user.debug modem[3518]: OK
Jul 25 10:43:43 novusautomation user.debug modem[3518]: AT+CGREG?
Jul 25 10:43:43 novusautomation user.debug modem[3518]: +CGREG: 2,0
Jul 25 10:43:43 novusautomation user.debug modem[3518]: OK
Jul 25 10:43:59 novusautomation user.debug modem[3518]: AT+CGREG?
Jul 25 10:43:59 novusautomation user.debug modem[3518]: +CGREG: 2,0
Jul 25 10:43:59 novusautomation user.debug modem[3518]: OK
Jul 25 10:44:14 novusautomation user.debug modem[3518]: AT+CGREG?
Jul 25 10:44:14 novusautomation user.debug modem[3518]: +CGREG: 2,0
Jul 25 10:44:14 novusautomation user.debug modem[3518]: OK
Jul 25 10:44:17 novusautomation daemon.warn dnsmasq-dhcp[1662]: no address range available for DHCP request via lan0
Jul 25 10:44:29 novusautomation user.debug modem[3518]: AT+CGREG?
Jul 25 10:44:29 novusautomation user.debug modem[3518]: +CGREG: 2,0
Jul 25 10:44:29 novusautomation user.debug modem[3518]: OK
Jul 25 10:44:34 novusautomation daemon.warn dnsmasq-dhcp[1662]: no address range available for DHCP request via lan0
Jul 25 10:44:44 novusautomation user.notice connection_manager[1645]: wait for modem init timeout
Jul 25 10:44:44 novusautomation user.debug connection_manager[1645]: wwan1 start disconnect
Jul 25 10:44:44 novusautomation user.debug connection_manager[1645]: wwan1 is disconnected
Jul 25 10:44:44 novusautomation user.warn connection_manager[1645]: wwan1 is unusable
Jul 25 10:44:44 novusautomation user.debug connection_manager[1645]: SIM switch from SIM1 to SIM2
Jul 25 10:44:44 novusautomation user.debug connection_manager[1645]: wwan2 reconnect in 10s
Jul 25 10:44:44 novusautomation user.debug modem[3518]: AT+CGREG?
Jul 25 10:44:44 novusautomation user.debug modem[3518]: +CGREG: 2,0
Jul 25 10:44:44 novusautomation user.debug modem[3518]: OK
Jul 25 10:44:54 novusautomation user.debug connection_manager[1645]: wwan2 reconnect ....
Jul 25 10:44:54 novusautomation user.debug connection_manager[1645]: wwan2 start connect
Jul 25 10:44:54 novusautomation user.debug modem[3518]: SIGTERM received
Jul 25 10:44:54 novusautomation user.debug modem[3518]: modemd exited
Jul 25 10:44:54 novusautomation user.debug connection_manager[1645]: waiting for modem to initialize using SIM 2
Jul 25 10:44:55 novusautomation user.debug modem[3801]: modem init with SIM2
Jul 25 10:44:55 novusautomation user.debug modem[3801]: modem power-on successfully
Jul 25 10:45:01 novusautomation daemon.warn dnsmasq-dhcp[1662]: no address range available for DHCP request via lan0
```

Figure 22 - Syslog

- **Download Diagnosis:** Allows you to download the diagnosis file for analysis. This function will create a compressed file with extension .en. The information, however, is confidential and, if necessary, must be sent to NOVUS Technical Support.
- **Download Syslog:** Allows you to download the complete syslog since last reboot.
- **Clear:** Allows you to clear the current page syslog.
- **Refresh:** Allows you to reload the current page.

5.3 LINK MANAGEMENT

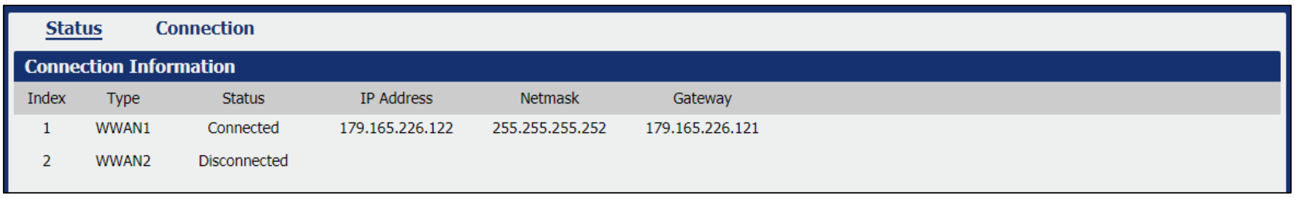
This section allows you to view information about device connection setup and management.

5.3.1 CONNECTION MANAGER

This tab allows you to view and manage the information of each connection configured for the device.

5.3.1.1 CONNECTION MANAGER → STATUS

This parameter group allows you to view information about the connections configured for the device. Each connection can be individually created, configured, or removed in the CONNECTION MANAGER → CONNECTION tab.



Status Connection

Connection Information

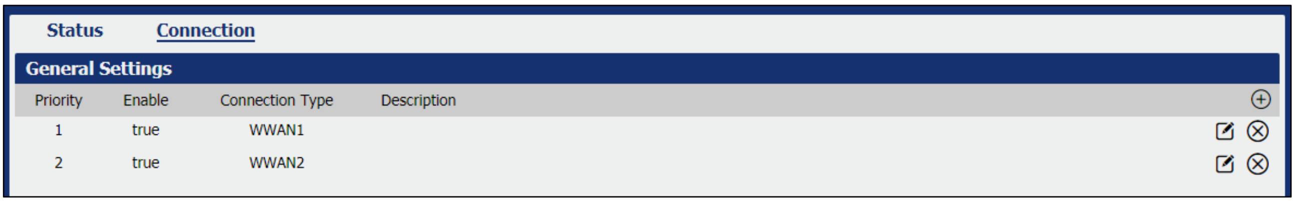
Index	Type	Status	IP Address	Netmask	Gateway
1	WWAN1	Connected	179.165.226.122	255.255.255.252	179.165.226.121
2	WWAN2	Disconnected			

Figure 23 – Connection information

- **Type:** Displays the connection interface.
- **Status:** Displays the connection status of this interface.
- **IP Address:** Displays the IP address of this interface.
- **Netmask:** Displays the netmask of this interface.
- **Gateway:** Displays the gateway of this interface. This is used for routing packets to remote networks.

5.3.1.2 CONNECTION MANAGER → CONNECTION

This parameter group allows you to add or delete connections, as well as edit parameters for connections previously created for the device.



Status Connection

General Settings

Priority	Enable	Connection Type	Description	⊕
1	true	WWAN1		✎ ⊗
2	true	WWAN2		✎ ⊗

Figure 24 – Connection: General settings

This parameter group has the following buttons:

⊕ **Button:** Allows you to add a new priority interface.

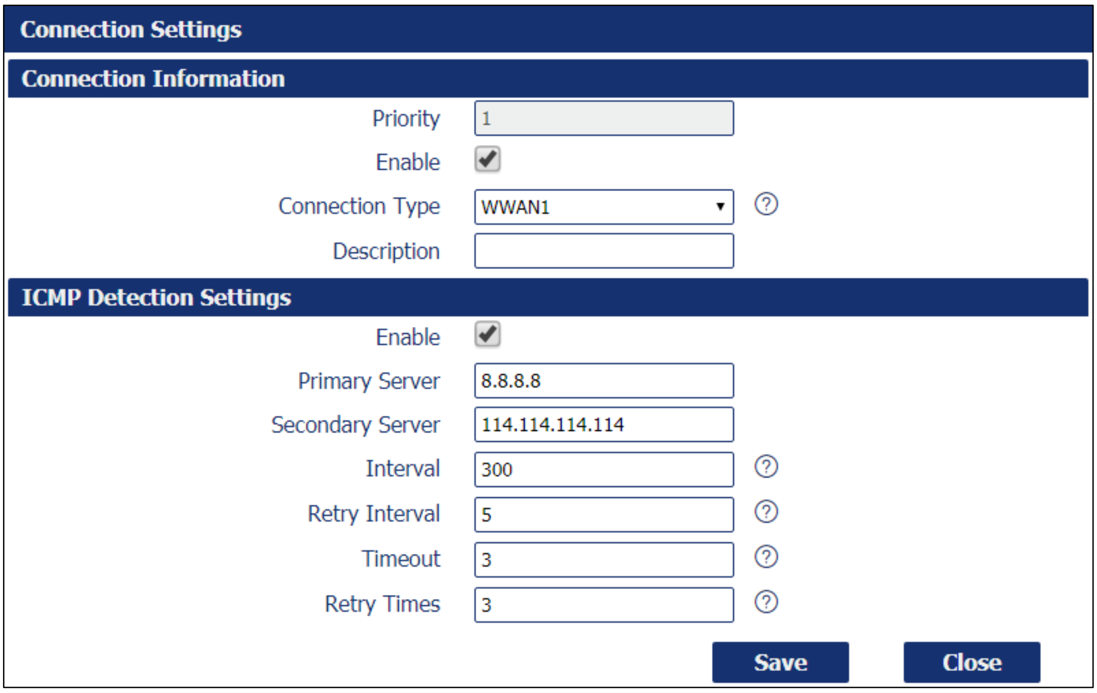
✎ **Button:** Allows you to edit current interface settings.

⊗ **Button:** Allows you to delete current interface settings.

This group displays the following parameters:

- **Priority:** Displays the priority list of default routing selection. The order of priorities will be defined by the order of creation of each connection, respecting the limit of three connections.
- **Enable:** Displays the connection enable status. Enabled connections will be displayed as "True" and disabled connections will be displayed as "False".
- **Connection Type:** Displays the name of this interface.
- **Description:** Displays the description of this connection.

As you can see in **Figure 25 –** , you can create a new connection by clicking the ⊕ button.



Connection Settings

Connection Information

Priority: 1

Enable: ☑

Connection Type: WWAN1

Description:

ICMP Detection Settings

Enable: ☑

Primary Server: 8.8.8.8

Secondary Server: 114.114.114.114

Interval: 300

Retry Interval: 5

Timeout: 3

Retry Times: 3

Figure 25 – Connection settings

GENERAL SETTINGS

This parameter group allows you to define the general connection settings.

- **Priority:** Displays current index on priority list. The order of priority will be defined by the connections creation order and cannot be manually changed.
- **Enable:** Allows you to enable or disable the connection.
- **Connection Type:** Allows you to define the connection type: "WWAN1", "WWAN2" or "WAN". It is recommended to specify the SIM1 operator link as "WWAN1" and the SIM2 operator link as "WWAN2".
- **Description:** Allows you to define a description for the connection.

ICMP DETECTION SETTINGS

This parameter group allows you to define the ICMP (Internet Control Message Protocol) protocol operation. The ICMP protocol is used to manage information about errors founded when a message is send.

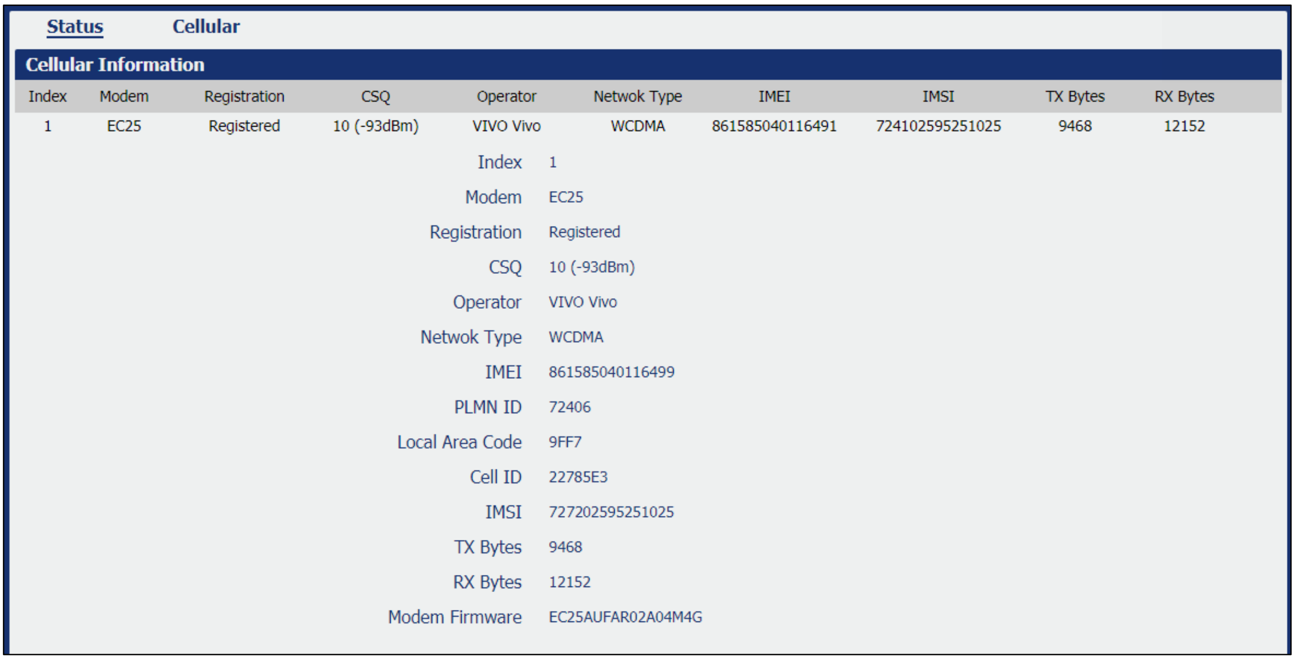
- **Enable:** Allows you to enable detection of link connection status based on pings to a specified IP address.
- **Primary Server:** Allows you to enter the primary IP address that pings will be sent to, to detect the link state. Recommend entering the IP address of known external reachable server or network (e.g. 8.8.8.8).
- **Secondary Server:** Allows you to enter the secondary IP address that pings will be sent to, when the primary server is ping failed, router would try to ping the secondary server.
- **Interval:** Allows you to enter the duration of each ICMP detection (in seconds). 1 to 1800 second interval is allowed
- **Retry Interval:** Allows you to enter the interval in seconds between each ping if no packets have been received. 1 to 300 second retry interval is allowed.
- **Timeout:** Allows you to enter a timeout period, in seconds, for the response of received pings to determine ICMP detection failures. 1 to 10 seconds timeout is allowed.
- **Retry Times:** Allows you to specify the retry times for ICMP detection. 1 to 10 seconds retry times is allowed.

5.3.2 CELLULAR

This tab allows you to view and manage the SIM card information for the device.

5.3.2.1 CELLULAR → STATUS

This parameter group allows you to view information about cellular connections configured for the device. Each cellular connection can be individually created, configured, or removed on the CELLULAR → CELLULAR tab.



Cellular Information

Index	Modem	Registration	CSQ	Operator	Netwok Type	IMEI	IMSI	TX Bytes	RX Bytes
1	EC25	Registered	10 (-93dBm)	VIVO Vivo	WCDMA	861585040116491	724102595251025	9468	12152

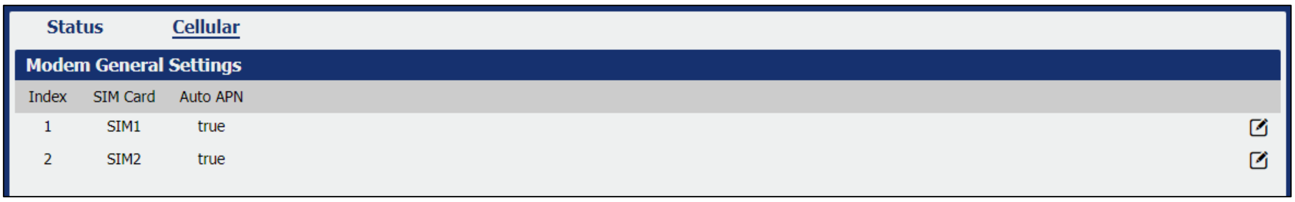
Index	1
Modem	EC25
Registration	Registered
CSQ	10 (-93dBm)
Operator	VIVO Vivo
Netwok Type	WCDMA
IMEI	861585040116499
PLMN ID	72406
Local Area Code	9FF7
Cell ID	22785E3
IMSI	727202595251025
TX Bytes	9468
RX Bytes	12152
Modem Firmware	EC25AUFAR02A04M4G

Figure 26 – Cellular information

- **Modem:** Displays the module of the modem used by this WWAN interface.
- **Registration:** Displays the registration status of SIM card.
- **CSQ:** Displays the signal strength of the carrier network.
- **Operator:** Displays the wireless network provider.
- **Network Type:** Displays the network type: "LTE" (Long Term Evolution), "UMTS" (Universal Mobile Telecommunications Service) or "CDMA" (Code Division Multiple Access).
- **IMEI:** Displays the IMEI (International Mobile Electronic Identifier). Depending on the carrier and technology used, this may be required for the carrier when activating the data contract. In some cases this will be blank.
- **PLMN ID:** Displays the current PLMN (Public Land Mobile Network) ID, including MCC (Mobile County Code), MNC (Mobile Network Code), LAC (Location Area Code) and Cell ID (Cell Identification).
- **Local Area Code:** Displays the location area code of the SIM card.
- **Cell ID:** Displays the Cell ID of the SIM card location.
- **IMSI:** International Mobile Subscriber Identity, as read from the SIM. This is the user's network subscription.
- **TX Bytes:** Displays the total bytes transmitted since the time the device was connected. **AirGate 4G** router would record this data with same SIM card. Reboot would not erase this data.
- **RX Bytes** Displays the total bytes received since the time the device was connected. **AirGate 4G** router would log this data with same SIM card. Reboot would not erase this data.
- **Modem Firmware:** Displays firmware version of the module used by the connection.

5.3.2.2 CELLULAR → CELLULAR

This parameter group allows you to configure the SIM cards parameters. **AirGate 4G** supports up to two individually configured SIM cards for 2G, 3G or 4G connection.



Modem General Settings

Index	SIM Card	Auto APN	
1	SIM1	true	✎
2	SIM2	true	✎

Figure 27 – Modem general settings

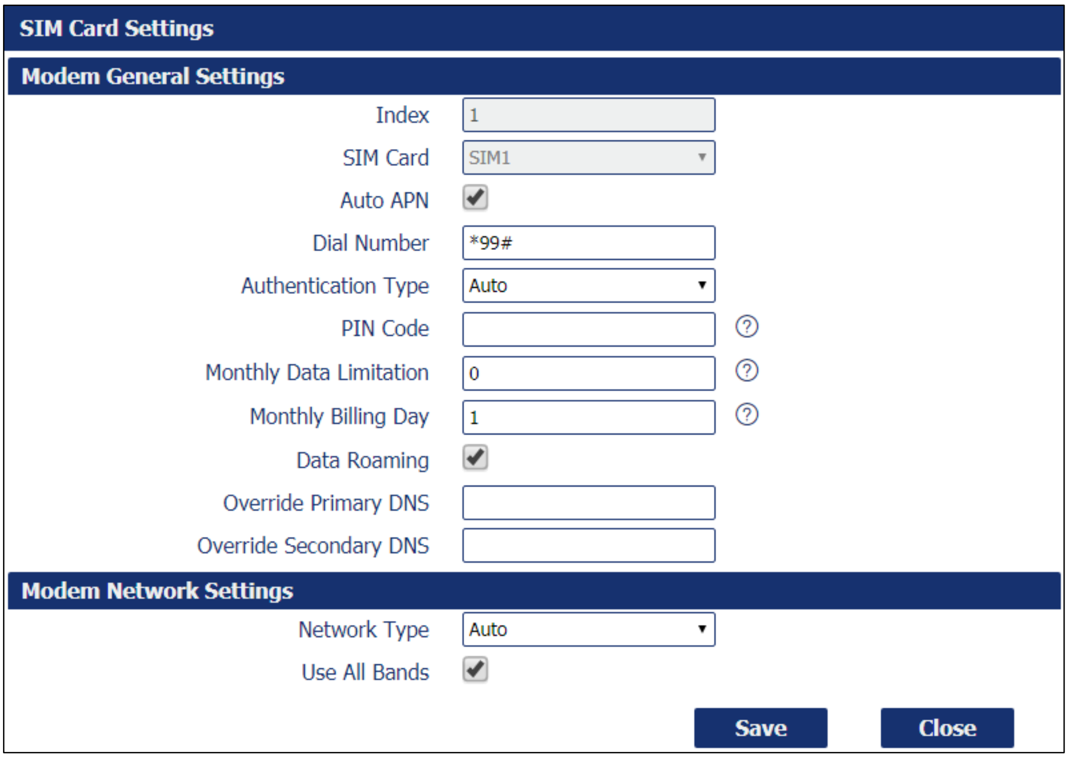
This parameter group has the following button:

✎ **Button:** Allows you to edit the settings of the selected SIM card.

This group displays the following parameters:

- **SIM Card:** Displays the SIM card support on this device.
- **Auto APN:** Displays the status of auto APN function.

As you can see in **Figure 28**, you can edit a SIM card setting by clicking the ✎ button.



SIM Card Settings

Modem General Settings

Index	1
SIM Card	SIM1 ▾
Auto APN	☑
Dial Number	*99#
Authentication Type	Auto ▾
PIN Code	
Monthly Data Limitation	0
Monthly Billing Day	1
Data Roaming	☑
Override Primary DNS	
Override Secondary DNS	

Modem Network Settings

Network Type	Auto ▾
Use All Bands	☑

Figure 28 - SIM card settings

SIM CARD GENERAL SETTINGS

- **SIM Card:** Displays the current SIM card settings.
- **Auto APN:** Allows you to enable auto checking the Access Point Name provided by the carrier.
- **APN:** You must manually add the APN to be used by the selected SIM card if **Auto APN** is disabled.
- **Username:** You must manually add the APN user to be used by the selected SIM card if **Auto APN** is disabled.
- **Password:** You must manually add the APN password to be used by the selected SIM card if **Auto APN** is disabled.
- **Dial Number:** Allows you to enter the dial number of the carrier.
- **Authentication Type:** Allows you to define the authentication method used by the carrier: "Auto", "PAP" (Password Authentication Protocol) or "CHAP" (Challenge Handshake Authentication Protocol).
- **PIN Code:** Allows you to enter a 4-8 characters PIN code to unlock the SIM.
- **Monthly Data Limitation:** Allows you to enter the data total amount for SIM card. SIM card switchover when data reach limitation. There is no limitation if set to "0".
- **Monthly Billing Day:** Allows you to enter the date of renew data amount every month. This parameter must remain disabled if set to "0".
- **Data Roaming:** Allows you to enable or disable the data roaming function on the router.
- **Override Primary DNS:** Allows you to enter the primary DNS server will override the automatically obtained DNS.
- **Override Secondary DNS:** Allows you to enter the secondary DNS server will override the automatically obtained DNS.

SIM CARD NETWORK SETTINGS

- **Network Type:** Allows you to define the network type: "Auto", "2G Only", "2G First", "3G Only", "3G First", "4G Only" or "4G First".
- **Use All Bands:** Allows you to enable all bands selection or choose specified bands. Otherwise you can manually select the bands to be used.

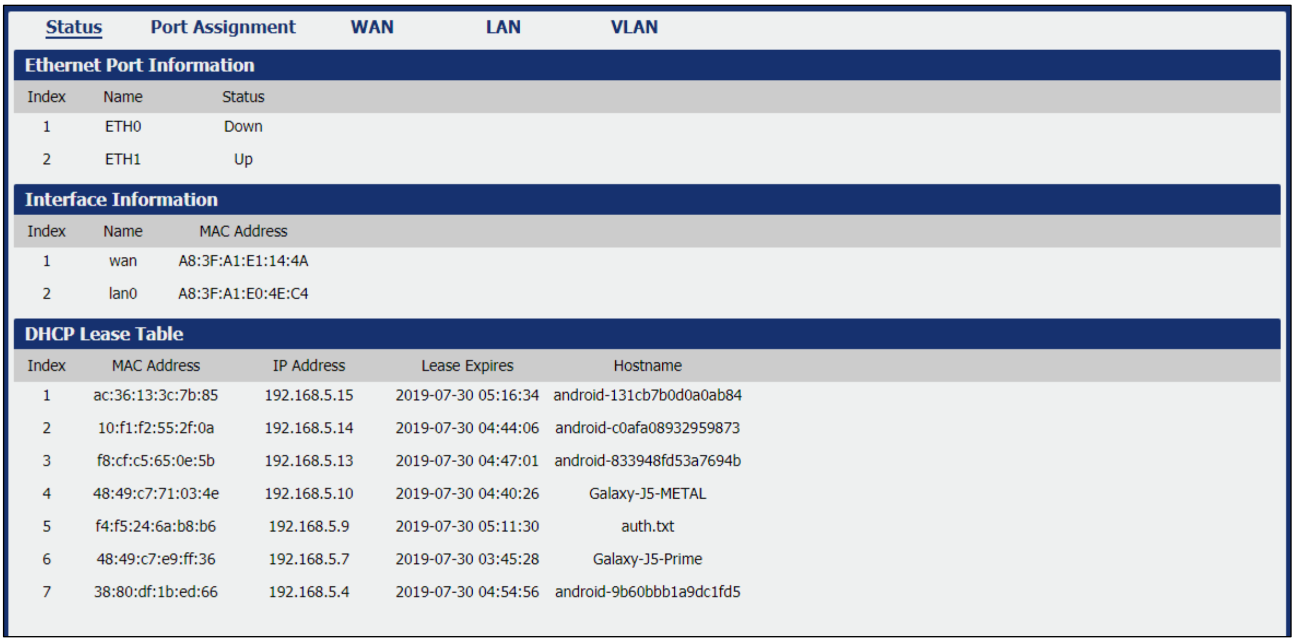
5.3.3 ETHERNET

This tab allows you to view and manage the information of Ethernet connection for the device.

5.3.3.1 ETHERNET → STATUS

This parameter group allows you to view general information about the device's Ethernet connection, such as the connection status of the Ethernet ports and the MAC address of the configured Ethernet interfaces.

As seen below, the IP addresses assigned by the DHCP server will be presented in a table. This table, created automatically by the DHCP server, is intended to store the IP address and MAC address of the receiving device - which will prevent the same IP from being delivered to the same device. Thus, the displayed lease period refers to the lease time of the IP addresses assigned to each device by the DHCP server.



Ethernet Port Information

Index	Name	Status
1	ETH0	Down
2	ETH1	Up

Interface Information

Index	Name	MAC Address
1	wan	A8:3F:A1:E1:14:4A
2	lan0	A8:3F:A1:E0:4E:C4

DHCP Lease Table

Index	MAC Address	IP Address	Lease Expires	Hostname
1	ac:36:13:3c:7b:85	192.168.5.15	2019-07-30 05:16:34	android-131cb7b0d0a0ab84
2	10:f1:f2:55:2f:0a	192.168.5.14	2019-07-30 04:44:06	android-c0afa08932959873
3	f8:cf:c5:65:0e:5b	192.168.5.13	2019-07-30 04:47:01	android-833948fd53a7694b
4	48:49:c7:71:03:4e	192.168.5.10	2019-07-30 04:40:26	Galaxy-J5-METAL
5	f4:f5:24:6a:b8:b6	192.168.5.9	2019-07-30 05:11:30	auth.txt
6	48:49:c7:e9:ff:36	192.168.5.7	2019-07-30 03:45:28	Galaxy-J5-Prime
7	38:80:df:1b:ed:66	192.168.5.4	2019-07-30 04:54:56	android-9b60bbb1a9dc1fd5

Figure 29 – Ethernet status

ETHERNET PORT INFORMATION

- **Name:** Displays the port physical connected states: "ETH0" or "ETH1".
- **Status:** Displays the status of the Ethernet port: If enabled, its status will be "Up". If disabled, its status will be "Down".

INTERFACE INFORMATION

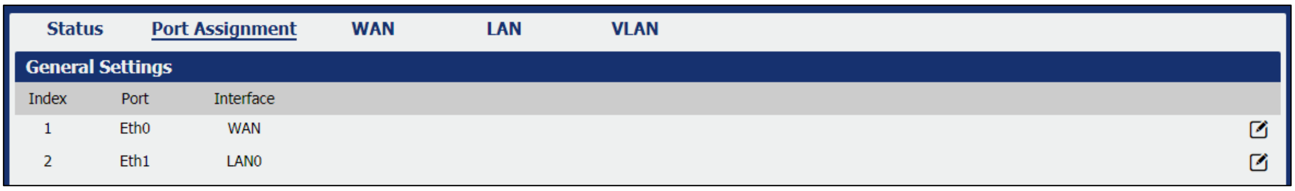
- **Name:** Displays the identification name of the Ethernet interface.
- **MAC Address:** Displays the MAC address of the Ethernet interface.
- **IP Address:** Displays the IP address of the Ethernet interface.

DHCP LEASE TABLE

- **MAC Address:** Displays the MAC address assigned to the device.
- **IP Address:** Displays the IP address assigned to the device.
- **Lease Expires:** Displays the lease time of the IP address assigned by the DHCP server.
- **Hostname:** Displays the hostname assigned to the device.

5.3.3.2 ETHERNET → PORT ASSIGNMENT

This group of parameters allows you to edit the Ethernet ports of the device. **AirGate 4G** supports up to two individually configured Ethernet ports.



General Settings

Index	Port	Interface	
1	Eth0	WAN	✎
2	Eth1	LAN0	✎

Figure 30 – Port assignment

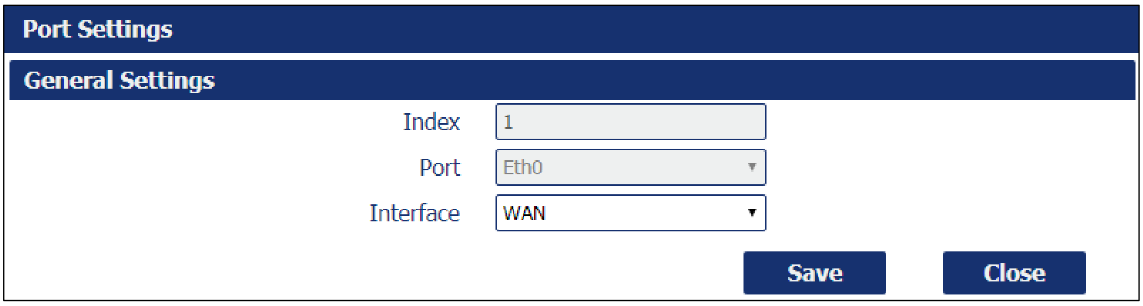
This parameter group has the following button:

✎ **Buttons:** Allows you to edit the settings of the selected Ethernet port.

This group displays the following parameters:

- **Port:** Displays the port states and numbers of this device: "ETH0" or "ETH1".
- **Interface:** Displays the interface configured for the Ethernet port: "LAN0", "LAN1" or "WAN".

As you can see in **Figure 25 –** , you can edit the Ethernet port setting by clicking the ✎ button.



Port Settings

General Settings

Index: 1

Port: Eth0

Interface: WAN

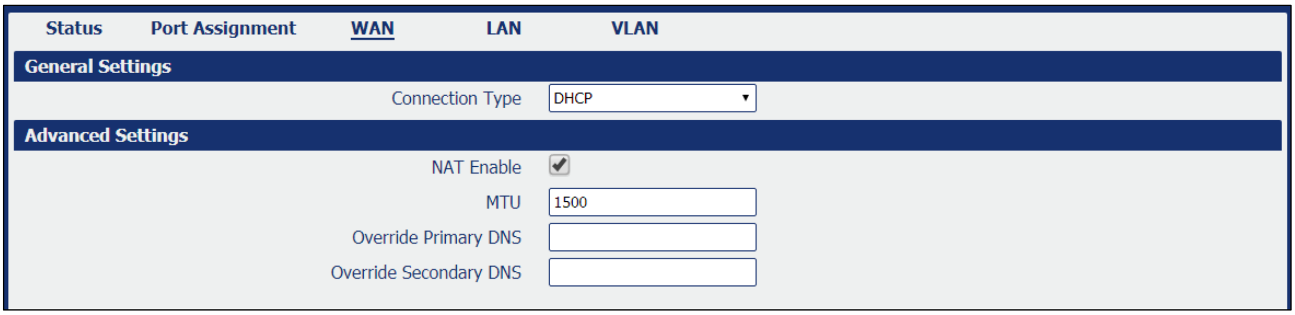
Figure 31 – Ethernet port settings

- **Port:** Displays the Ethernet port name configured.
- **Interface:** Allows you to configure an interface to the Ethernet port: "LAN0", "LAN1" or "WAN".

In order to be able to configure an interface as WAN, a configured LAN interface must already exist.

5.3.3.3 ETHERNET → WAN

This group of parameters allows you to edit the settings of the WAN (Wide Area Network) connection, used to cover a larger area, as opposed to the LAN (Local Area Network) connection.



General Settings

Connection Type: DHCP

Advanced Settings

NAT Enable: ☑

MTU: 1500

Override Primary DNS:

Override Secondary DNS:

Figure 32 – WAN configuration: DHCP

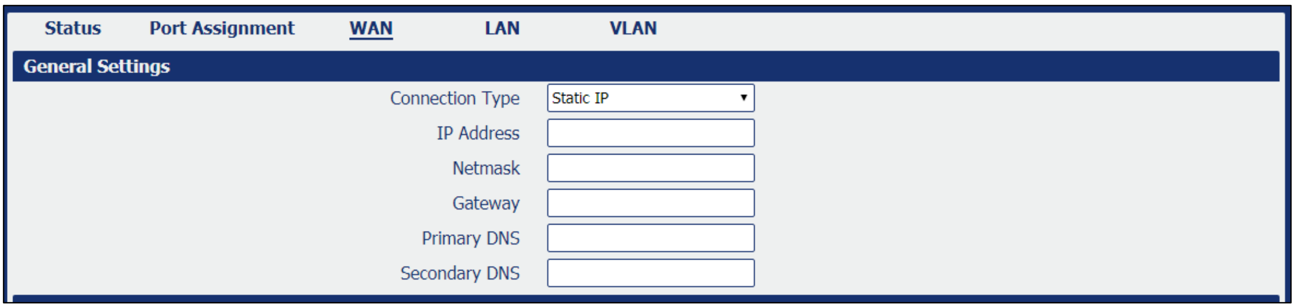
GENERAL SETTINGS

- **Connection Type:** Allows you to define the connection type: "DHCP", "Static IP" or "PPPoE" (Point-to-Point Protocol over Internet). In this case, "DHCP", which will allow the external DHCP server to assign an IP address to this device.

ADVANCED SETTINGS

- **NAT Enable:** Allows you to enable or disable NAT (Network Address Translation).
- **MTU:** Allows you to define the maximum transmission device. In most cases you should leave the default value of 1024.
- **Override Primary DNS:** Allows you to enter the primary DNS server will override the automatically obtained DNS.
- **Override Secondary DNS:** Allows you to enter the secondary DNS server will override the automatically obtained DNS.

If the **Connection Type** parameter is set to "Static IP", the following parameters will be displayed:



General Settings

Connection Type: Static IP

IP Address:

Netmask:

Gateway:

Primary DNS:

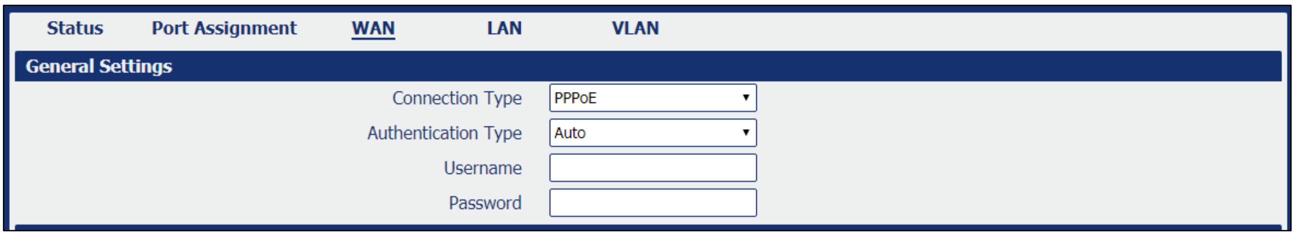
Secondary DNS:

Figure 33 – WAN configuration: Static IP

- **Connection Type** Allows you to define the connection type: "DHCP", "Static IP" or "PPPoE" (Point-to-Point Protocol over Internet). In this case "Static IP", which will allow the IP to be set manually.
- **IP Address:** Allows you to enter an IP address to be used for the WAN connection.
- **Netmask:** Allows you to enter a netmask to be used for the WAN connection.
- **Gateway:** Allows you to enter a gateway to be used for the WAN connection.
- **Primary DNS:** Allows you to enter a primary DNS to be used for the WAN connection.
- **Secondary DNS:** Allows you to enter a secondary DNS to be used for the WAN connection.

The **Advanced Settings** section parameters are the same as above and must be filled in the same way.

If the **Connection Type** parameter is set to "PPPoE" (Point-to-Point Protocol over Internet), the following parameters will be displayed:



General Settings

Connection Type	PPPoE ▾
Authentication Type	Auto ▾
Username	
Password	

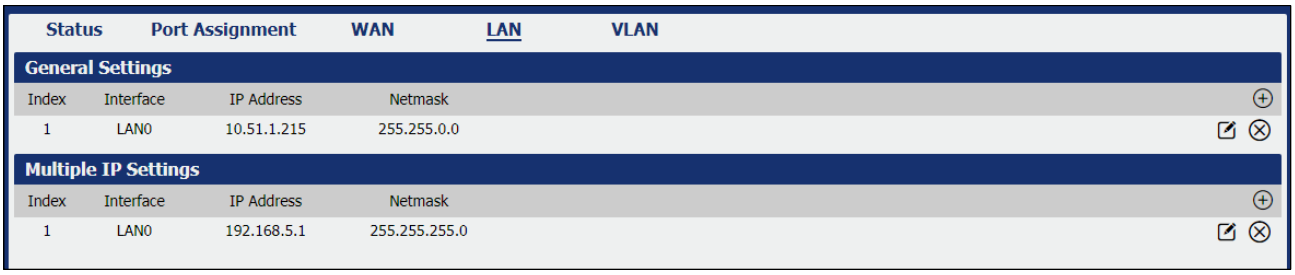
Figure 34 – WAN configuration: PPPoE

- **Connection Type:** Allows you to define the connection type: "DHCP", "Static IP" or "PPPoE" (Point-to-Point Protocol over Internet). In this case, "PPPoE".
- **Authentication Type:** Allows you to define the type of authentication to be used by the WAN connection: "Auto", "PAP" (Password Authentication Protocol) or "CHAP" (Challenge Handshake Authentication Protocol).
- **Username:** Allows you to enter a username to be used by the WAN connection.
- **Password:** Allows you to enter a password to be used by the WAN connection.

The **Advanced Settings** section parameters are the same as above and must be filled in the same way.

5.3.3.4 ETHERNET → LAN

This group of parameters allows you to define the settings of the LAN (Local Area Network) connection, a local area network designed for smaller areas, as opposed to the WAN (Wide Area Network) connection.



General Settings

Index	Interface	IP Address	Netmask	⊕
1	LAN0	10.51.1.215	255.255.0.0	✎ ⊗

Multiple IP Settings

Index	Interface	IP Address	Netmask	⊕
1	LAN0	192.168.5.1	255.255.255.0	✎ ⊗

Figure 35 – LAN settings

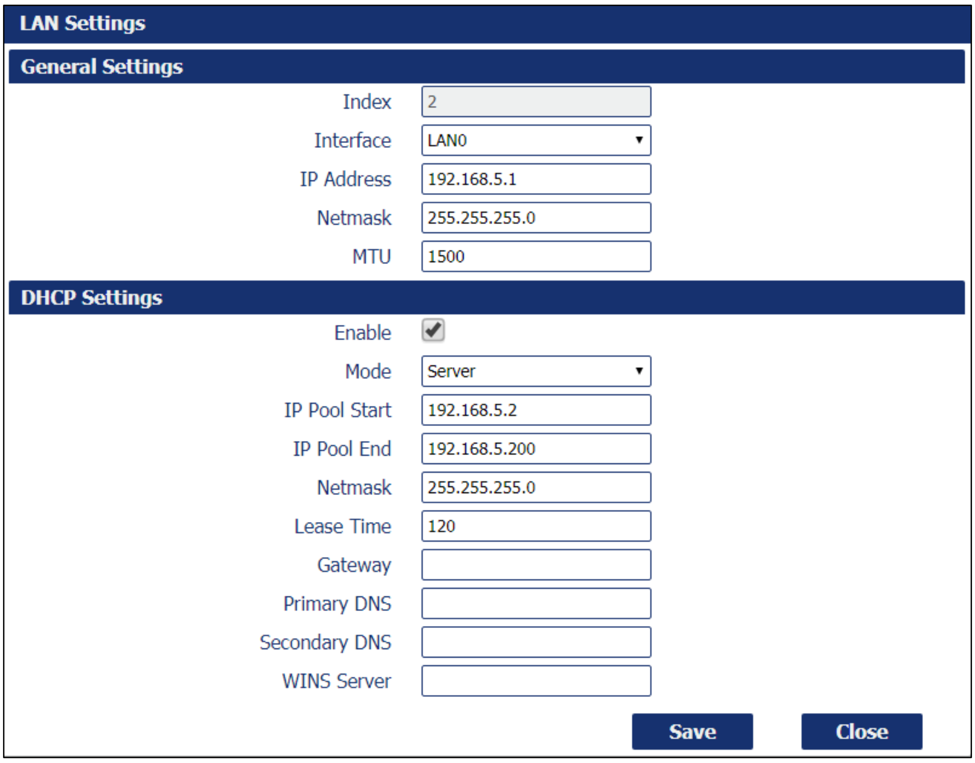
This parameter group has the following buttons:

⊕ **Button:** Allows you to add a new LAN connection.

✎ **Button:** Allows you to edit the current LAN connection settings.

⊗ **Button:** Allows you to delete the current LAN connection settings.

As you can see in **Figure 36**, you can create a new LAN setting by clicking the ⊕ button.



LAN Settings

General Settings

Index	2
Interface	LAN0
IP Address	192.168.5.1
Netmask	255.255.255.0
MTU	1500

DHCP Settings

Enable	☑
Mode	Server
IP Pool Start	192.168.5.2
IP Pool End	192.168.5.200
Netmask	255.255.255.0
Lease Time	120
Gateway	
Primary DNS	
Secondary DNS	
WINS Server	

Figure 36 – LAN settings

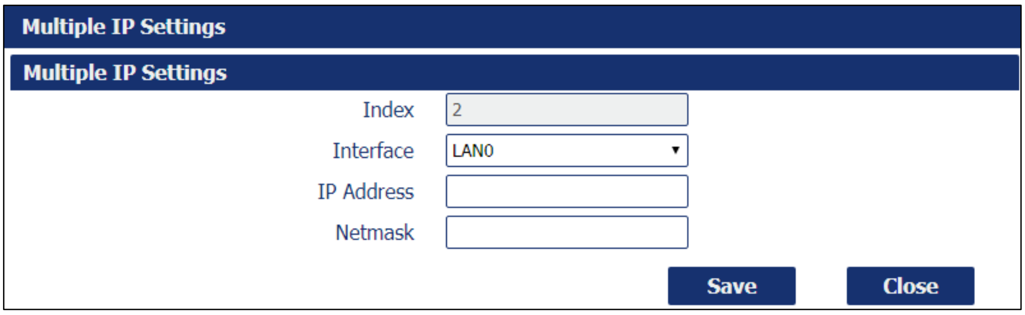
GENERAL SETTINGS

- **Interface:** Allows you to select the configure LAN port of this subnet.
- **IP Address:** Allows you to enter LAN IP address for this interface.
- **Netmask:** Allows you to enter the netmask for this subnet.
- **MTU:** Allows you to define the maximum packet size allowed to be transmitted. Should be left as default value of 1500 in most cases.

DHCP SETTINGS

- **Enable:** Allows you to enable or disable the DHCP feature of the current LAN port.
- **Mode:** Allows you to select the DHCP working mode: "Server" or "Relay".
- **Relay Server:** Allows you to enter the IP address of DHCP relay server.
- **IP Pool Start:** External LAN devices connected to this device will be assigned IP address in this range when DHCP is enabled. This is the beginning of the pool of IP addresses.
- **IP Pool End:** External LAN devices connected to this device will be assigned IP address in this range when DHCP is enabled. This is the end of the pool of IP addresses.
- **Netmask:** Subnet mask of the IP address obtained by DHCP clients from DHCP server.
- **Lease Time:** The lease time of the IP address obtained by DHCP clients from DHCP server.
- **Gateway:** The gateway address obtained by DHCP clients from DHCP server.
- **Primary DNS:** Primary DNS server address obtained by DHCP clients from DHCP server.
- **Secondary DNS:** Secondary DNS server address obtained by DHCP clients from DHCP server.
- **WINS Server:** Windows Internet Naming Service obtained by DHCP clients from DHCP server.

As you can see in **Figure 37**, you can create multiple IP settings by clicking the ⊕ button.



Multiple IP Settings

Multiple IP Settings

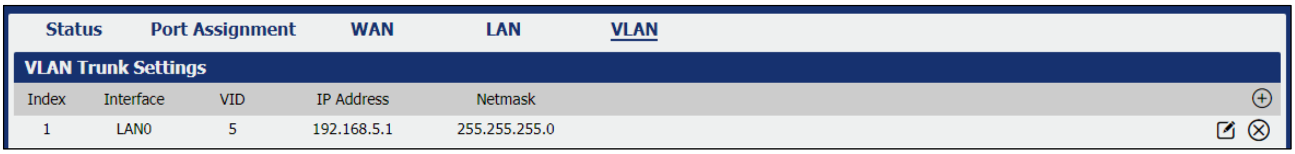
Index	2
Interface	LAN0 ▾
IP Address	
Netmask	

Figure 37 – Multiple IP settings

- **Interface:** Allows you to define a LAN port to be created.
- **IP Address:** Allows you to define an IP address for this network.
- **Netmask:** Allows you to define a netmask to be used.

5.3.3.5 ETHERNET → VLAN

This parameter group defines the VLAN (Virtual LAN) connection settings, a virtual local area network that enables physical network segmentation and grouping of multiple machines according to specific criteria.



VLAN Trunk Settings

Index	Interface	VID	IP Address	Netmask	⊕
1	LAN0	5	192.168.5.1	255.255.255.0	✎ ⊗

Figure 38 – VLAN Trunk settings

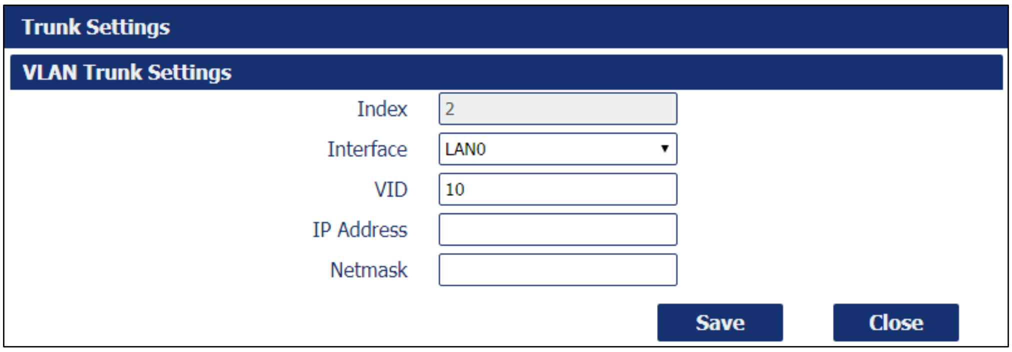
This parameter group has the following buttons:

⊕ **Button:** Allows you to add a new VLAN connection.

✎ **Button:** Allows you to edit the current VLAN connection.

⊗ **Button:** Allows you to delete the current VLAN connection.

As you can see in **Figure 39**, you can create a new VLAN connection by clicking the ⊕ button.



Trunk Settings

VLAN Trunk Settings

Index	2
Interface	LAN0 ▾
VID	10
IP Address	
Netmask	

Figure 39 – Create a new VLAN connection

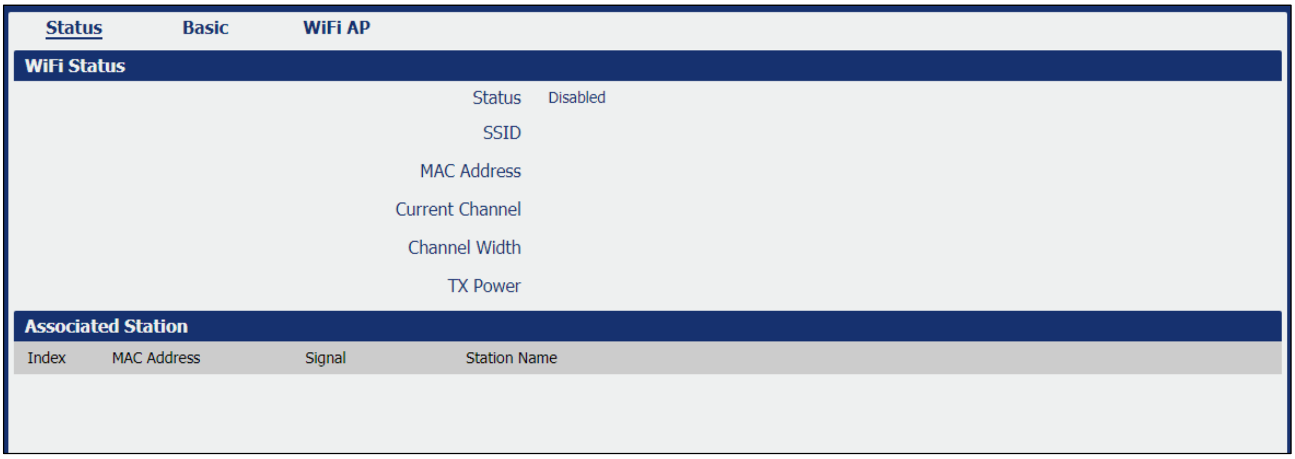
- **Interface:** Allows you to select the LAN port for VLAN trunk.
- **VID:** Allows you to define the VLAN ID for VLAN trunk.
- **IP Address:** Allows you to enter IP address for this VLAN trunk.
- **Netmask:** Allows you to enter subnet mask for this VLAN trunk.

5.3.4 WI-FI

This section allows you to view and manage information about the Wi-Fi connection and how the Wi-Fi interface works.

5.3.4.1 WI-FI → STATUS

This parameter group allows you to view information about the Wi-Fi connection and computers connected to the Wi-Fi network. In the section WI-FI → BASIC it is possible to define the operation mode of the Wi-Fi connection and to configure the other parameters.



WiFi Status

Status	Disabled
SSID	
MAC Address	
Current Channel	
Channel Width	
TX Power	

Associated Station

Index	MAC Address	Signal	Station Name

Figure 40 – Wi-Fi status

WI-FI STATUS

- **Status:** Displays the Wi-Fi connection status.
- **SSID:** Display the SSID (Service Set Identifier), that is, the identifier name assigned to the Wi-Fi connection.
- **MAC Address:** Displays the MAC address of the Wi-Fi connection.
- **Current Channel:** Displays the current channel of the Wi-Fi connection.
- **Channel Width:** Displays the current width of the Wi-Fi connection.
- **TX Power:** Displays TX power (in dBm) as configured for the Wi-Fi connection.

ASSOCIATED STATION

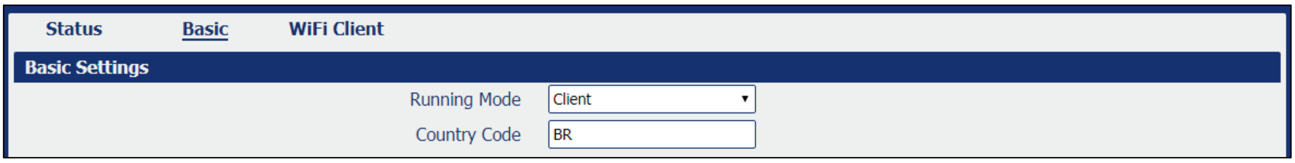
- **MAC Address:** Displays the MAC address of the device connected to the Wi-Fi network.
- **Signal:** Displays the quality of the Wi-Fi signal obtained by the computer connected to the network.
- **Station Name:** Displays the name of the workstation connected to the Wi-Fi network.

5.3.4.2 WI-FI → BASIC

This parameter group allows you to configure how the Wi-Fi connection of the device works. **AirGate 4G** can be configured to function as a Wi-Fi Client or as a Wi-Fi Access Point, but does not support both configurations simultaneously.

If the device is configured as "Access Point", proceed to chapter WI-FI → WI-FI AP.

If the device is configured as "Client", proceed to the chapter WI-FI → WI-FI CLIENT.



Basic Settings

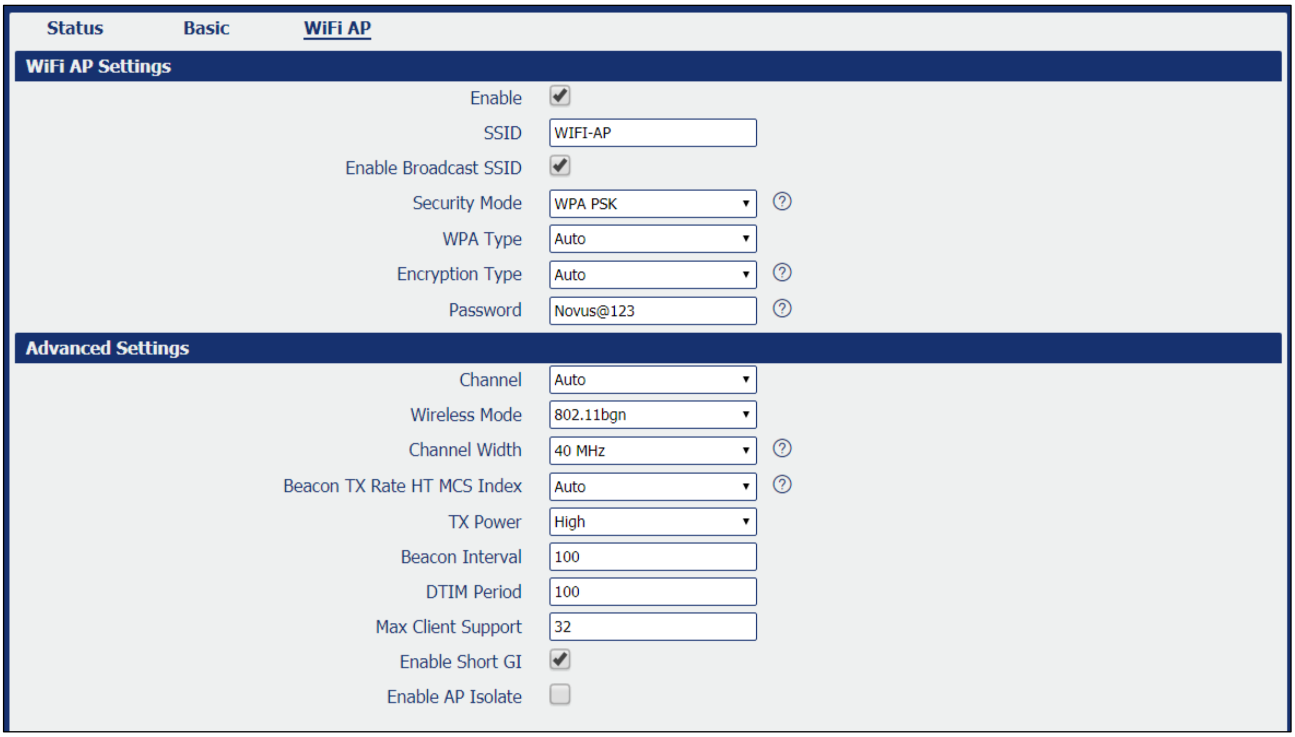
Running Mode	Client
Country Code	BR

Figure 39 – Basic settings

- **Running Mode:** Allows you to select the running mode of Wi-Fi connection: "Access Point" or "Client".
- **County Code:** Allows you to enter the country where the device is located.

5.3.4.3 WI-FI → WI-FI AP

This parameter group allows you to edit the Wi-Fi access point settings of the device.



WiFi AP Settings

Enable	☑
SSID	WIFI-AP
Enable Broadcast SSID	☑
Security Mode	WPA PSK
WPA Type	Auto
Encryption Type	Auto
Password	Novus@123

Advanced Settings

Channel	Auto
Wireless Mode	802.11bgn
Channel Width	40 MHz
Beacon TX Rate HT MCS Index	Auto
TX Power	High
Beacon Interval	100
DTIM Period	100
Max Client Support	32
Enable Short GI	☑
Enable AP Isolate	□

Figure 42 – Wi-Fi Access Point

WI-FI AP SETTINGS

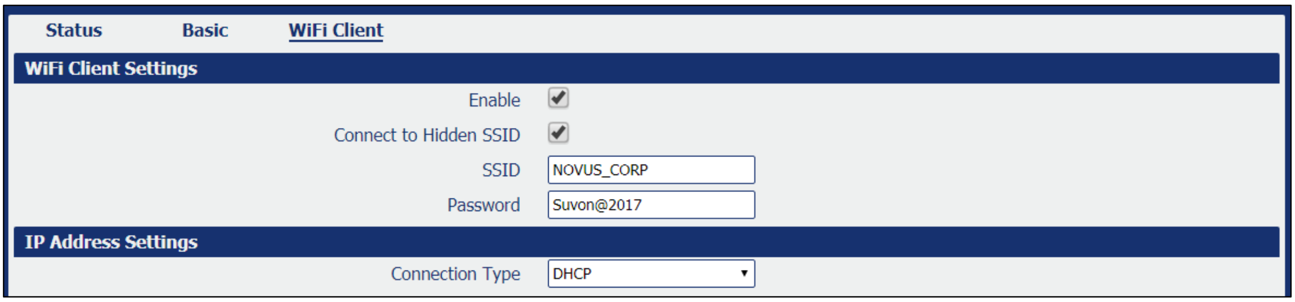
- **Enable:** Allows you to enable or disable the Wi-Fi interface.
- **SSID:** Allows you to define the SSID (Service Set Identifier), that is, the identifier name assigned to the Wi-Fi connection. Devices connected to the **AirGate 4G** Wi-Fi access will identify the Access Point by this SSID.
- **Enable Broadcast SSID:** Allows you to enable or disable the SSID broadcast. When this function is disabled, other wireless devices cannot find the SSID, and users have to enter the SSID manually.
- **Security Mode:** Allows you to select the connection security mode: "None", "WEP" or "WPA PSK".
- **WPA Type:** Allows you to select the WPA connection: "Auto", "WPA" or "WPA2".
- **Encryption Type:** Allows you to select the connection encryption type: "Auto", "TKIP" or "CCMP". Because these options depend on the authentication method selected, some options will not be available.
- **Password:** Allows you to enter the pre-shared key of WEP/WPA encryption.

ADVANCED SETTINGS

- **Channel:** Allows you to select the Wi-Fi channel to be transmitted. If there are other Wi-Fi devices in the area, **AirGate 4G** should be set to a different channel than the other access points. Channels available for selection depend on the selected Band.
- **Wireless Mode:** Allows you to select the Wi-Fi 802.11 mode: "B", "G" or "N". Available selections depend on selected Band.
- **Chanel Width:** Allows you to select the width of the Wi-Fi channel. 20 MHz will limit the channel to 20 MHz wide; 20/40 MHz will enable the use of a 40 MHz wide channel when available.
- **Beacon TX Rate HT MCS Index:** Modulation and Coding Scheme, the MCS modulation coding table is a representation proposed by 802.11n to characterize the communication rate of the WLAN. The MCS takes the factors affecting the communication rate as the columns of the table and uses the MCS index as a row to form a rate table.
- **TX Power:** Allows you to select the transmission power for the access point: "High", "Medium" or "Low".
- **Beacon Interval:** Allows you to enter the interval of time in which the router AP broadcasts a beacon which is used for wireless network authentication.
- **DTIM Period:** Allows you to enter the delivery traffic indication message period and the router AP will multicast the data according to this period.
- **Max Client Support:** Allows you to enter the maximum number of clients to access when the router is configured as access point.
- **Enable Short GI:** Allows you to enable or disable Short GI (guard interval), providing a long buffer time for signal delay.
- **Enable AP Isolate:** Allows you to enable or disable access point isolate. The route will isolate all connected wireless devices.

5.3.4.4 WI-FI → WI-FI CLIENT

This parameter group allows you to edit the Wi-Fi Client mode settings of the device.



WiFi Client Settings

Enable ☑

Connect to Hidden SSID ☑

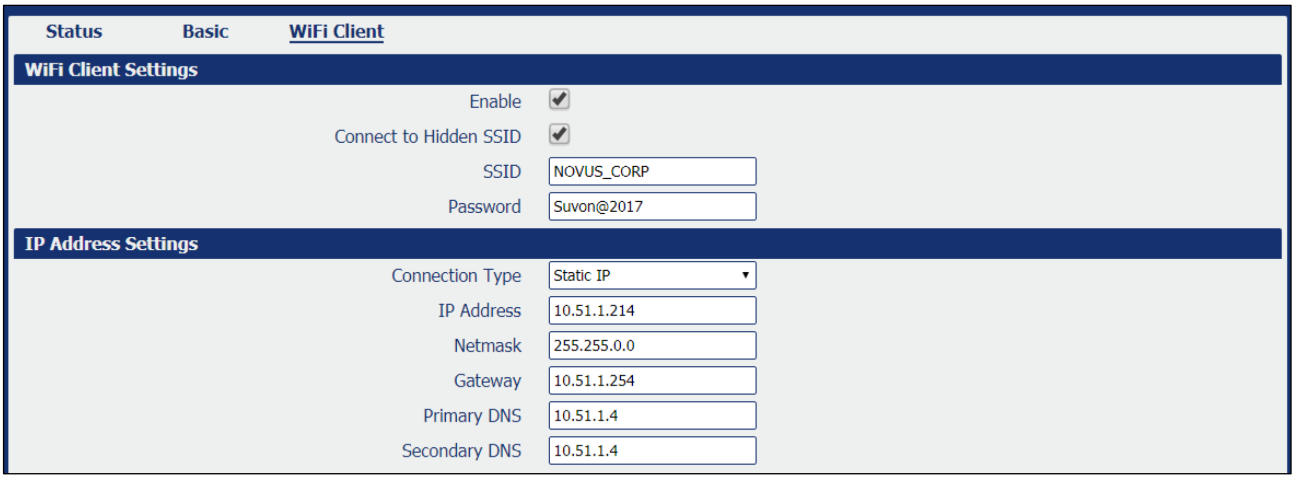
SSID: NOVUS_CORP

Password: Suvon@2017

IP Address Settings

Connection Type: DHCP

Figure 40 - Wi-Fi client: DHCP



WiFi Client Settings

Enable ☑

Connect to Hidden SSID ☑

SSID: NOVUS_CORP

Password: Suvon@2017

IP Address Settings

Connection Type: Static IP

IP Address: 10.51.1.214

Netmask: 255.255.0.0

Gateway: 10.51.1.254

Primary DNS: 10.51.1.4

Secondary DNS: 10.51.1.4

Figure 44 - Wi-Fi client: Static IP

WI-FI CLIENT SETTINGS

- **Enable:** Allows you to enable or disable the Wireless interface.
- **Connect to Hidden SSID:** Allows you to enable or disable connect to hidden SSID.
- **SSID:** Allows you to enter the password of external access point.
- **Password:** Allows you to enter the password of external access point.

IP ADDRESS SETTINGS

- **Connection Type:** Allows you to select the connection type: "DHCP Client" or "Static IP".
- **IP Address:** Allows you to enter the static address for this interface. It must be on the same subnet as the gateway.
- **Netmask:** Allows you to define the netmask to be assigned by the gateway.
- **Gateway:** Allows you to enter the IP address of the gateway.
- **Primary DNS:** Allows you to enter the primary DNS server, which will override the automatically obtained DNS.
- **Secondary DNS:** Allows you to enter the secondary DNS server, which will override the automatically obtained DNS.

5.4 INDUSTRIAL INTERFACE

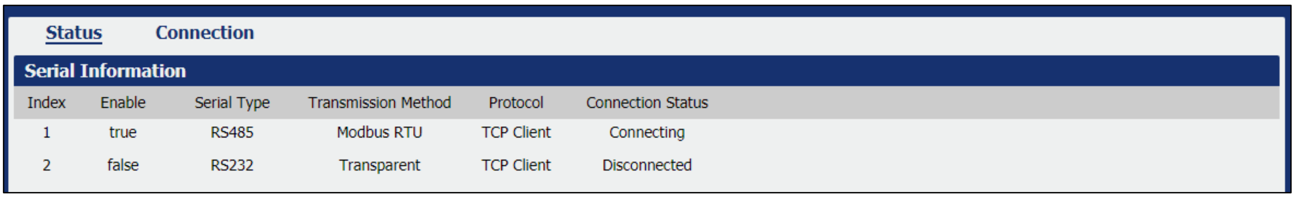
This section shows information about configuring RS232 and RS485 interfaces and device digital input and output.

5.4.1 SERIAL

This section allows you to view and manage information about device serial connections.

5.4.1.1 SERIAL → STATUS

This parameter group allows you to view information about device serial interfaces.



Serial Information

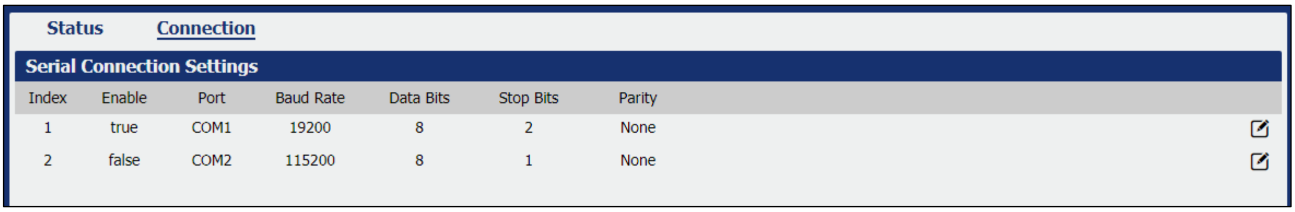
Index	Enable	Serial Type	Transmission Method	Protocol	Connection Status
1	true	RS485	Modbus RTU	TCP Client	Connecting
2	false	RS232	Transparent	TCP Client	Disconnected

Figure 45 – Serial information

- **Enable:** Displays the interface serial status.
- **Serial Type:** Displays the serial type of the COM port.
- **Transmission Method:** Displays the transmission method of the serial port.
- **Protocol:** Displays the protocol of the serial port.
- **Connection Status:** Displays the connection status of the serial port.

5.4.1.2 SERIAL → CONNECTION

This parameter group allows you to view information about device COM port connections.



Serial Connection Settings

Index	Enable	Port	Baud Rate	Data Bits	Stop Bits	Parity	
1	true	COM1	19200	8	2	None	✎
2	false	COM2	115200	8	1	None	✎

Figure 46 – Serial connection settings

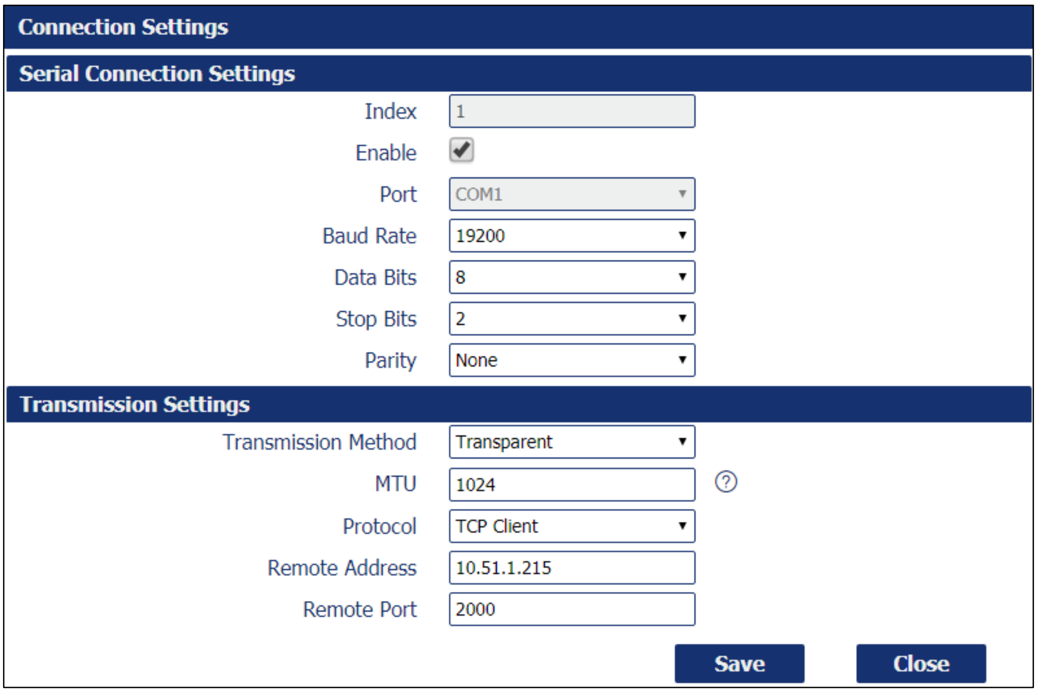
This parameter group has the following buttons:

✎ **Button:** Allows you to edit the settings of the serial port.

This group displays the following parameters:

- **Enable:** Displays the connection status of the serial port.
- **Port:** Displays the serial type of the serial port.
- **Baud Rate:** Displays the Baud Rate set for the serial port.
- **Data Bits:** Displays the data bits set for the serial port.
- **Stop Bits:** Displays the stop bits set for the serial port.
- **Parity:** Displays the parity set for the serial port.

As you can see in **Figure** 25 **– 47**, you can edit the settings of the selected serial port by clicking the ✎ button.



Connection Settings

Serial Connection Settings

Index: 1

Enable: ☑

Port: COM1

Baud Rate: 19200

Data Bits: 8

Stop Bits: 2

Parity: None

Transmission Settings

Transmission Method: Transparent

MTU: 1024

Protocol: TCP Client

Remote Address: 10.51.1.215

Remote Port: 2000

Figure 47 – Serial port connection settings

SERIAL CONNECTION SETTINGS

- **Enable:** Allows you to enable or disable the serial port.
- **Port:** Displays the serial type of the serial port.
- **Baud Rate:** Allows you to define the Baud Rate for the serial port: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 115200.
- **Data Bits:** Allows you to define the data bits set for the serial port. Select the values from 7 or 8.
- **Stop Bits:** Allows you to define the stop bits for the serial port. Select the values from 1 or 2.
- **Parity:** Allows you to define the parity for the serial port: "None", "Even" or "Odd".

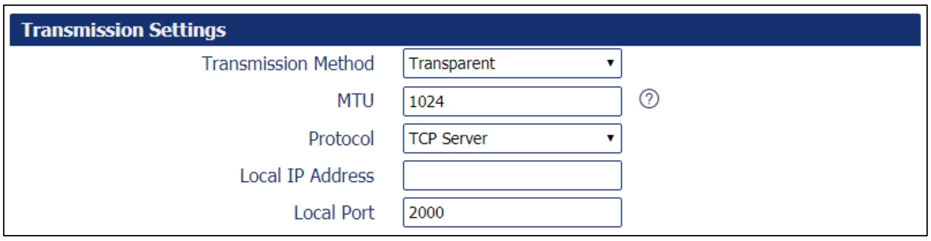
TRANSMISSION SETTINGS

This section allows you to set the transmission settings of the selected serial port if the **Protocol** parameter is set to "TCP Client".

- **Transmission Method:** Allows you to define the transmission method of serial port: "Transparent", "Modbus RTU Gateway" or "Modbus ASCII Gateway".
- **MTU:** Allows you to define the maximum packet size allowed to be transmitted. Should be left as default value of 1024 in most cases.
- **Protocol:** Allows you to define the mode for serial IP communication: "UDP", "TCP Server" or "TCP Client". In this case, "TCP Client".
- **Remote IP Address:** Allows you to enter the IP address of the remote server.
- **Remote Port:** Allows you to enter the port number of the remote server.

TRANSMISSION SETTINGS

This section allows you to set the transmission settings of the selected serial port if the **Protocol** parameter is set to "TCP Server".



Transmission Settings

Transmission Method: Transparent

MTU: 1024

Protocol: TCP Server

Local IP Address:

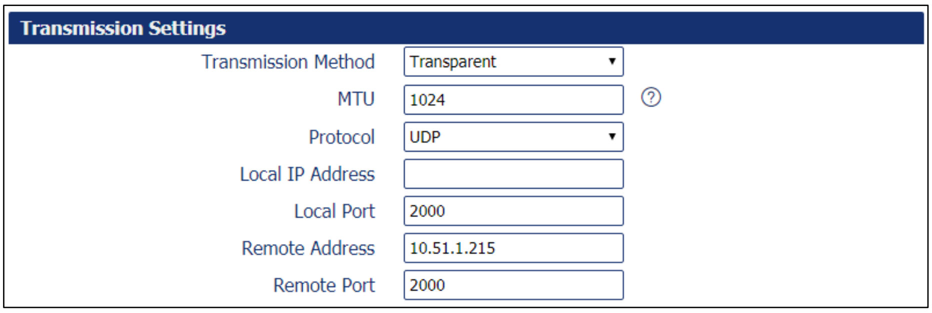
Local Port: 2000

Figure 48 - TCP Server protocol

- **Transmission Method:** Allows you to define the transmission method of serial port: "Transparent", "Modbus RTU Gateway" or "Modbus ASCII Gateway".
- **MTU:** Allows you to define the maximum packet size allowed to be transmitted. Should be left as default value of 1024 in most cases.
- **Protocol:** Allows you to define the mode for serial IP communication: "UDP", "TCP Server" or "TCP Client". In this case, "TCP Server".
- **Local IP Address:** Allows you to enter the IP address of the local endpoint.
- **Local Port:** Displays the port number assigned to the serial IP port on which communications will take place.

TRANSMISSION SETTINGS

This section allows you to set the transmission settings of the selected serial port if the **Protocol** parameter is set to "UDP".



Transmission Settings

Transmission Method	Transparent ▾
MTU	1024
Protocol	UDP ▾
Local IP Address	
Local Port	2000
Remote Address	10.51.1.215
Remote Port	2000

Figure 49 – UDP Protocol

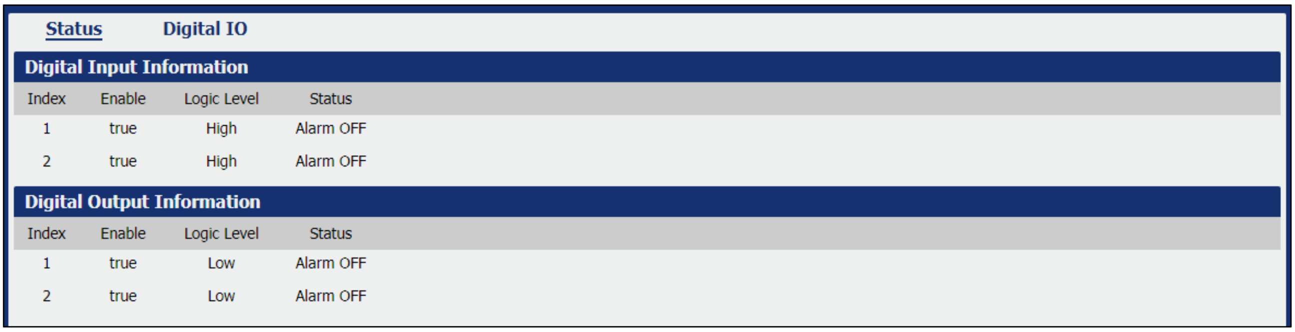
- **Transmission Method:** Allows you to define the transmission method of serial port: "Transparent", "Modbus RTU Gateway" or "Modbus ASCII Gateway".
- **MTU:** Allows you to define the maximum packet size allowed to be transmitted. Should be left as default value of 1024 in most cases.
- **Protocol:** Allows you to define the mode for serial IP communication: "UDP", "TCP Server" or "TCP Client". In this case, "TCP Server".
- **Local IP Address:** Allows you to enter the IP address of the local endpoint.
- **Local Port:** Displays the port number assigned to the serial IP port on which communications will take place.
- **Remote IP Address:** Allows you to enter the IP address of the remote server.
- **Remote Port:** Allows you to enter the port number of the remote server.

5.4.2 DIGITAL I/O

This section allows you to configure digital input and output parameters. The digital input can be used to trigger alarms. The digital output, in turn, can be used to control the slave device by means of the digital signal.

5.4.2.1 DIGITAL I/O → STATUS

This parameter group allows you to view digital input and output information.



Digital Input Information

Index	Enable	Logic Level	Status
1	true	High	Alarm OFF
2	true	High	Alarm OFF

Digital Output Information

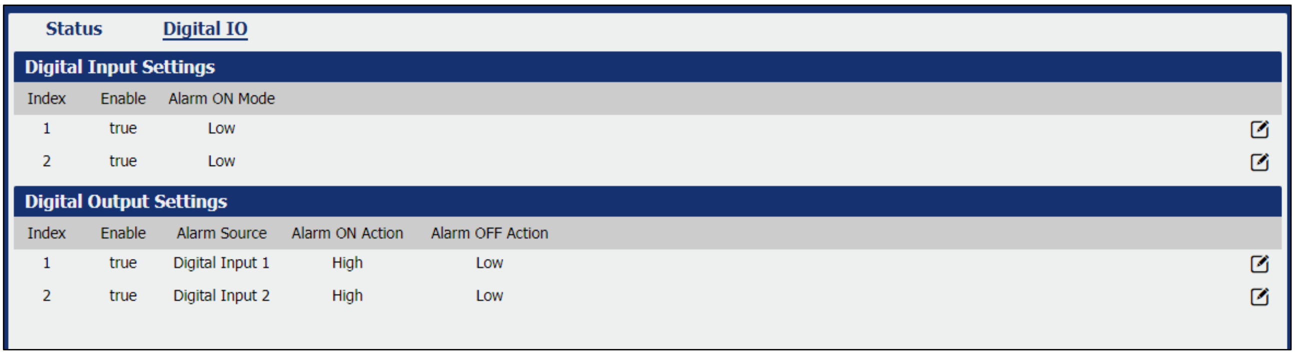
Index	Enable	Logic Level	Status
1	true	Low	Alarm OFF
2	true	Low	Alarm OFF

Figure 50 – Digital input and output status

- **Enable:** Displays the status of current digital IO function.
- **Logic Level:** Displays the electrical level of digital IO port.
- **Status:** Displays the alarm status of digital IO port.

5.4.2.2 DIGITAL I/O → DIGITAL I/O

This parameter group allows you to configure the digital input and output.



Digital Input Settings

Index	Enable	Alarm ON Mode	
1	true	Low	✎
2	true	Low	✎

Digital Output Settings

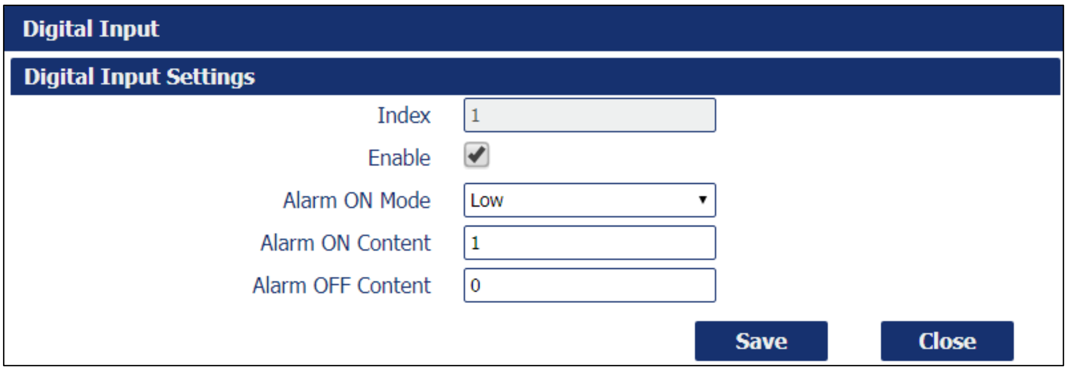
Index	Enable	Alarm Source	Alarm ON Action	Alarm OFF Action	
1	true	Digital Input 1	High	Low	✎
2	true	Digital Input 2	High	Low	✎

Figure 51 – Digital IP settings

This parameter group has the following buttons:

✎ **Button:** Allows you to edit the settings of the digital input or output selected.

As you can see in **Figure 52**, you can edit the settings of the selected digital input by clicking the ✎ button.



Digital Input

Digital Input Settings

Index: 1

Enable: ☑

Alarm ON Mode: Low

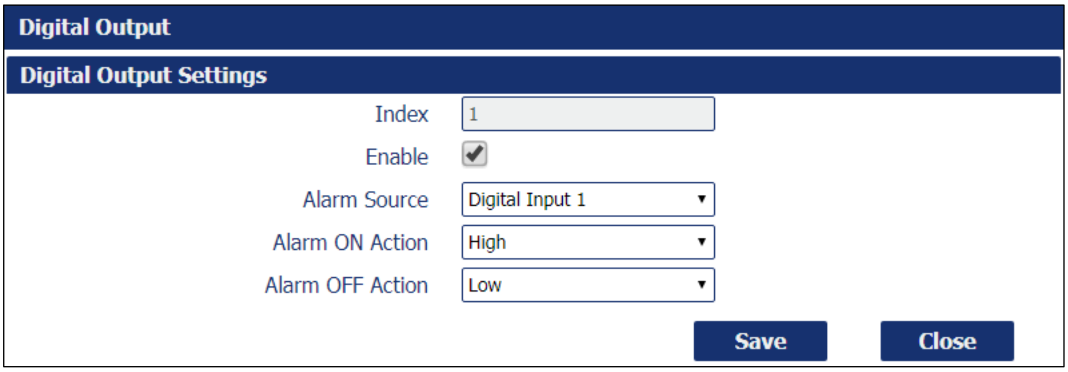
Alarm ON Content: 1

Alarm OFF Content: 0

Figure 52 – Digital input settings

- **Enable:** Allows you to enable or disable the digital input function.
- **Alarm ON Mode:** Allows you to select the electrical level to trigger alarm: "Low" or "High".
- **Alarm ON Content:** Allows you to specify the alarm on content to be sent out via SMS message.
- **Alarm OFF Content:** Allows you to specify the alarm off content to be sent out via SMS message.

As you can see in **Figure 53**, you can edit the settings of the selected digital output by clicking the ✎ button.



Digital Output

Digital Output Settings

Index: 1

Enable: ☑

Alarm Source: Digital Input 1

Alarm ON Action: High

Alarm OFF Action: Low

Figure 53 – Digital output settings

- **Enable:** Allows you to enable or disable the digital output function.
- **Alarm Source:** Allows you to select the alarm source: "Digital Input 1", "Digital Input 2" or "SMS". Digital output triggers the related action when there is alarm comes from Digital Input or SMS.
- **Alarm ON Action:** Allows you to select the alarm action when ON: "High", "Low" or "Pulse". "High" means high electrical level output. "Low" means low electrical level output. "Pulse" will generate a square wave as specified in the pulse mode parameters when triggered.
- **Alarm OFF Action:** Allows you to select the alarm action when OFF: "High", "Low" or "Pulse". "High" means high electrical level output. "Low" means low electrical level output. "Pulse" will generate a square wave as specified in the pulse mode parameters when triggered.
- **Pulse Width:** This parameter is available when select "Pulse" option in the **Alarm ON Action** or **Alarm OFF Action** parameters. The selected digital output channel will generate a square wave as specified in the pulse mode parameters.

5.5 NETWORK

This section shows information about Firewall, Router, VRRP (Virtual Routing Redundancy Protocol), and IP Passthrough settings.

5.5.1 FIREWALL

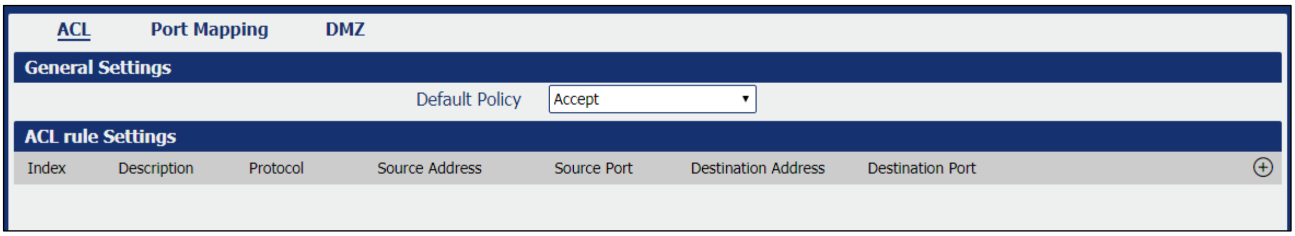
This section allows you to view and manage device firewall information.

Firewall rules are security rule-sets to implement control over users, applications or network objects in an organization. Using the firewall rule, you can create blanket or specialized traffic transit rules based on the requirement.

5.5.1.1 FIREWALL → ACL

This parameter group allows you to view information about firewall access control policies.

An access control list (ACL), with respect to a computer file system, is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.



General Settings

Default Policy: Accept

ACL rule Settings

Index	Description	Protocol	Source Address	Source Port	Destination Address	Destination Port	⊕

Figure 54 - Firewall: ACL

This parameter group hast the following buttons:

⊕ **Button:** Allows you to create a new access control list (ACL).

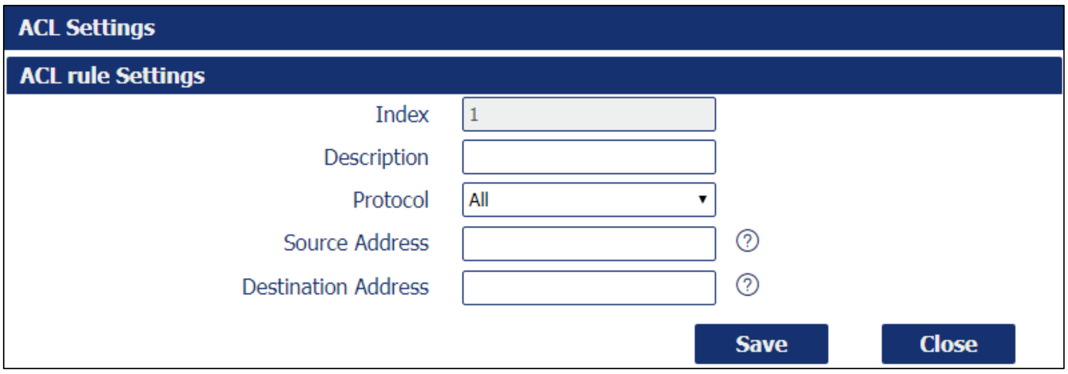
✎ **Button:** Allows you to edit the selected access control list.

⊗ **Button:** Allows you to delete the selected access control list.

This group displays the following parameter:

- **Default Policy:** Allows you to select the firewall default policy: "Accept" or "Drop". The packets which are not included in the access control list will be processed by the default filter policy.

As you can see in **Figure 55**, you can create a new access control list by clicking the ⊕ button.



ACL Settings

ACL rule Settings

Index: 1

Description:

Protocol: All

Source Address: ?

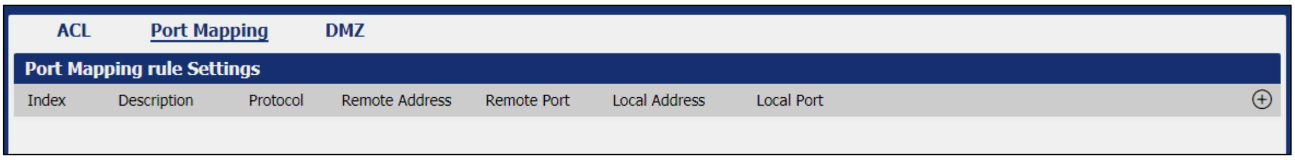
Destination Address: ?

Figure 55 – ACL rule settings

- **Description:** Allows you to enter a description for the rule to be created.
- **Protocol:** Allows you to select the protocol to be used: "All" (Any protocol number), "TCP", "UDP", "TCP & UDP" or "ICMP".
- **Source Address:** Allows you to enter a specific host IP address or a range of IP addresses via bitmask.
- **Destination Address:** Allows you to enter a specific IP address or a range of IP addresses via bitmask.

5.5.1.2 FIREWALL → PORT MAPPING

This parameter group allows you to view information about the firewall port mapping.



Port Mapping rule Settings

Index	Description	Protocol	Remote Address	Remote Port	Local Address	Local Port	⊕

Figure 5641 – Port mapping

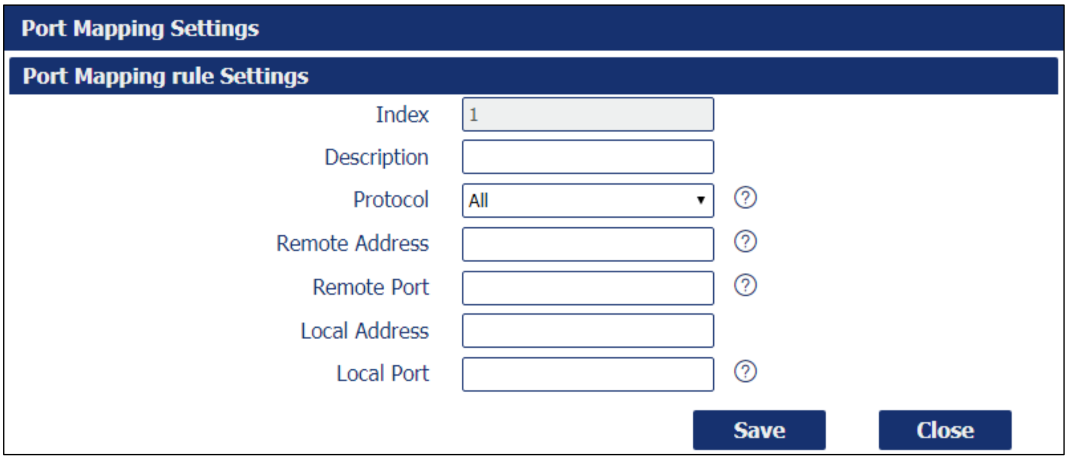
This parameter group has the following buttons:

⊕ **Button:** Allows you to create a new port mapping rule.

✎ **Button:** Allows you to edit a selected rule.

⊗ **Button:** Allows you to delete a selected rule.

As you can see in **Figure 57**, you can create a new port mapping rule by clicking the ⊕ button.



Port Mapping Settings

Port Mapping rule Settings

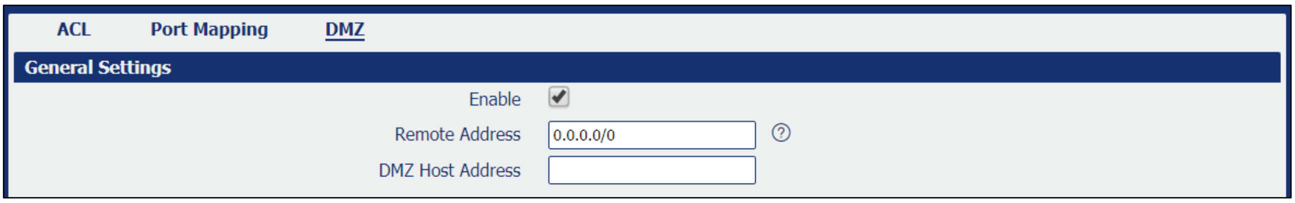
Index	1
Description	
Protocol	All ▾ ⓘ
Remote Address	ⓘ
Remote Port	ⓘ
Local Address	
Local Port	ⓘ

Figure 57 – Port mapping rule settings

- **Description:** Allows you to enter a description for the rule to be created.
- **Protocol:** Allows you to select the protocol to be used: "All" (Any protocol number), "TCP" or "UDP".
- **Remote Address:** Allows you to enter a WAN IP address that is allowed to access the device.
- **Remote Port:** Allows you to enter the external port number range for incoming requests.
- **Local Address:** Allows you to define the LAN address of a device connected to one of the **AirGate 4G** interfaces. Inbound requests will be forwarded to this IP address.
- **Local Port:** Allows you to define the LAN port number range used when forwarding to the destination IP address.

5.5.1.3 FIREWALL → DMZ

This parameter group allows you to configure a DeMilitarized Zone (DMZ) for the device.



General Settings

Enable	☑
Remote Address	0.0.0.0/0 ⓘ
DMZ Host Address	

Figure 58 - DMZ

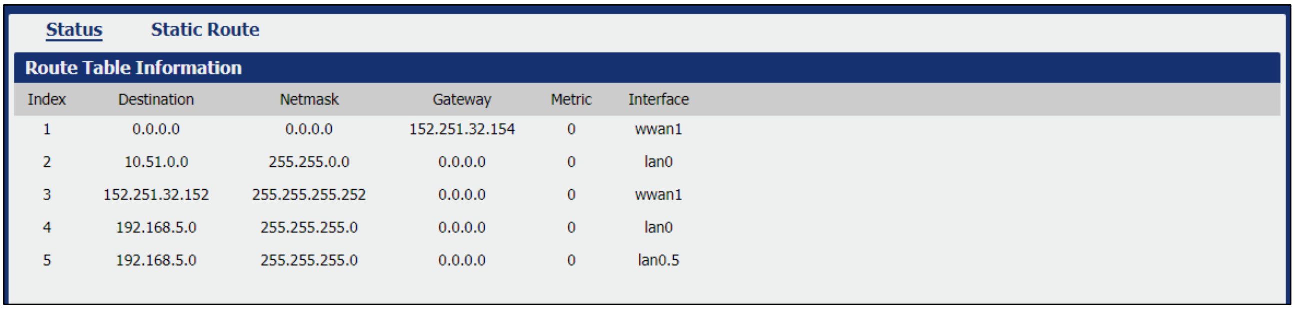
- **Enable:** Allows you to enable or disable DMZ function.
- **Remote Address:** Allows, if configured, optionally restricting DMZ access to the specified WAN IP address only. If set to 0.0.0.0/0, DMZ will be open for all WAN IP addresses.
- **DMZ Host Address:** Allows you to set a WAN IP address that will have access to all entries except for the ports defined during port forwarding setup.

5.5.2 ROUTE

This tab allows you to view and manage device data routing information.

5.5.2.1 ROUTE → STATUS

This parameter group allows you to view information about the configured routes for the device.



Route Table Information

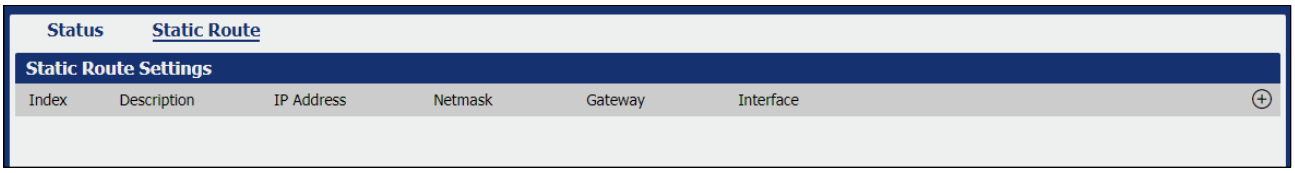
Index	Destination	Netmask	Gateway	Metric	Interface
1	0.0.0.0	0.0.0.0	152.251.32.154	0	wwan1
2	10.51.0.0	255.255.0.0	0.0.0.0	0	lan0
3	152.251.32.152	255.255.255.252	0.0.0.0	0	wwan1
4	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0
5	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0.5

Figure 59 – Route table information

- **Destination:** Displays the destination of this routing traffic.
- **Netmask:** Displays the subnet mask of this routing.
- **Gateway:** Displays the gateway of this interface. The gateway is used for routing packets to remote networks.
- **Metric:** Displays the metric value of this interface.
- **Interface:** Displays the outbound interface of this route.

5.5.2.2 ROUTE → ROUTE TABLE INFORMATION

This parameter group allows you to configure routes for the device. Static Routing refers to a manual method of setting up routing between networks.



Static Route Settings

Index	Description	IP Address	Netmask	Gateway	Interface

Figure 60 – Static route settings

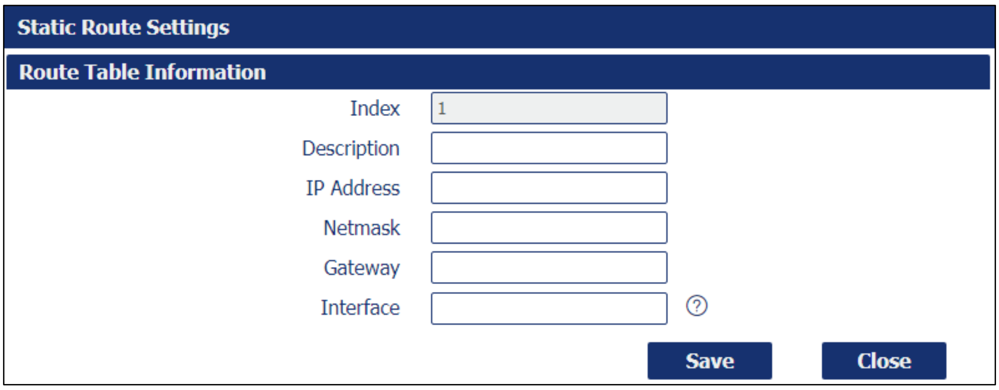
This parameter group has the following buttons:

⊕ **Button:** Allows you to create a new route for the device.

✎ **Button:** Allows you to edit the settings of the selected route.

⊗ **Button:** Allows you to delete the selected route.

As you can see in **Figure 61**, you can create a new route by clicking the ⊕ button.



Static Route Settings

Route Table Information

Index	1
Description	
IP Address	
Netmask	
Gateway	
Interface	

Figure 61 – Static route settings

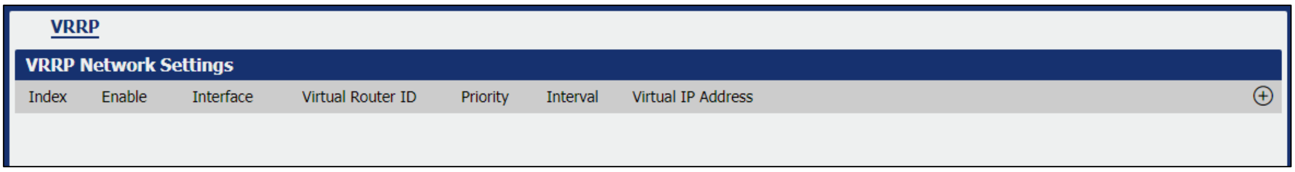
- **Description:** Allows you to enter the description of current static route rule.
- **IP Address:** Allows you to enter the IP address of the destination network.
- **Netmask:** Allows you to enter the subnet mask of the destination network.
- **Gateway**: Allows you to enter the IP address of the local gateway.
- **Interface**: Allows you to define the interface to be used.

5.5.3 VRRP

This tab allows you to view and manage information about the virtual router redundancy protocol.

The VRRP (*Virtual Router Redundancy Protocol*) is a computer networking protocol that provides automatic assignment of available Internet Protocol (IP) routers for participating hosts. The VRRP router who has the highest number will become the virtual master router. The VRRP router number ranges from 1 to 255 and usually we use 255 for the highest priority and 100 for backup.

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



VRRP

VRRP Network Settings

Index	Enable	Interface	Virtual Router ID	Priority	Interval	Virtual IP Address	⊕

Figure 62 - VRRP

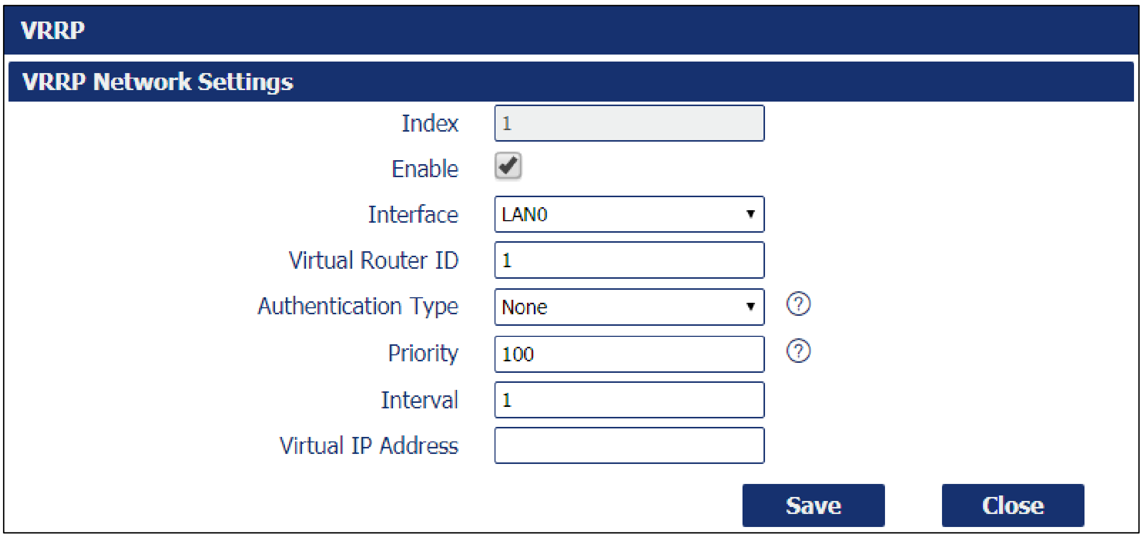
This parameter group has the following buttons:

⊕ **Button:** Allows you to create a new VRRP.

✎ **Button:** Allows you to edit the settings of the selected VRRP.

⊗ **Button:** Allows you to delete the selected VRRP.

As you can see in **Figure 63**, you can create a new VRRP by clicking the ⊕ button.



VRRP

VRRP Network Settings

Index	1
Enable	☑
Interface	LAN0 ▾
Virtual Router ID	1
Authentication Type	None ▾ ⓘ
Priority	100 ⓘ
Interval	1
Virtual IP Address	

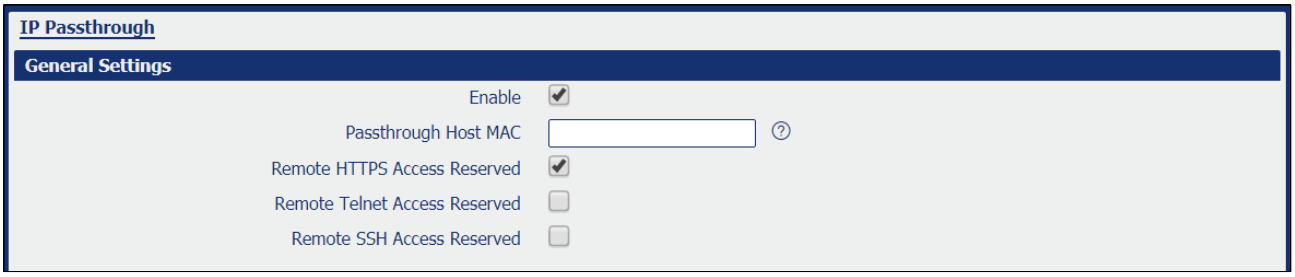
Figure 63 – VRRP network settings

- **Enable:** Allows you to enable or disable the VRRP.
- **Interface:** Allows you to select the virtual router interface.
- **Virtual Router ID:** Allows you to define the user-defined virtual router ID. Range: 1-255.
- **Authentication Type:** Allows you to select the authentication type for VRRP: "None" or "PASS".
- **Password:** If "PASS" option is selected in the **Authentication Type** parameter, allows you to set a password for the VRRP network.
- **Priority:** Allows you to define a VRRP priority range. Range: 1-254 (a bigger number indicates a higher priority).
- **Interval:** Allows you to define the heartbeat package transmission time interval between routers in the virtual IP group. Range: 1-255.
- **Virtual IP Address:** Allows you to enter the virtual IPP address of virtual gateway.

5.5.4 IP PASSTHROUGH

This parameter group allows you to manage information about IP Passthrough mode.

P Passthrough mode disables NAT (Network Address Translation) and routing and passes the WAN IP address from the WAN interface to the device connected on the local Interface. It is used instead of NAT in order to make the router "transparent" in the communication process.



IP Passthrough

General Settings

Enable	☑
Passthrough Host MAC	
Remote HTTPS Access Reserved	☑
Remote Telnet Access Reserved	□
Remote SSH Access Reserved	□

Figure 64 - IP Passthrough

- **Enable:** Allows you to enable or disable IP passthrough.
- **Passthrough Host MAC:** Allows you to enter the MAC of passthrough host to receive the WAN IP address.
- **Remote HTTPS Access Reserved:** Allows you to enable or disable remote HTTPS access.
- **Remote Telnet Access Reserved:** Allows you to enable or disable remote Telnet access.
- **Remote SSH Access Reserved:** Allows you to enable or disable remote SSH access.

5.6 APPLICATIONS

This section introduces applications that can be used for device improvement.

5.6.1 DDNS

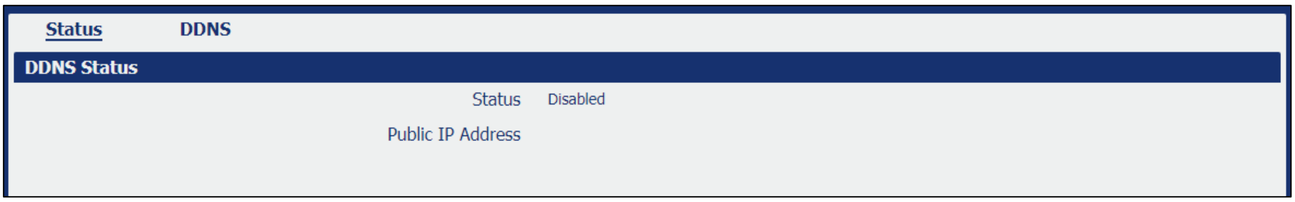
This tab allows you to view and manage information about DDNS.

DDNS is a system that allows the domain name data of a computer with a varying (dynamic) IP addresses held in a name server to be updated in real time in order to make it possible to establish connections to that machine without the need to track the actual IP addresses at all times.

A number of providers offer Dynamic DNS services (DDNS), free or for a charge.

5.6.1.1 DDNS → STATUS

This parameter group allows you to view information about the device DDNS.



Status DDNS

DDNS Status

Status: Disabled

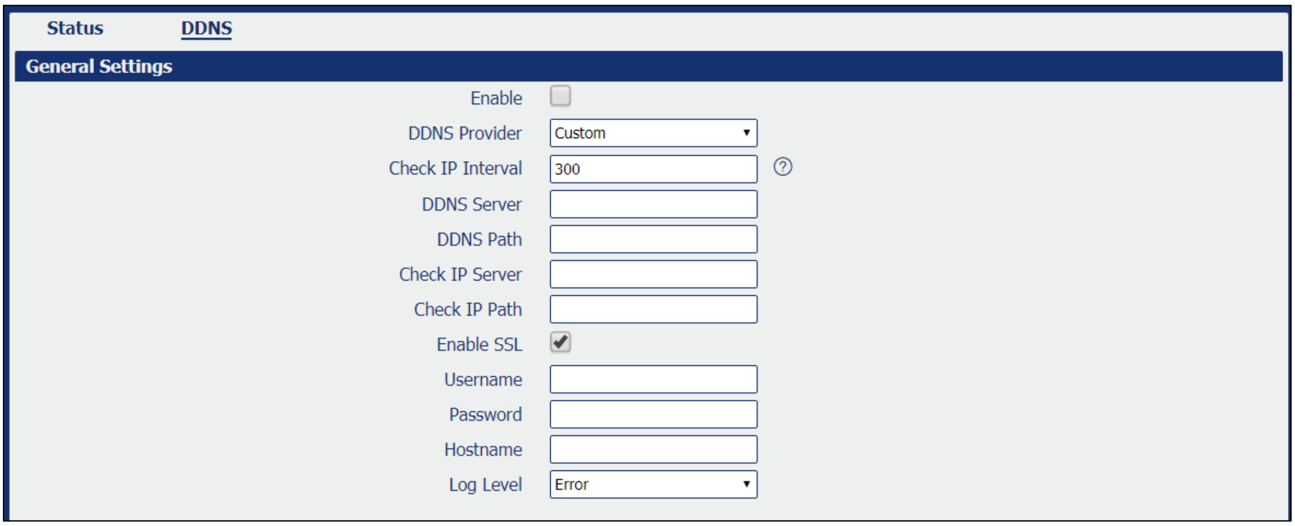
Public IP Address:

Figure 65 – DDNS status

- **Status:** Displays the DDNS status.
- **Public IP Address:** Displays the public IP address assigned to DDNS.

5.6.1.2 DDNS → DDNS

This parameter group allows you to manage the DDNS settings.



Status DDNS

General Settings

Enable: □

DDNS Provider: Custom

Check IP Interval: 300

DDNS Server:

DDNS Path:

Check IP Server:

Check IP Path:

Enable SSL: ☑

Username:

Password:

Hostname:

Log Level: Error

Figure 66 – DDNS settings

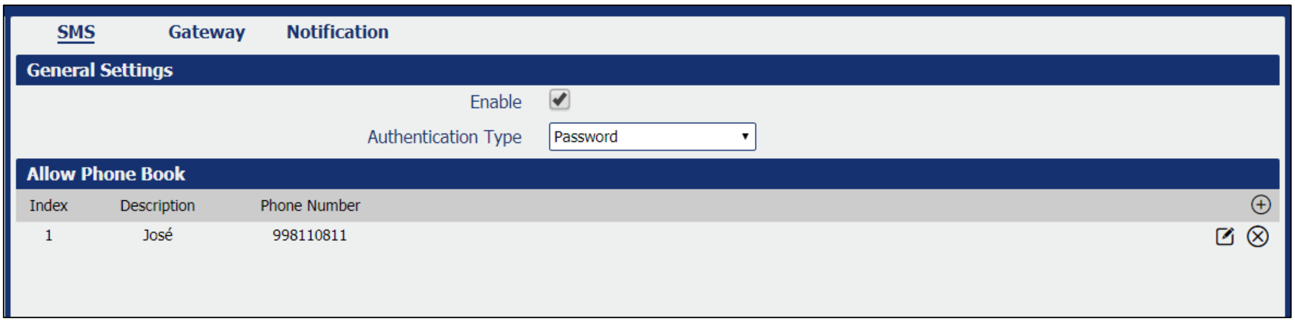
- **Enable:** Allows you to enable or disable DDNS service.
- **DDNS Provider:** Allows you to DDNS provider to be used: "DynDNS", "no-ip", "3322" or "custom".
- **Check IP Interval:** Allows you to enter the interval, in minutes (30 to 86400). The modem will update the Dynamic DNS server of its carrier assigned IP address.
- **DDNS Server:** If "custom" option is selected in the **DDNS Provider** parameter, allows you to set the Internet address to communicate Dynamic DNS information.
- **DDNS Path:** If "custom" option is selected in the **DDNS Provider** parameter, allows you to set the DDNS path for custom type.
- **Check IP Server:** If "custom" option is selected in the **DDNS Provider** parameter, allows you to check the IP server.
- **Check IP Path:** If "custom" option is selected in the **DDNS Provider** parameter, allows you to check the IP path.
- **Enable SSL:** Allows you to enable or disable SSL service for the connection.
- **Username:** Allows you to enter the user name used when setting up the account. Used to login to the Dynamic DNS service.
- **Password:** Allows you to enter the password associated with the account.
- **Hostname:** Allows you to enter the hostname associated with the account.
- **Log Level:** Allows you to select the log output level: "None", "Debug", "Notice", "Info" or "Error".

5.6.2 SMS

This tab allows you to enable and configure SMS sending. SMS allows user to send the SMS to control the router or get the running status of the router.

5.6.2.1 SMS → SMS

This parameter group allows you to enable and configure SMS sending.



SMS | Gateway | Notification

General Settings

Enable ☑

Authentication Type: Password

Allow Phone Book

Index	Description	Phone Number	⊕
1	José	998110811	✎ ⊗

Figure 67 – SMS sending

This parameter group has the following buttons:

⊕ **Button:** Allows you to add a new number to the phone book.

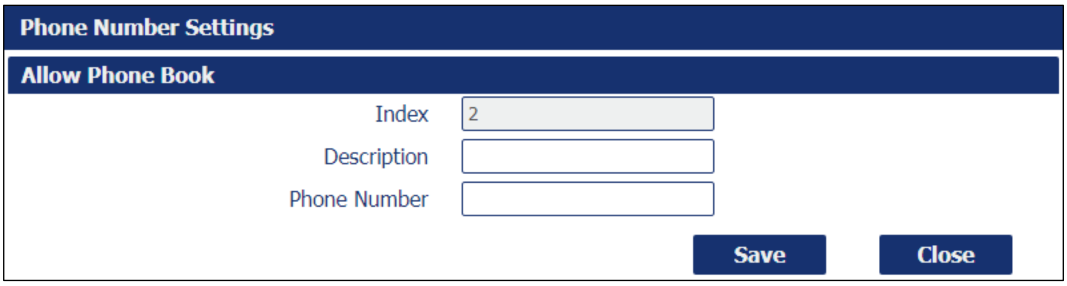
✎ **Button:** Allows you to edit the settings of the phone number selected.

⊗ **Button:** Allows you to delete the phone number selected.

This group displays the following parameters:

- **Enable:** Allows you to enable or disable SMS sending.
- **Authentication Type:** Allows you to define the authentication type for the SMS function: "None" or "Password".

As you can see in **Figure 68**, you can create a new phone number by clicking the ⊕ button.



Phone Number Settings

Allow Phone Book

Index: 2

Description:

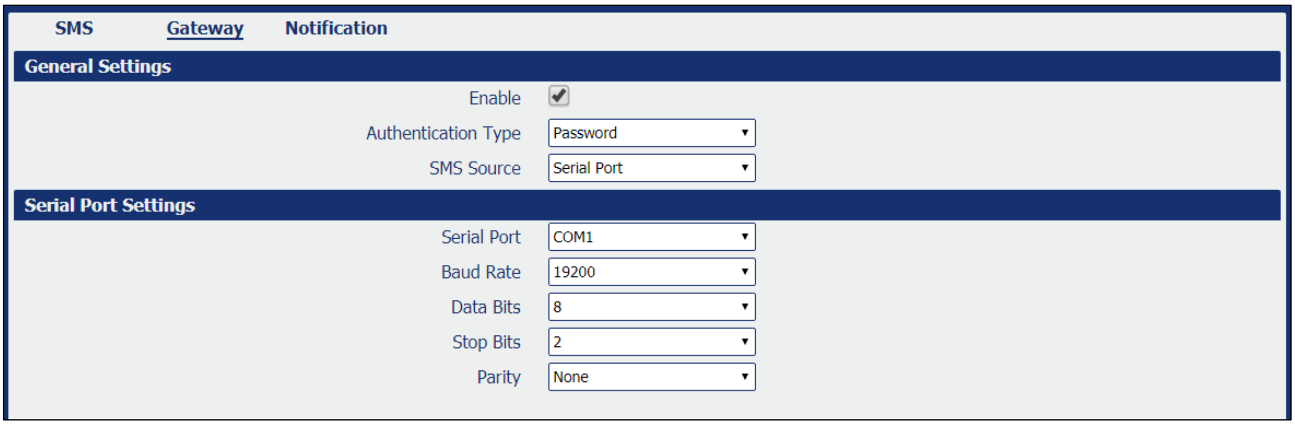
Phone Number:

Figure 68 – Phone number

- **Description:** Allows you to enter a description for the number to be created.
- **Phone Number:** Allows you to add a phone number.

5.6.2.2 SMS → GATEWAY

This parameter group allows you to send SMS messages by using a valid syntax from serial device or Ethernet device.



SMS | Gateway | Notification

General Settings

Enable ☑

Authentication Type: Password

SMS Source: Serial Port

Serial Port Settings

Serial Port: COM1

Baud Rate: 19200

Data Bits: 8

Stop Bits: 2

Parity: None

Figure 69 – Gateway settings

GENERAL SETTINGS

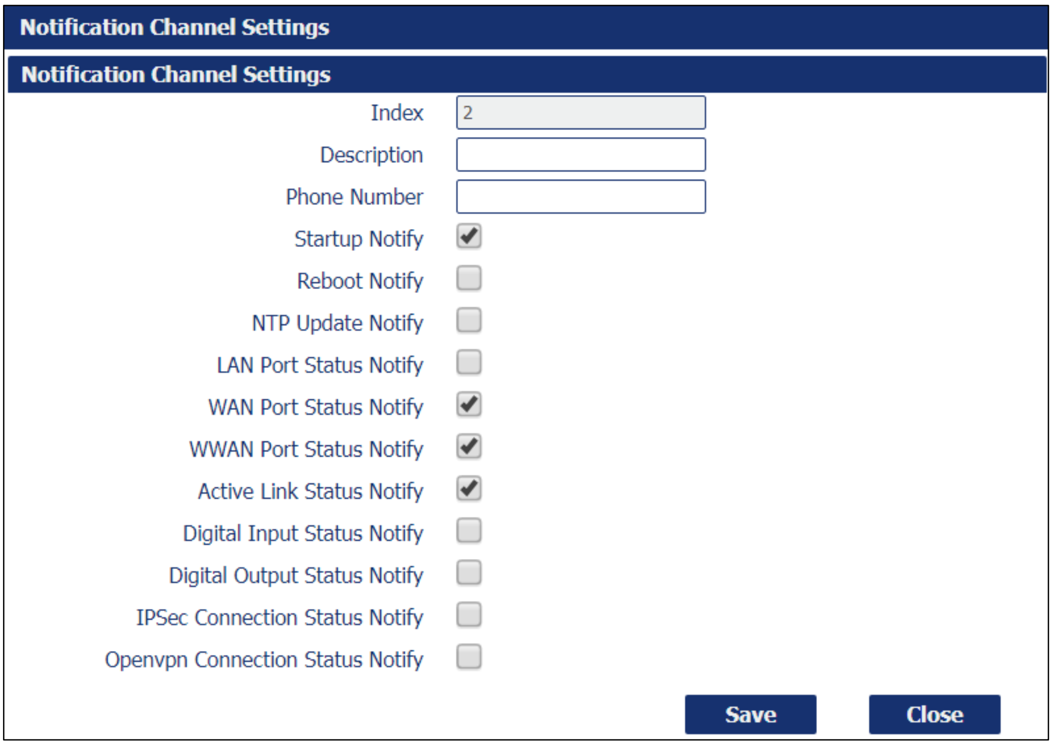
- **Enable:** Allows you to enable or disable SMS gateway.
- **Authentication Type:** Allows you to define an authentication type for SMS gateway: "None" or "Password".
- **SMS Source:** Allows you to define a valid syntax: "Serial Port" or "HTTP(S) GET/POST".

SERIAL PORT SETTINGS

- **Serial Port:** Allows you to select the serial port: COM1 or COM2.
- **Baud Rate:** Allows you to select the serial port Baud Rate: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600 or 115200.
- **Data Bits:** Allows you to select the data bits values: 7 to 8.
- **Stop Bits:** Allows you to select the serial port stop bits: 1 or 2.
- **Parity:** Allows you to select the serial port parity: "None", "Even" or "Odd".

5.6.2.3 SMS → NOTIFICATION

This parameter group allows sending SMS notification to the pre-setting phone number when some of router status changed.



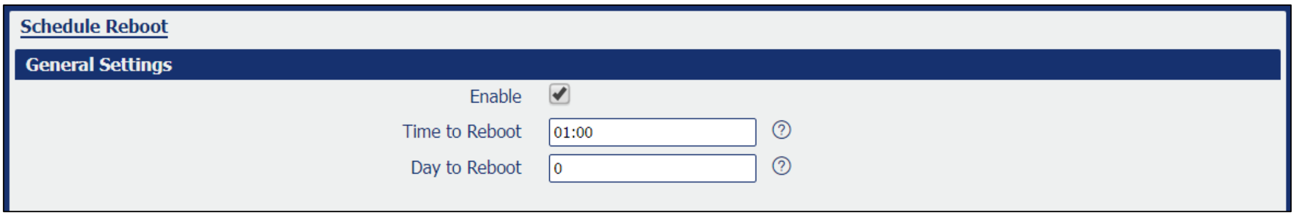
Index: 2
Description:
Phone Number:
Startup Notify ☑
Reboot Notify ☐
NTP Update Notify ☐
LAN Port Status Notify ☐
WAN Port Status Notify ☑
WWAN Port Status Notify ☑
Active Link Status Notify ☑
Digital Input Status Notify ☐
Digital Output Status Notify ☐
IPSec Connection Status Notify ☐
Openvpn Connection Status Notify ☐

Figure 70 – Notification channel settings

- **Description:** Allows you to add the description for notification channel.
- **Phone Number:** Allows you to add a pre-setting phone number to receive the notification.
- **Startup Notify:** Allows you to send SMS notification to the pre-setting phone number when system startup.
- **Reboot Notify:** Allows you to send SMS notification to the pre-setting phone number when system reboot.
- **NTP Update Notify:** Allows you to send SMS notification to the pre-setting phone number when system startup.
- **LAN Port Status Notify:** Allows you to send SMS notification to the pre-setting phone number when LAN port status changed.
- **WAN Port Status Notify:** Allows you to send SMS notification to the pre-setting phone number when WAN port status changed.
- **WWAN Port Status Notify:** Allows you to send SMS notification to the pre-setting phone number when WWAN port status changed.
- **Active Link Status Notify:** Allows you to send SMS notification to the pre-setting phone number when active link status changed.
- **Digital Input Status Notify:** Allows you to send SMS notification to the pre-setting phone number when DI status changed
- **Digital Output Status Notify:** Allows you to send SMS notification to the pre-setting phone number when DO status changed.
- **IPSec Connection Status Notify:** Allows you to send SMS notification to the pre-setting phone number when IPSec connection status changed.
- **OpenVPN Connection Status Notify:** Allows you to send SMS notification to the pre-setting phone number when OpenVPN Connection Status changed.

5.6.3 SCHEDULE REBOOT

This tab allows you to define the time for router reboot itself.



Schedule Reboot

General Settings

Enable	☑
Time to Reboot	01:00
Day to Reboot	0

Figure 71 – Schedule reboot

- **Enable:** Allows you to enable or disable schedule reboot feature.
- **Time to Reboot:** Allows you to enter the time of each day to reboot device. Format: HH(00-23):MM(00-59).
- **Day to Reboot:** Allows you to enter the day of each month to reboot device. 0 means every day.

5.7 VPN

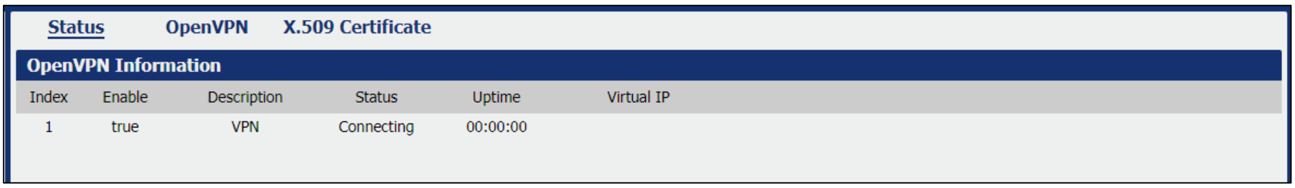
This section allows you to define VPN settings.

5.7.1 OpenVPN

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

5.7.1.1 OpenVPN → STATUS

This parameter group allows you to view the OpenVPN status. Each OpenVPN can be individually created, configured or removed in the OpenVPN → OpenVPN tab.



Status OpenVPN X.509 Certificate

OpenVPN Information

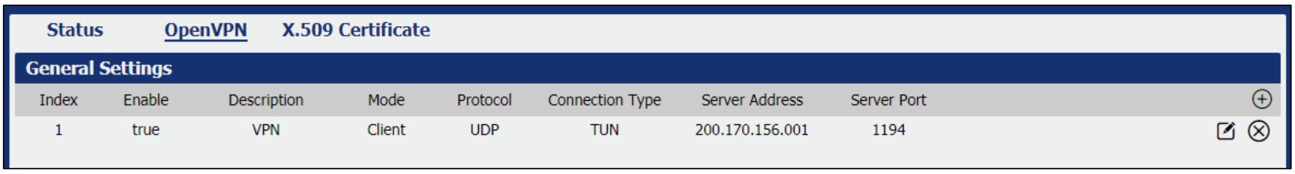
Index	Enable	Description	Status	Uptime	Virtual IP
1	true	VPN	Connecting	00:00:00	

Figure 72 - OpenVPN

- **Enable:** Displays current OpenVPN settings is enable or disable.
- **Status:** Displays the current VPN connection status.
- **Uptime:** Displays the connection time since VPN is established.
- **Virtual IP:** Displays the virtual IP address obtain from remote side.

5.7.1.2 OpenVPN → OpenVPN

This parameter group allows you to configure the OpenVPN.



Status OpenVPN X.509 Certificate

General Settings

Index	Enable	Description	Mode	Protocol	Connection Type	Server Address	Server Port	⊕
1	true	VPN	Client	UDP	TUN	200.170.156.001	1194	✎ ⊗

Figure 73 – OpenVPN settings

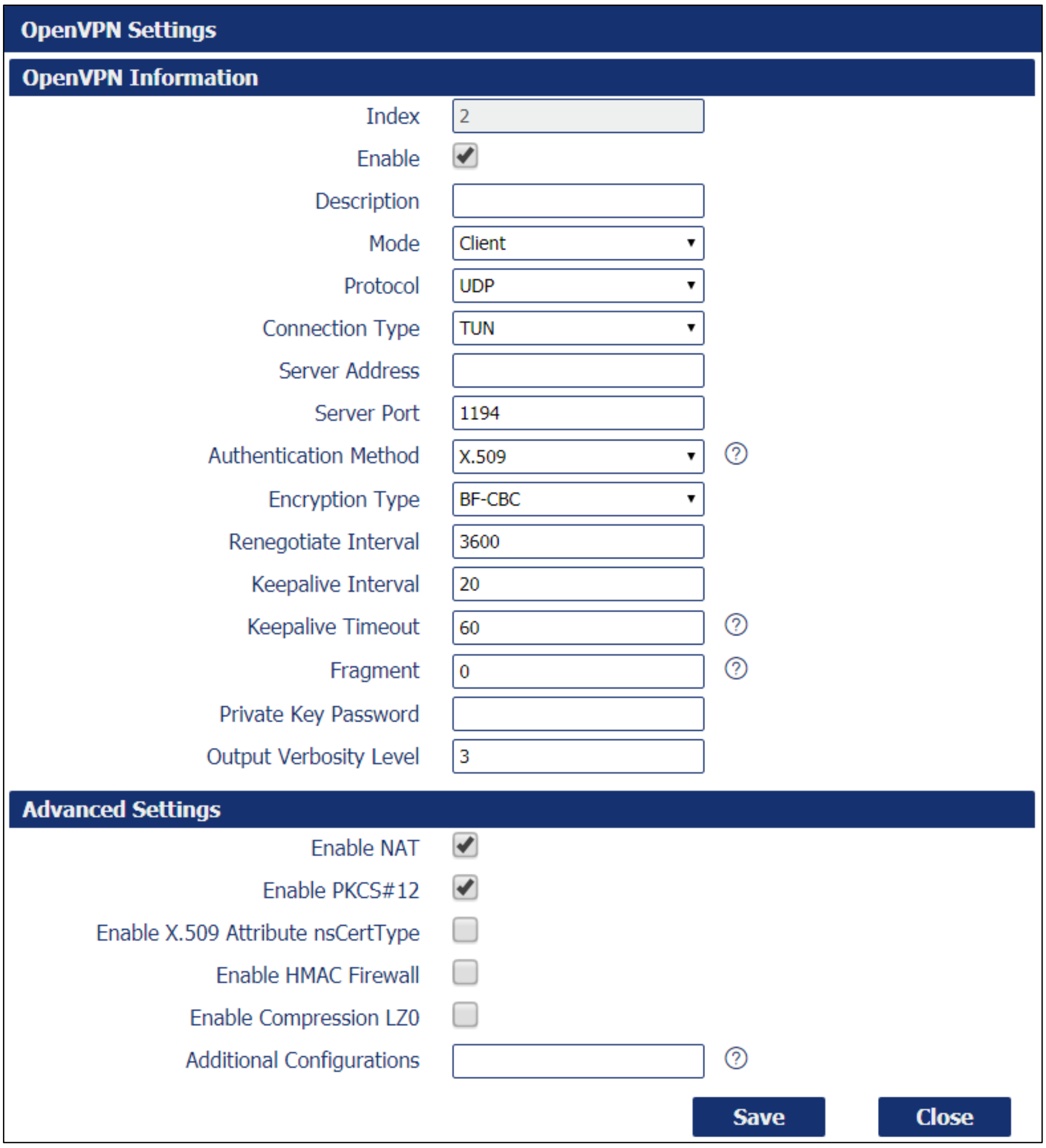
This parameter group has the following buttons:

⊕ **Button:** Allows you to add a new OpenVPN.

✎ **Button:** Allows you to edit the settings of the selected OpenVPN.

⊗ **Button:** Allows you to delete the selected OpenVPN.

As you can see in **Figure 74**, you can create a new OpenVPN by clicking the ⊕ button.



OpenVPN Settings

OpenVPN Information

Index	2
Enable	☑
Description	
Mode	Client
Protocol	UDP
Connection Type	TUN
Server Address	
Server Port	1194
Authentication Method	X.509
Encryption Type	BF-CBC
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	0
Private Key Password	
Output Verbosity Level	3

Advanced Settings

Enable NAT	☑
Enable PKCS#12	☑
Enable X.509 Attribute nsCertType	□
Enable HMAC Firewall	□
Enable Compression LZO	□
Additional Configurations	

Figure 74 – OpenVPN settings

- **Enable:** Allows you to enable or disable OpenVPN tunnel.
- **Description:** Allows you to Enter a description for this OpenVPN tunnel.
- **Mode:** Allows you to define a mode for the OpenVPN tunnel: "Client" or "P2P".
- **Protocol:** Allows you to define a protocol for the OpenVPN tunnel: "UDP" or "TCP Client".
- **Connection Type:** Allows you to define a connection type for the OpenVPN tunnel: "TUN" or "TAP". 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.
- **Server Address:** Allows you to Enter the IP address or domain of remote server
- **Server Port:** Allows you to Enter the negotiate port on OpenVPN server
- **Authentication Method:** Allows you to define an authentication method for the OpenVPN tunnel: "X.509", "Pre-shared", "Password" or "X.509 and Password".
- **Encryption Type:** Allows you to define a encryption type for the OpenVPN tunnel: "BF-CBC", "DES-CBC", "DES-EDE-CBC", "DES-EDE3-CBC", "AES-128-CBC", "AES-192-CBC" or "AES-256 -CBC".
- **Username:** Allows you to enter the username for authentication when selection from "Password" or "X.509 And Password".
- **Password:** Allows you to enter the password for authentication when selection from "Password" or "X.509 And Password".
- **Local IP Address:** Allows you to enter the local virtual IP address when select "P2P" mode.
- **Remote IP Address:** Allows you to enter the remote virtual IP address when select "P2P" mode.
- **Local Netmask:** Allows you to enter the local netmask when select "TAP" connection type.
- **TAP Bridge:** Allows you to select the specified LAN that bridge with OpenVPN tunnel when select "TAP" connection type.
- **Renegotiate Interval:** Allows you to enter the renegotiate interval if connection is failed.
- **Keep Alive Interval:** Allows you to enter the keep alive interval to check the tunnel is active or not.

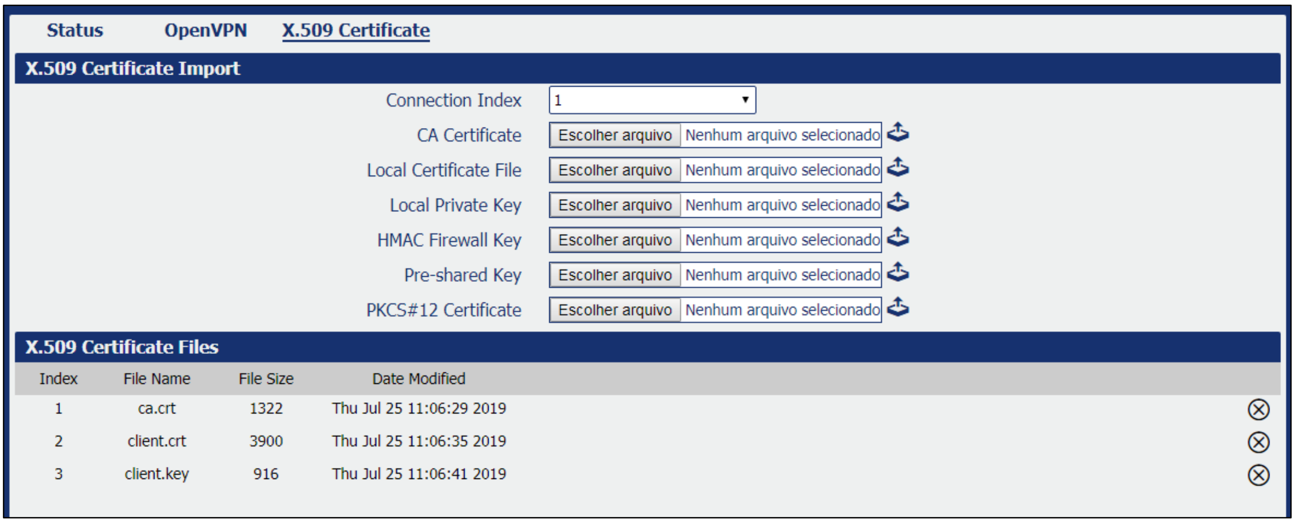
- **Keep Alive Timeout:** Allows you to enter the keep alive timeout, once connection is failed it will trigger the OpenVPN reconnect.
- **Fragment:** Allows you to enter the fragment size. 0 means disable
- **Private Key Password:** Allows you to enter the private key password for authentication when selection from "X.509" or "X.509 And Password".
- **Output Verbosity Level:** Allows you to enter the level of the output log and values.

AVANCED SETTINGS

- **Enable NAT:** Allows you to enable or disable NAT.
- **Enable PKCS#12:** Allows you to enable or disable PKCS#12. It is an exchange of digital certificate encryption standard, used to describe personal identity information.
- **Enable X.509 Attribute nsCertType:** Require that peer certificate was signed with an explicit nsCertType designation of "server".
- **Enable HMAC Firewall:** Add additional layer of HMAC authentication on the top of the TLS control channel to protect against DoS attacks.
- **Enable Compression LZO:** Allows you to enable or disable compress the data.
- **Additional Configurations:** Allows you to enter some other options of OpenVPN in this field. Each expression can be separated by a ";".

5.7.1.3 OpenVPN → X.509 CERTIFICATE

This parameter group allows you to add certificates to the device.



X.509 Certificate Import

Connection Index	1 ▾
CA Certificate	Escolher arquivo Nenhum arquivo selecionado
Local Certificate File	Escolher arquivo Nenhum arquivo selecionado
Local Private Key	Escolher arquivo Nenhum arquivo selecionado
HMAC Firewall Key	Escolher arquivo Nenhum arquivo selecionado
Pre-shared Key	Escolher arquivo Nenhum arquivo selecionado
PKCS#12 Certificate	Escolher arquivo Nenhum arquivo selecionado

X.509 Certificate Files

Index	File Name	File Size	Date Modified	
1	ca.crt	1322	Thu Jul 25 11:06:29 2019	⊗
2	client.crt	3900	Thu Jul 25 11:06:35 2019	⊗
3	client.key	916	Thu Jul 25 11:06:41 2019	⊗

Figure 75 – Certificate files

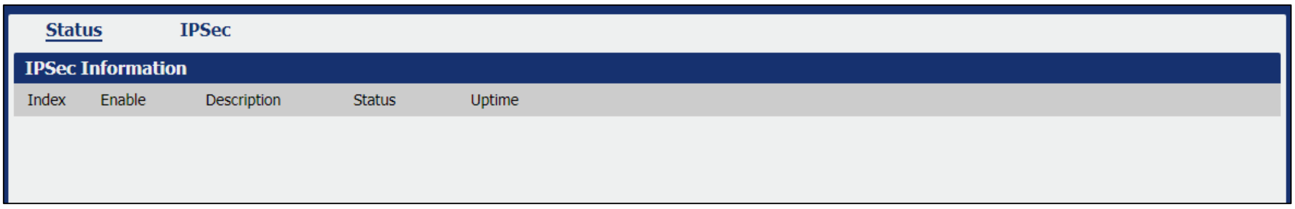
- **Connection Index:** Displays the current connection index for OpenVPN channel.
- **CA Certificate:** Allows you to import CA certificate file.
- **Local Certificate File:** Allows you to import local certificate file.
- **Local Private Key:** Allows you to import local private key file.
- **HMAC Firewall Key:** Allows you to import HMAC firewall key file.
- **Pre-shared Key:** Allows you to import the pre-shared key file.
- **PKCS#12 Certificate:** Allows you to import PKCS#12 certificate.

5.7.2 IPSec

IPSec facilitates configuration of secured communication tunnels. The various tunnel configurations will be displayed in the Tunnel Table at the bottom of the page. All tunnels are create using the ESP (Encapsulating Security Payload) protocol.

5.7.2.1 IPSec → STATUS

This section allows you to view IPSec status.



IPSec Information

Index	Enable	Description	Status	Uptime

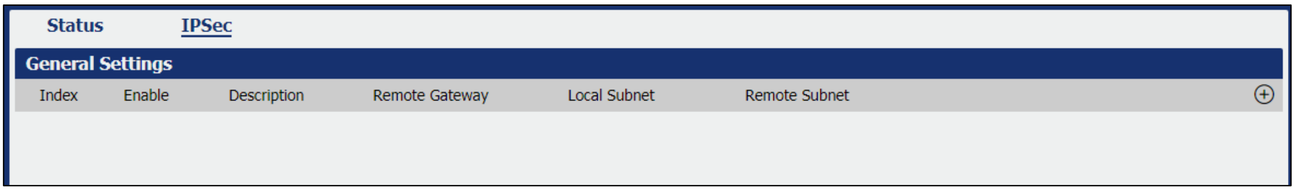
Figure 76 – IPSec status

- **Enable:** Displays current IPSec settings is enable or disable.
- **Description:** Displays the description of current VPN channel.
- **Status:** Displays the current VPN connection status.

- **Uptime:** Displays the connection time since VPN is established.

5.7.2.2 IPSec → IPSec

This section allows you to create or configure IPSec.



Status IPSec

General Settings

Index	Enable	Description	Remote Gateway	Local Subnet	Remote Subnet	⊕

Figure 77 – IPSec: general settings

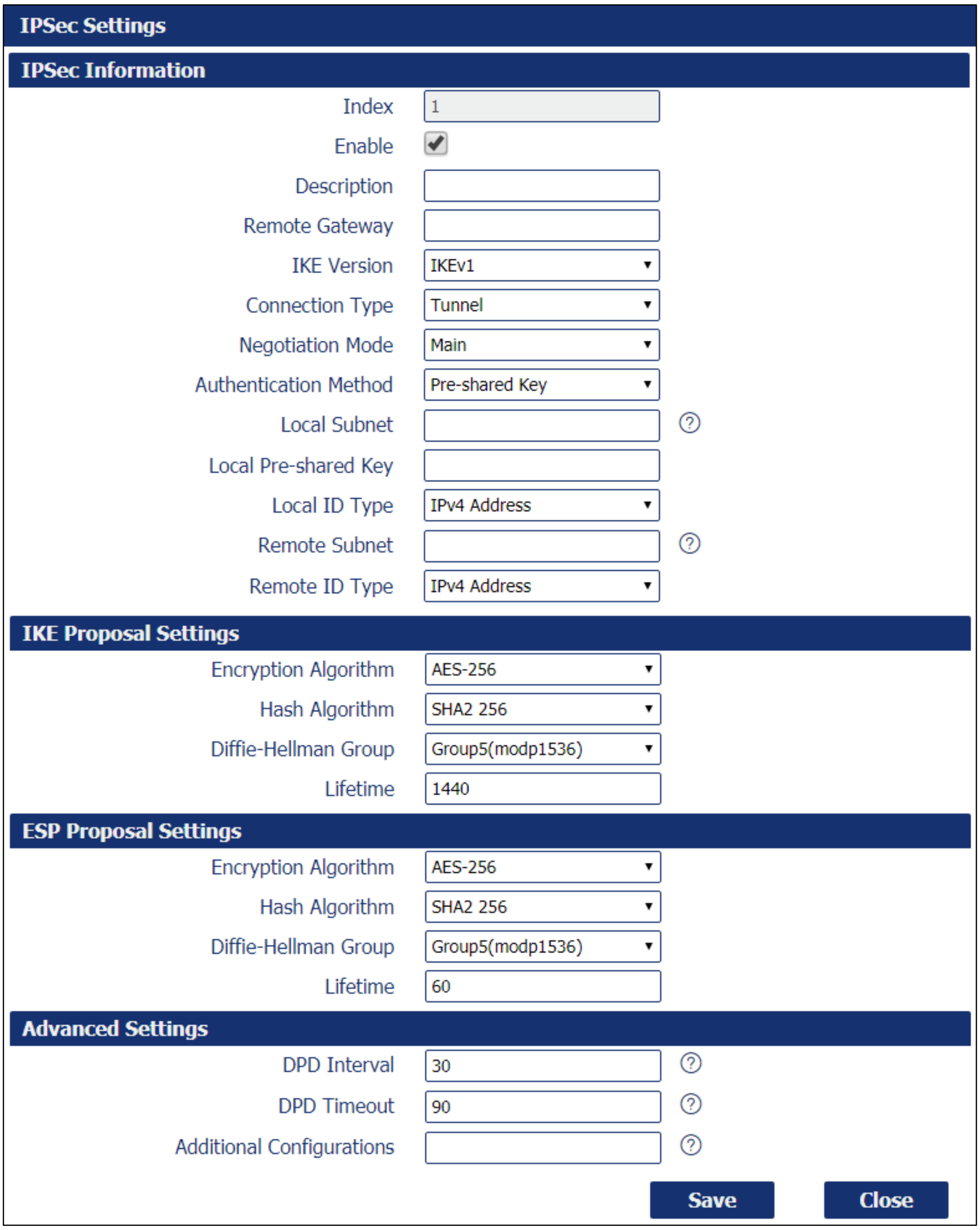
This parameter group has the following buttons:

⊕ **Button:** Allows you to add a new IPSec.

✎ **Button:** Allows you to edit the settings of the selected IPSec.

⊗ **Button:** Allows you to delete the selected IPSec.

As you can see in **Figure 78**, you can create a new IPSec by clicking the ⊕ button.



IPSec Settings

IPSec Information

Index	1
Enable	☑
Description	
Remote Gateway	
IKE Version	IKEv1 ▾
Connection Type	Tunnel ▾
Negotiation Mode	Main ▾
Authentication Method	Pre-shared Key ▾
Local Subnet	?
Local Pre-shared Key	
Local ID Type	IPv4 Address ▾
Remote Subnet	?
Remote ID Type	IPv4 Address ▾

IKE Proposal Settings

Encryption Algorithm	AES-256 ▾
Hash Algorithm	SHA2 256 ▾
Diffie-Hellman Group	Group5(modp1536) ▾
Lifetime	1440

ESP Proposal Settings

Encryption Algorithm	AES-256 ▾
Hash Algorithm	SHA2 256 ▾
Diffie-Hellman Group	Group5(modp1536) ▾
Lifetime	60

Advanced Settings

DPD Interval	30 ?
DPD Timeout	90 ?
Additional Configurations	?

Figure 78 – IPSec settings

GENERAL SETTINGS

- **Enable:** Allows you to enable or disable IPSec.
- **Description:** Allows you to enter a description for this IPSec VPN tunnel.
- **Remote Gateway:** Allows you to enter an IP address for the remote tunnel.
- **IKE Version:** Allows you to select an IKE (Internet Key Exchange) version: "IKEv1" or "IKEv2".
- **Connection Type:** Allows you to select the connection type: "Tunnel" or "Transport".
  - **Tunnel:** In tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header. Tunnel mode is used to create virtual private networks for network-to-network communications.
  - **Transport:** In transport mode, only the payload of the IP packet is usually encrypted or authenticated. The routing is intact, since the IP header is neither modified nor encrypted.
- **Negotiation Mode:** Allows you to select a negotiation mode: "Main" or "Aggressive".
- **Authentication Method:** Allows you to select an authentication method: "Pre-Shared Key" or "Pre-Shared Key and XAuth".
- **Local Subnet:** Allows you to enter the IP address with mask if a network beyond the local LAN will be sending packets through the tunnel. The remote subnet and Local subnet addresses must not overlap.
- **Local Pre-Shared Key:** Allows you to enter the pre-shared key which match the remote endpoint.
- **Local ID Type:** Allows you to enter the local endpoint's identification. The identifier can be a host name or an IP address.

- **Identity XAuth:** Allows you to enter Xauth identity after "Pre-shared Key and Xauth" on authentication Method is enabled.
- **Password XAuth:** Allows you to enter Xauth password "Pre-shared Key and Xauth" on authentication Method is enabled.
- **Remote Subnet:** Allows you to enter an IP address with mask if encrypted packets are also destined for the specified network that is beyond the Remote IP Address. The remote subnet and local subnet addresses must not overlap.
- **Remote ID Type:** Allows you to enter the authentication address of the remote endpoint.

IKE PROPOSAL SETTINGS

- **Encryption Algorithm (IKE):** Allows you to select the encryption algorithm: "3DES AES-128", "AES-192" or "AES-256".
- **Hash Algorithm (IKE):** Allows you to select the hash algorithm: "MD5", "SHA1", "SHA2 256", "SHA2 384" or "SHA2 512".
- **Diffie-Hellman Group (IKE):** Allows you to select the Diffie-Hellman method: "Negotiate (None)", "768 (Group 1)", "1024 (Group 2)", "1536 (Group 5)" or "2048 (Group 14)".
- **Lifetime (IKE):** How long a particular instance of a connection should last, from successful negotiation to expiry.

ESP PROPOSAL SETTINGS

- **Encryption Algorithm (ESP):** Allows you to select the encryption algorithm: "3DES AES-128", "AES-192" or "AES-256".
- **Hash Algorithm (ESP):** Allows you to select the hash algorithm: "MD5", "SHA1", "SHA2 256", "SHA2 384" or "SHA2 512".
- **Diffie-Hellman Group (ESP):** Allows you to select the Diffie-Hellman method: "Negotiate (None)", "768 (Group 1)", "1024 (Group 2)", "1536 (Group 5)" or "2048 (Group 14)".
- **Lifetime (ESP):** How long a particular instance of a connection should last, from successful negotiation to expiry.

ADVANCED SETTINGS

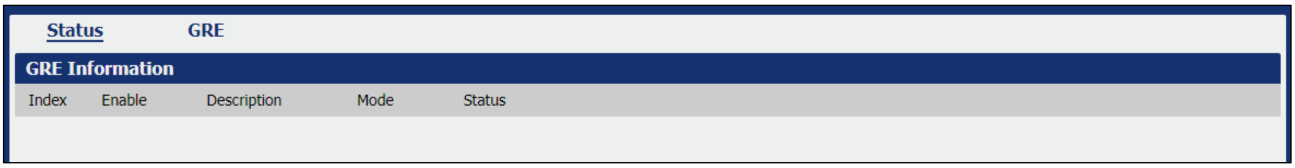
- **DPD Interval:** Allows you to enter the interval after which DPD is triggered if no IPsec protected packets is received from the peer.
- **DPD Timeout:** Allows you to enter the remote peer probe response timer.
- **Additional Configurations:** Allows you to enter some other options of IPSec in this field. Each expression can be separated by a ";".

5.7.3 GRE

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

5.7.3.1 GRE → STATUS

This parameter group allows you to view the GRE protocol status.



GRE Information

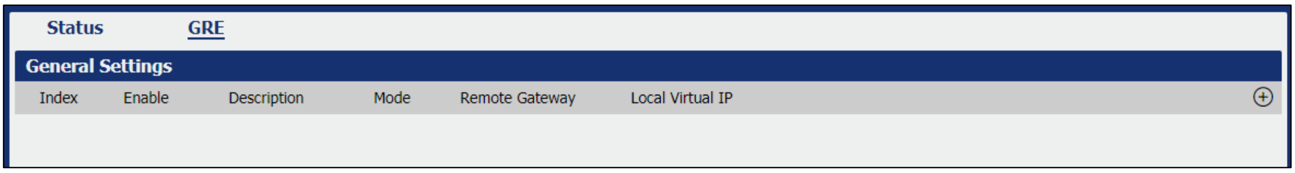
Index	Enable	Description	Mode	Status

Figure 79 – GRE status

- **Enable:** Displays current GRE settings is enable or disable.
- **Description:** Displays the description of current VPN channel.
- **Mode:** Displays the current VPN mode.
- **Status:** Displays the current VPN connection status.

5.7.3.2 GRE → GRE

This parameter group allows you to create or configure the GRE protocol.



General Settings

Index	Enable	Description	Mode	Remote Gateway	Local Virtual IP

Figure 80 – GRE settings

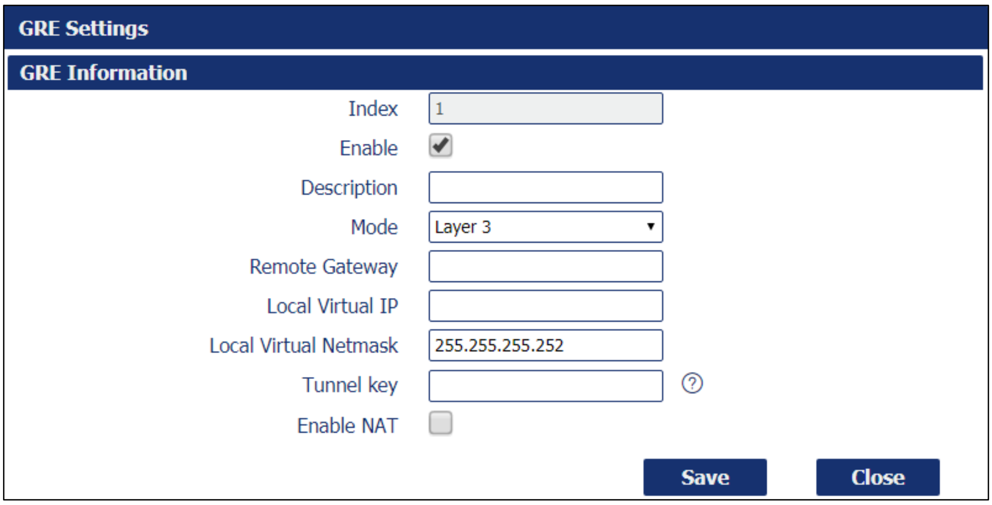
This parameter group has the following buttons:

⊕ **Button:** Allows you to add a new GRE.

✎ **Button:** Allows you to edit the settings of the selected GRE.

⊗ **Button:** Allows you to delete the selected GRE.

As you can see in **Figure 81 – GRE**, you can create a GRE by clicking the ⊕ button.



GRE Settings

GRE Information

Index	1
Enable	☑
Description	
Mode	Layer 3
Remote Gateway	
Local Virtual IP	
Local Virtual Netmask	255.255.255.252
Tunnel key	
Enable NAT	□

Figure 81 – GRE information

- **Enable:** Allows you to enable or disable GRE.
- **Description:** Allows you to enter the description of current VPN channel.
- **Mode:** Allows you to specify the running mode of GRE: "Layer 2" or "Layer 3".
- **Remote Gateway:** Allows you to enter the remote IP address of peer GRE tunnel.
- **Local Virtual IP:** Allows you to enter the local virtual netmask of GRE tunnel.
- **Local Virtual Netmask:** Allows you to enter the local virtual netmask of GRE tunnel.
- **Tunnel Key:** Allows you to enter the authentication key of GRE tunnel.
- **Enable NAT:** Allows you to enable or disable NAT.
- **Bridge Interface:** Allows you to specify the bridge interface work with Layer 2 mode.

5.8 MAINTENANCE

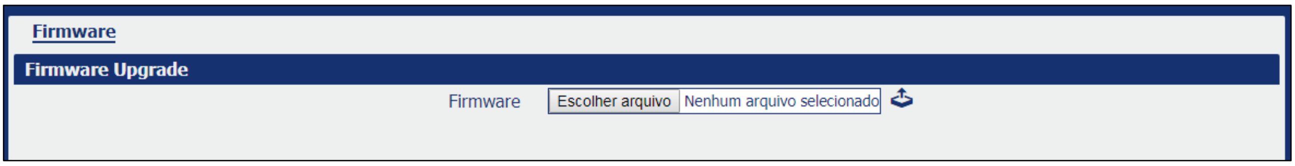
This section allows you to configure device maintenance settings.

5.8.1 UPGRADE

When new versions of **AirGate 4G** firmware become available, the user can manually update their device by uploading a package.

The device will need to be manually rebooted once the upload is complete, leaving **AirGate 4G** out of service for approximately 1 minute.

It is important to have a stable power source and ensure that power to the Fusion is not interrupted during a firmware upgrade.



Firmware

Firmware Upgrade

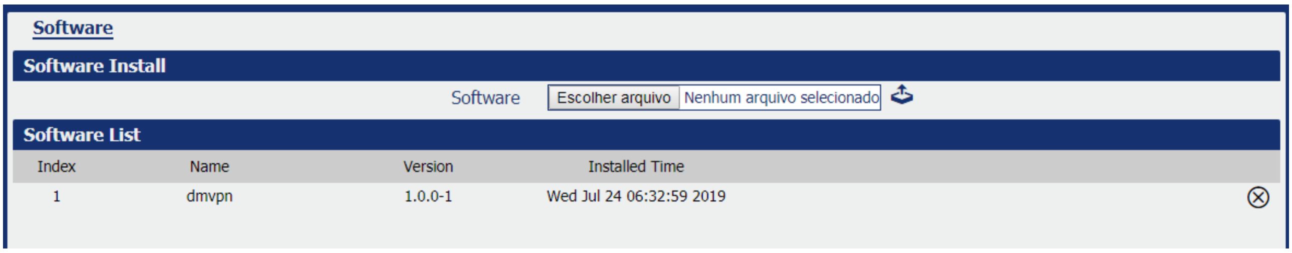
Firmware: Escolher arquivo | Nenhum arquivo selecionado ⇪

Figure 82 – Upgrade

5.8.2 SOFTWARE

When new versions of **AirGate 4G** software with new features become available, the user can manually update their device by uploading a package. You can also uninstall new device features.

The device will need to be manually restarted after a package has been uploaded or some functionality has been uninstalled, leaving **AirGate 4G** out of service for approximately 1 minute.



Software

Software Install

Software: Escolher arquivo | Nenhum arquivo selecionado ⇪

Software List

Index	Name	Version	Installed Time	
1	dmvpn	1.0.0-1	Wed Jul 24 06:32:59 2019	⊗

Figure 83 - Software

This parameter group has the following buttons:

⇪ **Button:** Allows you to upload a new update package.

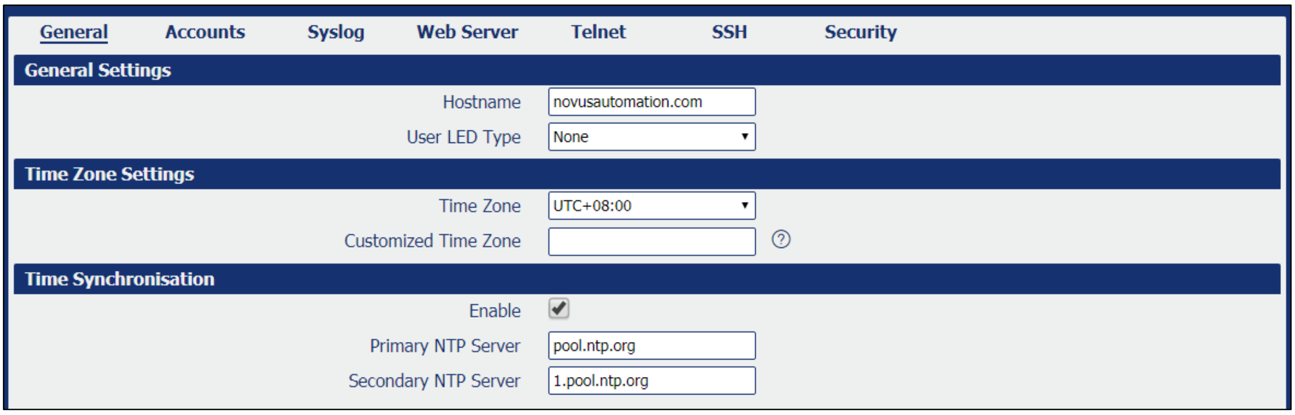
⊗ **Button:** Allows you to delete an update package.

5.8.3 SYSTEM

This tab allows you to configure the device.

5.8.3.1 SYSTEM → GENERAL

This parameter group allows you to define the general settings.



General | Accounts | Syslog | Web Server | Telnet | SSH | Security

General Settings

Hostname	novusautomation.com
User LED Type	None

Time Zone Settings

Time Zone	UTC+08:00
Customized Time Zone	

Time Synchronisation

Enable	☑
Primary NTP Server	pool.ntp.org
Secondary NTP Server	1.pool.ntp.org

Figure 84 – System

GENERAL SETTINGS

- **Hostname:** Allows you to define the router name, which might be used for IPSec local ID identify.
- **User LET Type:** Allows you to define the LED behavior: "None", "SIM" or "WiFi".

TIME ZONE SETTINGS

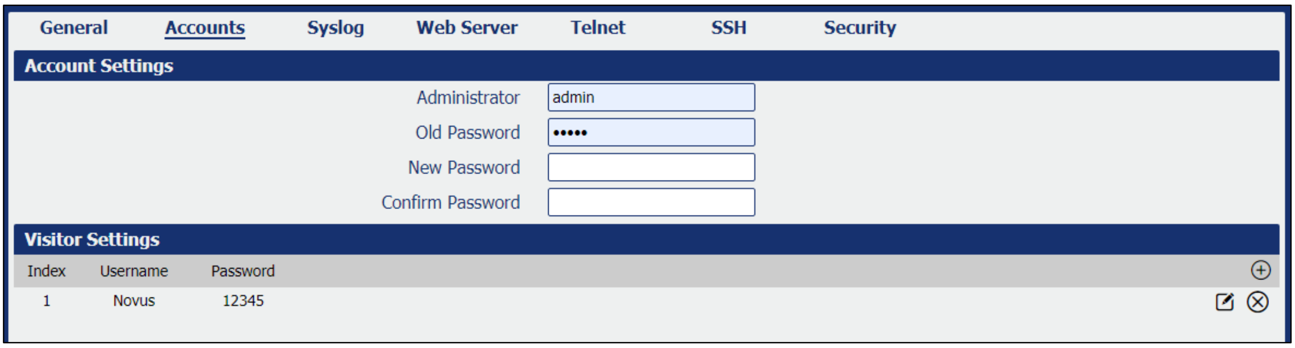
- **Time Zone:** Allows you to define the time zone where the device is in use.
- **Customized Time Zone:** Allows you to define a customized zone where the device is in use.

TIME SYNCHRONISATION

- **Enable (NTP Client):** If enabled, allows the NTP client to synchronize the device clock over the network when using a time server (NTP Server).
- **Primary NTP Server:** Allows you to enter the IP address (or host name) of the primary time server.
- **Secondary NTP Server:** Allows you to Enter the IP address (or host name) of the secondary time server.

5.8.3.2 SYSTEM → ACCOUNTS

This parameter group allows you to define user settings linked to the device.



General | Accounts | Syslog | Web Server | Telnet | SSH | Security

Account Settings

Administrator	admin
Old Password	•••••
New Password	
Confirm Password	

Visitor Settings

Index	Username	Password	⊕
1	Novus	12345	✎ ⊗

Figure 85 – Account settings

ACCOUNT SETTINGS

- **Administrator:** Displays the name of current administrator, default as "admin".
- **Old Password:** Allows you to enter the old password of administrator.
- **New Password:** Allows you to enter the new password of administrator.
- **Confirm Password:** Allows you to confirm the new password of administrator.

VISITOR SETTINGS

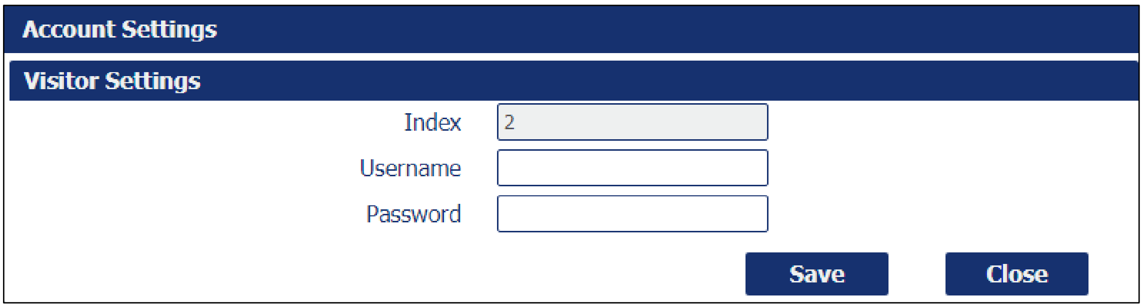
This parameter group hast the following buttons:

⊕ **Button:** Allows you to add a new visitor.

✎ **Button:** Allows you to edit the settings of the selected visitor.

⊗ **Button:** Allows you to delete the selected visitor.

As you can see in **Figure 86**, you can create a new visitor by clicking the ⊕ button.



Account Settings

Visitor Settings

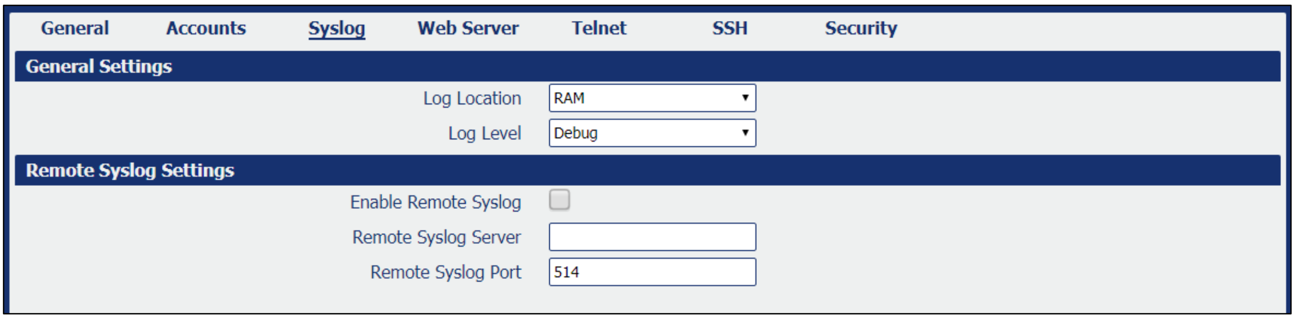
Index	2
Username	
Password	

Figure 86 – Visitor settings

- **Username:** Allows you to enter a username for the visitor.
- **Password:** Allows you to define a password for the visitor account.

5.8.3.3 SYSTEM → SYSLOG

This parameter group allows you to analyze stored system log settings.



General Settings

Log Location	RAM
Log Level	Debug

Remote Syslog Settings

Enable Remote Syslog	□
Remote Syslog Server	
Remote Syslog Port	514

Figure 87 - Syslog

GENERAL SETTINGS

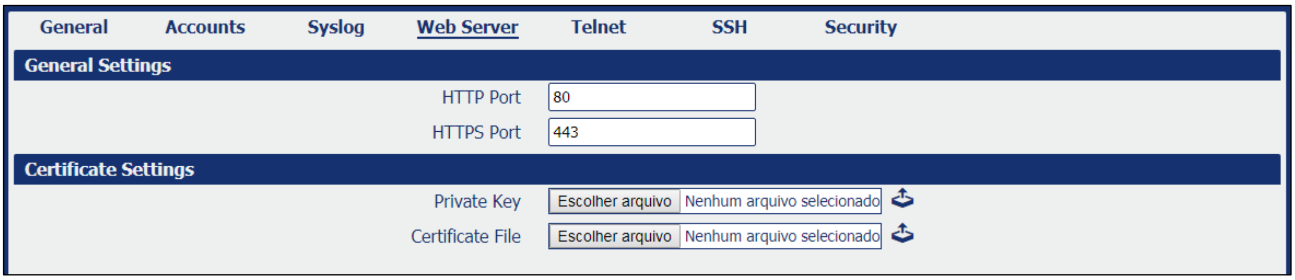
- **Log Location:** Allows you to select the log store location: "RAM" or "Flash".
- **Log Level:** Allows you to select the log output level: "Debug", "Notice", "Info", "Warning" or "Error".

REMOTE SYSLOG SETTINGS

- **Enable Remote Syslog:** Allows you to enable or disable remote syslog connection.
- **Remote Syslog Server:** Allows you to enter the IP address of remote syslog server.
- **Remote Syslog Port:** Allows you to enter the port for remote syslog server listening.

5.8.3.4 SYSTEM → WEB SERVER

This parameter group allows you to define HTTPS connection settings.



General Settings

HTTP Port	80
HTTPS Port	443

Certificate Settings

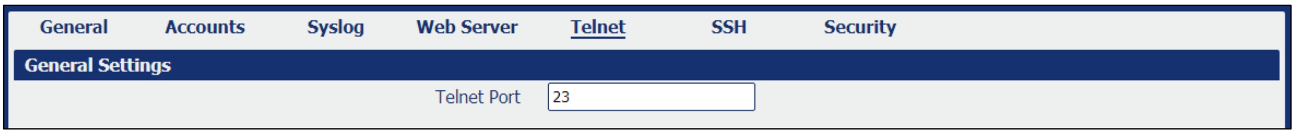
Private Key	Escolher arquivo Nenhum arquivo selecionado
Certificate File	Escolher arquivo Nenhum arquivo selecionado

Figure 88 - Web Server

- **HTTP Port:** Allows you to enter the port for Hypertext Transfer Protocol. A well-known port for HTTP is port 80.
- **HTTPS Port:** Allows you to enter the port for HTTPS Protocol. A well-known port for HTTPS is port 443.
- **Private Key:** Allows you to import private Key file for HTTPS connection.
- **Certificate File:** Allows you to import certificate file for HTTPS connection.

5.8.3.5 SYSTEM → TELNET

This parameter group allows you to define the Telnet port.



General Settings

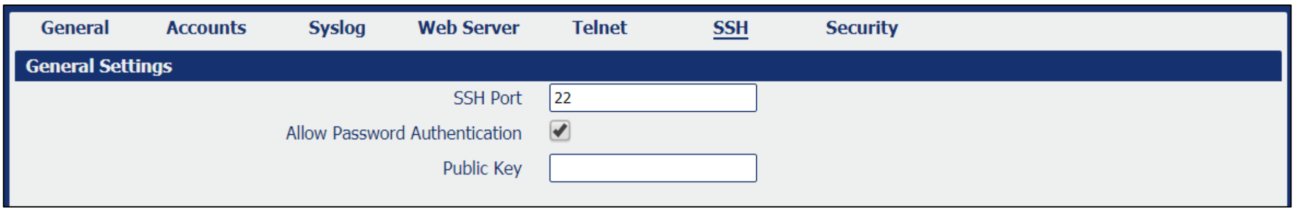
Telnet Port: 23

Figure 89 - Telnet

- **Telnet Port:** Allows you to enter the port for telnet access. A well-known port for HTTP is port 23.

5.8.3.6 SYSTEM → SSH

This parameter group allows you to enable and configure SSH.



General Settings

SSH Port: 22

Allow Password Authentication ☑

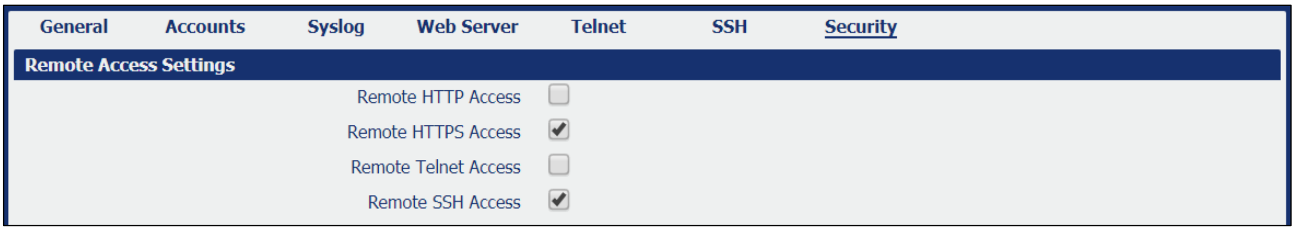
Public Key:

Figure 90 – SSH

- **SSH Port:** Allows you to enter the port for SSH access. A well-known port for HTTP is port 22.
- **Allow Password Authentication:** Allows you to enable or disable SSH authentication.
- **Public Key:** Allows you to enter the public Key SSH authentication.

5.8.3.7 SYSTEM → SECURITY

This parameter group allows you to enable or disable security settings for remote access.



Remote Access Settings

Remote HTTP Access ☐

Remote HTTPS Access ☑

Remote Telnet Access ☐

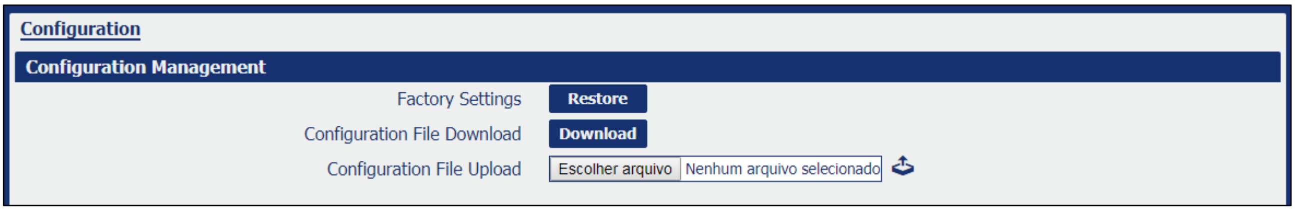
Remote SSH Access ☑

Figure 91 – Security

- **Remote HTTP Access:** Allows you to allow remote HTTP access.
- **Remote HTTPS Access:** Allows you to allow remote HTTPS access.
- **Remote Telnet Access:** Allows you to allow remote Telnet access.
- **Remote SSH Access:** Allows you to allow remote SSH access.

5.8.4 CONFIGURATION

This tab allows you to save parameters (settings in the Web interface) to a file. Conversely, if you have saved settings from the **AirGate 4G** router to a file, you can Import these previously-saved configuration settings to the **AirGate 4G** router as well.



Configuration

Configuration Management

Factory Settings: Restore

Configuration File Download: Download

Configuration File Upload: Escolher arquivo | Nenhum arquivo selecionado

Figure 92 – Configuration

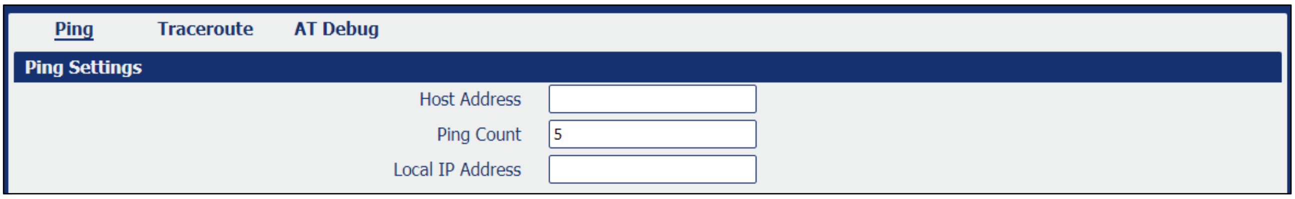
- **Factory Settings:** Click the **Restore** button allows you to reset the device to factory default settings.
- **Configuration File Download:** Click the **Download** button allows you to download the configuration file from **AirGate 4G** router.
- **Configuration File Upload:** Allows you to import previously-saved configuration file.

5.8.5 DEBUG TOOLS

This tab allows you to configure debug tools.

5.8.5.1 DEBUG TOOLS → PING

This parameter group allows you to configure the tool to perform ping commands.



Ping | Traceroute | AT Debug

Ping Settings

Host Address:

Ping Count: 5

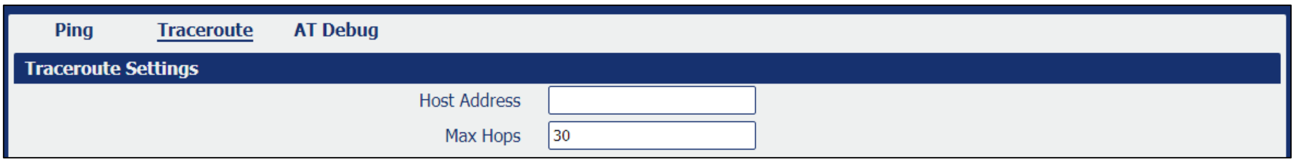
Local IP Address:

Figure 93 – Ping

- **Host Address:** Allows you to enter a host IP address or domain name for ping.
- **Ping Count:** Allows you to enter the ping times.
- **Local IP Address:** Allows you to enter the ping source IP address or leave it blank.

5.8.5.2 DEBUG TOOLS → TRACEROUTE

This parameter group allows you to configure Traceroute, whose purpose is to test the path taken by the package to its destination.



Ping | Traceroute | AT Debug

Traceroute Settings

Host Address:

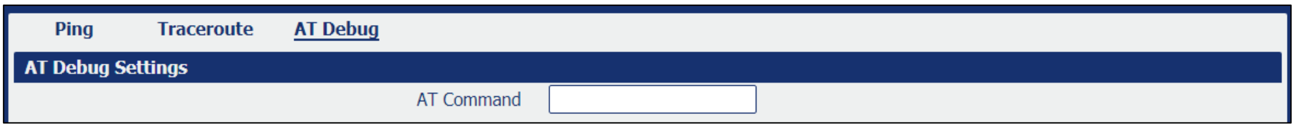
Max Hops: 30

Figure 94 - Traceroute

- **Host Address:** Allows you to enter a host IP address or domain name for traceroute.
- **Max Hops:** Allows you to enter the max hops for traceroute.

5.8.5.3 DEBUG TOOLS → AT DEBUG

This parameter allows you to enter an AT command.



Ping | Traceroute | AT Debug

AT Debug Settings

AT Command:

Figure 95 - AT Debug

- **AT Command:** Allows you to enter the AT command of the module.

6 TUTORIALS

This chapter presents tutorials that show how to configure different features of the **AirGate 4G**.

6.1 RS232: TRANSPARENT MODE WITH TCP CLIENT

This tutorial shows how to configure and use the Transparent mode of the RS232 interface with **AirGate 4G** configured as TCP Client.

6.1.1 TOPOLOGY

You can use the following topology:

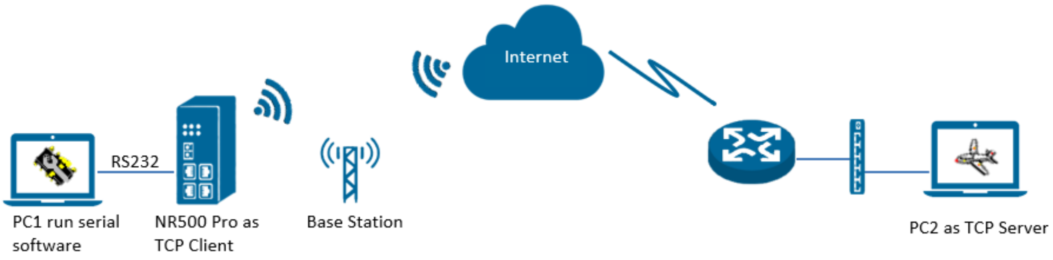


Figure 95 – RS232: Transparent mode

1. **AirGate 4G** runs as TCP Client and connect to Internet with SIM card.
2. PC1 simulate as serial device and runs serial software, such as Hercules. Hercules will send the data to the TCP server side through **AirGate 4G** with TCP transparent mode.
3. PC2 runs as TCP server and assume it can get the Public Static IP address. PC2 enable TCP software, such as TCPUDPDbg. TCPUDPDbg can receive the data from TCP Client side.

6.1.2 RS232 CABLE

Follow **Figure 96** bellow to make the RS232 cable:

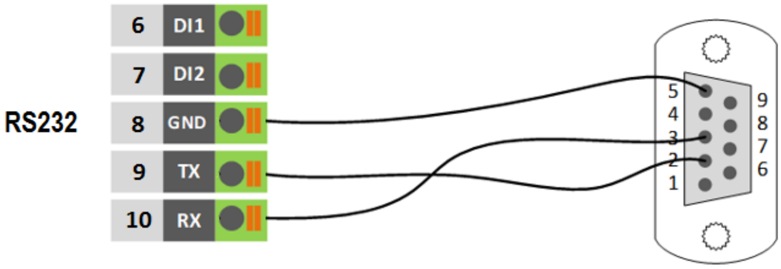


Figure 96 – RS232 Cable

Table 10 shows the connector pins:

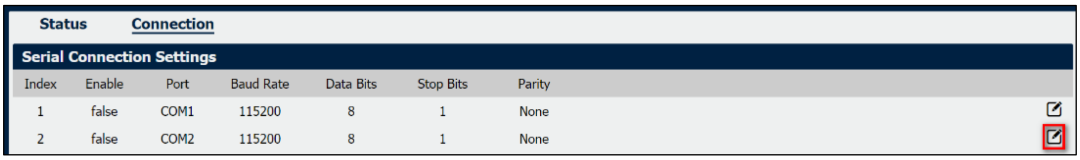
PIN	RS232	RS485	DI	DO	DIRECTION
6	--	--	DI1	--	Router ← Device
7	--	--	DI2	--	Router ← Device
8	GND	--	--	--	--
9	TX	--	--	--	Router → Device
10	RX	--	--	--	Router ← Device

Table 10 – RS232 connector pins

6.1.3 CONFIGURATION

6.1.3.1 RS232 CONFIGURATION

To configure RS232 interface, you must open the Web Interface of **AirGate 4G** and go to **Industrial Interface > Serial > Connection > Index 2**. To perform the interface configuration, just click on the COM2 edit button.

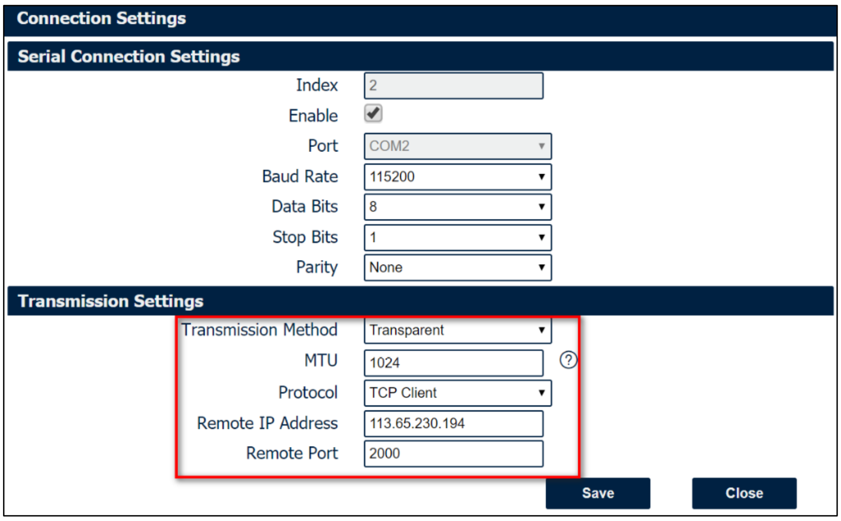


Serial Connection Settings

Index	Enable	Port	Baud Rate	Data Bits	Stop Bits	Parity
1	false	COM1	115200	8	1	None
2	false	COM2	115200	8	1	None

Figure 97 – RS232 configuration

To enable RS232 configuration, you must select the protocol as "TCP Client" and enter the server IP address and server port. Then click **Save**.



Connection Settings

Serial Connection Settings

Index	2
Enable	☑
Port	COM2
Baud Rate	115200
Data Bits	8
Stop Bits	1
Parity	None

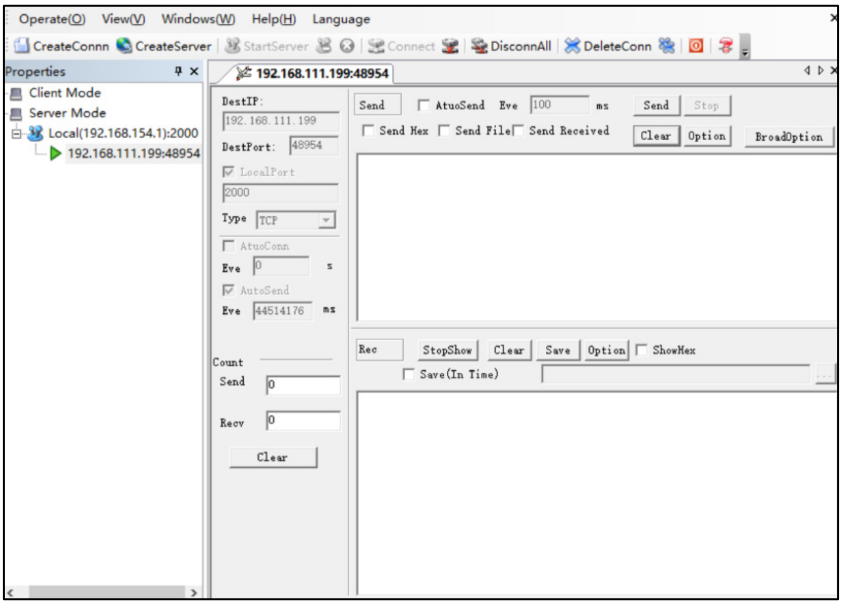
Transmission Settings

Transmission Method	Transparent
MTU	1024
Protocol	TCP Client
Remote IP Address	113.65.230.194
Remote Port	2000

Figure 98 – Transmission configurations

6.1.3.2 TCP SERVER CONFIGURATION

To configure TCP server, you must run the TCP Software "TCPUDPDbg" on server PC2. **AirGate 4G** will connect to the TCP Server automatically.



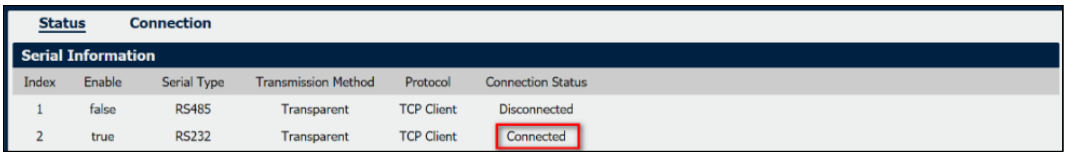
Local(192.168.154.1):2000
192.168.111.199:48954

DestIP:	192.168.111.199
DestPort:	48954
☑ LocalPort	2000
Type	TCP
□ AtuoConn	
Eve	0 s
☑ AutoSend	
Eve	44514176 ms
Count Send	0
Recv	0

□ AtuoSend Eve 100 ms

Figure 99 – TCPUDPDDbg Software

In the **AirGate 4G** Web Interface, go to **Industrial Interface > Serial > Status > Serial Information > Index2**. It will show the connection status.



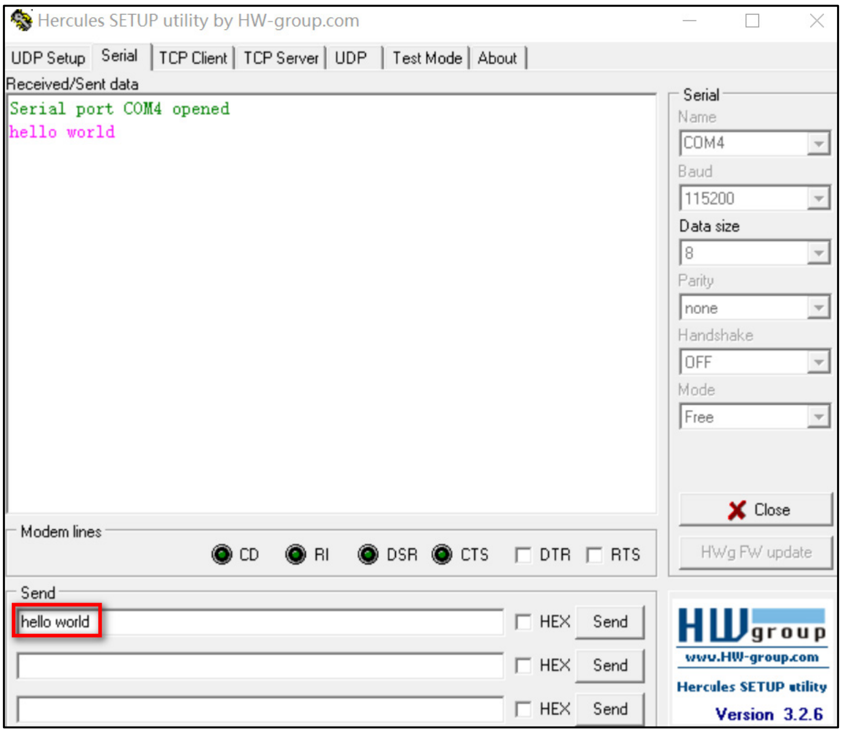
Serial Information

Index	Enable	Serial Type	Transmission Method	Protocol	Connection Status
1	false	RS485	Transparent	TCP Client	Disconnected
2	true	RS232	Transparent	TCP Client	Connected

Figure 100 – RS232 status connection

6.1.4 TEST

To perform a test, run serial software "Hercules" on PC1 and send the data "hello world".



Hercules SETUP utility by HW-group.com

Received/Sent data

```
Serial port COM4 opened
hello world
```

Serial

Name: COM4

Baud: 115200

Data size: 8

Parity: none

Handshake: OFF

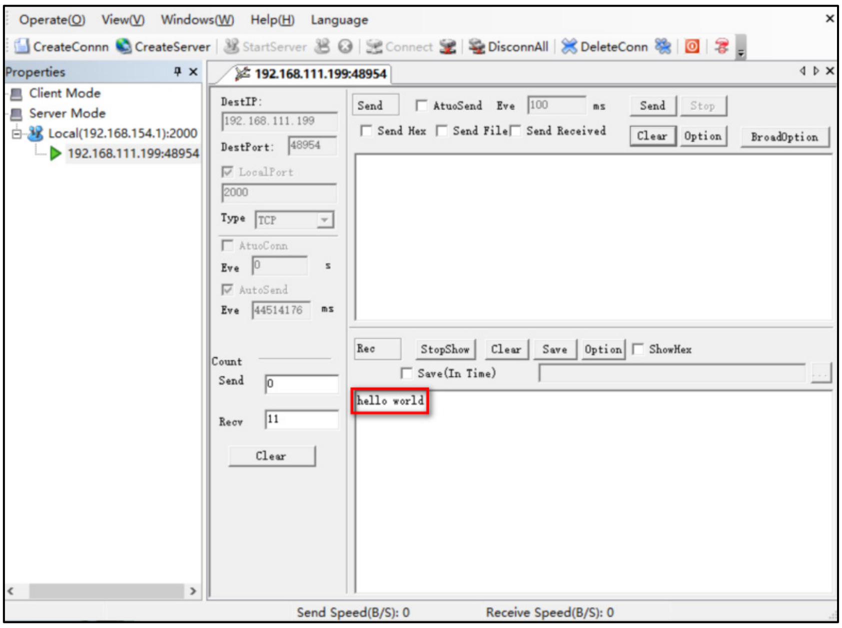
Mode: Free

Modem lines: ● CD ● RI ● DSR ● CTS □ DTR □ RTS

Send: hello world □ HEX

Figure 101 – RS232 test

TCP Server side can receive the data "hello world", as shown in **Figure 102**. Test successfully.



Properties

- Client Mode
- Server Mode
  - Local(192.168.154.1):2000
    - 192.168.111.199:48954

192.168.111.199:48954

DestIP: 192. 168. 111. 199

DestPort: 48954

☑ LocalPort: 2000

Type: TCP

□ AtuoConn Eve 0 s

☑ AutoSend Eve 44514176 ms

□ AtuoSend Eve 100 ms

□ Send Hex □ Send File □ Send Received

□ ShowHex

□ Save(In Time)

```
hello world
```

Count

Send: 0

Recv: 11

Send Speed(B/S): 0 Receive Speed(B/S): 0

Figure 102 – RS232 test result

6.2 RS485: TRANSPARENT MODE WITH TCP CLIENT

This tutorial shows how to configure and use the Transparent mode of the RS485 interface with **AirGate 4G** configured as TCP Client.

6.2.1 TOPOLOGY

You can use the following topology:

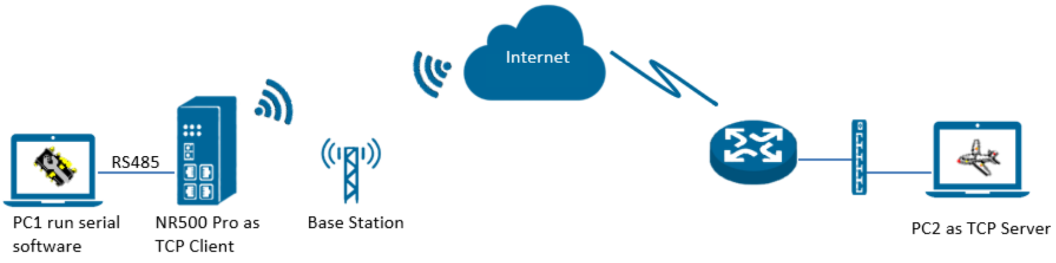


Figure 103 – RS485: Transparent mode

1. **AirGate 4G** runs as TCP Client and connect to Internet with SIM card.
2. PC1 simulate as serial device and runs serial software, such as Hercules. Hercules will send the data to the TCP server side through **AirGate 4G** with TCP transparent mode.
3. PC2 runs as TCP server and assume it can get the Public Static IP address. PC2 enable TCP software, such as TCPUDPDbg. TCPUDPDbg can receive the data from TCP Client side.

6.2.2 RS485 CABLE

Follow **Figure 104** bellow to make the RS485 cable:

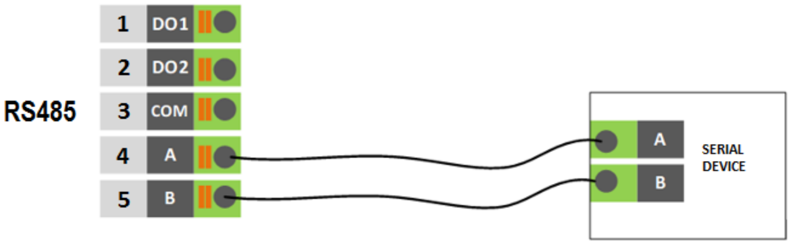


Figure 104 – RS485 Cable

Table 11 shows the connector pins:

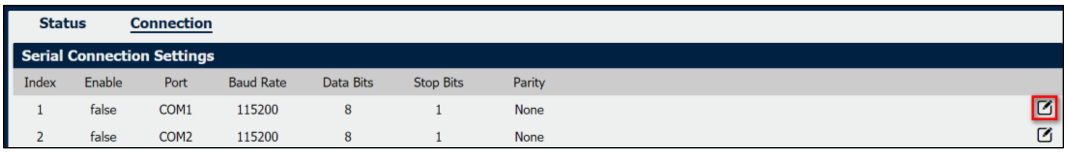
PIN	RS232	RS485	DI	DO	DIRECTION
1	--	--	--	DO1	Router → Device
2	--	--	--	DO2	Router → Device
3	--	--	--	COM	--
4	--	D1	--	--	Router ↔ Device
5	--	D0	--	--	Router ↔ Device

Table 11 – RS485 connector pins

6.2.3 CONFIGURATION

6.2.3.1 RS485 CONFIGURATION

To configure RS485 interface, you must open the Web Interface of **AirGate 4G** and go to **Industrial Interface** > **Serial** > **Connection** > **Index 1**. To perform the interface configuration, just click on the COM1 edit button.

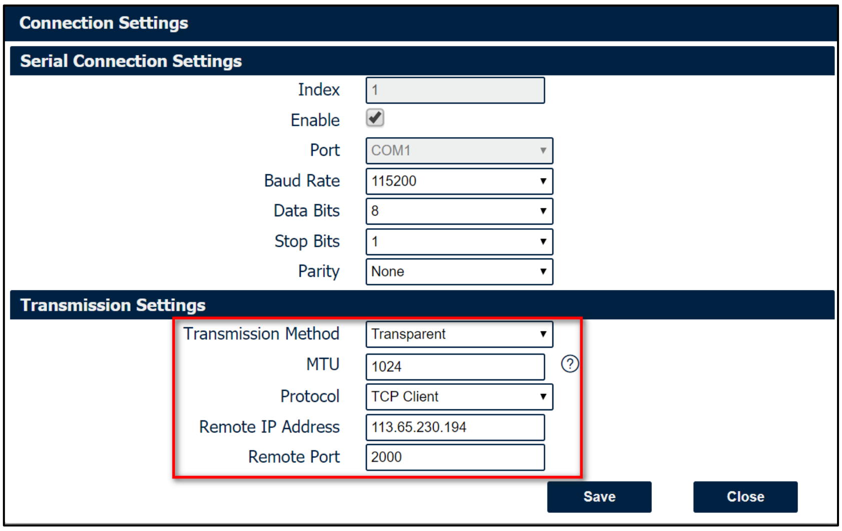

Status Connection

Serial Connection Settings

Index	Enable	Port	Baud Rate	Data Bits	Stop Bits	Parity
1	false	COM1	115200	8	1	None
2	false	COM2	115200	8	1	None

Figure 105 – RS485 configuration

To enable RS485 configuration, you must select the protocol as "TCP Client" and enter the server IP address and server port. Then click **Save.**



Connection Settings

Serial Connection Settings

Index: 1

Enable: ☑

Port: COM1

Baud Rate: 115200

Data Bits: 8

Stop Bits: 1

Parity: None

Transmission Settings

Transmission Method: Transparent

MTU: 1024

Protocol: TCP Client

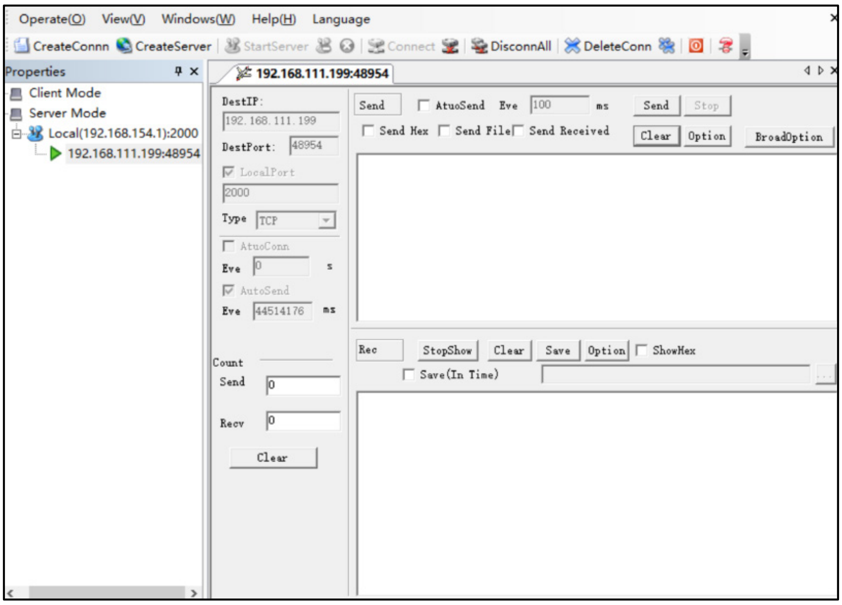
Remote IP Address: 113.65.230.194

Remote Port: 2000

Figure 106 – Transmission configurations

6.2.3.2 TCP SERVER CONFIGURATION

To configure TCP server, you must run the TCP Software "TCPUDPDbg" on server PC2. **AirGate 4G** will connect to the TCP Server automatically.



DestIP: 192.168.111.199

DestPort: 48954

☑ LocalPort 2000

Type TCP

☐ AtuoConn

Eve 0 s

☑ AutoSend

Eve 44514176 ms

☐ AtuoSend Eve 100 ms

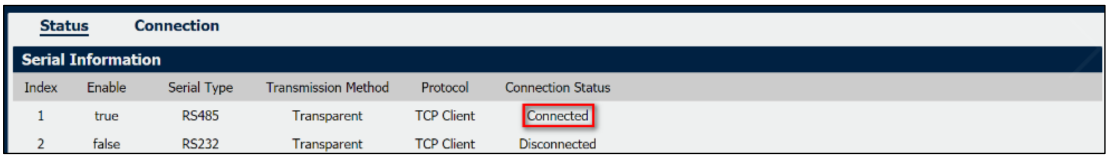
Count

Send 0

Recv 0

Figure 107 – TCPUDPDDbg Software

In the **AirGate 4G** Web Interface, go to **Industrial Interface > Serial > Status > Serial Information > Index1**. It will show the connection status.



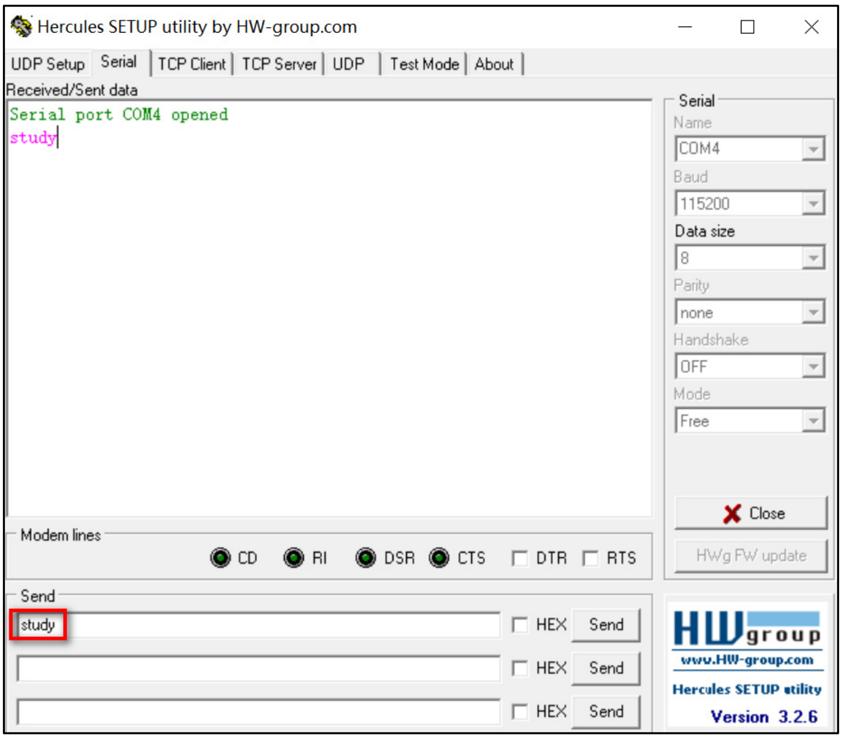
Serial Information

Index	Enable	Serial Type	Transmission Method	Protocol	Connection Status
1	true	RS485	Transparent	TCP Client	Connected
2	false	RS232	Transparent	TCP Client	Disconnected

Figure 108 – RS485 status connection

6.2.4 TEST

To perform a test, run serial software "Hercules" on PC1 and send the data "study".



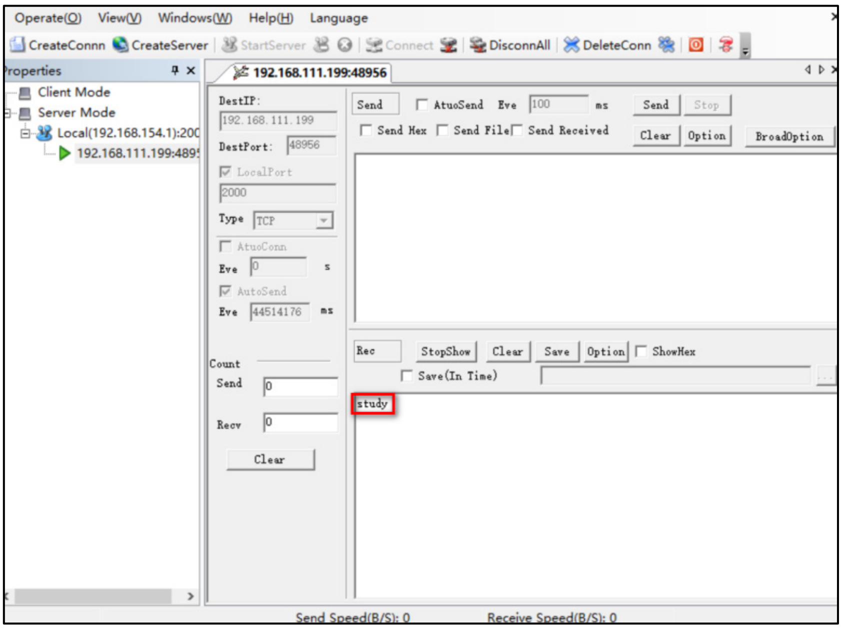
```
Serial port COM4 opened
study
```

Serial
Name: COM4
Baud: 115200
Data size: 8
Parity: none
Handshake: OFF
Mode: Free

Send: study

Figure 109 – RS485 test

TCP Server side can receive the data "study", as shown in **Figure 110**. Test successfully.



DestIP: 192.168.111.199
DestPort: 48956
☑ LocalPort: 2000
Type: TCP
□ AtuoConn Eve 0 s
☑ AutoSend Eve 44514176 ms
Count Send 0
Recv 0
Eve 100 ms

study

Send Speed(B/S): 0 Receive Speed(B/S): 0

Figure 110 – RS485 test result

6.3 OpenVPN CERTIFICATES GENERATED

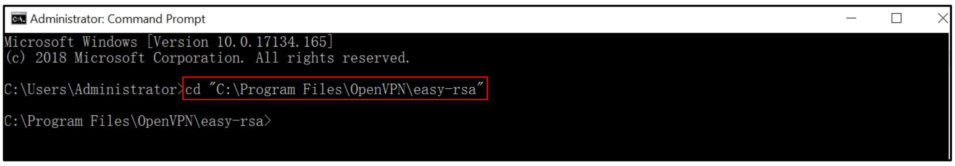
This tutorial shows how to generate certificates needed to use OpenVPN.

6.3.1 OpenVPN SOFTWARE INSTALLED

You must download the OpenVPN software, located at http://openvpn.net/index.php, and install it on a Windows computer.

6.3.2 CERTIFICATES GENERATED

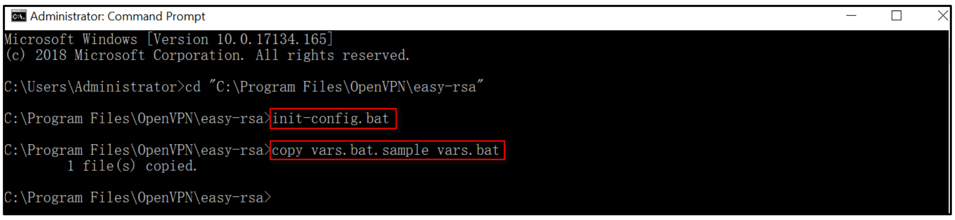
To generate a certificate, you must run as an administrator the Windows command prompt and type the following **cd** command to **"C:\Program Files\OpenVPN\easy-rsa"**, as shown in the figure below:



```
Microsoft Windows [Version 10.0.17134.165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd "C:\Program Files\OpenVPN\easy-rsa"

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 111 – **cd** "**C:\Program Files\OpenVPN\easy-rsa**" command

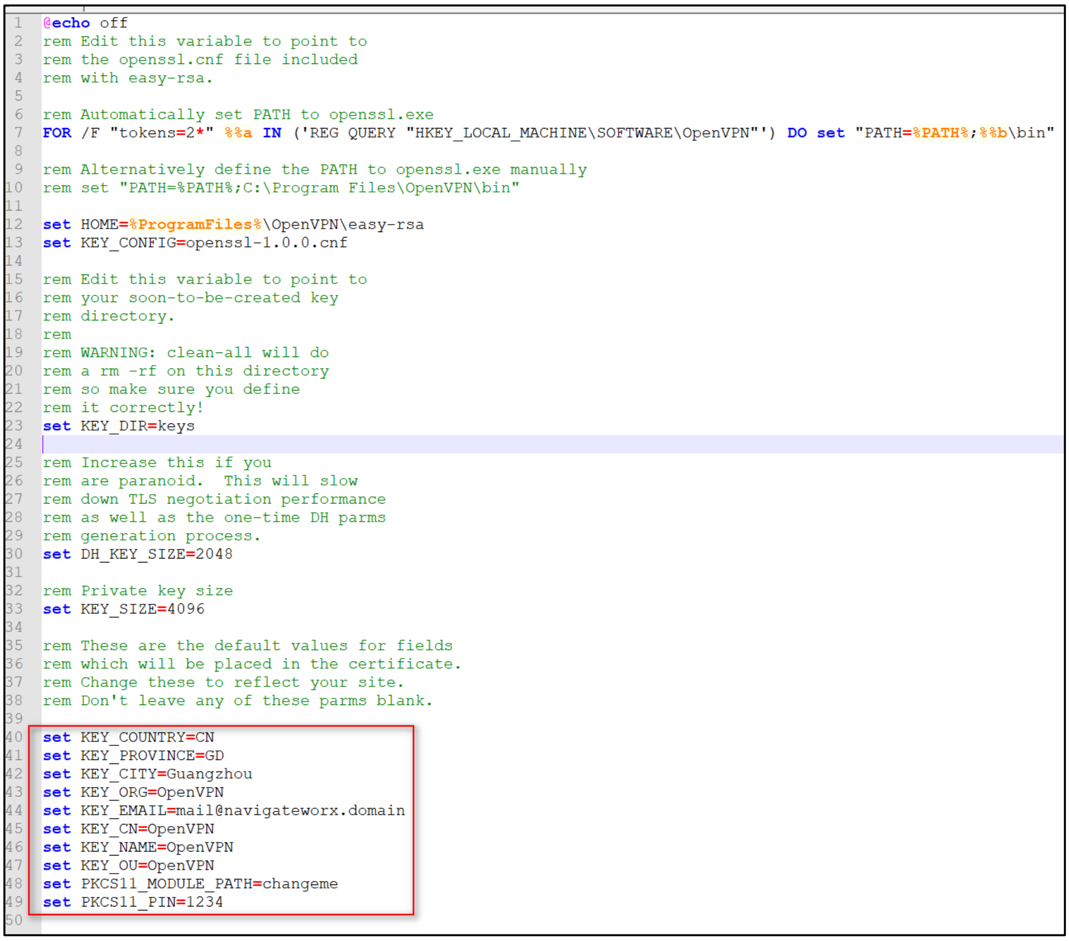
Then run the **init-config.bat** command to copy the configuration files to **vars.bat** (this command will overwrite both the previous **vars.bat** file and the **openssl.cnf** files).



```
Microsoft Windows [Version 10.0.17134.165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd "C:\Program Files\OpenVPN\easy-rsa"

C:\Program Files\OpenVPN\easy-rsa>init-config.bat

C:\Program Files\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
        1 file(s) copied.

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 112 – **init-config.bat** command

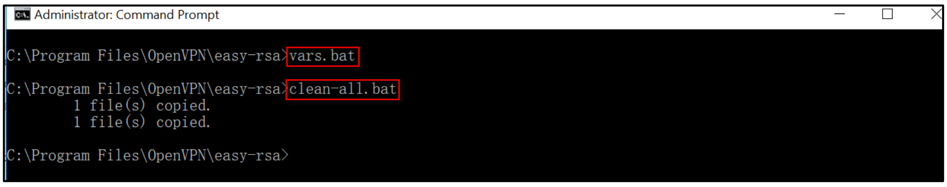
Edit the **vars.bat file** and set the KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, KEY_ORG, KEY_EMAIL, KEY_CN, KEY_NAME, KEY_OU, PKCS11_MODULE_PATH and PKCS11_PIN parameters (parameters must be entered without space):



```
@echo off
rem Edit this variable to point to
rem the openssl.cnf file included
rem with easy-rsa.

rem Automatically set PATH to openssl.exe
FOR /F "tokens=2*" %%a IN ('REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\OpenVPN"') DO set "PATH=%PATH%;%%b\bin"

rem Alternatively define the PATH to openssl.exe manually
rem set "PATH=%PATH%;C:\Program Files\OpenVPN\bin"

set HOME=%ProgramFiles%\OpenVPN\easy-rsa
set KEY_CONFIG=openssl-1.0.0.cnf

rem Edit this variable to point to
rem your soon-to-be-created key
rem directory.
rem
rem WARNING: clean-all will do
rem a rm -rf on this directory
rem so make sure you define
rem it correctly!
set KEY_DIR=keys

rem Increase this if you
rem are paranoid.  This will slow
rem down TLS negotiation performance
rem as well as the one-time DH parms
rem generation process.
set DH_KEY_SIZE=2048

rem Private key size
set KEY_SIZE=4096

rem These are the default values for fields
rem which will be placed in the certificate.
rem Change these to reflect your site.
rem Don't leave any of these parms blank.

set KEY_COUNTRY=CN
set KEY_PROVINCE=GD
set KEY_CITY=Guangzhou
set KEY_ORG=OpenVPN
set KEY_EMAIL=mail@navigateworx.domain
set KEY_CN=OpenVPN
set KEY_NAME=OpenVPN
set KEY_OU=OpenVPN
set PKCS11_MODULE_PATH=changeme
set PKCS11_PIN=1234

```

Figure 113 – Editing the parameters

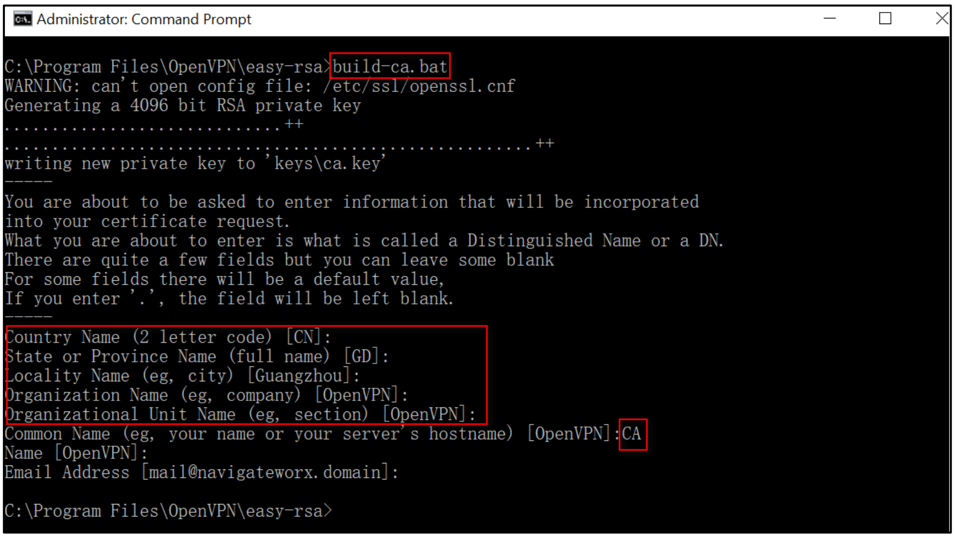
Run the **vars.bat** and **clean-all.bat** commands, as shown in the figure below, to initialize the environment:



```
C:\Program Files\OpenVPN\easy-rsa>vars.bat

C:\Program Files\OpenVPN\easy-rsa>clean-all.bat
        1 file(s) copied.
        1 file(s) copied.

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 114 – vars.bat and **clean-all.bat** commands

The **build-ca.bat** command will build the certificate authority (CA) and the private key via the interactive openssl command.

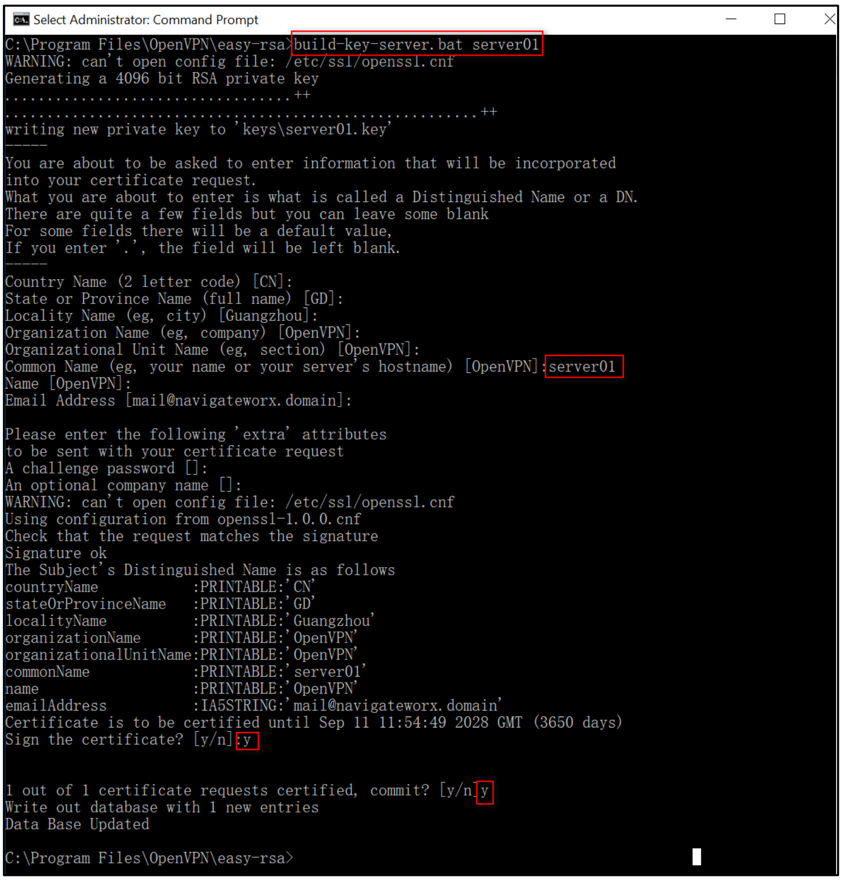


```
C:\Program Files\OpenVPN\easy-rsa>build-ca.bat
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating a 4096 bit RSA private key
.............................++
........................................................++
writing new private key to 'keys\ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [Guangzhou]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [OpenVPN]:
Common Name (eg, your name or your server's hostname) [OpenVPN]:CA
Name [OpenVPN]:
Email Address [mail@navigateworx.domain]:

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 115 – build-ca.bat command

In the sequence above, most of the parameters show the values configured in the **vars.bat file**. The only parameter to be filled in must be the Common Name parameter, as shown in **Figure 115**.

After that, you need to generate a certificate and private key for the server by using the **build-key-server.bad server01** command. When the information to be inserted in the **Common Name** parameter is requested, insert **server01**.

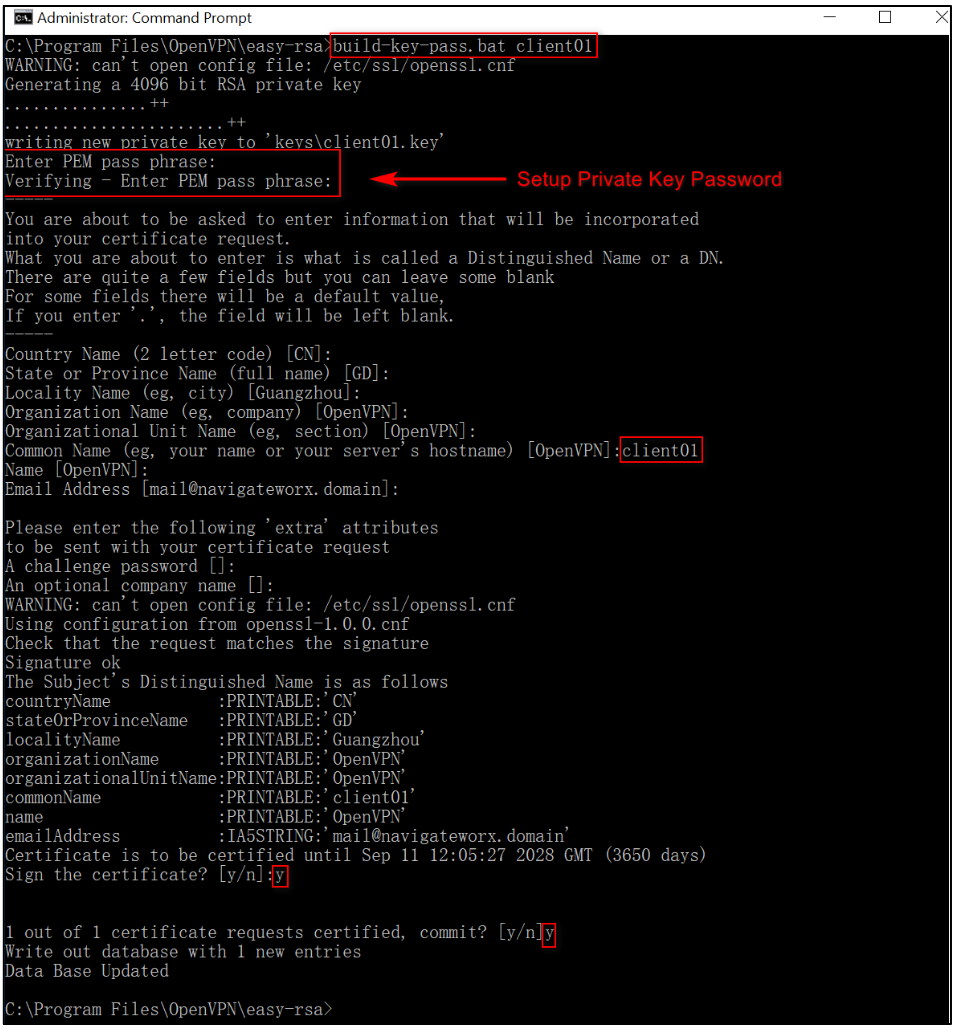


```
C:\Program Files\OpenVPN\easy-rsa>build-key-server.bat server01
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating a 4096 bit RSA private key
..................................++
........................................................++
writing new private key to 'keys\server01.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [Guangzhou]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [OpenVPN]:
Common Name (eg, your name or your server's hostname) [OpenVPN]:server01
Name [OpenVPN]:
Email Address [mail@navigateworx.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'GD'
localityName          :PRINTABLE:'Guangzhou'
organizationName      :PRINTABLE:'OpenVPN'
organizationalUnitName:PRINTABLE:'OpenVPN'
commonName            :PRINTABLE:'server01'
name                  :PRINTABLE:'OpenVPN'
emailAddress          :IA5STRING:'mail@navigateworx.domain'
Certificate is to be certified until Sep 11 11:54:49 2028 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 116 – build-key-server.bat server01 command

In the **build-key-server.bat server01** command, **server01** is the file name of the certificate (the name of the private key and the public key).

The next step involves generating the client's certificate and private key when using the **build-key-pass.bat client01** command. You will need to use the key authentication in the OpenVPN client configuration. When the information to be inserted in the **Common Name** parameter is requested, insert **client01**.

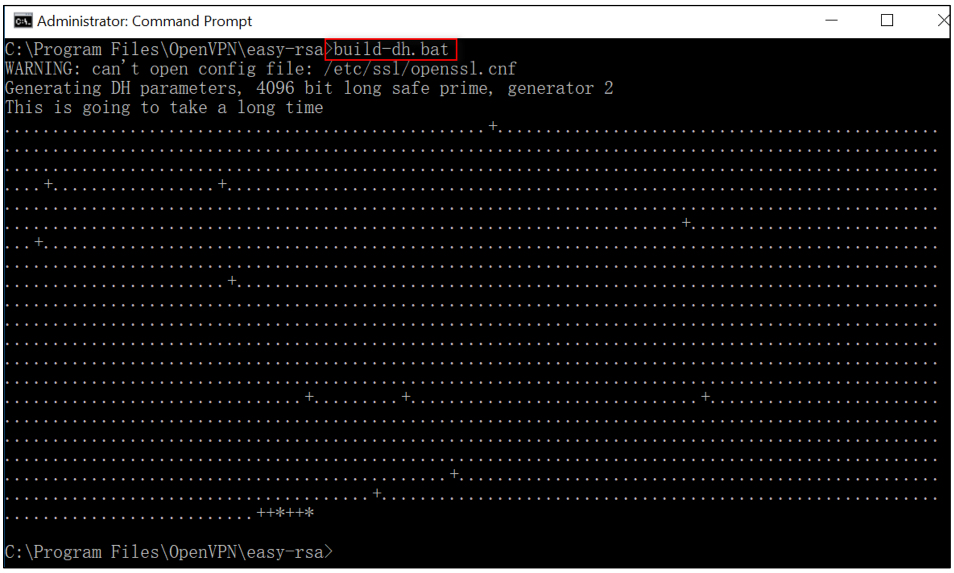


```
C:\Program Files\OpenVPN\easy-rsa>build-key-pass.bat client01
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating a 4096 bit RSA private key
..............++
......................++
writing new private key to 'keys\client01.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [GD]:
Locality Name (eg, city) [Guangzhou]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [OpenVPN]:
Common Name (eg, your name or your server's hostname) [OpenVPN]:client01
Name [OpenVPN]:
Email Address [mail@navigateworx.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'GD'
localityName          :PRINTABLE:'Guangzhou'
organizationName      :PRINTABLE:'OpenVPN'
organizationalUnitName:PRINTABLE:'OpenVPN'
commonName            :PRINTABLE:'client01'
name                  :PRINTABLE:'OpenVPN'
emailAddress          :IA5STRING:'mail@navigateworx.domain'
Certificate is to be certified until Sep 11 12:05:27 2028 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 117 – **build-key-pass.bat client01** command

In the **build-key-pass.bat client01** command, **client01** is the file name of the certificate (the name of the private key and the public key). **You must use a unique name for each client.**

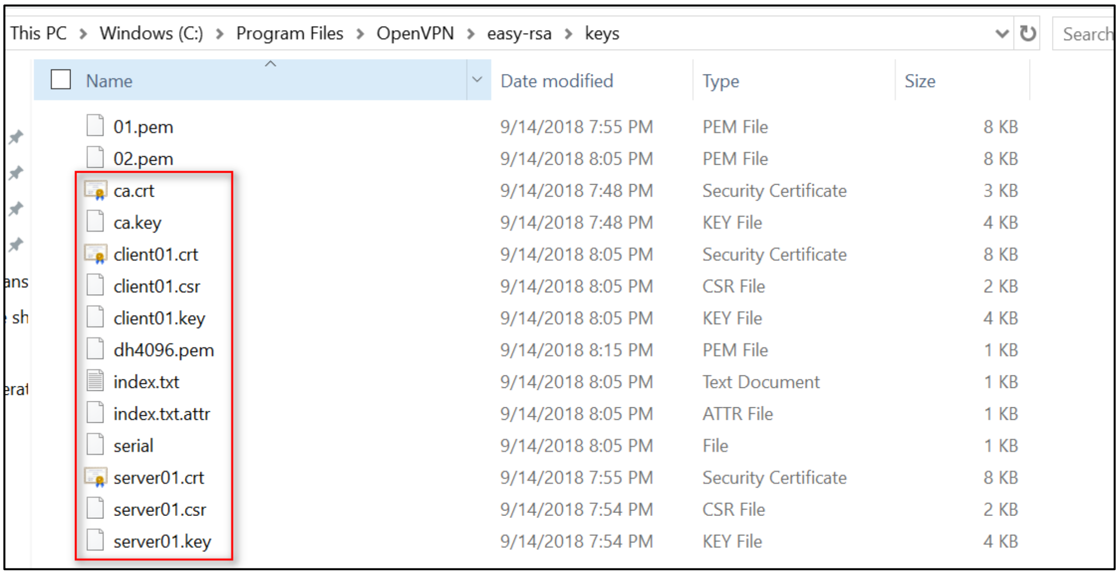
After that, generate Diffie Hellman parameters.



```
C:\Program Files\OpenVPN\easy-rsa>build-dh.bat
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating DH parameters, 4096 bit long safe prime, generator 2
This is going to take a long time
..................................................+..............................................
.................................................................................................
.................................................................................................
....+.................+..........................................................................
.................................................................................................
......................................................................+..........................
...+.............................................................................................
.................................................................................................
.......................+.........................................................................
.................................................................................................
.................................................................................................
.................................................................................................
.................................................................................................
.................................................................................................
...............................+.........+..............................+........................
.................................................................................................
.................................................................................................
.................................................................................................
..............................................+..................................................
......................................+..........................................................
..........................++*++*

C:\Program Files\OpenVPN\easy-rsa>
```

Figure 118 – Diffie Hellman parameters

Once the certificates had been generated, you can check them out on path **C:\Program Files\OpenVPN\easy-rsa\keys.**


This PC > Windows (C:) > Program Files > OpenVPN > easy-rsa > keys
Search
ans
sh
erat

Name	Date modified	Type	Size
01.pem	9/14/2018 7:55 PM	PEM File	8 KB
02.pem	9/14/2018 8:05 PM	PEM File	8 KB
ca.crt	9/14/2018 7:48 PM	Security Certificate	3 KB
ca.key	9/14/2018 7:48 PM	KEY File	4 KB
client01.crt	9/14/2018 8:05 PM	Security Certificate	8 KB
client01.csr	9/14/2018 8:05 PM	CSR File	2 KB
client01.key	9/14/2018 8:05 PM	KEY File	4 KB
dh4096.pem	9/14/2018 8:15 PM	PEM File	1 KB
index.txt	9/14/2018 8:05 PM	Text Document	1 KB
index.txt.attr	9/14/2018 8:05 PM	ATTR File	1 KB
serial	9/14/2018 8:05 PM	File	1 KB
server01.crt	9/14/2018 7:55 PM	Security Certificate	8 KB
server01.csr	9/14/2018 7:54 PM	CSR File	2 KB
server01.key	9/14/2018 7:54 PM	KEY File	4 KB

Figure 119 – List of certificates

6.4 OpenVPN WITH X.509 CERTIFICATE

This tutorial shows how to configure OpenVPN with a X.509 certificate.

6.4.1 TOPOLOGY

You can use the following topology:

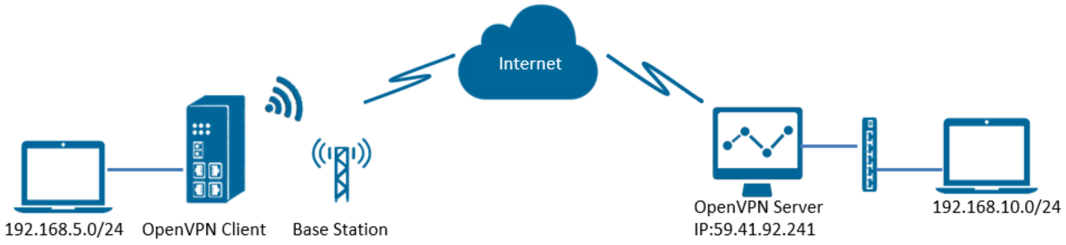


Figure 120 – OpenVPN with X.509 certificate

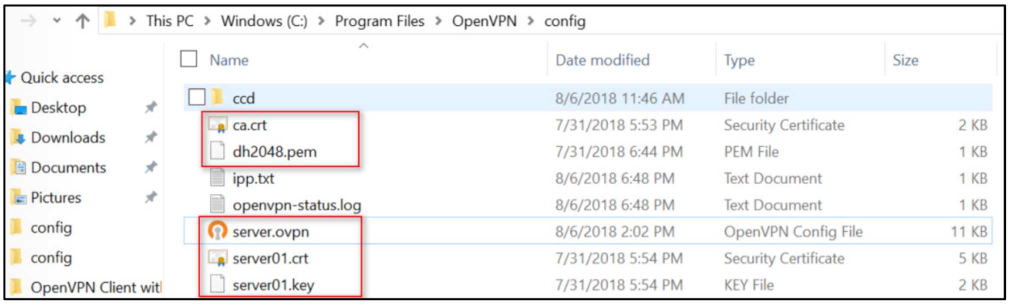
1. **AirGate 4G** runs as OpenVPN Client with any kind of IP, which can ping OpenVPN server IP successfully.
2. A PC runs as OpenVPN Server with a static public IP and open a specified a listening port for OpenVPN.
3. OpenVPN tunnel is established between Server and Client, the subnet can Ping each other successfully.

6.4.2 CONFIGURATION

6.4.2.1 SERVER CONFIGURATION

To configure a computer as a server, you must download the OpenVPN software, available at https://openvpn.net/, and run and install it with administrator authority.

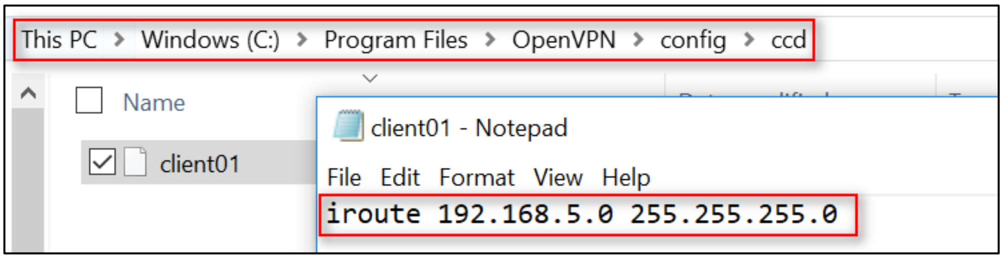
Once the software has been installed, you should copy the related certificates and the specific configuration to your computer, as shown in the figure below:



Name	Date modified	Type	Size
ccd	8/6/2018 11:46 AM	File folder	
ca.crt	7/31/2018 5:53 PM	Security Certificate	2 KB
dh2048.pem	7/31/2018 6:44 PM	PEM File	1 KB
ipp.txt	8/6/2018 6:48 PM	Text Document	1 KB
openvpn-status.log	8/6/2018 6:48 PM	Text Document	1 KB
server.ovpn	8/6/2018 2:02 PM	OpenVPN Config File	11 KB
server01.crt	7/31/2018 5:54 PM	Security Certificate	5 KB
server01.key	7/31/2018 5:54 PM	KEY File	2 KB

Figure 121 – OpenVPN configuration

After that, you must create a "ccd" folder, rename it ("client01" is the common name), rename it without suffix and configure it according to **Figure 122**:


This PC > Windows (C:) > Program Files > OpenVPN > config > ccd
Name
☑ client01
client01 - Notepad
File Edit Format View Help

```
iroute 192.168.5.0 255.255.255.0
```

Figure 122 – Client01 file

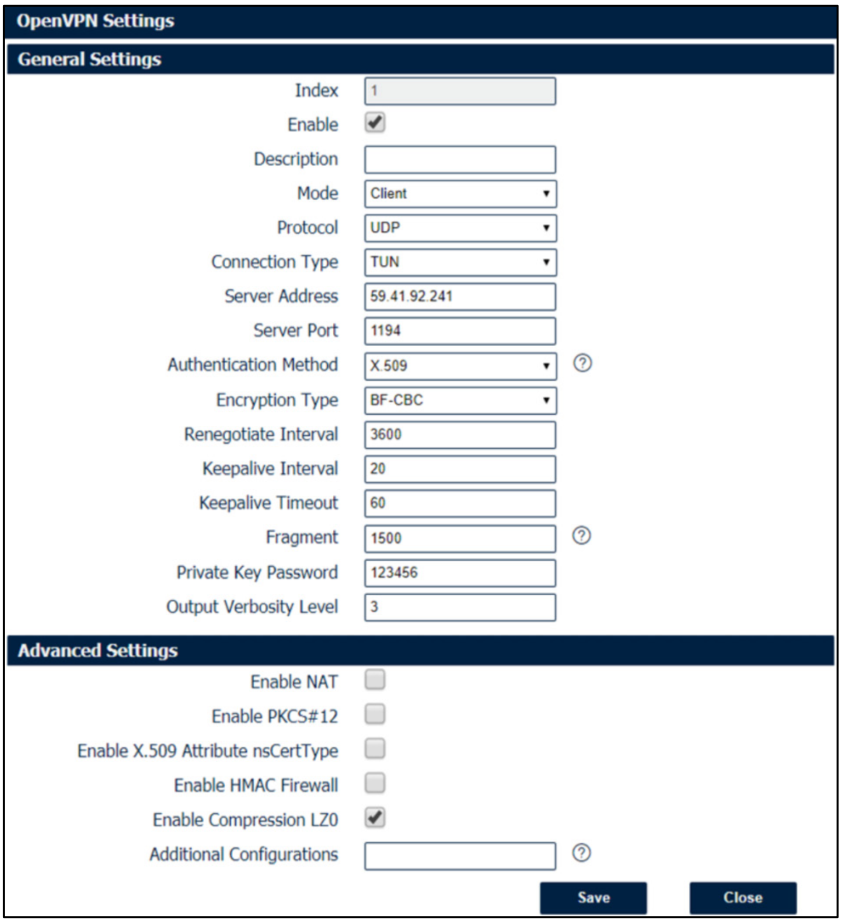
After that, just run the file **server.ovpn** and configure it as shown below:

```
local 59.41.92.241
mode server
port 1194
proto udp
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert server01.crt
key server01.key # This file should be kept secret
dh dh2048.pem
```

```
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.10.0 255.255.255.0"
client-config-dir ccd
route 192.168.5.0 255.255.255.0
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

6.4.2.2 CLIENT CONFIGURATION

To configure a computer as a client, you must open the Web Interface of **AirGate 4G** and go to **VPN > OpenVPN > OpenVPN > General Settings**. Click the edit button and configure OpenVPN as below:



OpenVPN Settings

General Settings

Index	1
Enable	☑
Description	
Mode	Client
Protocol	UDP
Connection Type	TUN
Server Address	59.41.92.241
Server Port	1194
Authentication Method	X.509
Encryption Type	BF-CBC
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500
Private Key Password	123456
Output Verbosity Level	3

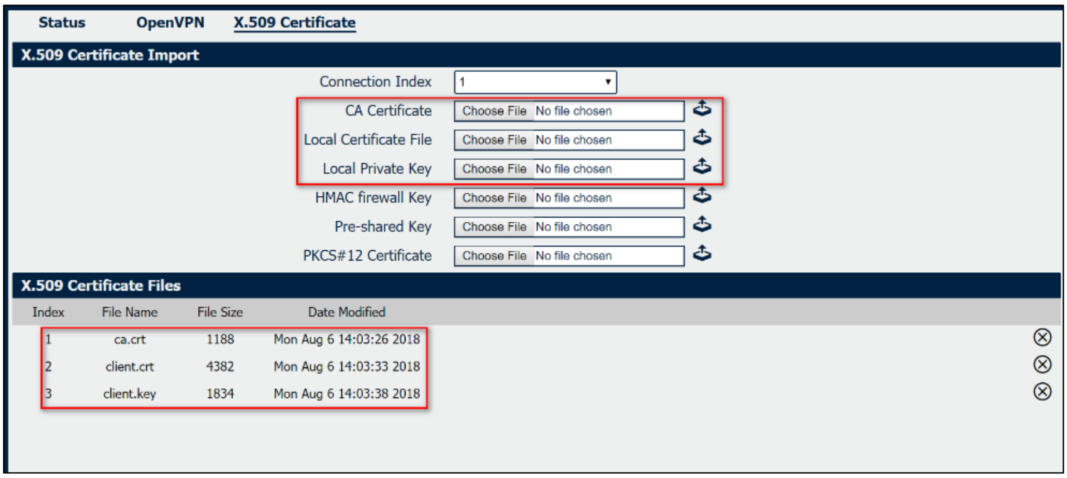
Advanced Settings

Enable NAT	☐
Enable PKCS#12	☐
Enable X.509 Attribute nsCertType	☐
Enable HMAC Firewall	☐
Enable Compression LZ0	☑
Additional Configurations	

Figure 123 – OpenVPN configuration

Click **Save > Apply**.

Once you have set up OpenVPN, go to **VPN > OpenVPN > X.509 Certificate** to import the related certification. Click **Apply**.



Status   OpenVPN   X.509 Certificate

X.509 Certificate Import

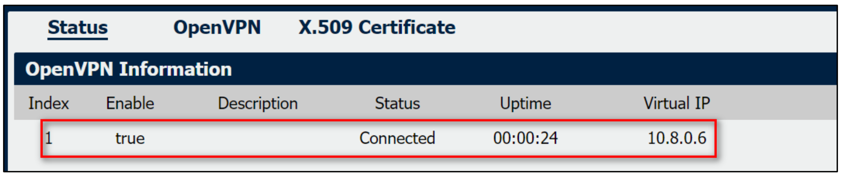
Connection Index	1
CA Certificate	Choose File No file chosen
Local Certificate File	Choose File No file chosen
Local Private Key	Choose File No file chosen
HMAC firewall Key	Choose File No file chosen
Pre-shared Key	Choose File No file chosen
PKCS#12 Certificate	Choose File No file chosen

X.509 Certificate Files

Index	File Name	File Size	Date Modified
1	ca.crt	1188	Mon Aug 6 14:03:26 2018
2	client.crt	4382	Mon Aug 6 14:03:33 2018
3	client.key	1834	Mon Aug 6 14:03:38 2018

Figure 124 – Certificate import

Route had connected to OpenVPN server. Go to **VPN > OpenVPN > Status** to check the connection status.



Status   OpenVPN   X.509 Certificate

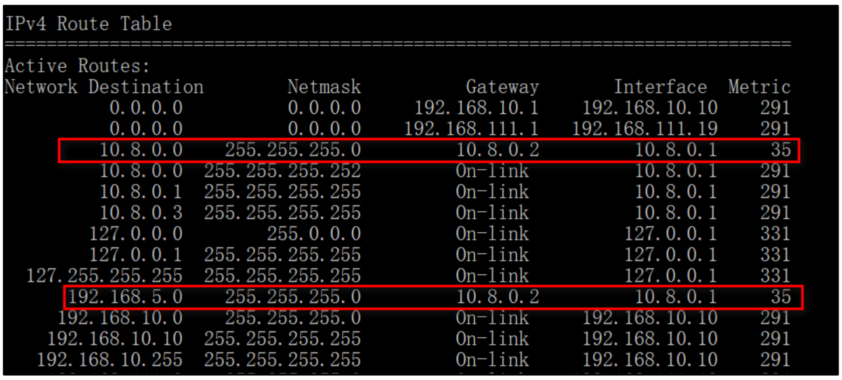
OpenVPN Information

Index	Enable	Description	Status	Uptime	Virtual IP
1	true		Connected	00:00:24	10.8.0.6

Figure 125 – OpenVPN connection status

6.4.3 ROUTE TABLE

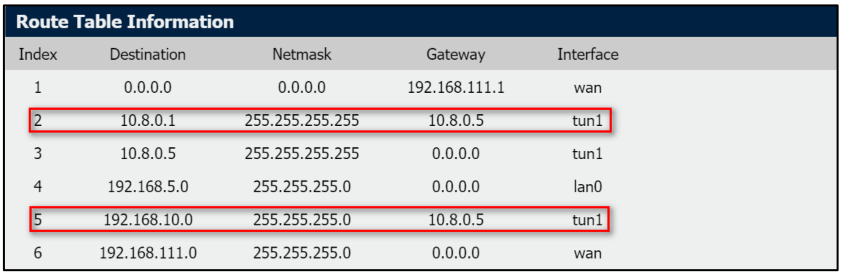
Figure 117 shows a route table of the OpenVPN server for reference:



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.10.1    192.168.10.10    291
          0.0.0.0          0.0.0.0    192.168.111.1   192.168.111.19    291
         10.8.0.0    255.255.255.0         10.8.0.2         10.8.0.1     35
         10.8.0.0  255.255.255.252          On-link         10.8.0.1    291
         10.8.0.1  255.255.255.255          On-link         10.8.0.1    291
         10.8.0.3  255.255.255.255          On-link         10.8.0.1    291
        127.0.0.0        255.0.0.0          On-link        127.0.0.1    331
        127.0.0.1  255.255.255.255          On-link        127.0.0.1    331
  127.255.255.255  255.255.255.255          On-link        127.0.0.1    331
      192.168.5.0    255.255.255.0         10.8.0.2         10.8.0.1     35
     192.168.10.0    255.255.255.0          On-link    192.168.10.10    291
    192.168.10.10  255.255.255.255          On-link    192.168.10.10    291
   192.168.10.255  255.255.255.255          On-link    192.168.10.10    291
```

Figure 126 – Route table of OpenVPN server

Figure 118 shows a route table of the OpenVPN client for reference:



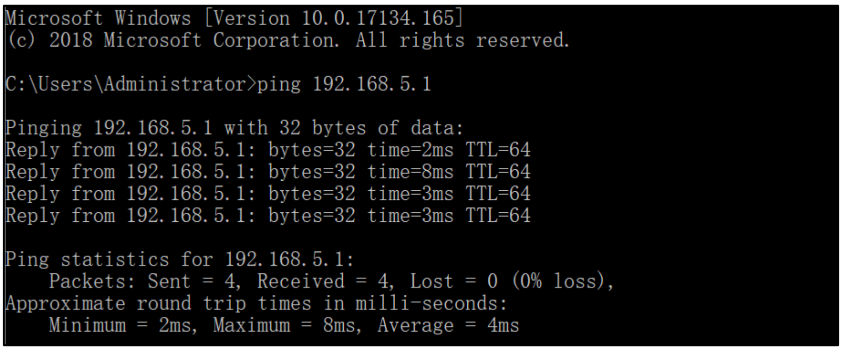
Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.1	255.255.255.255	10.8.0.5	tun1
3	10.8.0.5	255.255.255.255	0.0.0.0	tun1
4	192.168.5.0	255.255.255.0	0.0.0.0	lan0
5	192.168.10.0	255.255.255.0	10.8.0.5	tun1
6	192.168.111.0	255.255.255.0	0.0.0.0	wan

Figure 127 – Route table of OpenVPN client

6.4.4 TEST

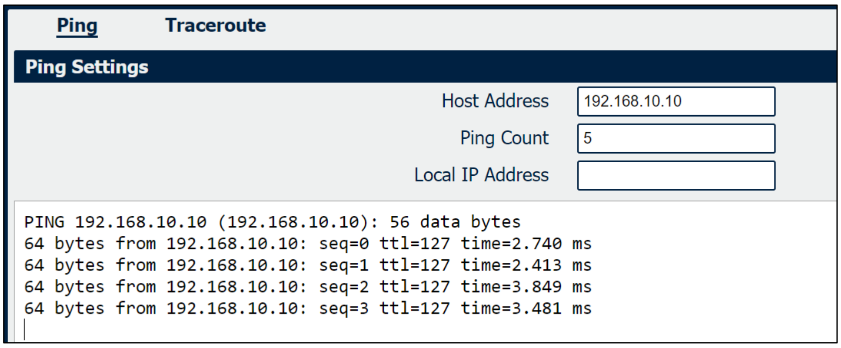
To perform a test, you must enable CMD and Ping from OpenVPN Server to LAN of OpenVPN client.



```
Microsoft Windows [Version 10.0.17134.165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.5.1

Pinging 192.168.5.1 with 32 bytes of data:
Reply from 192.168.5.1: bytes=32 time=2ms TTL=64
Reply from 192.168.5.1: bytes=32 time=8ms TTL=64
Reply from 192.168.5.1: bytes=32 time=3ms TTL=64
Reply from 192.168.5.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.5.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 8ms, Average = 4ms
```

Figure 128 – Prompt

After that, you must open the Web Interface of **AirGate 4G** and go to **Maintenance > Debug Tool > Ping** and Ping from OpenVPN client to OpenVPN Server.



Host Address: 192.168.10.10

Ping Count: 5

Local IP Address:

```
PING 192.168.10.10 (192.168.10.10): 56 data bytes
64 bytes from 192.168.10.10: seq=0 ttl=127 time=2.740 ms
64 bytes from 192.168.10.10: seq=1 ttl=127 time=2.413 ms
64 bytes from 192.168.10.10: seq=2 ttl=127 time=3.849 ms
64 bytes from 192.168.10.10: seq=3 ttl=127 time=3.481 ms
```

Figure 129 – Ping

Test successfully.

6.5 OpenVPN CLIENT WITH PRE-SHARED KEY

This tutorial shows how to configure OpenVPN with a pre-shared key.

6.5.1 TOPOLOGY

You can use the following topology:

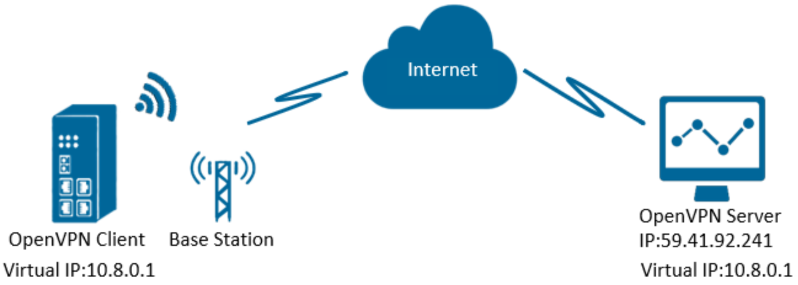


Figure 130 – OpenVPN with pre-shared key

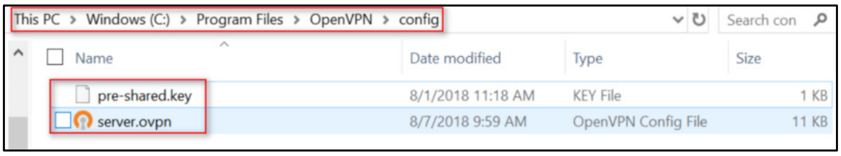
1. **AirGate 4G** runs as OpenVPN Client with any kind of IP, which can ping OpenVPN server IP successfully.
2. A PC runs as OpenVPN Server with a static public IP and open a specified a listening port for OpenVPN.
3. OpenVPN tunnel is established between Server and Client, the virtual IP can PING each other successfully. This is a point to point application.

6.5.2 CONFIGURATION

6.5.2.1 SERVER CONFIGURATION

To configure a computer as a server, you must download the OpenVPN software, available at https://openvpn.net/, and run and install it with administrator authority.

Once the software has been installed, you should copy the related certificates and the specific configuration to your computer, as shown in the figure below:


This PC > Windows (C:) > Program Files > OpenVPN > config

Name	Date modified	Type	Size
pre-shared.key	8/1/2018 11:18 AM	KEY File	1 KB
server.ovpn	8/7/2018 9:59 AM	OpenVPN Config File	11 KB

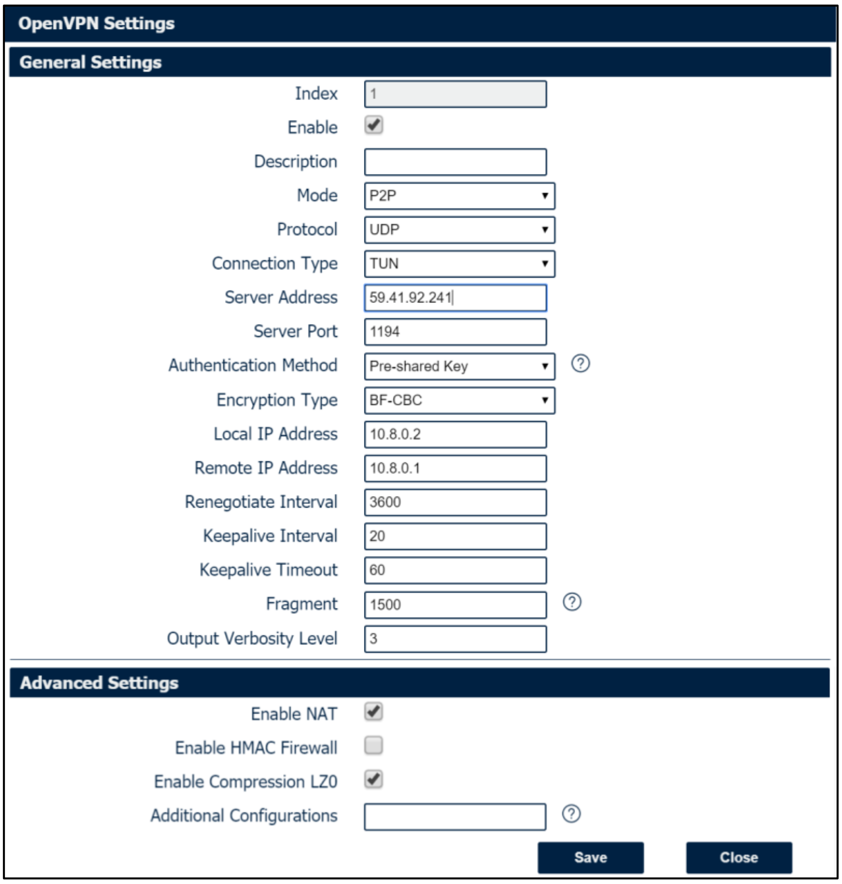
Figure 131 – OpenVPN folder

After that, just run the file **server.ovpn** and configure it as shown below:

```
local 59.41.92.241
proto udp
dev tun
tun-mtu 1500
fragment 1500
ifconfig 10.8.0.1 10.8.0.2
keepalive 10 120
secret pre-shared.key
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

6.5.2.2 CLIENT CONFIGURATION

To configure a PC as a client, you must open the Web Interface of **AirGate 4G** and go to **VPN > OpenVPN > OpenVPN > General Settings**. Click the edit button and configure OpenVPN as below:



OpenVPN Settings

General Settings

Index	1
Enable	☑
Description	
Mode	P2P
Protocol	UDP
Connection Type	TUN
Server Address	59.41.92.241
Server Port	1194
Authentication Method	Pre-shared Key
Encryption Type	BF-CBC
Local IP Address	10.8.0.2
Remote IP Address	10.8.0.1
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500
Output Verbosity Level	3

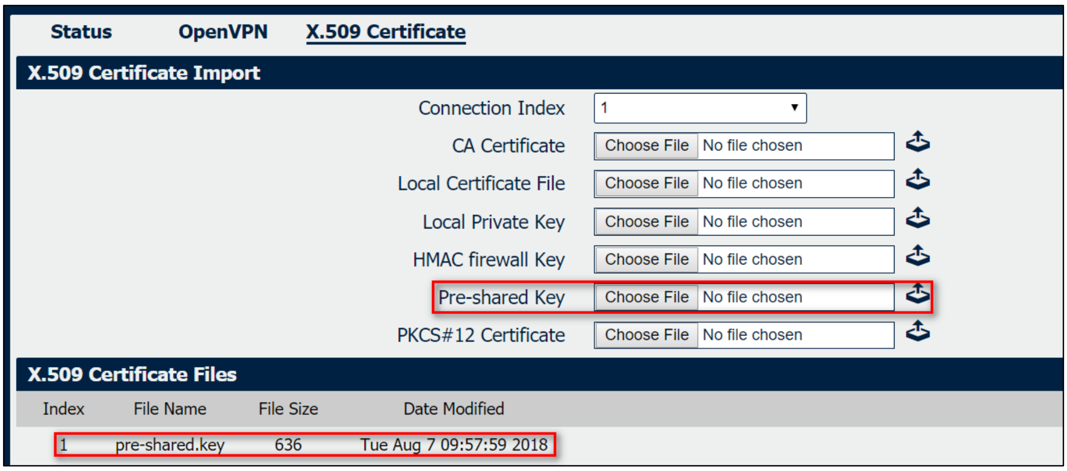
Advanced Settings

Enable NAT	☑
Enable HMAC Firewall	☐
Enable Compression LZO	☑
Additional Configurations	

Figure 132 – OpenVPN settings

Click **Save > Apply**.

After that, go to **VPN > OpenVPN > X.509 Certificate** to import the related certification. Click **Apply**.



X.509 Certificate Import

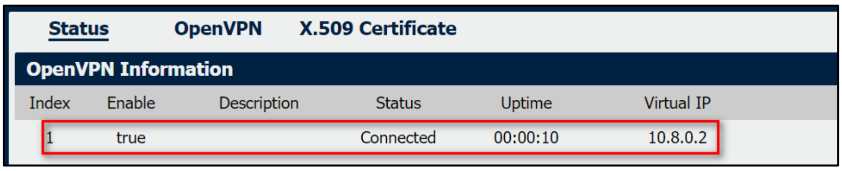
Connection Index	1
CA Certificate	Choose File No file chosen
Local Certificate File	Choose File No file chosen
Local Private Key	Choose File No file chosen
HMAC firewall Key	Choose File No file chosen
Pre-shared Key	Choose File No file chosen
PKCS#12 Certificate	Choose File No file chosen

X.509 Certificate Files

Index	File Name	File Size	Date Modified
1	pre-shared.key	636	Tue Aug 7 09:57:59 2018

Figure 133 – Pre-shared key

Route had connected to OpenVPN server. Go to **VPN > OpenVPN > Status** to check the connection status.



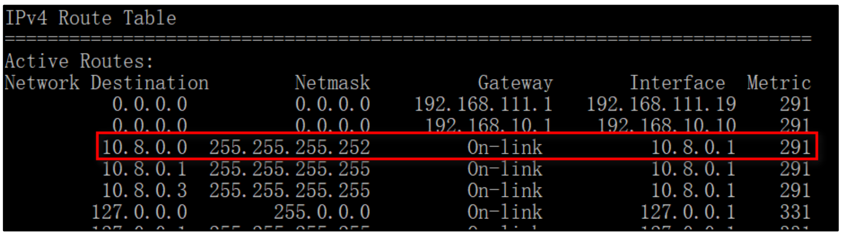
OpenVPN Information

Index	Enable	Description	Status	Uptime	Virtual IP
1	true		Connected	00:00:10	10.8.0.2

Figure 134 – OpenVPN status connection

6.5.3 ROUTE TABLE

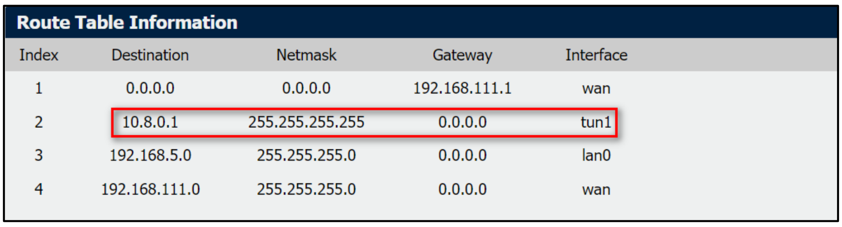
Figure 135 shows a route table of the OpenVPN server for reference:



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.111.1   192.168.111.19    291
          0.0.0.0          0.0.0.0     192.168.10.1    192.168.10.10    291
         10.8.0.0  255.255.255.252         On-link          10.8.0.1    291
         10.8.0.1  255.255.255.255         On-link          10.8.0.1    291
         10.8.0.3  255.255.255.255         On-link          10.8.0.1    291
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
```

Figure 135 – Server route table information

Figure 136 shows a route table of the OpenVPN client for reference:



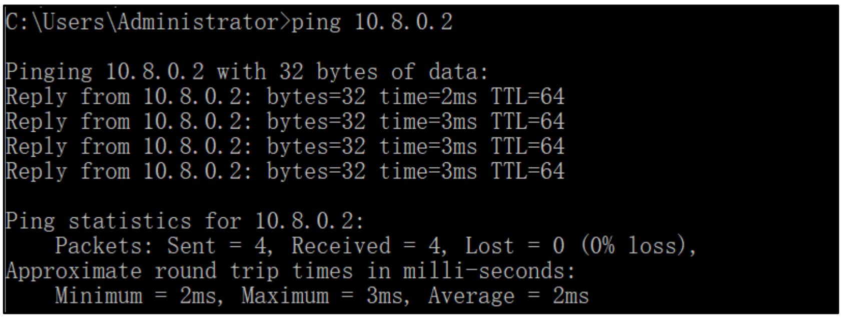
Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.1	255.255.255.255	0.0.0.0	tun1
3	192.168.5.0	255.255.255.0	0.0.0.0	lan0
4	192.168.111.0	255.255.255.0	0.0.0.0	wan

Figure 136 – Client route table information

6.5.4 TEST

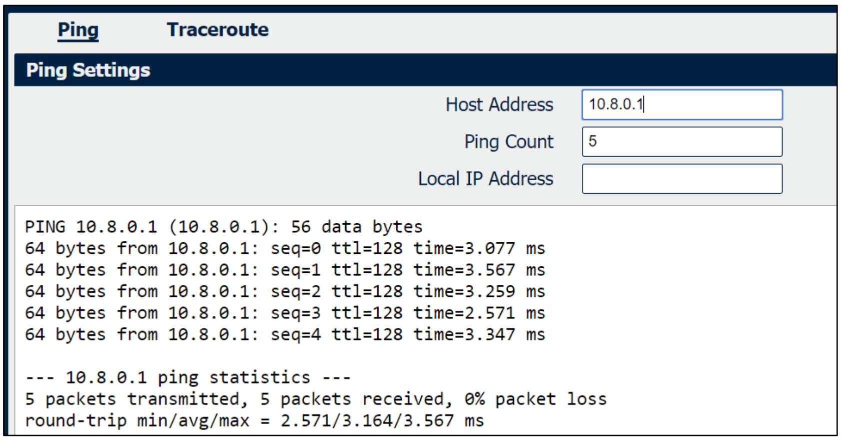
To perform a test, you must enable CMD and Ping from OpenVPN Server to LAN of OpenVPN client.



```
C:\Users\Administrator>ping 10.8.0.2

Pinging 10.8.0.2 with 32 bytes of data:
Reply from 10.8.0.2: bytes=32 time=2ms TTL=64
Reply from 10.8.0.2: bytes=32 time=3ms TTL=64
Reply from 10.8.0.2: bytes=32 time=3ms TTL=64
Reply from 10.8.0.2: bytes=32 time=3ms TTL=64

Ping statistics for 10.8.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Figure 137 – CMD

After that, you must open the Web Interface of **AirGate 4G** and go to **Maintenance > Debug Tool > Ping** and Ping from OpenVPN client to OpenVPN Server.



Ping Settings

Host Address: 10.8.0.1

Ping Count: 5

Local IP Address:

```
PING 10.8.0.1 (10.8.0.1): 56 data bytes
64 bytes from 10.8.0.1: seq=0 ttl=128 time=3.077 ms
64 bytes from 10.8.0.1: seq=1 ttl=128 time=3.567 ms
64 bytes from 10.8.0.1: seq=2 ttl=128 time=3.259 ms
64 bytes from 10.8.0.1: seq=3 ttl=128 time=2.571 ms
64 bytes from 10.8.0.1: seq=4 ttl=128 time=3.347 ms

--- 10.8.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.571/3.164/3.567 ms
```

Figure 138 – Ping

Test successfully.

6.6 OpenVPN CLIENT WITH USERNAME & PASSWORD

This tutorial shows how to configure OpenVPN with a username and password.

6.6.1 TOPOLOGY

You can use the following topology:

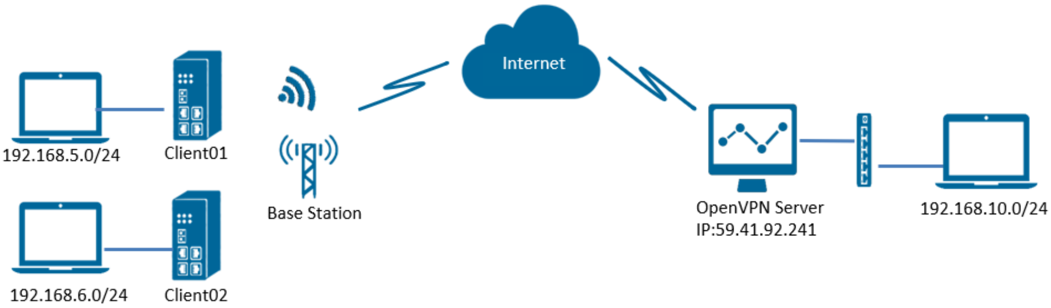


Figure 139 – OpenVPN with username and password

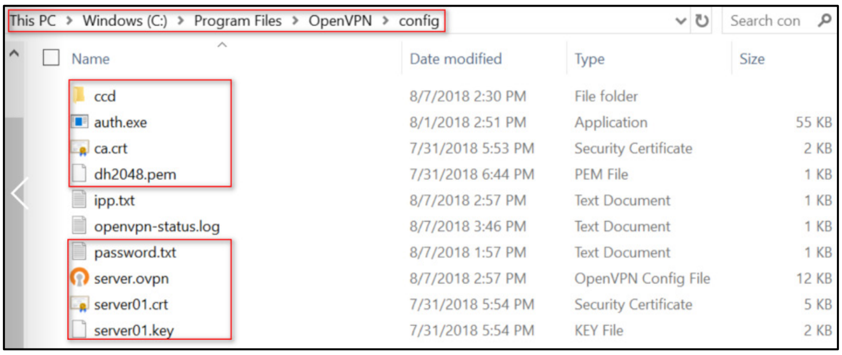
1. Two **AirGate 4G** run as OpenVPN Client01 and Client02 with any kind of IP, which can ping OpenVPN server IP successfully.
2. A PC runs as OpenVPN Server with a static public IP and open a specified a listening port for OpenVPN.
3. OpenVPN tunnel is established between Server and Client. Client01 can ping Client02 successfully and vice versa.

6.6.2 CONFIGURATION

6.6.2.1 SERVER CONFIGURATION

To configure a computer as a server, you must download the OpenVPN software, available at https://openvpn.net/, and run and install it with administrator authority.

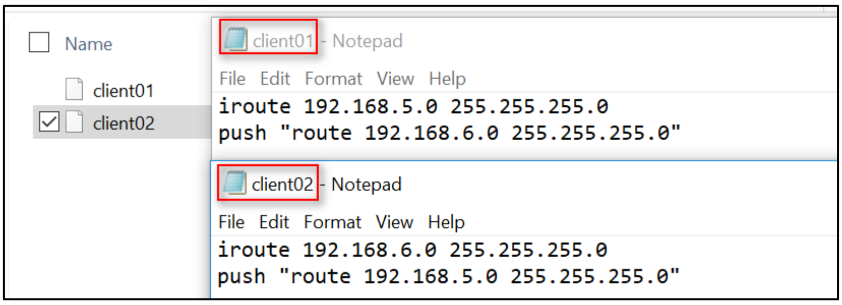
Once the software has been installed, you should copy the related certificates and the specific configuration to your computer, as shown in the figure below:


This PC > Windows (C:) > Program Files > OpenVPN > config

Name	Date modified	Type	Size
ccd	8/7/2018 2:30 PM	File folder	
auth.exe	8/1/2018 2:51 PM	Application	55 KB
ca.crt	7/31/2018 5:53 PM	Security Certificate	2 KB
dh2048.pem	7/31/2018 6:44 PM	PEM File	1 KB
ipp.txt	8/7/2018 2:57 PM	Text Document	1 KB
openvpn-status.log	8/7/2018 3:46 PM	Text Document	1 KB
password.txt	8/7/2018 1:57 PM	Text Document	1 KB
server.ovpn	8/7/2018 2:57 PM	OpenVPN Config File	12 KB
server01.crt	7/31/2018 5:54 PM	Security Certificate	5 KB
server01.key	7/31/2018 5:54 PM	KEY File	2 KB

Figure 140 – OpenVPN folders

After that, two new notepads must be created inside the "ccd" folder, renamed it without suffix (using the default names "client01" and "client02") and configured according to **Figure 141**:


□ Name

client01

☑ client02

client01 - Notepad

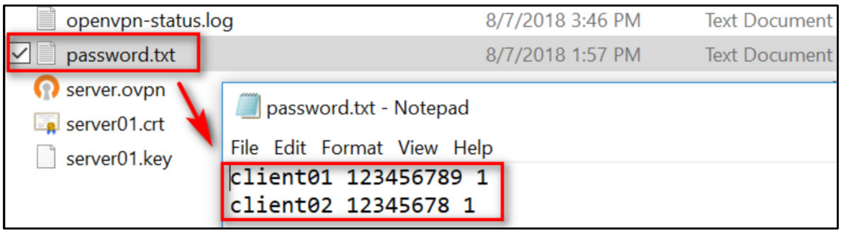
```
iroute 192.168.5.0 255.255.255.0
push "route 192.168.6.0 255.255.255.0"
```

client02 - Notepad

```
iroute 192.168.6.0 255.255.255.0
push "route 192.168.5.0 255.255.255.0"
```

Figure 141 – Client01 and client02 configuration files

It will also be necessary to create a "password.txt" file, which will include the contents of **Figure 142**, presented as follows: **common name > password > 1 or 0 (1 = enable / 0 = disable)**.


openvpn-status.log 8/7/2018 3:46 PM Text Document
password.txt 8/7/2018 1:57 PM Text Document
server.ovpn
server01.crt
server01.key
password.txt - Notepad
File Edit Format View Help

```
client01 123456789 1
client02 12345678 1
```

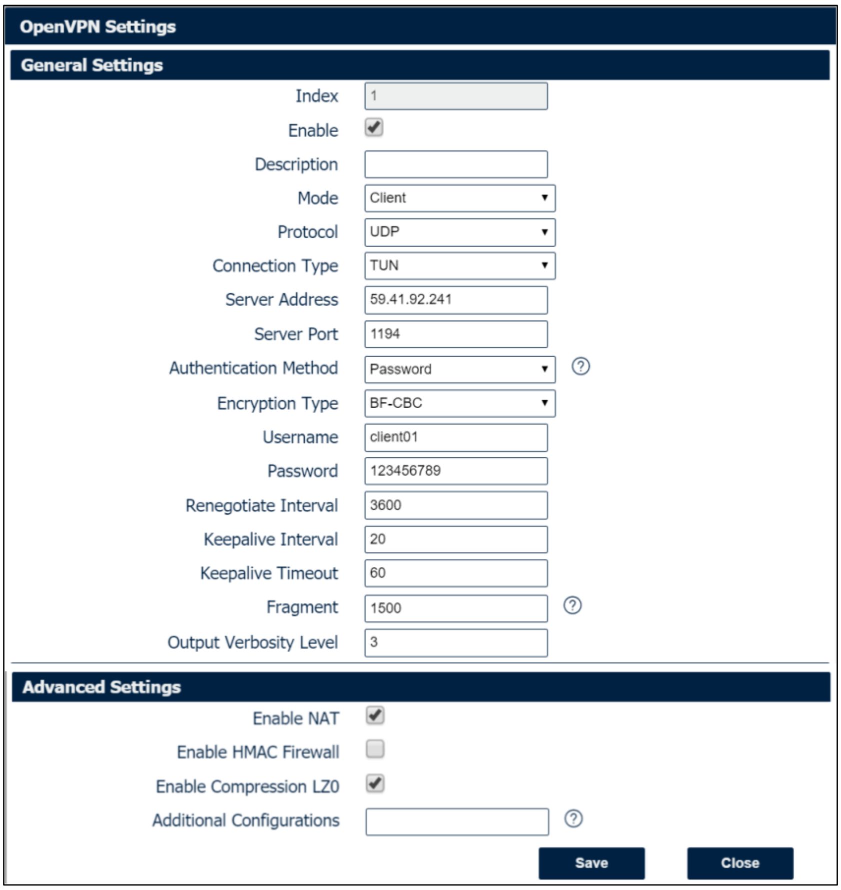
Figure 142 – Password configuration

After that, just run the file **server.ovpn** and configure it as shown below:

```
local 59.41.92.241
mode server
port 1194
proto udp
client-cert-not-required
username-as-common-name
auth-user-pass-verify auth.exe via-env
script-security 3 system
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert server01.crt
key server01.key # This file should be kept secret
dh dh2048.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.10.0 255.255.255.0"
client-config-dir ccd
route 192.168.5.0 255.255.255.0
route 192.168.6.0 255.255.255.0
client-to-client
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

6.6.2.2 CLIENT01 CONFIGURATION

To configure a computer as a client, you must open the Web Interface of **AirGate 4G** and go to **VPN** > **OpenVPN** > **OpenVPN** > **General Settings**. Click the edit button and configure OpenVPN as below:



OpenVPN Settings

General Settings

Index: 1
Enable: ☑
Description:
Mode: Client
Protocol: UDP
Connection Type: TUN
Server Address: 59.41.92.241
Server Port: 1194
Authentication Method: Password
Encryption Type: BF-CBC
Username: client01
Password: 123456789
Renegotiate Interval: 3600
Keepalive Interval: 20
Keepalive Timeout: 60
Fragment: 1500
Output Verbosity Level: 3

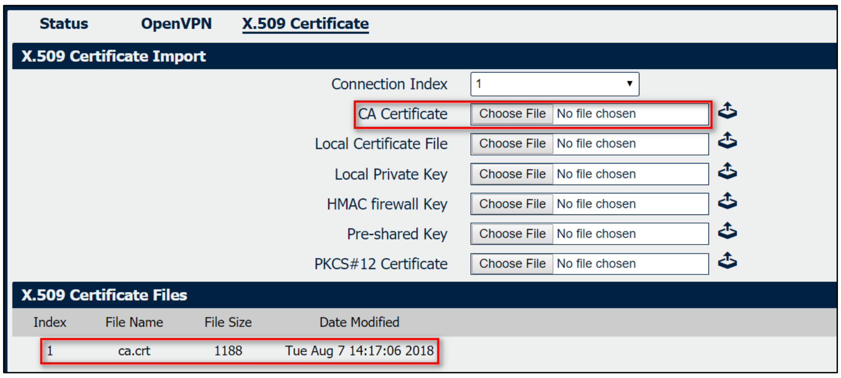
Advanced Settings

Enable NAT: ☑
Enable HMAC Firewall: ☐
Enable Compression LZ0: ☑
Additional Configurations:

Figure 143 – OpenVPN configuration

Click **Save > Apply**.

After that, go to **VPN** > **OpenVPN** > **X.509 Certificate** to import the related certification. Click **Apply**.



X.509 Certificate Import

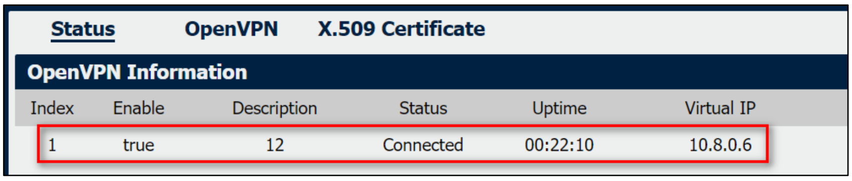
Connection Index: 1
CA Certificate: Choose File No file chosen
Local Certificate File: Choose File No file chosen
Local Private Key: Choose File No file chosen
HMAC firewall Key: Choose File No file chosen
Pre-shared Key: Choose File No file chosen
PKCS#12 Certificate: Choose File No file chosen

X.509 Certificate Files

Index	File Name	File Size	Date Modified
1	ca.crt	1188	Tue Aug 7 14:17:06 2018

Figure 144 – CA certificate import

Route had connected to OpenVPN server. Go to **VPN** > **OpenVPN** > **Status** to check the connection status.



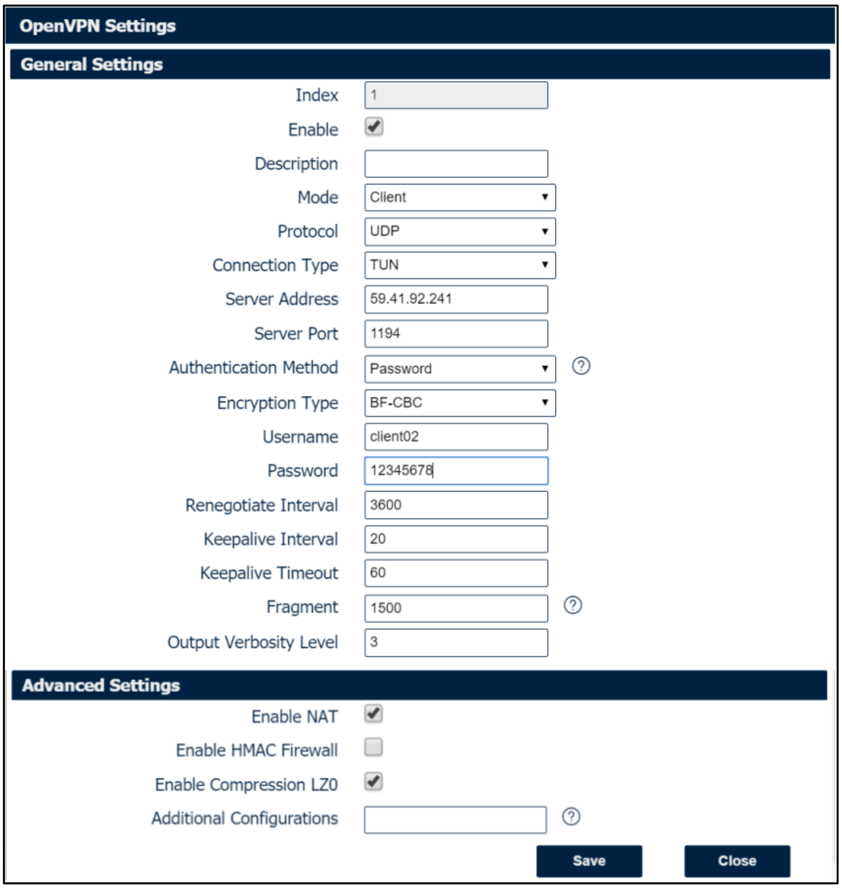
OpenVPN Information

Index	Enable	Description	Status	Uptime	Virtual IP
1	true	12	Connected	00:22:10	10.8.0.6

Figure 145 – OpenVPN status connection

6.6.2.3 CLIENT02 CONFIGURATION

To configure a computer as a client, you must open the Web Interface of **AirGate 4G** and go to **VPN > OpenVPN > OpenVPN > General Settings**. Click the edit button and configure OpenVPN as below:



OpenVPN Settings

General Settings

Index	1
Enable	☑
Description	
Mode	Client
Protocol	UDP
Connection Type	TUN
Server Address	59.41.92.241
Server Port	1194
Authentication Method	Password
Encryption Type	BF-CBC
Username	client02
Password	12345678
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500
Output Verbosity Level	3

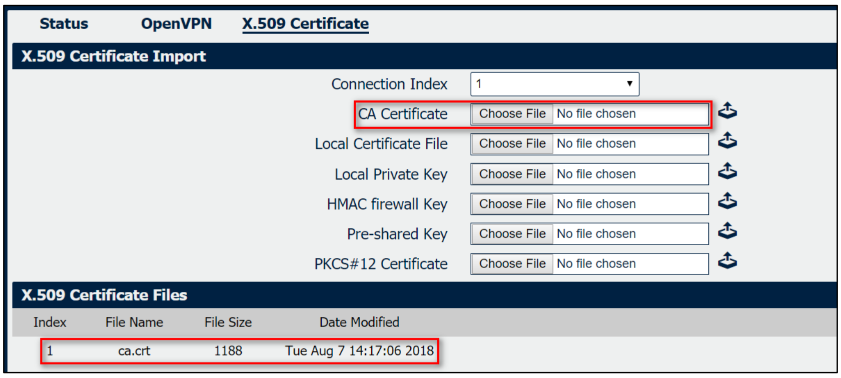
Advanced Settings

Enable NAT	☑
Enable HMAC Firewall	□
Enable Compression LZ0	☑
Additional Configurations	

Figure 146 – OpenVPN configuration

Click **Save > Apply**.

After that, go to **VPN > OpenVPN > X.509 Certificate** to import the related certification. Click **Apply**.



X.509 Certificate Import

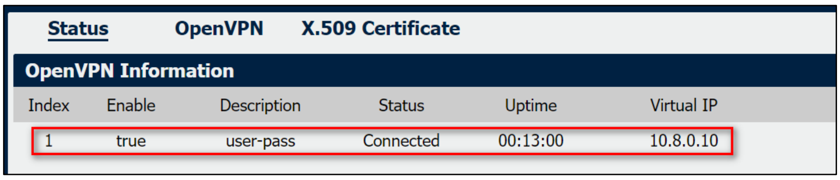
Connection Index	1
CA Certificate	Choose File No file chosen
Local Certificate File	Choose File No file chosen
Local Private Key	Choose File No file chosen
HMAC firewall Key	Choose File No file chosen
Pre-shared Key	Choose File No file chosen
PKCS#12 Certificate	Choose File No file chosen

X.509 Certificate Files

Index	File Name	File Size	Date Modified
1	ca.crt	1188	Tue Aug 7 14:17:06 2018

Figure 147 – X.509 certificate: CA certificate

Route had connected to OpenVPN server. Go to **VPN > OpenVPN > Status** to check the connection status.



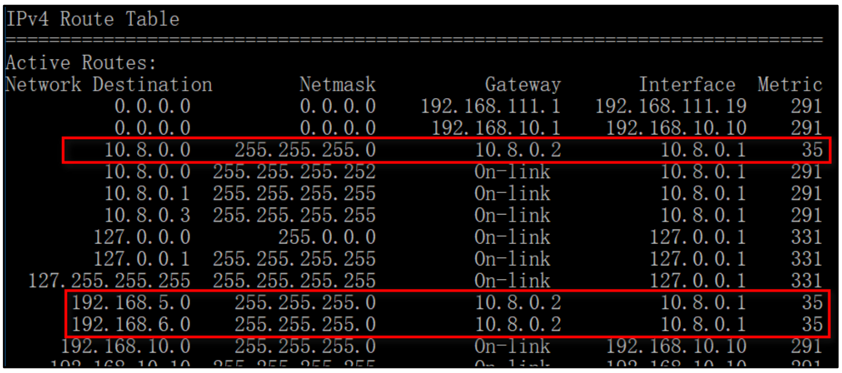
OpenVPN Information

Index	Enable	Description	Status	Uptime	Virtual IP
1	true	user-pass	Connected	00:13:00	10.8.0.10

Figure 148 – OpenVPN connection status

6.6.3 ROUTE TABLE

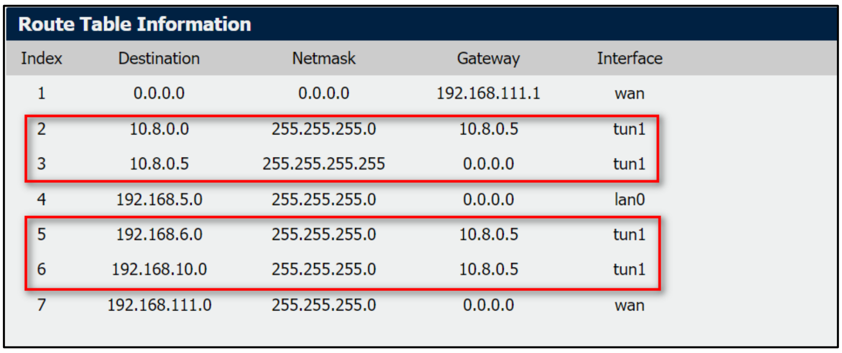
Figure 149 shows a route table of the OpenVPN server for reference:



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0. 0. 0. 0          0. 0. 0. 0   192. 168. 111. 1  192. 168. 111. 19    291
          0. 0. 0. 0          0. 0. 0. 0    192. 168. 10. 1   192. 168. 10. 10    291
         10. 8. 0. 0    255. 255. 255. 0        10. 8. 0. 2        10. 8. 0. 1     35
         10. 8. 0. 0  255. 255. 255. 252          On-link        10. 8. 0. 1    291
         10. 8. 0. 1  255. 255. 255. 255          On-link        10. 8. 0. 1    291
         10. 8. 0. 3  255. 255. 255. 255          On-link        10. 8. 0. 1    291
        127. 0. 0. 0        255. 0. 0. 0          On-link       127. 0. 0. 1    331
        127. 0. 0. 1  255. 255. 255. 255          On-link       127. 0. 0. 1    331
  127. 255. 255. 255  255. 255. 255. 255          On-link       127. 0. 0. 1    331
      192. 168. 5. 0    255. 255. 255. 0        10. 8. 0. 2        10. 8. 0. 1     35
      192. 168. 6. 0    255. 255. 255. 0        10. 8. 0. 2        10. 8. 0. 1     35
     192. 168. 10. 0    255. 255. 255. 0          On-link     192. 168. 10. 10    291
    192. 168. 10. 10  255. 255. 255. 255          On-link     192. 168. 10. 10    291
```

Figure 149 – OpenVPN server route table

Figure 150 shows a route table of the Client01 for reference:

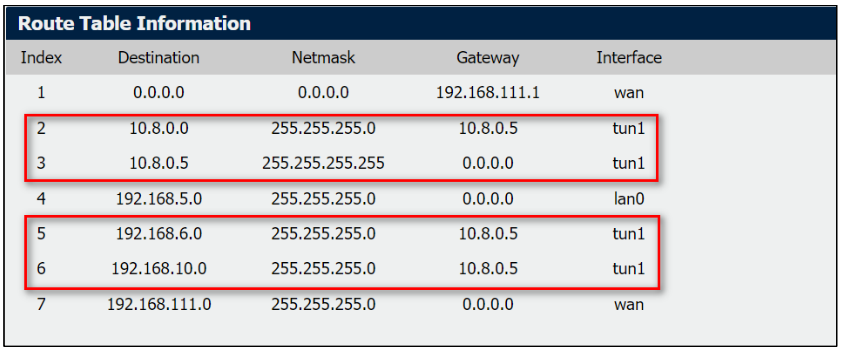


Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.0	255.255.255.0	10.8.0.5	tun1
3	10.8.0.5	255.255.255.255	0.0.0.0	tun1
4	192.168.5.0	255.255.255.0	0.0.0.0	lan0
5	192.168.6.0	255.255.255.0	10.8.0.5	tun1
6	192.168.10.0	255.255.255.0	10.8.0.5	tun1
7	192.168.111.0	255.255.255.0	0.0.0.0	wan

Figure 150 – Client01 route table

Figure 151 shows a route table of the Client02 for reference:



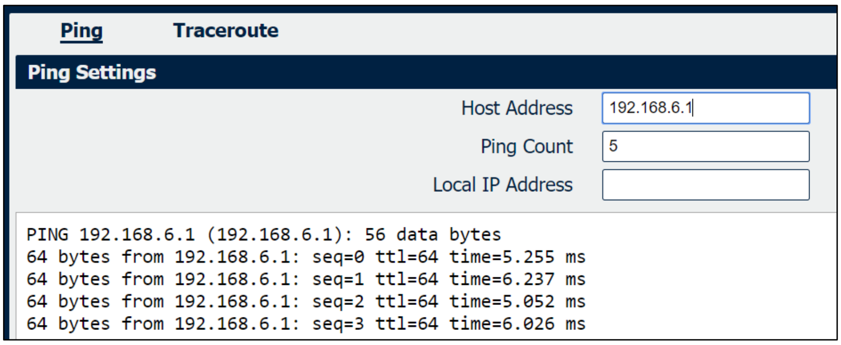
Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.0	255.255.255.0	10.8.0.5	tun1
3	10.8.0.5	255.255.255.255	0.0.0.0	tun1
4	192.168.5.0	255.255.255.0	0.0.0.0	lan0
5	192.168.6.0	255.255.255.0	10.8.0.5	tun1
6	192.168.10.0	255.255.255.0	10.8.0.5	tun1
7	192.168.111.0	255.255.255.0	0.0.0.0	wan

Figure 151 – Client02 route table

6.6.4 TEST

You must open the Web Interface of **AirGate 4G** and go to **Maintenance > Debug Tool > Ping** and ping from Client01 to Cliente02:



Ping Settings

Host Address: 192.168.6.1

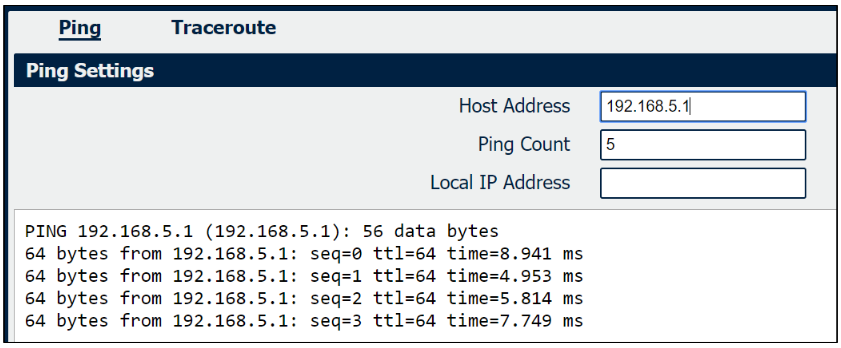
Ping Count: 5

Local IP Address:

```
PING 192.168.6.1 (192.168.6.1): 56 data bytes
64 bytes from 192.168.6.1: seq=0 ttl=64 time=5.255 ms
64 bytes from 192.168.6.1: seq=1 ttl=64 time=6.237 ms
64 bytes from 192.168.6.1: seq=2 ttl=64 time=5.052 ms
64 bytes from 192.168.6.1: seq=3 ttl=64 time=6.026 ms
```

Figure 152 – Ping from Client01 to Client02

After that, Ping from Client02 to Cliente01 as below:



Host Address: 192.168.5.1

Ping Count: 5

Local IP Address:

```
PING 192.168.5.1 (192.168.5.1): 56 data bytes
64 bytes from 192.168.5.1: seq=0 ttl=64 time=8.941 ms
64 bytes from 192.168.5.1: seq=1 ttl=64 time=4.953 ms
64 bytes from 192.168.5.1: seq=2 ttl=64 time=5.814 ms
64 bytes from 192.168.5.1: seq=3 ttl=64 time=7.749 ms
```

Figure 153 – Ping from Client02 to Client01

Test successfully.

6.7 OpenVPN WITH TAP AND PRE-SHARED KEY UNDER P2P MODE

This tutorial shows how to configure OpenVPN with TAP and pre-shared key under P2P mode.

6.7.1 TOPOLOGY

You can use the following topology:

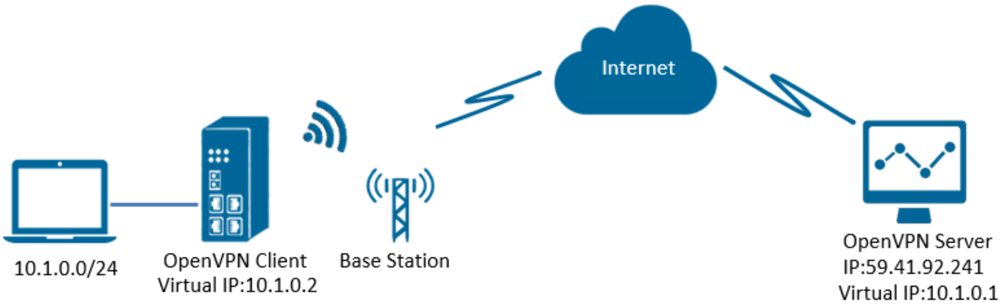


Figure 154 – OpenVPN with TAP and pre-shared key

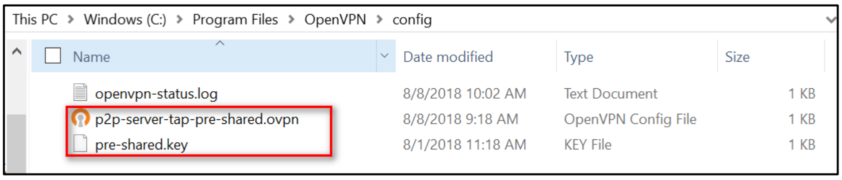
1. **AirGate 4G** runs as OpenVPN Client with any kind of IP, which can ping OpenVPN server IP successfully.
2. A PC runs as OpenVPN Server with a static public IP and open a specified a listening port for OpenVPN.
3. OpenVPN tunnel is established between Server and Client, the virtual IP can PING each other successfully. Also server can Ping LAN PC device and vice versa.

6.7.2 CONFIGURATION

6.7.2.1 SERVER CONFIGURATION

To configure a computer as a server, you must download the OpenVPN software, available at https://openvpn.net/, and run and install it with administrator authority.

Once the software has been installed, you should copy the related certificates and the specific configuration to your computer, as shown in the figure below:



This PC > Windows (C:) > Program Files > OpenVPN > config

Name	Date modified	Type	Size
openvpn-status.log	8/8/2018 10:02 AM	Text Document	1 KB
p2p-server-tap-pre-shared.ovpn	8/8/2018 9:18 AM	OpenVPN Config File	1 KB
pre-shared.key	8/1/2018 11:18 AM	KEY File	1 KB

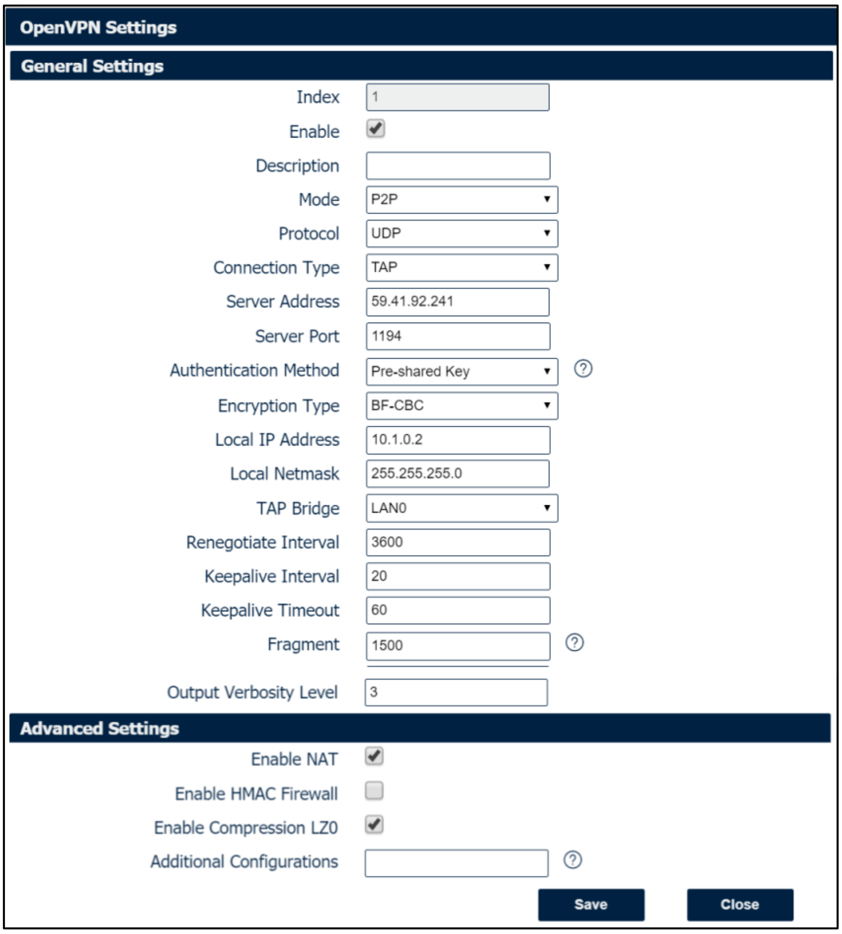
Figure 155 – OpenVPN folder

After that, just run the file **p2p-server-tap-pre-shared.ovpn** and configure it as shown below:

```
mode p2p
port 1194
proto udp
dev tap
# tap
ifconfig 10.1.0.1 255.255.255.0
keepalive 20 120
persist-key
persist-tun
secret pre-shared.key  # None TLS Mode
cipher BF-CBC
comp-lzo
status openvpn-status.log
verb 3
tun-mtu 1500
fragment 1500
```

6.7.2.2 CLIENT CONFIGURATION

To configure a computer as a client, you must open the Web Interface of **AirGate 4G** and go to **VPN > OpenVPN > OpenVPN > General Settings**. Click the edit button and configure OpenVPN as below:



OpenVPN Settings

General Settings

Index	1
Enable	☑
Description	
Mode	P2P
Protocol	UDP
Connection Type	TAP
Server Address	59.41.92.241
Server Port	1194
Authentication Method	Pre-shared Key
Encryption Type	BF-CBC
Local IP Address	10.1.0.2
Local Netmask	255.255.255.0
TAP Bridge	LAN0
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500
Output Verbosity Level	3

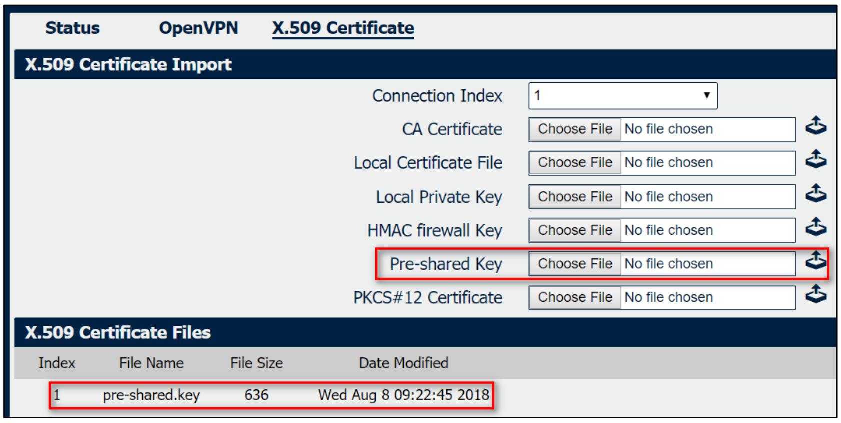
Advanced Settings

Enable NAT	☑
Enable HMAC Firewall	□
Enable Compression LZ0	☑
Additional Configurations	

Figure 156 – OpenVPN settings

Click **Save > Apply**.

After that, go to **VPN > OpenVPN > X.509 Certificate** to import the related certification. Click **Apply**.



X.509 Certificate Import

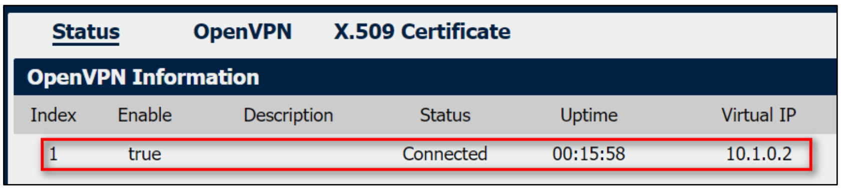
Connection Index	1
CA Certificate	Choose File No file chosen
Local Certificate File	Choose File No file chosen
Local Private Key	Choose File No file chosen
HMAC firewall Key	Choose File No file chosen
Pre-shared Key	Choose File No file chosen
PKCS#12 Certificate	Choose File No file chosen

X.509 Certificate Files

Index	File Name	File Size	Date Modified
1	pre-shared.key	636	Wed Aug 8 09:22:45 2018

Figure 157 – Pre-shared key

Route had connected to OpenVPN server. Go to **VPN > OpenVPN > Status** to check the connection status.



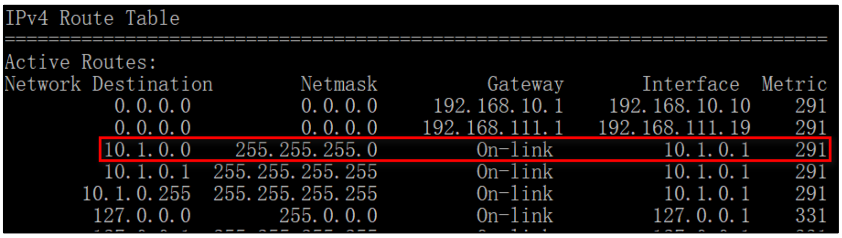
OpenVPN Information

Index	Enable	Description	Status	Uptime	Virtual IP
1	true		Connected	00:15:58	10.1.0.2

Figure 158 – OpenVPN connection status

6.7.3 ROUTE TABLE

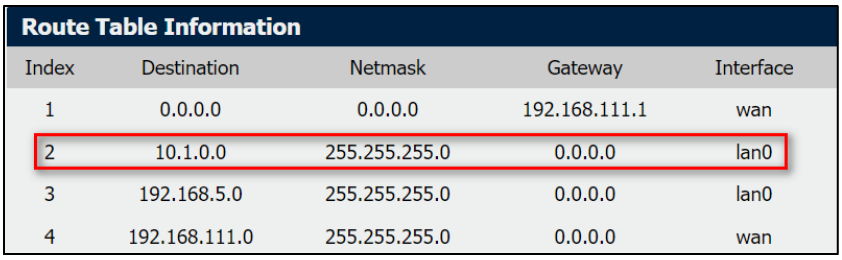
Figure 159 shows a route table of the OpenVPN server for reference:



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.10.1    192.168.10.10    291
          0.0.0.0          0.0.0.0    192.168.111.1   192.168.111.19    291
         10.1.0.0    255.255.255.0         On-link          10.1.0.1    291
         10.1.0.1  255.255.255.255         On-link          10.1.0.1    291
       10.1.0.255  255.255.255.255         On-link          10.1.0.1    291
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
```

Figure 159 – OpenVPN server route table

Figure 160 shows a route table of the client for reference:



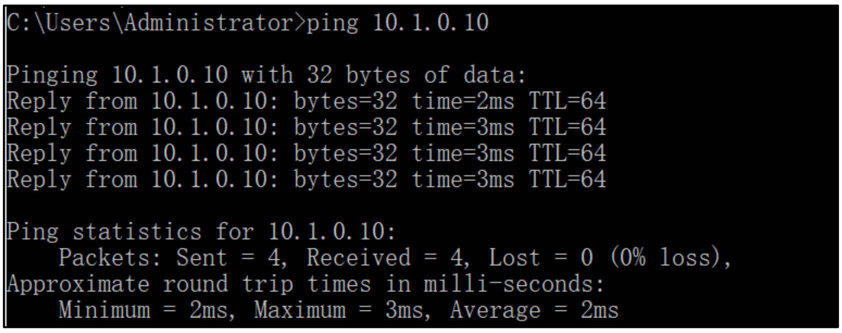
Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.1.0.0	255.255.255.0	0.0.0.0	lan0
3	192.168.5.0	255.255.255.0	0.0.0.0	lan0
4	192.168.111.0	255.255.255.0	0.0.0.0	wan

Figure 160 – Client route table

6.7.4 TEST

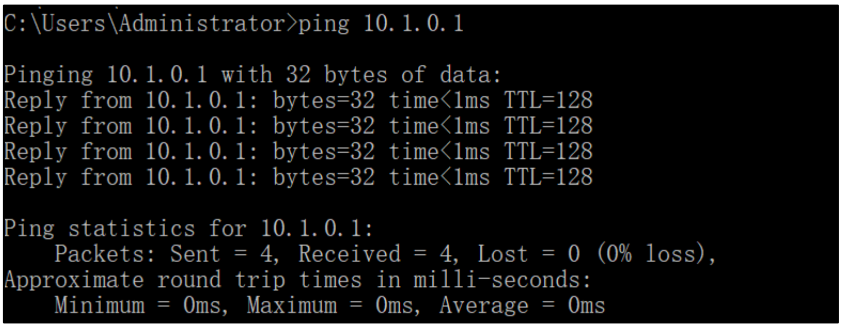
Enable CMD and Ping from PC to the LAN device of the router.



```
C:\Users\Administrator>ping 10.1.0.10

Pinging 10.1.0.10 with 32 bytes of data:
Reply from 10.1.0.10: bytes=32 time=2ms TTL=64
Reply from 10.1.0.10: bytes=32 time=3ms TTL=64
Reply from 10.1.0.10: bytes=32 time=3ms TTL=64
Reply from 10.1.0.10: bytes=32 time=3ms TTL=64

Ping statistics for 10.1.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Figure 161 – CMD

After that, Ping from LAN device of the router to PC.



```
C:\Users\Administrator>ping 10.1.0.1

Pinging 10.1.0.1 with 32 bytes of data:
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 162 – Ping

Test successfully.

6.8 OpenVPN WITH TAP UNDER P2P MODE

This tutorial shows how to configure OpenVPN with TAP and under P2P mode.

6.8.1 TOPOLOGY

You can use the following topology:

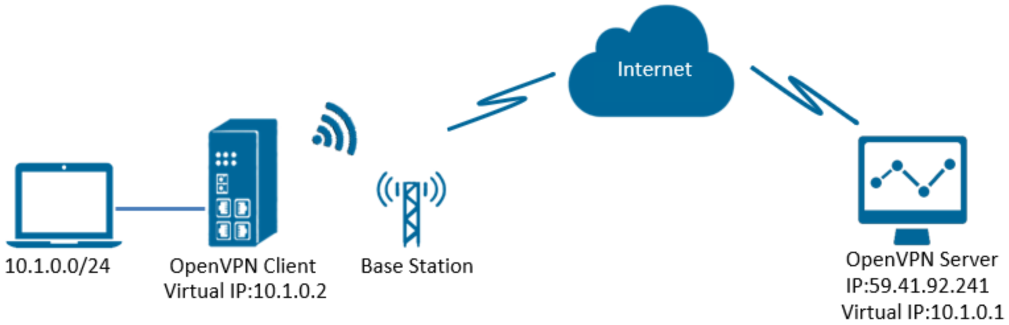


Figure 163 – OpenVPN with TAP under P2P

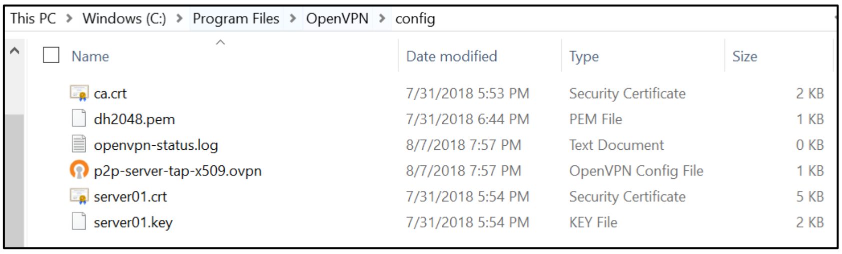
1. **AirGate 4G** runs as OpenVPN Client with any kind of IP, which can ping OpenVPN server IP successfully.
2. A PC runs as OpenVPN Server with a static public IP and open a specified a listening port for OpenVPN.
3. OpenVPN tunnel is established between Server and Client, the virtual IP can PING each other successfully. Also Server can ping LAN PC device and vice versa.

6.8.2 CONFIGURATION

6.8.2.1 PC CONFIGURATION

To configure the computer, you must download the OpenVPN software, available at https://openvpn.net/, and run and install it with administrator authority.

Once the software has been installed, you should copy the related certificates and the specific configuration to your computer, as shown in the figure below:



This PC > Windows (C:) > Program Files > OpenVPN > config

Name	Date modified	Type	Size
ca.crt	7/31/2018 5:53 PM	Security Certificate	2 KB
dh2048.pem	7/31/2018 6:44 PM	PEM File	1 KB
openvpn-status.log	8/7/2018 7:57 PM	Text Document	0 KB
p2p-server-tap-x509.ovpn	8/7/2018 7:57 PM	OpenVPN Config File	1 KB
server01.crt	7/31/2018 5:54 PM	Security Certificate	5 KB
server01.key	7/31/2018 5:54 PM	KEY File	2 KB

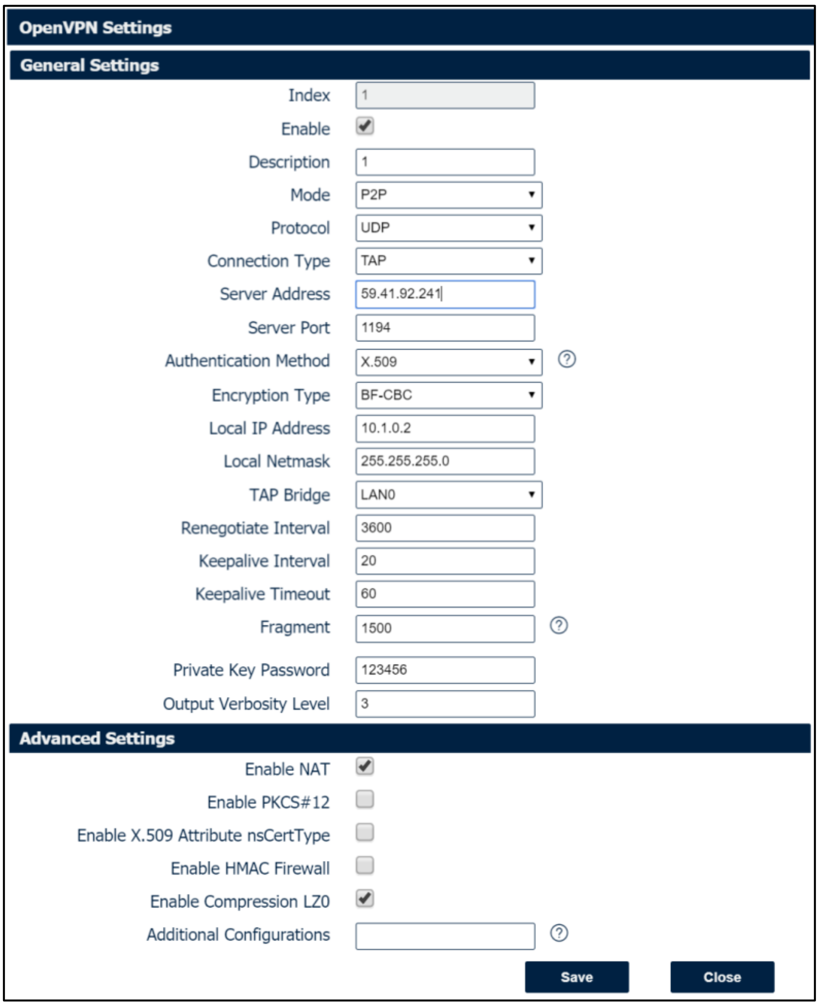
Figure 164 – OpenVPN configuration

After that, just run the file **p2p-server-tap-x.509.ovpn** and configure it as shown below:

```
mode p2p
port 1194
proto udp
dev tap
# tap
ifconfig 10.1.0.1 255.255.255.0
keepalive 20 120
persist-key
persist-tun
tls-server
ca ca.crt
cert server01.crt
key server01.key
dh dh2048.pem
#tls-auth ta.key 0
cipher BF-CBC
comp-lzo
status openvpn-status.log
verb 3
tun-mtu 1500
```

6.8.2.2 ROUTER CONFIGURATION

You must open the Web Interface of **AirGate 4G** and go to **VPN > OpenVPN > OpenVPN > General Settings**. Click the edit button and configure OpenVPN as below:



OpenVPN Settings

General Settings

Index	1
Enable	☑
Description	1
Mode	P2P
Protocol	UDP
Connection Type	TAP
Server Address	59.41.92.241
Server Port	1194
Authentication Method	X.509
Encryption Type	BF-CBC
Local IP Address	10.1.0.2
Local Netmask	255.255.255.0
TAP Bridge	LAN0
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500
Private Key Password	123456
Output Verbosity Level	3

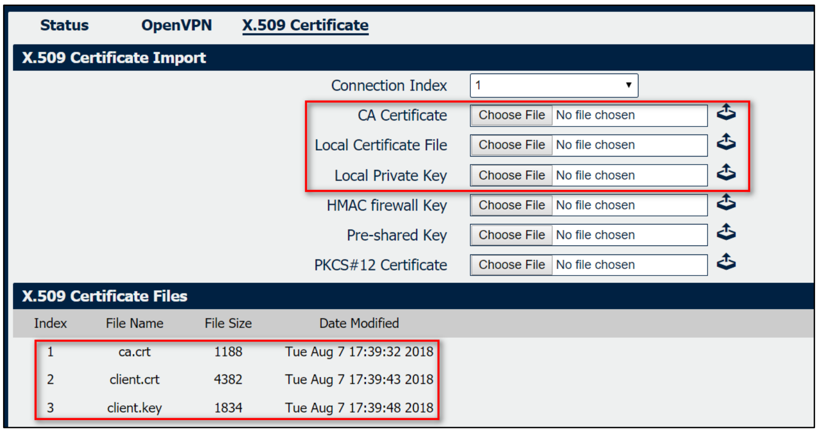
Advanced Settings

Enable NAT	☑
Enable PKCS#12	□
Enable X.509 Attribute nsCertType	□
Enable HMAC Firewall	□
Enable Compression LZ0	☑
Additional Configurations	

Figure 165 – OpenVPN configuration

Click **Save > Apply**.

After that, go to **VPN > OpenVPN > X.509 Certificate** to import the related certification. Click **Apply**.



X.509 Certificate Import

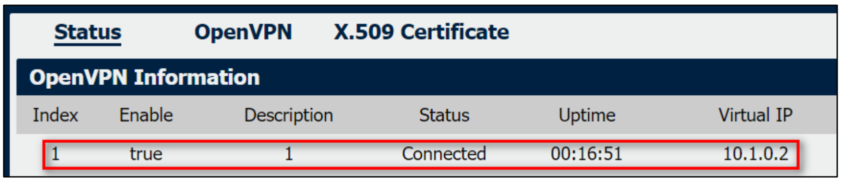
Connection Index	1
CA Certificate	Choose File No file chosen
Local Certificate File	Choose File No file chosen
Local Private Key	Choose File No file chosen
HMAC firewall Key	Choose File No file chosen
Pre-shared Key	Choose File No file chosen
PKCS#12 Certificate	Choose File No file chosen

X.509 Certificate Files

Index	File Name	File Size	Date Modified
1	ca.crt	1188	Tue Aug 7 17:39:32 2018
2	client.crt	4382	Tue Aug 7 17:39:43 2018
3	client.key	1834	Tue Aug 7 17:39:48 2018

Figure 166 – X.509 certificates

Route had connected to OpenVPN server. Go to **VPN > OpenVPN > Status** to check the connection status.



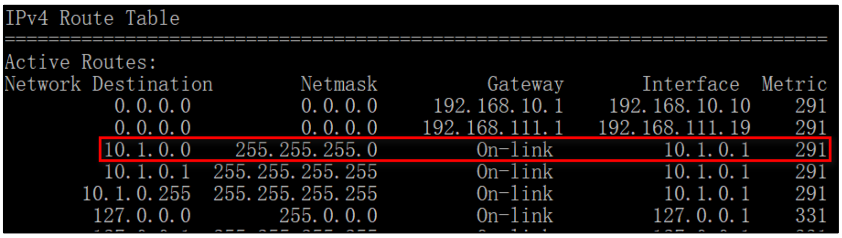
OpenVPN Information

Index	Enable	Description	Status	Uptime	Virtual IP
1	true	1	Connected	00:16:51	10.1.0.2

Figure 167 – OpenVPN status connection

6.8.3 ROUTE TABLE

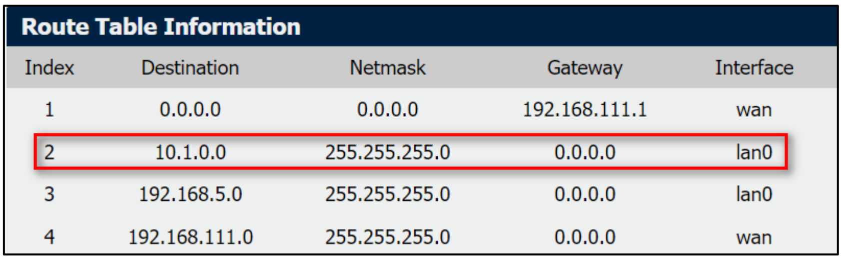
Figure 168 shows a route table of the PC for reference:



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.10.1    192.168.10.10    291
          0.0.0.0          0.0.0.0    192.168.111.1   192.168.111.19    291
         10.1.0.0    255.255.255.0         On-link          10.1.0.1    291
         10.1.0.1  255.255.255.255         On-link          10.1.0.1    291
       10.1.0.255  255.255.255.255         On-link          10.1.0.1    291
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
```

Figure 168 – PC route table

Figure 169 shows a route table of the router for reference:



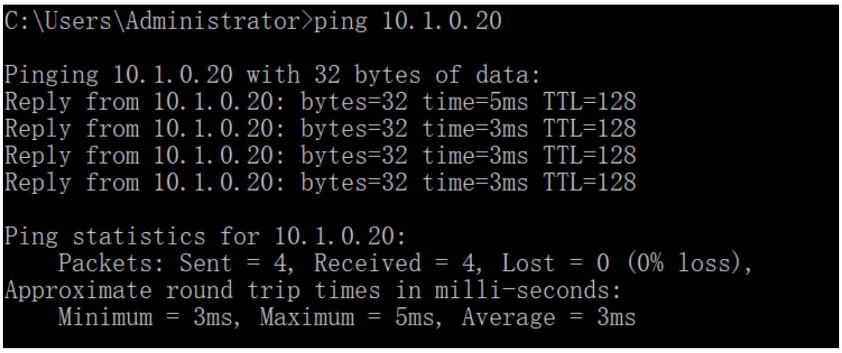
Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.1.0.0	255.255.255.0	0.0.0.0	lan0
3	192.168.5.0	255.255.255.0	0.0.0.0	lan0
4	192.168.111.0	255.255.255.0	0.0.0.0	wan

Figure 169 – Router table

6.8.4 TEST

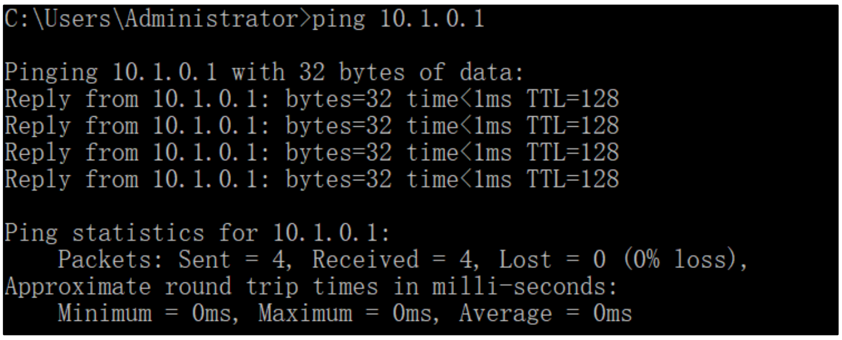
Enable CMD and Ping from PC side to LAN device of router.



```
C:\Users\Administrator>ping 10.1.0.20

Pinging 10.1.0.20 with 32 bytes of data:
Reply from 10.1.0.20: bytes=32 time=5ms TTL=128
Reply from 10.1.0.20: bytes=32 time=3ms TTL=128
Reply from 10.1.0.20: bytes=32 time=3ms TTL=128
Reply from 10.1.0.20: bytes=32 time=3ms TTL=128

Ping statistics for 10.1.0.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 5ms, Average = 3ms
```

Figure 170 – CMD

After that, ping from LAN device of router to PC side.



```
C:\Users\Administrator>ping 10.1.0.1

Pinging 10.1.0.1 with 32 bytes of data:
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 171 – Ping

Test successfully.

6.9 OpenVPN WITH TUN CERTIFICATE UNDER P2P MODE

This tutorial shows how to configure OpenVPN with TUN and under P2P mode.

6.9.1 TOPOLOGY

You can use the following topology:

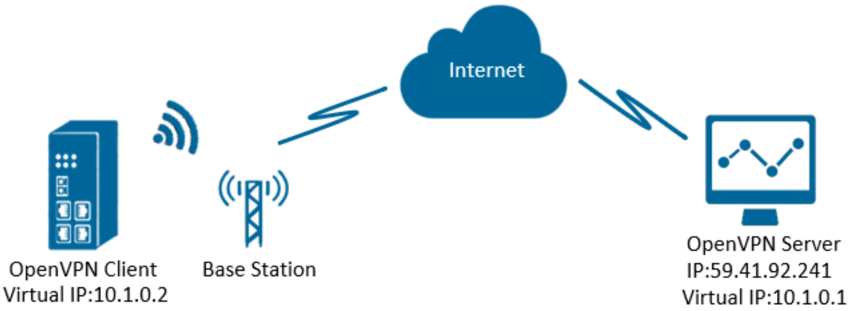


Figure 172 – OpenVPN with TUN under P2P mode

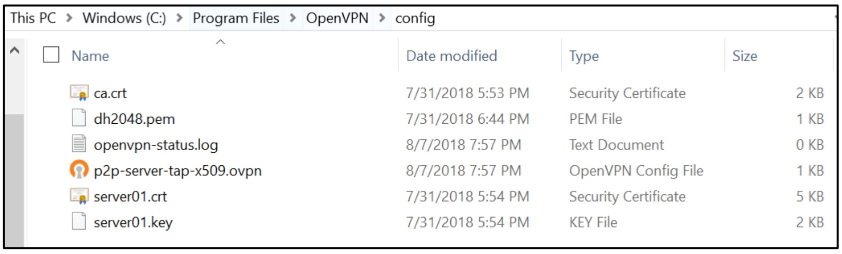
1. **AirGate 4G** runs as OpenVPN Client with any kind of IP, which can ping OpenVPN server IP successfully.
2. A PC runs as OpenVPN Server with a static public IP and open a specified a listening port for OpenVPN.
3. OpenVPN tunnel is established between Server and Client, the virtual IP can Ping each other successfully.

6.9.2 CONFIGURATION

6.9.2.1 PC CONFIGURATION

To configure the computer, you must download the OpenVPN software, available at https://openvpn.net/, and run and install it with administrator authority.

Once the software has been installed, you should copy the related certificates and the specific configuration to your computer, as shown in the figure below:



Name	Date modified	Type	Size
ca.crt	7/31/2018 5:53 PM	Security Certificate	2 KB
dh2048.pem	7/31/2018 6:44 PM	PEM File	1 KB
openvpn-status.log	8/7/2018 7:57 PM	Text Document	0 KB
p2p-server-tap-x509.ovpn	8/7/2018 7:57 PM	OpenVPN Config File	1 KB
server01.crt	7/31/2018 5:54 PM	Security Certificate	5 KB
server01.key	7/31/2018 5:54 PM	KEY File	2 KB

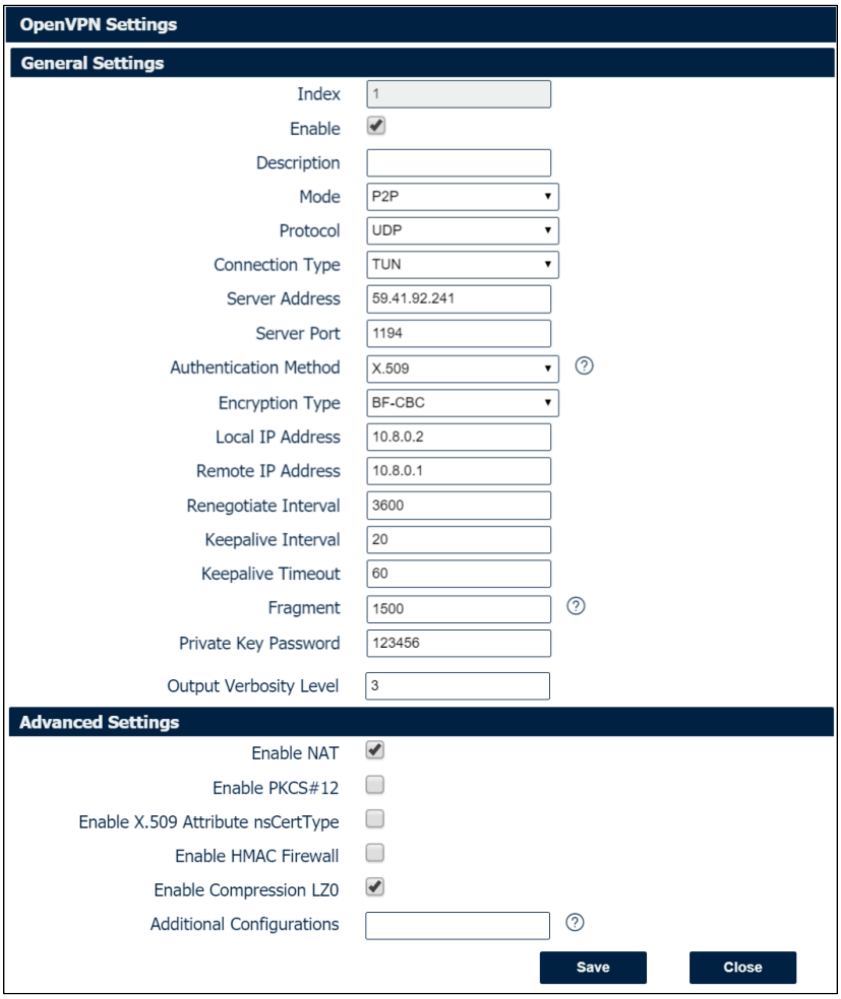
Figure 173 – OpenVPN configuration

After that, just run the file **p2p-server-tun-x.509** and configure it as shown below:

```
mode p2p
port 1194
proto udp
dev tun
# tun
ifconfig 10.8.0.1 10.8.0.2
keepalive 20 120
persist-key
persist-tun
tls-server
ca ca.crt
cert server01.crt
key server01.key
dh dh2048.pem
#tls-auth ta.key 0
cipher BF-CBC
comp-lzo
status openvpn-status.log
verb 3
tun-mtu 1500
fragment 1500
```

6.9.2.2 ROUTER CONFIGURATION

You must open the Web Interface of **AirGate 4G** and go to **VPN** > **OpenVPN** > **OpenVPN** > **General Settings**. Click the edit button and configure OpenVPN as below:



OpenVPN Settings

General Settings

Index	1
Enable	☑
Description	
Mode	P2P
Protocol	UDP
Connection Type	TUN
Server Address	59.41.92.241
Server Port	1194
Authentication Method	X.509
Encryption Type	BF-CBC
Local IP Address	10.8.0.2
Remote IP Address	10.8.0.1
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500
Private Key Password	123456
Output Verbosity Level	3

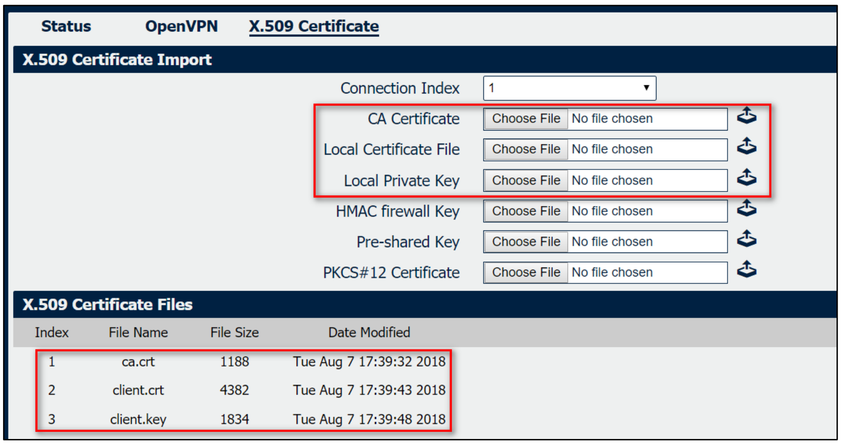
Advanced Settings

Enable NAT	☑
Enable PKCS#12	□
Enable X.509 Attribute nsCertType	□
Enable HMAC Firewall	□
Enable Compression LZO	☑
Additional Configurations	

Figure 174 – OpenVPN settings

Click **Save** > **Apply**.

After that, go to **VPN** > **OpenVPN** > **X.509 Certificate** to import the related certification. Click **Apply**.



X.509 Certificate Import

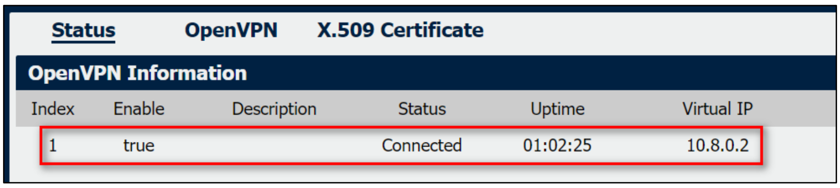
Connection Index	1
CA Certificate	Choose File No file chosen
Local Certificate File	Choose File No file chosen
Local Private Key	Choose File No file chosen
HMAC firewall Key	Choose File No file chosen
Pre-shared Key	Choose File No file chosen
PKCS#12 Certificate	Choose File No file chosen

X.509 Certificate Files

Index	File Name	File Size	Date Modified
1	ca.crt	1188	Tue Aug 7 17:39:32 2018
2	client.crt	4382	Tue Aug 7 17:39:43 2018
3	client.key	1834	Tue Aug 7 17:39:48 2018

Figure 175 – Certificate import

Route had connected to OpenVPN server. Go to **VPN** > **OpenVPN** > **Status** to check the connection status.



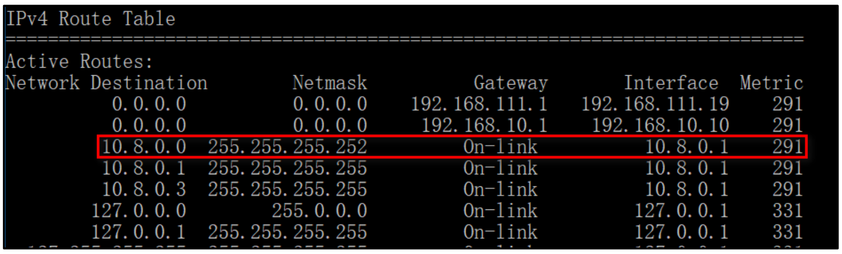
OpenVPN Information

Index	Enable	Description	Status	Uptime	Virtual IP
1	true		Connected	01:02:25	10.8.0.2

Figure 176 – OpenVPN status connection

6.9.3 ROUTE TABLE

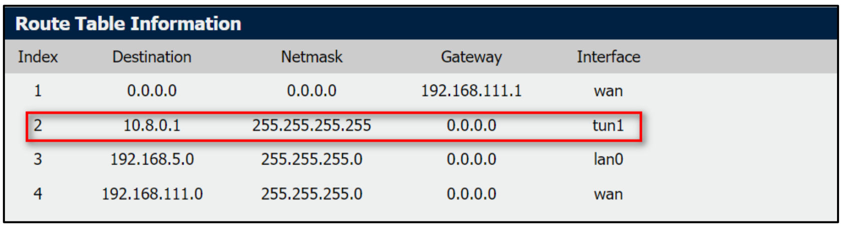
Figure 177 shows a route table of the PC for reference:



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.111.1  192.168.111.19    291
          0.0.0.0          0.0.0.0     192.168.10.1   192.168.10.10    291
         10.8.0.0  255.255.255.252         On-link         10.8.0.1    291
         10.8.0.1  255.255.255.255         On-link         10.8.0.1    291
         10.8.0.3  255.255.255.255         On-link         10.8.0.1    291
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    331
```

Figure 177 – PC route table

Figure 178 shows a route table of the router for reference:



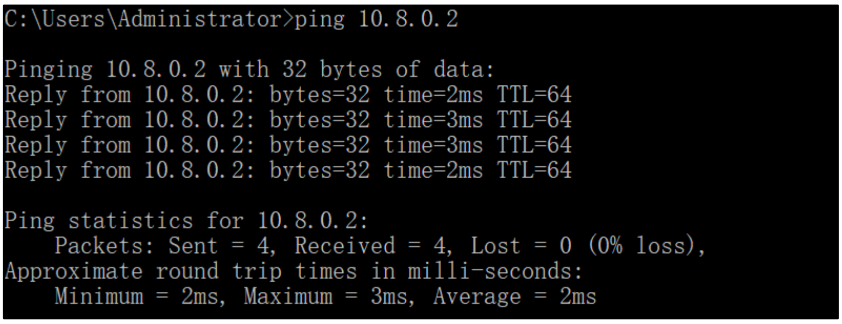
Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.1	255.255.255.255	0.0.0.0	tun1
3	192.168.5.0	255.255.255.0	0.0.0.0	lan0
4	192.168.111.0	255.255.255.0	0.0.0.0	wan

Figure 178 – Route table

6.9.4 TEST

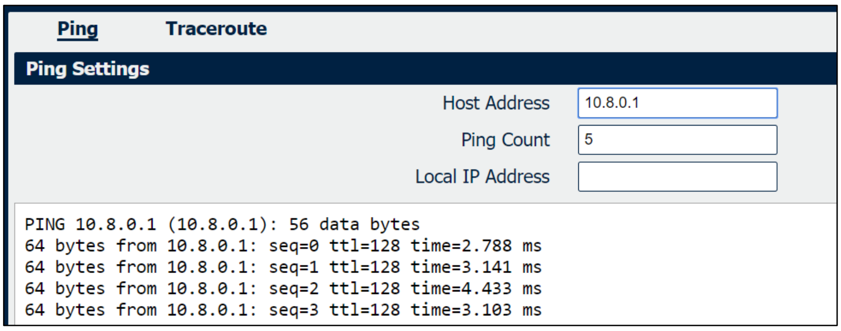
Enable CMD and Ping from PC side to router side.



```
C:\Users\Administrator>ping 10.8.0.2

Pinging 10.8.0.2 with 32 bytes of data:
Reply from 10.8.0.2: bytes=32 time=2ms TTL=64
Reply from 10.8.0.2: bytes=32 time=3ms TTL=64
Reply from 10.8.0.2: bytes=32 time=3ms TTL=64
Reply from 10.8.0.2: bytes=32 time=2ms TTL=64

Ping statistics for 10.8.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Figure 179 – CMD

You must open the Web Interface of **AirGate 4G** and go to **Maintenance > Debug Tool > Ping** and Ping from router side to PC side.



Host Address: 10.8.0.1

Ping Count: 5

Local IP Address:

```
PING 10.8.0.1 (10.8.0.1): 56 data bytes
64 bytes from 10.8.0.1: seq=0 ttl=128 time=2.788 ms
64 bytes from 10.8.0.1: seq=1 ttl=128 time=3.141 ms
64 bytes from 10.8.0.1: seq=2 ttl=128 time=4.433 ms
64 bytes from 10.8.0.1: seq=3 ttl=128 time=3.103 ms
```

Figure 180 – Ping

Test successfully.

6.10 IPsec: PRE-SHARED KEY WITH CISCO ROUTER

This tutorial shows how to configure IPsec with pre-shared key with Cisco router.

6.10.1 TOPOLOGY

You can use the following topology:

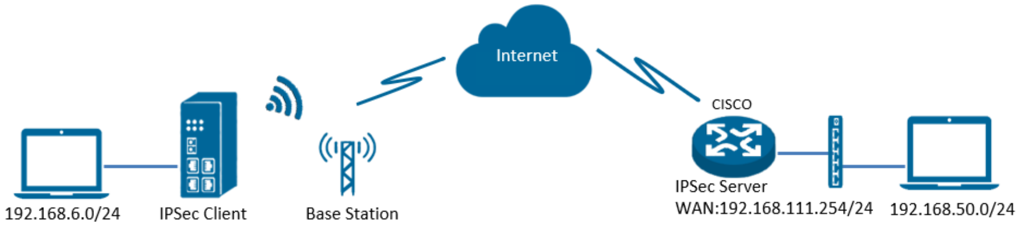


Figure 181 – IPsec topology

1. **AirGate 4G** runs as IPSec Client with any kind of IP, which can ping IPSec server IP successfully.
2. Cisco router runs as IPSec Server with a static public IP.
3. IPSec tunnel is established between **AirGate 4G** and Cisco router.

6.10.2 CONFIGURATION

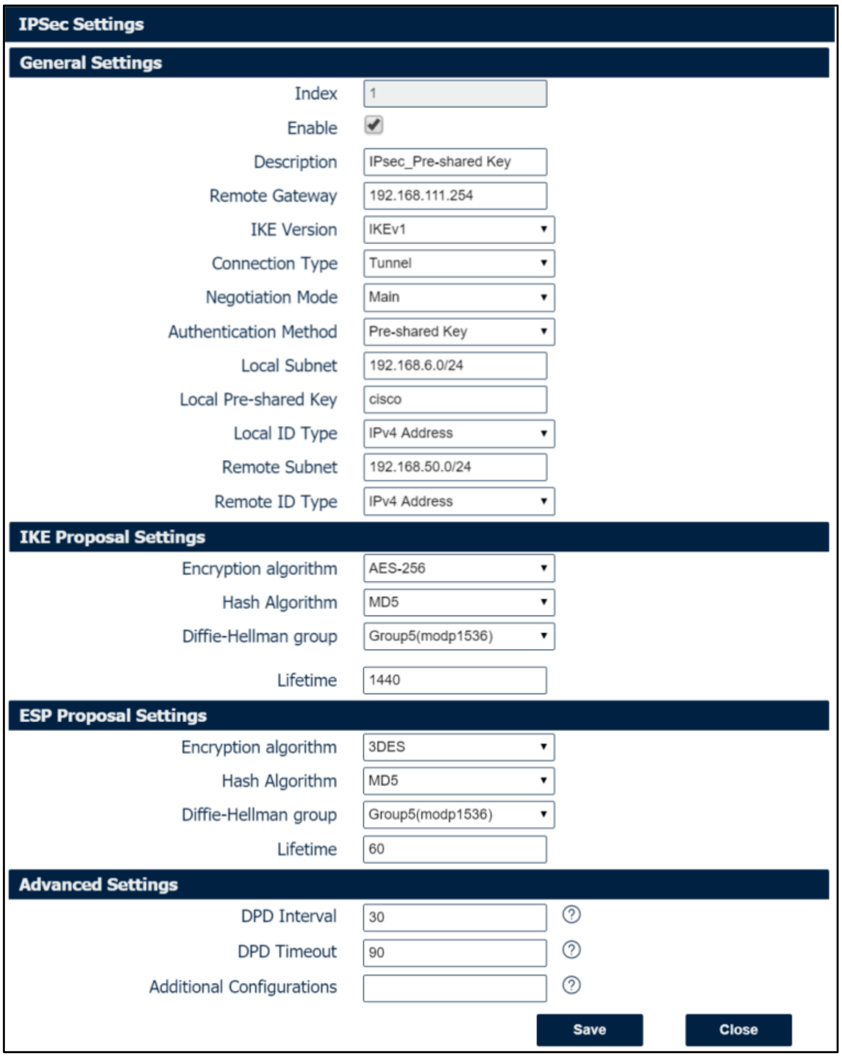
6.10.2.1 SERVER CONFIGURATION

Login to Cisco router and setting like below:

```
cisco2811#show running-config
Building configuration...
Current configuration : 3071 bytes
!
version 12.4
hostname cisco2811
logging message-counter syslog
enable secret 5 $1$tw/d$UQQ3Xh06n.2HHFeAVIgXJ.
!
no aaa new-model
!
ip domain name cisco.com
ip name-server 192.168.111.1
ip address-pool local
no ipv6 cef
!
multilink bundle-name authenticated
!
username cisco password 0 cisco
archive
 log config
 hidekeys
!
crypto isakmp policy 10
 encr aes 256
 hash md5
 authentication pre-share
 group 5
crypto isakmp key 6 cisco address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set NR500 esp-3des esp-md5-hmac
!
crypto dynamic-map DYN 10
 set transform-set NR500
 set pfs group5
 match address 101
 reverse-route
!
crypto map SMAP 10 ipsec-isakmp dynamic DYN
!
track 1 interface FastEthernet0/0 line-protocol
!
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
 speed auto
 no mop enabled
 crypto map SMAP
!
interface FastEthernet0/1
 ip address 192.168.5.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.111.1
no ip http server
no ip http secure-server
!
ip nat inside source list 10 interface FastEthernet0/0 overload
!
ip access-list extended VPN
 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
snmp-server community public RO

end
cisco2811#
```

6.10.2.2 CLIENT CONFIGURATION

You must open the Web Interface of **AirGate 4G** and go to **VPN > IPsec > IPsec > General Settings**. Click the edit button and configure IPsec as below:



IPSec Settings

General Settings

Index	1
Enable	☑
Description	IPsec_Pre-shared Key
Remote Gateway	192.168.111.254
IKE Version	IKEv1
Connection Type	Tunnel
Negotiation Mode	Main
Authentication Method	Pre-shared Key
Local Subnet	192.168.6.0/24
Local Pre-shared Key	cisco
Local ID Type	IPv4 Address
Remote Subnet	192.168.50.0/24
Remote ID Type	IPv4 Address

IKE Proposal Settings

Encryption algorithm	AES-256
Hash Algorithm	MD5
Diffie-Hellman group	Group5(modp1536)
Lifetime	1440

ESP Proposal Settings

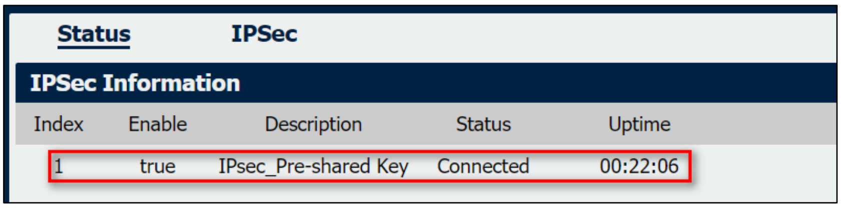
Encryption algorithm	3DES
Hash Algorithm	MD5
Diffie-Hellman group	Group5(modp1536)
Lifetime	60

Advanced Settings

DPD Interval	30
DPD Timeout	90
Additional Configurations	

Figure 182 – IPsec settings

Click **Save > Apply**. IPSec had been connected successfully. After that, go to **VPN>IPSec>Status** to check the connection status.



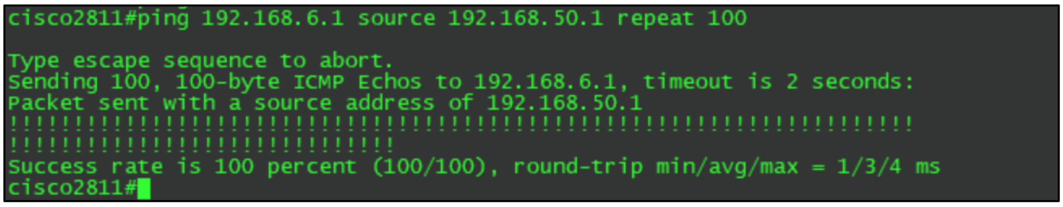
IPSec Information

Index	Enable	Description	Status	Uptime
1	true	IPsec_Pre-shared Key	Connected	00:22:06

Figure 183 – IPsec status connection

6.10.3 TEST

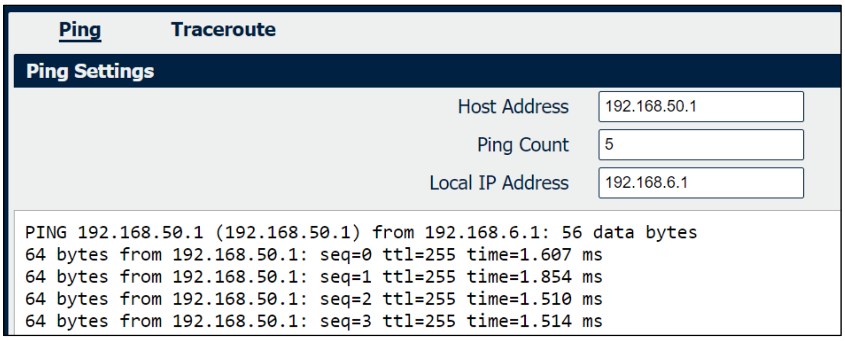
Ping from Cisco router to **AirGate 4G**. LAN to LAN communication is working correctly.



```
cisco2811#ping 192.168.6.1 source 192.168.50.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms
cisco2811#
```

Figure 184 – Teste do terminal Cisco

Ping from **AirGate 4G** to Cisco router. LAN to LAN communication is working correctly.



Host Address: 192.168.50.1

Ping Count: 5

Local IP Address: 192.168.6.1

```
PING 192.168.50.1 (192.168.50.1) from 192.168.6.1: 56 data bytes
64 bytes from 192.168.50.1: seq=0 ttl=255 time=1.607 ms
64 bytes from 192.168.50.1: seq=1 ttl=255 time=1.854 ms
64 bytes from 192.168.50.1: seq=2 ttl=255 time=1.510 ms
64 bytes from 192.168.50.1: seq=3 ttl=255 time=1.514 ms
```

Figure 185 – AirGate 4G test

Test successfully.

6.11 IPsec: FQDN WITH CISCO ROUTER

This tutorial shows how to configure IPsec_FQDN with Cisco router.

6.11.1 TOPOLOGY

You can use the following topology:

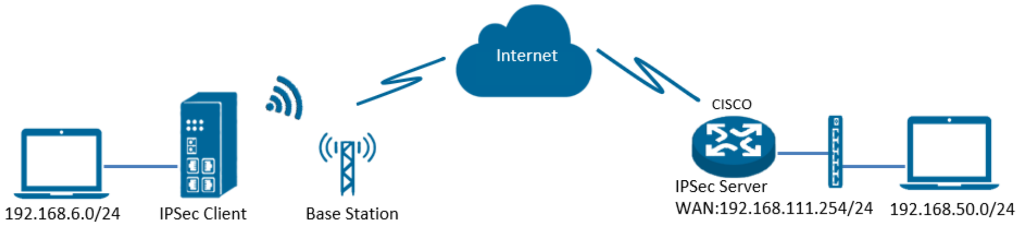


Figure 186 – IPsec topology

1. **AirGate 4G** runs as IPSec Client with any kind of IP, which can ping IPSec server IP successfully.
2. Cisco router runs as IPSec Server with a static public IP.
3. IPSec tunnel is established between **AirGate 4G** and Cisco router.

6.11.2 CONFIGURATION

6.11.2.1 SERVER CONFIGURATION

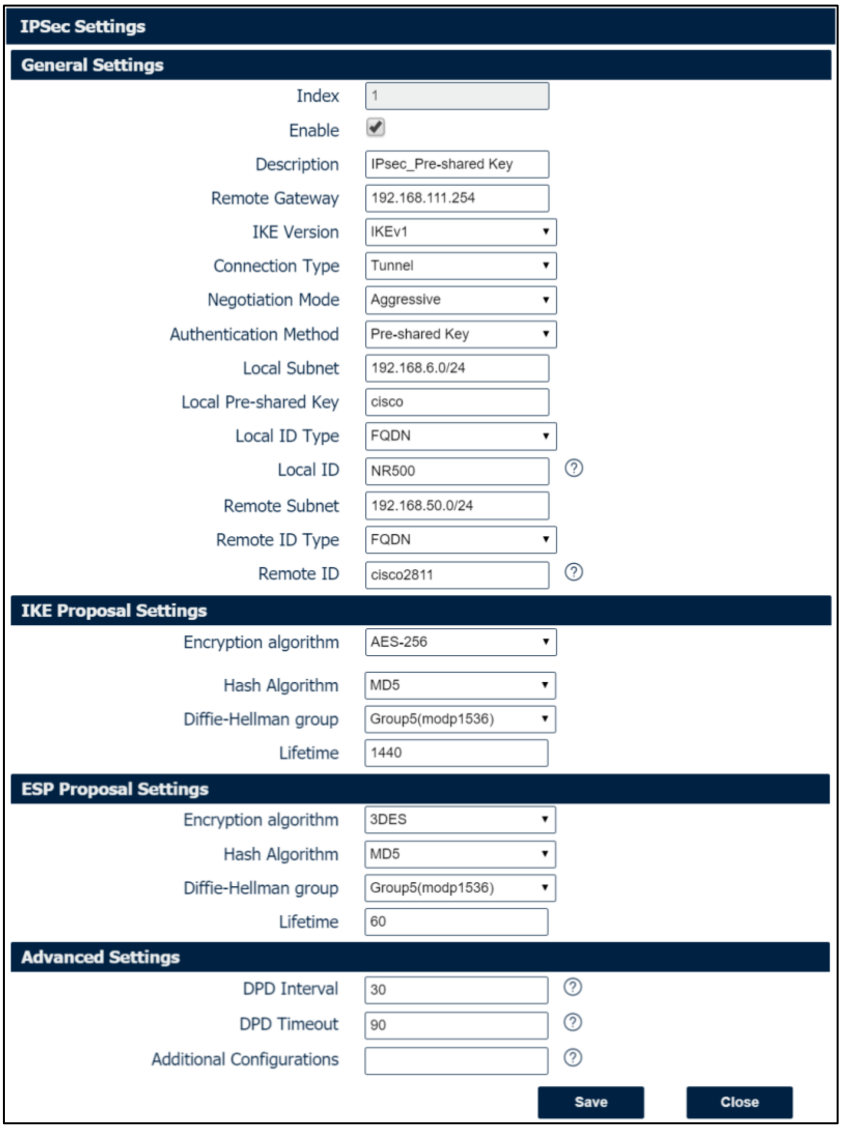
Login to Cisco router and setting like below:

```
cisco2811#show running-config
Building configuration...
version 12.4
hostname cisco2811
!
logging message-counter syslog
enable secret 5 $1$tw/d$UQQ3Xh06n.2HHFeAVIgXJ.
!
no aaa new-model
ip cef
!
ip name-server 192.168.111.1
ip address-pool local
multilink bundle-name authenticated
!
username cisco password 0 cisco
archive
 log config
 hidekeys
!
crypto isakmp policy 10
 encr aes 256
 hash md5
 authentication pre-share
 group 5
crypto isakmp key 6 cisco hostname NR500
crypto isakmp identity hostname
!
crypto isakmp peer address 0.0.0.0
 set aggressive-mode password cisco
 set aggressive-mode client-endpoint fqdn NR500
!
crypto ipsec transform-set NR500 esp-3des esp-md5-hmac
!
crypto dynamic-map DYN 10
```

```
 set transform-set NR500
 set pfs group5
 match address 101
 reverse-route
!
crypto map SMAP 10 ipsec-isakmp dynamic DYN
!
track 1 interface FastEthernet0/0 line-protocol
!
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
 speed auto
 no mop enabled
 crypto map SMAP
!
interface FastEthernet0/1
 ip address 192.168.5.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto

ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.111.1
ip nat inside source list 10 interface FastEthernet0/0 overload
!
ip access-list extended VPN
 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
snmp-server community public RO
!
end
cisco2811#
```

6.11.2.2 CLIENT CONFIGURATION

You must open the Web Interface of **AirGate 4G** and go to **VPN > IPsec > IPsec > General Settings**. Click the edit button and configure IPsec as below:



IPSec Settings

General Settings

Index	1
Enable	☑
Description	IPsec_Pre-shared Key
Remote Gateway	192.168.111.254
IKE Version	IKEv1
Connection Type	Tunnel
Negotiation Mode	Aggressive
Authentication Method	Pre-shared Key
Local Subnet	192.168.6.0/24
Local Pre-shared Key	cisco
Local ID Type	FQDN
Local ID	NR500
Remote Subnet	192.168.50.0/24
Remote ID Type	FQDN
Remote ID	cisco2811

IKE Proposal Settings

Encryption algorithm	AES-256
Hash Algorithm	MD5
Diffie-Hellman group	Group5(modp1536)
Lifetime	1440

ESP Proposal Settings

Encryption algorithm	3DES
Hash Algorithm	MD5
Diffie-Hellman group	Group5(modp1536)
Lifetime	60

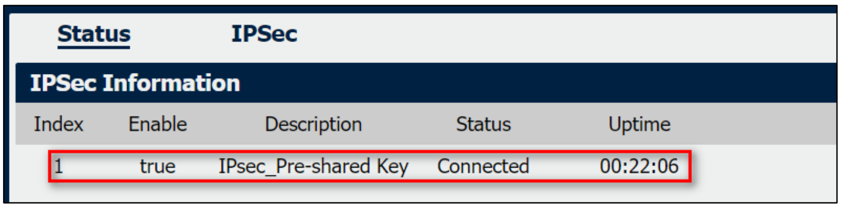
Advanced Settings

DPD Interval	30
DPD Timeout	90
Additional Configurations	

Figure 187 – IPsec settings

Click **Save > Apply**.

IPSec had been connected successfully. Go to **VPN > IPSec > Status** to check the connection status.



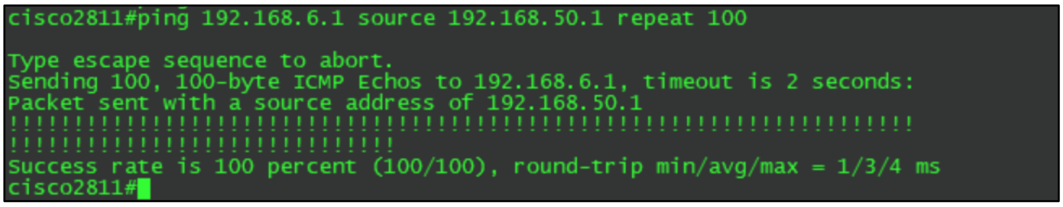
IPSec Information

Index	Enable	Description	Status	Uptime
1	true	IPsec_Pre-shared Key	Connected	00:22:06

Figure 188 – IPsec status connection

6.11.3 TEST

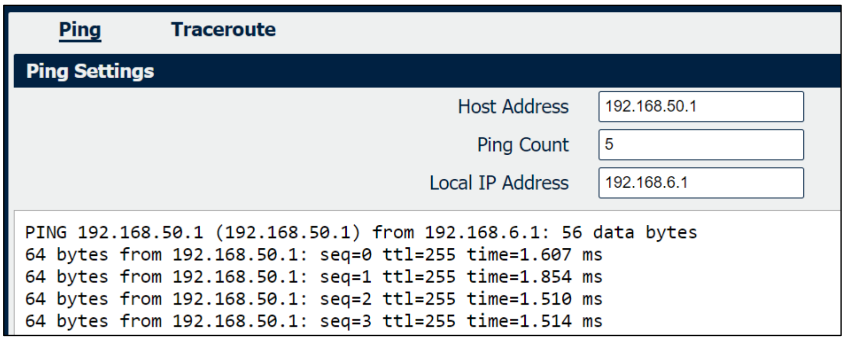
Ping from Cisco router to **AirGate 4G**. LAN to LAN communication is working correctly.



```
cisco2811#ping 192.168.6.1 source 192.168.50.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms
cisco2811#
```

Figure 189 – IPsec test

You must open the Web Interface of **AirGate 4G** and go to **Maintenance > Debug Tool > Ping** and Ping from **AirGate 4G** to Cisco router. LAN to LAN communication is working correctly.



Host Address: 192.168.50.1

Ping Count: 5

Local IP Address: 192.168.6.1

```
PING 192.168.50.1 (192.168.50.1) from 192.168.6.1: 56 data bytes
64 bytes from 192.168.50.1: seq=0 ttl=255 time=1.607 ms
64 bytes from 192.168.50.1: seq=1 ttl=255 time=1.854 ms
64 bytes from 192.168.50.1: seq=2 ttl=255 time=1.510 ms
64 bytes from 192.168.50.1: seq=3 ttl=255 time=1.514 ms
```

Figure 190 – IPsec test

Test successfully.

6.12 IPsec: PRE-SHARED KEY AND XAUTH WITH CISCO ROUTER

This tutorial shows how to configure IPsec_pre-shared key and Xauth with Cisco router.

6.12.1 TOPOLOGY

You can use the following topology:

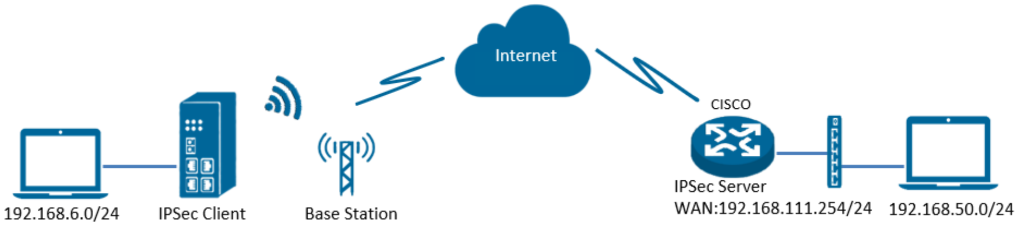


Figure 191 – IPsec topology

1. **AirGate 4G** runs as IPSec Client with any kind of IP, which can ping IPSec server IP successfully.
2. Cisco router runs as IPSec Server with a static public IP.
3. IPSec tunnel is established between **AirGate 4G** and Cisco router.

6.12.2 CONFIGURATION

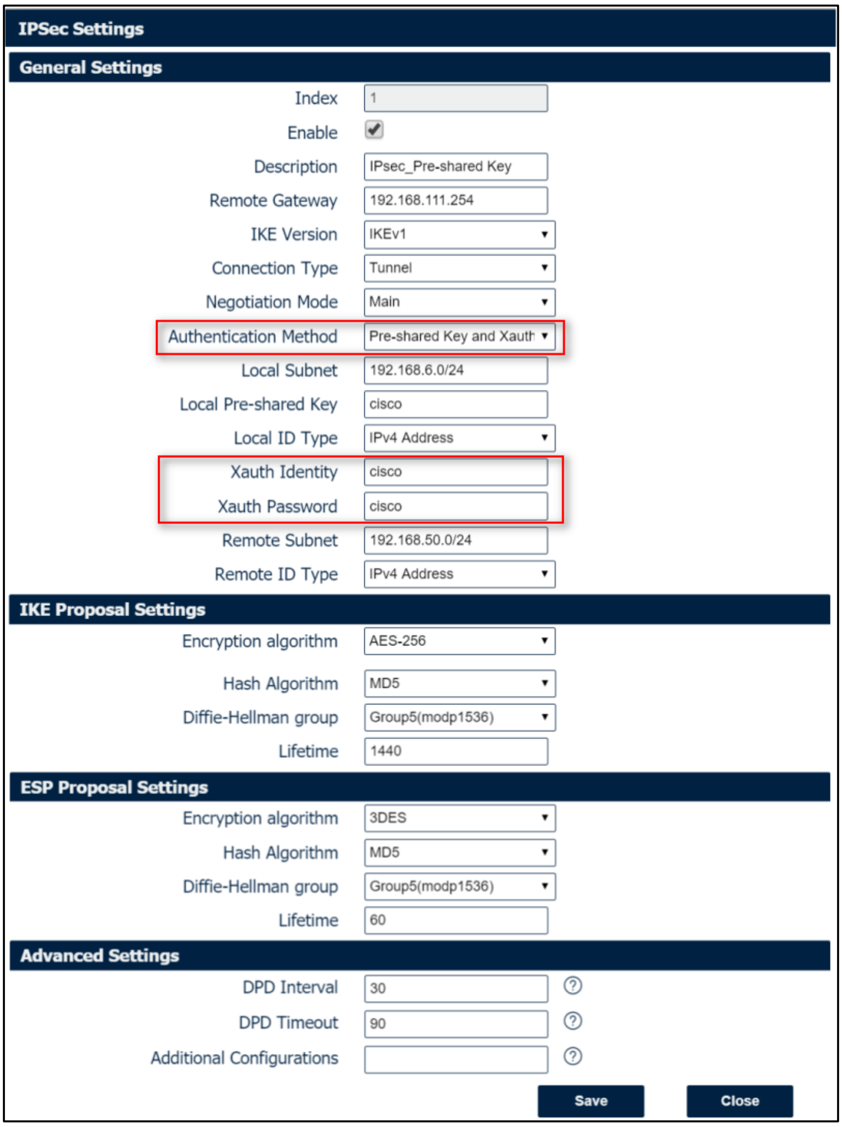
6.12.2.1 SERVER CONFIGURATION

Login to Cisco router and setting like below:

```
cisco2811#show running-config
version 12.4
hostname cisco2811
!
enable secret 5 $1$tw/d$UQQ3Xh06n.2HHFeAVIgXJ.
aaa new-model
aaa authentication login LOGIN local
!
aaa session-id common
dot11 syslog
ip source-route
!
ip cef
ip domain name cisco.com
ip name-server 192.168.111.1
ip address-pool local
no ipv6 cef
!
username cisco password 0 cisco
archive
 log config
 hidekeys
!
crypto isakmp policy 10
 encr aes 256
 hash md5
 authentication pre-share
 group 5
crypto isakmp key 6 cisco address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set NR500 esp-3des esp-md5-hmac
!
crypto dynamic-map DYN 10
 set transform-set NR500
 set pfs group5
 match address 101
 reverse-route
!
crypto map MAP client authentication list LOGIN
crypto map MAP 10 ipsec-isakmp dynamic DYN
!
track 1 interface FastEthernet0/0 line-protocol

interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
 speed auto
 no mop enabled
 crypto map MAP
!
interface FastEthernet0/1
 ip address 192.168.5.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.111.1
ip nat inside source list 10 interface FastEthernet0/0 overload
!
ip access-list extended VPN
 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
!!
line con 0
line vty 5 15
 exec-timeout 5 2
end
```

6.12.2.2 CLIENT CONFIGURATION

You must open the Web Interface of **AirGate 4G** and go to **VPN > IPsec > IPsec > General Settings**. Click the edit button and configure IPsec as below:



IPSec Settings

General Settings

Index: 1

Enable: ☑

Description: IPsec_Pre-shared Key

Remote Gateway: 192.168.111.254

IKE Version: IKEv1

Connection Type: Tunnel

Negotiation Mode: Main

Authentication Method: Pre-shared Key and Xauth

Local Subnet: 192.168.6.0/24

Local Pre-shared Key: cisco

Local ID Type: IPv4 Address

Xauth Identity: cisco

Xauth Password: cisco

Remote Subnet: 192.168.50.0/24

Remote ID Type: IPv4 Address

IKE Proposal Settings

Encryption algorithm: AES-256

Hash Algorithm: MD5

Diffie-Hellman group: Group5(modp1536)

Lifetime: 1440

ESP Proposal Settings

Encryption algorithm: 3DES

Hash Algorithm: MD5

Diffie-Hellman group: Group5(modp1536)

Lifetime: 60

Advanced Settings

DPD Interval: 30

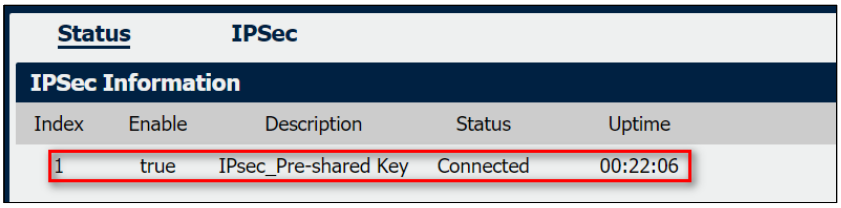
DPD Timeout: 90

Additional Configurations:

Figure 192 – IPsec settings

Click **Save > Apply**.

IPSec had been connected successfully. Go to **VPN > IPSec > Status** to check the connection status.



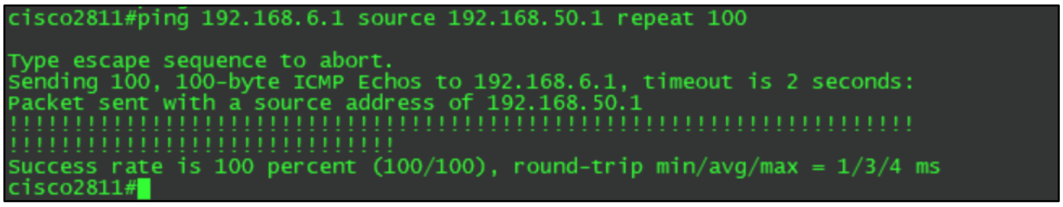
IPSec Information

Index	Enable	Description	Status	Uptime
1	true	IPsec_Pre-shared Key	Connected	00:22:06

Figure 193 – IPsec status connection

6.12.3 TEST

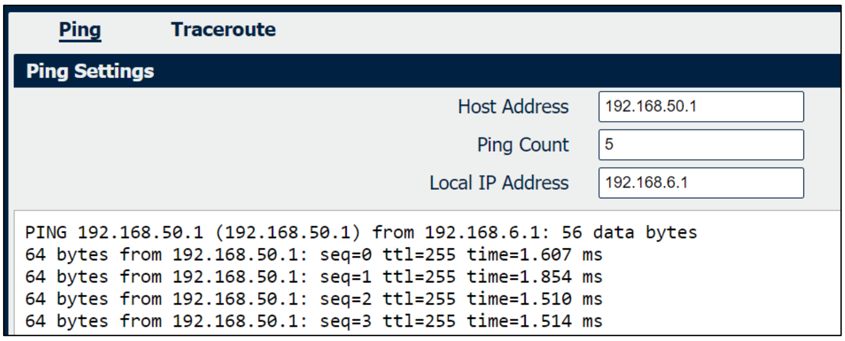
Ping from Cisco router to **AirGate 4G**. LAN to LAN communication is working correctly.



```
cisco2811#ping 192.168.6.1 source 192.168.50.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms
cisco2811#
```

Figure 194 – Cisco test

You must open the Web Interface of **AirGate 4G** and go to **Maintenance > Debug Tool > Ping** and Ping from **AirGate 4G** to Cisco router. LAN to LAN communication is working correctly.



Host Address: 192.168.50.1

Ping Count: 5

Local IP Address: 192.168.6.1

```
PING 192.168.50.1 (192.168.50.1) from 192.168.6.1: 56 data bytes
64 bytes from 192.168.50.1: seq=0 ttl=255 time=1.607 ms
64 bytes from 192.168.50.1: seq=1 ttl=255 time=1.854 ms
64 bytes from 192.168.50.1: seq=2 ttl=255 time=1.510 ms
64 bytes from 192.168.50.1: seq=3 ttl=255 time=1.514 ms
```

Figure 195 – AirGate 4G test

Test successfully.

6.13 IPsec: FQDN, PRE-SHARED KEY AND XAUTH WITH CISCO ROUTER

This tutorial shows how to configure IPSec_FQDN_Pre shared key and Xauth with Cisco router.

6.13.1 TOPOLOGY

You can use the following topology:

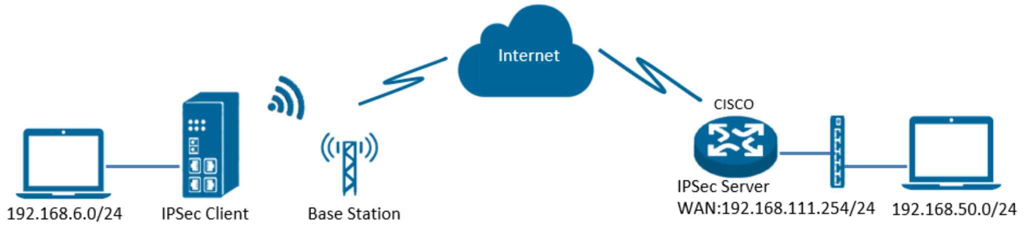


Figure 196 – IPsec toplogy

1. **AirGate 4G** runs as IPSec Client with any kind of IP, which can ping IPSec server IP successfully.
2. Cisco router runs as IPSec Server with a static public IP.
3. IPSec tunnel is established between **AirGate 4G** and Cisco router.

6.13.2 CONFIGURATION

6.13.2.1 SERVER CONFIGURATION

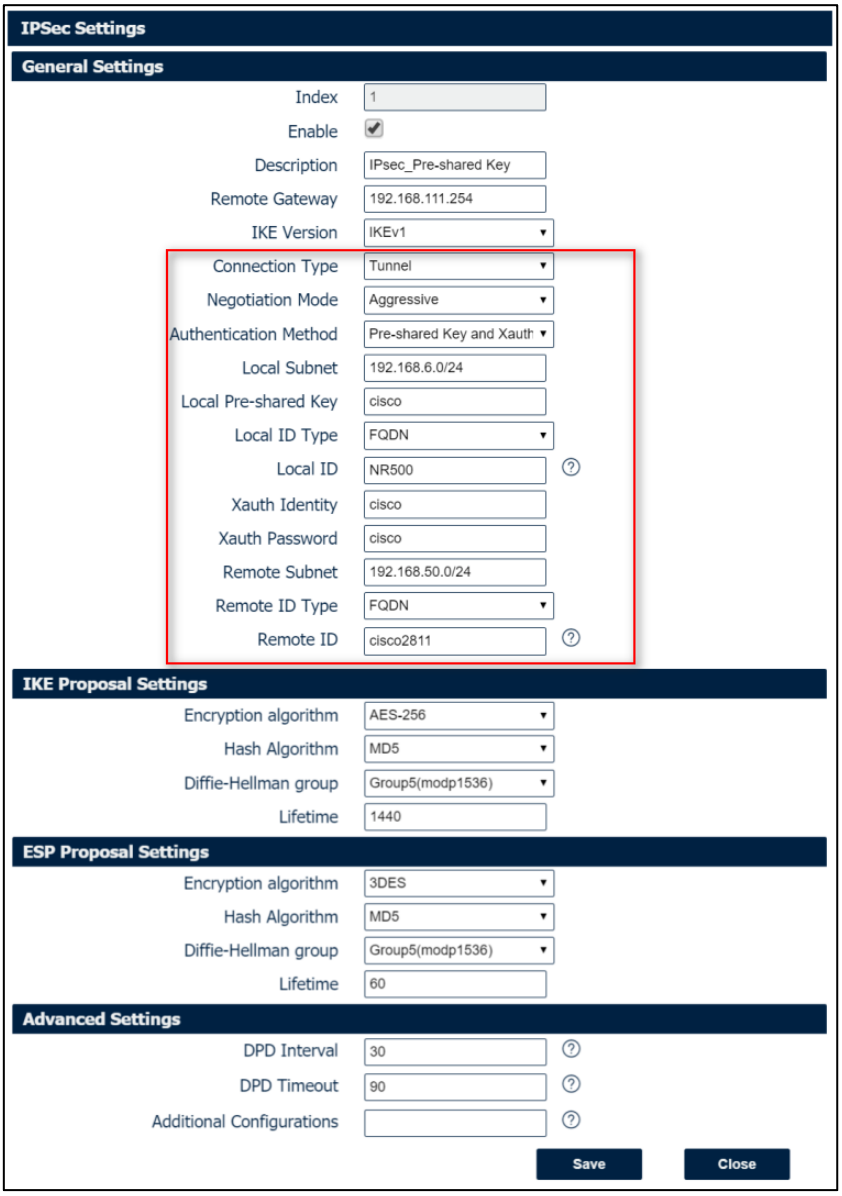
Login to Cisco router and setting like below:

```
cisco2811#show running-config
version 12.4
hostname cisco2811
!
logging message-counter syslog
enable secret 5 $1$tw/d$UQQ3Xh06n.2HHFeAVIgXJ.!
aaa new-model
!
aaa authentication login LOGIN local
!
aaa session-id common
!
ip name-server 192.168.111.1
ip address-pool local
!
multilink bundle-name authenticated
!
username cisco password 0 cisco
archive
 log config
 hidekeys
!
crypto isakmp policy 10
 encr aes 256
 hash md5
 authentication pre-share
 group 5
crypto isakmp key cisco hostname NR500
crypto isakmp identity hostname
!
crypto isakmp peer address 0.0.0.0
 set aggressive-mode password ken
 set aggressive-mode client-endpoint fqdn cisco2811
!
crypto ipsec transform-set NR500 esp-3des esp-md5-hmac
```

```
!
crypto dynamic-map DYN 10
 set transform-set NR500
 set pfs group5
 match address 101
 reverse-route
!
crypto map MAP client authentication list LOGIN
crypto map MAP 10 ipsec-isakmp dynamic DYN
!
track 1 interface FastEthernet0/0 line-protocol
!
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
no mop enabled
 crypto map MAP
!
interface FastEthernet0/1
 ip address 192.168.5.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto

ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.111.1
ip nat inside source list 10 interface FastEthernet0/0 overload
!
ip access-list extended VPN
 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
line con 0
line vty 5 15
end
```

6.13.2.2 CLIENT CONFIGURATION

You must open the Web Interface of **AirGate 4G** and go to **VPN > IPsec > IPsec > General Settings**. Click the edit button and configure IPsec as below:



IPSec Settings

General Settings

Index	1
Enable	☑
Description	IPsec_Pre-shared Key
Remote Gateway	192.168.111.254
IKE Version	IKEv1
Connection Type	Tunnel
Negotiation Mode	Aggressive
Authentication Method	Pre-shared Key and Xauth
Local Subnet	192.168.6.0/24
Local Pre-shared Key	cisco
Local ID Type	FQDN
Local ID	NR500
Xauth Identity	cisco
Xauth Password	cisco
Remote Subnet	192.168.50.0/24
Remote ID Type	FQDN
Remote ID	cisco2811

IKE Proposal Settings

Encryption algorithm	AES-256
Hash Algorithm	MD5
Diffie-Hellman group	Group5(modp1536)
Lifetime	1440

ESP Proposal Settings

Encryption algorithm	3DES
Hash Algorithm	MD5
Diffie-Hellman group	Group5(modp1536)
Lifetime	60

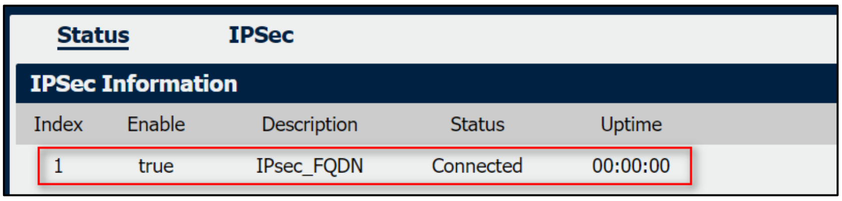
Advanced Settings

DPD Interval	30
DPD Timeout	90
Additional Configurations	

Figure 197 – IPsec settings

Click **Save > Apply**.

IPSec had been connected successfully. Go to **VPN > IPSec > Status** to check the connection status.



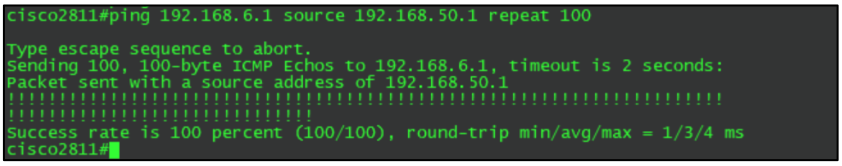
IPSec Information

Index	Enable	Description	Status	Uptime
1	true	IPsec_FQDN	Connected	00:00:00

Figure 198 – IPsec status connection

6.13.3 TEST

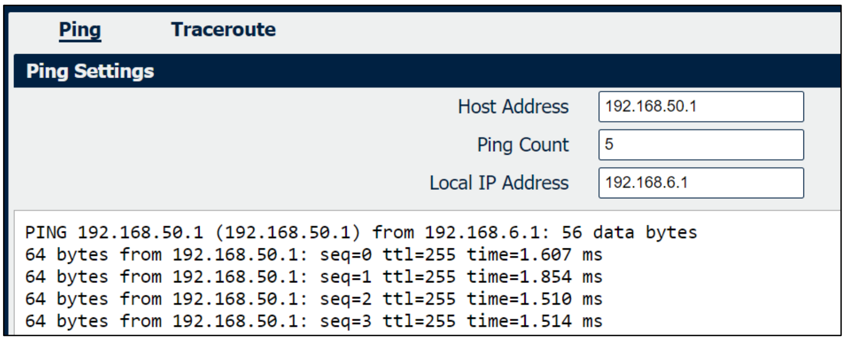
Ping from Cisco router to **AirGate 4G**, LAN to LAN communication is working correctly.



```
cisco2811#ping 192.168.6.1 source 192.168.50.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms
cisco2811#
```

Figure 199 – Cisco terminal

You must open the Web Interface of **AirGate 4G** and go to **Maintenance > Debug Tool > Ping** and Ping from **AirGate 4G** to Cisco router. LAN to LAN communication is working correctly.



Host Address 192.168.50.1

Ping Count 5

Local IP Address 192.168.6.1

```
PING 192.168.50.1 (192.168.50.1) from 192.168.6.1: 56 data bytes
64 bytes from 192.168.50.1: seq=0 ttl=255 time=1.607 ms
64 bytes from 192.168.50.1: seq=1 ttl=255 time=1.854 ms
64 bytes from 192.168.50.1: seq=2 ttl=255 time=1.510 ms
64 bytes from 192.168.50.1: seq=3 ttl=255 time=1.514 ms
```

Figure 200 – AirGate 4G test

Test successfully.

6.14 CELLULAR SETTING

This tutorial shows how to configure cellular settings.

6.14.1 TOPOLOGY

You can use the following topology:

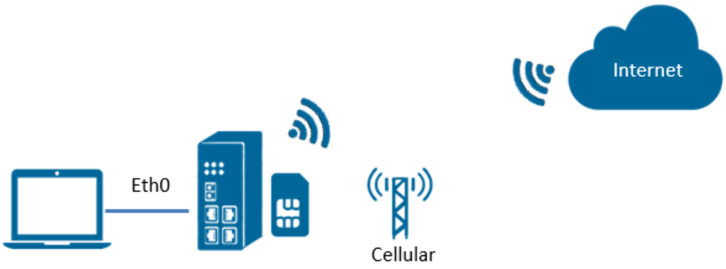
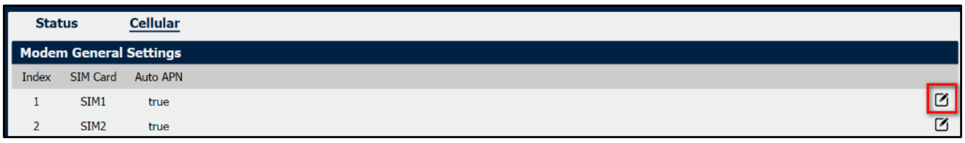


Figure 201 – Cellular connection topology

1. Specify WWAN1 as primary link and **AirGate 4G** pro access cellular network via SIM card (WWAN1).
2. ETH0 works as LAN interface and enable DHCP server, allocate IP to the end PC.

6.14.2 CELLULAR CONFIGURATION

You must open the Web Interface of **AirGate 4G** and go to **Link Management > Cellular > Cellular**. After that, just click on the SIM1 connection edit button:

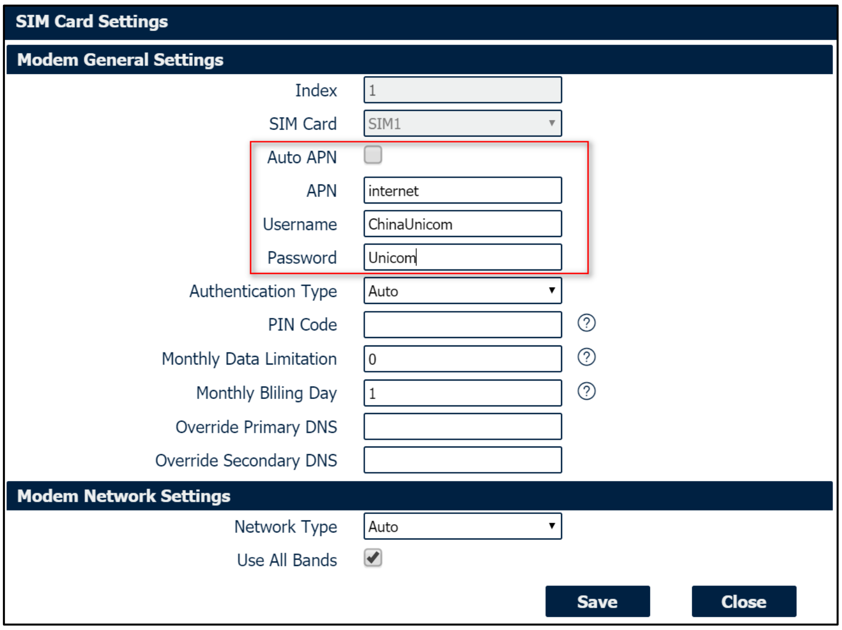


Modem General Settings

Index	SIM Card	Auto APN
1	SIM1	true
2	SIM2	true

Figure 202 – Cellular connection settings

Setup the APN, Username and Password of the SIM card, please also setup the PIN if the SIM work with the PIN code and left the other parameters as default.



SIM Card Settings

Modem General Settings

Index	1
SIM Card	SIM1
Auto APN	□
APN	internet
Username	ChinaUnicom
Password	Unicom
Authentication Type	Auto
PIN Code	
Monthly Data Limitation	0
Monthly Bliling Day	1
Override Primary DNS	
Override Secondary DNS	

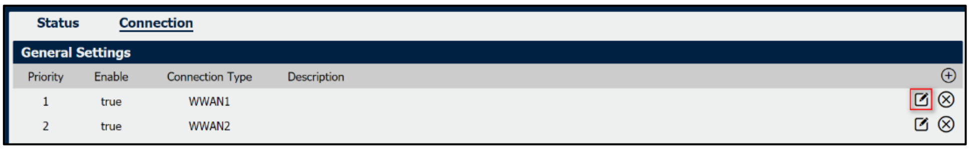
Modem Network Settings

Network Type	Auto
Use All Bands	☑

Figure 203 – SIM card settings

Click **Save** > **Apply**.

Go to Link **Management>Connection Manager>Connection**. Click the **Edit button** of WWAN1.

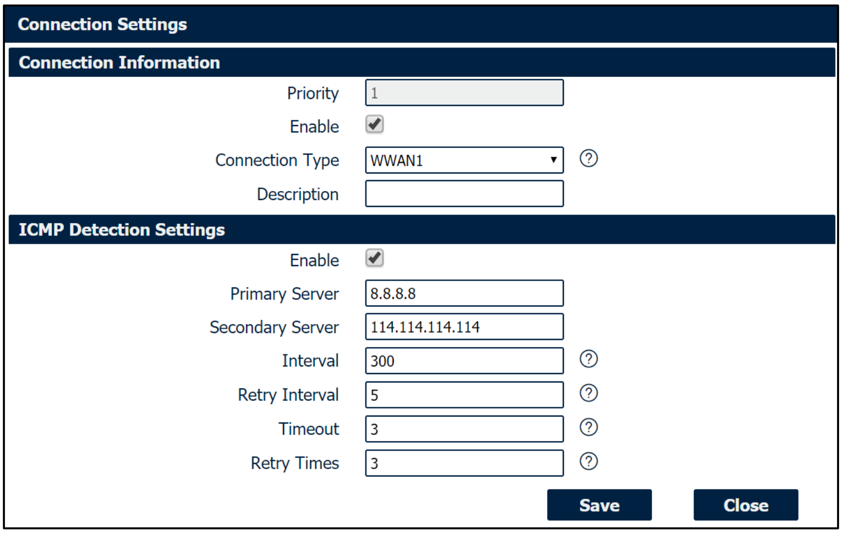


General Settings

Priority	Enable	Connection Type	Description
1	true	WWAN1	
2	true	WWAN2	

Figure 204 – WWAN1 connection

Setup the parameters of WWAN1 as below:



Connection Settings

Connection Information

Priority	1
Enable	☑
Connection Type	WWAN1
Description	

ICMP Detection Settings

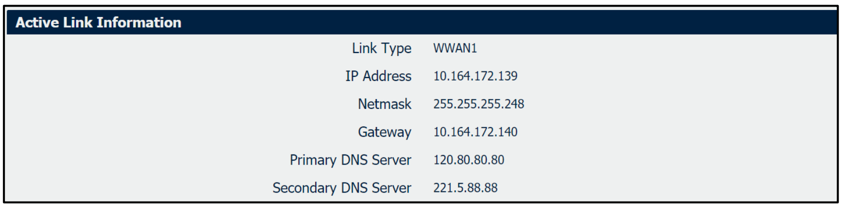
Enable	☑
Primary Server	8.8.8.8
Secondary Server	114.114.114.114
Interval	300
Retry Interval	5
Timeout	3
Retry Times	3

Figure 205 – IPsec status connection

Click **Save > Apply**.

6.14.3 TEST

Go to **Overview > Overview > Active Link Information**. The router had been got the IP information for ISP.

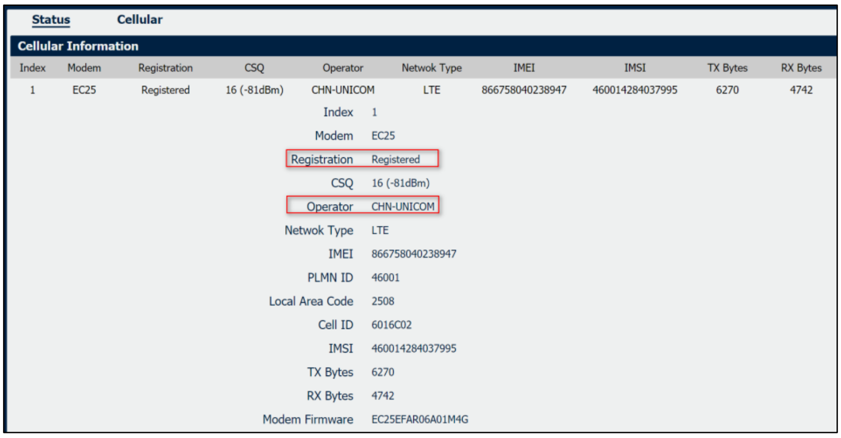


Active Link Information

Link Type	WWAN1
IP Address	10.164.172.139
Netmask	255.255.255.248
Gateway	10.164.172.140
Primary DNS Server	120.80.80.80
Secondary DNS Server	221.5.88.88

Figure 206 – IPsec status connection

Go to **Link Management > Cellular > Status** to check the registration information.



Cellular Information

Index	Modem	Registration	CSQ	Operator	Netwok Type	IMEI	IMSI	TX Bytes	RX Bytes
1	EC25	Registered	16 (-81dBm)	CHN-UNICOM	LTE	866758040238947	460014284037995	6270	4742

Index	1
Modem	EC25
Registration	Registered
CSQ	16 (-81dBm)
Operator	CHN-UNICOM
Netwok Type	LTE
IMEI	866758040238947
PLMN ID	46001
Local Area Code	2508
Cell ID	6016C02
IMSI	460014284037995
TX Bytes	6270
RX Bytes	4742
Modem Firmware	EC25EFAR06A01M4G

Figure 207 – Cellular status

6.15 ETHERNET SETTING

This tutorial shows how to configure Ethernet settings.

6.15.1 TOPOLOGY

You can use the following topology:

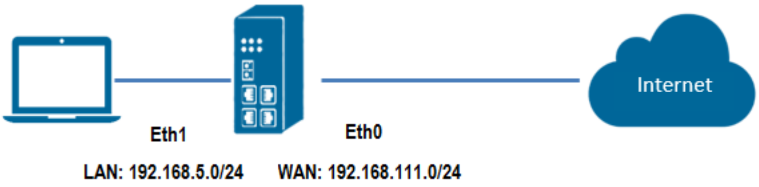


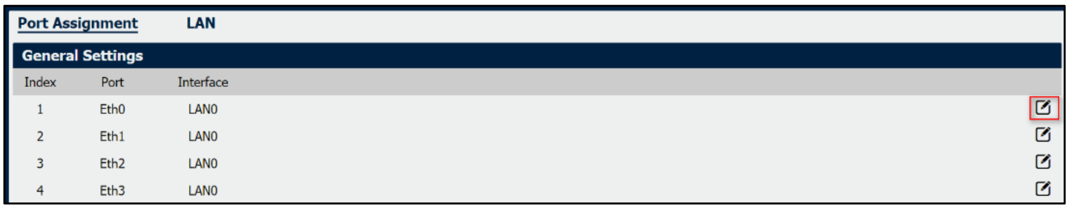
Figure 208 – Ethernet connection topology

1. Specify ETH0 port as WAN port and **AirGate 4G** communicate with Internet via WAN link.
2. ETH1 works as LAN interface and enable DHCP server, allocate IP to the end PC.

6.15.2 CONFIGURATION

6.15.2.1 ETHERNET CONFIGURATION

You must open the Web Interface of **AirGate 4G** and go to **Link Management>Ethernet>Port Assignment.** After that, just click the **Edit button** of Eth0.

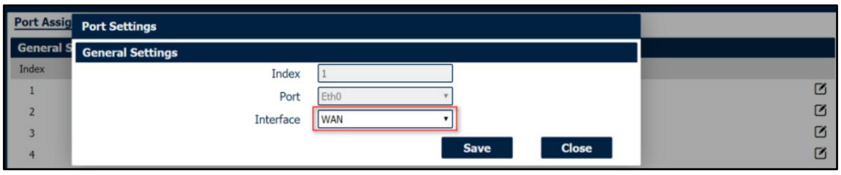


General Settings

Index	Port	Interface
1	Eth0	LAN0
2	Eth1	LAN0
3	Eth2	LAN0
4	Eth3	LAN0

Figure 209 – Eth0 port configuration

Assigned the port ETH0 as WAN, like below:



Port Settings

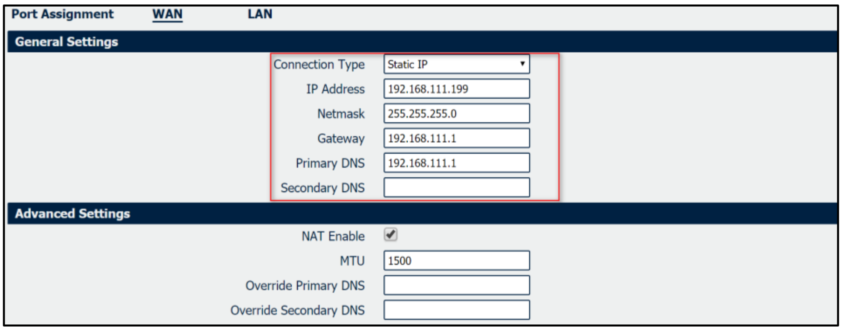
General Settings

Index: 1
Port: Eth0
Interface: WAN

Figure 210 – Eth0 interface

Click **Save > Apply**.

Go to **Industrial Interface > Ethernet > Status > WAN**, specify the Connection Type as "Static IP" and configure the IP information accordingly, setting like below:



General Settings

Connection Type: Static IP
IP Address: 192.168.111.199
Netmask: 255.255.255.0
Gateway: 192.168.111.1
Primary DNS: 192.168.111.1
Secondary DNS:

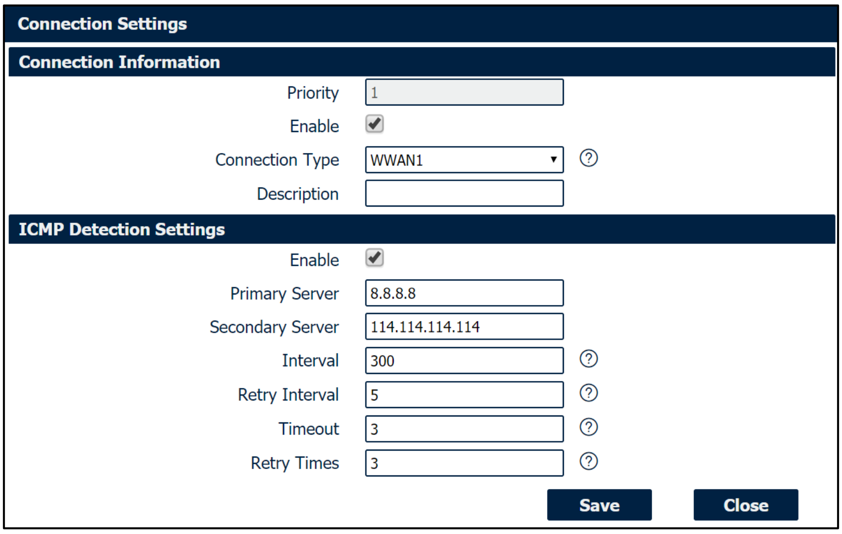
Advanced Settings

NAT Enable: ☑
MTU: 1500
Override Primary DNS:
Override Secondary DNS:

Figure 211 – WWAN1 connection

AirGate 4G also supports DHCP and PPPoE connection types. In this example, however, the static IP configuration is used.

Click **Save > Apply**.



Connection Settings

Connection Information

Priority	1
Enable	☑
Connection Type	WWAN1
Description	

ICMP Detection Settings

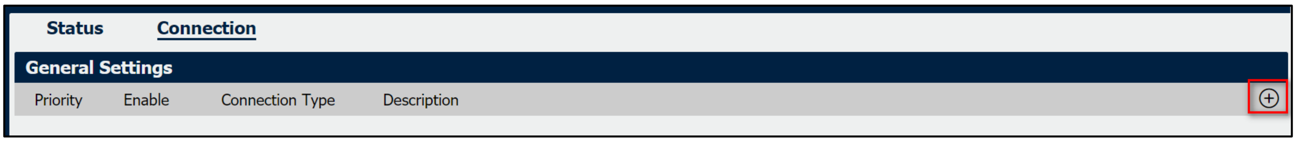
Enable	☑
Primary Server	8.8.8.8
Secondary Server	114.114.114.114
Interval	300
Retry Interval	5
Timeout	3
Retry Times	3

Figure 212 – Ethernet settings

Click **Save > Apply**.

6.15.2.2 PRIMARY LINK CONFIGURATION

You must open the Web Interface of **AirGate 4G** and go to **Link Management > Connection Manager > Connection**, delete the WWAN1 and WWAN2, then click **Save > Apply**. After that, add the "WAN" link as below picture:

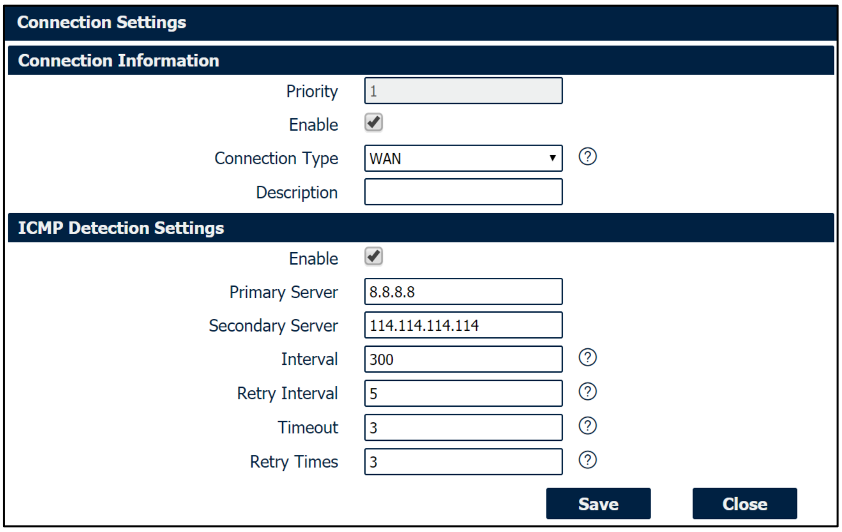


General Settings

Priority	Enable	Connection Type	Description

Figure 213 – Primary link settings

Configure the WAN parameters as below:



Connection Settings

Connection Information

Priority	1
Enable	☑
Connection Type	WAN
Description	

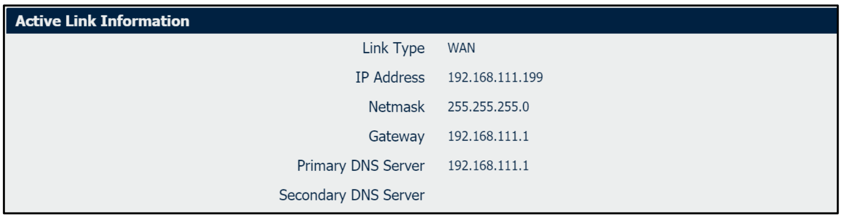
ICMP Detection Settings

Enable	☑
Primary Server	8.8.8.8
Secondary Server	114.114.114.114
Interval	300
Retry Interval	5
Timeout	3
Retry Times	3

Figure 214 – WAN parameters

6.15.3 TEST

You must open the Web Interface of **AirGate 4G** and go to **Overview > Status > Active Link Information**.

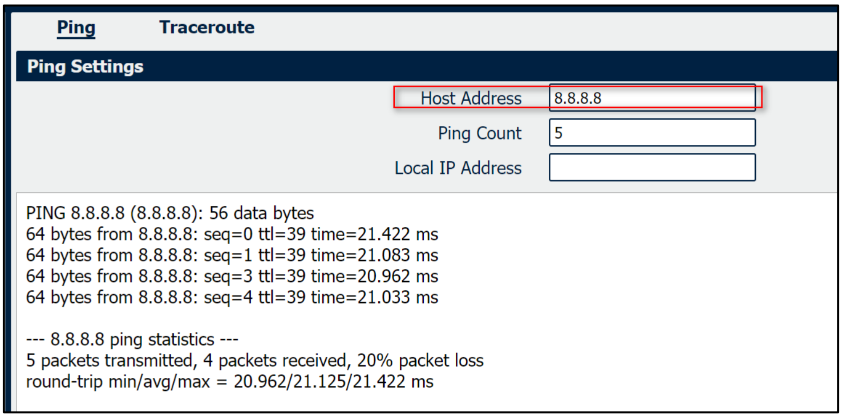


Active Link Information

Link Type	WAN
IP Address	192.168.111.199
Netmask	255.255.255.0
Gateway	192.168.111.1
Primary DNS Server	192.168.111.1
Secondary DNS Server	

Figure 215 – WAN status connection

After that, you must go to **Maintenance > Debug Tool > Ping.** Router can ping "8.8.8.8" successfully.



Ping Settings

Host Address: 8.8.8.8

Ping Count: 5

Local IP Address:

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=39 time=21.422 ms
64 bytes from 8.8.8.8: seq=1 ttl=39 time=21.083 ms
64 bytes from 8.8.8.8: seq=3 ttl=39 time=20.962 ms
64 bytes from 8.8.8.8: seq=4 ttl=39 time=21.033 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 4 packets received, 20% packet loss
round-trip min/avg/max = 20.962/21.125/21.422 ms
```

Figure 216 – Ethernet configuration test

6.16 DIGITAL INPUT SETTING

This tutorial shows how to configure the digital input.

6.16.1 TYPICAL APPLICATION DIAGRAM

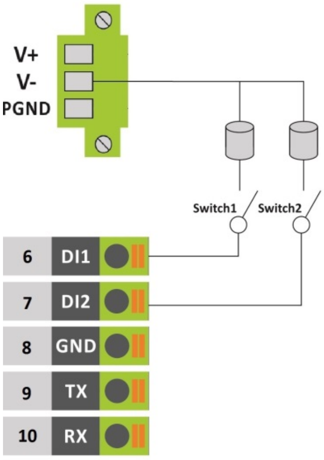
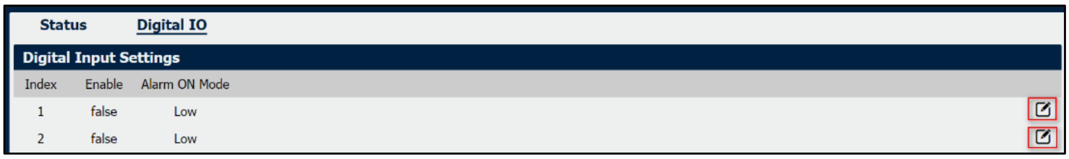


Figure 217 – Typical application diagram

6.16.2 DIGITAL INPUT CONFIGURATION

Go to **Industrial Interface > Digital IO > Digital IO > Digital Input Settings** and click the **Edit button** of DI1 and DI2.

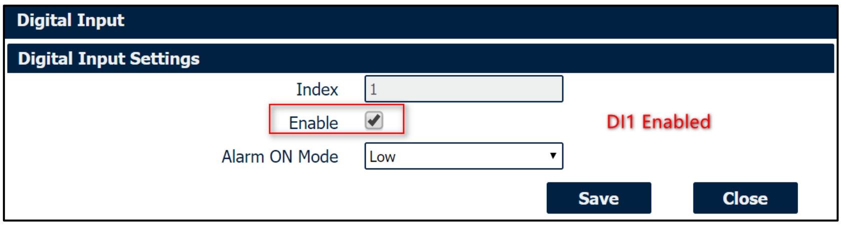


Digital Input Settings

Index	Enable	Alarm ON Mode
1	false	Low
2	false	Low

Figure 218 – Digital input settings

Enable DI1 and DI2, like below **Figure 219** and **Figure 220**:



Digital Input Settings

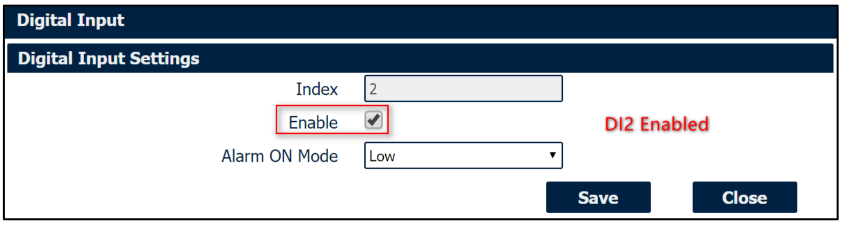
Index: 1

Enable: ☑

DI1 Enabled

Alarm ON Mode: Low

Figure 219 – DI1



Digital Input Settings

Index: 2

Enable: ☑

DI2 Enabled

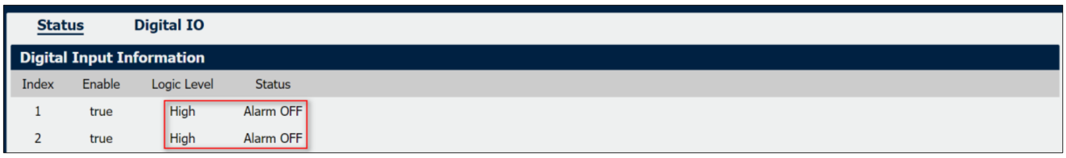
Alarm ON Mode: Low

Figure 220 – DI2

Click **Save > Apply**.

6.16.3 TEST

Go to **Industrial Interface > Digital IO > Status > Digital Input Information** to check the default DI1 and DI2 status like below:

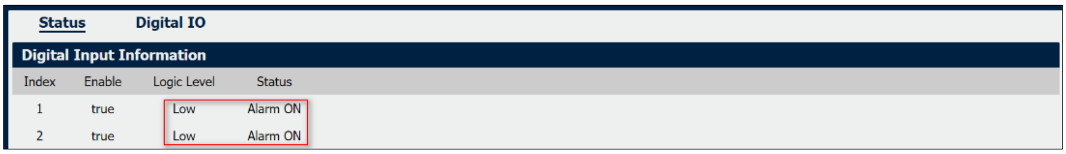


Digital Input Information

Index	Enable	Logic Level	Status
1	true	High	Alarm OFF
2	true	High	Alarm OFF

Figure 221 – Digital input information

Switch on (short to V-) for both DI1 and DI2, to check again the status of DI1 and DI2, like below:



Digital Input Information

Index	Enable	Logic Level	Status
1	true	Low	Alarm ON
2	true	Low	Alarm ON

Figure 222 – Logical level

- "Logic Level" changed from "High" to "Low";
- "Status" changed from "Alarm OFF" to "Alarm ON".

Test successfully.

6.17 DIGITAL OUTPUT SETTING

This tutorial shows how to configure the digital output.

6.17.1 TYPICAL APPLICATION DIAGRAM

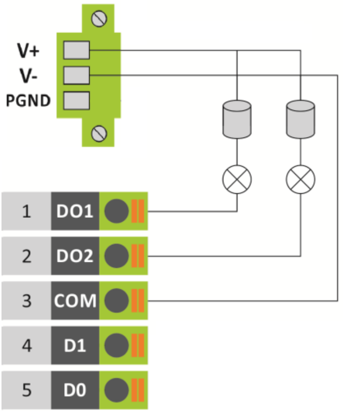
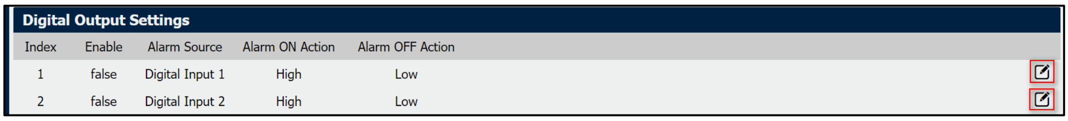


Figure 223 – Typical application diagram

6.17.2 DIGITAL OUTPUT CONFIGURATION

Go to **Industrial Interface > Digital IO > Digital IO > Digital Output Settings**. After that, click the **Edit button** of DO1 and DO2.

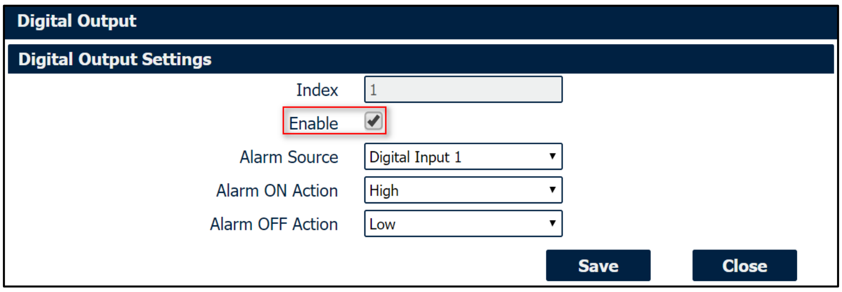


Digital Output Settings

Index	Enable	Alarm Source	Alarm ON Action	Alarm OFF Action
1	false	Digital Input 1	High	Low
2	false	Digital Input 2	High	Low

Figure 224 – Digital output settings

Enable DO1 and DO2, like below:

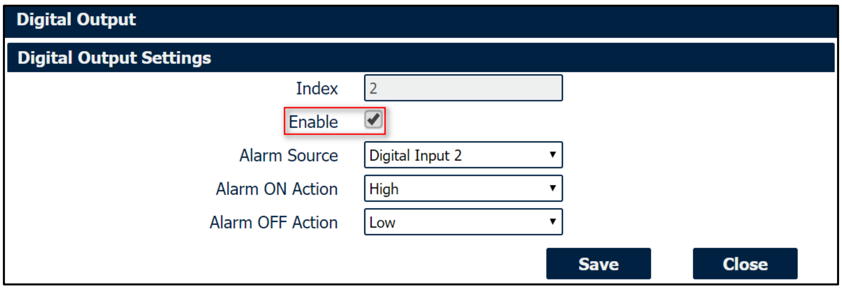


Digital Output

Digital Output Settings

Index	1
Enable	☑
Alarm Source	Digital Input 1
Alarm ON Action	High
Alarm OFF Action	Low

Figure 225 – DI1



Digital Output

Digital Output Settings

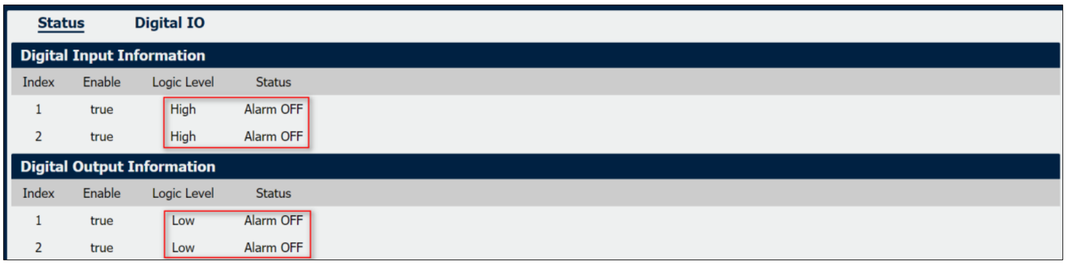
Index	2
Enable	☑
Alarm Source	Digital Input 2
Alarm ON Action	High
Alarm OFF Action	Low

Figure 226 – DI2

Click **Save > Apply**.

6.17.3 TEST

Go to **Industrial Interface > Digital IO > Status**, to check the default DI1, DI2, DO1 and DO2 status like below:



Status Digital IO

Digital Input Information

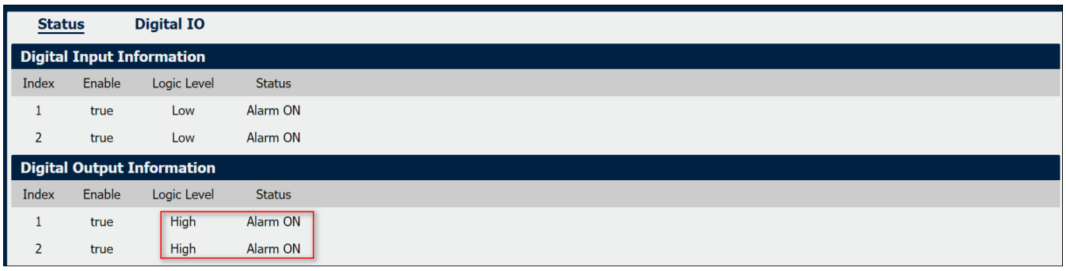
Index	Enable	Logic Level	Status
1	true	High	Alarm OFF
2	true	High	Alarm OFF

Digital Output Information

Index	Enable	Logic Level	Status
1	true	Low	Alarm OFF
2	true	Low	Alarm OFF

Figure 227 – Digital and output status

Switch on (short to V-) for both DI1 and DI2, DO1 and DO2 will receive the trigger signal from D11 and DI2, the LED will become ON and the DO status like below:



Status Digital IO

Digital Input Information

Index	Enable	Logic Level	Status
1	true	Low	Alarm ON
2	true	Low	Alarm ON

Digital Output Information

Index	Enable	Logic Level	Status
1	true	High	Alarm ON
2	true	High	Alarm ON

Figure 228 – Digital output test

- "Logic Level" changed from "High" to "Low";
- "Status" changed from "Alarm OFF" to "Alarm ON".

Test successfully.

6.18 SMS CONTROL

This tutorial contains information about configuring and using the SMS control function.

6.18.1 TOPOLOGY

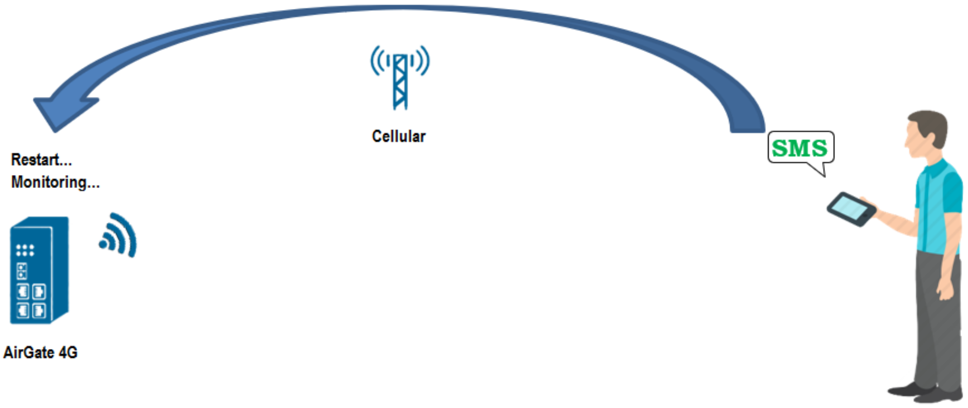


Figure 229 – SMS

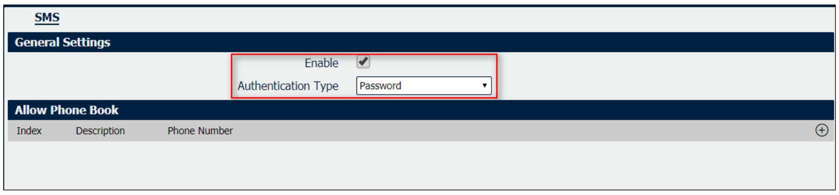
1. **AirGate 4G** router dial up successfully with a SIM card.
2. Engineer sends SMS to the router with Special SMS Command to control **AirGate 4G** router restart or configure **AirGate 4G** router.

Special SMS Command means the router CLI Command. The engineer will send the SMS with CLI Command to control or monitoring the router.

6.18.2 CONFIGURATION

6.18.2.1 AIRGATE 4G CONFIGURATION

Go to **Applications > SMS**, SMS control function is enable by default settings.



SMS

General Settings

Enable ☑

Authentication Type: Password

Allow Phone Book

Index	Description	Phone Number

Figure 230 – SMS configuration

It is also necessary to define the type of authentication ("Password", which will allow sending an SMS command with user and password, or "None") and register a phone number, which must be added to the phone book.

AirGate 4G only receive the SMS message from the special phone number on the phone book.

6.18.2.2 SMS COMMAND

AUTHENTICATION TYPE: PASSWORD

The following commands are allowed:

1. **admin$admin$enable$enable$version** // send SMS to check the firmware version

The first "admin" means the router username. The second "admin" means the router password. "enable" means to send the CLI Command of "enable mode". "version" is the CLI command under enable mode.

2. **admin$admin$config$config$set syslog info** // send SMS to set router syslog to info level

The first "admin" means the router username. The second "admin" means the router password. "config" means to send the CLI Command of "config mode". "set syslog level info" is the CLI command under config mode.

You also can send SMS with **multiple** CLI Commands, like below:

3. **admin$admin$enable$enable$version;show active_link** // send SMS to check firmware version and link information together
4. **admin$admin$config$config$set syslog location ram;set syslog level info** // send SMS to set syslog location and syslog level

AUTHENTICATION TYPE: NONE

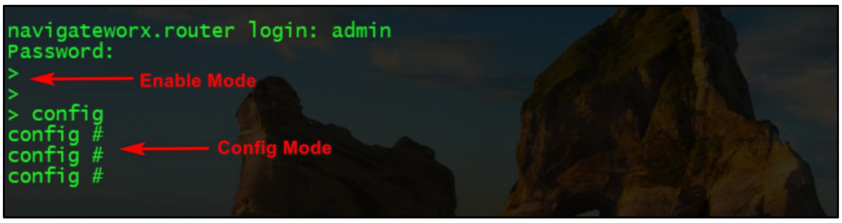
The following commands are allowed:

1. enable$version
2. config$set syslog level info
3. enable$version;show active_link
4. config$set syslog location ram;set syslog level info

6.18.3 CLI COMMAND

Telnet to the router to check the CLI command under "enable mode" or "config mode".
When telnet to the router successfully, it pop up character ">", means that the router under "enable mode".

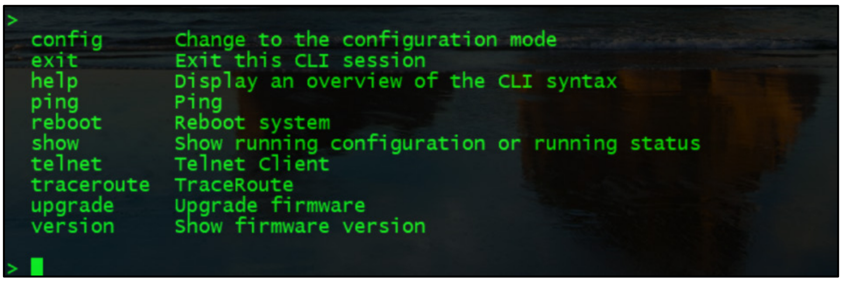
When enter CLI command "config", then the router will go into "config mode".



```
navigateworx.router login: admin
Password:
>
>
> config
config #
config #
config #
```

Figure 231 – Telnet Terminal

Enter the "?" or keyboard "Tab", then we can see what CLI command could be set in the next. Like **Figure 231**:

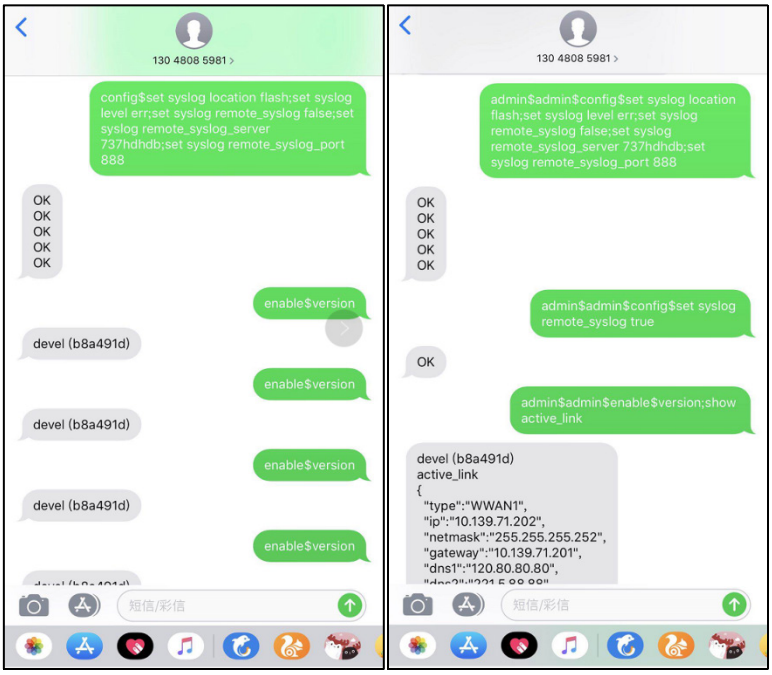


```
>
  config       Change to the configuration mode
  exit         Exit this CLI session
  help         Display an overview of the CLI syntax
  ping         Ping
  reboot       Reboot system
  show         Show running configuration or running status
  telnet       Telnet Client
  traceroute   TraceRoute
  upgrade      Upgrade firmware
  version      Show firmware version

> █
```

Figure 231 – Auto-complete

6.18.4 TEST

Figure 232 presents results of a test for reference:



130 4808 5981 >

config$set syslog location flash;set syslog level err;set syslog remote_syslog false;set syslog remote_syslog_server 737hdhdb;set syslog remote_syslog_port 888

OK
OK
OK
OK
OK

enable$version

devel (b8a491d)

enable$version

devel (b8a491d)

enable$version

devel (b8a491d)

enable$version

130 4808 5981 >

admin$admin$config$set syslog location flash;set syslog level err;set syslog remote_syslog false;set syslog remote_syslog_server 737hdhdb;set syslog remote_syslog_port 888

OK
OK
OK
OK
OK

admin$admin$config$set syslog remote_syslog true

OK

admin$admin$enable$version;show active_link

```
devel (b8a491d)
active_link
{
  "type":"WWAN1",
  "ip":"10.139.71.202",
  "netmask":"255.255.255.252",
  "gateway":"10.139.71.201",
  "dns1":"120.80.80.80",
  "dns2":"221.5.88.88"
```

Figure 232 – SMS

6.19 SMS EVENT (DIDO)

This tutorial contains information about configuring and using the SMS control function.

6.19.1 TOPOLOGY

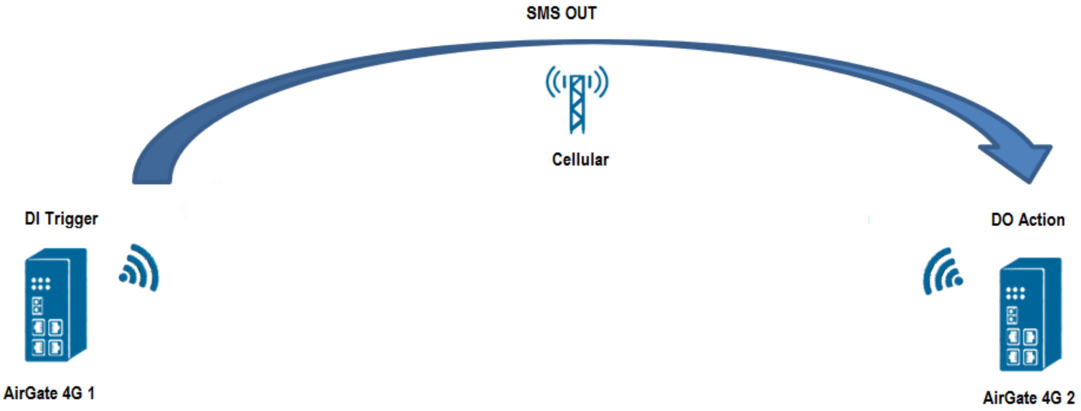


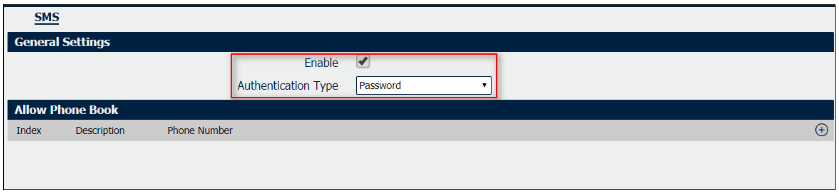
Figure 233 – SMS

1. **AirGate 4G** 1 dial up successfully with SIM card and Phone No:13265900210.
2. **AirGate 4G** 2 dial up successfully with SIM card and Phone No:13265143432.
3. Trigger the DI status changed on Router 1 to make it send out the Pre-set special SMS command to Router 2.
4. Router 2 receives the special SMS command and controls DO on or off.

6.19.2 CONFIGURATION

6.19.2.1 AIRGATE 4G 1 CONFIGURATION

To configure router 1, you must open the Web Interface of **AirGate 4G** and go to **Applications > SMS** and enable SMS function.



SMS

General Settings

Enable ☑

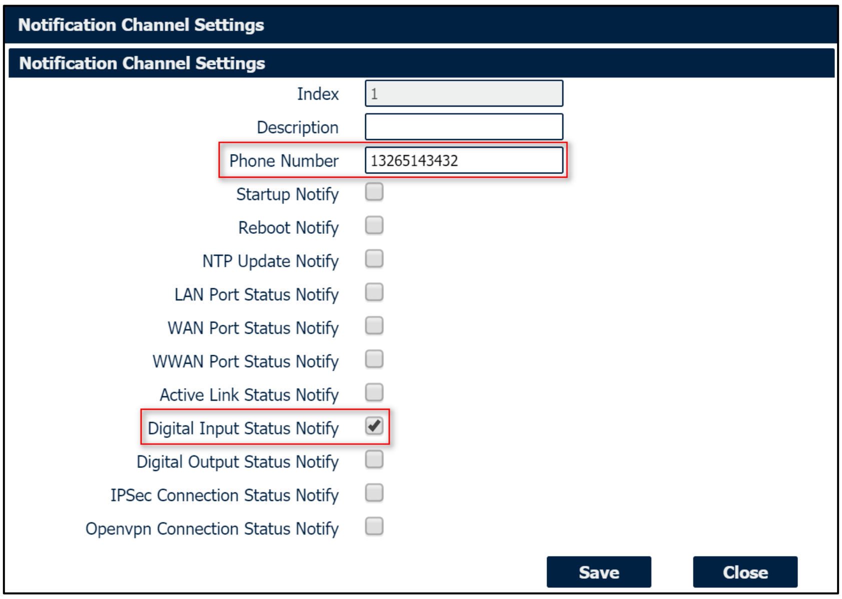
Authentication Type: Password

Allow Phone Book

Index	Description	Phone Number

Figure 234 – SMS configuration

After that, go to **Applications** > **SMS** > **Notification,** specify the phone number of router 2 to receive the special SMS content from router 1 and enable DI status notify, like below:



Notification Channel Settings

Notification Channel Settings

Index: 1

Description:

Phone Number: 13265143432

Startup Notify ☐

Reboot Notify ☐

NTP Update Notify ☐

LAN Port Status Notify ☐

WAN Port Status Notify ☐

WWAN Port Status Notify ☐

Active Link Status Notify ☐

Digital Input Status Notify ☑

Digital Output Status Notify ☐

IPSec Connection Status Notify ☐

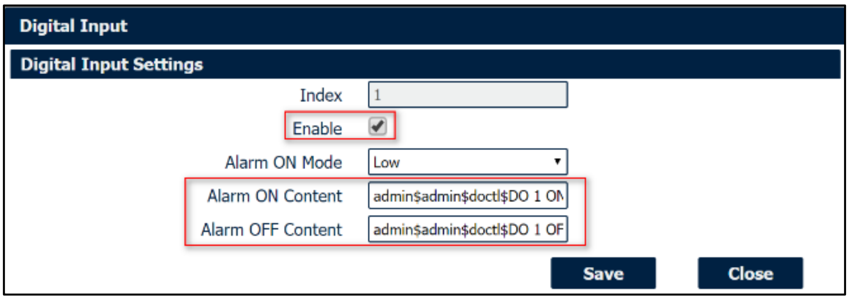
Openvpn Connection Status Notify ☐

Figure 235 – Digital input status notify

Digital Input Status Notify parameter content is defined according to **Alarm ON/OFF Content** parameter. If **Alarm ON/OFF Content** is empty, then router will send out default content, like "Digital input 1/2 alarm on/off".

Click **Save** > **Apply**.

Go to **Industrial Interface > Digital IO > Digital Input Settings**, to specify the special content of Alarm ON and OFF, like below:



Digital Input

Digital Input Settings

Index: 1
Enable: ☑
Alarm ON Mode: Low
Alarm ON Content: admin$admin$doctl$DO 1 ON
Alarm OFF Content: admin$admin$doctl$DO 1 OF

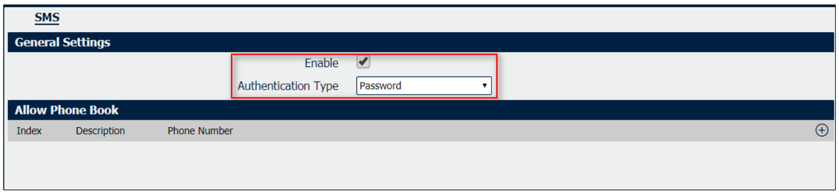
Figure 236 – Alarms content

The special SMS content to control DO on and off like below:

- **DO ON:** admin$admin$doctl$DO 1/2 ON
- **DO OFF:** admin$admin$doctl$DO 1/2 OFF
- **Format:** <username>$<password>$<control command>$<DO> <DO_index> <ON/OFF>

6.19.2.2 AIRGATE 4G 2 CONFIGURATION

To configure router 1, you must open the Web Interface of **AirGate 4G** and go to **Applications > SMS.** SMS control function is already enabled.



SMS

General Settings

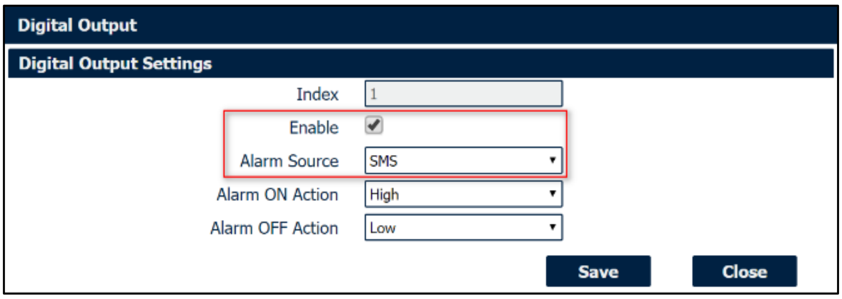
Enable: ☑
Authentication Type: Password

Allow Phone Book

Index	Description	Phone Number

Figure 237 – Router 2: SMS sending

After that, go to **Industrial Interface > Digital IO > Digital Output Settings**, to specify the Alarm Source from SMS, like below:



Digital Output

Digital Output Settings

Index: 1
Enable: ☑
Alarm Source: SMS
Alarm ON Action: High
Alarm OFF Action: Low

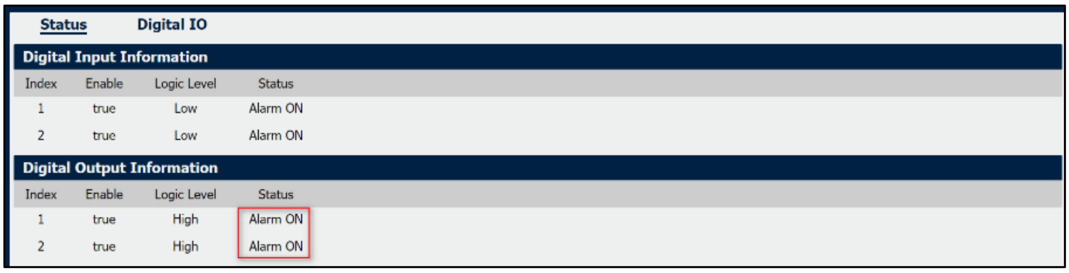
Figure 238 – Digital output settings

Click **Save > Apply**.

6.19.3 TEST

DI activated, send the special SMS to router 2. DO of Router 2 will be ON or OFF after received the special SMS from router 1.

6.19.3.1 TRIGGER ON STATUS



Digital Input Information

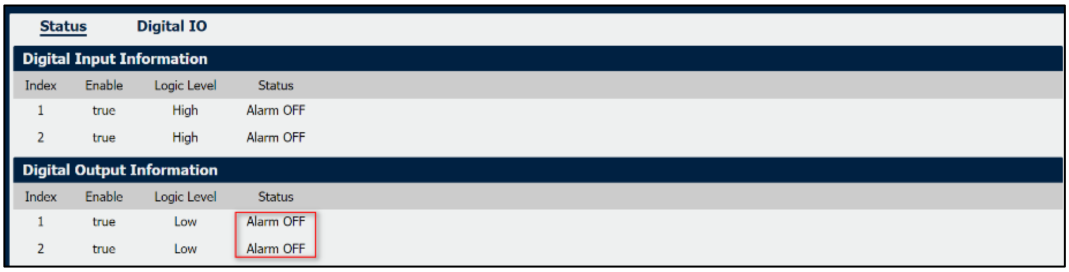
Index	Enable	Logic Level	Status
1	true	Low	Alarm ON
2	true	Low	Alarm ON

Digital Output Information

Index	Enable	Logic Level	Status
1	true	High	Alarm ON
2	true	High	Alarm ON

Figure 239 – On status

6.19.3.2 TRIGGER OFF STATUS



Digital Input Information

Index	Enable	Logic Level	Status
1	true	High	Alarm OFF
2	true	High	Alarm OFF

Digital Output Information

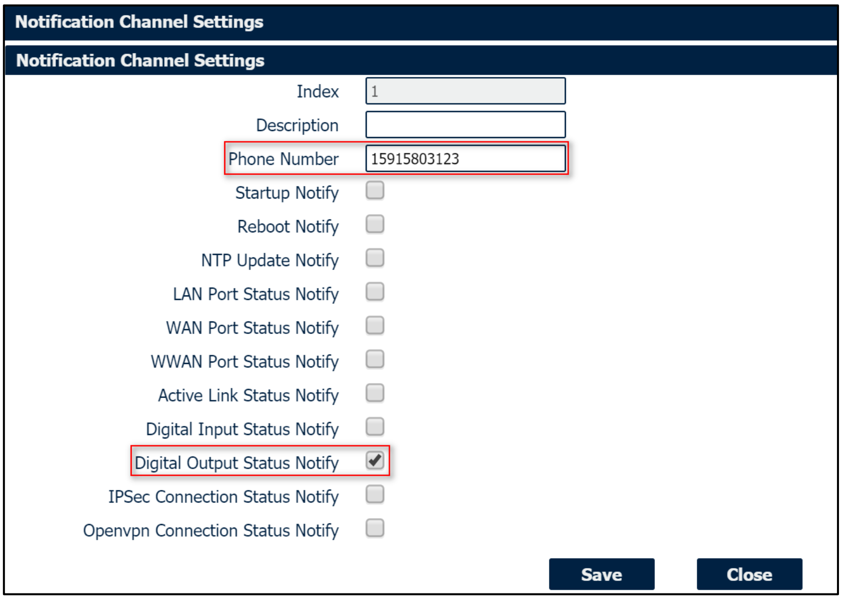
Index	Enable	Logic Level	Status
1	true	Low	Alarm OFF
2	true	Low	Alarm OFF

Figure 240 – Off status

Test successfully.

6.19.4 DO STATUS TO MOBILE PHONE

DO status on router 2 could be send to the special phone number, configuration like below. Go to **Applications > SMS > Notification**, specify the phone number to receive the DO status and enable DO status notify.

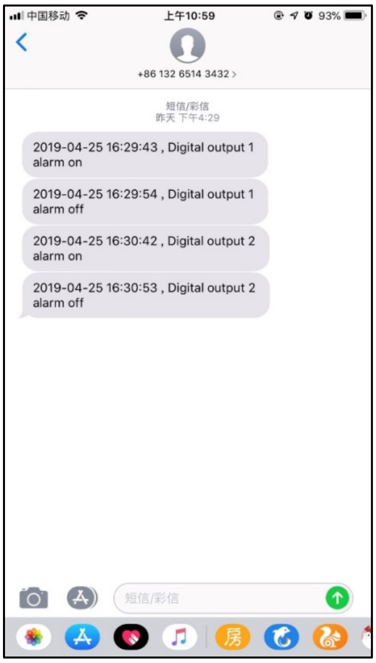


Index	1
Description	
Phone Number	15915803123
Startup Notify	□
Reboot Notify	□
NTP Update Notify	□
LAN Port Status Notify	□
WAN Port Status Notify	□
WWAN Port Status Notify	□
Active Link Status Notify	□
Digital Input Status Notify	□
Digital Output Status Notify	☑
IPSec Connection Status Notify	□
Openvpn Connection Status Notify	□

Figure 241 – Digital output configuration

Click **Save > Apply**.

DO status was sent to the mobile phone.



2019-04-25 16:29:43 , Digital output 1 alarm on

2019-04-25 16:29:54 , Digital output 1 alarm off

2019-04-25 16:30:42 , Digital output 2 alarm on

2019-04-25 16:30:53 , Digital output 2 alarm off

Figure 242 – SMS

7 TROUBLESHOOTING

NO SIGNAL

Phenomenon: AirGate 4G modem status shows no signal.

Possible Reason:

- Antenna installation is wrong.
- Modem failure.

Solution:

- Check the operation of the LTE antenna or replace it with a new one.
- In the LINK MANAGEMENT section, confirm that modem has been detected correctly.

CANNOT DETECT SIM CARD

Phenomenon: AirGate 4G cannot detect SIM card even though the cellular connection has no connection problems.

Possible Reason:

- SIM card damage.
- SIM card with poor contact.

Solution:

- Replace SIM card.
- Reinstall SIM card.

SINAL FRACO

Phenomenon: No signal or weak signal device.

Possible Reason:

- Antenna installation is wrong.
- Area signal weak.

Solution:

- Check and reconnect the antenna.
- Contact the telecommunications company to confirm the existence of signal problems.
- Replace the actual antenna with a more powerful antenna.

IPSec VPN ESTABLISHED, BUT LAN TO LAN CANNOT COMMUNICATE

Phenomenon: IPSec VPN established, but LAN to LAN cannot communicate.

Possible Reason:

- Both networks do not match the selected traffic.
- IPSec second phase (ESP) settings do not match.

Solution:

- Check both networks settings.
- Check IPSec second phase (ESP) setting.

FORGET ROUTER PASSWORD

Phenomenon: User forgot device login password.

Possible Reason:

User has changed the password.

Solution:

After initializing the router, press the RESET button for 3 to 10 seconds. The router will need to be rebooted manually and will return to factory default settings (username/password: **admin**/**admin**).

8 COMMAND LINE INTERFACE

Command-line interface (CLI) is a software interface that provides another configurable way to set parameters on the router. You can use Telnet or SSH connect the router for CLI input.

8.1 AIRGATE 4G CLI ACCESS

```
login novusautomation.router: admin
Password: admin
>
```

8.2 CLI REFERENCE COMMANDS

```
>?
    config         Change to the configuration mode
    exit        Exit this CLI session
    help        Display an overview of the CLI syntax
    ping        Ping
    reboot      Reboot system
    show        Show running configuration or running status
    telnet      Telnet Client
    traceroute  Traceroute
    upgrade     Upgrade firmware
    version     Show firmware version
```

Example:

```
> version
1.0.0 (1017.4)

> show wifi
wifi
{
 "status":"Ready",
 "mac":"a8: 3f: a1: e0: ab: 81",
 "ssid":"NR500-WAN",
 "channel":"6",
 "width":"40 MHz",
 "txpower":"20,00 dBm"
}

> ping www.baidu.com
PING www.baidu.com (14.215.177.38): 56 data bytes
64 bytes from 14.215.177.38: seq=0 ttl=54 time=10.826 ms
64 bytes from 14.215.177.38: seq=1 ttl=54 time=10.284 ms
64 bytes from 14.215.177.38: seq=2 ttl=54 time=10.073 ms
64 bytes from 14.215.177.38: seq=3 ttl=54 time=10.031 ms
64 bytes from 14.215.177.38: seq=4 ttl=54 time=10.347 ms

--- www.baidu.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 10.031/10.312/10.826 ms
>
```

8.3 HOW TO CONFIGURE THE CLI

CONTEXT SENSITIVE HELP

[?] - Display context sensitive help. This is either a list of possible command completions with summaries, or the full syntax of the current command. A subsequent repeat of this key, when a command has been resolved, will display a detailed reference.

AUTO-COMPLETION

The following keys both perform auto-completion for the current command line. If the command prefix is not unique then the bell will ring and a subsequent repeat of the key will display possible completions.

[enter] Auto-completes, syntax-checks then executes a command. If there is a syntax error then offending part of the command line will be highlighted and explained.

[space] Auto-completes, or if the command is already resolved inserts a space.

MOVEMENT KEYS

[CTRL-A] Move to the start of the line

[CTRL-E] Move to the end of the line.

[up] Move to the previous command line held in history.

[down] Move to the next command line held in history.

[left] Move the insertion point left one character.

[right] Move the insertion point right one character.

DELETION KEYS

[CTRL-C] Delete and abort the current line

[CTRL-D] Delete the character to the right on the insertion point.

[CTRL-K] Delete all the characters to the right of the insertion point.

[CTRL-U] Delete the whole line.

[backspace] Delete the character to the left of the insertion point.

ESCAPE SEQUENCES

!! Substitute the last command line.

!N Substitute the Nth command line (absolute as per 'history' command).

!-N Substitute the command line entered N lines before (relative).

9 TECHNICAL SPECIFICATIONS

CHARACTERISTICS	AIRGATE 4G
Cellular Interface	Frequency bands: • **4G LTE:** LTE FDD: 2100 (B1) / 1900 (B2) / 1800 (B3) / 1700 (B4) / 850 (B5) / 2600 (B7) / 900 (B8) / 700 (B28) MHz LTE TDD: 2300 (B40) MHz • **3G UMTS**: 2100 (B1) / 1900 (B2) / 850 (B5) / 900 (B8) MHz • **2G GSM**: 1900 (B2) / 1800 (B3) / 850 (B5) / 900 (B8) MHz
	Data transfer rate: • **4G LTE**: LTE FDD: Max 150 Mbps (DL) / Max 50 Mbps (UL) LTE TDD: Max 130 Mbps (DL) / Max 30 Mbps (UL) • **3G UMTS**: DC-HSDPA: Max 42 Mbps (DL) HSUPA: Max 5.76 Mbps (UL) WCDMA: Max 384 Kbps (DL) / Max 384 Kbps (UL) • **2G GSM**: EDGE: Max 296 Kbps (DL) / Max 236.8 Kbps (UL) GPRS: Max 107 Kbps (DL) / Max 85.6 Kbps (UL)
	2 x SMA female antenna connectors.
	2 x SIM (3.0 V and 1.8 V).
Wi-Fi Interface (Optional)	• Standards: 802.11 b/g/n, 300 Mbps; • 2 x RP-SMA male antenna connector; • Support Wi-Fi Access Point and Client modes; • Security: WEP, WPA and WPA2 encryption; • Encryption: TKIP and CCMP.
Ethernet Interface	• Standards: IEEE 802.3, IEEE 802.3u; • 2 x ports 10/100 Mbps, RJ45 connector; • 1 x WAN interface (conFigureble on Web GUI interface); • 1.5KV magnetic isolation protection.
Serial Interface	• 1 x RS232 (3 pin): TX, RX, GND; • 1 x RS485 (2 pin): D1, D0; • Baud Rate: 300 bps to 115.200 bps; • 15 KV ESD protection.
Digital Input and Digital Output	• 2 x Digital Inputs; • 2 x Digital Outputs; • Isolation: 3 KVDC or 2 KVrms; • Absolute maximum VDC: 36 VCC; • Absolute maximum ADC: 100 mA.
Wi-Fi Antenna	Wi-Fi Magnet Antenna, 3 Meters Long, 2.412-2.483 GHz, 7 dBi, Φ 29×220 mm.
Cellular Antenna	4G / 3G / 2G Magnet Antenna, 3 Meters Long, 698-960 / 1710-2700 MHz, 2.5 dBi, Φ 29×112 mm.
LED	• 1 x SYS; • 1 x NET; • 1 x USR; • 3 x RSSI.
Software	• Network protocols: TCP, UDP, DHCP, ICMP, PPPoE, HTTP, HTTPS, DNS, VRRP, NTP; • VPN: IPSec, GRE, OpenVPN, DMVPN; • Policy: RIPv1 / RIPv2 / OSPF / BGP (optional); • Firewall & Filter: Port forwarding, DMZ, anti-DoS, ACL; • Serial Port: TCP, UDP; • Management: Web Interface.
Power Supply	• Connector: 3-pin 3.5 mm female socket with lock; • Input voltage range: 9 to 48 VDC; • Power consumption: o Idle: 100 mA @ 12 V;

	○ Data Link: 400 mA (peak) @ 12 V.
Dimension	106 mm x 106 mm x 40 mm (excluding antenna).
Mounting	DIN rail mounting.
Environmental	• Operation temperature: -40 to 60 °C (-40 to 140 °F); • Storage temperature: -40 a 85 °C (-40 to 185 °F); • Operation humidity: 5 to 95 % non-condensing.
Housing	Metal. 300 g.
Protection	IP30
Electromagnetic Compatibility	• **EMI**: EN 55032:2012 Class B • **EMS**: ○ IEC 61000-4-2 ESD: Level 4 ○ IEC 61000-4-3 RS: Level 3 ○ IEC 61000-4-4 EFT: Level 3 ○ IEC 61000-4-5 Surge: Level 3 ○ IEC 61000-4-6 CS: Level 3
Certifications	CE, Anatel (07661-19-12560), RoHS.

Table 10 – Technical Specifications

RoHS

NOVUS Automation declares and certifies that all of their products are designed and fabricated in compliance with the requirements of Directive 2011/65/EU (EU RoHS 2) of The European Parliament and of the Council of the 8th of June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (EEE) and the amendment (EU) 2015/863/EU.

CE Mark

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

ANATEL

This device is homologated by ANATEL, in accordance with the procedures regulated by Resolution 242/2000, and meets the technical requirements applied.
This equipment is not subject to the protection from harmful interference and may not cause interference with duly authorized systems.
For more information, see the ANATEL website www.anatel.gov.br.

NORMA CISPR 22

In a domestic environment, this product may cause interference, which may require that the user take appropriate measures to minimize the interference.

10 WARRANTY

Warranty conditions are available on our website www.novusautomation.com/warranty.