Modbus Cellular Gateway

IOG700AM-0TCR1 / IOG700AM-0PCR1

User Manual

Modbus Cellular Gateway

Modbus Cellular Gateway

Modbus Cellular Gateway

Modbus Cellular Gateway

1.1 Introduction

Congratulations on your purchase of this outstanding product: Modbus Cellular Gateway. For M2M (Machine-to-Machine) applications, AMIT Modbus Cellular Gateway is absolutely the right choice. With built-in world-class 3G HSPA+ or 4G LTE module(*[1]), you just need to insert SIM card from local mobile carrier to get to Internet. The redundant SIM design provides a more reliable WAN connection for critical applications. By VPN tunneling technology, remote sites easily become a part of Intranet, and all data are transmitted in a secure (256-bit AES encryption) link.

The IOG700 series product is loaded with luxuriant security features including VPN, firewall, NAT, port forwarding, DHCP server and many other powerful features for complex and demanding business and M2M (Machine-to-Machine) applications. The redundancy design in fallback 9-48 VDC power terminal and dual SIM cards make the device as a back-up in power, network connection and data transmission without lost.

Main Features:

- Provide various and configurable WAN connection.
- Support dual SIMs for the redundant wireless WAN connection.
- Provide one Ethernet port for comprehensive LAN connection.
- Provide one RS232/RS485 serial port for controlling legacy serial device, or Modbus devices.
- Digital I/O ports for integrating sensors or alarm devices.
- Feature with VPN and NAT firewall to have powerful security.
- Support the robust remote or local management to monitor network.
- Designed by solid and easy-to-mount metal body for business and M2M environment to work with a variety M2M (Machine-to-Machine) applications.

Before you install and use this product, please read this manual in detail for fully exploiting the functions of this product.

---

1 The specification of embedded module depends on respective model. IOG700AM-0PCR1 is with an embedded 3G HSPA+ module. IOG700AM-0TCR1 is with an embedded 4G LTE module.

Modbus Cellular Gateway

1.2 Contents List

1.2.1 Package Contents
#Standard Package

Items	Description	Contents	Quantity
1	IOG700AM-0TCR1 (or IOG700AM-0PCR1) Modbus Cellular Gateway		1pcs
2	Cellular Antenna		2pcs
3	Power Adapter (DC 12V/1A) $(*^2)$		1pcs
4	RJ45 Cable		1pcs
5	Console Cable		1pcs
6	CD (Manual)		1pcs
7	4 Pin Terminal Block		1pcs
8	Mounting Bracket		2pcs
9	DIN-Rail Bracket		1pcs

---

2 The maximum power consumption of IOG700AM-0TCR1 is 7W.

Modbus Cellular Gateway

1.3 Hardware Configuration

➢ Front View

LED Indicators

Reset Button

3G / 4G Antenna

**Auto MDI/MDIX RJ45 Ports
1x FE LAN to connect local devices**
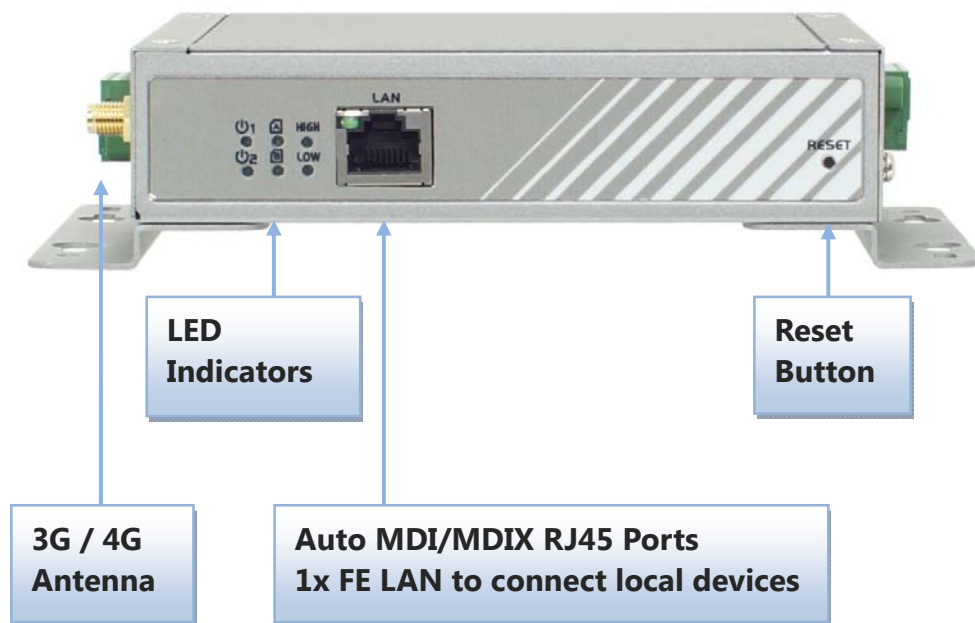
※Reset Button
The RESET button provides user with a quick and easy way to resort the default setting. Press the RESET button continuously for 6 seconds, and then release it. The device will restore to factory default settings.

Modbus Cellular Gateway

➢ Bottom View

SIM A Slot

SIM B Slot

➢ Left View

3G/4G (Aux) Antenna

3G/4G (Main) Antenna

Power Terminal Block
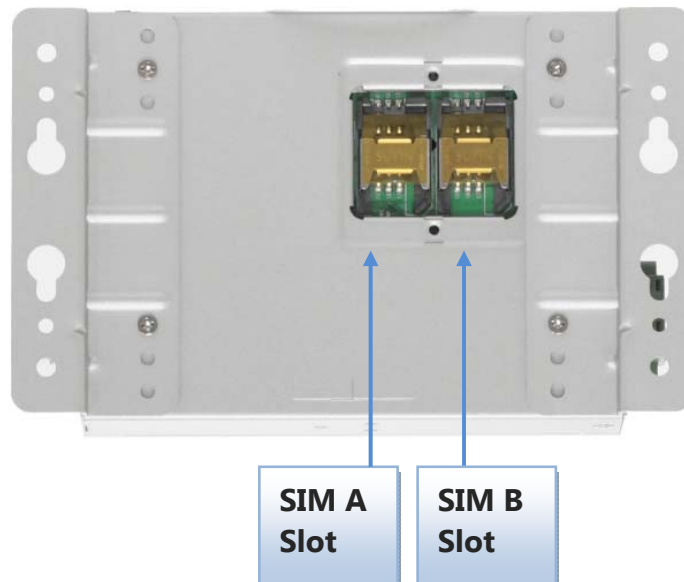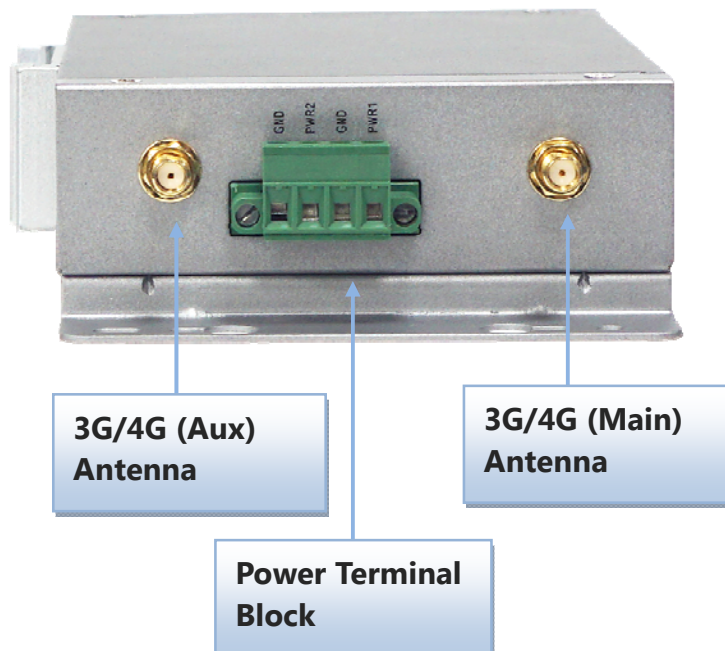
Modbus Cellular Gateway

➢ Right View

| Serial Port | MicroSD Slot | DI/DO Terminal Block |
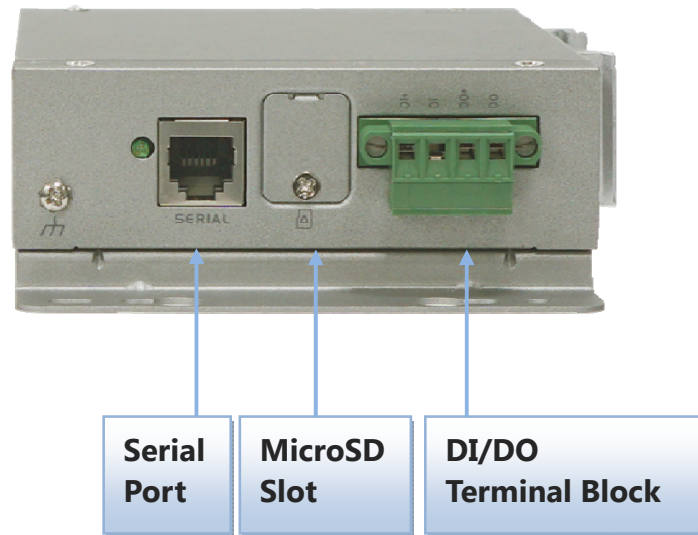
Modbus Cellular Gateway

1.4 LED Indication

LED Icon	Indication	LED Color	Description
$\bigcirc$1	Power Source 1	Green	**Steady ON:** Device is powered on by power source 1
$\bigcirc$2	Power Source 2 (*[3])	Green	**Steady ON:** Device is powered on by power source 2
A	SIM A (*[4])	Green	**Steady ON:** SIM card A is chosen for connection
B	SIM B	Green	**Steady ON:** SIM card B is chosen for connection
HIGH	High Cellular Signal	Green	**Steady ON:** The signal strength of Cellular is strong
LOW	Low Cellular Signal	Green	**Steady ON:** The signal strength of Cellular is weak
LAN	LAN	Green	**Steady ON:** Ethernet connection of LAN WAN is established **Flash:** Data packets are transferred
Serial	Serial Port	Green	**Steady ON:** If serial device is attached

---

3 If both of power source 1 and power source 2 are connected, the device will choose power source 1 first. The LED of power source 2 will remain OFF at this condition.

4 The SIM LED indicates which SIM socket will be chosen for connection by system setting, no matter SIM card is inserted or not.

1.5 Installation & Maintenance Notice

1.5.1 SYSTEM REQUIREMENTS

Network Requirements	• A fast Ethernet RJ45 cable • 3G/4G cellular service subscription • 10/100 Ethernet adapter on PC
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 6.0 or higher • Chrome 2.0 or higher • Firefox 3.0 or higher • Safari 3.0 or higher

1.5.2 WARNING

Attention	● Only use the power adapter that comes with the package. Using a different voltage rating power adaptor is dangerous and may damage the product. ● Do not open or repair the case yourself. If the product is too hot, turn off the power immediately and have it repaired at a qualified service center. ● Place the product on a stable surface and avoid using this product and all accessories outdoors.

Modbus Cellular Gateway

1.5.3 HOT SURFACE CAUTION

CAUTION: The surface temperature for the metallic enclosure can be very high! Especially after operating for a long time, installed at a close cabinet without air conditioning support, or in a high ambient temperature space.

DO NOT touch the hot surface with your fingers while servicing!!

Modbus Cellular Gateway

1.6 Hardware Installation

This chapter describes how to install and configure the hardware

1.6.1 Mount the Unit

The IOG700AM series can be placed on a desktop, or mounted on the DIN Rail, and wall. The DIN-rail bracket is not screwed on the product when out of factory. Please screw the DIN-rail bracket on the product first if necessary.

1.6.2 Insert the SIM Card

WARNING: BEFORE INSERTING OR CHANGING THE SIM CARD, PLEASE MAKE SURE THAT POWER OF THE DEVICE IS SWITCHED OFF.

The SIM card slots are located at the bottom side of the housing. You need to unscrew and remove the outer SIM card cover before installing or removing the SIM card. Please follow the instructions to insert a SIM card. After SIM card is well placed, screw back the outer SIM card cover.

Step 1: Follow red arrow to unlock SIM socket	Step 2: Lift up SIM holder, and insert SIM card	Step 3: Put back SIM holder, and follow red arrow to lock SIM socket
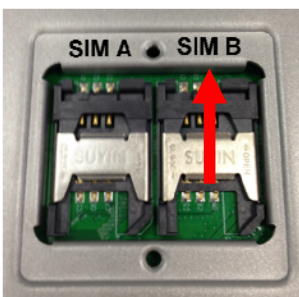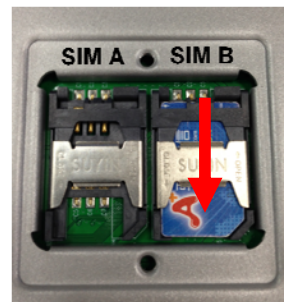
Modbus Cellular Gateway

1.6.3 Connecting Power

The IOG700 series product can be powered by connecting a power source to the terminal block . **It supports dual 9 to 48VDC power inputs**. Following picture is the power terminal block pin assignments. Please check carefully and connect to the right power requirements and polarity.

There is a DC12V/1A power adapter[5] in the package for you to easily connect DC power adapter to this terminal block.

WARNNING: This commercial-grade power adapter is mainly for ease of powering up the purchased device while initial configuration. It's not for operating at wide temperature range environment. PLEASE PREPARE OR PURCHASE OTHER INDUSTRIAL-GRADE POWER SUPPLY FOR POWERING UP THE DEVICE.

For the dual power supply design on PWR1 and PWR2, the primary/backup power mode is implemented. If there is only one power source, no matter it is connected to PWR1 or PWR2, the device can be powered up with the power source.

However, if there are two power sources available and connected to both PWR1 and PWR2 simutaneously, the device will choose PWR1 as the primary power, and supply required power to the entire system. The PWR2 is treated as a backup power source, and the device will seamlessly switch to use the PWR2 as the power source for the device when there is a power failure on PWR1. Whenever PWR1 is recovered, it will continute to supply the required power to the system since PWR1 is the treated as the primary power source.

---

5 The maximum power consumption of IOG700-0T001 is 7W.

Modbus Cellular Gateway

1.6.4 Connecting DI/DO Devices

There are a DI and a DO ports together with power terminal block. Please refer to following specification to connect DI and DO devices.

Mode	Specification	
Digital Input	Trigger Voltage (high)	Logic level 1: 5V~30V
	Normal Voltage (low)	Logic level 0: 0V~2.0V
Digital Output	Voltage (Relay Mode)	Depends on external device maximum voltage is 30V
	Maximum Current	1A

Example of Connection Diagram
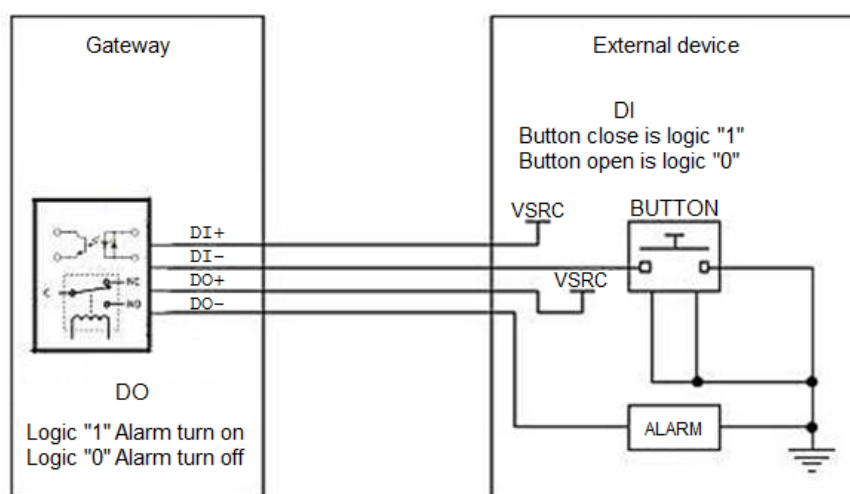
1.6.5 Connecting Serial Devices

The IOG700 series products provide one standard serial port RJ12 female connector and one RJ11 to DB9 conversion cable. Connect the serial device to the unit DB9 male port with the right pin assignments of RS-232/485 are shown as below.

RS232/485 Pinout

Pin1:Data Camier Detect (DCD)
Pin2:Received Data (RXD)
Pin3:Transmit Data (TXD)
Pin4:Data Teminal Ready (DTR)
Pin5:Ground (GND)

Pin6:Data Set Ready (DSR)
Pin7:Request To Send (RTS)
Pin8:Clear To Send (CTS)
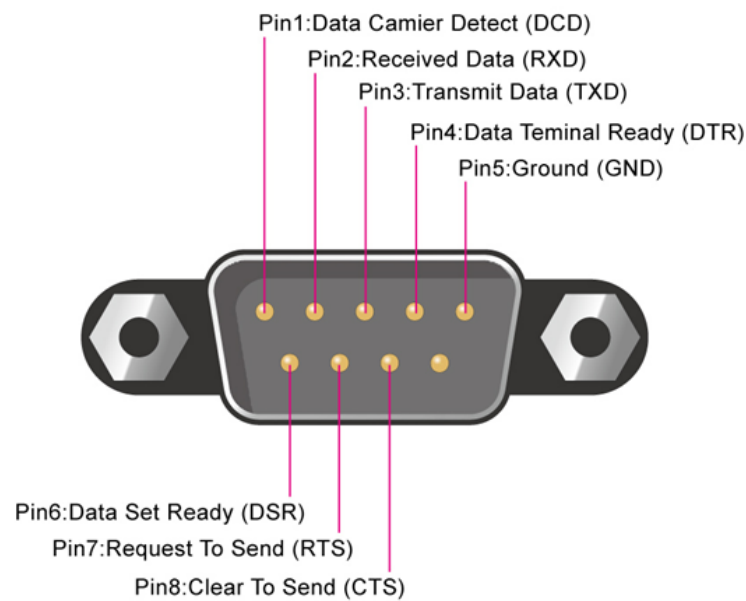
	Pin1	Pin2	Pin3	Pin4	Pin5	Pin6	Pin7	Pin8
RS-232	DCD	RXD	TXD	DTR	GND	DSR	RTS	CTS
RS-485			DATA+	DATA-	GND			

1.6.6 Connecting to the Network or a Host

The IOG700 series product provides one RJ45 port to connect 10/100Mbps Ethernet. It can auto detect the transmission speed on the network and configure itself automatically. Connect the Ethernet cable to the RJ45 port of the device. Plug one end of an Ethernet cable into your computer's network port and the other end into the LAN port on the front panel. If you need to configure or troubleshoot the device, you may need to connect the gateway directly to the host PC. In this way, you can also use the RJ45 Ethernet cable to connect the gateway to the host PC's Ethernet port.

Modbus Cellular Gateway

1.6.7 Setup by Configuring WEB UI

You can browse web UI to configure the device.

Type in the IP Address (**http://192.168.123.254**)[6]

When you see the login page, enter the password **'admin'** [7] and then click **'Login'** button.

---
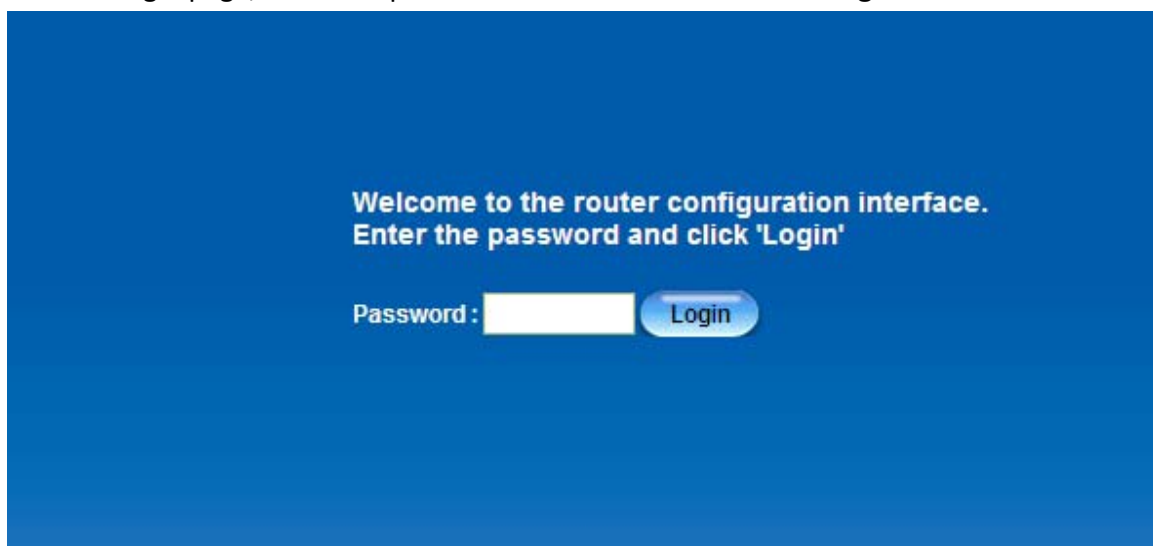
6 The default LAN IP address of this gateway is 192.168.123.254. If you change it, you need to login by using the new IP address.

7 It's strongly recommending you to change this login password from default value.

Chapter 2 Basic Network

2.1 WAN & Uplink

The gateway provides one WAN interface to let all client hosts in Intranet of the gateway access the Internet via ISP. But ISPs in the world apply various connection protocols to let gateways or user's devices dial in ISPs and then link to the Internet via different kinds of transmit media.

So, the WAN Connection lets you specify the WAN Physical Interface, WAN Internet Setup and WAN Load Balance for Intranet to access Internet. For each WAN interface, you must specify its physical interface first and then its Internet setup to connect to ISP.

Modbus Cellular Gateway

2.1.1 Physical Interface
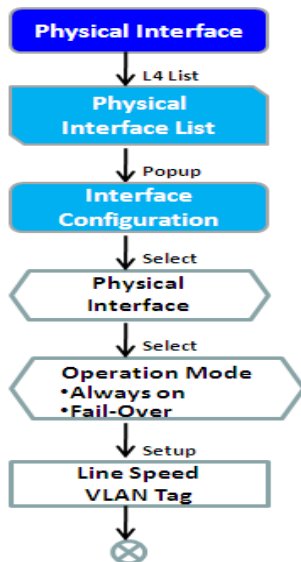
Physical Interface List			
Interface Name	**Physical Interface**	**Operation Mode**	**Action**
WAN-1	3G/4G	Always on	Edit

Interface Configuration (WAN - 1)	
Item	**Setting**
▶ Physical Interface	3G/4G ▼
▶ Operation Mode	Always on ▼
▶ VLAN Tagging	☐ Enable 0 (1-4095)

The first step to configure one WAN interface is to specify which kind of connection media to be used for the WAN connection, as shown in "Physical Interface" page.

In "Physical Interface" page, there are two configuration windows, "Physical Interface List" and "Interface Configuration". "Physical Interface List" window shows all the available physical interfaces. After clicking on the "Edit" button for the interface in "Physical Interface List" window the "Interface Configuration" window will appear to let you configure a WAN interface.

Physical Interface:

- **3G/4G WAN:** The gateway has one built-in 3G/4G cellular as WAN connection. For each cellular WAN, there are 1 or 2 SIM cards to be inserted for special failover function.

Attention
- Please **MUST POWER OFF** the gateway before you insert or remove SIM card.
- The SIM card can be damaged if you insert or remove SIM card while the gateway is in operation.

Modbus Cellular Gateway

Operation Mode:

There are three option items "Always on", "Failover", and "Disable" for the operation mode setting. However, for the single WAN device, only "Always on" is available.

> **Always on:** Set this WAN interface to be active all the time. When two or more WAN are established at "Always on" mode, outgoing data will through these WAN connections base on load balance policies.

VLAN Tagging

Sometimes, your ISP required a VLAN tag to be inserted into the WAN packets from Gateway for specific services. Please enable VLAN tagging and specify tag in the WAN physical interface. Please be noted that only Ethernet and ADSL physical interfaces support the feature. For the device with 3G/4G WAN only, it is disabled.

Physical Interface Setting

Go to Basic Network > WAN > Physical Interface tab.

The Physical Interface allows user to setup the physical WAN interface and to adjust WAN's behavior.

Note: Numbers of available WAN Interfaces can be different for the purchased gateway.

Interface Name	Physical Interface	Operation Mode	Line Speed	Action
WAN-1	3G/4G	Always on	50 (Mbps) / 100 (Mbps)	Edit

When **Edit** button is applied, an **Interface Configuration** screen will appear. WAN-1 interface is used in this example.

Modbus Cellular Gateway

Interface Configuration:

Interface Configuration (WAN - 1)	
Item	**Setting**
▶ Physical Interface	3G/4G ▼
▶ Operation Mode	Always on ▼
▶ VLAN Tagging	☐ Enable 0 (1-4095)

Interface Configuration		
Item	**Value setting**	**Description**
Physical Interface	1. A Must fill setting 2. WAN-1 is the primary interface and is factory set to Always on.	Select one expected interface from the available interface dropdown list. Depending on the router model, **Disable** and **Failover** options will be available only to multiple WAN gateways. WAN-2 and WAN-3 interfaces are only available to multiple WAN gateway.
Operation Mode	A Must fill setting	Define the operation mode of the interface. Select **Always on** to make this WAN always active. Select **Disable** to disable this WAN interface. Select **Failover** to make this WAN a Failover WAN when the primary or the secondary WAN link failed. Then select the primary or the existed secondary WAN interface to switch Failover from. (Note: for WAN-1, only **Always on** option is available.)
VLAN Tagging	Optional setting	Check **Enable** box to enter tag value provided by your ISP. Otherwise uncheck the box. *Value Range*: 1 ~ 4096. Note: This feature is NOT available for 3G/4G WAN connection.

Modbus Cellular Gateway

2.1.2 Internet Setup
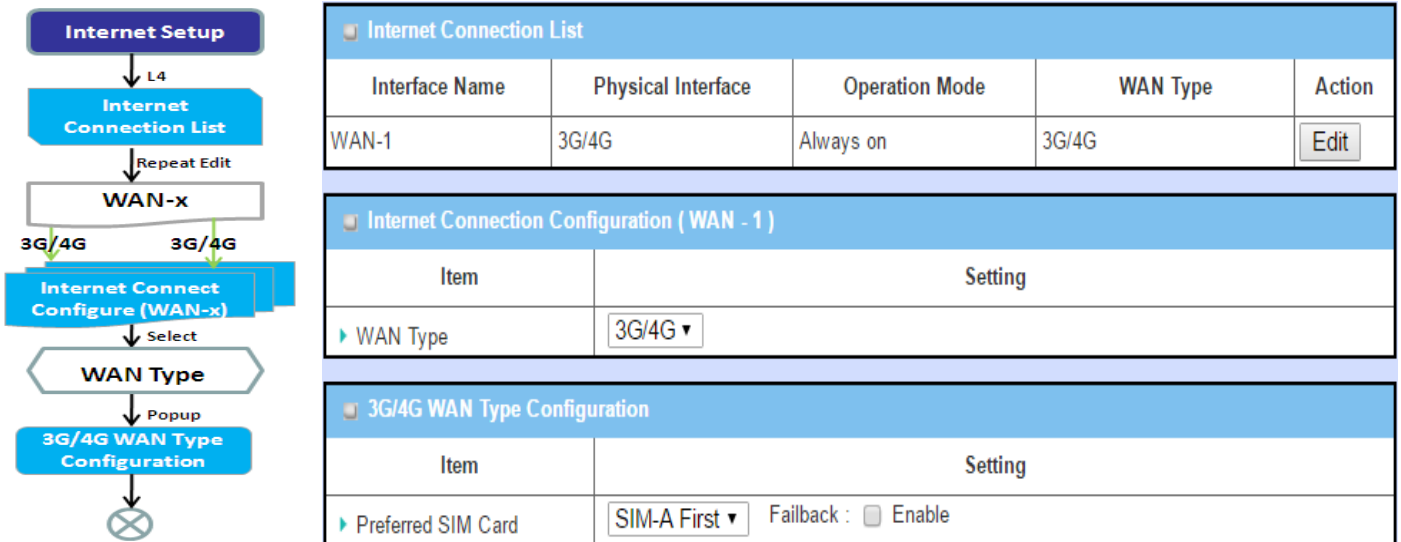
After specifying the physical interface for each WAN connection, administrator must configure their connection profile to meet the dial in process of ISP, so that all client hosts in the Intranet of the gateway can access the Internet.

In "Internet Setup" page, there are some configuration windows: "Internet Connection List", "Internet Connection Configuration", "WAN Type Configuration" and related configuration windows for each WAN type. For the Internet setup of each WAN interface, you must specify its WAN type of physical interface first and then its related parameter configuration for that WAN type.

After clicking on the "Edit" button of a physical interface in "Internet Setup List" window, the "Internet Connection Configuration" window will appear to let you specify which kind of WAN type that you will use for that physical interface to make an Internet connection. Based on your chosen WAN type, you can configure necessary parameters in each corresponding configuration window.

Modbus Cellular Gateway

Internet Connection – 3G/4G WAN

Preferred SIM Card – Dual SIM Fail Over

For 3G/4G embedded device, one embedded cellular module can create only one WAN interface. This device has featured by using dual SIM cards for one module with special fail-over mechanism. It is called Dual SIM Failover. This feature is useful for ISP switch over when location is changed. Within "Dual SIM Failover", there are various usage scenarios, including "SIM-A First", "SIM-B First" with "Failback" enabled or not, and "SIM-A Only and "SIM-B Only".

Modbus Cellular Gateway

SIM-A/SIM-B only: When "SIM-A Only" or "SIM-B Only" is used, the specified SIM slot card is the only one to be used for negotiation parameters between gateway device and cellular ISP.

SIM-A / SIM-B first without enable Failback
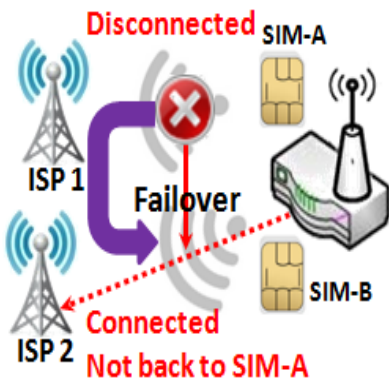
By default, "SIM-A First" scenario is used to connect to cellular ISP for data transfer. In the case of "SIM-A First" or "SIM-B First" scenario, the gateway will try to connect to the Internet by using SIM-A or SIM-B card first. And when the connection is broken, the gateway will switch to use the other SIM card for an alternate automatically and **will not switch back** to use original SIM card except current SIM connection is also broken. That is, SIM-A and SIM-B are used iteratively, but either one will keep being used for data transfer when current connection is still alive.

SIM-A / SIM-B first with Failback enable
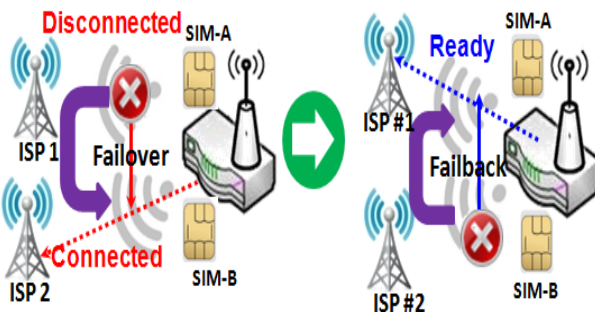
With Failback option enabled, "SIM-A First" scenario is used to connect when the connection is broken, gateway system will switch to use SIM-B. And when SIM-A connection is recovered, it will switch back to use original SIM-A card

Modbus Cellular Gateway

Internet Setup Setting

Go to **Basic Network > WAN > Internet Setup** tab.

Internet Setup allows user to setup WAN connection of the gateway. Numbers of available WAN Interfaces can be different for the purchased gateway.

Internet Connection List shows the basic information of each WAN. Click **Edit** button to configure. Then follow the following pages for detail settings.

Internet Connection List				
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	3G/4G	Always on	3G/4G	Edit

Internet Connection List		
Item	**Value setting**	**Description**
Interface Name	N/A	Shows the name of WAN interface.
Physical Interface	N/A	Physical Interface (i.e. 3G/4G) shows the type of interface configured to map with **Interface Name**.
Operation Mode	N/A	**Operation Mode** shows the current setting of Connection Control mode of WAN interface to keep WAN connection. ● **Auto-reconnect (Always on)** ● **Connect-on-demand** ● **Connect Manually**
WAN Type	N/A	**WAN Type** shows the type of connection method to your ISP. Depending on the device model, the following WAN connection types are supported. ● **3G/4G:** 3G/4G

Note: If **Edit** button is disabled for the Interface, you will need to enable the Interface first by going to **Basic Network > WAN & Uplink > Physical Interface** page. Then Click **Edit** button then select Always on or Failover.

Modbus Cellular Gateway

Internet Setup – 3G/4G WAN

Internet Connection List				
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	3G/4G	Always on	3G/4G	Edit

Configure 3G/4G WAN Setting

When **Edit** button is applied, **Internet Connection Configuration**, and **3G/4G WAN Configuration** screens will appear.

Internet Connection Configuration (WAN - **1**)	
Item	Setting
▶ WAN Type	3G/4G ▾

3G/4G WAN Type Configuration	
Item	Setting
▶ Preferred SIM Card	SIM-A First ▾ Failback : ☐ Enable

3G/4G Connection Configuration		
Item	Value setting	Description
WAN Type	1. A Must filled setting 2. **3G/4G** is set by default.	From the dropdown box, select Internet connection method for 3G/4G WAN Connection. Only **3G/4G** is available.
Preferred SIM Card	1. A Must filled setting 2. By default **SIM-A First** is selected 3. **Failback** is unchecked by default	Choose which SIM card you want to use for the connection. When **SIM-A First** or **SIM-B First** is selected, it means the connection is built first by using SIM A/SIM B. And if the connection is failed, it will change to the other SIM card and try to dial again, until the connection is up. When **SIM-A only** or **SIM-B only** is selected, it will try to dial up only using the SIM card you selected. When **Failback** is checked, it means if the connection is dialed-up not using the main SIM you selected, it will failback to the main SIM and try to establish the connection periodically. Note_1: In some AMIT's products, only **SIM-A** can be chose. Note_2: **Failback** is available only when **SIM-A First** or **SIM-B First** is selected.

Modbus Cellular Gateway

Configure SIM-A / SIM-B Card

Here you can set configurations for the cellular connection according to your situation or requirement.

Connection with SIM-A Card	
Item	**Setting**
▸ Network Type	Auto ▾
▸ Band Selection	Auto ▾
▸ Band List	2G 3G LTE
▸ Dial-Up Profile	Manual-configuration ▾
▸ APN	[ ] (Optional)
▸ PIN Code	[ ] (Optional)
▸ Dial Number	[ ]
▸ Account	[ ] (Optional)
▸ Password	[ ] (Optional)
▸ Authentication	Auto ▾
▸ IP Mode	Dynamic IP ▾
▸ Primary DNS	[ ] (Optional)
▸ Secondary DNS	[ ] (Optional)
▸ Roaming	☐ Enable

Note_1: Configurations of SIM-B Card follows the same rule of Configurations of SIM-A Card, here we list SIM-A as the example.

Note_2: Both **Connection with SIM-A Card** and **Connection with SIM-B Card** will pop up only when the **SIM-A First** or **SIM-B First** is selected, otherwise it only pops out one of them.

Connection with SIM-A/-B Card		
Item	**Value setting**	**Description**
Network Type	1. A Must filled setting 2. By default **Auto** is selected	Select **Auto** to register a network automatically, regardless of the network type. Select **2G Only** to register the 2G network only. Select **2G Prefer** to register the 2G network first if it is available. Select **3G only** to register the 3G network only. Select **3G Prefer** to register the 3G network first if it is available. Select **LTE only** to register the LTE network only. **Note**: Options may be different due to the specification of the module.
Band Selection	1. A Must filled setting 2. By default **Auto** is selected	Select **Auto** to register a network automatically, regardless of the band. Select **Manual** to choose specific bands you want to appoint to.

Modbus Cellular Gateway

Band List	1. A Must filled setting 2. The box is all checked by default	When **Band Selection > Auto** is selected, all bands are enabled and can't be unchecked. When **Band Selection > Manual** is selected, at least one band needs to be checked in each network type.
Dial-Up Profile	1. A Must filled setting 2. By default **Auto-detection** is selected	Specify the type of dial-up profile for your 3G/4G network. It can be **Manual-configuration**, **APN Profile List**, or **Auto-detection**. Select **Manual-configuration** to set APN (Access Point Name), **Dial Number**, **Account**, and **Password** to what your carrier provides. Select **APN Profile List** to set more than one profile to dial up in turn, until the connection is established. It will pop up a new filed, please go to **Basic Network > WAN & Uplink > Internet Setup > SIM-A APN Profile List** for details. Select **Auto-detection** to automatically bring out all configurations needed while dialing-up, by comparing the IMSI of the SIM card to the record listed in the manufacture's database. **Note_1:** You are highly recommended to select the **Manual** or **APN Profile List** to specify the network for your subscription. Your ISP always provides such network settings for the subscribers. **Note_2:** If you select **Auto-detection**, it is likely to connect to improper network, or failed to find a valid APN for your ISP.
APN	1. A Must filled setting 2. String format : any text	Enter the **APN** you want to use to establish the connection. This is a must-filled setting if you selected **Manual-configuration** as dial-up profile scheme.
PIN code	String format : interger	Enter the PIN (Personal Identification Number) code if it needs to unlock your SIM card.
Authentication	1. A Must filled setting 2. By default **Auto** is selected	Select **PAP** (Password Authentication Protocol) and use such protocol to be authenticated with the carrier's server. Select **CHAP** (Challenge Handshake Authentication Protocol) and use such protocol to be authenticated with the carrier's server. When **Auto** is selected, it means it will authenticate with the server either **PAP** or **CHAP**.
IP Mode	1. A Must filled setting 2. By default **Dynamic IP** is selected	When **Dynamic IP** is selected, it means it will get all IP configurations from the carrier's server and set to the device directly. If you have specific application provided by the carrier, and want to set IP configurations on your own, you can switch to **Static IP** mode and fill in all parameters that required, such as IP address, subnet mask and gateway. **Note**: **IP Subnet Mask** is a must filled setting, and make sure you have the right configuration. Otherwise, the connection may get issues.
Primary DNS	String format : IP address (IPv4 type)	Enter the IP address to change the primary DNS (Domain Name Server) setting. If it is not filled-in, the server address is given by the carrier while dialing-up.
Secondary DNS	String format : IP address (IPv4 type)	Enter the IP address to change the secondary DNS (Domain Name Server) setting. If it is not filled-in, the server address is given by the carrier while dialing-up.
Roaming	The box is unchecked by default	Check the box to establish the connection even the registration status is roaming, not in home network. **Note**: It may cost additional charges if the connection is under roaming.

Modbus Cellular Gateway

Create/Edit SIM-A / SIM-B APN Profile List

You can add a new APN profile for the connection, or modify the content of the APN profile you added. It is available only when you select **Dial-Up Profile** as **APN Profile List**.

ID	Profile Name	MCC	MNC	APN	Dial Number	Account	Password	Priority	Enable	Actions

SIM-A APN Profile List [Add] [Delete]

List all the APN profile you created, easily for you to check and modify. It is available only when you select **Dial-Up Profile** as **APN Profile List**.

When **Add** button is applied, an **APN Profile Configuration** screen will appear.

SIM-A APN Profile Configuration

Item	Setting
▶ Profile Name	Profile-1
▶ MCC	(Optional)
▶ MNC	(Optional)
▶ APN	
▶ Dial Number	(Optional)
▶ Account	(Optional)
▶ Password	(Optional)
▶ Priority	
▶ Profile	☑ Enable

SIM-A/-B APN Profile Configuration		
Item	**Value setting**	**Description**
Profile Name	1. By default **Profile-x** is listed 2. String format : any text	Enter the profile name you want to describe for this profile.
MCC	String format : integer	Enter the **MCC** (Mobile Country Code) you want to use for this profile. **Note**: the **MCC** should be related to the **MNC**, this filed can't be invalid value if **MNC** is filled-in.
MNC	String format : integer	Enter the **MNC** (Mobile Network Code) you want to use for this profile. **Note**: the **MNC** should be related to the **MCC**, this filed can't be invalid value if **MCC** is filled-in.
APN	String format : any text	Enter the **APN** you want to use to establish the connection.
Account	String format : any text	Enter the **Account** you want to use for the authentication. ***Value Range***: 0 ~ 53 characters.
Password	String format : any text	Enter the **Password** you want to use for the authentication.
Authentication	1. A Must filled setting 2. By default **Auto** is	Select the Authentication method for the 3G/4G connection. It can be **Auto**, **PAP**, **CHAP**, or **None**.

	selected	
Priority	1. A Must filled setting 2. String format : integer	Enter the value for the dialing-up order. The valid value is from 1 to 16. It will start to dial up with the profile that assigned with the smallest number. ***Value Range*****: 1 ~ 16.**
Profile	The box is checked by default	Check the box to enable this profile. Uncheck the box to disable this profile in dialing-up action.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	N/A	When the **Back** button is clicked, the screen will return to the previous page.

Modbus Cellular Gateway

Setup 3G/4G Connection Common Configuration

Here you can change common configurations for 3G/4G WAN.

3G/4G Connection Common Configuration	
Item	Setting
▶ Connection Control	Auto-reconnect (Always on) ▾
▶ Time Schedule	(0) Always ▾
▶ MTU	0 (0 is Auto)
▶ NAT	☑ Enable
▶ Network Monitoring	☑ Enable ◉ DNS Query ○ ICMP Checking ☑ Loading Check Check Interval 5 (seconds) Check Timeout 3 (seconds) Latency Threshold 3000 (ms) Fail Threshold 5 (Times) Target1 DNS1 ▾ Target2 None ▾
▶ IGMP	Disable ▾
▶ WAN IP Alias	☐ Enable 10.0.0.1

3G/4G Connection Common Configuration		
Item	**Value setting**	**Description**
Connection Control	By default **Auto-reconnect** is selected	When **Auto-reconnect** is selected, it means it will try to keep the Internet connection on all the time whenever the physical link is connected. When **Connect-on-demand** is selected, it means the Internet connection will be established only when detecting data traffic. When **Connect Manually** is selected, it means you need to click the **Connect** button to dial up the connection manually. Please go to **Status > Basic Network > WAN & Uplink** tab for details. **Note**: This field is available only when **Basic Network > WAN > Physical Interface > Operation Mode** is selected to **Always on**.
Time Schedule	1. A Must filled setting 2. By default **(0) Always** is selected	When **(0) Always** is selected, it means this WAN is under operation all the time. Once you have set other schedule rules, there will be other options to select. Please go to **Object Definition > Scheduling** for details.
MTU	1. A Must filled setting 2. By default **0** is filled-in	Specify the **MTU** (Maximum Transmission Unit) for the 3G/4G connection. *Value Range*: 512 ~ 1500, but 0 is for auto.
NAT	Checked by default	Uncheck the box to disable **NAT** (Network Address Translation) function.
Network Monitoring	1. An optional setting 2. Enabled by default	When the Network Monitoring feature is enabled, the gateway will use DNS Query or ICMP to periodically check Internet connection –connected or disconnected. ● Choose either **DNS Query** or **ICMP Checking** to detect WAN link. With **DNS Query,** the system checks the connection by sending DNS

Modbus Cellular Gateway

		Query packets to the destination specified in Target 1 and Target 2. With **ICMP Checking,** the system will check connection by sending ICMP request packets to the specified destination.
		● **Loading Check**
		Enable Loading Check allows the router to ignore unreturned DNS Queries or ICMP requests when WAN bandwidth is fully occupied. This is to prevent false link-down status.
		● **Check Interval** defines the transmitting interval between two DNS Query or ICMP checking packets.
		***Value Range*: 2 ~ 30 seconds.**
		● **Check Timeout** defines the timeout of each DNS query/ICMP.
		***Value Range*: 2 ~ 5 seconds.**
		● **Latency Threshold** defines the threshold of responding time.
		***Value Range*: 2000 ~ (1000* Check Timeout) ms.**
		● **Fail Threshold** specifies the detected disconnection before the router recognize the WAN link down status. Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged.
		***Value Range*: 2 ~ 10 seconds.**
		● **Target1** (**DNS1** set by default**)** specifies the first target of sending DNS query/ICMP request.
		  ■ **DNS1**: set the primary DNS to be the target.
		  ■ **DNS2**: set the secondary DNS to be the target.
		  ■ **Gateway**: set the Current gateway to be the target.
		  ■ **Other Host**: enter an IP address to be the target.
		● **Target2** (**None** set by default**)** specifies the second target of sending DNS query/ICMP request.
		  ■ **None**: to disable **Target2.**
		  ■ **DNS1**: set the primary DNS to be the target.
		  ■ **DNS2**: set the secondary DNS to be the target.
		  ■ **Gateway**: set the Current gateway to be the target.
		  ■ **Other Host**: enter an IP address to be the target.

IGMP	By default **Disable** is selected	Select **Auto** to enable **IGMP** function. Check the **Enable** box to enable **IGMP Proxy**.
WAN IP Alias	1. Unchecked by default 2. String format: IP address (IPv4 type)	Check the box to enable **WAN IP Alias**, and fill in the IP address you want to assign.

2.2 LAN & VLAN

This section provides the configuration of LAN and VLAN. VLAN is an optional feature, and it depends on the product specification of the purchased gateway.

2.2.1 Ethernet LAN
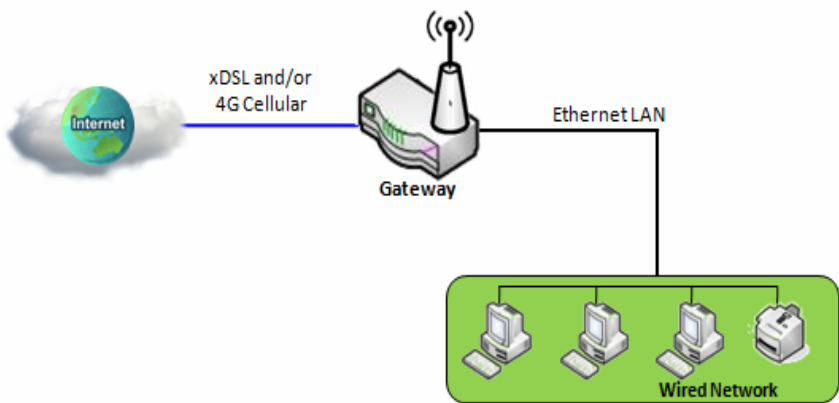
The Local Area Network (LAN) can be used to share data or files among computers attached to a network. Following diagram illustrates the network that wired and interconnects computers.

Please follow the following instructions to do IPv4 Ethernet LAN Setup.

Configuration	
Item	**Setting**
▸ LAN IP Address	192.168.123.254
▸ Subnet Mask	255.255.255.0 (/24) ▾

Configuration Item	Value setting	Description
LAN IP Address	1. A Must filled setting **2. 192.168.123.254 is set by default**	Enter the local IP address of this device. The network device(s) on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary. **Note**: *It's also the IP address of web UI. If you change it, you need to type new IP address in the browser to see web UI.*
Subnet Mask	1. A Must filled setting 2. **255.255.255.0 (/24)** is set by default	Select the subnet mask for this gateway from the dropdown list. Subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0 (/24), and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway, so there are maximum 253 clients allowed in LAN network. ***Value Range***: 255.0.0.0 (/8) ~ 255.255.255.252 (/30).
Save	N/A	Click the **Save** button to save the configuration

Modbus Cellular Gateway

Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.

Create / Edit Additional IP

This gateway provides the LAN IP alias function for some special management consideration. You can add additional LAN IP for this gateway, and access to this gateway with the additional IP.

ID	Name	Interface	IP Address	Subnet Mask	Enable	Action

(Additional IP — Add | Delete)

When **Add** button is applied, **Additional IP Configuration** screen will appear.

Additional IP Configuration

Item	Setting
▶ Name	
▶ Interface	lo ▾
▶ IP Address	
▶ Subnet Mask	255.255.255.0 (/24) ▾
▶ Enable	☐

Save

Configuration Item	Value setting	Description
Name	.1 An Optional Setting	Enter the name for the alias IP address.
Interface	1. A Must filled setting 2. **Lo** is set by default	Specify the Interface type. It can be **Lo** or **Br0**.
IP Address	1. An Optional setting 2. **192.168.123.254 is set by default**	Enter the addition IP address for this device.
Subnet Mask	1. A Must filled setting 2. **255.255.255.0 (/24)** is set by default	Select the subnet mask for this gateway from the dropdown list. Subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0 (/24), and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway, so there are maximum 253 clients allowed in LAN network. ***Value Range***: 255.0.0.0 (/8) ~ 255.255.255.255 (/32).
Save	NA	Click the **Save** button to save the configuration

Modbus Cellular Gateway

2.2.2 VLAN

VLAN (Virtual LAN) is a logical network under a certain switch or router device to group client hosts with a specific VLAN ID. This gateway supports both Port-based VLAN and Tag-based VLAN. These functions allow you to divide local network into different "virtual LANs". It is common requirement for some application scenario. For example, there are various departments within SMB. All client hosts in the same department should own common access privilege and QoS property. You can assign departments either by port-based VLAN or tag-based VLAN as a group, and then configure it by your plan. In some cases, ISP may need router to support "VLAN tag" for certain kinds of services (e.g. IPTV). You can group all devices required this service as one tag-based VLAN.

If the gateway has only one physical Ethernet LAN port, only very limited configuration is available if you enable the Port-based VLAN.

➢ Port-based VLAN

Port-based VLAN function can group Ethernet ports, Port-1 ~ Port-4, and WiFi Virtual Access Points, VAP-1 ~ VAP-8, together for differentiated services like Internet surfing, multimedia enjoyment, VoIP talking, and so on. Two operation modes, NAT and Bridge, can be applied to each VLAN group. One DHCP server can be allocated for a NAT VLAN group to let group host member get its IP address. Thus, each host can surf Internet via the NAT mechanism of business access gateway. In bridge mode, Intranet packet flow is delivered out WAN trunk port with VLAN tag to upper link for different services.
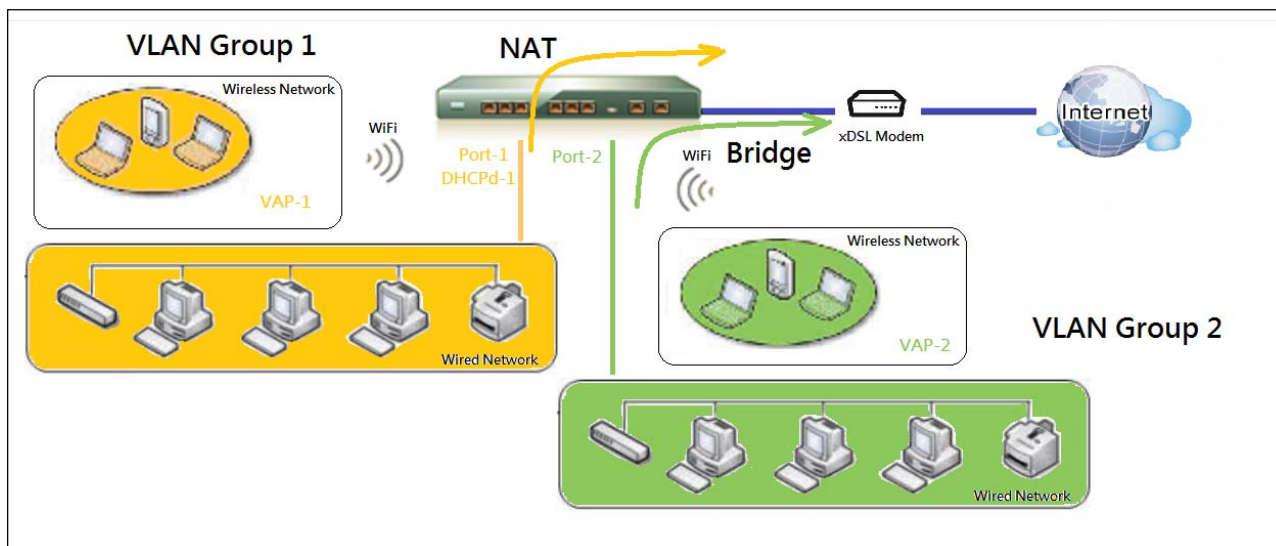
A port-based VLAN is a group of ports on an Ethernet or Virtual APs of Wired or Wireless Gateway that form a logical LAN segment. Following is an example.

For example, in a company, administrator schemes out 3 network segments, Lobby/Meeting Room, Office, and Data Center. In a Wireless Gateway, administrator can configure Lobby/Meeting Room segment with VLAN ID 3. The VLAN group includes Port-3 and VAP-8 (SSID: Guest) with NAT mode and DHCP-3 server equipped. He also configure Office segment with VLAN ID 2. The VLAN group includes Port-2 and VAP-1 (SSID:

Modbus Cellular Gateway

Staff) with NAT mode and DHCP-2 server equipped. At last, administrator also configure Data Center segment with VLAN ID 1. The VLAN group includes Port-1 with NAT mode to WAN interface as shown in following diagram.
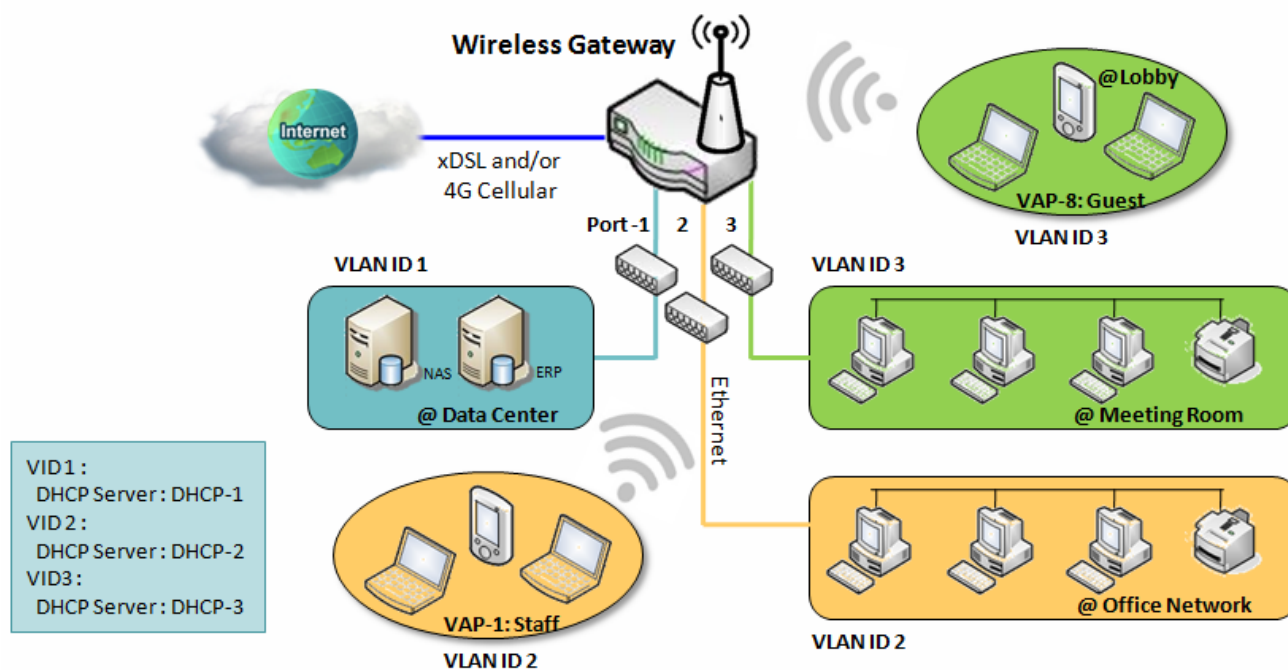
Above is the general case for 3 Ethernet LAN ports in the gateway. But if the device just has one Ethernet LAN port, there will be only one VLAN group for the device. Under such situation, it still supports both the NAT and Bridge mode for the Port-based VLAN configuration.

➢ Tag-based VLAN

Tag-based VLAN function can group Ethernet ports, Port-1 ~ Port-4, and WiFi Virtual Access Points, VAP-1 ~ VAP-8, together with different VLAN tags for deploying subnets in Intranet. All packet flows can carry with different VLAN tags even at the same physical Ethernet port for Intranet. These flows can be directed to different destination because they have differentiated tags. The approach is very useful to group some hosts at different geographic location to be in the same workgroup.

Tag-based VLAN is also called a VLAN Trunk. The VLAN Trunk collects all packet flows with different VLAN IDs from Router device and delivers them in the Intranet. VLAN membership in a tagged VLAN is determined by VLAN ID information within the packet frames that are received on a port. Administrator can further use a VLAN switch to separate the VLAN trunk to different groups based on VLAN ID. Following is an example.

Modbus Cellular Gateway
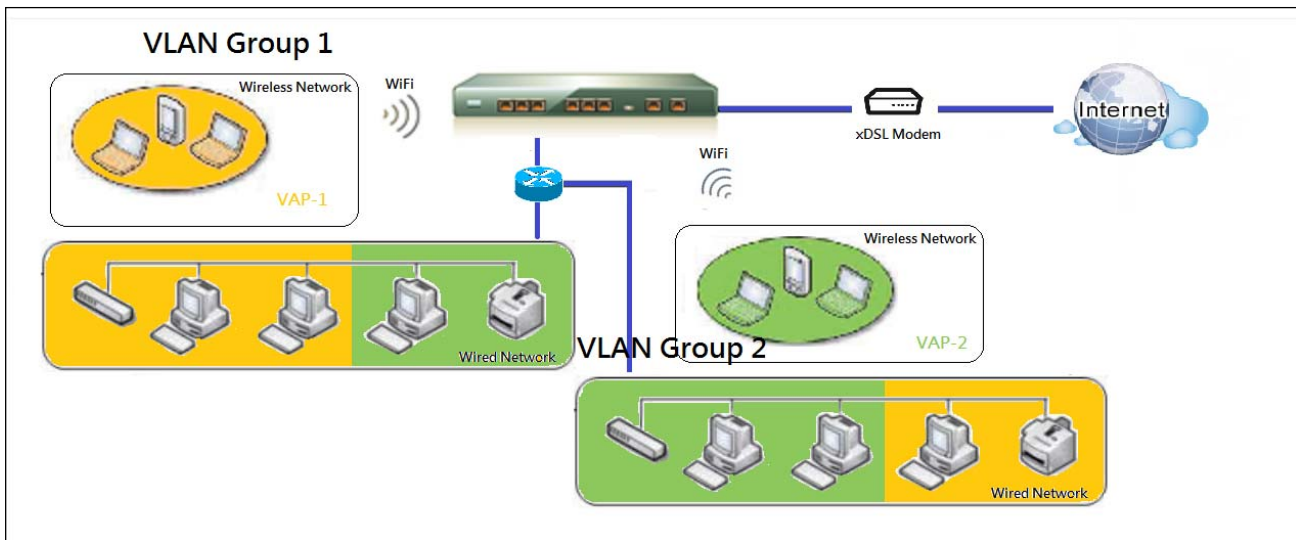
For example, in a company, administrator schemes out 3 network segments, Lab, Meeting Rooms, and Office. In a Security VPN Gateway, administrator can configure Office segment with VLAN ID 12. The VLAN group is equipped with DHCP-3 server to construct a 192.168.12.x subnet. He also configure Meeting Rooms segment with VLAN ID 11. The VLAN group is equipped with DHCP-2 server to construct a 192.168.11.x subnet for Intranet only. That is, any client host in VLAN 11 group can't access the Internet. At last, he configures Lab segment with VLAN ID 10. The VLAN group is equipped with DHCP-1 server to construct a 192.168.10.x subnet.
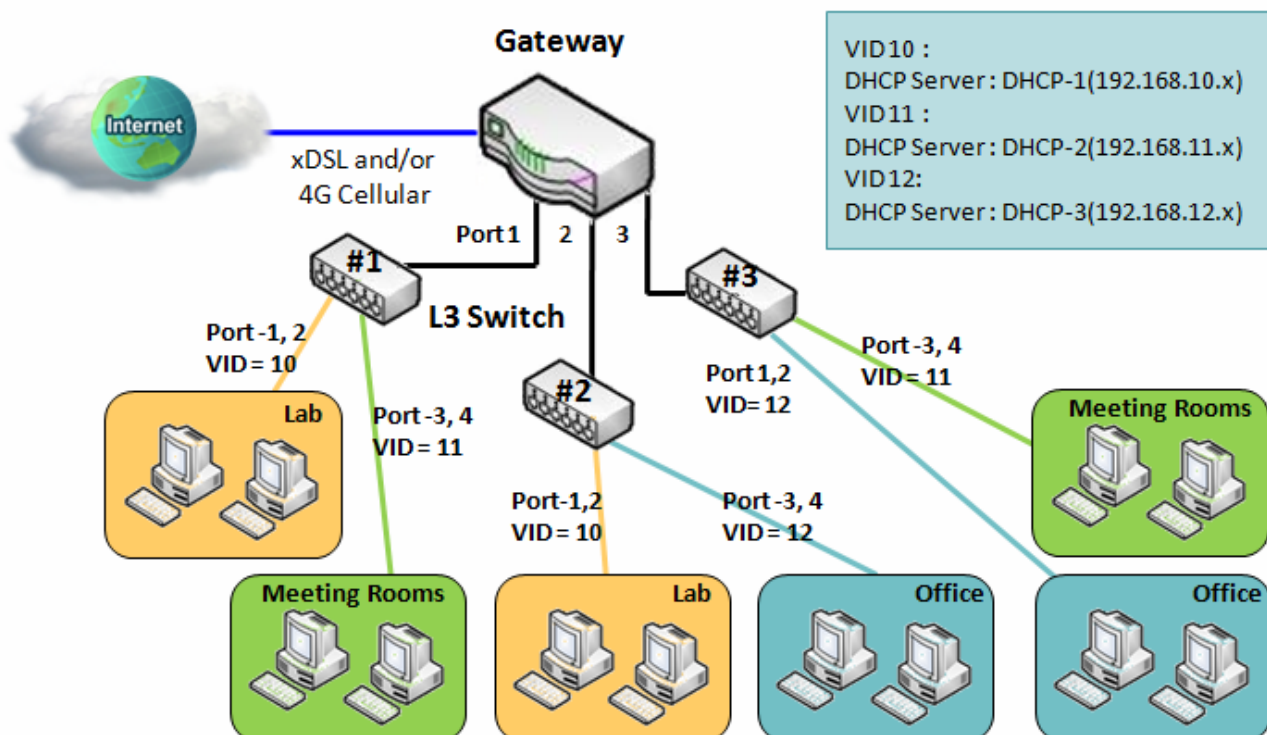
Modbus Cellular Gateway

➢ VLAN Groups Access Control

Administrator can specify the Internet access permission for all VLAN groups. He can also configure which VLAN groups are allowed to communicate with each other.

VLAN Group Internet Access

Administrator can specify members of one VLAN group to be able to access Internet or not. Following is an example that VLAN groups of VID is 2 and 3 can access Internet but the one with VID is 1 cannot access Internet. That is, visitors in meeting room and staffs in office network can access Internet. But the computers/servers in data center cannot access Internet since security consideration. Servers in data center only for trusted staffs or are accessed in secure tunnels.
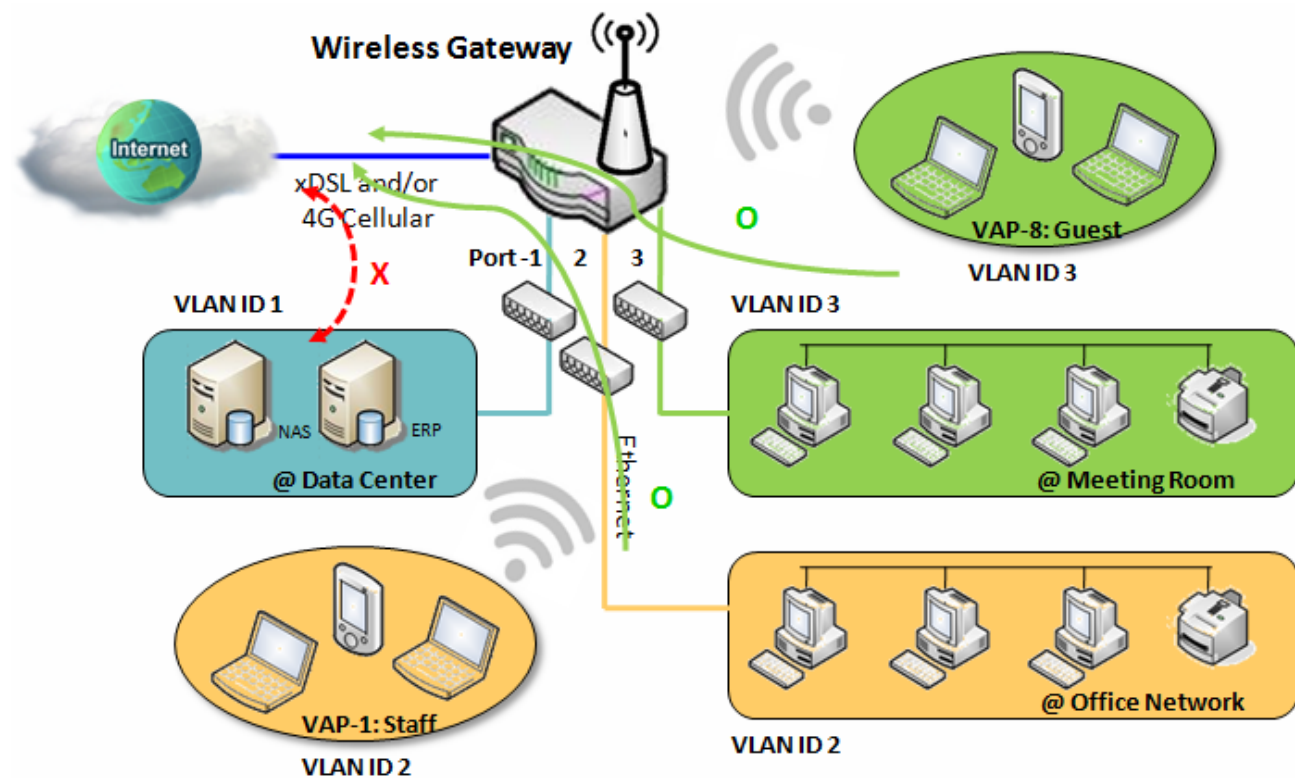
Modbus Cellular Gateway

Inter VLAN Group Routing:

In Port-based tagging, administrator can specify member hosts of one VLAN group to be able to communicate with the ones of another VLAN group or not. This is a communication pair, and one VLAN group can join many communication pairs. But communication pair doesn't have the transitive property. That is, A can communicate with B, and B can communicate with C, it doesn't imply that A can communicate with C. An example is shown at following diagram. VLAN groups of VID is 1 and 2 can access each other but the ones between VID 1 and VID 3 and between VID 2 and VID 3 can't.
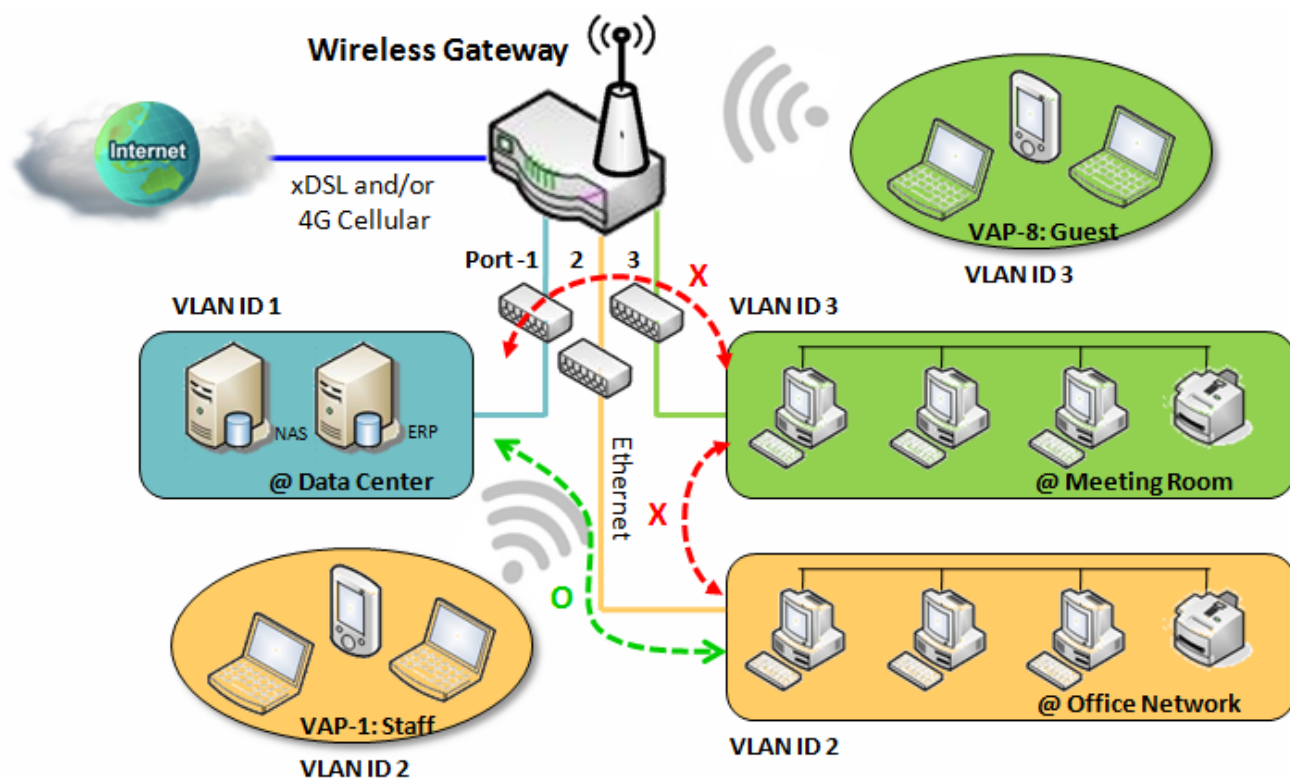
Modbus Cellular Gateway

VLAN Setting

Go to **Basic Network > LAN & VLAN > VLAN** Tab.

The VLAN function allows you to divide local network into different virtual LANs. There are Port-based and Tag-based VLAN types. Select one that applies.

Item	Setting
▶ VLAN Types	Port-based ▼

Configuration

Item	Value setting	Description
VLAN Type	**Port-based** is selected by default	Select the VLAN type that you want to adopt for organizing you local subnets. **Port-based**: Port-based VLAN allows you to add rule for each LAN port, and you can do advanced control with its VLAN ID. **Tag-based**: Tag-based VLAN allows you to add VLAN ID, and select member and DHCP Server for this VLAN ID. Go to **Tag-based VLAN List** table.
Save	NA	Click the **Save** button to save the configuration

Port-based VLAN – Create/Edit VLAN Rules

The port-based VLAN allows you to custom each LAN port. There is a default rule shows the configuration of all LAN ports. Also, if your device has a DMZ port, you will see DMZ configuration, too. The maxima rule numbers is based on LAN port numbers.

Port-based VLAN List Add Delete

Name	VLAN ID	VLAN Tagging	NAT / Bridge	Port Members	LAN IP Address	Subnet Mask	Joined WAN	WAN VID	Enable	Actions
DMZ	4094	X	NAT	DMZ Port	192.168.6.254	255.255.255.0	WAN - 1	0	☑	Edit
LAN	Native VLAN	X	NAT	Detail	192.168.123.254	255.255.255.0	All WANs	0	☑	Edit

Apply Inter VLAN Group Routing

When **Add** button is applied, Port-based VLAN Configuration screen will appear, which is including 3 sections: **Port-based VLAN Configuration**, **IP Fixed Mapping Rule List,** and **Inter VLAN Group Routing** (enter through a button)

Port-based VLAN – Configuration

Modbus Cellular Gateway

Port-based VLAN Configuration	
Item	**Setting**
▶ Name	VLAN-1
▶ VLAN ID	
▶ VLAN Tagging	Disable ▾
▶ NAT / Bridge	NAT ▾
▶ Port Members	☐ PORT2 ☐ PORT3 ☐ PORT4 ☐ VAP1 ☐ VAP2 ☐ VAP3 ☐ VAP4 ☐ VAP5 ☐ VAP6 ☐ VAP7 ☐ VAP8
▶ WAN & WAN VID to Join	All WANs ▾ None
▶ LAN IP Address	192.168.2.254
▶ Subnet Mask	255.255.255.0 (/24) ▾
▶ DHCP Server/Relay	Server ▾
▶ DHCP Server Name	
▶ IP Pool	Starting Address: 192.168.2.100 Ending Address: 192.168.2.200
▶ Lease Time	86400 seconds
▶ Domain Name	(Optional)
▶ Primary DNS	(Optional)
▶ Secondary DNS	(Optional)
▶ Primary WINS	(Optional)
▶ Secondary WINS	(Optional)
▶ Gateway	(Optional)
▶ Enable	☐

Port-based VLAN Configuration		
Item	**Value setting**	**Description**
Name	1. A Must filled setting 2. String format: already have default texts	Define the **Name** of this rule. It has a default text and cannot be modified.
VLAN ID	A Must filled setting	Define the VLAN ID number, range is 1~4094.
VLAN Tagging	**Disable** is selected by default.	The rule is activated according to **VLAN ID** and **Port Members** configuration when **Enable** is selected. The rule is activated according **Port Members** configuration when **Disable** is selected.
NAT / Bridge	**NAT** is selected by default.	Select **NAT** mode or **Bridge** mode for the rule.
Port Members	These box is unchecked by default.	Select which LAN port(s) and VAP(s) that you want to add to the rule. Note: The available member list can be different for the purchased product.

Modbus Cellular Gateway

WAN & WAN VID to Join	**All WANs** is selected by default.	Select which **WAN** or **All WANs** that allow accessing Internet. Note: If Bridge mode is selected, you need to select a WAN and enter a VID.
LAN IP Address	A Must filled setting	Assign an **IP Address** for the DHCP Server that the rule used, this IP address is a gateway IP.
Subnet Mask	**255.255.255.0(/24)** is selected by default.	Select a **Subnet Mask** for the DHCP Server.
DHCP Server /Relay	**Server** is selected by default.	Define the **DHCP Server** type. There are three types you can select: **Server**, **Relay**, and **Disable**. **Relay**: Select **Relay** to enable DHCP Relay function for the VLAN group, and you only need to fill the **DHCP Server IP Address** field. **Server**: Select **Server** to enable DHCP Server function for the VLAN group, and you need to specify the DHCP Server settings. **Disable**: Select **Disable** to disable the DHCP Server function for the VLAN group.
DHCP Server IP Address (for DHCP **Relay** only)	A Must filled setting	If you select **Relay** type of DHCP Server, assign a **DHCP Server IP Address** that the gateway will relay the DHCP requests to the assigned DHCP server.
DHCP Server Name	A Must filled setting	Define name of the DHCP Server.
IP Pool	A Must filled setting	Define the IP Pool range. There are **Starting Address** and **Ending Address** fields. If a client requests an IP address from this DHCP Server, it will assign an IP address in the range of **IP pool**.
Lease Time	A Must filled setting	Define a period of time for an IP Address that the DHCP Server leases to a new device. By default, the **lease time** is 86400 seconds.
Domain Name	String format can be any text	The Domain Name of this DHCP Server. ***Value Range***: 0 ~ 31 characters.
Primary DNS	IPv4 format	The Primary DNS of this DHCP Server.
Secondary DNS	IPv4 format	The Secondary DNS of this DHCP Server.
Primary WINS	IPv4 format	The Primary WINS of this DHCP Server.
Secondary WINS	IPv4 format	The Secondary WINS of this DHCP Server.
Gateway	IPv4 format	The Gateway of this DHCP Server.
Enable	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore what you just configured back to the previous setting.

Modbus Cellular Gateway

Besides, you can add some IP rules in the **IP Fixed Mapping Rule List** if DHCP Server for the VLAN groups is required.

When **Add** button is applied, **Mapping Rule Configuration** screen will appear.

Mapping Rule Configuration		
Item	**Value setting**	**Description**
MAC Address	A Must filled setting	Define the **MAC Address** target that the DHCP Server wants to match.
IP Address	A Must filled setting	Define the **IP Address** that the DHCP Server will assign. If there is a request from the MAC Address filled in the above field, the DHCP Server will assign this **IP Address** to the client whose **MAC Address** matched the rule.
Enable	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	NA	Click the **Save** button to save the configuration

Note: ensure to always click on **Apply** button to apply the changes after the web browser refreshed taken you back to the VLAN page.

Modbus Cellular Gateway

Port-based VLAN – Inter VLAN Group Routing

Click **VLAN Group Routing** button, the **VLAN Group Internet Access Definition** and **Inter VLAN Group Routing** screen will appear.

VLAN Group Internet Access Definition		
VLAN IDs	**Members**	**Internet Access(WAN)**
1	Port : 2,3,4 ; VAP : 1,2,3,4,5,6,7,8	Allow Edit
Inter VLAN Group Routing		
VLAN IDs	**Members**	**Action**
		Edit
		Edit
		Edit
		Edit
	Save Back	

When **Edit** button is applied, a screen similar to this will appear.

VLAN Group Internet Access Definition		
VLAN IDs	**Members**	**Internet Access(WAN)**
☑ 1, ☑ 2	Port : 2,3,4 ; VAP : 1,2,3,4,5,6,7,8	Allow Edit
Inter VLAN Group Routing		
VLAN IDs	**Members**	**Action**
☐ 1, ☐ 2		Edit

Inter VLAN Group Routing		
Item	**Value setting**	**Description**
VALN Group Internet Access Definition	All boxes are checked by default.	By default, all boxes are checked means all **VLAN ID** members are allow to access WAN interface. If uncheck a certain **VLAN ID** box, it means the VLAN ID member can't access Internet anymore. Note: **VLAN ID 1** is available always; it is the default VLAN ID of **LAN** rule. The other **VLAN IDs** are available only when they are enabled.
Inter VLAN Group Routing	The box is unchecked by default.	Click the expected VLAN IDs box to enable the Inter VLAN access function. By default, members in different VLAN IDs can't access each other. The gateway supports up to 4 rules for **Inter VLAN Group Routing.** For example, if ID_1 and ID_2 are checked, it means members in VLAN ID_1 can access members of VLAN ID_2, and vice versa.

Save	N/A	Click the **Save** button to save the configuration

Tag-based VLAN – Create/Edit VLAN Rules

The **Tag-based VLAN** allows you to customize each LAN port according to VLAN ID. There is a default rule shows the configuration of all LAN ports and all VAPs. Also, if your device has a DMZ port, you will see DMZ configuration, too. The router supports up to a maximum of 128 tag-based VLAN rule sets.

Tag-based VLAN List	Add	Delete			
VLAN ID	Internet	Port	VAP	DHCP Server	Actions
Native VLAN	☑	☑ 2 ☑ 3 ☑ 4	☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8	DHCP 1	Edit ☐ Select

When **Add** button is applied, **Tag-based VLAN Configuration** screen will appear.

Tag-based VLAN Configuration	
Item	Setting
▸ VLAN ID	0
▸ Internet Access	☑ Enable
▸ Port	☐ 2 ☐ 3 ☐ 4
▸ VAP	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8
▸ DHCP Server	DHCP 1 ▾
	Save

Tag-based VLAN Configuration		
Item	**Value setting**	**Description**
VALN ID	A Must filled setting	Define the **VLAN ID** number, range is 6~4094.
Internet Access	The box is checked by default.	Click **Enable** box to allow the members in the VLAN group access to internet.
Port	The box is unchecked by default.	Check the LAN port box(es) to join the VLAN group.
VAP	The box is unchecked by default.	Check the VAP box(es) to join the VLAN group. Note: Only the wireless gateway has the VAP list.
DHCP Server	**DHCP 1** is selected by default.	Select a **DHCP Server** to these members of this VLAN group. To create or edit DHCP server for VLAN, refer **to Basic Network > LAN & VLAN > DHCP Server**.
Save	N/A	Click **Save** button to save the configuration Note: After clicking **Save** button, always click **Apply** button to apply the settings.

Modbus Cellular Gateway

2.2.3 DHCP Server

➢ DHCP Server

The gateway supports up to 4 DHCP servers to fulfill the DHCP requests from different VLAN groups (please refer to VLAN section for getting more usage details). And there is one default setting for whose LAN IP Address is the same one of gateway LAN interface, with its default Subnet Mask setting as "255.255.255.0", and its default IP Pool ranges is from ".100" to ".200" as shown at the DHCP Server List page on gateway's WEB UI.
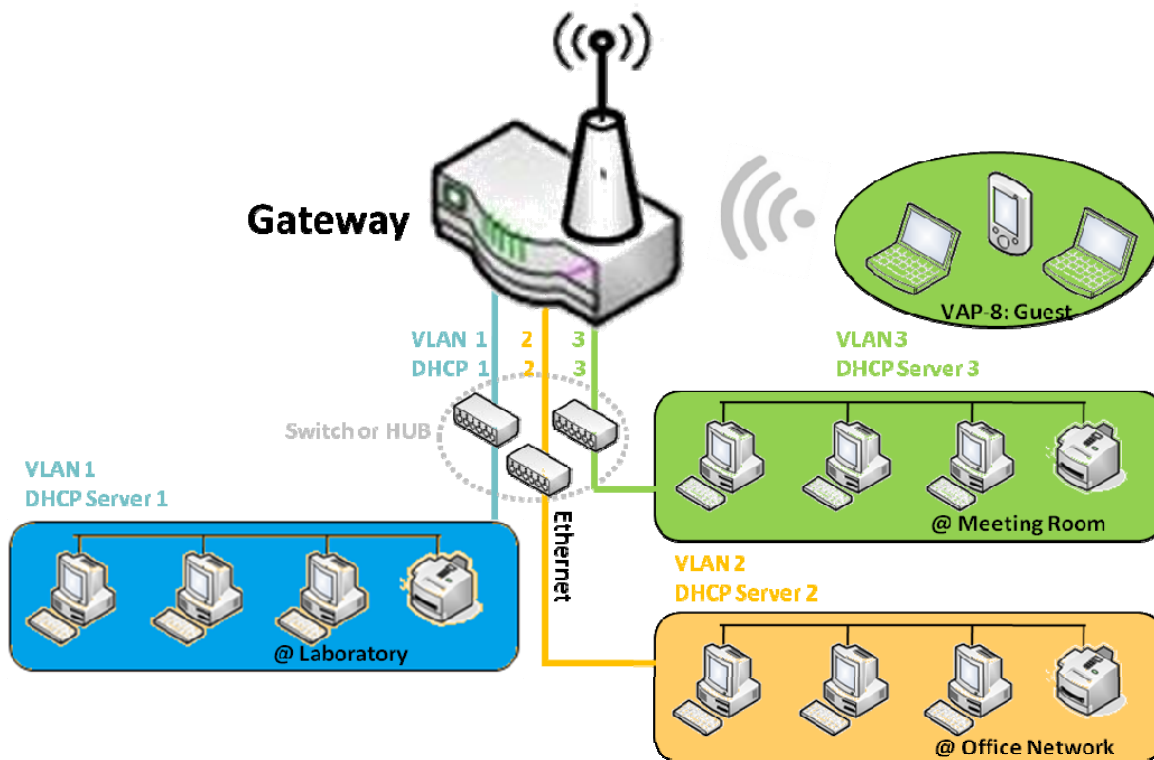
User can add more DHCP server configurations by clicking on the "Add" button behind "DHCP Server List", or clicking on the "Edit" button at the end of each DHCP Server on list to edit its current settings. Besides, user can select a DHCP Server and delete it by clicking on the "Select" check-box and the "Delete" button.

Modbus Cellular Gateway

➢ Fixed Mapping

User can assign fixed IP address to map the specific client MAC address by select them then copy, when targets were already existed in the **DHCP Client List**, or to add some other Mapping Rules by manually in advance, once the target's MAC address was not ready to connect.
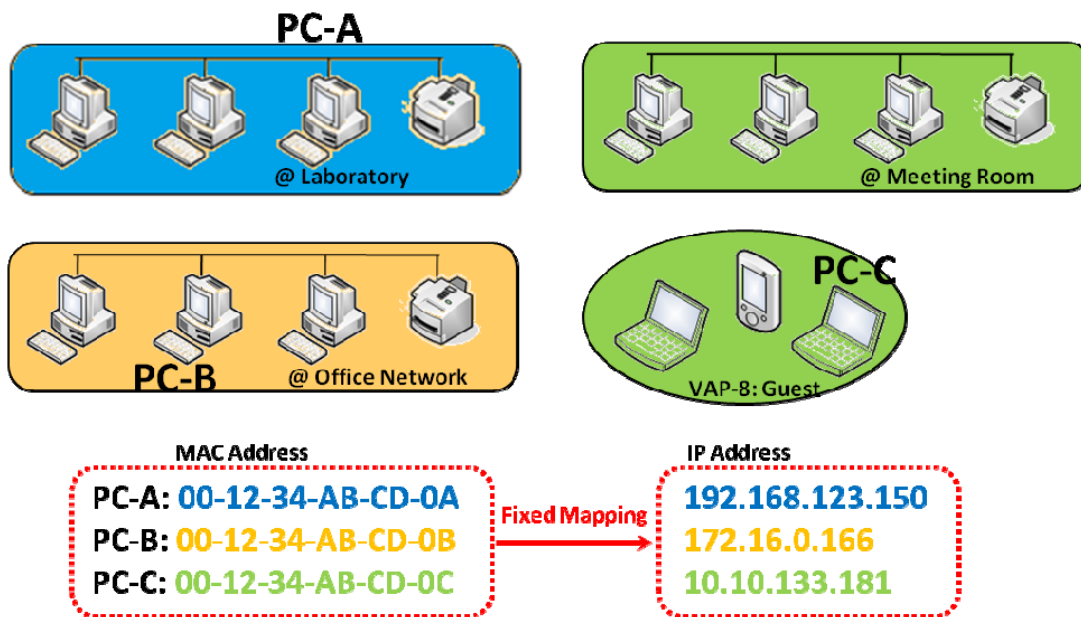
Modbus Cellular Gateway

DHCP Server Setting

Go to **Basic Network > LAN & VLAN > DHCP Server** Tab.

The DHCP Server setting allows user to create and customize DHCP Server policies to assign IP Addresses to the devices on the local area network (LAN).

Create / Edit DHCP Server Policy

The gateway allows you to custom your DHCP Server Policy. If multiple LAN ports are available, you can define one policy for each LAN (or VLAN group), and it supports up to a maximum of 4 policy sets.

DHCP Server Name	LAN IP Address	Subnet Mask	IP Pool	Lease Time	Domain Name	Primary DNS	Secondary DNS	Primary WINS	Secondary WINS	Gateway	Enable	Actions
DHCP 1	192.168.123.254	255.255.255.0	192.168.123.100-192.168.123.200	3600		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	☑	Edit Fixed Mapping

When **Add** button is applied, **DHCP Server Configuration** screen will appear.

DHCP Server Configuration	
Item	Setting
▶ DHCP Server Name	DHCP 2
▶ LAN IP Address	192.168.2.254
▶ Subnet Mask	255.0.0.0 (/8) ▼
▶ IP Pool	Starting Address: Ending Address:
▶ Lease Time	86400 seconds
▶ Domain Name	(Optional)
▶ Primary DNS	(Optional)
▶ Secondary DNS	(Optional)
▶ Primary WINS	(Optional)
▶ Secondary WINS	(Optional)
▶ Gateway	(Optional)
▶ Server	☐ Enable

Modbus Cellular Gateway

DHCP Server Configuration		
Item	**Value setting**	**Description**
DHCP Server Name	1. String format can be any text 2. A Must filled setting	Enter a DHCP Server name. Enter a name that is easy for you to understand.
LAN IP Address	1. IPv4 format. 2. A Must filled setting	The LAN IP Address of this DHCP Server.
Subnet Mask	255.0.0.0 (/8) is set by default	The Subnet Mask of this DHCP Server.
IP Pool	1. IPv4 format. 2. A Must filled setting	The IP Pool of this DHCP Server. It composed of Starting Address entered in this field and Ending Address entered in this field.
Lease Time	1. Numberic string format. 2. A Must filled setting	The Lease Time of this DHCP Server. ***Value Range:*** 300 ~ 604800 seconds.
Domain Name	String format can be any text	The Domain Name of this DHCP Server.
Primary DNS	IPv4 format	The Primary DNS of this DHCP Server.
Secondary DNS	IPv4 format	The Secondary DNS of this DHCP Server.
Primary WINS	IPv4 format	The Primary WINS of this DHCP Server.
Secondary WINS	IPv4 format	The Secondary WINS of this DHCP Server.
Gateway	IPv4 format	The Gateway of this DHCP Server.
Server	The box is unchecked by default.	Click **Enable** box to activate this DHCP Server.
Save	N/A	Click the **Save** button to save the configuration
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	N/A	When the **Back** button is clicked the screen will return to the DHCP Server Configuration page.

Create / Edit Mapping Rule List on DHCP Server

The router allows you to custom your Mapping Rule List on DHCP Server. It supports up to a maximum of 64 rule sets. When **Fix Mapping** button is applied, the **Mapping Rule List** screen will appear.

Mapping Rule List Add Delete			[Help]
MAC Address	**IP Address**	**Enable**	**Actions**

When **Add** button is applied, **Mapping Rule Configuration** screen will appear.

Modbus Cellular Gateway

Mapping Rule Configuration Item	Value setting	Description
MAC Address	1. MAC Address string format 2. A Must filled setting	The MAC Address of this mapping rule.
IP Address	1. IPv4 format. 2. A Must filled setting	The IP Address of this mapping rule.
Rule	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	N/A	When the **Back** button is clicked the screen will return to the **DHCP Server Configuration** page.

View / Copy DHCP Client List

When **DHCP Client List** button is applied, **DHCP Client List** screen will appear.

When the DHCP Client is selected and **Copy to Fixed Mapping** button is applied. The IP and MAC address of DHCP Client will apply to the Mapping Rule List on specific DHCP Server automatically.

Enable / Disable DHCP Server Options

The **DHCP Server Options** setting allows user to set **DHCP OPTIONS 66**, **72**, or **114**. Click the **Enable** button to activate the DHCP option function, and the DHCP Server will add the expected options in its sending out DHCPOFFER DHCPACK packages.

Option	Meaning	RFC
66	TFTP server name	[RFC 2132]
72	Default World Wide Web Server	[RFC 2132]
114	URL	[RFC 3679]

Create / Edit DHCP Server Options

The router supports up to a maximum of 99 option settings.

When **Add/Edit** button is applied, **DHCP Server Option Configuration** screen will appear.

DHCP Server Option Configuration		
Item	**Value setting**	**Description**
Option Name	1. String format can be any text 2. A Must filled setting.	Enter a DHCP Server Option name. Enter a name that is easy for you to understand.
DHCP Server Select	Dropdown list of all available DHCP servers.	Choose the DHCP server this option should apply to.
Option Select	1. A Must filled setting. 2. **Option 66** is selected by default.	Choose the specific option from the dropdown list. It can be **Option 66**, **Option 72**, or **Option 144**. **Option 66** for tftp; **Option 72** for www; **Option 144** for url.

Modbus Cellular Gateway

Type	Dropdown list of DHCP server option value's type	Each different options has different value types.		
		66	Single IP Address	
			Single FQDN	
		72	IP Addresses List, separated by ","	
		114	Single URL	
Value	1. IPv4 format 2. FQDN format 3. IP list 4. URL format 5. A Must filled setting	Should conform to Type :		
			Type	Value
		66	Single IP Address	IPv4 format
			Single FQDN	FQDN format
		72	IP Addresses List, separated by ","	IPv4 format, separated by ","
		114	Single URL	URL format
Enable	The box is unchecked by default.	Click **Enable** box to activate this setting.		
Save	NA	Click the **Save** button to save the setting.		
Undo	NA	When the **Undo** button is clicked the screen will return back with nothing changed.		

2.3 ~~WiFi~~ (not supported)

Not supported feature for the purchased product, leave it as blank.

Modbus Cellular Gateway

2.4 IPv6

The growth of the Internet has created a need for more addresses than are possible with IPv4. IPv6 (Internet Protocol version 6) is a version of the Internet Protocol (IP) intended to succeed IPv4, which is the protocol currently used to direct almost all Internet traffic. IPv6 also implements additional features not present in IPv4. It simplifies aspects of address assignment (stateless address auto-configuration), network renumbering and router announcements when changing Internet connectivity providers.

2.4.1 IPv6 Configuration
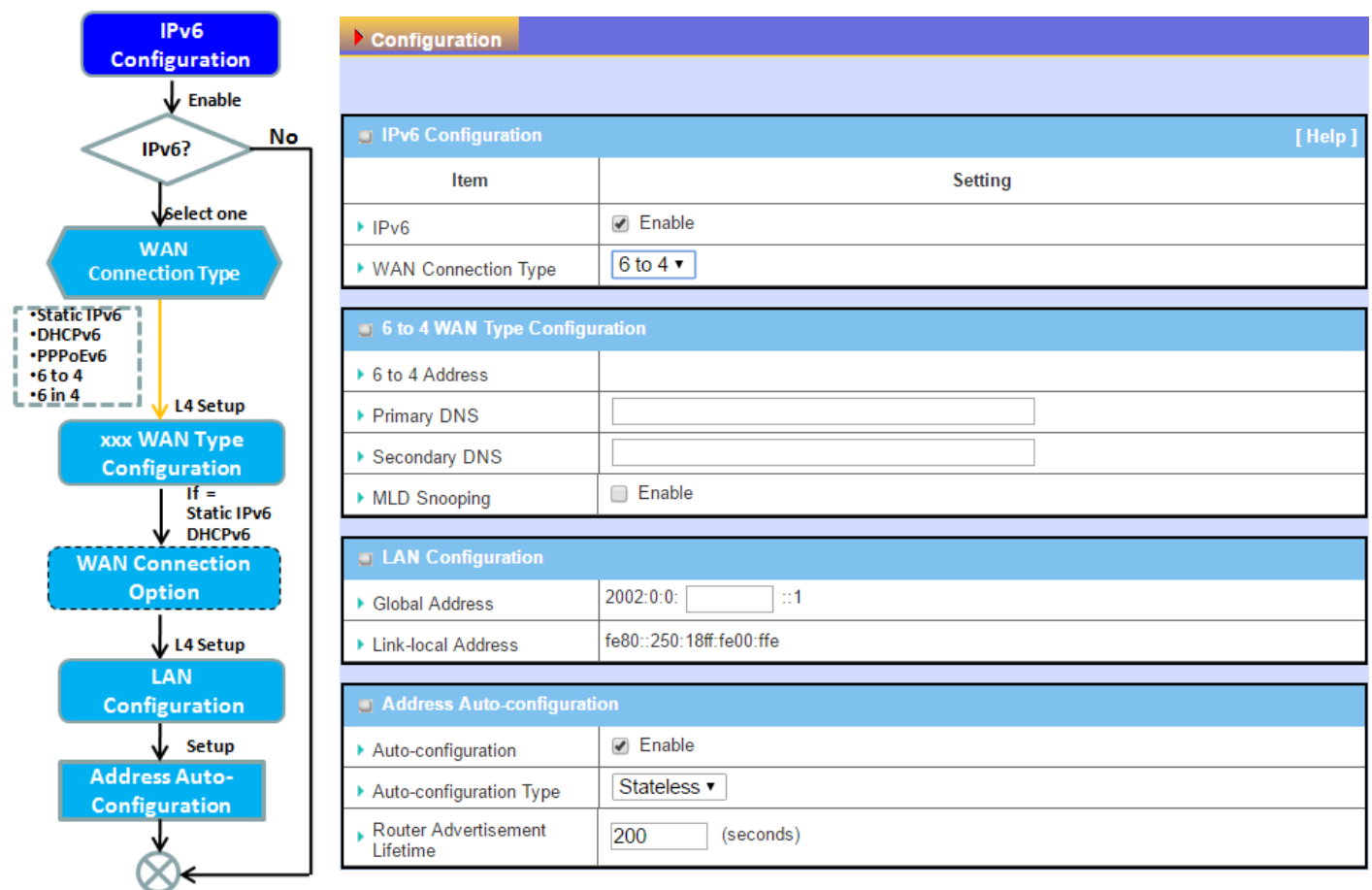
The **IPv6 Configuration** setting allows user to set the IPv6 connection type to access the IPv6 network. This gateway supports various types of IPv6 connection, including **Static IPv6**, **DHCPv6**, **PPPoEv6**, **6to4**, and **6in4**

Note: For the products just having 3G/4G WAN interface, only **6to4** and **6in4** are supported. Please contact your ISP for the IPv6 supports before you proceed with IPv6 setup.

Modbus Cellular Gateway

IPv6 WAN Connection Type

Static IPv6

Static IPv6 does the same function as static IPv4. The static IPv6 provides manual setting of IPv6 address, IPv6 default gateway address, and IPv6 DNS.
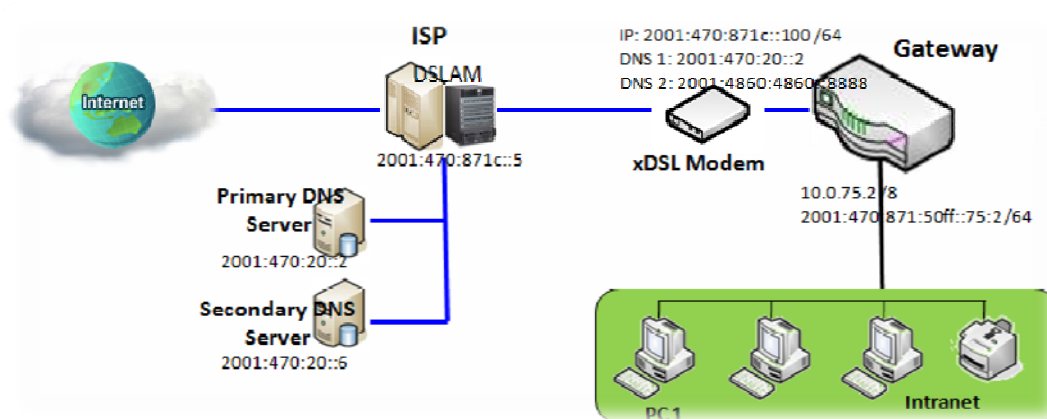
Above diagram depicts the IPv6 IP addressing, type in the information provided by your ISP to setup the IPv6 network.

DHCPv6

DHCP in IPv6 does the same function as DHCP in IPv4. The DHCP server sends IP address, DNS server addresses and other possible data to the DHCP client to configure automatically. The server also sends a lease time of the address and time to re-contact the server for IPv6 address renewal. The client has then to resend a request to renew the IPv6 address.
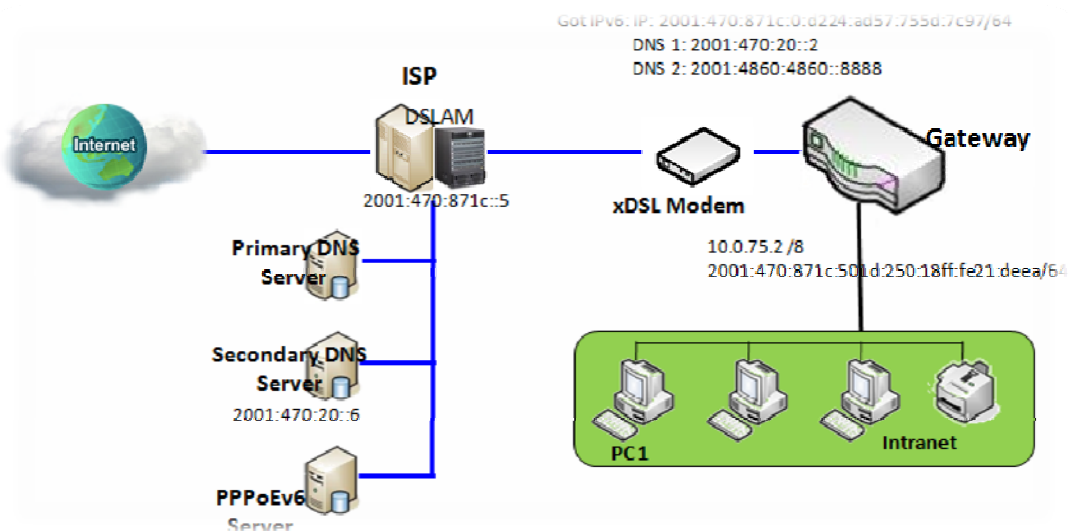
Modbus Cellular Gateway

Above diagram depicts DHCP IPv6 IP addressing, the DHCPv6 server on the ISP side assigns IPv6 address, IPv6 default gateway address, and IPv6 DNS to client host's automatically.

PPPoEv6

PPPoEv6 in IPv6 does the same function as PPPoE in IPv4. The PPPoEv6 server provides configuration parameters based on PPPoEv6 client request. When PPPoEv6 server gets client request and successfully authenticates it, the server sends IP address, DNS server addresses and other required parameters to automatically configure the client.
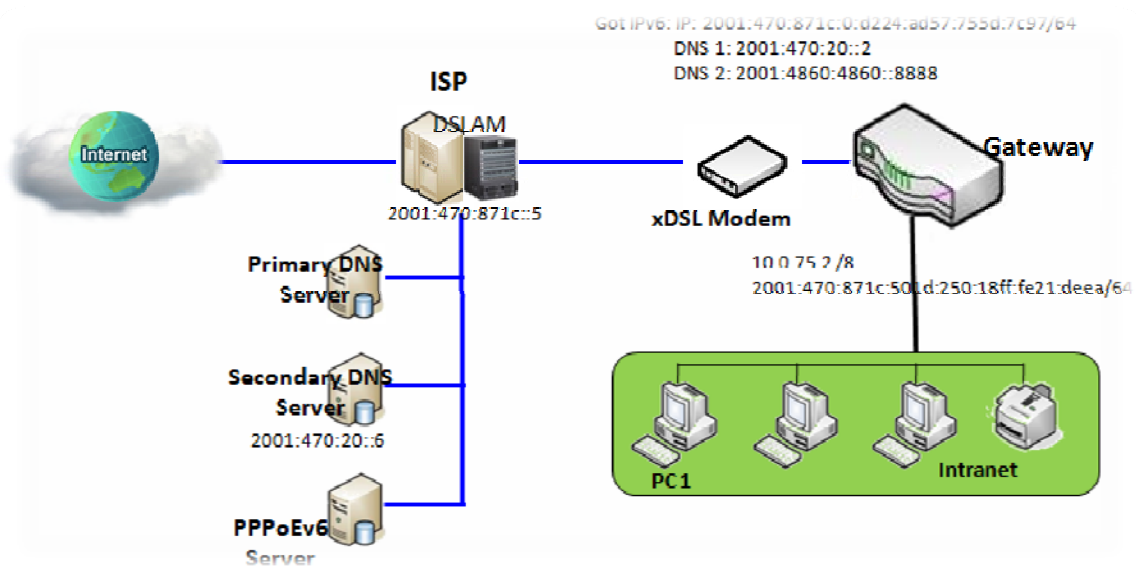
The diagram above depicts the IPv6 addressing through PPPoE, PPPoEv6 server (DSLAM) on the ISP side provides IPv6 configuration upon receiving PPPoEv6 client request. When PPPoEv6 server gets client request and successfully authenticates it, the server sends IP address, DNS server addresses and other required parameters to automatically configure the client.

6to4

6to4 is one mechanism to establish automatic IPv6 in IPv4 tunnels and to enable complete IPv6 sites communication. The only thing a 6to4 user needs is a global IPv4 address.

6to4 may be used by an individual host, or by a local IPv6 network. When used by a host, it must have a global IPv4 address connected, and the host is responsible for encapsulation of outgoing IPv6 packets and decapsulation of incoming 6to4 packets. If the host is configured to forward packets for other clients, often a local network, it is then a router.

Modbus Cellular Gateway
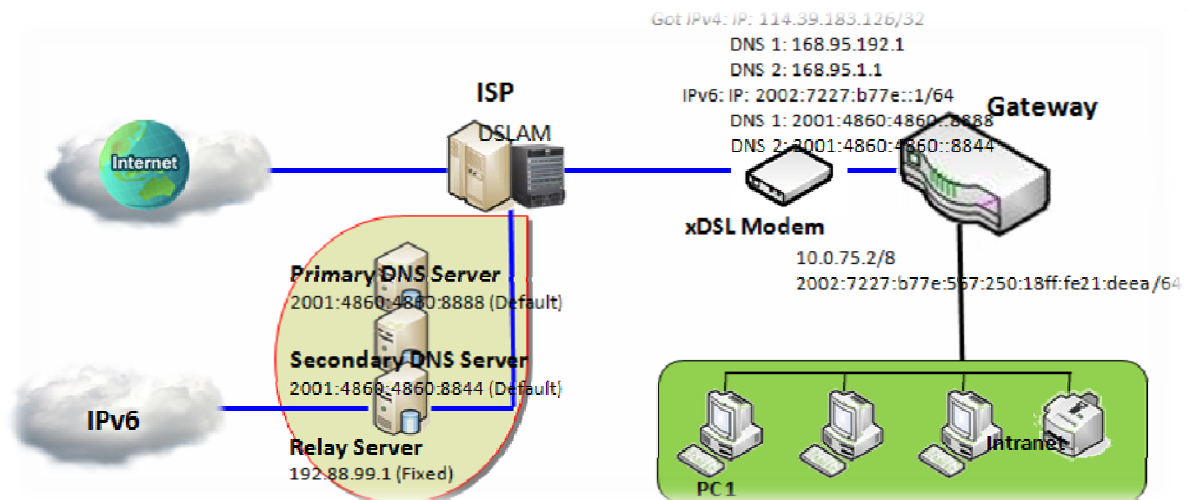
In above diagram, the 6to4 means no need to set gateway address "automatic" tunneling solution. The automatic mean have relay server, as defined in RFC 3068 has included segments draw 192.88.99.0/24 used as 6to4 relay of any-cast address to complete 6in4 setting.

6in4

6in4 is an Internet transition mechanism for Internet IPv4 to IPv6 migration. 6in4 uses tunneling to encapsulate IPv6 traffic over explicitly-configured IPv4 links. As defined in RFC 4213, the 6in4 traffic is sent over the IPv4 Internet inside IPv4 packets whose IP headers have the IP protocol number set to 41. This protocol number is specifically designated for IPv6 encapsulation.
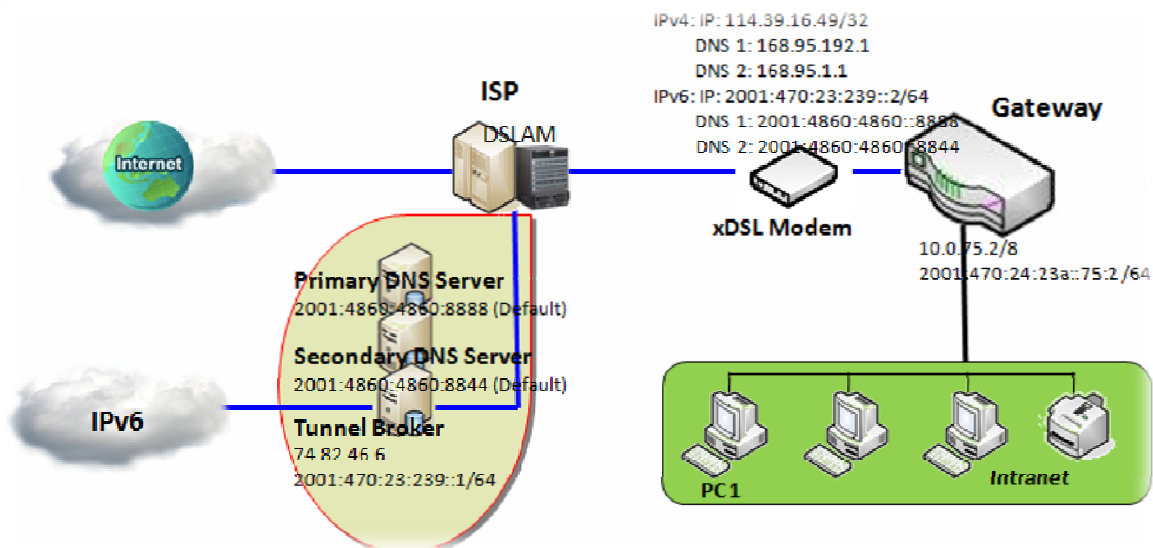
In above diagram, the 6in4 usually needs to register to a 6in4 tunnel service, known as Tunnel Broker, in order to use. It also need end point global IPv4 address as 114.39.16.49 to complete 6in4 setting.

Modbus Cellular Gateway

IPv6 Configuration Setting

Go to Basic Network > IPv6 > Configuration Tab.

The **IPv6 Configuration** setting allows user to set the IPv6 connection type to access the IPv6 network.

IPv6 Configuration	[Help]
Item	**Setting**
▶ IPv6	☑ Enable
▶ WAN Connection Type	DHCPv6 ▼

IPv6 Configuration Item	Value setting	Description
IPv6	The box is unchecked by default,	Check the **Enable** box to activate the IPv6 function.
WAN Connection Type	1. Only can be selected when IPv6 Enable 2. A Must filled setting	Define the selected IPv6 WAN Connection Type to establish the IPv6 connectivity. Select **Static IPv6** when your ISP provides you with a set IPv6 addresses. Then go to **Static IPv6 WAN Type Configuration**. Select **DHCPv6** when your ISP provides you with DHCPv6 services. Select **PPPoEv6** when your ISP provides you with PPPoEv6 account settings. Select **6to4** when you want to user IPv6 connection over IPv4. Select **6in4** when you want to user IPv6 connection over IPv4. **Note**: For the products just having 3G/4G WAN interface, only **6to4** and **6in4** are supported.

Static IPv6 WAN Type Configuration

Static IPv6 WAN Type Configuration	
▶ IPv6 Address	
▶ Subnet Prefix Length	
▶ Default Gateway	
▶ Primary DNS	
▶ Secondary DNS	
▶ MLD Snooping	☐ Enable

Modbus Cellular Gateway

Static IPv6 WAN Type Configuration		
Item	**Value setting**	**Description**
IPv6 Address	A Must filled setting	Enter the WAN **IPv6 Address** for the router.
Subnet Prefix Length	A Must filled setting	Enter the WAN **Subnet Prefix Length** for the router.
Default Gateway	A Must filled setting	Enter the WAN **Default Gateway** IPv6 address.
Primary DNS	An optional setting	Enter the WAN **primary DNS Server**.
Secondary DNS	An optional setting	Enter the WAN **secondary DNS Server**.
MLD Snooping	The box is unchecked by default	Enable/Disable the MLD Snooping function

LAN Configuration

LAN Configuration		
Item	**Value setting**	**Description**
Global Address	A Must filled setting	Enter the LAN **IPv6 Address** for the router.
Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

Then go to **Address Auto-configuration (summary)** for setting LAN environment.

If above setting is configured, click the **Save** button to save the configuration, and click the **Reboot** button to reboot the router.

Modbus Cellular Gateway

DHCPv6 WAN Type Configuration

DHCPv6 WAN Type Configuration Item	Value setting	Description
DNS	The option [From Server] is selected by default	Select the [Specific DNS] option to active Primary DNS and Secondary DNS. Then fill the DNS information.
Primary DNS	Can not modified by default	Enter the WAN **primary DNS Server**.
Secondary DNS	Can not modified by default	Enter the WAN **secondary DNS Server**.
MLD	The box is unchecked by default	Enable/Disable the MLD Snooping function

LAN Configuration

LAN Configuration Item	Value setting	Description
Global Address	Value auto-created	Enter the LAN **IPv6 Address** for the router.
Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

Then go to **Address Auto-configuration (summary)** for setting LAN environment.

If above setting is configured, click the **Save** button to save the configuration, and click **Reboot** button to reboot the router.

Modbus Cellular Gateway

PPPoEv6 WAN Type Configuration

PPPoEv6 WAN Type Configuration		
Item	**Value setting**	**Description**
Account	A Must filled setting	Enter the Account for setting up PPPoEv6 connection. If you want more information, please contact your ISP. ***Value Range***: 0 ~ 45 characters.
Password	A Must filled setting	Enter the Password for setting up PPPoEv6 connection. If you want more information, please contact your ISP.
Service Name	A Must filled setting/Option	Enter the Service Name for setting up PPPoEv6 connection. If you want more information, please contact your ISP. ***Value Range***: 0 ~ 45 characters.
Connection Control	Fixed value	The value is **Auto-reconnect(Always on)**.
MTU	A Must filled setting	Enter the MTU for setting up PPPoEv6 connection. If you want more information, please contact your ISP. ***Value Range***: 1280 ~ 1492.
MLD Snooping	The box is unchecked by default	Enable/Disable the MLD Snooping function

LAN Configuration

LAN Configuration		
Item	**Value setting**	**Description**
Global Address	Value auto-created	The LAN **IPv6 Address** for the router.
Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

Then go to **Address Auto-configuration (summary)** for setting LAN environment.

Modbus Cellular Gateway

If above setting is configured, click the **save button** to save the configuration and click **reboot button** to reboot the router.

6to4 WAN Type Configuration

6to4 WAN Type Configuration		
Item	**Value setting**	**Description**
6to4 Address	Value auto-created	IPv6 address for access the IPv6 network.
Primary DNS	An optional setting	Enter the WAN primary DNS Server.
Secondary DNS	An optional setting	Enter the WAN secondary DNS Server.
MLD	The box is unchecked by default	Enable/Disable the MLD Snooping function

LAN Configuration

LAN Configuration		
Item	**Value setting**	**Description**
Global Address	An optional setting	Enter the LAN **IPv6 Address** for the router. *Value Range*: 0 ~ FFFF.
Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

Then go to **Address Auto-configuration (summary)** for setting LAN environment.

If above setting is configured, click the **save button** to save the configuration and click **reboot button** to reboot the router.

Modbus Cellular Gateway

6in4 WAN Type Configuration

Please go to find IPv6 tunnel brokers to establish 6in4 tunnel. (You can find List of IPv6 tunnel brokers that support 6in4 service from wiki.)

Then enter the **Local IPv4 address** of router into **Client IPv4 Address** field in IPv6 tunnel broker setting page.

6in4 WAN Type Configuration		
Item	**Value setting**	**Description**
Remote IPv4 Address	A Must filled setting	Filled **Server IPv4 Address** gotten from tunnel broker in this field.
Local IPv4 Address	Value auto-created	IPv4 address of this router.
Local IPv6 Address	A Must filled setting	Filled **Client IPv6 Address** gotten from tunnel broker in this field.
Primary DNS	An optional setting	Enter the WAN primary DNS Server.
Secondary DNS	An optional setting	Enter the WAN secondary DNS Server.
MLD	The box is unchecked by default	Enable/Disable the MLD Snooping function

LAN Configuration

LAN Configuration		
Item	**Value setting**	**Description**
Global Address	A Must filled setting	Filled **Routed /64** gotten from tunnel broker in this field.
Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

Then go to **Address Auto-configuration (summary)** for setting LAN environment.
If above setting is configured, click the **save button** to save the configuration and click **reboot button** to reboot the router.

Modbus Cellular Gateway

Address Auto-configuration

Address Auto-configuration	
▶ Auto-configuration	☑ Enable
▶ Auto-configuration Type	Stateless ▼
▶ Router Advertisement Lifetime	200 (seconds)

Address Auto-configuration	
▶ Auto-configuration	☑ Enable
▶ Auto-configuration Type	Stateful ▼
▶ IPv6 Address Range(Start)	XXX:: [ ] /64
▶ IPv6 Address Range(End)	XXX:: [ ] /64
▶ IPv6 Address Lifetime	[ ] (seconds)

Address Auto-configuration		
Item	**Value setting**	**Description**
Auto-configuration	The box is unchecked by default	Check to enable the Auto configuration feature.
Auto-configuration Type	1. Only can be selected when **Auto-configuration** enabled 2. Stateless is selected by default	Define the selected IPv6 WAN Connection Type to establish the IPv6 connectivity. Select **Stateless** to manage the Local Area Network to be SLAAC + RDNSS **Router Advertisement Lifetime** (A Must filled setting): Enter the Router Advertisement Lifetime (in seconds). 200 is set by default. *Value Range*: 0 ~ 65535. Select **Stateful** to manage the Local Area Network to be **Stateful (DHCPv6)**. **IPv6 Address Range (Start)** (A Must filled setting): Enter the start IPv6 Address for the DHCPv6 range for your local computers. 0100 is set by default. *Value Range*: 0001 ~ FFFF. **IPv6 Address Range (End)** (A Must filled setting): Enter the end IPv6 Address for the DHCPv6 range for your local computers. 0200 is set by default. *Value Range*: 0001 ~ FFFF. **IPv6 Address Lifetime** (A Must filled setting): Enter the DHCPv6 lifetime for your local computers. 36000 is set by default. *Value Range*: 0 ~ 65535.

2.5 Port Forwarding

Network address translation (NAT) is a methodology of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device. The technique was originally used for ease of rerouting traffic in IP networks without renumbering every host. It has become a popular and essential tool in conserving global address space allocations in face of IPv4 address exhaustion. The product you purchased embeds and activates the NAT function. You also can disable the NAT function in **[Basic Network]-[WAN & Uplink]-[Internet Setup]-[WAN Type Configuration]** page.
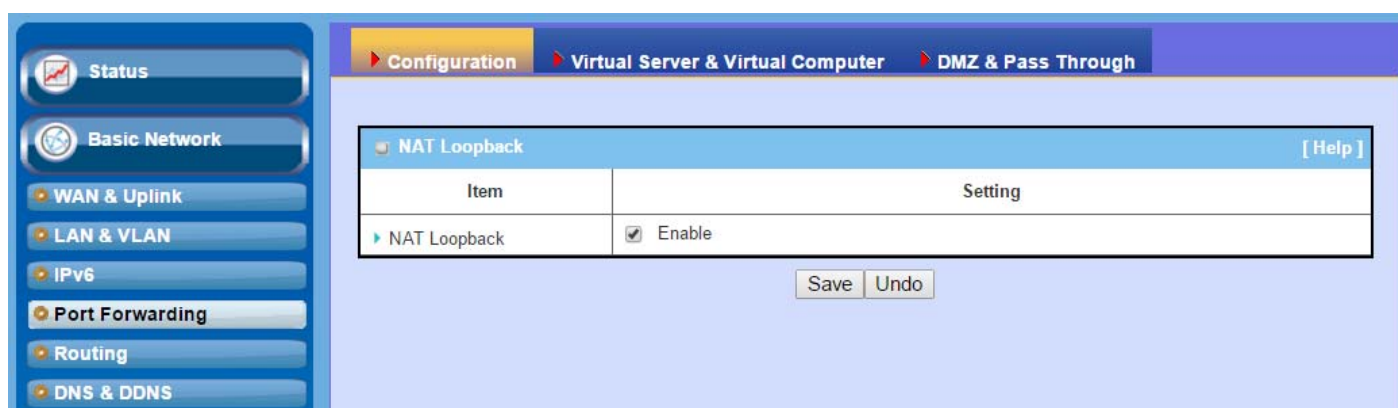
Usually all local hosts or servers behind corporate gateway are protected by NAT firewall. NAT firewall will filter out unrecognized packets to protect your Intranet. So, all local hosts are invisible to the outside world. Port forwarding or port mapping is function that redirects a communication request from one address and port number combination to assigned one. This technique is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the gateway (external network), by remapping the destination IP address and port number

There are several optional Port Forwarding related functions in this gateway. They are Virtual Server, Virtual Computer, IP Translation, Special AP & ALG, DMZ and Pass Through, etc. The available functions might be different for the purchased model.

Modbus Cellular Gateway

2.5.1 Configuration

NAT Loopback

This feature allows you to access the WAN global IP address from your inside NAT local network. It is useful when you run a server inside your network. For example, if you set a mail server at LAN side, your local devices can access this mail server through gateway's global IP address when enable NAT loopback feature. On either side are you in accessing the email server, at the LAN side or at the WAN side, you don't need to change the IP address of the mail server.

Configuration Setting

Go to Basic Network > Port Forwarding > Configuration tab.

The NAT Loopback allows user to access the WAN IP address from inside your local network.

Enable NAT Loopback

NAT Loopback		[Help]
Item	**Setting**	
▶ NAT Loopback	☑ Enable	

Configuration Item	Value setting	Description
NAT Loopback	The box is checked by default	Check the **Enable** box to activate this NAT function
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the settings

2.5.2 Virtual Server & Virtual Computer

Configuration	
Item	**Setting**
▶ Virtual Server	☑ Enable
▶ Virtual Computer	☑ Enable

Virtual Server List [Add] [Delete]

ID	WAN Interface	Server IP	Protocol	Public Port	Private Port	Time Schedule	Enable	Actions
1	All	10.0.75.101	TCP(6) & UDP(17)	25	25	(0) Always	☑	[Edit] ☐ Select
2	All	10.0.75.101	TCP(6) & UDP(17)	110	110	(0) Always	☑	[Edit] ☐ Select

Virtual Computer List [Add] [Delete]

ID	Global IP	Local IP	Enable	Actions
1	118.18.81.44	10.0.75.102	☑	[Edit] ☐ Select

There are some important Pot Forwarding functions implemented within the gateway, including "Virtual Server", "NAT loopback" and "Virtual Computer".

It is necessary for cooperate staffs who travel outside and want to access various servers behind office gateway. You can set up those servers by using "Virtual Server" feature. After trip, if want to access those servers from LAN side by global IP, without change original setting, NAT Loopback can achieve it.

"Virtual computer" is a host behind NAT gateway whose IP address is a global one and is visible to the outside world. Since it is behind NAT, it is protected by gateway firewall. To configure Virtual Computer, you just have to map the local IP of the virtual computer to a global IP.

Modbus Cellular Gateway

Virtual Server & NAT Loopback
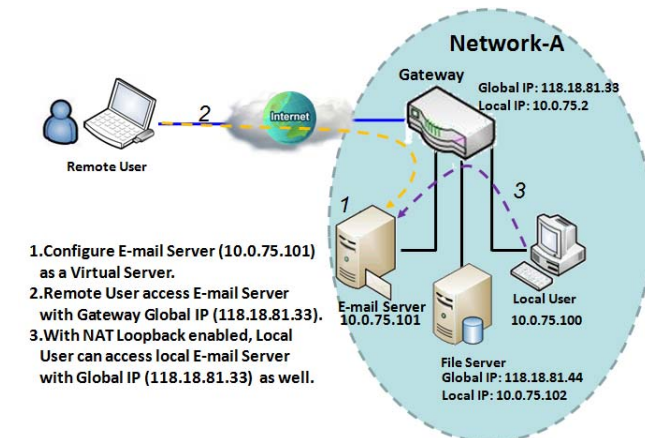
"Virtual Server" allows you to access servers with the global IP address or FQDN of the gateway as if they are servers existed in the Internet. But in fact, these servers are located in the Intranet and are physically behind the gateway. The gateway serves the service requests by port forwarding the requests to the LAN servers and transfers the replies from LAN servers to the requester on the WAN side. As shown in example, an E-mail virtual server is defined to be located at a server with IP address 10.0.75.101 in the Intranet of Network-A, including SMTP service port 25 and POP3 service port 110. So, the remote user can access the E-mail server with the gateway's global IP 118.18.81.33 from its WAN side. But the real E-mail server is located at LAN side and the gateway is the port forwarder for E-mail service.

NAT Loopback allows you to access the WAN global IP address from your inside NAT local network. It is useful when you run a server inside your network. For example, if you set a mail server at LAN side, your local devices can access this mail server through gateway's global IP address when enable NAT loopback feature. On either side are you in accessing the email server, at the LAN side or at the WAN side, you don't need to change the IP address of the mail server.

Virtual Computer
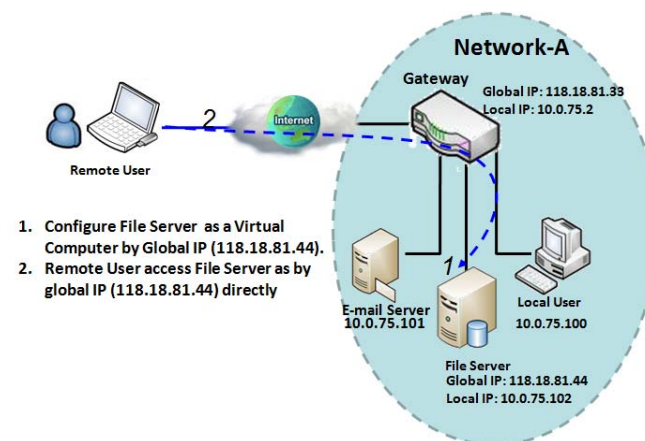
"Virtual Computer" allows you to assign LAN hosts to global IP addresses, so that they can be visible to outside world. While so, they are also protected by the gateway firewall as being client hosts in the Intranet. For example, if you set a FTP file server at LAN side with local IP address 10.0.75.102 and global IP address 118.18.82.44, a remote user can access the file server while it is hidden behind the NAT gateway. That is because the gateway takes care of all accessing to the IP address 118.18.82.44, including to forward the access requests to the file server and to send the replies from the server to outside world.

Modbus Cellular Gateway

Virtual Server & Virtual Computer Setting

Go to **Basic Network > Port Forwarding > Virtual Server & Virtual Computer** tab.

Enable Virtual Server and Virtual Computer

Configuration	
Item	**Setting**
▶ Virtual Server	☑ Enable
▶ Virtual Computer	☑ Enable

Configuration Item	Value setting	Description
Virtual Server	The box is unchecked by default	Check the **Enable** box to activate this port forwarding function
Virtual Computer	The box is checked by default	Check the **Enable** box to activate this port forwarding function
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the settings.

Create / Edit Virtual Server

The gateway allows you to custom your Virtual Server rules. It supports up to a maximum of 20 rule-based Virtual Server sets.

ID	WAN Interface	Server IP	Protocol	Public Port	Private Port	Time Schedule	Enable	Actions

Virtual Server List [Add] [Delete]

When **Add** button is applied, **Virtual Server Rule Configuration** screen will appear.

Modbus Cellular Gateway

Virtual Server Rule Configuration		
Item	**Value setting**	**Description**
WAN Interface	1. A Must filled setting 2. Default is **ALL**.	Define the selected interface to be the packet-entering interface of the gateway. If the packets to be filtered are coming from **WAN-x** then select **WAN-x** for this field. Select **ALL** for packets coming into the gateway from any interface. It can be selected **WAN-x** box when **WAN-x** enabled. **Note**: The available check boxes (**WAN-1** ~ **WAN-4**) depend on the number of WAN interfaces for the product.
Server IP	A Must filled setting	This field is to specify the IP address of the interface selected in the WAN Interface setting above.
Protocol	A Must filled setting	When **"ICMPv4"** is selected It means the option "Protocol" of packet filter rule is ICMPv4. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. (refer to **Scheduling setting** under **Object Definition**) Then check **Enable** box to enable this rule. When **"TCP"** is selected It means the option "Protocol" of packet filter rule is TCP. **Public Port** selected a predefined port from **Well-known Service**, and **Private Port** is the same with **Public Port** number. **Public Port** is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number. **Public Port** is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**. *Value Range*: 1 ~ 65535 for Public Port, Private Port. When **"UDP"** is selected It means the option "Protocol" of packet filter rule is UDP.

		Public Port selected a predefined port from **Well-known Service**, and **Private Port** is the same with **Public Port** number. **Public Port** is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number. **Public Port** is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**. *Value Range*: 1 ~ 65535 for Public Port, Private Port. When **"TCP & UDP"** is selected It means the option "Protocol" of packet filter rule is TCP and UDP. **Public Port** selected a predefined port from **Well-known Service**, and **Private Port** is the same with **Public Port** number. **Public Port** is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number. **Public Port** is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**. *Value Range*: 1 ~ 65535 for Public Port, Private Port. When **"GRE"** is selected It means the option "Protocol" of packet filter rule is GRE.
		When **"ESP"** is selected It means the option "Protocol" of packet filter rule is ESP. When **"SCTP"** is selected It means the option "Protocol" of packet filter rule is SCTP. When **"User-defined"** is selected It means the option "Protocol" of packet filter rule is User-defined. For **Protocol Number**, enter a port number.
Time Schedule	1. An optional filled setting 2. **(0)Always** Is selected by default.	Apply Time Schedule to this rule; otherwise leave it as (0)Always. (refer to Scheduling setting under Object Definition)
Rule	1. An optional filled setting 2.The box is unchecked by default.	Check the Enable box to activate the rule.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the settings.
Back	N/A	When the **Back** button is clicked the screen will return to previous page.

Modbus Cellular Gateway

Create / Edit Virtual Computer

The gateway allows you to custom your Virtual Computer rules. It supports up to a maximum of 20 rule-based Virtual Computer sets.

When **Add** button is applied, **Virtual Computer Rule Configuration** screen will appear.

Virtual Computer Rule Configuration		
Item	**Value setting**	**Description**
Global IP	A Must filled setting	This field is to specify the IP address of the WAN IP.
Local IP	A Must filled setting	This field is to specify the IP address of the LAN IP.
Enable	N/A	Then check **Enable** box to enable this rule.
Save	N/A	Click the **Save** button to save the settings.

2.5.3 DMZ & Pass Through

DMZ (De Militarized Zone) Host is a host that is exposed to the Internet cyberspace but still within the protection of firewall by gateway device. So, the function allows a computer to execute 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications. In some cases when a specific application is blocked by NAT mechanism, you can indicate that LAN computer as a DMZ host to solve this problem.

The DMZ function allows you to ask the gateway pass through all normal packets to the DMZ host behind the NAT gateway only when these packets are not expected to receive by applications in the gateway or by other client hosts in the Intranet. Certainly, the DMZ host is also protected by the gateway firewall. Activate the feature and specify the DMZ host with a host in the Intranet when needed.

Configuration	[Help]
Item	**Setting**
▸ DMZ	☑ Enable ☑ All ☐ WAN-1 ☐ WAN-2 DMZ Host : 10.0.75.100
▸ Pass Through Enable	☑ IPSec ☑ PPTP ☑ L2TP

DMZ Scenario

Global IP:118.18.81.33
Local IP: 10.0.75.2
Gateway
Remote User 2
3
1
DMZ Host
10.0.75.100

1.Set X Server as DMZ Host
2.Request X server service by Gateway Global IP
3.Gateway redirect service request to DMZ host:
10.0.75.100
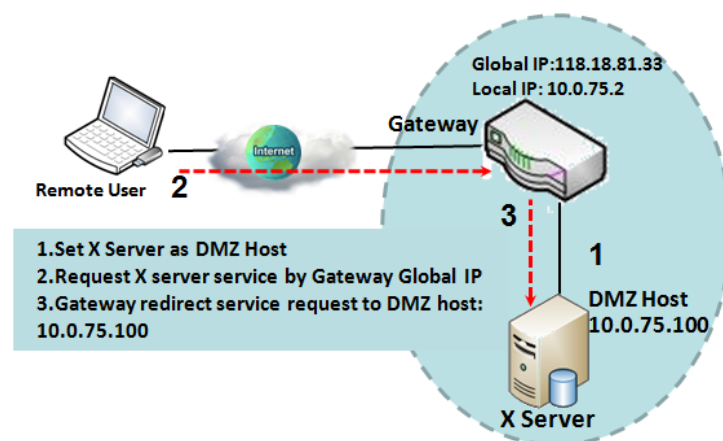
X Server

When the network administrator wants to set up some service daemons in a host behind NAT gateway to allow remote users request for services from server actively, you just have to configure this host as DMZ Host. As shown in the diagram, there is an X server installed as DMZ host, whose IP address is 10.0.75.100. Then, remote user can request services from X server just as it is provided by the gateway whose global IP address is 118.18.81.33. The gateway will forward those packets, not belonging to any configured virtual server or applications, directly to the DMZ host.

Modbus Cellular Gateway

VPN Pass through Scenario
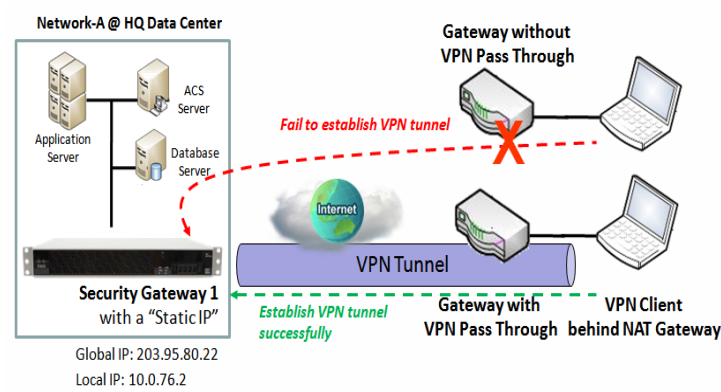
Since VPN traffic is different from that of TCP or UDP connection, it will be blocked by NAT gateway. To support the pass through function for the VPN connections initiating from VPN clients behind NAT gateway, the gateway must implement some kind of VPN pass through function for such application. The gateway support the pass through function for IPSec, PPTP, and L2TP connections, you just have to check the corresponding checkbox to activate it.

DMZ & Pass Through Setting

Go to **Basic Network > Port Forwarding > DMZ & Pass Through** tab.

The DMZ host is a host that is exposed to the Internet cyberspace but still within the protection of firewall by gateway device.

Enable DMZ and Pass Through

Configuration Item	Value setting	Description
DMZ	1. A Must filled setting 2. Default is **ALL**.	Check the **Enable** box to activate the DMZ function Define the selected interface to be the packet-entering interface of the gateway, and fill in the IP address of Host LAN IP in **DMZ Host** field . If the packets to be filtered are coming from **WAN-x** then select **WAN-x** for this field.

Modbus Cellular Gateway

		Select **ALL** for packets coming into the router from any interfaces. It can be selected **WAN-x** box when **WAN-x** enabled. **Note**: The available check boxes (**WAN-1** ~ **WAN-4**) depend on the number of WAN interfaces for the product.
Pass Through Enable	The boxes are checked by default	Check the box to enable the pass through function for the **IPSec**, **PPTP**, and **L2TP**. With the pass through function enabled, the VPN hosts behind the gateway still can connect to remote VPN servers.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the settings

Modbus Cellular Gateway

2.6 Routing

If you have more than one router and subnet, you will need to enable routing function to allow packets to find proper routing path and allow different subnets to communicate with each other. Routing is the process of selecting best paths in a network. It is performed for many kinds of networks, like electronic data networks (such as the Internet), by using packet switching technology. The routing process usually directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing. Most routing algorithms use only one network path at a time.

The routing tables record your pre-defined routing paths for some specific destination subnets. It is **static routing**. However, if the contents of routing tables record the obtained routing paths from neighbor routers by using some protocols, such as RIP, OSPF and BGP. It is **dynamic routing**. These both routing approaches will be illustrated one after one. In addition, the gateway also built in one advanced configurable routing software Quagga for more complex routing applications, you can configure it if required via Telnet CLI.

Modbus Cellular Gateway

2.6.1 Static Routing
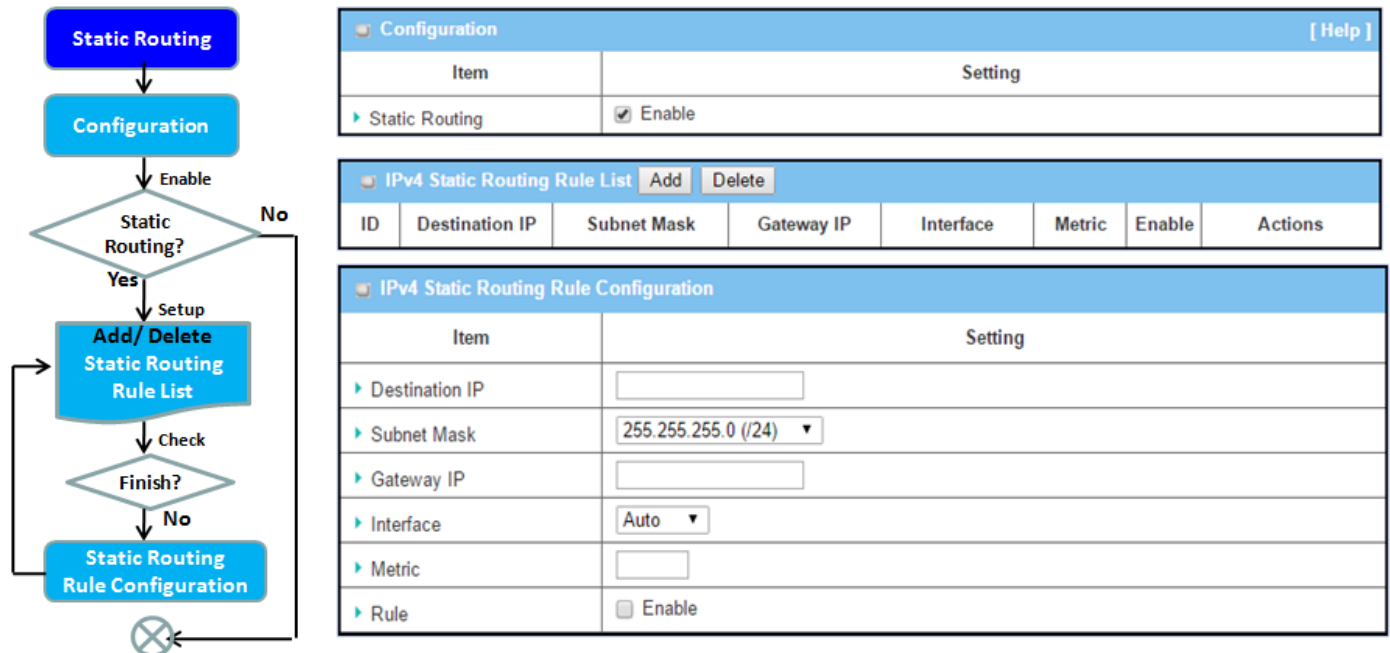
"Static Routing" function lets you define the routing paths for some dedicated hosts/servers or subnets to store in the routing table of the gateway. The gateway routes incoming packets to different peer gateways based on the routing table. You need to define the static routing information in gateway routing rule list.
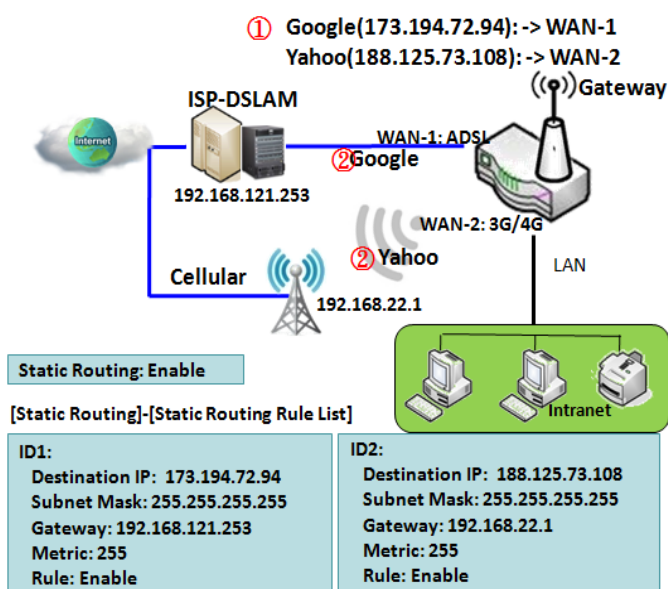
When the administrator of the gateway wants to specify what kinds of packets to be transferred via which gateway interface and which peer gateway to their destination. It can be carried out by the "Static Routing" feature. Dedicated packet flows from the Intranet will be routed to their destination via the pre-defined peer gateway and corresponding gateway interface that are defined in the system routing table by manual.

As shown in the diagram, when the destination is Google access, rule 1 set interface as ADSL, routing gateway as IP-DSLAM gateway 192.168.121.253. All the packets to Google will go through WAN-1. And the same way applied to rule 2 of access Yahoo. Rule 2 sets 3G/4G as interface.

Modbus Cellular Gateway

Static Routing Setting

Go to **Basic Network** > **Routing** > **Static Routing** Tab.

There are three configuration windows for static routing feature, including "Configuration", "Static Routing Rule List" and "Static Routing Rule Configuration" windows. "Configuration" window lets you activate the global static routing feature. Even there are already routing rules, if you want to disable routing temporarily, just uncheck the Enable box to disable it. "Static Routing Rule List" window lists all your defined static routing rule entries. Using "Add" or "Edit" button to add and create one new static routing rule or to modify an existed one.

When "**Add**" or "**Edit**" button is applied, the "Static Routing Rule Configuration" window will appear to let you define a static routing rule.

Enable Static Routing

Just check the **Enable** box to activate the "Static Routing" feature.

Configuration	[Help]
Item	**Setting**
▶ Static Routing	☑ Enable

Static Routing

Item	Value setting	Description
Static Routing	The box is unchecked by default	Check the **Enable** box to activate this function

Create / Edit Static Routing Rules

The Static Routing Rule List shows the setup parameters of all static routing rule entries. To configure a static routing rule, you must specify related parameters including the destination IP address and subnet mask of dedicated host/server or subnet, the IP address of peer gateway, the metric and the rule activation.

IPv4 Static Routing Rule List Add Delete						
ID	Destination IP	Subnet Mask	Gateway IP	Interface	Metric	Enable	Actions

The gateway allows you to custom your static routing rules. It supports up to a maximum of 64 rule sets. When

Modbus Cellular Gateway

Add button is applied, **Static Routing Rule Configuration** screen will appear, while the **Edit** button at the end of each static routing rule can let you modify the rule.

IPv4 Static Routing Rule Configuration	
Item	**Setting**
▶ Destination IP	[ ]
▶ Subnet Mask	255.255.255.0 (/24) ▼
▶ Gateway IP	[ ]
▶ Interface	Auto ▼
▶ Metric	[ ]
▶ Rule	☐ Enable

IPv4 Static Routing		
Item	**Value setting**	**Description**
Destination IP	1. IPv4 Format 2. A Must filled setting	Specify the Destination IP of this static routing rule.
Subnet Mask	255.255.255.0 (/24) is set by default	Specify the Subnet Mask of this static routing rule.
Gateway IP	1. IPv4 Format 2. A Must filled setting	Specify the Gateway IP of this static routing rule.
Interface	Auto is set by default	Select the Interface of this static routing rule. It can be **Auto**, or the available WAN / LAN interfaces.
Metric	1. Numberic String Format 2. A Must filled setting	The Metric of this static routing rule. *Value Range*: 0 ~ 255.
Rule	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	NA	When the **Back** button is clicked the screen will return to the Static Routing Configuration page.

Modbus Cellular Gateway

2.6.2 Dynamic Routing

Dynamic Routing, also called adaptive routing, describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in network conditions.
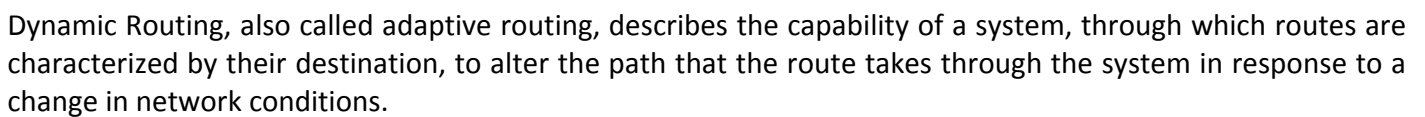
This gateway supports dynamic routing protocols, including RIPv1/RIPv2 (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol), for you to establish routing table automatically. The feature of dynamic routing will be very useful when there are lots of subnets in your network. Generally speaking, RIP is suitable for small network. OSPF is more suitable for medium network. BGP is more used for big network infrastructure.

The supported dynamic routing protocols are described as follows.

Modbus Cellular Gateway

RIP Scenario
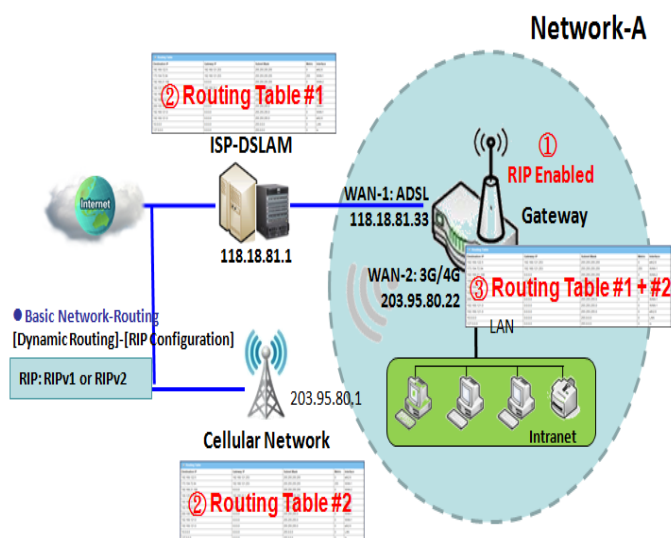
The Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance, in other words the route is considered unreachable. RIP implements the split horizon, route poisoning and hold-down mechanisms to prevent incorrect routing information from being propagated.

OSPF Scenario
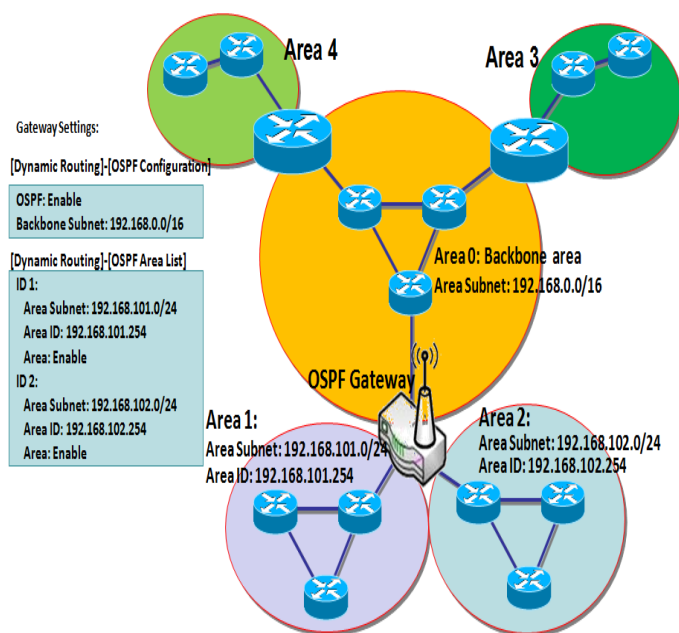
Open Shortest Path First (OSPF) is a routing protocol that uses link state routing algorithm. It is the most widely used interior gateway protocol (IGP) in large enterprise networks. It gathers link state information from available routers and constructs a topology map of the network. The topology is presented as a routing table which routes datagrams based solely on the destination IP address.

Network administrator can deploy OSPF gateway in large enterprise network to get its routing table from the enterprise backbone, and forward routing information to other routers, which are no linked to the enterprise backbone. Usually, an OSPF network is subdivided into routing areas to simplify administration and optimize traffic and resource utilization.

As shown in the diagram, OSPF gateway gathers routing information from the backbone gateways in area 0, and will forward its routing information to the routers in area 1 and area 2 which are not in the backbone.

Modbus Cellular Gateway

BGP Scenario

Border Gateway Protocol (BGP) is a standard exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet. It usually makes routing decisions based on paths, network policies, or rule-sets.

Most ISPs use BGP to establish routing between one another (especially for multi-homed). Very large private IP networks also use BGP internally. The major BGP gateway within one AS will links with some other border gateways for exchanging routing information. It will distribute the collected data in AS to all routers in other AS.

As shown in the diagram, BGP 0 is gateway to dominate AS0 (self IP is 10.100.0.1 and self ID is 100). It links with other BGP gateways in the Internet. The scenario is like Subnet in one ISP to be linked with the ones in other ISPs. By operating with BGP protocol, BGP 0 can gather routing information from other BGP gateways in the Internet. And then it forwards the routing data to the routers in its dominated AS. Finally, the routers resided in AS 0 know how to route packets to other AS.

Advanced Configurable Routing

Within this gateway, there is built-in configurable routing software Quagga. It is a routing software package that provides TCP/IP based routing services with routing protocols support such as OSPF and BGP. Quagga is made from a collection of several daemons that work together to build the routing table, so it provides an interactive user interface for each routing protocol and supports common client commands.

Modbus Cellular Gateway

Dynamic Routing Setting

Go to **Basic Network** > **Routing** > **Dynamic Routing** Tab.

The dynamic routing setting allows user to customize RIP, OSPF, and BGP protocol through the router based on their office setting.

In the "Dynamic Routing" page, there are seven configuration windows for dynamic routing feature. They are the "RIP Configuration" window, "OSPF Configuration" window, "OSPF Area List", "OSPF Area Configuration", "BGP Configuration", "BGP Neighbor List" and "BGP Neighbor Configuration" window. RIP, OSPF and BGP protocols can be configured individually.

The "RIP Configuration" window lets you choose which version of RIP protocol to be activated or disable it. The "OSPF Configuration" window can let you activate the OSPF dynamic routing protocol and specify its backbone subnet. Moreover, the "OSPF Area List" window lists all defined areas in the OSPF network. However, the "BGP Configuration" window can let you activate the BGP dynamic routing protocol and specify its self ID. The "BGP Neighbor List" window lists all defined neighbors in the BGP network.

Enable Dynamic Routing

Just check the "**Enable**" box to activate the "Dynamic Routing" feature.

Configuration	
Item	Setting
▶ Dynamic Routing	☑ Enable

Configuration Item	Value setting	Description
Dynamic Routing	The box is unchecked by default	Check the **Enable** box to activate this function

Modbus Cellular Gateway

RIP Configuration

The RIP configuration setting allows user to customize RIP protocol through the router based on their office setting.

Item	Setting
RIP Configuration	[Help]
▶ RIP Enable	Disable ▼

RIP Configuration		
Item	**Value setting**	**Description**
RIP Enable	Disable is set by default	Select **Disable** will disable RIP protocol. Select **RIP v1** will enable RIPv1 protocol. Select **RIP v2** will enable RIPv2 protocol.

OSPF Configuration

The OSPF configuration setting allows user to customize OSPF protocol through the router based on their office setting.

Item	Setting
OSPF Configuration	
▶ OSPF	☐ Enable
▶ Router ID	
▶ Authentication	None ▼
▶ Backbone Subnet	

OSPF Configuration		
Item	**Value setting**	**Description**
OSPF	Disable is set by default	Click **Enable** box to activate the OSPF protocol.
Router ID	1. IPv4 Format 2. A Must filled setting	The Router ID of this router on OSPF protocol
Authentication	None is set by default	The Authentication method of this router on OSPF protocol. Select **None** will disable Authentication on OSPF protocol. Select **Text** will enable Text Authentication with entered the Key in this field on OSPF protocol.

Modbus Cellular Gateway

		Select **MD5** will enable MD5 Authentication with entered the ID and Key in these fields on OSPF protocol.
Backbone Subnet	1. Classless Inter Domain Routing (CIDR) Subnet Mask Notation. (Ex: 192.168.1.0/24) 2. A Must filled setting	The Backbone Subnet of this router on OSPF protocol.

Create / Edit OSPF Area Rules

The router allows you to custom your OSPF Area List rules. It supports up to a maximum of 32 rule sets.

ID	Area Subnet	Area ID	Enable	Actions

When **Add** button is applied, **OSPF Area Rule Configuration** screen will appear.

Item	Setting
▶ Area Subnet	
▶ Area ID	
▶ Area	☐ Enable
	Save

OSPF Area Configuration		
Item	**Value setting**	**Description**
Area Subnet	1. Classless Inter Domain Routing (CIDR) Subnet Mask Notation. (Ex: 192.168.1.0/24) 2. A Must filled setting	The Area Subnet of this router on OSPF Area List.
Area ID	1. IPv4 Format 2. A Must filled setting	The Area ID of this router on OSPF Area List.
Area	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration

Modbus Cellular Gateway

BGP Configuration

The BGP configuration setting allows user to customize BGP protocol through the router setting.

Item	Setting
▶ BGP	☐ Enable
▶ ASN	[ ]
▶ Router ID	[ ]

BGP Network Configuration		
Item	**Value setting**	**Description**
BGP	The box is unchecked by default	Check the **Enable** box to activate the BGP protocol.
ASN	1. Numberic String Format 2. A Must filled setting	The ASN Number of this router on BGP protocol. *Value Range*: 1 ~ 4294967295.
Router ID	1. IPv4 Format 2. A Must filled setting	The Router ID of this router on BGP protocol.

Create / Edit BGP Network Rules

The router allows you to custom your BGP Network rules. It supports up to a maximum of 32 rule sets.

ID	Network Subnet	Enable	Actions

When **Add** button is applied, **BGP Network Rule Configuration** screen will appear.

Item	Setting	
▶ Network Subnet	IP : [ ]	255.255.255.0 (/24) ▼
▶ Network	☐ Enable	
	Save	

Item	Value setting	Description
Network Subnet	1. IPv4 Format	The Network Subnet of this router on BGP Network List. It composes of entered

Modbus Cellular Gateway

	2. A Must filled setting	the IP address in this field and the selected subnet mask.
Network	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration

Create / Edit BGP Neighbor Rules

The router allows you to custom your BGP Neighbor rules. It supports up to a maximum of 32 rule sets.

BGP Neighbor List	Add	Delete		
ID	Neighbor IP	Remote ASN	Enable	Actions

When **Add** button is applied, **BGP Neighbor Rule Configuration** screen will appear.

BGP Neighbor Configuration	
Item	Setting
▶ Neighbor IP	
▶ Remote ASN	
▶ Neighbor	☐ Enable
	Save

BGP Neighbor Configuration		
Item	**Value setting**	**Description**
Neighbor IP	1. IPv4 Format 2. A Must filled setting	The Neighbor IP of this router on BGP Neighbor List.
Remote ASN	1. Numberic String Format 2. A Must filled setting	The Remote ASN of this router on BGP Neighbor List. ***Value Range***: 1 ~ 4294967295.
Neighbor	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration

Modbus Cellular Gateway

2.6.3 Routing Information

The routing information allows user to view the routing table and policy routing information. Policy Routing Information is only available when the Load Balance function is enabled and the Load Balance Strategy is By User Policy.

Go to **Basic Network > Routing > Routing Information** Tab.

Destination IP	Subnet Mask	Gateway IP	Metric	Interface
192.168.1.0	255.255.255.0	0.0.0.0	0	LAN
169.254.0.0	255.255.0.0	0.0.0.0	0	LAN
239.0.0.0	255.0.0.0	0.0.0.0	0	LAN
127.0.0.0	255.0.0.0	0.0.0.0	0	lo

Routing Table Item	Value setting	Description
Destination IP	N/A	Routing record of Destination IP. IPv4 Format.
Subnet Mask	N/A	Routing record of Subnet Mask. IPv4 Format.
Gateway IP	N/A	Routing record of Gateway IP. IPv4 Format.
Metric	N/A	Routing record of Metric. Numeric String Format.
Interface	N/A	Routing record of Interface Type. String Format.

Policy Routing Source	Source IP	Destination IP	Destination Port	WAN Interface
Load Balance	-	-	-	-

Policy Routing Information Item	Value setting	Description
Policy Routing Source	N/A	Policy Routing of Source. String Format.
Source IP	N/A	Policy Routing of Source IP. IPv4 Format.
Destination IP	N/A	Policy Routing of Destination IP. IPv4 Format.
Destination Port	N/A	Policy Routing of Destination Port. String Format.
WAN Interface	N/A	Policy Routing of WAN Interface. String Format.

2.7   DNS & DDNS

How does user access your server if your WAN IP address changes all the time? One way is to register a new domain name, and maintain your own DNS server. Another simpler way is to apply a domain name to a third-party DDNS service provider. The service can be free or charged. If you want to understand the basic concepts of DNS and Dynamic DNS, you can refer to Wikipedia website[8,9].

2.7.1 DNS & DDNS Configuration

Pre-defined Domain Name List Add Delete			
Domain Name	IP Address	Definition Enable	Actions
db.network-a.b.com	10.0.75.2	☑	Edit ☐ Select

Dynamic DNS	[Help]
Item	Setting
▸ DDNS	☑ Enable
▸ WAN Interface	WAN-1 ▾
▸ Provider	No-IP.com ▾
▸ Host Name	mygw
▸ User Name / E-Mail	account
▸ Password / Key	••••••

DNS

The gateway supports DNS server function for the connected local clients which get the LAN IP from dynamic IP scheme. So, you can create a private host list for easily access the hosts / servers in your intranet with corresponding domain names. As the configuration setting in above diagram, instead of access 10.0.75.2, you can access your File Server with its domain name ***db.network-a.b.com*** in your intranet.

---

8 http://en.wikipedia.org/wiki/Domain_Name_System
9 http://en.wikipedia.org/wiki/Dynamic_DNS

Modbus Cellular Gateway

Dynamic DNS
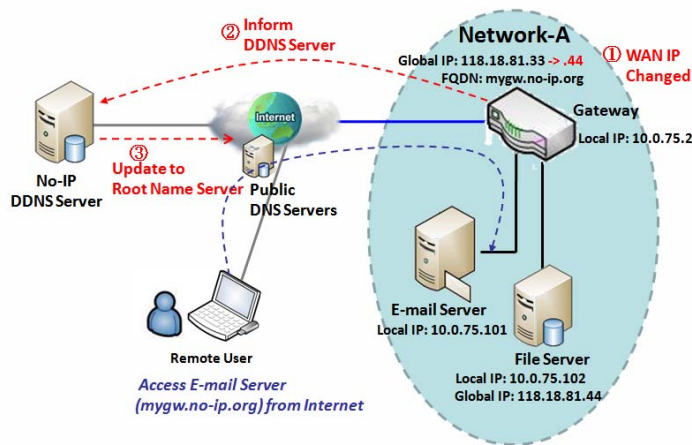
To host your server on a changing IP address, you have to use dynamic domain name service (DDNS). Therefore, anyone wishing to reach your host only needs to know the domain name. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

The Dynamic DNS service allows the gateway to alias a public dynamic IP address to a static domain name, allowing the gateway to be more easily accessed from various locations on the Internet. As shown in the diagram, user registered a domain name to a third-party DDNS service provider (NO-IP) to use DDNS function. Once the IP address of designated WAN interface has changed, the dynamic DNS agent in the gateway will inform the DDNS server with the new IP address. The server automatically re-maps your domain name with the changed IP address. So, other hosts or remote users in the Internet world are able to link to your gateway by using your domain name regardless of the changing global IP address.

Modbus Cellular Gateway

DNS & DDNS Setting

Go to **Basic Network** > **DNS & DDNS** > **Configuration** Tab.

The DNS & DDNS setting allows user to create/modify pre-defined domain name list and setup Dynamic DNS feature.

Create / Edit Pre-defined Domain Name List

The gateway allows you to custom your pre-defined domain name list. It supports up to a maximum of 128 sets.

Pre-defined Domain Name List Add Delete			
Domain Name	IP Address	Definition Enable	Actions

When **Add** button is applied, **Pre-defined Domain Name Configuration** screen will appear.

Pre-defined Domain Name Configuration	
Item	**Setting**
▶ Domain Name	
▶ IP Address	
▶ Definition Enable	☐ Enable

Pre-defined Domain Name Configuration		
Item	**Value setting**	**Description**
Domain Name	1. String format can be any text 2. A Must filled setting	Enter a domain name that mapping the IP Address. _**Value Range**_: at least 1 character is required.
IP Address	1. IPv4 format 2. A Must filled setting	Enter a IP Address that mapping the Domain Name.
Definition Enable	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings
Back	N/A	When the **Back** button is clicked the screen will return to the Dynamic DNS configuration page.

Modbus Cellular Gateway

Setup Dynamic DNS

The gateway allows you to custom your Dynamic DNS settings.

Dynamic DNS	[Help]
Item	**Setting**
▶ DDNS	☐ Enable
▶ WAN Interface	WAN-1 ▾
▶ Provider	DynDNS.org(Dynamic) ▾
▶ Host Name	
▶ User Name / E-Mail	
▶ Password / Key	

DDNS (Dynamic DNS) Configuration		
Item	**Value setting**	**Description**
DDNS	The box is unchecked by default	Check the **Enable** box to activate this function.
WAN Interface	WAN 1 is set by default	Select the WAN Interface IP Address of the gateway.
Provider	**DynDNS.org (Dynamic)** is set by default	Select your DDNS provider of Dynamic DNS. It can be **DynDNS.org(Dynamic)**, **DynDNS.org(Custom)**, **NO-IP.com**, etc…
Host Name	1. String format can be any text 2. A Must filled setting	Your registered host name of Dynamic DNS. ***Value Range***: 0 ~ 63 characters.
User Name / E-Mail	1. String format can be any text 2. A Must filled setting	Enter your User name or E-mail addresss of Dynamic DNS.
Password / Key	1. String format can be any text 2. A Must filled setting	Enter your Password or Key of Dynamic DNS.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Chapter 3 Object Definition

3.1 Scheduling

Scheduling provides ability of adding/deleting time schedule rules, which can be applied to other functionality.

3.1.1 Scheduling Configuration

Go to **Object Definition > Scheduling > Configuration** tab.

ID	Rule Name	Actions

Time Schedule List [Add] [Delete]

Button description		
Item	**Value setting**	**Description**
Add	N/A	Click the **Add** button to configure time schedule rule
Delete	N/A	Click the **Delete** button to delete selected rule(s)

When **Add** button is applied, Time Schedule Configuration and Time Period Definition screens will appear.

Time Schedule Configuration

Item	Setting
▶ Rule Name	
▶ Rule Policy	Inactivate ▾ the Selected Days and Hours Below.

Time Schedule Configuration		
Item	**Value Setting**	**Description**
Rule Name	String: any text	Set rule name
Rule Policy	Default Inactivate	Inactivate/activate the function been applied to in the time period below

Modbus Cellular Gateway

Time Period Definition			
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one -- ▾		
2	-- choose one -- ▾		
3	-- choose one -- ▾		
4	-- choose one -- ▾		
5	-- choose one -- ▾		
6	-- choose one -- ▾		
7	-- choose one -- ▾		
8	-- choose one -- ▾		

Time Period Definition		
Item	**Value Setting**	**Description**
Week Day	Select from menu	Select everyday or one of weekday
Start Time	Time format (hh :mm)	Start time in selected weekday
End Time	Time format (hh :mm)	End time in selected weekday
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings
Refresh	N/A	Click the **Refresh** button to refresh the time schedule list.

3.2 ~~User~~ (not supported)

Not supported feature for the purchased product, leave it as blank.

Modbus Cellular Gateway

3.3 Grouping

The Grouping function allows user to make group for some services.

3.3.1 Host Grouping

Go to **Object Definition > Grouping > Host Grouping** tab.

The Host Grouping function allows user to make host group for some services, such as QoS, Firewall, and Communication Bus. The supported service types could be different for the purchased product.

ID	Group Name	Group Type	Member List	Bound Services	Enable	Actions

When **Add** button is applied, **Host Group Configuration** screen will appear.

Item	Setting
▸ Group Name	
▸ Member List	
▸ Multiple Bound Services	☐ Firewall ☐ QoS ☐ Communication Bus
▸ Member Type	IP Address-based ▼
▸ Member to Join	[ ] Join
▸ Group	☐ Enable

Host Group Configuration		
Item	**Value setting**	**Description**
Group Name	1. String format can be any text 2. A Must filled setting	Enter a group name for the rule. It is a name that is easy for you to understand.
Member List	NA	This field will indicate the hosts (members) contained in the group.
Multiple Bound Services	The boxes are unchecked by default	Binding the services that the host group can be applied. If you enable the **Firewall**, the produced group can be used in firewall service. Same as by enable **QoS** and **Communication Bus**. **Note**: The supported service type can be different for the purchased product.
Member Type	1. **IP Address-based** is selected by default.	Select the member type for the host group. It can be **IP Address-based**, **MAC Address-based**, or **Host Name-based**.

98

	2. A Must filled setting	When **IP Address-based** is selected, only IP address can be added in **Member to Join.**
		When **MAC Address-based** is selected, only MAC address can be added in **Member to Join.**
		When **Host Name-based** is selected, only host name can be added in **Member to Join.**
Member to Join	N/A	Add the members to the group in this field. You can enter the member information as specified in the Member Type above, and press the **Join** button to add. Only one member can be add at a time, so you have to add the members to the group one by one.
Group	The box is unchecked by default	Check the **Enable** checkbox to activate the host group rule. So that the group can be bound to selected service(s) for further configuration.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Modbus Cellular Gateway

3.4 External Server

Go to **Object Definition > External Server > External Server** tab.

The External Server setting allows user to add external server.

Create External Server

ID	Server Name	Server Type	Server IP/FQDN	Server Port	Server Enable	Actions
External Server List	Add	Delete				

When **Add** button is applied, **External Server Configuration** screen will appear.

Item	Setting
▶ Server Name	
▶ Server Type	Email Server ▼ User Name: Password:
▶ Server IP/FQDN	
▶ Server Port	25
▶ Server	☑ Enable
	Save Undo

Modbus Cellular Gateway

External Server Configuration		
Item	**Value setting**	**Description**
Sever Name	1. String format can be any text 2. A Must filled setting	Enter a server name. Enter a name that is easy for you to understand.
Server Type	A Must filled setting	Specify the Server Type of the external server, and enter the required settings for the accessing the server. **Email Server** (A Must filled setting) : When **Email Server** is selected, **User Name**, and **Password** are also required. **User Name** (String format: any text) **Password** (String format: any text) **RADIUS Server** (A Must filled setting) : When **RADIUS Server** is selected, the following settings are also required. **Accounting Port** (A Must filled setting) Primary : **Shared Key** (String format: any text) Authentication Protocol (By default CHAP is selected) Session Timeout (By default **1**) The values must be between 1 and 60. Idle Timeout: (By default 1) The values must be between 1 and 26. Secondary : **Shared Key** (String format: any text) Authentication Protocol (By default CHAP is selected) Session Timeout (By default **1**) The values must be between 1 and 60. Idle Timeout: (By default 1) The values must be between 1 and 26. **Active Directory Server** (A Must filled setting) : When **Active Directory Server** is selected, **Domain** setting is also required. **Domain** (String format: any text) **LDAP Server** (A Must filled setting) : When **LDAP Server** is selected, the following settings are also required. **Base DN** (String format: any text) **Identity** (String format: any text) **Password** (String format: any text) **UAM Server** (A Must filled setting) : When **UAM Server** is selected, the following settings are also required. **Login URL** (String format: any text) **Shared Secret** (String format: any text) **N/AS/Gateway ID** (String format: any text) **Location ID** (String format: any text)

Modbus Cellular Gateway

<table>
<tr><td></td><td></td><td>Location Name (String format: any text)</td></tr>
<tr><td></td><td></td><td>TACACS+ Server (A Must filled setting) :
When TACACS+ Server is selected, the following settings are also required.
Shared Key (String format: any text)
Session Timeout (String format: any number)
The values must be between 1 and 60.</td></tr>
<tr><td></td><td></td><td>SCEP Server (A Must filled setting) :
When SCEP Server is selected, the following settings are also required.
Path (String format: any text, By default cgi-bin is filled)
Application (String format: any text, By default pkiclient.exe is filled)</td></tr>
<tr><td></td><td></td><td>FTP(SFTP) Server (A Must filled setting) :
When FTP(SFTP) Server is selected, the following settings are also required.
User Name (String format: any text)
Password (String format: any text)
Protocol (Select FTP or SFTP)
Encryprion (Select Plain, Explicit FTPS or Implicit FTPS)
Transfer mode (Select Passive or Active)</td></tr>
<tr><td>Server IP/FQDN</td><td>A Must filled setting</td><td>Specify the IP address or FQDN used for the external server.</td></tr>
<tr><td>Server Port</td><td>A Must filled setting</td><td>Specify the Port used for the external server. If you selected a certain server type, the default server port number will be set.
For Email Server 25 will be set by default;
For Syslog Server, port 514 will be set by default;
For RADIUS Server, port 1812 will be set by default;
For Active Directory Server, port 389 will be set by default;
For LDAP Server, port 389 will be set by default;
For UAM Server, port 80 will be set by default;
For TACACS+ Server, port 49 will be set by default;
For SCEP Server, port 80 will be set by default;
For FTP(SFTP) Server, port 21 will be set by default;</td></tr>
<tr><td>Server</td><td>The box is checked by default</td><td>Click Enable to activate this External Server.</td></tr>
<tr><td>Save</td><td>N/A</td><td>Click Save to save the settings</td></tr>
<tr><td>Undo</td><td>N/A</td><td>Click Undo to cancel the settings</td></tr>
<tr><td>Refresh</td><td>N/A</td><td>Click the Refresh button to refresh the external server list.</td></tr>
</table>

3.5 Certificate

In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are genuine. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner[10].

In a typical public-key infrastructure (PKI) scheme, the signer is a certificate authority (CA), usually a company such as VeriSign which charges customers to issue certificates for them. In a web of trust scheme, the signer is either the key's owner (a self-signed certificate) or other users ("endorsements") whom the person examining the certificate might know and trust. The device also plays as a CA role.

Certificates are an important component of Transport Layer Security (TLS, sometimes called by its older name SSL), where they prevent an attacker from impersonating a secure website or other server. They are also used in other important applications, such as email encryption and code signing. Here, it can be used in IPSec tunneling for user authentication.

3.5.1 Configuration

The configuration setting allows user to create Root Certificate Authority (CA) certificate and configure to set enable of SCEP. Root CA is the top-most certificate of the tree, the private key of which is used to "sign" other certificates.

Go to **Object Definition > Certificate > Configuration** tab.

Create Root CA

ID	Name	Subject	Issuer	Vaild To	Action

Root CA [Generate]

When **Generate** button is applied, **Root CA Certificate Configuration** screen will appear. The required information to be filled for the root CA includes the name, key, subject name and validity.

---

10 http://en.wikipedia.org/wiki/Public_key_certificate.

Modbus Cellular Gateway

Root CA Certificate Configuration		
Item	**Value setting**	**Description**
Name	1. String format can be any text 2. A Must filled setting	Enter a Root CA Certificate name. It will be a certificate file name
Key	A Must filled setting	This field is to specify the key attribute of certificate. **Key Type** to set public-key cryptosystems. It only supports RSA now. **Key Length** to set s the size measured in bits of the key used in a cryptographic algorithm. **Digest Algorithm** to set identifier in the signature algorithm identifier of certificates
Subject Name	A Must filled setting	This field is to specify the information of certificate. **Country(C)** is the two-letter ISO code for the country where your organization is located. **State(ST)** is the state where your organization is located. **Location(L)** is the location where your organization is located. **Organization(O)** is the name of your organization. **Organization Unit(OU)** is the name of your organization unit. **Common Name(CN)** is the name of your organization. **Email** is the email of your organization. It has to be email address style.
Validity Period	A Must filled setting	This field is to specify the validity period of certificate.

Modbus Cellular Gateway

Setup SCEP

Item	Setting
▸ SCEP	☐ Enable
▸ Automatically re-enroll aging certificates	☐ Enable

SCEP Configuration		
Item	**Value setting**	**Description**
SCEP	The box is unchecked by default	Check the **Enable** box to activate SCEP function.
Automatically re-enroll aging certificates	The box is unchecked by default	When **SCEP** is activated, check the **Enable** box to activate this function. It will be automatically check which certificate is aging. If certificate is aging, it will activate SCEP function to re-enroll automatically.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Modbus Cellular Gateway

3.5.2 My Certificate

My Certificate includes a Local Certificate List. Local Certificate List shows all generated certificates by the root CA for the gateway. And it also stores the generated Certificate Signing Requests (CSR) which will be signed by other external CAs. The signed certificates can be imported as the local ones of the gateway.

Self-signed Certificate Usage Scenario
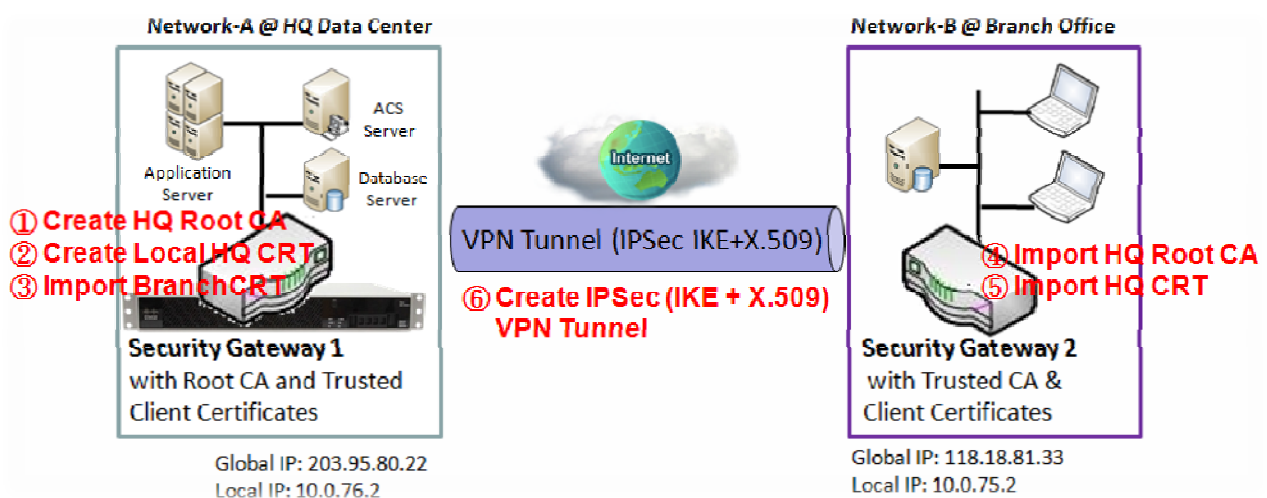
Scenario Application Timing

When the enterprise gateway owns the root CA and VPN tunneling function, it can generate its own local certificates by being signed by itself or import any local certificates that are signed by other external CAs. Also import the trusted certificates for other CAs and Clients. In addition, since it has the root CA, it also can sign Certificate Signing Requests (CSR) to form corresponding certificates for others. These certificates can be used for two remote peers to make sure their identity during establishing a VPN tunnel.

Scenario Description

Gateway 1 generates the root CA and a local certificate (HQCRT) signed by itself. Import a trusted certificate (BranchCRT) –a BranchCSR certificate of Gateway 2 signed by root CA of Gateway 1.

Gateway 2 creates a CSR (BranchCSR) to let the root CA of the Gateway 1 sign it to be the BranchCRT certificate. Import the certificate into the Gateway 2 as a local certificate. In addition, also import the certificates of the root CA of the Gateway 1 into the Gateway 2 as the trusted ones. (Please also refer to following two sub-sections)

Establish an IPSec VPN tunnel with IKE and X.509 protocols by starting from either peer, so that all

Modbus Cellular Gateway

client hosts in these both subnets can communicate with each other.

Parameter Setup Example

For Network-A at HQ

Following tables list the parameter configuration as an example for the "My Certificate" function used in the user authentication of IPSec VPN tunnel establishing, as shown in above diagram. The configuration example must be combined with the ones in following two sections to complete the whole user scenario.

Use default value for those parameters that are not mentioned in the tables.

Configuration Path	[My Certificate]-[Root CA Certificate Configuration]
Name	*HQRootCA*
Key	Key Type: *RSA* Key Length: *1024-bits*
Subject Name	Country(C): *TW* State(ST): *Taiwan* Location(L): *Tainan* Organization(O): *AMITHQ* Organization Unit(OU): *HQRD* Common Name(CN): *HQRootCA* E-mail: *hqrootca@amit.com.tw*

Configuration Path	[My Certificate]-[Local Certificate Configuration]
Name	*HQCRT* Self-signed: ■
Key	Key Type: *RSA* Key Length: *1024-bits*
Subject Name	Country(C): *TW* State(ST): *Taiwan* Location(L): *Tainan* Organization(O): *AMITHQ* Organization Unit(OU): *HQRD* Common Name(CN): *HQCRT* E-mail: *hqcrt@amit.com.tw*

Configuration Path	[IPSec]-[Configuration]
IPSec	■ *Enable*

Configuration Path	[IPSec]-[Tunnel Configuration]
Tunnel	■ *Enable*
Tunnel Name	*s2s-101*
Interface	*WAN 1*
Tunnel Scenario	*Site to Site*
Operation Mode	*Always on*

Configuration Path	[IPSec]-[Local & Remote Configuration]
Local Subnet	*10.0.76.0*
Local Netmask	*255.255.255.0*
Full Tunnel	*Disable*
Remote Subnet	*10.0.75.0*
Remote Netmask	*255.255.255.0*
Remote Gateway	*118.18.81.33*

Modbus Cellular Gateway

Configuration Path	[IPSec]-[Authentication]
Key Management	*IKE+X.509* Local Certificate: *HQCRT* Remote Certificate: *BranchCRT*
Local ID	*User Name Network-A*
Remote ID	*User Name Network-B*

Configuration Path	[IPSec]-[IKE Phase]
Negotiation Mode	*Main Mode*
X-Auth	*None*

For Network-B at Branch Office

Following tables list the parameter configuration as an example for the "My Certificate" function used in the user authentication of IPSec VPN tunnel establishing, as shown in above diagram. The configuration example must be combined with the ones in following two sections to complete the whole user scenario.

Use default value for those parameters that are not mentioned in the tables.

Configuration Path	[My Certificate]-[Local Certificate Configuration]
Name	*BranchCRT* Self-signed: □
Key	Key Type: *RSA* Key Length: *1024-bits*
Subject Name	Country(C): *TW* State(ST): *Taiwan* Location(L): *Tainan* Organization(O): *AMITBranch* Organization Unit(OU): *BranchRD* Common Name(CN): *BranchCRT* E-mail: *branchcrt@amit.com.tw*

Configuration Path	[IPSec]-[Configuration]
IPSec	■ *Enable*

Configuration Path	[IPSec]-[Tunnel Configuration]
Tunnel	■ *Enable*
Tunnel Name	*s2s-102*
Interface	*WAN 1*
Tunnel Scenario	*Site to Site*
Operation Mode	*Always on*

Configuration Path	[IPSec]-[Local & Remote Configuration]
Local Subnet	*10.0.75.0*
Local Netmask	*255.255.255.0*
Full Tunnel	*Disable*
Remote Subnet	*10.0.76.0*

Modbus Cellular Gateway

Remote Netmask	*255.255.255.0*
Remote Gateway	*203.95.80.22*

Configuration Path	[IPSec]-[Authentication]
Key Management	*IKE+X.509* Local Certificate: *BranchCRT* Remote Certificate: *HQCRT*
Local ID	*User Name Network-B*
Remote ID	*User Name Network-A*

Configuration Path	[IPSec]-[IKE Phase]
Negotiation Mode	*Main Mode*
X-Auth	*None*

Scenario Operation Procedure

In above diagram, "Gateway 1" is the gateway of Network-A in headquarters and the subnet of its Intranet is 10.0.76.0/24. It has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN-1 interface. "Gateway 2" is the gateway of Network-B in branch office and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. They both serve as the NAT security gateways.

Gateway 1 generates the root CA and a local certificate (HQCRT) that is signed by itself. Import the certificates of the root CA and HQCRT into the "Trusted CA Certificate List" and "Trusted Client Certificate List" of Gateway 2.

Gateway 2 generates a Certificate Signing Request (BranchCSR) for its own certificate (BranchCRT) (Please generate one not self-signed certificate in the Gateway 2, and click on the "View" button for that CSR. Just downloads it). Take the CSR to be signed by the root CA of Gateway 1 and obtain the BranchCRT certificate (you need rename it). Import the certificate into the "Trusted Client Certificate List" of the Gateway 1 and the "Local Certificate List" of Gateway 2.

Gateway 2 can establish an IPSec VPN tunnel with "Site to Site" scenario and IKE and X.509 protocols to Gateway 1.

Finally, the client hosts in two subnets of 10.0.75.0/24 and 10.0.76.0/24 can communicate with each other.

Modbus Cellular Gateway

My Certificate Setting

Go to **Object Definition > Certificate > My Certificate** tab.

The My Certificate setting allows user to create local certificates. In "My Certificate" page, there are two configuration windows for the "My Certificate" function. The "Local Certificate List" window shows the stored certificates or CSRs for representing the gateway. The "Local Certificate Configuration" window can let you fill required information necessary for corresponding certificate to be generated by itself, or corresponding CSR to be signed by other CAs.

Create Local Certificate

When **Add** button is applied, **Local Certificate Configuration** screen will appear. The required information to be filled for the certificate or CSR includes the name, key and subject name. It is a certificate if the "Self-signed" box is checked; otherwise, it is a CSR.

Modbus Cellular Gateway

Local Certificate Configuration		
Item	**Value setting**	**Description**
Name	1. String format can be any text 2. A Must filled setting	Enter a certificate name. It will be a certificate file name If **Self-signed** is checked, it will be signed by root CA. If **Self-signed** is not checked, it will generate a certificate signing request (CSR).
Key	A Must filled setting	This field is to specify the key attributes of certificate. **Key Type** to set public-key cryptosystems. Currently, only RSA is supported. **Key Length** to set the length in bits of the key used in a cryptographic algorithm. It can be 512/768/1024/1536/2048. **Digest Algorithm** to set identifier in the signature algorithm identifier of certificates. It can be MD5/SHA-1.
Subject Name	A Must filled setting	This field is to specify the information of certificate. **Country(C)** is the two-letter ISO code for the country where your organization is located. **State(ST)** is the state where your organization is located. **Location(L)** is the location where your organization is located. **Organization(O)** is the name of your organization. **Organization Unit(OU)** is the name of your organization unit. **Common Name(CN)** is the name of your organization. **Email** is the email of your organization. It has to be email address setting only.
Extra Attributes	A Must filled setting	This field is to specify the extra information for generating a certificate. **Challenge Password** for the password you can use to request certificate revocation in the future. **Unstructured Name** for additional information.
SCEP Enrollment	A Must filled setting	This field is to specify the information of SCEP. If user wants to generate a certificate signing request (CSR) and then signed by SCEP server online, user can check the **Enable** box. Select a **SCEP Server** to identify the SCEP server for use. The server detailed information could be specified in External Servers. Refer to **Object Definition** > **External Server** > **External Server**. You may click **Add Object** button to generate. Select a **CA Certificate** to identify which certificate could be accepted by SCEP server for authentication. It could be generated in Trusted Certificates. Select an optional **CA Encryption Certificate**, if it is required, to identify which certificate could be accepted by SCEP server for encryption data information. It could be generated in Trusted Certificates. Fill in optional **CA Identifier** to identify which CA could be used for signing certificates.
Save	N/A	Click the **Save** button to save the configuration.
Back	N/A	When the **Back** button is clicked, the screen will return to previous page.

When **Import** button is applied, an Import screen will appear. You can import a certificate from an existed certificate file, or directly paste a PEM encoded string as the certificate.

Modbus Cellular Gateway

Import		
Item	**Value setting**	**Description**
Import	A Must filled setting	Select a certificate file from user's computer, and click the **Apply** button to import the specified certificate file to the gateway.
PEM Encoded	1. String format can be any text 2. A Must filled setting	This is an alternative approach to import a certificate. You can directly fill in (Copy and Paste) the PEM encoded certificate string, and click the **Apply** button to import the specified certificate to the gateway.
Apply	N/A	Click the **Apply** button to import the certificate.
Cancel	N/A	Click the **Cancel** button to discard the import operation and the screen will return to the My Certificates page.

3.5.3 Trusted Certificate

Trusted Certificate includes Trusted CA Certificate List, Trusted Client Certificate List, and Trusted Client Key List. The Trusted CA Certificate List places the certificates of external trusted CAs. The Trusted Client Certificate List places the others' certificates what you trust. And the Trusted Client Key List places the others' keys what you trusted.

Self-signed Certificate Usage Scenario

Scenario Application Timing (same as the one described in "My Certificate" section)

When the enterprise gateway owns the root CA and VPN tunneling function, it can generate its own local certificates by being signed by itself. Also imports the trusted certificates for other CAs and Clients. These certificates can be used for two remote peers to make sure their identity during establishing a VPN tunnel.

Scenario Description (same as the one described in "My Certificate" section)

Gateway 1 generates the root CA and a local certificate (HQCRT) signed by itself. Import a trusted certificate (BranchCRT) –a BranchCSR certificate of Gateway 2 signed by root CA of Gateway 1.

Gateway 2 creates a CSR (BranchCSR) to let the root CA of the Gateway 1 sign it to be the BranchCRT certificate. Import the certificate into the Gateway 2 as a local certificate. In addition, also imports the certificates of the root CA of Gateway 1 into the Gateway 2 as the trusted ones. (Please also refer to "My Certificate" and "Issue Certificate" sections).

Establish an IPSec VPN tunnel with IKE and X.509 protocols by starting from either peer, so that all client hosts in these both subnets can communicate with each other.

Parameter Setup Example (same as the one described in "My Certificate" section)

Modbus Cellular Gateway

For Network-A at HQ

Following tables list the parameter configuration as an example for the "Trusted Certificate" function used in the user authentication of IPSec VPN tunnel establishing, as shown in above diagram. The configuration example must be combined with the ones in "My Certificate" and "Issue Certificate" sections to complete the setup for the whole user scenario.

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate List]
Command Button	*Import*

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate Import from a File]
File	*BranchCRT.crt*

For Network-B at Branch Office

Following tables list the parameter configuration as an example for the "Trusted Certificate" function used in the user authentication of IPSec VPN tunnel establishing, as shown in above diagram. The configuration example must be combined with the ones in "My Certificate" and "Issued Certificate" sections to complete the setup for the whole user scenario.

Configuration Path	[Trusted Certificate]-[Trusted CA Certificate List]
Command Button	*Import*

Configuration Path	[Trusted Certificate]-[Trusted CA Certificate Import from a File]
File	*HQRootCA.crt*

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate List]
Command Button	*Import*

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate Import from a File]
File	*HQCRT.crt*

Scenario Operation Procedure (same as the one described in "My Certificate" section)

In above diagram, the "Gateway 1" is the gateway of Network-A in headquarters and the subnet of its Intranet is 10.0.76.0/24. It has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN-1 interface. The "Gateway 2" is the gateway of Network-B in branch office and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. They both serve as the NAT security gateways.

In Gateway 2 import the certificates of the root CA and HQCRT that were generated and signed by

Modbus Cellular Gateway

Gateway 1 into the "Trusted CA Certificate List" and "Trusted Client Certificate List" of Gateway 2.

Import the obtained BranchCRT certificate (the derived BranchCSR certificate after Gateway 1's root CA signature) into the "Trusted Client Certificate List" of the Gateway 1 and the "Local Certificate List" of the Gateway 2. For more details, refer to the Network-B operation procedure in "My Certificate" section of this manual.

Gateway 2 can establish an IPSec VPN tunnel with "Site to Site" scenario and IKE and X.509 protocols to Gateway 1.

Finally, the client hosts in two subnets of 10.0.75.0/24 and 10.0.76.0/24 can communicate with each other.

Modbus Cellular Gateway

Trusted Certificate Setting

Go to **Object Definition > Certificate > Trusted Certificate** tab.

The Trusted Certificate setting allows user to import trusted certificates and keys.

Import Trusted CA Certificate

When **Import** button is applied, a **Trusted CA import** screen will appear. You can import a Trusted CA certificate from an existed certificate file, or directly paste a PEM encoded string as the certificate.

Trusted CA Certificate List		
Item	**Value setting**	**Description**
Import from a File	A Must filled setting	Select a CA certificate file from user's computer, and click the **Apply** button to import the specified CA certificate file to the gateway.
Import from a PEM	1. String format can be any text 2. A Must filled setting	This is an alternative approach to import a CA certificate. You can directly fill in (Copy and Paste) the PEM encoded CA certificate string, and click the **Apply** button to import the specified CA certificate to the gateway.
Apply	N/A	Click the **Apply** button to import the certificate.
Cancel	N/A	Click the **Cancel** button to discard the import operation and the screen will return to the Trusted Certificates page.

Instead of importing a Trusted CA certificate with mentioned approaches, you can also get the CA certificate from the SECP server.

If **SCEP** is enabled (Refer to **Object Definition** > **Certificate** > **Configuration**), you can click **Get CA** button, a Get CA Configuration screen will appear.

Modbus Cellular Gateway

Get CA Configuration		
Item	**Value setting**	**Description**
SCEP Server	A Must filled setting	Select a **SCEP Server** to identify the SCEP server for use. The server detailed information could be specified in External Servers. Refer to **Object Definition** > **External Server** > **External Server**. You may click **Add Object** button to generate.
CA Identifier	1. String format can be any text	Fill in optional **CA Identifier** to identify which CA could be used for signing certificates.
Save	N/A	Click **Save** to save the settings.
Close	N/A	Click the **Close** button to return to the Trusted Certificates page.

Import Trusted Client Certificate

When **Import** button is applied, a **Trusted Client Certificate Import** screen will appear. You can import a Trusted Client Certificate from an existed certificate file, or directly paste a PEM encoded string as the certificate.

Trusted Client Certificate List		
Item	Value setting	Description
Import from a File	A Must filled setting	Select a certificate file from user's computer, and click the **Apply** button to import the specified certificate file to the gateway.
Import from a PEM	1. String format can be any text 2. A Must filled setting	This is an alternative approach to import a certificate. You can directly fill in (Copy and Paste) the PEM encoded certificate string, and click the **Apply** button to import the specified certificate to the gateway.
Apply	N/A	Click the **Apply** button to import certificate.
Cancel	N/A	Click the **Cancel** button to discard the import operation and the screen will return to the Trusted Certificates page.

Import Trusted Client Key

When **Import** button is applied, a **Trusted Client Key Import** screen will appear. You can import a Trusted Client Key from an existed file, or directly paste a PEM encoded string as the key.

Trusted Client Key List		
Item	Value setting	Description
Import from a File	A Must filled setting	Select a certificate key file from user's computer, and click the **Apply** button to import the specified key file to the gateway.
Import from a PEM	1. String format can be any text 2. A Must filled setting	This is an alternative approach to import a certificate key. You can directly fill in (Copy and Paste) the PEM encoded certificate key string, and click the **Apply** button to import the specified certificate key to the gateway.
Apply	N/A	Click the **Apply** button to import the certificate key.
Cancel	N/A	Click the **Cancel** button to discard the import operation and the screen will return to the Trusted Certificates page.

3.5.4 Issue Certificate

When you have a Certificate Signing Request (CSR) that needs to be certificated by the root CA of the device, you can issue the request here and let Root CA sign it. There are two approaches to issue a certificate. One is from a CSR file importing from the managing PC and another is copy-paste the CSR codes in gateway's web-based utility, and then click on the "Sign" button.

If the gateway signs a CSR successfully, the "Signed Certificate View" window will show the resulted certificate contents. In addition, a "Download" button is available for you to download the certificate to a file in the managing PC.

Self-signed Certificate Usage Scenario
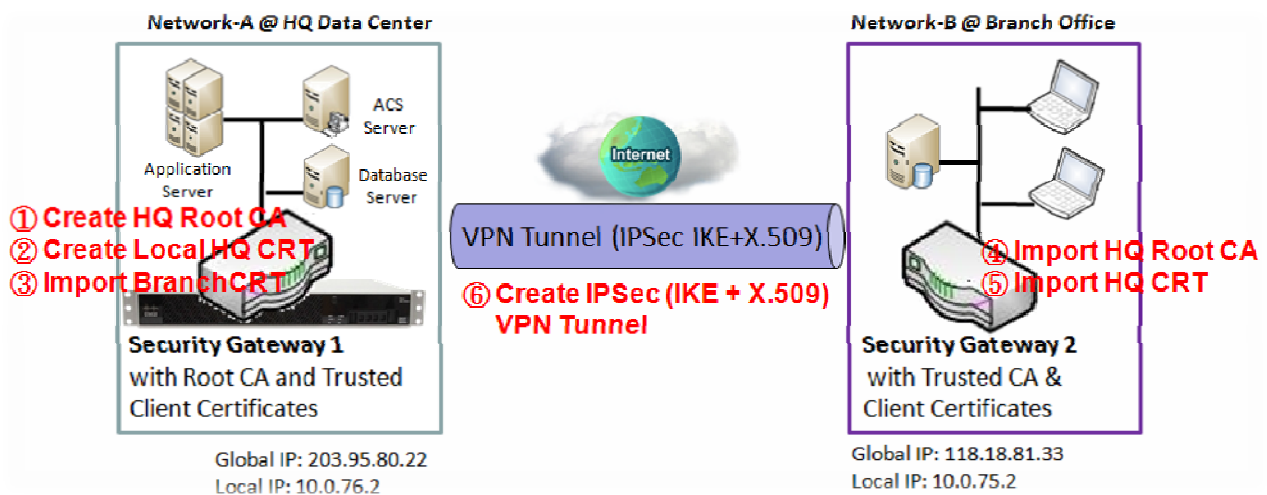
Scenario Application Timing (same as the one described in "My Certificate" section)

When the enterprise gateway owns the root CA and VPN tunneling function, it can generate its own local certificates by being signed by itself. Also imports the trusted certificates for other CAs and Clients. These certificates can be used for two remote peers to make sure their identity during establishing a VPN tunnel.

Scenario Description (same as the one described in "My Certificate" section)

Gateway 1 generates the root CA and a local certificate (HQCRT) signed by itself. Also imports a trusted certificate (BranchCRT) –a BranchCSR certificate of Gateway 2 signed by root CA of Gateway 1.

Gateway 2 creates a CSR (BranchCSR) to let the root CA of the Gateway 1 sign it to be the BranchCRT certificate. Import the certificate into the Gateway 2 as a local certificate. In addition, also imports the certificates of the root CA of the Gateway 1 into the Gateway 2 as the trusted ones. (Please also refer

Modbus Cellular Gateway

to "My Certificate" and "Trusted Certificate" sections).

Establish an IPSec VPN tunnel with IKE and X.509 protocols by starting from either peer, so that all client hosts in these both subnets can communicate with each other.

Parameter Setup Example (same as the one described in "My Certificate" section)

For Network-A at HQ

Following tables list the parameter configuration as an example for the "Issue Certificate" function used in the user authentication of IPSec VPN tunnel establishing, as shown in above diagram. The configuration example must be combined with the ones in "My Certificate" and "Trusted Certificate" sections to complete the setup for whole user scenario.

Configuration Path	[Issue Certificate]-[Certificate Signing Request Import from a File]
Browse	*C:/BranchCSR*
Command Button	*Sign*

Configuration Path	[Issue Certificate]-[Signed Certificate View]
Command Button	*Download* (default name is "issued.crt")

Scenario Operation Procedure (same as the one described in "My Certificate" section)

In above diagram, the "Gateway 1" is the gateway of Network-A in headquarters and the subnet of its Intranet is 10.0.76.0/24. It has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN-1 interface. The "Gateway 2" is the gateway of Network-B in branch office and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. They both serve as the NAT security gateways.

Gateway 1 generates the root CA and a local certificate (HQCRT) that is signed by itself. Import the certificates of the root CA and HQCRT into the "Trusted CA Certificate List" and "Trusted Client Certificate List" of Gateway 2.

Gateway 2 generates a Certificate Signing Request (BranchCSR) for its own certificate BranchCRT to be signed by root CA (Please generate one not self-signed certificate in the Gateway 2, and click on the "View" button for that CSR. Just downloads it). Take the CSR to be signed by the root CA of the Gateway 1 and obtain the BranchCRT certificate (you need rename it). Import the certificate into the "Trusted Client Certificate List" of the Gateway 1 and the "Local Certificate List" of the Gateway 2.

Gateway 2 can establish an IPSec VPN tunnel with "Site to Site" scenario and IKE and X.509 protocols to Gateway 1.

Finally, the client hosts in two subnets of 10.0.75.0/24 and 10.0.76.0/24 can communicate with each other.

Modbus Cellular Gateway

Issue Certificate Setting

Go to **Object Definition > Certificate > Issue Certificate** tab.

The Issue Certificate setting allows user to import Certificate Signing Request (CSR) to be signed by root CA.

Import and Issue Certificate

Certificate Signing Request (CSR) Import from a File		
Item	Value setting	Description
Certificate Signing Request (CSR) Import from a File	A Must filled setting	Select a certificate signing request file you're your computer for importing to the gateway.
Certificate Signing Request (CSR) Import from a PEM	1. String format can be any text 2. A Must filled setting	Enter (copy-paste) the certificate signing request PEM encoded certificate to the gateway.
Sign	N/A	When root CA is exist, click the **Sign** button sign and issue the imported certificate by root CA.

Chapter 4 Field Communication

4.1 Bus & Protocol

The gateway may equip a DB-9 male port or other type of serial port for various serial communication use through connecting the RS-232 or RS-485 serial device to an IP-based Ethernet LAN. These communication protocols make user access serial devices anywhere over a local LAN or the Internet easily. They can be "Virtual COM" and "Modbus".
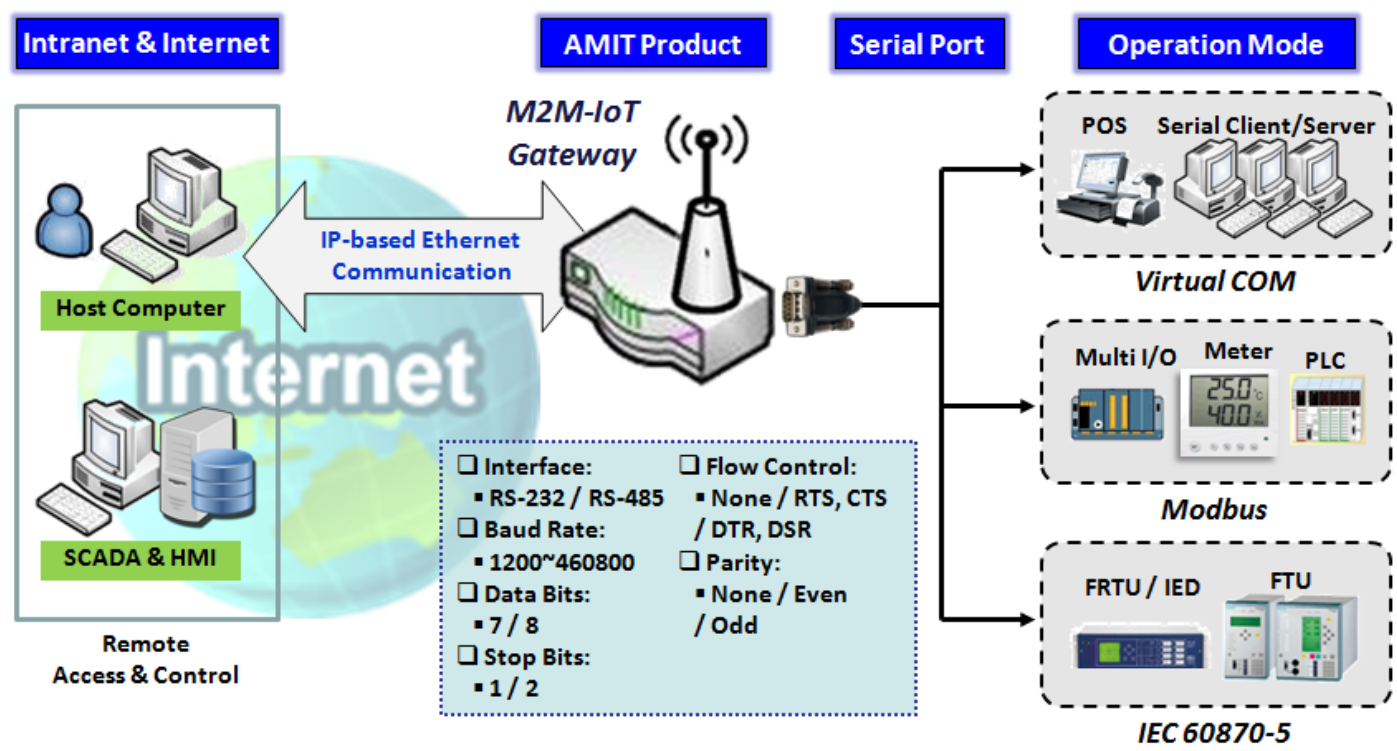
4.1.1 Port Configuration

Before using the supported field communication function, like Virtual COM or Modbus, you need to configure the physical communication port first.

The port configuration screen allows user to configure the operation mode and physical layer settings for each serial interface, and also can quick switch from one communication protocol to another for the serial port. The number of ports and type of the supported protocols could be different for the purchased gateway model.

Modbus Cellular Gateway

Port Configuration Setting

Go to **Field Communication > Bus & Protocol > Port Configuration** tab.

In "Port Configuration" page, there is only one configuration window for the serial port settings. The "Configuration" window can let you specify serial port parameters including the operation mode being "Virtual COM", "Modbus" or disabled, the interface being "RS-232" or "RS-485", the baud rate, the data bit length, the stop bit length, the flow control being "RTS/CTS", "DTS/DSR" or "None", and the parity.

Serial Port Definition								
Serial Port	Operation Mode	Interface	Baud Rate	Data Bits	Stop Bits	Flow Control	Parity	Action
SPort-0	Disable ▾	RS-232 ▾	9600 ▾	8 ▾	1 ▾	None ▾	None ▾	Edit

Port Configuration Window		
Item	**Value setting**	**Description**
Serial Port	*N/A*	It displays the serial port ID of the serial port. The number of serial ports varies from the purchased model.
Operation Mode	Disable is set by default	It displays the current selected operation mode for the serial interface. Depending on the purchase model, the available modes can be Virtual COM, Modbus, and IEC 60870-5.
Interface	RS-232 is set by default	Select RS-232 or RS-485 physical interface for connecting to the access device(s) with the same interface specification.
Baud Rate	19200 is set by default	Select the appropriate baud rate for serial device communication. RS-232: 1200 / 2400 / 4800 / 9600 / 19200 / 38400 / 57600 / 115200 RS-485 can use higher baud rate for 230400 and 460800. It depends on the cable length and the installed environment. The longer cable, the lower baud rate for it.
Data Bits	8 is set by default	Select 8 or 7 for data bits.
Stop Bits	1 is set by default	Select 1 or 2 for stop bits.
Flow Control	None is set by default	Select None / RTS, CTS / DTS, DSR for Flow Control in RS-232 mode. The supporting of Flow Control depends on the purchased model.
Parity	None is set by default	Select None / Even / Odd for Parity bit.
Action	N/A	Click **Edit** button to change the operation mode, or modify the parameters mentioned above for the serial interface communication.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.

Modbus Cellular Gateway

4.1.2 Virtual COM

Create a virtual COM port on user's PC/Host to provide access to serial device connected to the serial port on gateway. Therefore, users can access, control, and manage the connected serial device through Internet (fixed line, or cellular network) anywhere. This application is also known as Ethernet pass-through communication.

Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	TCP Client ▼	4001	Allow All ▼	1 ▼	Always on ▼	0 (0-60)min	0 (0-60)min	✓	Edit
	TCP Client								
	TCP Server								
	UDP								
	RFC-2217								

Virtual COM Serial Definition

Legal IP ... n (TCP Client)

Virtual COM setting screen enables user to connect a Virtual COM port based device to the Internet. It allows user to access serial data remotely. There are TCP Client, TCP Server, UDP, and RFC2217 modes for remote accessing the connected serial device. These operation modes are illustrated as below.

TCP Client Mode

❶ Gateway get Data received from Serial Device.
❷ Establish a TCP Connection and Transmit Data to Remote Host.
❸ Terminate this TCP Connection once Idle Timeout reached 5 mins.
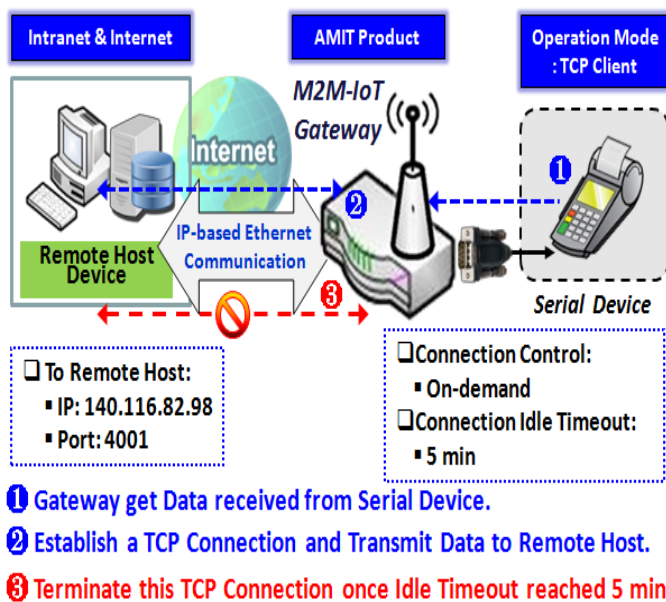
When the administrator expects the gateway to actively establish a TCP connection to a pre-defined host computer when serial data arrives, the operation mode for the "Virtual COM" function is required to be "TCP Client" and when the connection control of virtual COM is "On-demand", once the gateway receives data from the connected serial device, it will establish a TCP connection to transfer the received serial data to the remote host. Besides, after the data has been transferred, the gateway automatically disconnects the established TCP session from the host computer by using the TCP alive check timeout or idle timeout settings.

Modbus Cellular Gateway

TCP Server Mode

Intranet & Internet | **AMIT Product** | **Operation Mode : TCP Server**

M2M-IoT Gateway

Internet

IP-based Ethernet Communication

Host Device

Serial Device

❑ Host IP :
▪ 140.116.82.98

Gateway IP:
140.113.71.125
❑ Listen Port : 4001

❑ Trust Type :
▪ Specific IPs:
  140.116.82.98
❑ Connection Idle Timeout:
▪ 5 min

❶ Gateway remain Listening and Host will Establish a TCP Connection with it.
❷ Host Send Data then Gateway Transmit it to the Serial Device.
❸ Terminate this TCP Connection once Idle Timeout reached 5 mins.

When the administrator expects the gateway to wait passively for the serial data requests from the Host Device (usually we use a computer to play as a Host), and the Host will establish a TCP connection to get data from the serial device, the operation mode for the "Virtual COM" function is required to be "TCP Server". In this mode, the gateway provides a unique "IP: Port" address on a TCP/IP network. It supports up to 4 simultaneous connections, so that multiple hosts can collect data from the same serial device at the same time. After the data has been transferred, the TCP connection will be automatically disconnected from the host computer by using the TCP alive check timeout or idle timeout settings.

UDP Mode

Intranet & Internet | **AMIT Product** | **Operation Mode : UDP**

M2M-IoT Gateway

Internet

IP-based Ethernet Communication

Remote Host

Serial Device

Data is Transferred between Remote Host and Serial Device Directly

❑ Remote Host:
▪ IP: 140.116.82.98
▪ Port: 4001

Gateway IP:
140.113.71.125
❑Listen Port : 4001
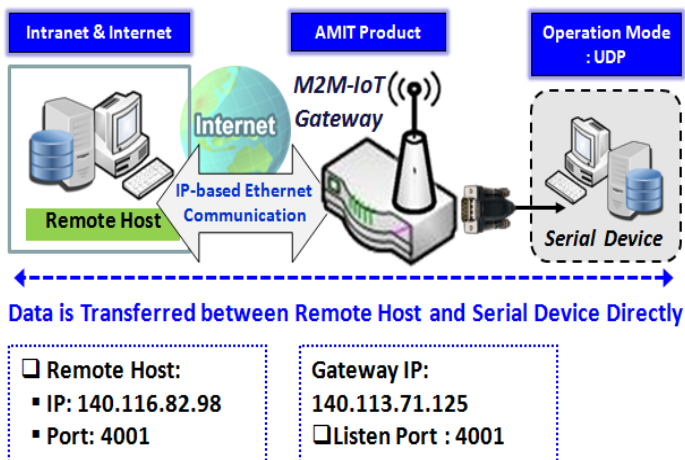
If both the Remote Host Computer and the serial device are expected to initiate a data transfer when it requires doing that, the operation mode for the "Virtual COM" function in the gateway is required to be "UDP". In this mode, the UDP data can be transferred between the gateway and multiple host computers from either peer, making this mode ideal for message display applications.

The remote host computer can directly send UDP data to the serial device via the gateway, and also receive UDP data from the serial device via the gateway at the same time. The gateway supports up to 4 legal hosts to connect simultaneously to the serial device via the gateway.

Modbus Cellular Gateway

RFC-2217 Mode
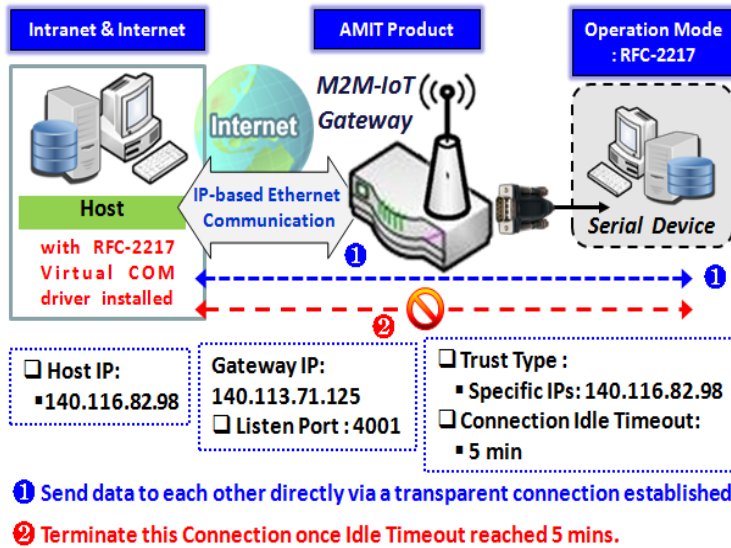
RFC-2217 defines general COM port control options based on telnet protocol. A host computer with RFC-2217 driver installed can monitor and manage the remote serial device attached to the gateway's serial port, as though they were connected to the local serial port. When a virtual serial port on the local serial device is being created, it is required to specify the IP-address of the host computers to establish connection with.

Any 3rd party driver supporting RFC2217 can be used to install in the host computer, the driver establishes a transparent connection between host and serial device by mapping the IP:Port of the gateway's serial port to a virtual local COM port on the host computer.

The host computer can directly send data to the serial device via the gateway, and also receive data from the serial device via the gateway at the same time. The gateway supports up to 4 Internet host computers.

Modbus Cellular Gateway

Virtual COM Setting

Virtual COM setting screen enables user to connect a Virtual COM port based device to the Internet. It allows user to access serial data remotely. There are TCP Client, TCP Server, UDP, and RFC2217 modes for remote accessing the connected serial device.

To use the Virtual COM function, you have to specify the operation mode for the multi-function serial port first. Go to Field Communication > Bus & Protocol > Port Configuration tab, select the Virtual COM as expected operation mode, and finish the related port configuration as well.
After that, go to **Field Communication > Bus & Protocol > Virtual COM** tab for detailed configuration of Virtual COM setting.

Enable TCP Client Mode

Configure the gateway as the TCP (Transmission Control Protocol) Client. In TCP Client mode, device initiates a TCP connection with a TCP server when there is data to transmit. Device disconnects from the server when the connection is Idle for a specified period. You may also enable full time connection with the TCP server.

Operation Mode Definition for each Serial Port									
Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	TCP Client	N/A	N/A	N/A	Always on	N/A	N/A	☐	Edit

Enable TCP Client Mode Window		
Item	**Value setting**	**Description**
Operation Mode	A Must filled setting	Select **TCP Client**.
Connection Control	**Always on** is set by default	Choose **Always on** for a TCP full time connection. Otherwise, choose **On-Demand** to initiate TCP connection only when required to transmit and disconnect at idle timeout.
Connection Idle Timeout	1. 0 is set by default 2. Range 0 to 60 min.	Enter the idle timeout in minutes. The idle timeout is used to disconnect the TCP connection when idle time elapsed . Idle timeout is only available when **On-Demand** is selected in the **Connection Control** field. ***Value Range*: 0 ~ 60 minutes.**
Alive Check Timeout	1. 0 is set by default 2. Range 0 to 60 min.	Enter the time period of alive check timeout. The TCP connection will be terminated if it doesn't receive response of alive-check longer than this timeout setting ***Value Range*: 0 ~ 60 minutes.**
Enable	The box is unchecked by default.	Check the **Enable** box to activate the corresponding serial port in specified operation mode.
Save	*N/A*	Click the **Save** button to save the configuration

Modbus Cellular Gateway

Specify Remote TCP Server

ID	To Remote Host	Remote Port	Serial Port	Definition Enable	Action
1		4001	SPort-0	☐	Edit
2		4001	SPort-0	☐	Edit
3		4001	SPort-0	☐	Edit
4		4001	SPort-0	☐	Edit

Legal Host IP/ FQDN Definition (for TCP Client operation mode)

Specify TCP Server Window		
Item	**Value setting**	**Description**
To Host	A Must filled setting	Press **Edit** button to enter IP address or FQDN of the remote TCP server to transmit serial data.
Remote Port	1.A Must filled setting 2.Default value is 4001	Enter the TCP port number. This is the listen port of the remote TCP server. *Value Range*: 1 ~ 65535.
Serial Port	SPort-0 is set by default	Apply the TCP server connection for a selected serial port. Up to 4 TCP servers can be configured at the same time for each serial port.
Definition Enable	The box is unchecked by default	Check the **Enable** box to enable the TCP server configuration.
Save	*N/A*	Click the **Save** button to save the configuration

Modbus Cellular Gateway

Enable TCP Server Mode

Configure the gateway as the TCP (Transmission Control Protocol) Server. The TCP Server waits for connections to be initiated by a remote TCP client device to receive serial data. The setting allows user to specify specific TCP clients or allow any to send serial data for serial data transmission bandwidth control and access control. The TCP Server supports up to 4 simultaneous connections to receive serial data from multiple TCP clients.

Operation Mode Definition for each Serial Port									
Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	TCP Server	4001	Allow All	1	N/A	0	0	☐	Edit

Enable TCP Server Mode Window		
Item	**Value setting**	**Description**
Operation Mode	A Must filled setting	Select **TCP Server** mode.
Listen Port	4001 is set by default	Indicate the listening port of TCP connection. ***Value Range***: 1 ~ 65535.
Trust Type	**Allow All** is set by default	Choose **Allow All** to allow any TCP clients to connect. Otherwise choose **Specific IP** to limit certain TCP clients.
Max Connection	1. Max. 4 connections 2. 1 is set by default	Set the maximum number of concurrent TCP connections. Up to 4 simultaneous TCP connections can be established. ***Value Range***: 1 ~ 4.
Connection Idle Timeout	0 is set by default	Enter the idle timeout in minutes. The idle timeout is used to disconnect the TCP connection when idle time elapsed . Idle timeout is only available when **On-Demand** is selected in the **Connection Control** field. ***Value Range***: 0 ~ 60 minutes.
Alive Check Timeout	0 is set by default	Input the time period of alive check timeout. The TCP connection will be terminated if it doesn't receive response of alive-check longer than this timeout setting. ***Value Range***: 0 ~ 60 minutes.
Enable	The box is unchecked by default.	Check the **Enable** box to activate the corresponding serial port in specified operation mode.
Save	*N/A*	Click **Save** button to save the settings.

Modbus Cellular Gateway

Specify TCP Clients for TCP Server Access

If you selected **Specific IPs** as the trust Type, the Trusted IP Definition window appears. The settings are valid for both TCP Server and RFC-2217 modes.

ID	Host	Serial Port	Definition Enable	Action
1			☐	Edit
2			☐	Edit
3			☐	Edit
4			☐	Edit
5			☐	Edit
6			☐	Edit
7			☐	Edit
8			☐	Edit

Specify TCP Clients Window		
Item	**Value setting**	**Description**
Host	A Must filled setting	Enter the IP address range of allowed TCP clients.
Serial Port	The box is unchecked by default	Check the box to specify the rule for selected Serial Port.
Definition Enable	The box is unchecked by default	Check the **Enable** box to enable the rule.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Enable UDP Mode

UDP (User Datagram Protocol) enables applications using UDP socket programs to communicate with the serial ports on the serial server. The UDP mode provides connectionless communications, which enable you to multicast data from the serial device to multiple host computers, and vice versa, making this mode ideal for message display applications.

Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	UDP	4001	N/A	N/A	N/A	N/A	N/A	☐	Edit

Modbus Cellular Gateway

Enable UDP Mode Window		
Item	**Value setting**	**Description**
Operation Mode	A Must filled setting	Select **UDP** mode.
Listen Port	4001 is set by default	Indicate the listening port of UDP connection. ***Value Range*: 1 ~ 65535**
Enable	The box is unchecked by default.	Check the **Enable** box to activate the corresponding serial port in specified operation mode.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Specify Remote UDP

Specify Remote UDP hosts Window		
Item	**Value setting**	**Description**
Host	A Must filled setting	Press **Edit** button to enter IP address range of remote UDP hosts.
Remote Port	4001 is set by default	Indicate the UDP port of peer UDP hosts. ***Value Range*: 1 ~ 65535**
Serial Port	SPort-0 is set by default	Apply the UDP hosts for a selected serial port. Up to 4 UDP servers can be configured at the same time for each serial port.
Definition Enable	The box is unchecked by default	Check the **Enable** box to enable the rule.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Modbus Cellular Gateway

Enable RFC-2217 Mode

RFC-2217 defines general COM port control options based on telnet protocol. With the RFC-2217 mode, remote host can monitor and manage remote serially attached devices, as though they were connected to the local serial port. When a virtual serial port on the local serial device is being created, it is required to specify the IP-address of the remote hosts to establish connection with.

Operation Mode Definition for each Serial Port									
Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	RFC-2217	4001	Allow All	N/A	N/A	0	0	☐	Edit

Enable RFC-2217 Mode Window		
Item	**Value setting**	**Description**
Operation Mode	A Must filled setting	Select **RFC-2217** mode.
Listen Port	4001 is set by default	Indicate the listening port of RFC-2217 connection. *Value Range*: 1 ~ 65535
Trust Type	**Allow All** is set by default	Choose **Allow All** to allow any clients to connect. Otherwise choose **Specific IP** to limit certain clients.
Connection Idle Timeout	0 is set by default	Enter the idle timeout in minutes. The idle timeout is used to disconnect the connection when idle time elapsed . *Value Range*: 0 ~ 60 minutes.
Alive Check Timeout	0 is set by default	Input the time period of alive check timeout. The connection will be terminated if it doesn't receive response of alive-check longer than this timeout setting. *Value Range*: 0 ~ 60 minutes.
Enable	The box is unchecked by default.	Check the **Enable** box to activate the corresponding serial port in specified operation mode.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Modbus Cellular Gateway

Specify Remote Host for Access

If you selected **Specific IPs** as the trust Type, the Trusted IP Definition window appears. The settings are valid for both TCP Server and RFC-2217 modes.

ID	Host	Serial Port	Definition Enable	Action
1			☐	Edit
2			☐	Edit
3			☐	Edit
4			☐	Edit
5			☐	Edit
6			☐	Edit
7			☐	Edit
8			☐	Edit

Trusted IP Definition (for TCP Server & RFC-2217 operation mode)

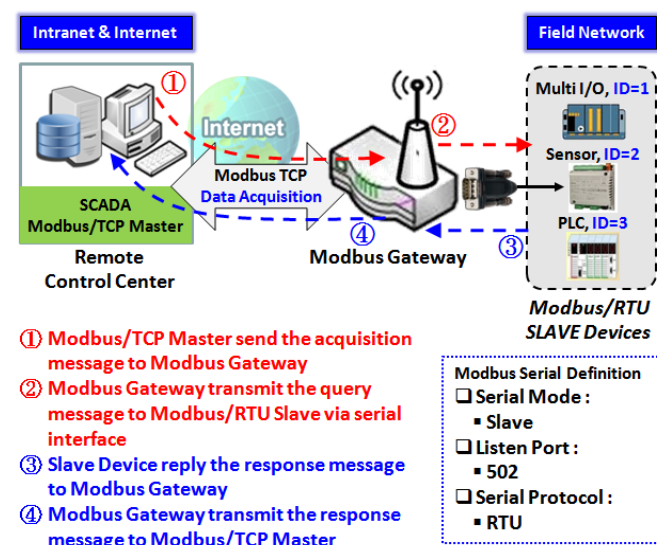| Specify RFC-2217 Clients for Access Window		
Item	**Value setting**	**Description**
Host	A Must filled setting	Enter the IP address range of allowed clients.
Serial Port	The box is unchecked by default	Check the box to specify the rule for selected Serial Port.
Definition Enable	The box is unchecked by default	Check the **Enable** box to enable the rule.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Modbus Cellular Gateway

4.1.3 Modbus

Modbus is one of the most popular automation protocols in the world, supporting traditional RS-232/422/485 devices and recently developed Ethernet devices. Many industrial devices, such as PLCs, DCSs, HMIs, instruments, and smart meters, use Modbus protocol as the communication standard. It is used to establish master-slave communication between intelligent devices.

However, the Ethernet-based Modbus protocol is so different from the original serial-based protocols. In order to integrate Modbus networks, the IoT Gateway, including one or more serial ports that support RS-232 and RS-485 communication interface, can automatically and intelligently translate between Modbus TCP (Ethernet) and Modbus RTU/ASCII (serial) protocols, allowing Ethernet-based PLCs to control instruments over RS-485 without additional programming or effort.

Serial Port Definition

Serial Port	Operation Mode	Interface	Baud Rate	Data Bits	Stop Bits	Flow Control	Parity	Action
SPort-0	Modbus	RS-485	115200	8	1	None	None	Edit

NOTE: When Modbus devices are connected to/under the same serial port of IoT Modbus Gateway, those Modbus devices must use the same protocol with the same configuration (i.e., either Modbus RTU or Modbus ASCII with same Baud Rate setting).

Modbus Gateway Scenario

① Modbus/TCP Master send the acquisition message to Modbus Gateway
② Modbus Gateway transmit the query message to Modbus/RTU Slave via serial interface
③ Slave Device reply the response message to Modbus Gateway
④ Modbus Gateway transmit the response message to Modbus/TCP Master

Modbus Serial Definition
❏ Serial Mode :
  ▪ Slave
❏ Listen Port :
  ▪ 502
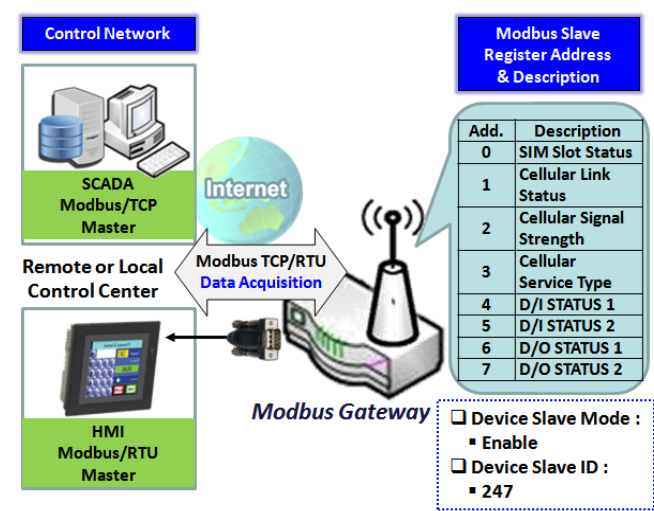❏ Serial Protocol :
  ▪ RTU

The IoT Gateway serves as a Modbus gateway to communicate with the Modbus TCP Master, the SCADA Server, located at remote control center for Modbus device accessing.

The Modbus TCP Master requests the IoT Gateway for Modbus devices' information, e.g., Data Acquisition or Register/Value Modification, via general Internet accessing, and the IoT Gateway serves as the gateway for data forwarding.

Under such configuration, the Modbus TCP Master requests the information from or sending control commands to various Modbus/RTU Slave devices that attached to the Modbus Gateway. And the Modbus gateway executes corresponding processes and replies the Modbus/TCP Master with the results.

Modbus Cellular Gateway

Modbus Slave Scenario

Add.	Description
0	SIM Slot Status
1	Cellular Link Status
2	Cellular Signal Strength
3	Cellular Service Type
4	D/I STATUS 1
5	D/I STATUS 2
6	D/O STATUS 1
7	D/O STATUS 2

❑ Device Slave Mode :
  ▪ Enable
❑ Device Slave ID :
  ▪ 247

In addition to behave as a Modbus Gateway, there is an integrated Modus Slave option for providing some device status, like Cellular Network Status, device DI/DO status, to remote Modbus Master via Modbus communication.

With the Slave option enabled, the Modbus Master device can request the information or sending control commands to the IoT Gateway, the Modbus TCP/RTU Slave device. And IoT Gateway executes corresponding processes and replies the Modbus Master devices.

Modbus Cellular Gateway

Modbus Setting

Go to **Field Communication > Bus & Protocol > Modbus** tab.

The Modbus setting page enables user to configure the gateway to operate as a Modbus gateway, and allow access among Modbus TCP devices (which are connected to Ethernet network) and Modbus RTU/ASCII devices (which are connected to the Serial Port of the gateway). Once completed the Modbus settings in this section, ensure to select Modbus Operation Mode in Port Configuration screen to enable Modbus communication on the serial port.

Enable Modbus Gateway

Gateway Configuration		
Item	**Value setting**	**Description**
Modbus Gateway	The box is checked by default.	Check the **Enable** box to enable Modbus gateway function.
Response Timeout	**1000 ms** is set by default	This sets the response timeout of the slave after master request sent. If the slave does not response within the specified time, data would be discarded. This applies to the serially attached Master sent request over to the remote Slave or requests send from the remote Master sent to the serially attached Slave. *Value Range*: 1 ~ 65535.

Modbus Cellular Gateway

Timeout Retries	**0** is set by default	If the slave does not respond to the Master's request, the gateway will resend the request stored in the buffer. If Timeout retries is set to null (value zero), the gateway would not buffer Master requests. If a value other than zero is specified, the gateway would store the Master request in the buffer and retries to send the request in a number of specified times. Once the retries are exhausted, the gateway will send a Modbus error message to the Master. However, if the 0Bh exception box is checked (see below), a 0Bh hex code based-error message will be send instead. ***Value Range:*** 0 ~ 5.
0Bh Exception	The box is unchecked by default.	Check the **Enable** box to enable gateway to send a 0Bh exception code message to Modbus Master to indicate that the slave device does not respond within the timeout interval.
Tx Delay	The box is unchecked by default.	Check the **Enable** box to activate to the minimum amount of time after receiving a response before the next message can be sent out. When Tx Delay is enabled the Gateway would insert a Tx delay between Master requests. The delay gives sufficient time for the slave devices to turn their transmitters off and their receivers back on.

Setup TCP/IP Connection for Receiving Modbus Master Request

The following Modbus TCP Configuration items allow user to set up the TCP connection settings so that the remote Modbus Master can access to the Modbus gateway. Besides, it also allows user to specify authorized masters on the TCP network.

Item	Value setting	Description
TCP Connection Idle Time	1. **300** is set by default 2. Range 1 to 65535	Enter the idle timeout in seconds. If the gateway does not receive another TCP request before the idle timeout elapsed, the TCP session will be terminated automatically. ***Value Range:*** 1 ~ 65535.
Maximum TCP Connections	1. 4 is set by default 2. Range 1 to 4	Enter the allowed maximum simultaneous TCP connections. ***Value Range:*** 1 ~ 4.
TCP Keep-alive	The box is unchecked by default.	Check the **Enable** box to ensure to keep the TCP session connected.
Modbus Master IP Access	**Allow All** is selected by default.	Specify authorized masters on the TCP network. Select **Allow All** to allow any Modbus Master to reach the attached Slave(s). Otherwise, limit only specific Master to reach the Slave(s) by selecting **Specific IPs**. When **Specific IPs** is selected, a Trusted IP Definition dialog will appear.

Specify Trusted Modbus Masters on the TCP network

When **Specific IPs** is selectes, user has to specify the Master(s) by their IP addresses to reach the serially attached Slave(s).

Modbus Cellular Gateway

Item	Value setting	Description
Source IP	A Must fill setting	Select **Specific IP Address** to only allow an IP address of the allowed Master to access the attached Slave(s). Select **IP Range** to only allow a set range of IP addresses of the allowed Master to access the attached Slave(s). Select **IP Address-based Group** to only allow pre-defined group of IP address of the allowed Master to access the attached Slave(s). Note: group must be pre-defined before this selection become available. Refer to **Object Definition > Grouping > Host grouping**. You may also access to create a group by the Add Rule shortcut button. Setting done through the Add Rule button will also appear in the Host grouping setting screen. Then check **Enable** box to enable this rule.
Serial Port	Unchecked by default	Check the **Enable** box to enable the rule in chosen Serial Port.
Enable	Unchecked by default	Check the **Enable** box to enable this rule.

Enable Integrated Modbus Slave for the Gateway

This setting can setup the Gateway as a standalone Modbus Slave Device. Local SCADA Management System can treat the Gateway as a Slave device, and hence is able to read its information for device monitoring.

Item	Value setting	Description
Device Slave Mode	The box is unchecked by default.	Check the **Enable** box to activate the integrated Modbus Salve function, so that it can function as a Modbus Slave device, and can be accessed with legacy Modbus Function Code from a SCADA management system. Supported Modbus commands are listed in the following Table.
Device Slave ID	1. 1 is set by default 2. Range 1 to 247	Enter the preferred ID for the integrated Modbus slave. *Value Range*: 1 ~ 247.

Modbus Cellular Gateway

Currently, the integrated Modbus Slave device supports the following commands for accessing the 3G/4G Modem Status of the Gateway.

Function Code: 0x03(/Read). 0x06(/Write)
Address: 0 ~ 7

Register Address	Register Name	R / W	Register Range / Description
0	3G/4G_PHYSICAL_INTERFACE	R	1=3G/4G
1	3G/4G_LINK_STATUS	R	0 ~ 6, 0=Disconnected, 1=Connecting…, 2=Connected, 3=Disconnecting…, 5=Wait for Traffic…, 6=Diconnected
2	3G/4G_SIGNAL_STRENGTH	R	0 ~ 100
3	3G/4G_SERVICE_TYPE	R	0 ~ 7, 0=2G, 1=none, 2=3G, 3=3.5G, 4~6=3.75G, 7=LTE
4	DI_STATUS_1	R	0 : OFF, 1:ON
5	DI_STATUS_2	R	0 : OFF, 1:ON
6	DO_STATUS_1	R/W	0 : OFF, 1:ON
7	DO_STATUS_2	R/W	0 : OFF, 1:ON

Modbus Priority Definition

Message Buffering must be enabled to prioritize Master request queue to transmit to Modbus Slave as mentioned in the above. Click the **Edit** button to fill in the priority settings.

Item	Value setting	Description
Message Buffering	1. Unchecked by default 2. Buffer up to 32	Check the **Enable** box to buffer up to 32 requests from Modbus Master. If the **Enable** box is checked, a Modbus Priority Definition dialog will appear consequently. So that, the buffered Master requests can further be configured

Modbus Cellular Gateway

	requests	to prioritize request queue to transmit to Slave based on Master's IP address if requests are coming from remote Master, or based on remote Slave ID if requests are coming from serially attached Master, or based on Function Code.
Modbus Priority	N/A	A Priority List for setting the priority of specified Modbus identity. Modbus Priority 1 ~ Modbus Priority 4.
Priority Base	IP Address by Default	User can specify a Modbus identity with **IP Address**, **Slave ID**, or **Function Code**. The buffered Modbus message that matched the specified identity will be handled with given priority. The Modbus Master requests can be buffered to a certain priority queue according to the Master's IP address if requests are coming from remote Master, or the remote Slave's device ID if requests are coming from serially attached Master, or the specific Function Code that issued by Master.
Enable	Unchecked by default	Check the **Enable** box to enable the priority settings.
Save	N/A	Click the **Save** button to save the settings.

Specify the definition of attached serial device(s)

Press **Edit** Button to select serial mode and other configuration in the following setting.

Modbus Serial Definition					
Serial Port	**Serial Mode**	**Listen Port**	**Serial Protocol**	**Enable**	**Action**
▶ SPort-0	Slave ▾	502 (1~65535)	RTU ▾	☑	Edit

Modbus Serial Definition		
Item	**Value setting**	**Description**
Serial Port	N/A	It displays the name of the serial port used. E.g. SPort-0. The number of serial ports varies from the purchased model.
Serial Mode	**Slave** is set by default	Specify the serial device mode for the attached Modbus device(s). It can be **Slave** or **Master**. A serial port can be attached with one Modbus Master, or daisy-chained a group of Modbus Salve devices.
Listen Port	1. 502 is set by default 2. Range 1 to 65535	Specify the Listen Port number if a Slave device is attached. It is a don't care setting if a Master device is attached. ***Value Range*: 1 ~ 65535.**
Serial Protocol	RTU is set by default	Select the serial protocol that is adopted by the attached Modbus device(s) It can be **RTU** or **ASCII**.
Enable	N/A	It displays whether the specific Modbus Serial Port is enabled or disabled. To enable or disable Modbus Serial Port, go to **Field Communication > Bus & Protocol > Port Configuration** tab, and set the operation mode as **Modbus**.

Modbus Cellular Gateway

Specify Modbus TCP Slave device(s)

If there is a Modbus Master device is attached to the serial port of the Modbus Gateway, user has to further specify the Modbus TCP Slave device(s) to send requests to from the attached Modbus RTU/ASCII Master device.

ID	IP	Port	ID Range	Local Serial Port	Enable	Actions

When the **Add** button is applied, a **Modbus TCP Slave Configuration** screen will appear.

Item	Setting
▶ IP	
▶ Port	(1~65535)
▶ ID Range	(1~247) ~ (1~247)
▶ Local Serial Port	☐ SPort-0
▶ Enable	☐

Modbus Remote Slave Configuration		
Item	**Value setting**	**Description**
IP	A Must fill setting	Enter the IP address of the remote Modbus TCP Slave device.
Port	1. A Must fill setting 2. Range 1 to 65535	Enter the TCP port on which the remote Modbus TCP Slave device listens (to the TCP client session request). ***Value Range*: 1 ~ 65535.**
ID Range	Range 1 to 247	Enter the Modbus ID range for the Modbus TCP Slave(s) that will respond to the Master's request. In addition to specify the Slave IP and Port, for accessing those Remote Modbus RTU Salve(s) located behind another Modbus Gateway, user has to specify the Modus ID range of the Modbus RTU Slave(s). ***Value Range*: 1 ~ 247.**
Local Serial Port	It is unchecked by default.	Select the Serial port(s) from which the Master's request will be sent to the Modbus TCP Slave(s). If the check box is grayed out and not available, ensure that you have Master option selected in the Modbus Serial Definition sub-screen and save the setting. Note: The number of Serial Port supported depends on the gateway model purchased.
Enable	It is unchecked by default.	Check the **Enable** box to enable this rule.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the changes.

Modbus Cellular Gateway

4.2 Data Logging

Data logging is the process of collecting and storing data over a period of time in order to analyze specific trends or record the data-based events/actions of a system, or connected devices. Data logging function is a very useful and also important feature for SCADA telemetry; it makes the monitoring and analyzing tasks easier by checking the status and historical data during whole data acquisition period.

Even facing the network connection problems with remote NOC/SCADA side, you can also enable the data logging proxy function provided by the purchased gateway and keep doing the data acquisition and storing the collected data in local storage (in .CSV file format). When the network connection recovered, admin/user can download the data log files manually via FTP or web UI for further reference and maintenance.
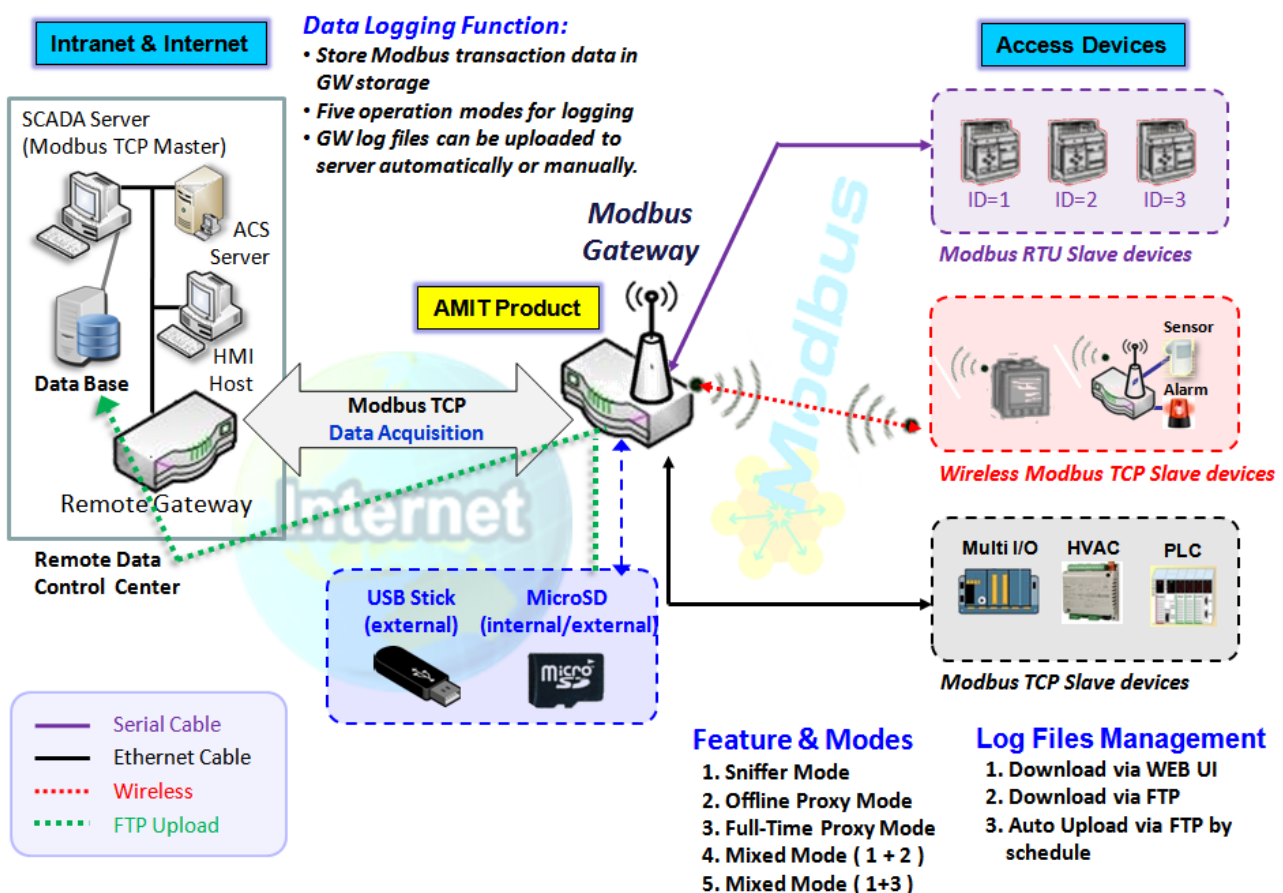
The Modbus Cellular Gateway provides a complete data logging function for collecting the Modbus transaction data for application requirements. There are some data logging schemes to meet different management requirements. They are the Sniffer Mode, Offline Proxy Mode, Full-Time Proxy Mode, and the mixed modes for sniffer and proxy combinations.

With the Sniffer mode enabled, the gateway will monitor and record the communication among a specific Modbus Master and related slaves. It will store the Modbus communication as log files and administrator can check what Modbus communication went over the Modbus gateway, and if there is any communication loss

Modbus Cellular Gateway

among the Master and Slave sides or not.

However, if there is any network connection problem between the Modbus gateway and remote NOC/SCADA, the remote Modbus server can't reach the Slave devices attached to the Modbus gateway, and consequently, nothing can be monitored and stored under such situation.

With the Proxy mode option enabled, when the Modbus gateway lost the connection with specified Modbus server, it will take over the data acquisition task and keep collecting the required data from Slave devices automatically. Once the connection is recovered, the Modbus gateway may stop the data log proxy function. Remote Modbus server can keep its data acquisition process, and if required, the administrator can also get the stored data log files to tell if everything goes well or not.

Under the Data Logging Proxy mode, user has to create some data acquisition rules via "Proxy Mode Rule Configuration" for collecting the Slave devices data by the Gateway when required. Once the network connection to remote SCADA was lost unexpectedly, the Data Logging Proxy function will be triggered and begin to do the data polling tasks by those pre-defined rules running in background.

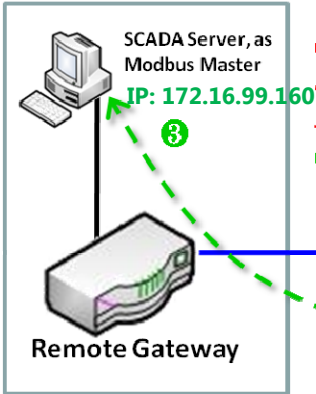➢ **Scenario for Sniffer Mode Data Logging**
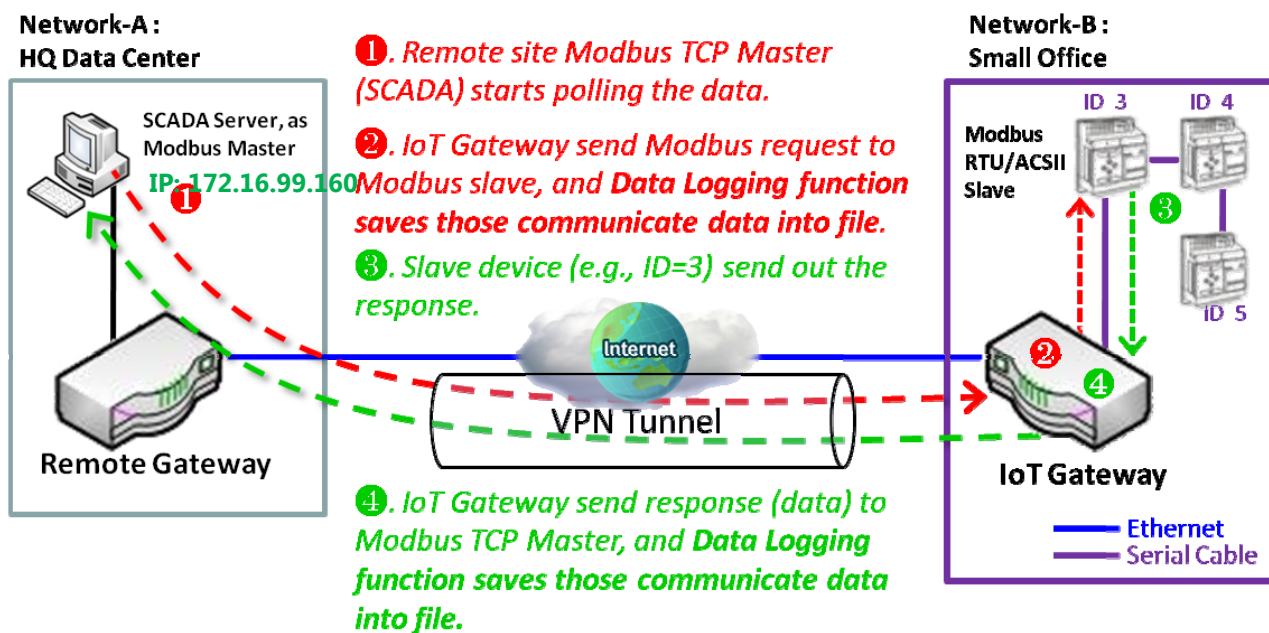
As Illustrated in the diagram, the Modbus gateway will store the following Modbus activities into a log file.
- The Modbus request sent from Remote Modbus TCP Master.
- The response (data) that sent out from the polled Slave device (ID=3)

➢ **Scenario for Off-Line Proxy Mode Data Logging**

Modbus Cellular Gateway
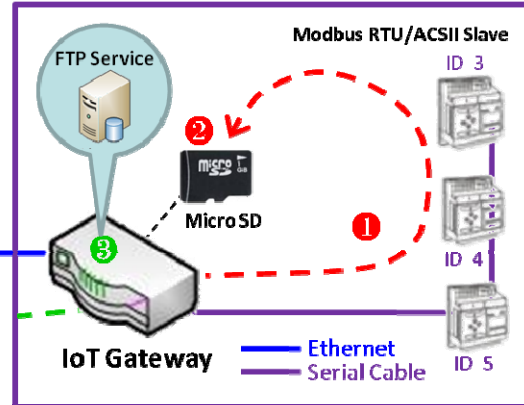
As illustrated, when the connection to a remote Modbus Master broken, the Modbus Gateway will activate the data logging proxy function and execute the pre-defined data acquisition task by itself.

- The Modbus request issued by the Modbus Gateway (Data Logging Proxy).
- The response (data) that sent out from the polled Slave device (ID=3)

Repeat above data acquisition and data logging activities on every 5 sec interval until the connection recovered.

Modbus Cellular Gateway

4.2.1 Data Logging Configuration

Data Logging is commonly used in monitoring systems to collect and analyze the field data. With proper configuration, the Gateway will record Modbus messages according to the specified rule list.

Go to **Field Communication > Data Logging > Configuration** tab.

Enable Data Logging

Configuration		
Item		**Setting**
▸ Data Logging		☐ Enable
▸ Storage Device		External ▾

Configuration Item	Value setting	Description
Data Logging	The box is unchecked by default.	Check the **Enable** box to activate to data logging function.
Storage Device	**External** is set by default	Choose the sotrage device to store the log files. It can be **External** or **Internal**, depends on the product specification.
Save	*NA*	Click the **Save** button to save the settings.

Note:

1. If there is no available storage device, the Enable checkbox will be grayed, and you can't enable it for the data logging. That is, if you selected External Storage, plug-in the storage first, and then enable the function and also make the required configuration.

2. Make sure the Modbus Operation Mode is selected and enabled, or there will be no Modbus transactions to be logged. Please refer to **Field Communication > Bus & Protocol > Port Configuration** and **Modbus** tabs.

Create/Edit Modbus Proxy Rules
The Gateway allows you to customize your proxy mode rule list. It supports up to a maximum of 20 rules.

☐ Modbus Proxy Rule List [Add] [Delete]								
ID	Name	Modbus Slave Type	Slave ID	Function Code	Start Address	Number of Coils/Registers	Polling Rate (ms)	Actions

When the **Add** button is applied, **Modbus Proxy Rule Configuration** screen will appear.

Modbus Cellular Gateway

Modbus Proxy Rule Configuration		
Item	**Value setting**	**Description**
Name	A Must filled setting.	Specify a name as the identifier of the Modbus proxy rule. **_Value Range_**: 1 ~ 32 characters.
Modbus Slave Type	**IP Address :Port** is selected by default.	Specify the Modbus Slave devices to apply with the Modbus proxy rule. It can be **IP Address:Port** for Modbus TCP slaves or **Local Serial Port** for local attached Modbus RTU/ASCII slaves. **_Value Range_**: 1 ~ 65535 for port number
Slave ID	1. A Must filled setting. 2. Range 1 to 247	Specify the ID range for the slave device(s) to apply with the Modbus proxy rule. **_Value Range_**: 1 ~ 247.
Function Code	**Read Coils (0x01)** is seelected by default.	Specify a certain read function for the Data Logging Proxy to issue and record the responses from device(s).
Start Address	1. A Must filled setting. 2. Range 0 to 65535	Specify the Start Address of registers to apply with the specified function code. **_Value Range_**: 0 ~ 65535.
Number of Coils/Registers	1. A Must filled setting. 2. Range 1 to 125	Specify the number of coils/registers to apply with the specified function code. **_Value Range_**: 1 ~ 125. Note: **Start Address** plus **Number** must be smaller than 65536.
Polling Rate (ms)	1. A Must filled setting. 2. **1000** ms is set by default	Enter the poll time in milliseconds to apply the Proxy Mode Rule. Once the proxy mode is activated, the Modbus Gateway will issue pre-defined Modbus message on each Poll Time interval accordingly. **_Value Range_**: 500 ~ 99999.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the changes.

Modbus Cellular Gateway

4.2.2 Scheme Setup

There are five data logging schemes to meet different management requirements. They are the Sniffer Mode, Offline Proxy Mode, Full-Time Proxy Mode, and the mixed modes for sniffer and proxy combinations. User has to configure the required data logging rules with selected scheme in this Scheme Setup page.

Go to **Field Communication > Data Logging > Scheme Setup** tab.

Create/Edit Data Logging Rules

When the **Add** button is applied, **Scheme Configuration** screen will appear.

Scheme Configuration		
Item	**Value setting**	**Description**
Name	A Must filled setting.	Specify a name as the identifier of the data logging rule. ***Value Range*: 1 ~ 16 characters.**
Mode	**Sniffer** is selected by default.	Select an expected data logging scheme for the data logging rule. There are five available schemes : **Sniffer** : The Modbus gateway will record all the Modbus transcations between the Master and Slave devices. **Off-Line Proxy**: When the connection between the Modbus gateway and Master is lost, the pre-defined proxy rule will be triggered and the Modbus gateway will issue specified function code to collect and record the data / status from the slave devices **Full-Time Proxy**: The pre-defined proxy rule will be triggered all the time and the Modbus gateway will issue specified function code to collect and record the data / status from the slave devices

Modbus Cellular Gateway

		Sniffer & Off-Line Proxy: This is a mixed mode for both Sniffer and Off-Line Proxy modes.
		Sniffer & Full-Time Proxy: This is a mixed mode for both Sniffer and Full-Time Proxy modes.
Master Type	**IP Address** is selected by default.	Specify the Modbus master device to apply with the data logging rule. It can be **IP Address** for Modbus TCP master, or **Local Serial Port** for local attached Modbus RTU/ASCII master.
Master Query Timeout (sec.)	1. An Optional setting. 2. **60** sec is set by default 3. Range 1 to 99999	Specify the timeout value for querying Modbus Master. If no response from the master for the specified timeout setting, selected proxy rule will be triggered and applied with the data logging rule. Note: If Off-Line proxy scheme is selected, the timeout setting will be used to check. Otherwise, it is a don't care value.
Proxy Rules	An Optional setting.	Select the Proxy rule to be applied with the data logging rule. Note: If any proxy scheme is selected, please create the required Proxy rules in advance, and select from the list.
Enable	The box is unchecked by default.	Check the box to activate the data logging rule.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the changes.

Modbus Cellular Gateway

4.2.3 Log File Management

There are five data logging schemes to meet different management requirements. They are the Sniffer Mode, Off-Line Proxy Mode, Full-Time Proxy Mode, and the mixed modes for sniffer and proxy combinations. User has to configure the required data logging rules with selected scheme in this Scheme Setup page.

Go to **Field Communication > Data Logging > Log File Management** tab.

If user had created data log rules in the **Field Communication > Data Logging > Scheme Setup** tab, there will be a log file list shown in the following Log File list screen. The default Log File management settings will be applied if user didn't change it via the **Edit** button.

ID	Name	File Content Format	Split File by	Auto Upload	Log File Compression	Delete File After Upload	When Storage Full	Actions
1	Sniffer Log	Raw Data	200 KB	Disabled	N/A	N/A	Remove the Oldest	Edit / Download Log

When the **Edit** button is applied, **Log File Configuration** screen will appear.

Item	Setting
▶ File Content Format	Raw Data ▼
▶ Split File by	Size ▼ 200 KB ▼
▶ Auto Upload	☑ Enable --- Option --- ▼ Add Object
▶ Log File Compression	☐ Enable
▶ Delete File After Upload	☐ Enable
▶ When Storage Full	Remove the Oldest ▼

Log File Configuration		
Item	**Value setting**	**Description**
Name	N/A	The name of corresponding data log rule will be displayed. The default log file name will be named as ' Name_yyyyMMddHHmmSS.csv '.
File Content Format	**Raw Data** is selected by default	Select the data format for the log files. It can be **Raw Data**, or **Modbus Type**.
Split File by	**Size** and **200 KB** are set by default	Specify the split file methodology. It can be by **Size**, or by **Time Interval**. User has to dpecify a certain file size or time interval for splitting the data logs into a series of files.

Modbus Cellular Gateway

|		
		***Value Range*:** 1 ~ 99999.
Auto Upload	1. An Optional filled setting 2. The box is unchecked by default.	Check the **Enable** box to activate the auto upload function for logged files. Once been enabled, user has to specify an external FTP server from the dropdown list for auto uploading the log files to the server. Refer to **Object Definition > External Server > External Server** tab, or create the FTP server with the **Add Object** button.
Log File Compression	1. An Optional filled setting 2. The box is unchecked by default	If Auto Upload is activated, user can further specify whether to compress the log file prior it is uploaded or not. Check the **Enable** button to activate the Log File Compression function...
Delete File After Upload	1. An Optional filled setting 2. The box is unchecked by default	If Auto Upload is activated, user can further specify whether to delete the transferred log from the gateway storage or not. Check the **Enable** button to activate the function.
When Storage Full	**Remove the Oldest** is selected by default	Specify the operation to take when the storage is full. It can be **Remove the Oldest** log file, or **Stop Recording**. When **Remove the Oldest** is selected, the gateway will delete the oldest file once the storage is full, and keep on the data logging activity; When **Stop Recording** is selected, the gateway will stop the data logging activity once the storage is full.
Save	*NA*	Click the **Save** button to save the settings.
Undo	*NA*	Click the **Undo** button to cancel the changes.

When the **Download Log** button is applied, the web browser will download a file named as 'log.tar' to the managing host computer.

Chapter 5 Security

5.1 VPN

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The tunnel technology supports data confidentiality, data origin authentication and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.
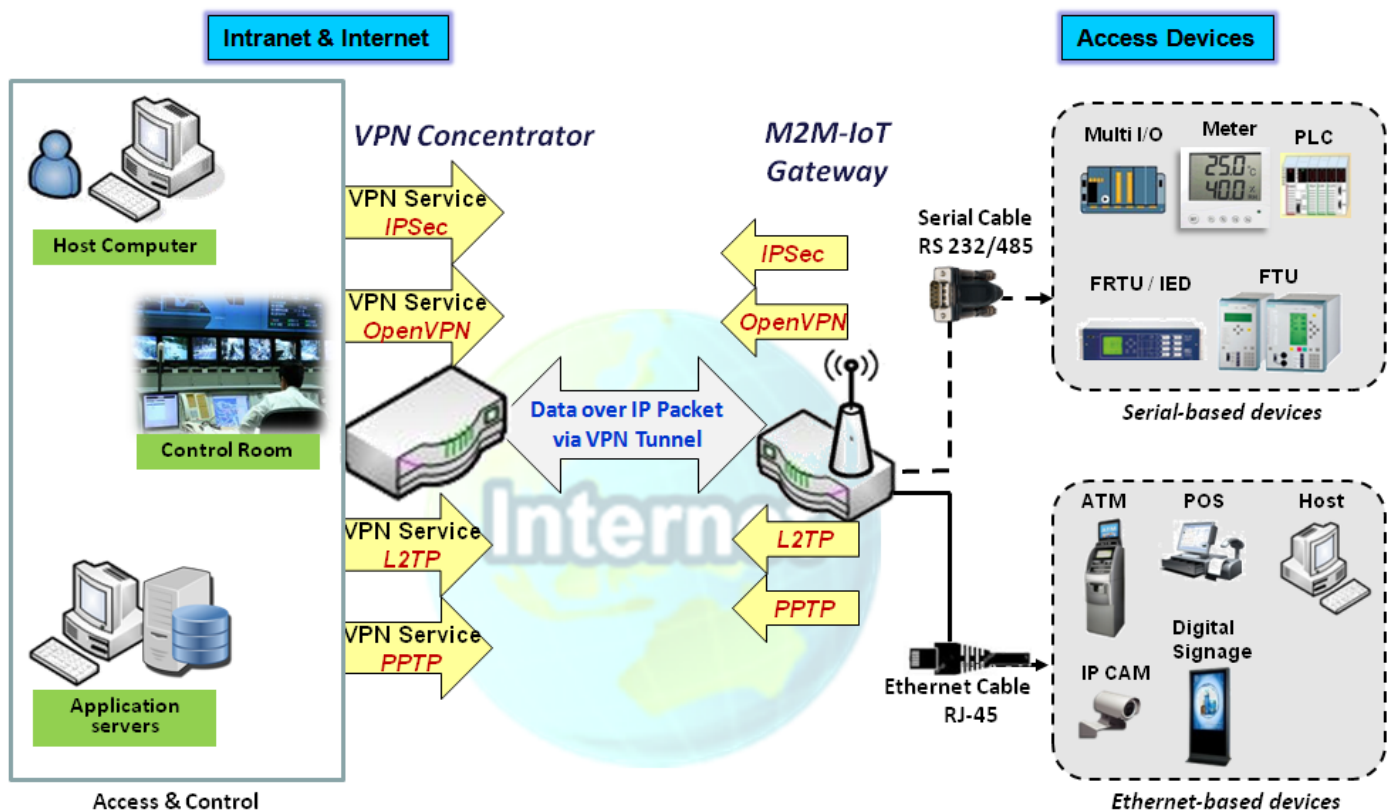
The product series supports different tunneling technologies to establish secure tunnels between multiple sites for data transferring, such as IPSec, OpenVPN, L2TP (over IPSec), PPTP and GRE. Besides, some advanced functions, like Full Tunnel, Tunnel Failover, Tunnel Load Balance, NetBIOS over IPSec, NAT Traversal and Dynamic VPN, are also supported.

Go to **Security > VPN > Configuration** tab. The VPN enable check box must be checked to enable to allow IPSec, OpenVPN, L2TP, PPTP and GRE to function.

Modbus Cellular Gateway

5.1.1 IPSec

Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

An IPSec VPN tunnel is established between IPSec client and server. Sometimes, we call the IPSec VPN client as the initiator and the IPSec VPN server as the responder. This gateway can be configured as different roles and establish number of tunnels with various remote devices. Before going to setup the VPN connections, you may need to decide the scenario type for the tunneling.

IPSec Tunnel Scenarios
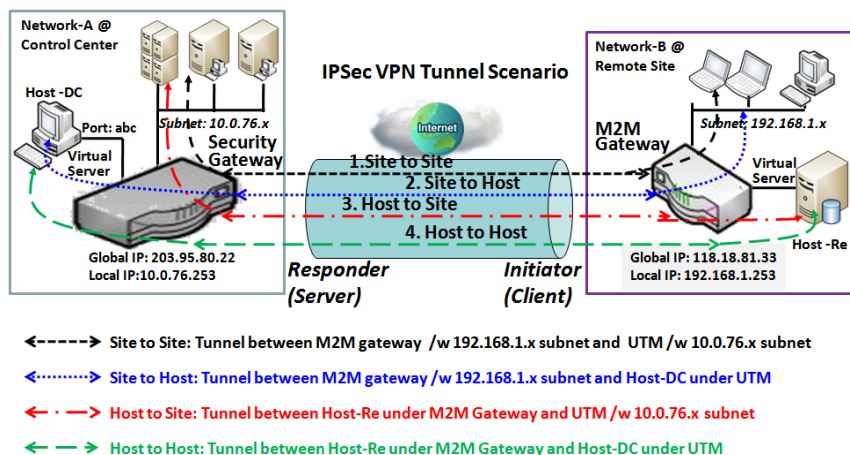
To build IPSec tunnel, you need to fill in remote gateway global IP, and optional subnet if the hosts behind IPSec peer can access to remote site or hosts. Under such configuration, there are four scenarios:

Site to Site: You need to setup remote gateway IP and subnet of both gateways. After the IPSec tunnel established, hosts behind both gateways can communication each other through the tunnel.

152

Modbus Cellular Gateway

Site to Host: Site to Host is suitable for tunneling between clients in a subnet and an application server (host). As in the diagram, the clients behind the M2M gateway can access to the host "Host-DC" located in the control center through Site to Host VPN tunnel.

Host to Site: On the contrast, for a single host (or mobile user to) to access the resources located in an intranet, the Host to Site scenario can be applied.

Host to Host: Host to Host is a special configuration for building a VPN tunnel between two single hosts.

Site to Site with "Full Tunnel" enabled
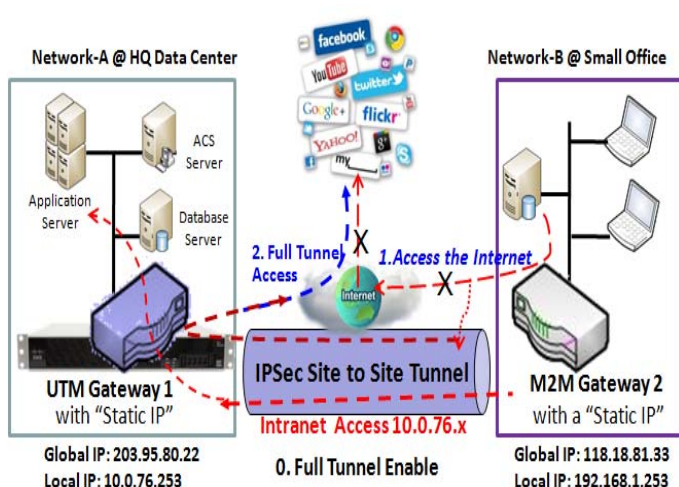
In "Site to Site" scenario, client hosts in remote site can access the enterprise resources in the Intranet of HQ gateway via an established IPSec tunnel, as described above. However, Internet access originates from remote site still go through its regular WAN connection. If you want all packets from remote site to be routed via this IPSec tunnel, including HQ server access and Internet access, you can just enable the "Full Tunnel" setting. As a result, every time users surfs web or searching data on Internet, checking personal emails, or HQ server access, all traffics will go through the secure IPSec tunnel and route by the Security Gateway in control center..

Site to Site with "Hub and Spoke" mechanism
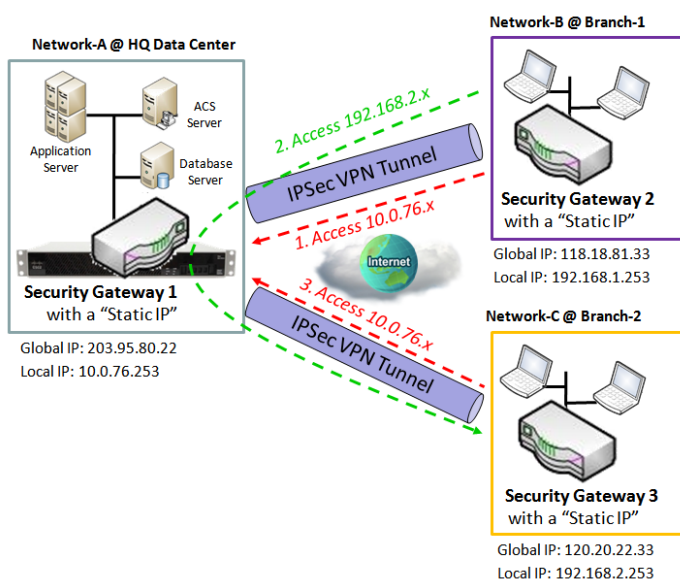
For a control center to manage the secure Intranet among all its remote sites, there is a simple configuration, called **Hub and Spoke**, for the whole VPN network. A Hub and Spoke VPN Network is set up in organizations with centralized control center over all its remote sites, like shops or offices. The control center acts as the Hub role and the remote shops or Offices act as Spokes. All VPN tunnels from remote sites terminate at this Hub, which acts as a concentrator. Site-to-site connections between spokes do not exist. Traffic originating from one spoke and destined for another spoke has to go via the Hub. Under such configuration, you don't need to maintain VPN tunnels between each two remote clients.

Modbus Cellular Gateway

Dynamic VPN Server Scenario
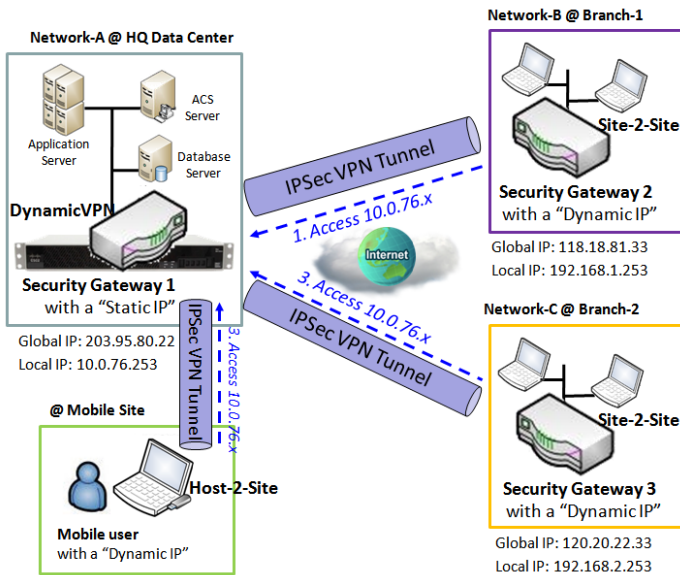
Dynamic VPN Server Scenario is an efficient way to build multiple tunnels with remote sites, especially for mobile clients with dynamic IP. In this scenario, gateway can only be role of server (responder), and it must have a "Static IP" or "FQDN". It can allow many VPN clients (initiators) to connect to with various tunnel scenarios. In short, with a simple Dynamic VPN server setting, many VPN clients can connect to the server. But, in comparison to the Hub and Spoke mechanism, it is not allowed to directly communicate between any two clients via the Dynamic VPN server.

For the purchased gateway, you can configure one Dynamic VPN server for each WAN interface.

Modbus Cellular Gateway

IPSec Setting

Go to **Security > VPN > IPSec** tab.

The IPSec Setting allows user to create and configure IPSec tunnels.

Enable IPSec

Configuration Window		
Item	**Value setting**	**Description**
IPsec	Unchecked by default	Click the **Enable** box to enable IPSec function.
NetBIOS over IPSec	Unchecked by default	Click the **Enable** box to enable NetBIOS over IPSec function.
NAT Traversal	Unchecked by default	Click the **Enable** box to enable NAT Traversal function.
Max. Concurrent IPSec Tunnels	Depends on Product specification.	The specified value will limit the maximum number of simultaneous IPSec tunnel connection. The default value can be different for the purchased model.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Create/Edit IPSec tunnel

Ensure that the IPSec enable box is checked to enable before further configuring the IPSec tunnel settings.

When **Add/Edit** button is applied, a series of configuration screens will appear. They are Tunnel Configuration, Local & Remote Configuration, Authentication, IKE Phase, IKE Proposal Definition, IPSec Phase, and IPSec Proposal Definition. You have to configure the tunnel details for both local and remote VPN devices.

Modbus Cellular Gateway

Tunnel Configuration Window		
Item	**Value setting**	**Description**
Tunnel	Unchecked by default	Check the **Enable** box to activate the IPSec tunnel
Tunnel Name	1. A Must fill setting 2. String format can be any text	Enter a tunnel name. Enter a name that is easy for you to identify. ***Value Range***: 1 ~ 19 characters.
Interface	1. A Must fill setting 2. WAN 1 is selected by default	Select WAN interface on which IPSec tunnel is to be established.
Tunnel Scenario	1. A Must fill setting 2. Site to site is selected by default	Select an IPSec tunneling scenario from the dropdown box for your application. Select **Site-to-Site**, **Site-to-Host**, **Host-to-Site**, or **Host-to-Host**. With **Site-to-Site** or **Site-to-Host** or **Host-to-Site**, IPSec operates in tunnel mode. The difference among them is the number of subnets. With **Host-to-Host**, IPSec operates in transport mode.
Hub and Spoke	1. An optional setting 2. None is set by default	Select from the dropdown box to setup your gateway for Hub-and-Spoke IPSec VPN Deployments. Select **None** if your deployments will not support Hub or Spoke encryption. Select **Hub** for a Hub role in the IPSec design. Select **Spoke** for a Spoke role in the IPSec design. Note: Hub and Spoke are available only for Site-to-Site VPN tunneling specified in Tunnel Scenario. It is not available for Dynamic VPN tunneling application.
Operation Mode	1. A Must fill setting 2. Alway on is selected by default	There are three available operation modes. Always On, Failover, Load Balance. **Failover/ Always on**: Define whether the IPSec tunnel is a failover tunnel function or an Always on tunnel. Note: If this IPSec is a failover tunneling, you will need to select a primary IPSec tunnel from which to failover to. **Load Balance**: Define whether the IPSec tunnel connection will take part in load balance function of the gateway. You will not need to select with WAN interface

Modbus Cellular Gateway

		as the system will automatically utilize the available WAN interfaces to balance traffic loads. For more details on WAN Load Balance, refer to **Basic Network > WAN > Load Balance** tab. Note_1: Load Balance function is not available for the gateway with single WAN. Note_2: Failover and Load Balance functions are not available for Dynamic VPN specified in Tunnel Scenario.
Encapsulation Protocol	1. A Must fill setting 2. ESP is selected by default	Select the Encapsulation Protocol from the dropdown box for this IPSec tunnel. Available encapsulations are ESP and AH.
Keep alive	1. Unchecked by default 2. 30s is set by default	Check the **Enable** box to enable Keep alive function. Select Ping IP to keep live and enter the IP address to ping. Enter the ping time interval in seconds. *Value Range*: 30 ~ 999 seconds. Note: Keep alive option is not available for Dynamic VPN specified in Tunnel Scenario.

Local & Remote Configuration Window		
Item	**Value setting**	**Description**
Local Subnet List	A Must fill setting	Specify the Local Subnet IP address and Subnet Mask. Click the Add or Delete button to add or delete a Local Subnet. Note_1: When Dynamic VPN option in Tunnel Scenario is selected, there will be only one subnet available. Note_2: When Host-to-Site or Host-to-Host option in Tunnel Scenario is selected, Local Subnet will not be available. Note_3: When Hub and Spoke option in Hub and Spoke is selected, there will be only one subnet available.

Modbus Cellular Gateway

Full Tunnel	Unchecked by default	Click **Enable** box to enable Full Tunnel. Note: Full tunnel is available only for Site-to-Site specified in Tunnel Scenario.
Remote Subnet List	A Must fill setting	Specify the Remote Subnet IP address and Subnet Mask. Click the Add or Delete button to add or delete Remote Subnet setting.
Remote Gateway	1. A Must fill setting. 2. Format can be a ipv4 address or FQDN	Specify the Remote Gateway.

Authentication Configuration Window		
Item	**Value setting**	**Description**
Key Management	1. A Must fill setting 2. Pre-shared Key 8 to 32 characters.	Select Key Management from the dropdown box for this IPSec tunnel. **IKE+Pre-shared Key**: user needs to set a key (8 ~ 32 characters). **IKE+X.509**: user needs Certificate to authenticate. IKE+X.509 will be available only when Certificate has been configured properly. Refer to Certificate section of this manual and also **Object Definition > Certificate** in web-based utility. **Manually**: user needs to enter key ID to authenticate. Manual key configuration will be explained in the following Manual Key Management section.
Local ID	An optional setting	Specify the Local ID for this IPSec tunnel to authenticate. Select **User Name** for Local ID and enter the username. The username may include but can't be all numbers. Select **FQDN** for Local ID and enter the FQDN. Select **User@FQDN** for Local ID and enter the User@FQDN. Select **Key ID** for Local ID and enter the Key ID (English alphabet or number).
Remote ID	An optional setting	Specify the Remote ID for this IPSec tunnel to authenticate. Select **User Name** for Remote ID and enter the username. The username may include but can't be all numbers. Select **FQDN** for Local ID and enter the FQDN. Select **User@FQDN** for Remote ID and enter the User@FQDN. Select **Key ID** for Remote ID and enter the Key ID (English alphabet or number). Note: Remote ID will be not available when Dynamic VPN option in Tunnel Scenario is selected.

Modbus Cellular Gateway

IKE Phase Window		
Item	**Value setting**	**Description**
IKE Version	1. A must fill setting 2. v1 is selected by default	Specify the IKE version for this IPSec tunnel. Select v1 or v2 Note: IKE versions will not be available when Dynamic VPN option in Tunnel Scenario is selected, or AH option in Encapsulation Protocol is selected.
Negotiation Mode	Main Mode is set by default default	Specify the Negotiation Mode for this IPSec tunnel. Select Main Mode or Aggressive Mode.
X-Auth	None is selected by default	Specify the X-Auth role for this IPSec tunnel. Select Server, Client, or None. Selected None no X-Auth authentication is required. Selected Server this gateway will be an X-Auth server. Click on the X-Auth Account button to create remote X-Auth client account. Selected Client this gateway will be an X-Auth client. Enter User name and Password to be authenticated by the X-Auth server gateway. Note: X-Auth Client will not be available for Dynamic VPN option selected in Tunnel Scenario.
Dead Peer Detection (DPD)	1. Unchecked by default 2. Default Timeout 180s and Delay 30s	Click **Enable** box to enable **DPD** function. Specify the **Timeout** and **Delay** time in seconds. **_Value Range_**: 0 ~ 999 seconds for **Timeout** and **Delay**.
Phase1 Key Life Time	1. A Must fill setting 2. Default 3600s 3. Max. 86400s	Specify the Phase1 Key Life Time. **_Value Range_**: 30 ~ 86400.

Modbus Cellular Gateway

ID	Encryption	Authentication	DH Group	Definition
IKE Proposal Definition				
1	AES-auto ▼	SHA1 ▼	Group 2 ▼	☑ Enable
2	AES-auto ▼	MD5 ▼	Group 2 ▼	☑ Enable
3	DES ▼	SHA1 ▼	Group 2 ▼	☑ Enable
4	3DES ▼	SHA1 ▼	Group 2 ▼	☑ Enable

IKE Proposal Definition Window		
Item	**Value setting**	**Description**
IKE Proposal Definition	A Must fill setting	Specify the Phase 1 Encryption method. It can be AES-auto / AES128 / AES192 / AES256 / DES / 3DES. Specify the Authentication method. It can be None / MD5 / SHA1 / SHA2-256 / SHA2-512. Specify the DH Group. It can be None / Group1 / Group2 / Group5 / Group14 / Group15 / Group16 / Group17 / Group18. Check **Enable** box to enable this setting

Item	Setting
IPSec Phase	
▶ Phase2 Key Life Time	28800 (seconds) (Max. 86400)

IPSec Phase Window		
Item	**Value setting**	**Description**
Phase2 Key Life Time	1. A Must fill setting 2. 28800s is set by default 3. Max. 86400s	Specify the Phase2 Key Life Time in second. ***Value Range*: 30 ~ 86400.**

ID	Encryption	Authentication	PFS Group	Definition
IPSec Proposal Definition				
1	AES-auto ▼	SHA1 ▼		☑ Enable
2	AES-auto ▼	MD5 ▼		☑ Enable
3	DES ▼	SHA1 ▼	Group 2 ▼	☑ Enable
4	3DES ▼	SHA1 ▼		☑ Enable

IPSec Proposal Definition Window		
Item	**Value setting**	**Description**
IPSec Proposal Definition	A Must fill setting	Specify the Encryption method. It can be None / AES-auto / AES128 / AES192 / AES256 / DES / 3DES. Specify the Authentication method. It can be None / MD5 / SHA1 / SHA2-256 / SHA2-512. Specify the PFS Group. It can be None / Group1 / Group2 / Group5 / Group14 / Group15 / Group16 / Group17 / Group18.

Click **Enable** to enable this setting |
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings
Back	N/A	Click **Back** to return to the previous page.

Manual Key Management

When the Manually option is selected for Key Management as described in Authentication Configuration Window, a series of configuration windows for Manual IPSec Tunnel configuration will appear. The configuration windows are the Local & Remote Configuration, the Authentication, and the Manual Proposal.

Authentication Window		
Item	**Value setting**	**Description**
Key Management	A Must fill setting	Select Key Management from the dropdown box for this IPSec tunnel. In this section **Manually** is the option selected.
Local ID	An optional setting	Specify the **Local ID** for this IPSec tunnel to authenticate. Select the **Key ID** for Local ID and enter the Key ID (English alphabet or number).
Remote ID	An optional setting	Specify the **Remote ID** for this IPSec tunnel to authenticate. Select **Key ID** for Remote ID and enter the Key ID (English alphabet or number).

Modbus Cellular Gateway

Local & Remote Configuration

Item	Setting
▶ Local Subnet	
▶ Local Netmask	255.255.255.0
▶ Remote Subnet	
▶ Remote Netmask	
▶ Remote Gateway	(IP Address/FQDN)

Local & Remote Configuration Window

Item	Value setting	Description
Local Subnet	A Must fill setting	Specify the Local Subnet IP address and Subnet Mask.
Local Netmask	A Must fill setting	Specify the Local Subnet Mask.
Remote Subnet	A Must fill setting	Specify the Remote Subnet IP address
Remote Netmask	A Must fill setting	Specify the Remote Subnet Mask.
Remote Gateway	1. A Must fill setting 2. An IPv4 address or FQDN format	Specify the Remote Gateway. The Remote Gateway

Under the Manually Key Management authentication configuration, only one subnet is supported for both Local and Remote IPSec peer.

Manual Proposal

Item	Setting
▶ Outbound SPI	0x
▶ Inbound SPI	0x
▶ Encryption	DES ▼
▶ Authentication	None ▼

Manual Proposal Window

Item	Value setting	Description
Outbound SPI	Hexadecimal format	Specify the Outbound SPI for this IPSec tunnel. *Value Range*: 0 ~ FFFF.
Inbound SPI	Hexadecimal format	Specify the Inbound SPI for this IPSec tunnel. *Value Range*: 0 ~ FFFF.
Encryption	1. A Must fill setting 2. Hexadecimal format	Specify the Encryption Method and Encryption key Available encryption methods are DES/3DES/AES128/AES192/AES256 The key length for DES is 16, 3DES is 48, AES128 is 32, AES192 is 48, and AES256 is 64. Note: When AH option in Encapsulation is selected, encryption will not be

Modbus Cellular Gateway

		available.
Authentication	1. A Must fill setting 2. Hexadecimal format	Specify the Authentication Method and Authentication key Available encryptions are None/MD5/SHA1/SHA2-256 Enter the key string (String length by the method which choose) The key length for MD5 is 32, SHA1 is 40, and SHA2-256 is 64. Note: When AH option in Encapsulation Protocol is selected, None option in Authentication will not be available.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings
Back	N/A	Click **Back** to return to the previous page.

Create/Edit Dynamic VPN Server List

Similar to create an IPSec VPN Tunnel for site/host to site/host scenario, when **Edit** button is applied a series of configuration screen will appear. They are Tunnel Configuration, Local & Remote Configuration, Authentication, IKE Phase, IKE Proposal Definition, IPSec Phase, and IPSec Proposal Definition. You have to configure the tunnel details for the gateway as a Dynamic VPN server.

Note: For the purchased gateway, you can configure one Dynamic VPN server for each WAN interface.

Tunnel Configuration Window		
Item	**Value setting**	**Description**
Tunnel	Unchecked by default	Check the **Enable** box to activate the Dynamic IPSec VPN tunnel
Tunnel Name	1. A Must fill setting 2. String format can be any text	Enter a tunnel name. Enter a name that is easy for you to identify. ***Value Range***: 1 ~ 19 characters.
Interface	1. A Must fill setting	Select WAN interface on which IPSec tunnel is to be established.

	2. WAN 1 is selected by default	
Tunnel Scenario	1. A Must fill setting 2. Dynamic VPN is selected by default	The IPSec tunneling scenario is fixed to Dynamic VPN.
Operation Mode	1. A Must fill setting 2. Alway on is selected by default	The available operation mode is Always On. Failover and Load Balance options are not available for the Dynamic IPSec scenario.
Encapsulation Protocol	1. A Must fill setting 2. ESP is selected by default	Select the Encapsulation Protocol from the dropdown box for this IPSec tunnel. Available encapsulations are ESP and AH.

Local & Remote Configuration Window		
Item	Value setting	Description
Local Subnet	A Must fill setting	Specify the Local Subnet IP address.
Local Netmask	A Must fill setting	Specify the Local Subnet Mask.

Authentication Configuration Window		
Item	Value setting	Description
Key Management	1. A Must fill setting 2. Pre-shared Key 8 to 32 characters.	Select Key Management from the dropdown box for this IPSec tunnel. **IKE+Pre-shared Key**: user needs to set a key (8 ~ 32 characters).
Local ID	An optional setting	Specify the Local ID for this IPSec tunnel to authenticate. Select **User Name** for Local ID and enter the username. The username may include but can't be all numbers. Select **FQDN** for Local ID and enter the FQDN. Select **User@FQDN** for Local ID and enter the User@FQDN.

Modbus Cellular Gateway

		Select **Key ID** for Local ID and enter the Key ID (English alphabet or number).
Remote ID	An optional setting	Specify the Remote ID for this IPSec tunnel to authenticate. Select **User Name** for Remote ID and enter the username. The username may include but can't be all numbers. Select **FQDN** for Local ID and enter the FQDN. Select **User@FQDN** for Remote ID and enter the User@FQDN. Select **Key ID** for Remote ID and enter the Key ID (English alphabet or number). Note: Remote ID will be not available when Dynamic VPN option in Tunnel Scenario is selected.

For the rest IKE Phase, IKE Proposal Definition, IPSec Phase, and IPSec Proposal Definition settings, they are the same as that of creating an IPSec Tunnel described in previous section. Please refer to the related description.

Modbus Cellular Gateway

5.1.2 OpenVPN

OpenVPN is an application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls.

OpenVPN allows peers to authenticate each other using a Static Key (pre-shared key) or certificates. When used in a multi-client-server configuration, it allows the server to release an authentication certificate for every client, using signature and certificate authority. It uses the OpenSSL encryption library extensively, as well as the SSLv3/TLSv1 protocol, and contains many security and control features.

OpenVPN Tunneling is a Client and Server based tunneling technology. The OpenVPN Server must have a Static IP or a FQDN, and maintain a Client list. The OpenVPN Client may be a mobile user or mobile site with public IP or private IP, and requesting the OpenVPN tunnel connection. The product supports both OpenVPN Server and OpenVPN Client features to meet different application requirements.

There are two OpenVPN connection scenarios. They are the TAP and TUN scenarios. The product can create either a layer-3 based IP tunnel (TUN), or a layer-2 based Ethernet TAP that can carry any type of Ethernet traffic. In addition to configuring the device as a Server or Client, you have to specify which type of OpenVPN connection scenario is to be adopted.

OpenVPN TUN Scenario
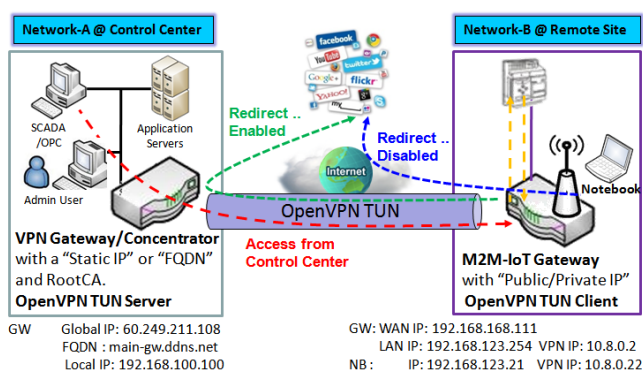
1. M2M-IoT Gateway (as OpenVPN TUN Client) connects to peer VPN Gateway/Concentrator (as OpenVPN TUN Server).
2. M2M-IoT Gateway will be assigned 10.8.0.2 IP Address after OpenVPN TUN Connection establbshed. (10.8.0.x is a virtual subnet)
3. Local networked device will get a virtual IP 10.8.0.x if its traffic goes through the OpenVPN TUN connection (when NAT disabled & Redirect Internet Traffic enabled).
4. SCADA Server in Control Center can access remote attached device(s) with the assigned IP Address 10.8.0.2.

The term "TUN" mode is referred to routing mode and operates with layer 3 packets. In routing mode, the VPN client is given an IP address on a different subnet than the local LAN under the OpenVPN server. This virtual subnet is created for connecting to any remote VPN computers. In routing mode, the OpenVPN server creates a "TUN" interface with its own IP address pool which is different to the local LAN. Remote hosts that dial-in will get an IP address inside the virtual network and will have access only to the server where OpenVPN resides.

If you want to offer remote access to a VPN server from client(s), and inhibit the access to remote LAN resources under VPN server, OpenVPN TUN mode is the simplest solution.

As shown in the diagram, the M2M-IoT Gateway is configured as an OpenVPN TUN Client, and connects to an

Modbus Cellular Gateway

OpenVPN UN Server. Once the OpenVPN TUN connection is established, the connected TUN client will be assigned a virtual IP (10.8.0.2) which is belong to a virtual subnet that is different to the local subnet in Control Center. With such connection, the local networked devices will get a virtual IP 10.8.0.x if its traffic goes through the OpenVPN TUN connection when Redirect Internet Traffic settings is enabled; Besides, the SCADA Server in Control Center can access remote attached serial device(s) with the virtual IP address (10.8.0.2).

OpenVPN TAP Scenario

Network-A @ Control Center

SCADA /OPC
Application Servers
Admin User

VPN Gateway/Concentrator
with a "Static IP" or "FQDN" and RootCA.
OpenVPN TAP Server

GW   Global IP: 60.249.211.108
      FQDN : main-gw.ddns.net
      Local IP: 192.168.100.100

Network-B @ Remote Site

Serial Cable

M2M-IoT Gateway
with a "Public or Private IP"
OpenVPN TAP Client

WAN IP: 192.168.168.111
Local IP: 192.168.123.254
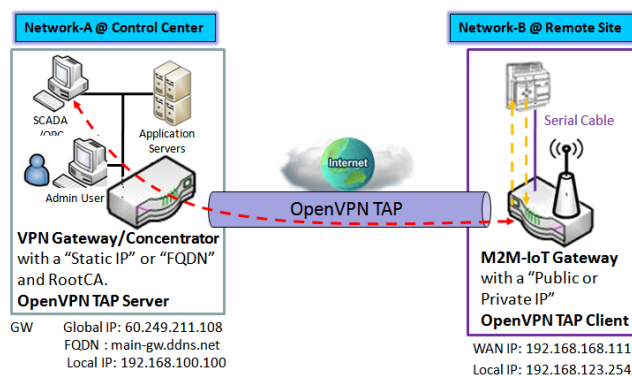
1. M2M-IoT Gateway (as OpenVPN TAP Client) connects to peer VPN Gateway/Concentrator (as OpenVPN TAP Server).
2. M2M-IoT Gateway will be assigned 192.168.100.210 IP Address after OpenVPN TAP Connection estabilshed. (same subnet as in Control Center)
3. SCADA Server in Control Center can access remote attached device(s) with the assigned IP Address 192.168.100.210.

The term "TAP" is referred to bridge mode and operates with layer 2 packets. In bridge mode, the VPN client is given an IP address on the same subnet as the LAN resided under the OpenVPN server. Under such configuration, the OpenVPN client can directly access to the resources in LAN. If you want to offer remote access to the entire remote LAN for VPN client(s), you have to setup OpenVPN in "TAP" bridge mode.

As shown in the diagram, the M2M-IoT Gateway is configured as an OpenVPN TAP Client, and connects to an OpenVPN TAP Server. Once the OpenVPN TAP connection is established, the connected TAP client will be assigned a virtual IP (192.168.100.210) which is the same subnet as that of local subnet in Control Center. With such connection, the SCADA Server in Control Center can access remote attached serial device(s) with the virtual IP address (192.168.100.210).

Modbus Cellular Gateway

Open VPN Setting

Go to **Security > VPN > OpenVPN** tab.

The OpenVPN setting allows user to create and configure OpenVPN tunnels.

Enable OpenVPN

Enable OpenVPN and select an expected configuration, either server or client, for the gateway to operate.

Configuration	
Item	Setting
▶ OpenVPN	☐ Enable
▶ Server / Client	Server ▼

Configuration Item	Value setting	Description
OpenVPN	The box is unchecked by default	Check the **Enable** box to activate the OpenVPN function.
Server/ Client	Server Configuration is selected by default.	When **Server** is selected, as the name indicated, server configuration will be displayed below for further setup. When **Client** is selected, you can specify the client settings in another client configuration window.

Modbus Cellular Gateway

As an OpenVPN Server

If **Server** is selected, an OpenVPN Server Configuration screen will appear. **OpenVPN Server Configuration** window can let you enable the OpenVPN server function, specify the virtual IP address of OpenVPN server, when remote OpenVPN clients dial in, and the authentication protocol.

OpenVPN Server Configuration	
Item	**Setting**
▸ OpenVPN Server	☑ Enable
▸ Protocol	TCP ▾
▸ Port	4430
▸ Tunnel Scenario	TUN ▾
▸ Authorization Mode	Static Key ▾
▸ Local Endpoint IP Address	
▸ Remote Endpoint IP Address	
▸ Static Key	
▸ Server Virtual IP	10.8.0.0
▸ DHCP-Proxy Mode	☑ Enable
▸ IP Pool	Starting Address: _____ ~ Ending Address: _____
▸ Gateway	
▸ Netmask	255.255.255.0(/24) ▾
▸ Redirect Default Gateway	☐ Enable
▸ Encryption Cipher	Blowfish ▾
▸ Hash Algorithm	SHA-1 ▾
▸ LZO Compression	Adaptive ▾
▸ Persist Key	☑ Enable
▸ Persist Tun	☑ Enable
▸ Advanced Configuration	Edit

OpenVPN Server Configuration		
Item	**Value setting**	**Description**
OpenVPN Server	The box is unchecked by	Click the **Enable** to activate OpenVPN Server functions.

Modbus Cellular Gateway

		default.
Protocol	1. A Must filled setting 2. By default **TCP** is selected.	Define the selected **Protocol** for connecting to the OpenVPN Server. • Select **TCP , or TCP /UDP** -> The TCP protocol will be used to access the OpenVPN Server, and **Port** will be set as 4430 automatically. • Select **UDP** -> The UDP protocol will be used to access the OpenVPN Server, and **Port** will be set as 1194 automatically.
Port	1. A Must filled setting 2. By default **4430** is set.	Specify the **Port** for connecting to the OpenVPN Server. ***Value Range***: 1 ~ 65535.
Tunnel Scenario	1. A Must filled setting 2. By default **TUN** is selected.	Specify the type of **Tunnel Scenario** for connecting to the OpenVPN Server. It can be **TUN** for TUN tunnel scenario, or **TAP** for TAP tunnel scenario.
Authorization Mode	1. A Must filled setting 2. By default **Static Key** is selected.	Specify the authorization mode for the OpenVPN Server. • **TLS** ->The OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Server Cert.** and **DH PEM** will be displayed. **CA Cert.** could be generated in Certificate. Refer to **Object Definition** > **Certificate** > **Trusted Certificate**. **Server Cert.** could be generated in Certificate. Refer to **Object Definition** > **Certificate** > **My Certificate**. • **Static Key** ->The OpenVPN will use static key (pre-shared) authorization mode, and the following items **Local Endpoint IP Address**, **Remote Endpoint IP Address** and **Static Key** will be displayed. Note: Static Key will be available only when TUN is chosen in Tunnel Scenario.
Local Endpoint IP Address	A Must filled setting	Specify the virtual **Local Endpoint IP Address** of this OpenVPN gateway. ***Value Range***: The IP format is 10.8.0.x, the range of x is 1~254. Note: Local Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Remote Endpoint IP Address	A Must filled setting	Specify the virtual **Remote Endpoint IP Address** of the peer OpenVPN gateway. ***Value Range***: The IP format is 10.8.0.x, the range of x is 1~254. Note: Remote Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Static Key	A Must filled setting	Specify the **Static Key**. Note: Static Key will be available only when Static Key is chosen in Authorization Mode.
Server Virtual IP	A Must filled setting	Specify the **Server Virtual IP**. ***Value Range***: The IP format is 10.y.0.0, the range of y is 1~254. Note: Server Virtual IP will be available only when TLS is chosen in Authorization Mode.
DHCP-Proxy Mode	1. A Must filled setting 2. The box is checked by default.	Check the **Enable** box to activate the **DHCP-Proxy Mode**. Note: DHCP-Proxy Mode will be available only when TAP is chosen in Tunnel Device.
IP Pool	A Must filled setting	Specify the virtual **IP pool** setting for the OpenVPN server. You have to specify the **Starting Address** and **Ending Address** as the IP address pool for the OpenVPN clients. Note: IP Pool will be available only when TAP is chosen in Tunnel Device, and DHCP-Proxy Mode is unchecked (disabled).
Gateway	A Must filled setting	Specify the **Gateway** setting for the OpenVPN server. It will be assigned to the connected OpenVPN clients.

Modbus Cellular Gateway

		Note: Gateway will be available only when TAP is chosen in Tunnel Device, and DHCP-Proxy Mode is unchecked (disabled).
Netmask	By default **- select one -** is selected.	Specify the **Netmask** setting for the OpenVPN server. It will be assigned to the connected OpenVPN clients. ***Value Range***: 255.255.255.0/24 (only support class C) Note_1: Netmask will be available when TAP is chosen in Tunnel Device, and DHCP-Proxy Mode is unchecked (disabled). Note_2: Netmask will also be available when TUN is chosen in Tunnel Device.
Redirect Default Gateway	1. An Optional setting. 2. The box is unchecked by default.	Check the **Enable** box to activate the **Redirect Default Gateway** function.
Encryption Cipher	1. A Must filled setting. 2. By default **Blowfish** is selected.	Specify the **Encryption Cipher** from the dropdown list. It can be **Blowfish/AES-256/AES-192/AES-128/None.**
Hash Algorithm	By default **SHA-1** is selected.	Specify the **Hash Algorithm** from the dropdown list. It can be **SHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable.**
LZO Compression	By default **Adaptive** is selected.	Specify the **LZO Compression** scheme. It can be **Adaptive/YES/NO/Default.**
Persis Key	1. An Optional setting. 2. The box is checked by default.	Check the **Enable** box to activate the **Persis Key** function.
Persis Tun	1. An Optional setting. 2. The box is checked by default.	Check the **Enable** box to activate the **Persis Tun** function.
Advanced Configuration	N/A	Click the **Edit** button to specify the **Advanced Configuration** setting for the OpenVPN server. If the button is clicked, **Advanced Configuration** will be displayed below.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **Undo** to cancel the changes.

Modbus Cellular Gateway

When **Advanced Configuration** is selected, an OpenVPN Server Advanced Configuration screen will appear.

Item	Setting
▶ TLS Cipher	TLS-RSA-WITH-AES128-SHA ▼
▶ TLS Auth. Key	(Optional)
▶ Client to Client	☑ Enable
▶ Duplicate CN	☑ Enable
▶ Tunnel MTU	1500
▶ Tunnel UDP Fragment	1500
▶ Tunnel UDP MSS-Fix	☐ Enable
▶ CCD-Dir Default File	
▶ Client Connection Script	
▶ Additional Configuration	

OpenVPN Server Advanced Configuration

Item	Value setting	Description
TLS Cipher	1. A Must filled setting. 2. **TLS-RSA-WITH-AES128-SHA** is selected by default	Specify the **TLS Cipher** from the dropdown list. It can be **TLS-RSA-WITH-AES128-SHA / TLS-DHE-DSS-AES256-SHA / TLS-DHE-DSS-AES128-SHA / TLS-RSA-WITH-AES256-SHA / TLS-RSA-WITH-RC4-MD5 / None.** Note: TLS Cipher will be available only when TLS is chosen in Authorization Mode.
TLS Auth. Key	1. An Optional setting. 2. String format: any text	Specify the **TLS Auth. Key.** Note: TLS Auth. Key will be available only when TLS is chosen in Authorization Mode.
Client to Client	The box is checked by default	Check the **Enable** box to enable the traffics among different OpenVPN Clients. Note: Client to Client will be available only when TLS is chosen in Authorization Mode
Duplicate CN	The box is checked by default	Check the **Enable** box to activate the **Duplicate CN** function. Note: Duplicate CN will be available only when TLS is chosen in Authorization Mode
Tunnel MTU	1. A Must filled setting 2. The value is **1500** by default	Specify the **Tunnel MTU.** ***Value Range***: 0 ~ 1500.
Tunnel UDP Fragment	1. A Must filled setting 2. The value is **1500** by	Specify the **Tunnel UDP Fragment.** By default, it is equal to **Tunnel MTU**. ***Value Range***: 0 ~ 1500.

	default	Note: Tunnel UDP Fragment will be available only when UDP is chosen in Protocol.
Tunnel UDP MSS-Fix	1. An Optional setting. 2. The box is unchecked by default.	Check the **Enable** box to activate the **Tunnel UDP MSS-Fix** Function. Note: Tunnel UDP MSS-Fix will be available only when UDP is chosen in Protocol.
CCD-Dir Default File	1. An Optional setting. 2. String format: any text	Specify the **CCD-Dir Default File.** ***Value Range***: 0 ~ 256 characters.
Client Connection Script	1. An Optional setting. 2. String format: any text	Specify the **Client Connection Script.** ***Value Range***: 0 ~ 256 characters.
Additional Configuration	1. An Optional setting. 2. String format: any text	Specify the **Additional Configuration.** ***Value Range***: 0 ~ 256 characters.

Modbus Cellular Gateway

As an OpenVPN Client

If **Client** is selected, an OpenVPN Client List screen will appear.

ID	Client Name	Interface	Protocol	Port	Tunnel Scenario	Remote IP/FQDN	Remote Subnet	Redirect Internet Traffic	NAT	Authorization Mode	Encryption Cipher	Hash Algorithm	Enable	Actions

OpenVPN Client List [Add] [Delete]

When **Add** button is applied, OpenVPN Client Configuration screen will appear. **OpenVPN Client Configuration** window let you specify the required parameters for an OpenVPN VPN client, such as "OpenVPN Client Name", "Interface", "Protocol", "Tunnel Scenario", "Remote IP/FQDN", "Remote Subnet", "Authorization Mode", "Encryption Cipher", "Hash Algorithm" and tunnel activation.

OpenVPN Client Configuration

Item	Setting
▶ OpenVPN Client Name	OpenVPN Client #1
▶ Interface	WAN 1 ▾
▶ Protocol	TCP ▾ Port: 443
▶ Tunnel Scenario	TUN ▾
▶ Remote IP/FQDN	
▶ Remote Subnet	255.255.255.0(/24) ▾
▶ Redirect Internet Traffic	☐ Enable
▶ NAT	☐ Enable
▶ Authorization Mode	TLS ▾ CA Cert.: ▾ Client Cert.: ▾ Client Key.: ▾ Please set the Certificate.
▶ Encryption Cipher	Blowfish ▾
▶ Hash Algorithm	SHA-1 ▾
▶ LZO Compression	Adaptive ▾
▶ Persist Key	☑ Enable
▶ Persist Tun	☑ Enable
▶ Advanced Configuration	[Edit]
▶ Tunnel	☐ Enable

Modbus Cellular Gateway

OpenVPN Client Configuration		
Item	**Value setting**	**Description**
OpenVPN Client Name	A Must filled setting	The **OpenVPN Client Name** will be used to identify the client in the tunnel list. *Value Range*: 1 ~ 32 characters.
Interface	1. A Must filled setting 2. By default **WAN-1** is selected.	Define the physical interface to be used for this OpenVPN Client tunnel.
Protocol	1. A Must filled setting 2. By default **TCP** is selected.	Define the **Protocol** for the OpenVPN Client. • Select **TCP** ->The OpenVPN will use TCP protocol, and **Port** will be set as 443 automatically. • Select **UDP** -> The OpenVPN will use UDP protocol, and **Port** will be set as 1194 automatically.
Port	1. A Must filled setting 2. By default **443** is set.	Specify the **Port** for the OpenVPN Client to use. *Value Range*: 1 ~ 65535.
Tunnel Scenario	1. A Must filled setting 2. By default **TUN** is selected.	Specify the type of **Tunnel Scenario** for the OpenVPN Client to use. It can be **TUN** for TUN tunnel scenario, or **TAP** for TAP tunnel scenario.
Remote IP/FQDN	A Must filled setting	Specify the **Remote IP/FQDN** of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the IP address or FQDN.
Remote Subnet	A Must filled setting	Specify **Remote Subnet** of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the remote subnet address and remote subnet mask.
Redirect Internet Traffic	1. An Optional setting. 2. The box is unchecked by default.	Check the **Enable** box to activate the **Redirect Internet Traffic** function.
NAT	1. An Optional setting. 2. The box is unchecked by default.	Check the **Enable** box to activate the **NAT** function.
Authorization Mode	1. A Must filled setting 2. By default **TLS** is selected.	Specify the authorization mode for the OpenVPN Server. • **TLS** ->The OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Client Cert.** and **Client Key** will be displayed. **CA Cert.** could be selected in Trusted CA Certificate List. Refer to **Object Definition** > **Certificate** > **Trusted Certificate**. **Client Cert.** could be selected in Local Certificate List. Refer to **Object Definition** > **Certificate** > **My Certificate**. **Client Key** could be selected in Trusted Client key List. Refer to **Object Definition** > **Certificate** > **Trusted Certificate**. • **Static Key** ->The OpenVPN will use static key authorization mode, and the following items **Local Endpoint IP Address**, **Remote Endpoint IP Address** and **Static Key** will be displayed.
Local Endpoint IP Address	A Must filled setting	Specify the virtual **Local Endpoint IP Address** of this OpenVPN gateway. *Value Range*: The IP format is 10.8.0.x, the range of x is 1~254. Note: Local Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.

Modbus Cellular Gateway

Remote Endpoint IP Address	A Must filled setting	Specify the virtual **Remote Endpoint IP Address** of the peer OpenVPN gateway. ***Value Range***: The IP format is 10.8.0.x, the range of x is 1~254. Note: Remote Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Static Key	A Must filled setting	Specify the **Static Key**. Note: Static Key will be available only when Static Key is chosen in Authorization Mode.
Encryption Cipher	By default **Blowfish** is selected.	Specify the **Encryption Cipher.** It can be **Blowfish/AES-256/AES-192/AES-128/None.**
Hash Algorithm	By default **SHA-1** is selected.	Specify the **Hash Algorithm.** It can be **SHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable.**
LZO Compression	By default **Adaptive** is selected.	Specify the **LZO Compression** scheme. It can be **Adaptive/YES/NO/Default.**
Persis Key	1. An Optional setting. 2. The box is checked by default.	Check the **Enable** box to activate the **Persis Key** function.
Persis Tun	1. An Optional setting. 2. The box is checked by default.	Check the **Enable** box to activate the **Persis Tun** function.
Advanced Configuration	N/A	Click the **Edit** button to specify the **Advanced Configuration** setting for the OpenVPN server. If the button is clicked, **Advanced Configuration** will be displayed below.
Tunnel	The box is unchecked by default	Check the **Enable** box to activate this OpenVPN tunnel.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **Undo** to cancel the changes.
Back	N/A	Click **Back** to return to last page.

Modbus Cellular Gateway

When **Advanced Configuration** is selected, an OpenVPN Client Advanced Configuration screen will appear.

OpenVPN Advanced Client Configuration		
Item	**Value setting**	**Description**
TLS Cipher	1. A Must filled setting. 2. **TLS-RSA-WITH-AES128-SHA** is selected by default	Specify the **TLS Cipher** from the dropdown list. It can be **TLS-RSA-WITH-AES128-SHA / TLS-DHE-DSS-AES256-SHA / TLS-DHE-DSS-AES128-SHA / TLS-RSA-WITH-AES256-SHA / TLS-RSA-WITH-RC4-MD5 / None.** Note: TLS Cipher will be available only when TLS is chosen in Authorization Mode.
TLS Auth. Key	1. An Optional setting. 2. String format: any text	Specify the **TLS Auth. Key** for connecting to an OpenVPN server, if the server required it. Note: TLS Auth. Key will be available only when TLS is chosen in Authorization Mode.
User Name	An Optional setting.	Enter the **User account** for connecting to an OpenVPN server, if the server required it. Note: User Name will be available only when TLS is chosen in Authorization Mode.
Password	An Optional setting.	Enter the **Password** for connecting to an OpenVPN server, if the server required it.

		Note: User Name will be available only when TLS is chosen in Authorization Mode.
Bridge TAP to	By default **VLAN 1** is selected	Specify the setting of "**Bridge TAP to**" to bridge the TAP interface to a certain local network interface or VLAN. Note: Bridge TAP to will be available only when TAP is chosen in Tunnel Scenario and NAT is unchecked.
Firewall Protection	The box is unchecked by default.	Check the box to activate the **Firewall Protection** function. Note: Firewall Protection will be available only when NAT is enabled.
Client IP Address	By default **Dynamic IP** is selected	Specify the virtual IP Address for the OpenVPN Client. It can be **Dynamic IP/Static IP.**
Tunnel MTU	1. A Must filled setting 2. The value is 1500 by default	Specify the value of **Tunnel MTU.** ***Value Range*: 0 ~ 1500.**
Tunnel UDP Fragment	The value is 1500 by default	Specify the value of **Tunnel UDP Fragment.** ***Value Range*: 0 ~ 1500.** Note: Tunnel UDP Fragment will be available only when UDP is chosen in Protocol.
Tunnel UDP MSS-Fix	The box is unchecked by default.	Check the **Enable** box to activate the **Tunnel UDP MSS-Fix** function. Note: Tunnel UDP MSS-Fix will be available only when UDP is chosen in Protocol.
nsCerType Verification	The box is unchecked by default.	Check the **Enable** box to activate the **nsCerType Verification** function. Note: nsCerType Verification will be available only when TLS is chosen in Authorization Mode.
TLS Renegotiation Time (seconds)	The value is 3600 by default	Specify the time interval of **TLS Renegotiation Time.** ***Value Range*: -1 ~ 86400.**
Connection Retry(seconds)	The value is -1 by default	Specify the time interval of **Connection Retry.** The default -1 means that it is no need to execute connection retry. ***Value Range*: -1 ~ 86400, and -1 means no retry is required.**
DNS	By default **Automatically** is selected	Specify the setting of **DNS.** It can be **Automatically/Manually.**

Modbus Cellular Gateway

5.1.3 L2TP

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy. This Gateway can behave as a L2TP server and a L2TP client both at the same time.

L2TP Server: It must have a static IP or a FQDN for clients to create L2TP tunnels. It also maintains "User Account list" (user name/ password) for client login authentication; There is a virtual IP pool to assign virtual IP to each connected L2TP client.

L2TP Client: It can be mobile users or gateways in remote offices with dynamic IP. To setup tunnel, it should

get "user name", "password" and server's global IP. In addition, it is required to identify the operation mode for each tunnel as main connection, failover for another tunnel, or load balance tunnel to increase overall bandwidth. It needs to decide "Default Gateway" or "Remote Subnet" for packet flow. Moreover, you can also define what kind of traffics will pass through the L2TP tunnel in the "Default Gateway / Remote Subnet" parameter.
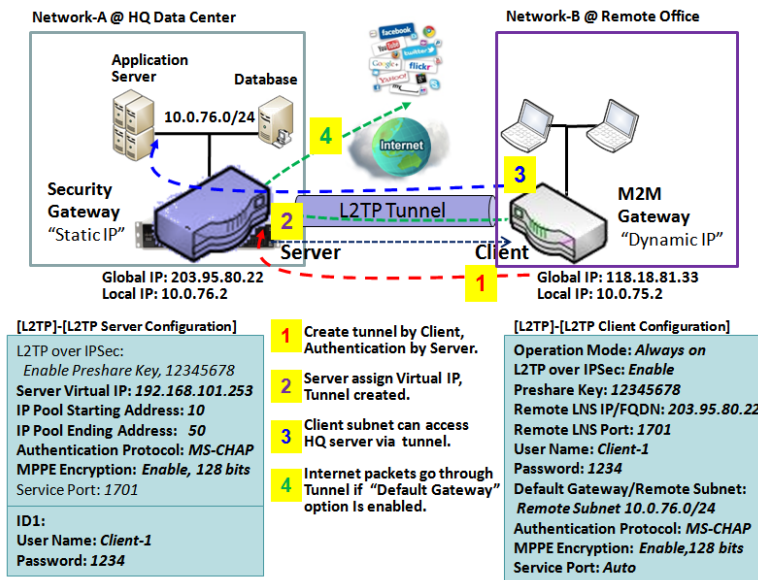
There are two options, "Default Gateway" and "Remote Subnet" for the "Default Gateway / Remote Subnet" configuration item. When you choose "Remote Subnet", you need to specify one more setting: the remote subnet. It is for the Intranet of L2TP VPN server. So, at L2TP client peer, the packets whose destination is in the dedicated subnet will be transferred via the L2TP VPN tunnel. Others will be transferred based on current routing policy of the security gateway at L2TP client peer. But, if you choose "Default Gateway" option for the L2TP client peer, all packets, including the Internet accessing of L2TP Client peer, will go through the established L2TP VPN tunnel. That means the remote L2TP VPN server controls the flowing of any packets from the L2TP client peer. Certainly, those packets come through the L2TP VPN tunnel.

Modbus Cellular Gateway

L2TP Setting

Go to **Security > VPN > L2TP** tab.

The L2TP setting allows user to create and configure L2TP tunnels.

Enable L2TP

Item	Setting
▶ L2TP	☐ Enable
▶ Client/Server	Server ▼

Configuration [Help]

Enable L2TP Window		
Item	**Value setting**	**Description**
L2TP	Unchecked by default	Click the **Enable** box to activate L2TP function.
Client/Server	A Must fill setting	Specify the role of L2TP. Select **Server** or **Client** role your gateway will take. Below are the configuration windows for L2TP Server and for Client.
Save	N/A	Click **Save** button to save the settings

As a L2TP Server

When select **Server** in Client/Server, the L2TP server Configuration will appear.

L2TP Server Configuration

Item	Setting
▶ L2TP Server	☐ Enable
▶ L2TP over IPsec	☐ Enable Preshared Key [_____] (Min. 8 characters)
▶ Server Virtual IP	192.168.10.1
▶ IP Pool Starting Address	10
▶ IP Pool Ending Address	100
▶ Authentication Protocol	☐ PAP ☐ CHAP ☐ MS-CHAP ☐ MS-CHAP v2
▶ MPPE Encryption	☐ Enable 40 bits ▼
▶ Service Port	1701

Modbus Cellular Gateway

L2TP Server Configuration		
Item	**Value setting**	**Description**
L2TP Server	The box is unchecked by default	When click the **Enable** box It will active L2TP server
L2TP over IPSec	The box is unchecked by default	When click the **Enable** box. It will enable L2TP over IPSec and need to fill in the Pre-shared Key (8~32 characters).
Server Virtual IP	A Must filled setting	Specify the L2TP server Virtual IP It will set as this L2TP server local virtual IP
IP Pool Starting Address	A Must filled setting	Specify the L2TP server starting IP of virtual IP pool It will set as the starting IP which assign to L2TP client ***Value Range***: 1 ~ 255.
IP Pool Ending Address	A Must filled setting	Specify the L2TP server ending IP of virtual IP pool It will set as the ending IP which assign to L2TP client ***Value Range***: 1 ~ 255.
Authentication Protocol	A Must filled setting	Select single or multiple Authentication Protocols for the L2TP server with which to authenticate L2TP clients. Available authentication protocols are **PAP / CHAP / MS-CHAP / MS-CHAP v2**.
MPPE Encryption	A Must filled setting	Specify whether to support MPPE Protocol. Click the **Enable** box to enable MPPE and from dropdown box to select **40 bits / 56 bits / 128 bits**. Note: when MPPE Encryption is enabled, the Authentication Protocol **PAP / CHAP** options will not be available.
Service Port	A Must filled setting	Specify the **Service Port** which L2TP server use. ***Value Range***: 1 ~ 65535.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to recovery the configuration.

L2TP Server Status		
Item	**Value setting**	**Description**
L2TP Server Status	N/A	It displays the User Name, Remote IP, Remote Virtual IP, and Remote Call ID of the connected L2TP clients. Click the **Refresh** button to renew the L2TP client information.

Modbus Cellular Gateway

User Account List Window		
Item	**Value setting**	**Description**
User Account List	Max.of 10 user accounts	This is the L2TP authentication user account entry. You can create and add accounts for remote clients to establish L2TP VPN connection to the gateway device. Click **Add** button to add user account. Enter User name and password. Then check the **enable** box to enable the user. Click **Save** button to save new user account. The selected user account can permanently be deleted by clicking the **Delete** button. **_Value Range_**: 1 ~ 32 characters.

As a L2TP Client

When select Client in Client/Server, a series L2TP Client Configuration will appear.

L2TP Client Configuration		
Item Setting	**Value setting**	**Description**
L2TP Client	The box is unchecked by default	Check the **Enable** box to enable PPTP client role of the gateway.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.

Modbus Cellular Gateway

Create/Edit L2TP Client

ID	Tunnel Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/ Remote Subnet	Status	Enable	Actions

(L2TP Client List & Status — Add | Delete | Refresh)

When **Add/Edit** button is applied, a series of configuration screen will appear.

L2TP Client Configuration

Item	Setting
▶ Tunnel Name	L2TP #1
▶ Interface	WAN1 ▾
▶ Operation Mode	Always on ▾
▶ L2TP over IPsec	☐ Enable Preshared Key [ ] (Min. 8 characters)
▶ Remote LNS IP/FQDN	[ ]
▶ Remote LNS Port	1701
▶ User Name	[ ]
▶ Password	[ ]
▶ Tunneling Password (Optional)	[ ]
▶ Default Gateway/Remote Subnet	Remote Subnet ▾ [ ]
▶ Authentication Protocol	☐ PAP ☐ CHAP ☐ MS-CHAP ☐ MS-CHAP v2
▶ MPPE Encryption	☐ Enable
▶ NAT before Tunneling	☐ Enable
▶ LCP Echo Type	Auto ▾ Interval 30 seconds Max. Failure Time 6 times
▶ Service Port	Auto ▾ 0
▶ Tunnel	☐ Enable

L2TP Client Configuration

Item Setting	Value setting	Description
Tunnel Name	A Must filled setting	Enter a tunnel name. Enter a name that is easy for you to identify. **Value Range**: 1 ~ 32 characters.
Interface	A Must filled setting	Define the selected interface to be the used for this L2TP tunnel Select **WAN-1** for this tunnel using. (WAN-1 is available only when WAN-1 interface is enabled) The same applies to other WAN interfaces (i.e. **WAN-2).**
Operation Mode	1. A Must fill setting	There are three available operation modes. **Always on**, **Failover**, **Load Balance**.

Modbus Cellular Gateway

	2. Alwasy on is selected by default	**Failover/ Always on**: Define whether the PPTP client is a failover tunnel function or an always on tunnel. Note: If this PPTP is a failover tunneling, you will need to select a primary IPSec tunnel from which to failover to. **Load Balance**: Define whether the PPTP tunnel connection will take part in load balance function of the gateway. You will not need to select which WAN interface as the system will automatically utilize the available WAN interfaces to balance traffic loads. For more details on WAN Load Balance, refer to **Basic Network > WAN & Uplink > Load Balance** tab. Note: Load Balance function is not available for the gateway with single WAN.
L2TP over IPSec	The box is unchecked by default	Check the **Enable** box to activate L2TP over IPSec, and further specify a Pre-shared Key (8~32 characters).
Remote LNS IP/FQDN	A Must filled setting	Enter the public IP address or the FQDN of the L2TP server.
Remote LNS Port	A Must filled setting	Enter the Remote LNS Port for this L2TP tunnel. ***Value Range***: 1 ~ 65535.
Use Nname	A Must filled setting	Enter the **User Name** for this L2TP tunnel to be authenticated when connect to L2TP server. ***Value Range***: 1 ~ 32 characters.
Password	A Must filled setting	Enter the **Password** for this L2TP tunnel to be authenticated when connect to L2TP server.
Tunneling Password(Optional)	The box is unchecked by default	Enter the **Tunneling Password** for this L2TP tunnel to authenticate.
Default Gateway / Remote Subnet	A Must filled setting	Specify a gateway for this PPTP tunnel to reach PPTP server. When you choose **Remote Subnet**, you need to specify one more setting: the remote subnet. It is for the Intranet of PPTP VPN server. So, at PPTP client peer, the packets whose destination is in the dedicated subnet will be transferred via the PPTP VPN tunnel. Others will be transferred based on current routing policy of the security gateway at PPTP client peer. But, if you choose **Default Gateway** option for the PPTP client peer, all packets, including the Internet accessing of PPTP Client peer, will go through the established PPTP VPN tunnel. That means the remote PPTP VPN server controls the flowing of any packets from the PPTP client peer. Certainly, those packets come through the PPTP VPN tunnel. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24).
Authentication Protocol	A Must filled setting	Specify **Authentication Protocol** for this L2TP tunnel will can be used. Click the PAP/CHAP/MS-CHAP/MS-CHAP v2 ->The protocol will be enable which box is click.
Authentication Protocol	1. A Must fill setting 2. Unchecked by default	Specify one ore multiple **Authentication Protocol** for this PPTP tunnel. Available authentication methods are **PAP / CHAP / MS-CHAP / MS-CHAP v2**.
MPPE Encryption	1. Unchecked by default 2. an optional setting	Specify whether PPTP server supports **MPPE Protocol**. Click the **Enable** box to enable MPPE. Note: when MPPE Encryption is enabled, the Authentication Protocol **PAP / CHAP** options will not be available.
NAT before	1. Unchecked by	Check the **Enable** box to enable NAT function for this PPTP tunnel.

Modbus Cellular Gateway

Tunneling	default	
	2. an optional setting	
LCP Echo Type	Auto is set by default	Specify the LCP Echo Type for this L2TP tunnel. It can be **Auto**, **User-defined**, or **Disable**. **Auto**: the system sets the Interval and Max. Failure Time. **User-defined:** enter the Interval and Max. Failure Time. **Disable**: disable the LCP Echo. ***Value Range*:** 1 ~ 99999 for Interval Time, 1~999 for Failure Time.
Service Port	A Must filled setting	Specify the **Service Port** for this L2TP tunnel to use. ***Value Range*:** 1 ~ 65535.
Tunnel	Unchecked by default	Check the **Enable** box to enable this PPTP tunnel.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.
Back	N/A	Click **Back** button to return to the previous page.

Modbus Cellular Gateway

5.1.4 PPTP

Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. It is a client-server based technology. There are various levels of authentication and encryption for PPTP tunneling, usually natively as standard features of the Windows PPTP stack. The security gateway can play either "PPTP Server" role or "PPTP Client" role for a PPTP VPN tunnel, or both at the same time for different tunnels. PPTP tunnel process is nearly the same as L2TP.

PPTP Server: It must have a static IP or a FQDN for clients to create PPTP tunnels. It also maintains "User Account list" (user name / password) for client login authentication; There is a virtual IP pool to assign virtual IP to each connected PPTP client.

Modbus Cellular Gateway

PPTP Client: It can be mobile users or gateways in remote offices with dynamic IP. To setup tunnel, it should get "user name", "password" and server's global IP. In addition, it is required to identify the operation mode for each tunnel as main connection, failover for another tunnel, or load balance tunnel to increase overall bandwidth. It needs to decide "Default Gateway" or "Remote Subnet" for packet flow. Moreover, you can also define what kind of traffics will pass through the PPTP tunnel in the "Default Gateway / Remote Subnet" parameter.

Network-A @ HQ Data Center

Application Server
Database

10.0.76.0/24

Security Gateway
"Static IP"

Global IP: 203.95.80.22
Local IP: 10.0.76.2

PPTP Tunnel

Server

Network-B @ Remote Office

M2M Gateway
"Dynamic IP"

Client

Global IP: 118.18.81.33
Local IP: 10.0.75.2

[PPTP]-[PPTP Server Configuration]

Server Virtual IP: *192.168.101.253*
IP Pool Starting Address: *10*
IP Pool Ending Address: *50*
Authentication Protocol: *MS-CHAP*
MPPE Encryption: *Enable, 128 bits*

ID1:
User Name: *Client-1*
Password: *1234*

1 Create tunnel by Client, Authentication by Server.

2 Server assign Virtual IP, Tunnel created.

3 Client subnet can access HQ server via tunnel.

4 Internet packets go through Tunnel if "Default Gateway" option is enabled.

[PPTP]-[PPTP Client Configuration]

Operation Mode: *Always on*
Remote IP/FQDN: *203.95.80.22*
User Name: *Client-1*
Password: *1234*
Default Gateway/Remote Subnet:
  Remote Subnet, 10.0.76.0/24
Authentication: *MS-CHAP*
MPPE Encryption: *Enable, 128 bits*

There are two options, "Default Gateway" and "Remote Subnet" for the "Default Gateway / Remote Subnet" configuration item. When you choose "Remote Subnet", you need to specify one more setting: the remote subnet. It is for the Intranet of PPTP VPN server. So, at PPTP client peer, the packets whose destination is in the dedicated subnet will be transferred via the PPTP VPN tunnel. Others will be transferred based on current routing policy of the security gateway at PPTP client peer. But, if you choose "Default Gateway" option for the PPTP client peer, all packets, including the Internet accessing of PPTP Client peer, will go through the established PPTP VPN tunnel. That means the remote PPTP VPN server controls the flowing of any packets from the PPTP client peer. Certainly, those packets come through the PPTP VPN tunnel.

Modbus Cellular Gateway

PPTP Setting

Go to **Security > VPN > PPTP** tab.

The PPTP setting allows user to create and configure PPTP tunnels.

Enable PPTP

Enable PPTP Window		
Item	**Value setting**	**Description**
PPTP	Unchecked by default	Click the **Enable** box to activate PPTP function.
Client/Server	A Must fill setting	Specify the role of PPTP. Select **Server** or **Client** role your gateway will take. Below are the configuration windows for PPTP Server and for Client.
Save	N/A	Click **Save** button to save the settings.

As a PPTP Server

The gateway supports up to a maximum of 10 PPTP user accounts.
When **Server** in the Client/Server field is selected, the PPTP server configuration window will appear.

Modbus Cellular Gateway

PPTP Server Configuration Window		
Item	**Value setting**	**Description**
PPTP Server	Unchecked by default	Check the **Enable** box to enable PPTP server role of the gateway.
Server Virtual IP	1. A Must fill setting 2. Default is 192.168.0.1	Specify the PPTP server Virtual IP address. The virtual IP address will serve as the virtual DHCP server for the PPTP clients. Clients will be assigned a virtual IP address from it after the PPTP tunnel has been established.
IP Pool Starting Address	1. A Must fill setting 2. Default is 10	This is the PPTP server's Virtual IP DHCP server. User can specify the first IP address for the subnet from which the PPTP client's IP address will be assigned. *Value Range*: 1 ~ 255.
IP Pool Ending Address	1. A Must fill setting 2. Default is 100	This is the PPTP server's Virtual IP DHCP server. User can specify the last IP address for the subnet from which the PPTP client's IP address will be assigned. *Value Range*: 1 ~ 255.
Authentication Protocol	1. A Must fill setting 2. Unchecked by default	Select single or multiple Authentication Protocols for the PPTP server with which to authenticate PPTP clients. Available authentication protocols are **PAP / CHAP / MS-CHAP / MS-CHAP v2**.
MPPE Encryption	1. A Must fill setting 2. Unchecked by default	Specify whether to support MPPE Protocol. Click the **Enable** box to enable MPPE and from dropdown box to select **40 bits / 56 bits / 128 bits**. Note: when MPPE Encryption is enabled, the Authentication Protocol **PAP / CHAP** options will not be available.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.

PPTP Server Status Refresh				
User Name	**Remote IP**	**Remote Virtual IP**	**Remote Call ID**	**Actions**
No connection from remote				

PPTP Server Status Window		
Item	**Value setting**	**Description**
PPTP Server Status	N/A	It displays the User Name, Remote IP, Remote Virtual IP, and Remote Call ID of the connected PPTP clients. Click the **Refresh** button to renew the PPTP client information.

User Account List Add Delete				
ID	**User Name**	**Password**	**Enable**	**Actions**

User Account Configuration		
User Name	**Password**	**Account**
		☐ Enable
Save		

Modbus Cellular Gateway

User Account List Window		
Item	**Value setting**	**Description**
User Account List	Max.of 10 user accounts	This is the PPTP authentication user account entry. You can create and add accounts for remote clients to establish PPTP VPN connection to the gateway device. Click **Add** button to add user account. Enter User name and password. Then check the **enable** box to enable the user. Click **Save** button to save new user account. The selected user account can permanently be deleted by clicking the **Delete** button. ***Value Range*: 1 ~ 32 characters.**

As a PPTP Client

When select Client in Client/Server, a series PPTP Client Configuration will appear.

PPTP Client Configuration	
Item	**Setting**
▶ PPTP Client	☐ Enable

PPTP Client Configuration		
Item	**Value setting**	**Description**
PPTP Client	Unchecked by default	Check the **Enable** box to enable PPTP client role of the gateway.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.

Create/Edit PPTP Client

PPTP Client List & Status [Add] [Delete] [Refresh]							
ID	Tunnel Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/ Remote Subnet	Status	Enable	Actions

The gateway supports up to a maximum of 32 simultaneous PPTP tunnels.
When **Add/Edit** button is applied, a series PPTP Client Configuration will appear.

Modbus Cellular Gateway

PPTP Client Configuration	
Item	Setting
▶ Tunnel Name	PPTP #1
▶ Interface	WAN1 ▾
▶ Operation Mode	Always on ▾
▶ Remote IP/FQDN	
▶ User Name	
▶ Password	
▶ Default Gateway/Remote Subnet	Remote Subnet ▾
▶ Authentication Protocol	☐ PAP ☐ CHAP ☐ MS-CHAP ☐ MS-CHAP v2
▶ MPPE Encryption	☐ Enable
▶ NAT before Tunneling	☐ Enable
▶ LCP Echo Type	Auto ▾ Interval 30 seconds Max. Failure Time 6 times
▶ Tunnel	☐ Enable

PPTP Client Configuration Window		
Item	**Value setting**	**Description**
Tunnel Name	A Must fill setting	Enter a tunnel name. Enter a name that is easy for you to identify. *Value Range*: 1 ~ 32 characters.
Interface	1. A Must fill setting 2. WAN1 is selected by default	Define the selected interface to be the used for this PPTP tunnel Select **WAN-1** for this tunnel using. (WAN-1 is available only when WAN-1 interface is enabled) The same applies to other WAN interfaces (i.e. **WAN-2).**
Operation Mode	1. A Must fill setting 2. **Alwasy on** is selected by default	There are three available operation modes. **Always on**, **Failover**, **Load Balance**. **Failover/ Always on**: Define whether the PPTP client is a failover tunnel function or an always on tunnel. Note: If this PPTP is a failover tunneling, you will need to select a primary IPSec tunnel from which to failover to. **Load Balance**: Define whether the PPTP tunnel connection will take part in load balance function of the gateway. You will not need to select which WAN interface as the system will automatically utilize the available WAN interfaces to balance traffic loads. For more details on WAN Load Balance, refer to **Basic Network > WAN & Uplink > Load Balance** tab. Note: Load Balance function is not available for the gateway with single WAN.
Remote IP/FQDN	1. A Must fill setting. 2. Format can be a ipv4 address or FQDN	Enter the public IP address or the FQDN of the PPTP server.

Modbus Cellular Gateway

User Name	A Must fill setting	Enter the **User Name** for this PPTP tunnel to be authenticated when connect to PPTP server. ***Value Range***: 1 ~ 32 characters.
Password	A Must fill setting	Enter the **Password** for this PPTP tunnel to be authenticated when connect to PPTP server.
Default Gateway / Remote Subnet	A Must fill setting	Specify a gateway for this PPTP tunnel to reach PPTP server. When you choose **Remote Subnet**, you need to specify one more setting: the remote subnet. It is for the Intranet of PPTP VPN server. So, at PPTP client peer, the packets whose destination is in the dedicated subnet will be transferred via the PPTP VPN tunnel. Others will be transferred based on current routing policy of the security gateway at PPTP client peer. But, if you choose **Default Gateway** option for the PPTP client peer, all packets, including the Internet accessing of PPTP Client peer, will go through the established PPTP VPN tunnel. That means the remote PPTP VPN server controls the flowing of any packets from the PPTP client peer. Certainly, those packets come through the PPTP VPN tunnel. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24).
Authentication Protocol	1. A Must fill setting 2. Unchecked by default	Specify one ore multiple **Authentication Protocol** for this PPTP tunnel. Available authentication methods are **PAP / CHAP / MS-CHAP / MS-CHAP v2**.
MPPE Encryption	1. Unchecked by default 2. an optional setting	Specify whether PPTP server supports **MPPE Protocol**. Click the **Enable** box to enable MPPE. Note: when MPPE Encryption is enabled, the Authentication Protocol **PAP / CHAP** options will not be available.
NAT before Tunneling	1. Unchecked by default 2. an optional setting	Check the **Enable** box to enable NAT function for this PPTP tunnel.
LCP Echo Type	Auto is set by default	Specify the LCP Echo Type for this PPTP tunnel. It can be **Auto**, **User-defined**, or **Disable**. **Auto**: the system sets the Interval and Max. Failure Time. **User-defined:** enter the Interval and Max. Failure Time. **Disable**: disable the LCP Echo. ***Value Range***: 1 ~ 99999 for Interval Time, 1~999 for Failure Time.
Tunnel	Unchecked by default	Check the **Enable** box to enable this PPTP tunnel.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.
Back	N/A	Click **Back** button to return to the previous page.

Modbus Cellular Gateway

5.1.5 GRE

Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco Systems that encapsulates a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork.

Deploy a M2M gateway for remote site and establish a virtual private network with control center by using GRE tunneling. So, all client hosts behind M2M gateway can make data communication with server hosts behind control center gateway.

> GRE Tunneling is similar to IPSec Tunneling, client requesting the tunnel establishment with the server. Both the client and the server must have a Static IP or a FQDN. Any peer gateway can be worked as either a client or a server, even using the same set of configuration rule.

GRE Tunnel Scenario
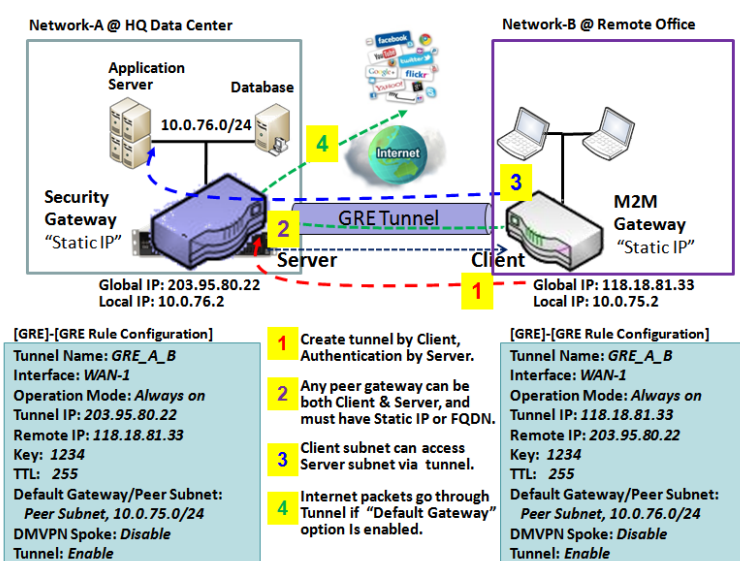
To setup a GRE tunnel, each peer needs to setup its global IP as tunnel IP and fill in the other's global IP as remote IP.

There are two options, "Default Gateway" and "Peer Subnet" for the "Default Gateway / Peer Subnet" configuration item. When you choose "Peer Subnet", you need to specify one more setting: the peer subnet. It is for the Intranet of GRE server. So, at GRE client peer, the packets whose destination is in the dedicated subnet will be transferred via the GRE tunnel. Others will be transferred based on current routing policy of the gateway at GRE client peer. But, if you choose "Default Gateway" option for the GRE client peer, all packets, including the

Modbus Cellular Gateway

Internet accessing of GRE client peer, will go through the established GRE tunnel. That means the remote GRE server controls the flowing of any packets from the GRE client peer. Certainly, those packets come through the GRE tunnel.

If the GRE server supports DMVPN Hub function, like Cisco router as the VPN concentrator, the GRE client can active the DMVPN spoke function here since it is implemented by GRE over IPSec tunneling.

GRE Setting

Go to **Security > VPN > GRE** tab.

The GRE setting allows user to create and configure GRE tunnels.

Enable GRE

Enable GRE Window		
Item	**Value setting**	**Description**
GRE Tunnel	Unchecked by default	Click the **Enable** box to enable GRE function.
Max. Concurrent GRE Tunnels	1. 32 is set by default 2. Max. of 32 connections	It specifies the maximum number of simultaneous GRE tunnel connections. Note: The maximum supported tunnels can be different for the purchased gateway.
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

Create/Edit GRE tunnel

When **Add/Edit** button is applied, a GRE Rule Configuration screen will appear.

Modbus Cellular Gateway

GRE Rule Configuration Window		
Item	**Value setting**	**Description**
Tunnel Name	A Must fill setting	Enter a tunnel name. Enter a name that is easy for you to identify. **Value Range**: 1 ~ 9 characters.
Interface	1. A Must fill setting 2. WAN 1 is selected by default	Select WAN interface on which GRE tunnel is to be established.
Operation Mode	1. A Must fill setting 2. Alway on is selected by default	There are three available operation modes. Always On, Failover, Load Balance. **Failover/ Always** Define whether the GRE tunnel is a failover tunnel function or an Always on tunnel. Note: If this GRE is a failover tunneling, you will need to select a primary GRE tunnel from which to failover to. **Load Balance** Define whether the GRE tunnel connection will take part in load balance function of the gateway. You will not need to select with WAN interface as the system will automatically utilize the available WAN interfaces to balance traffic loads. For more details on WAN Load Balance, refer to **Basic Network > WAN & Uplink > Load Balance** tab. Note: Load Balance function is not available for the gateway with single WAN.
Tunnel IP	An Optional setting	Enter the Tunnel IP address.

Modbus Cellular Gateway

Remote IP	A Must fill setting	Enter the Remote IP address of remote GRE tunnel gateway. Normally this is the public IP address of the remote GRE gateway.
Key	An Optional setting	Enter the Key for the GRE connection. ***Value Range***: 0 ~ 9999999999.
TTL	1. A Must fill setting 2. 1 to 255 range	Specify **TTL** hop-count value for this GRE tunnel. ***Value Range***: 1 ~ 255.
Keep alive	1. Unchecked by default 2. 5s is set by default	Check the **Enable** box to enable Keep alive function. Select Ping IP to keep live and enter the IP address to ping. Enter the ping time interval in seconds. ***Value Range***: 5 ~ 999 seconds.
Default Gateway / Remote Subnet	A Must fill setting	Specify a gateway for this GRE tunnel to reach GRE server. If the gateway uses its gateway IP address to connect to the internet to connect to the GRE server then select Default Gateway, otherwise, specified a subnet and its netmask –the remote subnet, if the default gateway is not used to connect to the GRE server. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24).
DMVPN Spoke	Unchecked by default	Specify whether the gateway will support DMVPN Spoke for this GRE tunnel. Check Enable box to enable DMVPN Spoke.
IPSec Pre-shared Key	2. Pre-shared Key 8 to 32 character length	Enter a DMVPN spoke authentication Pre-shared Key (8~32 characters). Note: Pre-shared Key will not be available when DMVPN Spoke is not enabled.
IPSec NAT Traversal	Unchecked by default	Check **Enable** box to enable NAT-Traversal. Note: IPSec NAT Traversal will not be available when DMVPN is not enabled.
IPSec Encapsulation Mode	Unchecked by default	Specify IPSec Encapsulation Mode from the dropdown box. There are Transport mode and Tunnel mode supported. Note: IPSec Encapsulation Mode will not be available when DMVPN is not enabled.
Tunnel	Unchecked by default	Check **Enable** box to enable this GRE tunnel.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.
Back	N/A	Click **Back** button to return to the previous page.

Modbus Cellular Gateway

5.2 Firewall
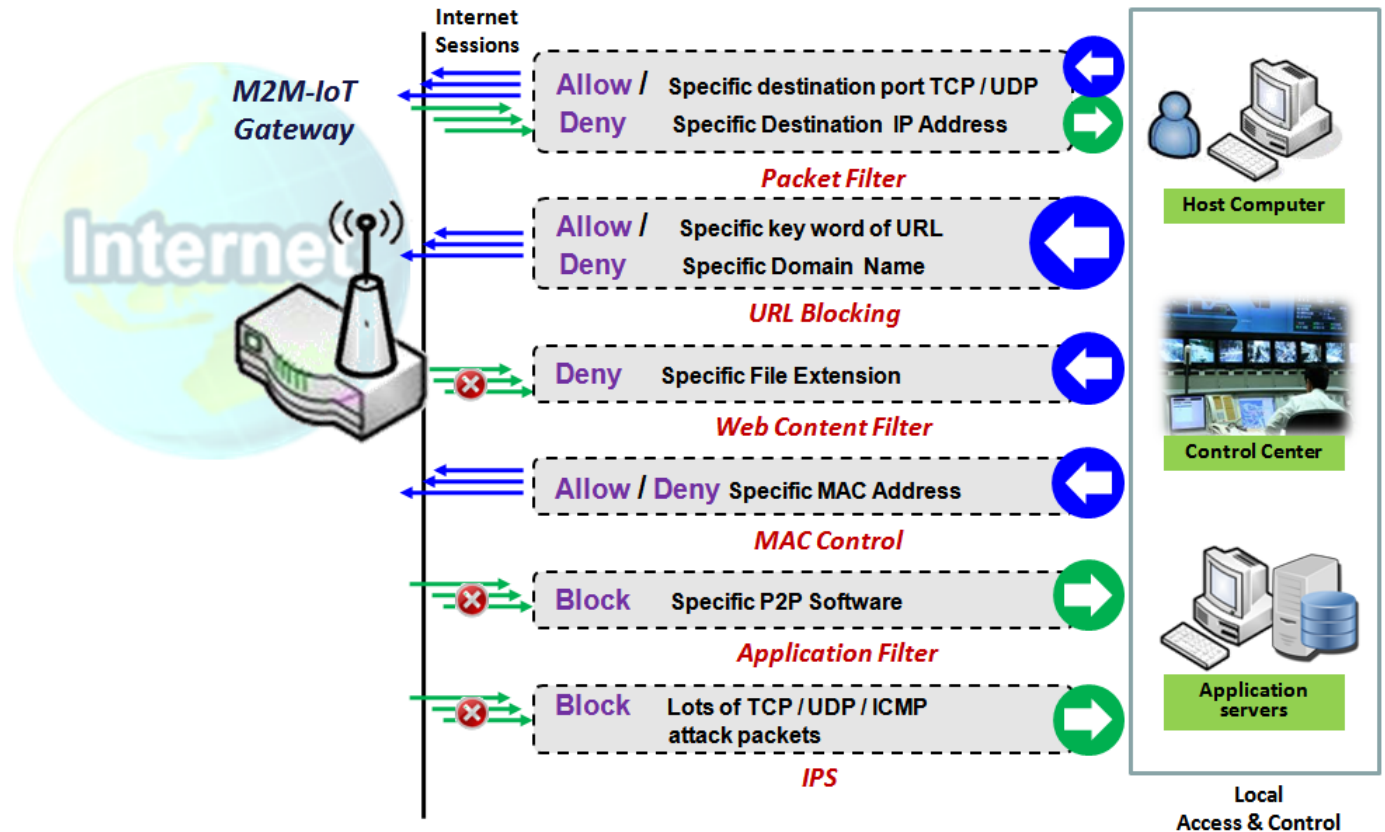
The firewall functions include Packet Filter, URL Blocking, Content Filter, MAC Control, Application Filter, IPS and some firewall options. The supported function can be different for the purchased gateway.

5.2.1 Packet Filter

Configuration												[Help]
Item				**Setting**								
▶ Packet Filters				☑ Enable								
▶ Black List / White List				Deny those match the following rules. ▼								
▶ Log Alert				☐ Log Alert								

Packet Filter List Add Delete												
ID	Rule Name	From Interface	To Interface	Source IP	Destination IP	Source MAC	Protocol	Source Port	Destination Port	Time Schedule	Enable	Actions

Modbus Cellular Gateway

"Packet Filter" function can let you define some filtering rules for incoming and outgoing packets. So the gateway can control what packets are allowed or blocked to pass through it. A packet filter rule should indicate from and to which interface the packet enters and leaves the gateway, the source and destination IP addresses, and destination service port type and port number. In addition, the time schedule to which the rule will be active.

Packet Filter with White List Scenario
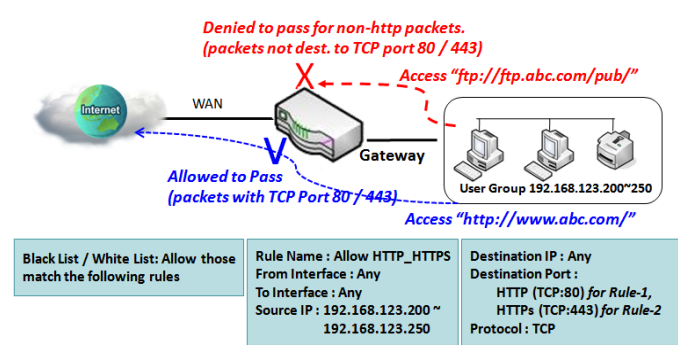
As shown in the diagram, specify "Packet Filter Rule List" as white list (*Allow those match the following rules*) and define the rules. Rule-1 is to allow HTTP packets to pass, and Rule-2 is to allow HTTPS packets to pass.

Under such configuration, the gateway will allow only HTTP and HTTPS packets, issued from the IP range 192.168.123.200 to 250, which are targeted to TCP port 80 or 443 to pass the WAN interface.

Packet Filter Setting

Go to **Security > Firewall > Packet Filter** Tab.

The packet filter setting allows user to create and customize packet filter policies to allow or reject specific inbound/outbound packets through the router based on their office setting.

Enable Packet Filter

Configuration Window		
Item Name	**Value setting**	**Description**
Packet Filter	The box is unchecked by	Check the **Enable** box to activate Packet Filter function

Modbus Cellular Gateway

	default	
Black List / White List	Deny those match the following rules is set by default	When **Deny those match the following rules** is selected, as the name suggest, packets specified in the rules will be blocked –black listed. In contrast, with **Allow those match the following rules**, you can specifically white list the packets to pass and the rest will be blocked.
Log Alert	The box is unchecked by default	Check the **Enable** box to activate Event Log.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Create/Edit Packet Filter Rules

The gateway allows you to customize your packet filtering rules. It supports up to a maximum of 20 filter rule sets.

ID	Rule Name	From Interface	To Interface	Source IP	Destination IP	Source MAC	Protocol	Source Port	Destination Port	Time Schedule	Enable	Actions

Packet Filter List Add Delete

When **Add** button is applied, **Packet Filter Rule Configuration** screen will appear.

Packet Filter Rule Configuration

Item	Setting
▸ Rule Name	Rule1
▸ From Interface	Any ▼
▸ To Interface	Any ▼
▸ Source IP	Any ▼
▸ Destination IP	Any ▼
▸ Source MAC	Any ▼
▸ Protocol	Any(0) ▼
▸ Source Port	User-defined Service ▼ [ ] - [ ]
▸ Destination Port	User-defined Service ▼ [ ] - [ ]
▸ Time Schedule	(0) Always ▼
▸ Rule	☐ Enable

Packet Filter Rule Configuration		
Item Name	**Value setting**	**Description**
Rule Name	1. String format can be	Enter a packet filter rule name. Enter a name that is easy for you to remember.

	any text 2. A Must filled setting	***Value Range***: 1 ~ 30 characters.
From Interface	1. A Must filled setting **2. By default Any is selected**	Define the selected interface to be the packet-entering interface of the router. If the packets to be filtered are coming from **LAN to WAN** then select LAN for this field. Or **VLAN-1 to WAN** then select **VLAN-1** for this field. Other examples are VLAN-1 to VLAN-2. VLAN-1 to WAN. Select **Any** to filter packets coming into the router from any interfaces. Please note that two identical interfaces are not accepted by the router. e.g., VLAN-1 to VLAN-1.
To Interface	1. A Must filled setting 2. By default Any is selected	Define the selected interface to be the packet-leaving interface of the router. If the packets to be filtered are entering from **LAN to WAN then** select **WAN** for this field. Or **VLAN-1 to WAN** then select **WAN** for this field. Other examples are VLAN-1 to VLAN-2. VLAN-1 to WAN. Select **Any** to filter packets leaving the router from any interfaces. Please note that two identical interfaces are not accepted by the router. e.g., VLAN-1 to VLAN-1.
Source IP	1. A Must filled setting 2. By default Any is selected	This field is to specify the **Source IP address**. Select **Any** to filter packets coming from any IP addresses. Select **Specific IP Address** to filter packets coming from an IP address. Select **IP Range** to filter packets coming from a specified range of IP address. Select **IP Address-based Group** to filter packets coming from a pre-defined group. Note: group must be pre-defined before this option become available. Refer to **Object Definition** > **Grouping > Host grouping.** You may also access to create a group by the **Add Rule** shortcut button.
Destination IP	1. A Must filled setting 2. By default Any is selected	This field is to specify the **Destination IP address**. Select **Any** to filter packets that are entering to any IP addresses. Select **Specific IP Address** to filter packets entering to an IP address entered in this field. Select **IP Range** to filter packets entering to a specified range of IP address entered in this field. Select **IP Address-based Group** to filter packets entering to a pre-defined group selected. Note: group must be pre-defined before this selection become available. Refer to **Object Definition** > **Grouping > Host grouping.** You may also access to create a group by the **Add Rule** shortcut button. Setting done through the **Add Rule** button will also appear in the **Host grouping** setting screen.
Source MAC	1. A Must filled setting 2. By default Any is selected	This field is to specify the **Source MAC address**. Select **Any** to filter packets coming from any MAC addresses. Select **Specific MAC Address** to filter packets coming from a MAC address. Select **MAC Address-based Group** to filter packets coming from a pre-defined group selected. Note: group must be pre-defined before this selection become available. Refer to **Object Definition** > **Grouping > Host grouping.** You may also access to create a group by the **Add Rule** shortcut button.
Protocol	1. A Must filled setting 2. By default Any(0) is selected	For **Protocol**, select **Any** to filter any protocol packets Then for **Source Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range.

		Then for **Destination Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. ***Value Range***: 1 ~ 65535 for Source Port, Destination Port.
		For **Protocol**, select **ICMPv4** to filter ICMPv4 packets
		For **Protocol**, select **TCP** to filter **TCP** packets Then for **Source Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. Then for **Destination Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. ***Value Range***: 1 ~ 65535 for Source Port, Destination Port.
		For **Protocol**, select **UDP** to filter **UDP** packets Then for **Source Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. Then for **Destination Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. ***Value Range***: 1 ~ 65535 for Source Port, Destination Port.
		For **Protocol**, select **GRE** to filter **GRE** packets
		For **Protocol**, select **ESP** to filter **ESP** packets
		For **Protocol**, select **SCTP** to filter **SCTP** packets
		For **Protocol**, select **User-defined** to filter packets with specified port number. Then enter a pot number in **Protocol Number** box.
Time Schedule	A Must filled setting	Apply **Time Schedule** to this rule, otherwise leave it as Always. If the dropdown list is empty ensure **Time Schedule** is pre-configured. Refer to **Object Definition > Scheduling > Configuration** tab.
Rule	The box is unchecked by default.	Click **Enable** box to activate this rule then save the settings.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings
Back	N/A	When the **Back** button is clicked the screen will return to the Packet Filter Configuration page.

5.2.2 URL Blocking

"URL Blocking" function can let you define blocking or allowing rules for incoming and outgoing Web request packets. With defined rules, gateway can control the Web requests containing the complete URL, partial domain name, or pre-defined keywords. For example, one can filter out or allow only the Web requests based on domain input suffixes like .com or .org or keywords like "bct" or "mpe".

An URL blocking rule should specify the URL, partial domain name, or included keywords in the Web requests from and to the gateway and also the destination service port. Besides, a certain time schedule can be applied to activate the URL Blocking rules during pre-defined time interval(s).

The gateway will logs and displays the disallowed web accessing requests that matched the defined URL blocking rule in the black-list or in the exclusion of the white-list.

When you choose "Allow all to pass except those match the following rules" for the "URL Blocking Rule List", you are setting the defined URL blocking rules to belong to the black list. The packets, listed in the rule list, will be blocked if one pattern in the requests matches to one rule. Other Web requests can pass through the gateway. In contrast, when you choose "Deny all to pass except those match the following rules" for the "URL Blocking Rule List", you are setting the defined packet filtering rules to belong to the white list. The Web requests, listed in the rule, will be allowed if one pattern in the requests matches to one rule. Other Web requests will be blocked.

URL Blocking Rule with Black List
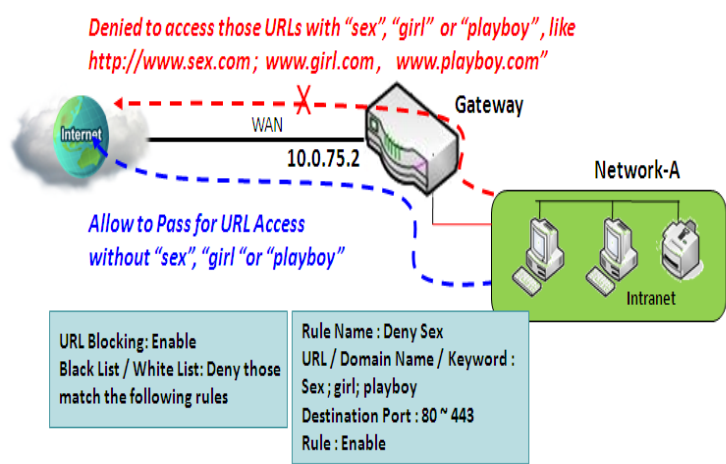
When the administrator of the gateway wants to block the Web requests with some dedicated patterns, he can use the "URL Blocking" function to block specific Web requests by defining the black list as shown in above diagram. Certainly, when the administrator wants to allow only the Web requests with some dedicated patterns to go through the gateway, he can also use the "URL Blocking" function by defining the white list to meet the requirement.

As shown in the diagram, enable the URL blocking function and create the first rule to deny the Web requests with "sex" or "sexygirl" patterns and the other to deny the Web requests with "playboy" pattern to go through the gateway. System will block the Web requests with "sex", "sexygirl" or "playboy" patterns to pass through the gateway.

Modbus Cellular Gateway

URL Blocking Setting

Go to **Security > Firewall > URL Blocking** Tab.

In "URL Blocking" page, there are three configuration windows. They are the "Configuration" window, "URL Blocking Rule List" window, and "URL Blocking Rule Configuration" window.

The "Configuration" window can let you activate the URL blocking function and specify to black listing or to white listing the packets defined in the "URL Blocking Rule List" entry. In addition, log alerting can be enabled to record on-going events for any disallowed Web request packets. Refer to "System Status" in "6.1.1 System Related" section in this user manual for how to view recorded log.

The "URL Blocking Rule List" window lists all your defined URL blocking rule entry. And finally, the "URL Blocking Rule Configuration" window can let you define URL blocking rules. The parameters in a rule include the rule name, the Source IP or MAC, the URL/Domain Name/Keyword, the destination service ports, the integrated time schedule rule and the rule activation.

Enable URL Blocking

Configuration	[Help]
Item	**Setting**
▶ URL Blocking	☐ Enable
▶ Black List / White List	Deny those match the following rules. ▾
▶ Log Alert	☐ Enable

Configuration Item	Value setting	Description
URL Blocking	The box is unchecked by default	Check the **Enable** box to activate URL Blocking function.
Black List / White List	**Deny those match the following rules** is set by default	Specify the URL Blocking Policy, either Black List or White List. Black List: When **Deny those match the following rules** is selected, as the name suggest, the matched Web request packets will be blocked. White List: When **Allow those match the following rules** is selected, the matched Web request packets can pass through the Gateway, and the others that don't match the rules will be blocked.
Log Alert	The box is unchecked by default	Check the **Enable** box to activate Event Log.
Save	NA	Click **Save** button to save the settings
Undo	NA	Click **Undo** button to cancel the settings

Create/Edit URL Blocking Rules

The Gateway supports up to a maximum of 20 URL blocking rule sets. Ensure that the URL Blocking is enabled before we can create blocking rules.

Modbus Cellular Gateway

When **Add** button is applied, the **URL Blocking Rule Configuration** screen will appear.

URL Blocking Rules Configuration		
Item	**Value setting**	**Description**
Rule Name	1. String format can be any text 2. A Must filled setting	Specify an URL Blocking rule name. Enter a name that is easy for you to understand.
Source IP	1. A Must filled setting 2. **Any** is set by default	This field is to specify the **Source IP address**. • Select **Any** to filter packets coming from any IP addresses. • Select **Specific IP Address** to filter packets coming from an IP address entered in this field. • Select **IP Range** to filter packets coming from a specified range of IP address entered in this field. • Select **IP Address-based Group** to filter packets coming from a pre-defined group selected. Note: group must be pre-defined before this option become available. Refer to **Object Definition** > **Grouping > Host grouping**.
Source MAC	1. A Must filled setting 2. **Any** is set by default	This field is to specify the **Source MAC address**. • Select **Any** to filter packets coming from any MAC addresses. • Select **Specific MAC Address** to filter packets coming from a MAC address entered in this field. • Select **MAC Address-based Group** to filter packets coming from a pre-defined group selected. Note: group must be pre-defined before this selection become available. Refer to **Object Definition** > **Grouping > Host grouping**.
URL / Domain Name / Keyword	1. A Must filled setting 2. Supports up to a maximum of 10 Keywords in a rule by using the	Specify URL, Domain Name, or Keyword list for URL checking. • In the **Black List** mode, if a matched rule is found, the packets will be dropped. • In the **White List** mode, if a matched rule is found, the packets will be accepted and the others which don't match any rule will be dropped.

	delimiter ";".	
Destination Port	1. A Must filled setting 2. **Any** is set by default	This field is to specify the **Destination Port number**. • Select **Any** to filter packets going to any Port. • Select **Specific Service Port** to filter packets going to a specific Port entered in this field. • Select **Port Range** to filter packets going to a specific range of Ports entered in this field.
Time Schedule Rule	A Must filled setting	Apply a specific **Time Schedule** to this rule; otherwise leave it as **(0) Always**. If the dropdown list is empty ensure **Time Schedule** is pre-configured. Refer to **Object Definition** > **Scheduling > Configuration** tab.
Rule	The box is unchecked by default.	Click the **Enable** box to activate this rule.
Save	*NA*	Click the **Save** button to save the settings.
Undo	*NA*	Click the **Undo** button to cancel the changes.
Back	*NA*	Click the **Back** button to return to the URL Blocking Configuration page.

5.2.3 MAC Control

"MAC Control" function allows you to assign the accessibility to the gateway for different users based on device's MAC address. When the administrator wants to reject the traffics from some client hosts with specific MAC addresses, he can use the "MAC Control" function to reject with the black list configuration.

MAC Control with Black List Scenario
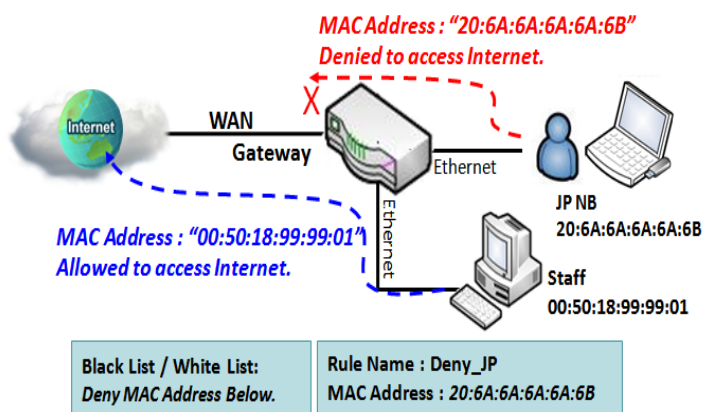
As shown in the diagram, enable the MAC control function and specify the "MAC Control Rule List" is a black list, and configure one MAC control rule for the gateway to deny the connection request from the "JP NB" with its own MAC address 20:6A:6A:6A:6A:6B.

System will block the connecting from the "JP NB" to the gateway but allow others.

Modbus Cellular Gateway

MAC Control Setting

Go to **Security > Firewall > MAC Control** Tab.

The MAC control setting allows user to create and customize MAC address policies to allow or reject packets with specific source MAC address.

Enable MAC Control

Configuration	[Help]
Item	**Setting**
▶ MAC Control	☐ Enable
▶ Black List / White List	Deny MAC Address Below. ▼
▶ Log Alert	☐ Enable
▶ Known MAC from LAN PC List	192.168.123.100(James-P45V) ▼ [Copy to]

Configuration Window		
Item	**Value setting**	**Description**
MAC Control	The box is unchecked by default	Check the **Enable** box to activate the MAC filter function
Black List / White List	Deny MAC Address Below is set by default	When **Deny MAC Address Below** is selected, as the name suggest, packets specified in the rules will be blocked –black listed. In contrast, with **Allow MAC Address Below**, you can specifically white list the packets to pass and the rest will be blocked.
Log Alert	The box is unchecked by default	Check the **Enable** box to activate to activate Event Log.
Known MAC from LAN PC List	N/A	Select a MAC Address from LAN Client List. Click the **Copy to** to copy the selected **MAC Address** to the filter rule.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Modbus Cellular Gateway

Create/Edit MAC Control Rules

The gateway supports up to a maximum of 20 filter rule sets. Ensure that the MAC Control is enabled before we can create control rules.

ID	Rule Name	MAC Address	Time Schedule Rule	Enable	Actions

When **Add** button is applied, **Filter Rule Configuration** screen will appear.

Rule Name	MAC Address (Use : to Compose)	Time Schedule	Enable
Rule1		(0) Always ▾	☐

Save

MAC Control Rule Configuration		
Item	**Value setting**	**Description**
Rule Name	1. String format can be any text 2. A Must fill setting	Enter a MAC Control rule name. Enter a name that is easy for you to remember.
MAC Address (Use: to Compose)	1. MAC Address string Format 2. A Must fill setting	Specify the **Source MAC Address** to filter rule.
Time Schedule	A Must fill setting	Apply **Time Schedule** to this rule; otherwise leave it as **(0) Always**. If the dropdown list is empty, ensure **Time Schedule** is pre-configured. Refer to **Object Definition > Scheduling > Configuration tab**
Enable	The box is unchecked by default.	Click **Enable** box to activate this rule, and then save the settings.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings
Back	N/A	Click **Back** to return to the MAC Control Configuration page.

5.2.4 ~~Content Filter~~ (not supported)

Not supported feature for the purchased product, leave it as blank.

5.2.5 ~~Application Filter~~ (not supported)

Not supported feature for the purchased product, leave it as blank.

Modbus Cellular Gateway

5.2.6 IPS

To provide application servers in the Internet, administrator may need to open specific ports for the services. However, there are some risks to always open service ports in the Internet. In order to avoid such attack risks, it is important to enable IPS functions.

Intrusion Prevention System (IPS) is network security appliances that monitor network and/or system activities for malicious activity. The main functions of IPS are to identify malicious activity, log information about this activity, attempt to block/stop it and report it. You can enable the IPS function and check the listed intrusion activities when needed. You can also enable the log alerting so that system will record Intrusion events when corresponding intrusions are detected.

IPS Scenario
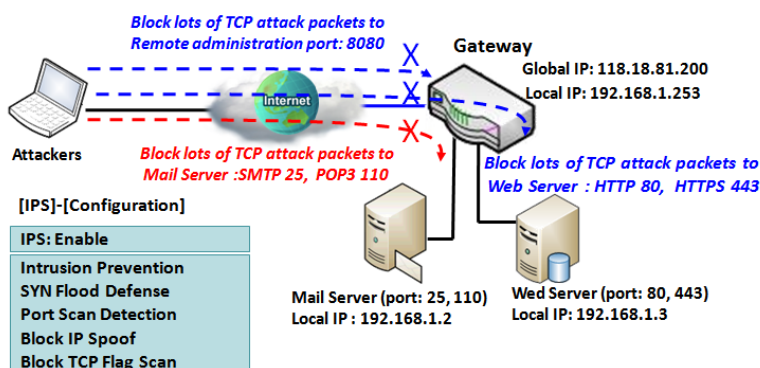
As shown in the diagram, the gateway serves as an E-mail server, Web Server and also provides TCP port 8080 for remote administration. So, remote users or unknown users can request those services from Internet. With IPS enabled, the gateway can detect incoming attack packets, including the TCP ports (25, 80, 110, 443 and 8080) with services. It will block the attack packets and let the normal access to pass through the gateway

Modbus Cellular Gateway

IPS Setting

Go to **Security > Firewall > IPS** Tab.

The Intrusion Prevention System (IPS) setting allows user to customize intrusion prevention rules to prevent malicious packets.

Enable IPS Firewall

Configuration		[Help]
Item	**Setting**	
▶ IPS	☐ Enable	
▶ Log Alert	☐ Enable	

Configuration Window		
Item	**Value setting**	**Description**
IPS	The box is unchecked by default	Check the **Enable** box to activate IPS function
Log Alert	The box is unchecked by default	Check the **Enable** box to activate to activate Event Log.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Setup Intrusion Prevention Rules

The router allows you to select intrusion prevention rules you may want to enable. Ensure that the IPS is enabled before we can enable the defense function.

Modbus Cellular Gateway

Setup Intrusion Prevention Rules		
Item Name	**Value setting**	**Description**
SYN Flood Defense	1. A Must filled setting	Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field.
UDP Flood Defense	2. The box is unchecked by default. 3. Traffic threshold is set to 300 by default	Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field.
ICMP Flood Defense	4. The value range can be from 10 to 10000.	Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field. *Value Range*: 10 ~ 10000.
Port Scan Defection	1. A Must filled setting 2. The box is unchecked by default. 3. Traffic threshold is set to 200 by default 4. The value range can be from 10 to 10000.	Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field. *Value Range*: 10 ~ 10000.
Block Land Attack **Block Ping of Death** **Block IP Spoof** **Block TCP Flag Scan** **Block Smurf**	The box is unchecked by default.	Click **Enable** box to activate this intrusion prevention rule.

Modbus Cellular Gateway

Block Traceroute Block Fraggle Attack		
ARP Spoofing Defence	1. A Must filled setting 2. The box is unchecked by default. 3. Traffic threshold is set to 300 by default 4. The value range can be from 10 to 10000.	Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field. ***Value Range***: 10 ~ 10000.
Save	NA	Click **Save** to save the settings
Undo	NA	Click **Undo** to cancel the settings

Modbus Cellular Gateway

5.2.7 Options

Firewall Options	[Help]
Item	**Setting**
▸ Stealth Mode	☐ Enable
▸ SPI	☑ Enable
▸ Discard Ping from WAN	☐ Enable

Remote Administrator Host Definition

ID	Interface	Protocol	IP	Subnet Mask	Service Port	Enable	Action
1	All WAN	HTTP	Any IP	N/A	80	☐	Edit
2	All WAN	HTTP	Any IP	N/A	80	☐	Edit
3	All WAN	HTTP	Any IP	N/A	80	☐	Edit
4	All WAN	HTTP	Any IP	N/A	80	☐	Edit
5	All WAN	HTTP	Any IP	N/A	80	☐	Edit

There are some additional useful firewall options in this page.

"Stealth Mode" lets gateway not to respond to port scans from the WAN so that makes it less susceptible to discovery and attacks on the Internet. "SPI" enables gateway to record the packet information like IP address, port address, ACK, SEQ number and so on while they pass through the gateway, and the gateway checks every incoming packet to detect if this packet is valid.

"Discard Ping from WAN" makes any host on the WAN side can`t ping this gateway. And finally, "Remote Administrator Hosts" enables you to perform administration task from a remote host. If this feature is enabled, only specified IP address(es) can perform remote administration.

Modbus Cellular Gateway

Enable SPI Scenario
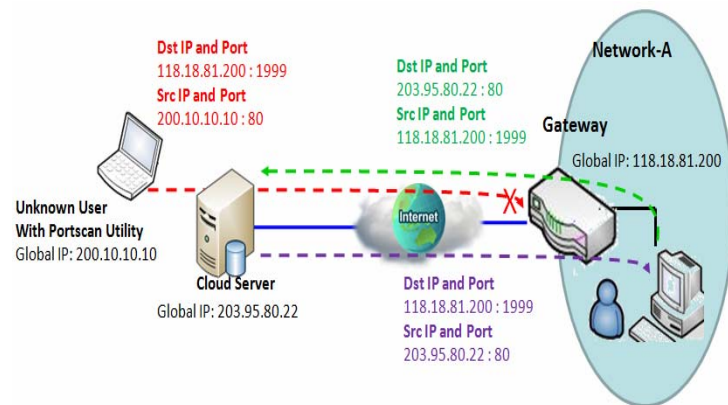
As shown in the diagram, Gateway has the IP address of 118.18.81.200 for WAN interface and 192.168.1.253 for LAN interface. It serves as a NAT gateway. Users in Network-A initiate to access cloud server through the gateway. Sometimes, unknown users will simulate the packets but use different source IP to masquerade. With the SPI feature been enabled at the gateway, it will block such packets from unknown users.

Discard Ping from WAN & Remote Administrator Hosts Scenario
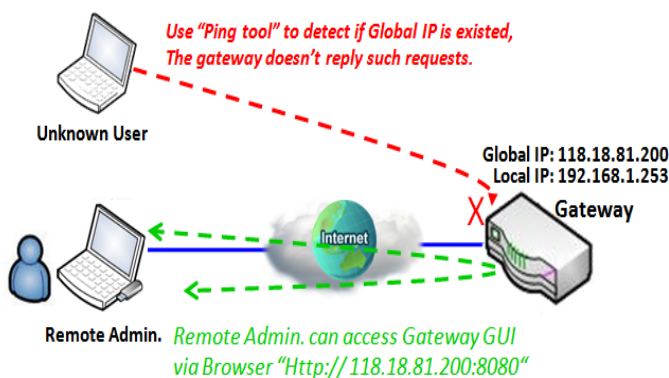
"Discard Ping from WAN" makes any host on the WAN side can`t ping this gateway reply any ICMP packets. Enable the Discard Ping from WAN function to prevent security leak when local users surf the internet.

Remote administrator knows the gateway's global IP, and he can access the Gateway GUI via TCP port 8080.

Firewall Options Setting

Go to **Security > Firewall > Options** Tab.

The firewall options setting allows network administrator to modify the behavior of the firewall and to enable Remote Router Access Control.

Enable Firewall Options

Modbus Cellular Gateway

Item	Setting
▸ Stealth Mode	☐ Enable
▸ SPI	☑ Enable
▸ Discard Ping from WAN	☐ Enable

Firewall Options

Item	Value setting	Description
Stealth Mode	The box is unchecked by default	Check the **Enable** box to activate the Stealth Mode function
SPI	The box is checked by default	Check the **Enable** box to activate the SPI function
Discard Ping from WAN	The box is unchecked by default	Check the **Enable** box to activate the Discard Ping from WAN function

Define Remote Administrator Host

The router allows network administrator to manage router remotely. The network administrator can assign specific IP address and service port to allow accessing the router.

Remote Administrator Host Definition

ID	Interface	Protocol	IP	Subnet Mask	Service Port	Enable	Action
1	All WAN	HTTP	Any IP	N/A	80	☐	Edit
2	All WAN	HTTP	Any IP	N/A	80	☐	Edit
3	All WAN	HTTP	Any IP	N/A	80	☐	Edit
4	All WAN	HTTP	Any IP	N/A	80	☐	Edit
5	All WAN	HTTP	Any IP	N/A	80	☐	Edit

Remote Administrator Host Definition

Item	Value setting	Description
Protocol	HTTP is set by default	Select **HTTP** or **HTTPS** method for router access.
IP	A Must filled setting	This field is to specify the remote host to assign access right for remote access. Select **Any IP** to allow any remote hosts Select **Specific IP** to allow the remote host coming from a specific subnet. An IP address entered in this field and a selected **Subnet Mask** to compose the subnet.

Modbus Cellular Gateway

Service Port	1. 80 for HTTP by default 2. 443 for HTTPS by default	This field is to specify a Service Port to HTTP or HTTPS connection. ***Value Range***: 1 ~ 65535.
Enabling the rule	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click **Enable** box to activate this rule then save the settings.
Undo	N/A	Click **Undo** to cancel the settings

Chapter 6 Administration

6.1 Configure & Manage
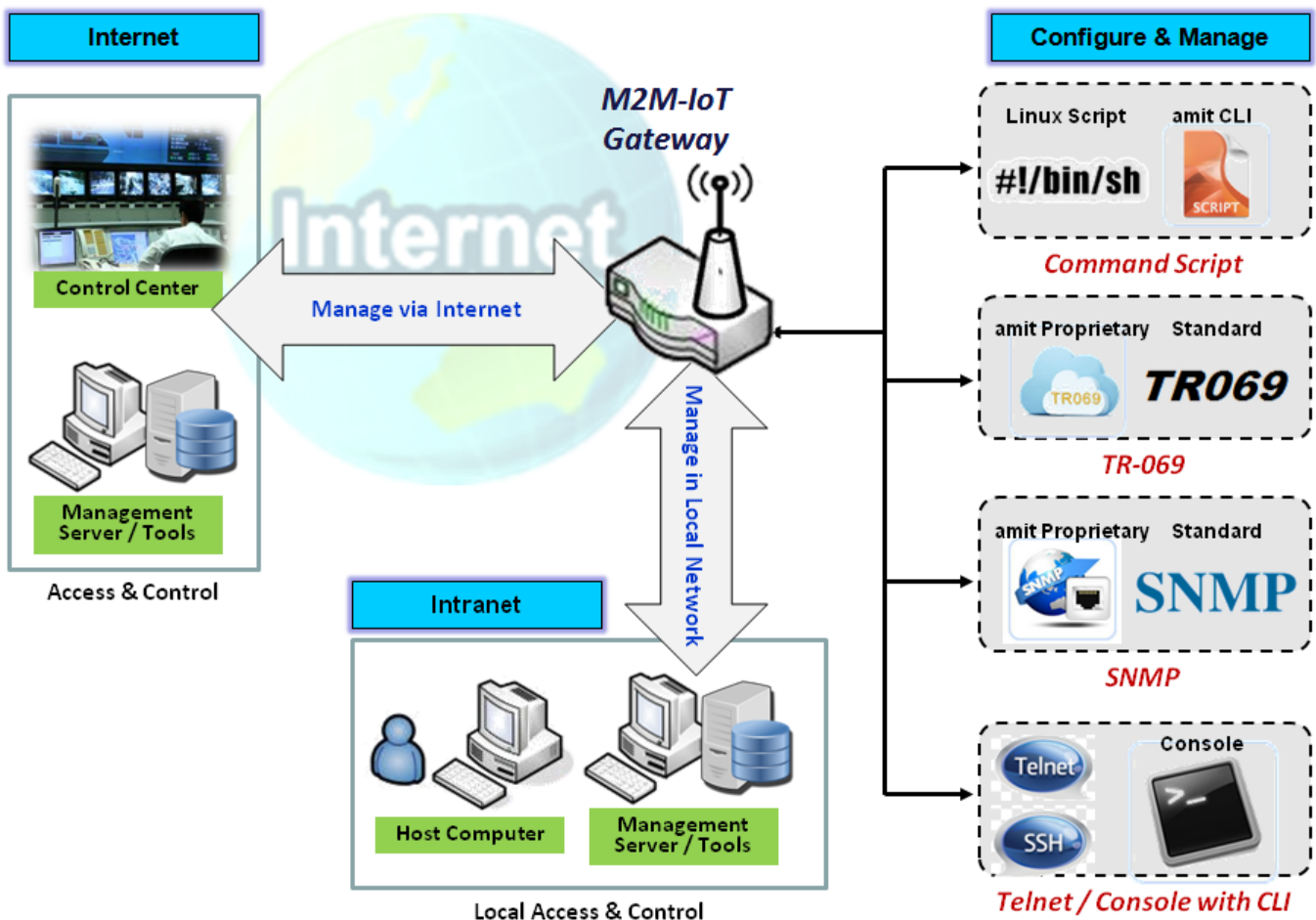
Configure & Manage refers to enterprise-wide administration of distributed systems including (and commonly in practice) computer systems. Centralized management has a time and effort trade-off that is related to the size of the company, the expertise of the IT staff, and the amount of technology being used. This device supports many system management protocols, such as Command Script, TR-069, SNMP, and Telnet with CLI. You can setup those configurations in the "Configure & Manage" section.

Modbus Cellular Gateway

6.1.1 Command Script

Command script configuration is the application that allows administrator to setup the pre-defined configuration in plain text style and apply configuration on startup.

Go to **Administration > Command Script > Configuration** Tab.

Enable Command Script Configuration

Configuration Item	Value setting	Description
Configuration	The box is unchecked by default	Check the **Enable** box to activate the Command Script function.

Edit/Backup Plain Text Command Script

You can edit the plain text configuration settings in the configuration screen as above.

Plain Text Configuration Item	Value setting	Description
Clean	NA	Clean text area. (You should click **Save** button to further clean the configuration already saved in the system.)
Backup	NA	Backup and download configuration.
Save	NA	Save configuration

The supported plain text configuration items are shown in the following list. For the settings that can be executed with standard Linux commands, you can put them in a script file, and apply to the system configure with **STARTUP** command. For those configurations without corresponding Linux command set to configure, you can configure them with proprietary command set.

Modbus Cellular Gateway

Configuration Content		
Key	**Value setting**	**Description**
OPENVPN_ENABLED	1 : enable 0 : disable	Enable or disable OpenVPN Client function.
OPENVPN_DESCRIPTION	A Must filled Setting	Specify the tunnel name for the OpenVPN Client connection.
OPENVPN_PROTO	udp tcp	Define the **Protocol** for the OpenVPN Client. • Select **TCP** or **TCP /UDP** ->The OpenVPN will use TCP protocol, and **Port** will be set as 443 automatically. • Select **UDP** -> The OpenVPN will use UDP protocol, and **Port** will be set as 1194 automatically.
OPENVPN_PORT	A Must filled Setting	Specify the **Port** for the OpenVPN Client to use.
OPENVPN_REMOTE_IPADDR	IP or FQDN	Specify the **Remote IP/FQDN** of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the IP address or FQDN.
OPENVPN_PING_INTVL	seconds	Specify the time interval for OpenVPN keep-alive checking.
OPENVPN_PING_TOUT	seconds	Specify the timeout value for OpenVPN Client keep-alive checking.
OPENVPN_COMP	Adaptive	Specify the **LZO Compression** algorithm for OpenVPN client.
OPENVPN_AUTH	Static Key/TLS	Specify the authorization mode for the OpenVPN tunnel. • **TLS** ->The OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Client Cert.** and **Client Key** need to specify as well.
OPENVPN_CA_CERT	A Must filled Setting	Specify the Trusted CA certificate for the OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_CERT	A Must filled Setting	Specify the local certificate for OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_KEY	A Must filled Setting	Specify the local key for the OpenVPN client. It will go through Base64 Conversion.
OPENVPN_EXTRA_OPTS	Options	Specify the extra options setting for the OpenVPN client.
IP_ADDR1	Ip	Ethernet LAN IP
IP_NETM1	Net mask	Ethernet LAN MASK
PPP_MONITORING	1 : enable 0 : disable	When the Network Monitoring feature is enabled, the router will use DNS Query or ICMP to periodically check Internet connection – connected or disconnected.
PPP_PING	0 : DNS Query 1 : ICMP Query	With **DNS Query,** the system checks the connection by sending DNS Query packets to the destination specified in PPP_PING_IPADDR. With **ICMP Query,** the system will check connection by sending ICMP request packets to the destination specified in PPP_PING_IPADDR.
PPP_PING_IPADDR	IP	Specify an IP address as the target for sending DNS query/ICMP request.
PPP_PING_INTVL	seconds	Specify the time interval for between two DNS Query or ICMP checking packets.
STARTUP	Script file	For the configurations that can be configured with standard Linux commands, you can put them in a script file, and apply the script file with STARTUP command. For example, STARTUP=#!/bin/sh STARTUP=echo "startup done" > /tmp/demo

Modbus Cellular Gateway

Plain Text System Configuration with Telnet

In addition to the web-style plain text configuration as mentioned above, the gateway system also allow the configuration via Telnet CLI. Administrator can use the proprietary telnet command "***txtConfig***" and related action items to perform the plain system configuration.

The command format is: txtConfig (action) [option]

Action	Option	Description
clone	*Output file*	Duplicate the configuration content from database and stored as a configuration file. (ex: *txtConfig clone /tmp/config*) The contents in the configuration file are the same as the plain text commands mentioned above. This action is exactly the same as performing the "Backup" plain text configuration.
commit	a existing file	Commit the configuration content to database. (ex: *txtConfig commit /tmp/config*)
enable	*NA*	Enable plain text system config. (ex: *txtConfig enable*)
disable	*NA*	Disable plain text system config. (ex: *txtConfig disable*)
run_immediately	*NA*	Apply the configuration content that has been committed in database. (ex: *txtConfig run_immediately*)
run_immediately	a existing file	Assign a configuration file to apply. (ex: *txtConfig run_immediately /tmp/config*)

Modbus Cellular Gateway

6.1.2 TR-069

TR-069 (Technical Report 069) is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices, like this gateway device. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS). The Security Gateway is such CPE.

TR-069 is a customized feature for ISP. It is not recommend that you change the configuration for this. If you have any problem in using this feature for device management, please contact with your ISP or the ACS provider for help. At the right upper corner of TR-069 Setting screen, one "[Help]" command let you see the same message about that.

Scenario - Managing deployed gateways through an ACS Server
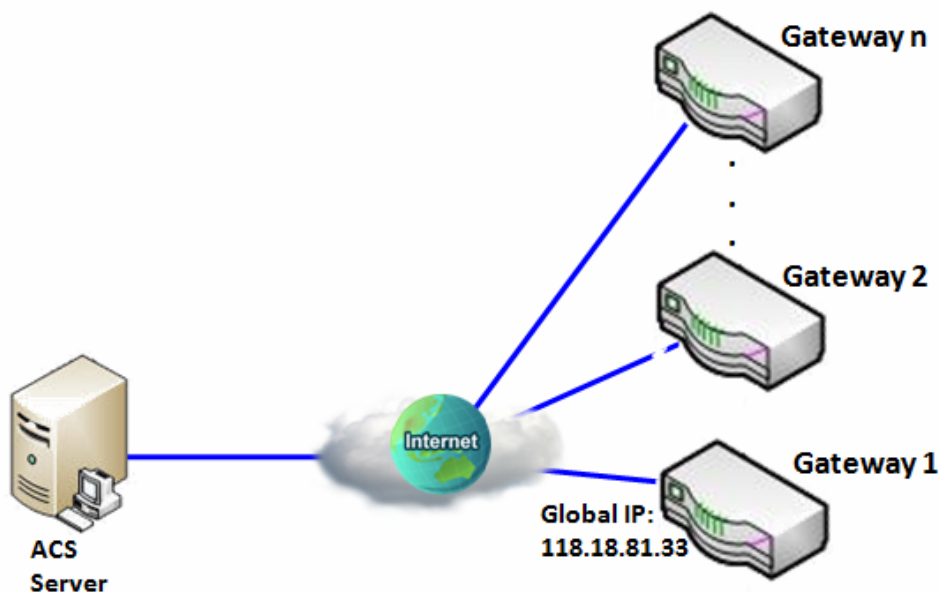
Scenario Application Timing

When the enterprise data center wants to use an ACS server to manage remote gateways geographically distributed elsewhere in the world, the gateways in all branch offices must have an embedded TR-069 agent to communicate with the ACS server. So that the ACS server can configure, FW upgrade and monitor these gateways and their corresponding Intranets.

Scenario Description

The ACS server can configure, upgrade with latest FW and monitor these gateways.

Remote gateways inquire the ACS server for jobs to do in each time period.

The ACS server can ask the gateways to execute some urgent jobs.

Modbus Cellular Gateway

Parameter Setup Example

Following tables list the parameter configuration as an example for the Gateway 1 in above diagram with "TR-069" enabling.

Use default value for those parameters that are not mentioned in the tables.

Configuration Path	[TR-069]-[Configuration]
TR-069	■ *Enable*
ACS URL	**http://qaamit.acslite.com/cpe.php**
ACS User Name	*ACSUserName*
ACS Password	*ACSPassword*
ConnectionRequest Port	*8099*
ConnectionRequest User Name	*ConnReqUserName*
ConnectionRequest Password	*ConnReqPassword*
Inform	■ *Enable Interval 900*

Scenario Operation Procedure

In above diagram, the ACS server can manage multiple gateways in the Internet. The "Gateway 1" is one of them and has 118.18.81.33 IP address for its WAN-1 interface.

When all remote gateways have booted up, they will try to connect to the ACS server.

Once the connections are established successfully, the ACS server can configure, upgrade with latest FW and monitor these gateways.

Remote gateways inquire the ACS server for jobs to do in each time period.

If the ACS server needs some urgent jobs to be done by the gateways, it will issue the "Connection Request" command to those gateways. And those gateways make immediate connections in response to the ACS server's immediate connection request for executing the urgent jobs.

Modbus Cellular Gateway

TR-069 Setting

Go to **Administration > Configure & Manage > TR-069** tab.

In "TR-069" page, there is only one configuration window for TR-069 function. In the window, you must specify the related information for your security gateway to connect to the ACS. Drive the function to work by specifying the URL of the ACS server, the account information to login the ACS server, the service port and the account information for connection requesting from the ACS server, and the time interval for job inquiry. Except the inquiry time, there are no activities between the ACS server and the gateways until the next inquiry cycle. But if the ACS server has new jobs that are expected to do by the gateways urgently, it will ask these gateways by using connection request related information for immediate connection for inquiring jobs and executing.

Configuration	[Help]
Item	**Setting**
▶ TR-069	☐ Enable
▶ Interface	WAN-1 ▾
▶ Data model	Standard ▾
▶ ACS URL	
▶ ACS UserName	
▶ ACS Password	
▶ ConnectionRequest Port	8099
▶ ConnectionRequest UserName	
▶ ConnectionRequest Password	
▶ Inform	☑ Enable Interval 300

TR-069		
Item	**Value setting**	**Description**
TR-069	The box is unchecked by default	Check the **Enable** box for activate TR-069

Modbus Cellular Gateway

Interface	WAN-1 is selected by default.	When you finish set basic network WAN-1 ~ WAN-n, you can choose WAN-1 ~ WAN-n When you finish set Security > VPN > IPSec/OpenVPN/PPTP/L2TP/GRE, you can choose IPSec/OpenVPN/PPTP/L2TP/GRE tunnel, the interface just like "IPSec #1"
Data Model	Standard is selected by default.	Select the TR-069 dat model for the remote management. **Standard** : the ACS Server is a standard one, which is fully comply with TR-069. **AMIT's ACS Data Model** : Select this data model if you intend to use AMIT's Cloud ACS Server to managing the deployed gateways.
ACS URL	A Must filled setting	You can ask ACS manager provide ACS URL and manually set
ACS Username	A Must filled setting	You can ask ACS manager provide ACS username and manually set
ACS Password	A Must filled setting	You can ask ACS manager provide ACS password and manually set
ConnectionRequest Port	1. A Must filled setting. **2. By default 8099 is set.**	You can ask ACS manager provide ACS ConnectionRequest Port and manually set *Value Range*: 0 ~ 65535.
ConnectionRequest UserName	A Must filled setting	You can ask ACS manager provide ACS ConnectionRequest Username and manually set
ConnectionRequest Password	A Must filled setting	You can ask ACS manager provide ACS ConnectionRequest Password and manually set
Inform	1. The box is checked by default. **2. The Interval value is 300 by default.**	When the **Enable** box is checked, the gateway (CPE) will periodicly send inform message to ACS Server according to the **Interval** setting. *Value Range*: 0 ~ 86400 for Inform Interval.
Save	N/A	Click Save to save the settings

When you finish set **ACS URL ACS Username ACS Password,** your gateway (CPE, Client Premium Equipment) can send inform to ACS Server.

When you finish set **ConnectionRequest Port ConnectionRequest Username ConnectionRequest Password**, ACS Server can ask the gateway (CPE) to send inform to ACS Server.

Modbus Cellular Gateway

6.1.3 SNMP

In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

In typical SNMP uses, one or more administrative computers, called managers, have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes, at all times, a software component called an agent which reports information via SNMP to the manager.

SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. These hierarchies, and other metadata (such as type and description of the variable), are described by Management Information Bases (MIBs).

The device supports several public MIBs and one private MIB for the SNMP agent. The supported MIBs are as follow: MIB-II (RFC 1213, Include IPv6), IF-MIB, IP-MIB, TCP-MIB, UDP-MIB, SMIv1 and SMIv2, SNMPv2-TM and SNMPv2-MIB, and AMIB (AMIT Private MIB)

SNMP Management Scenario
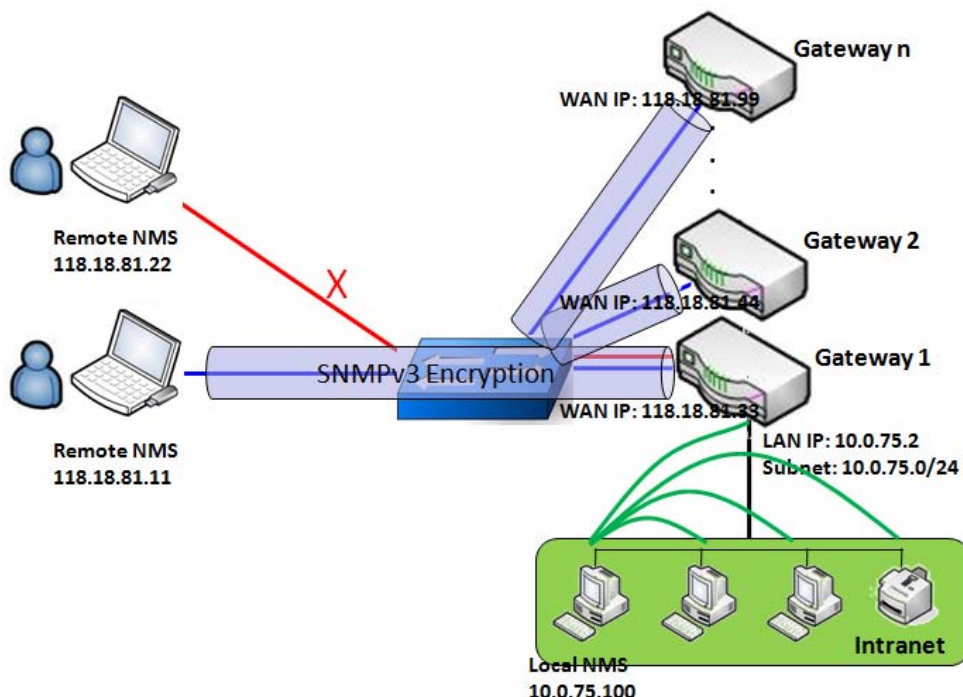
Scenario Application Timing

There are two application scenarios of SNMP Network Management Systems (NMS). Local NMS is in

the Intranet and manage all devices that support SNMP protocol in the Intranet. Another one is the Remote NMS to manage some devices whose WAN interfaces are connected together by using a switch or a router with UDP forwarding. If you want to manage some devices and they all have supported SNMP protocol, use either one application scenario, especially the management of devices in the Intranet. In managing devices in the Internet, the TR-069 is the better solution. Please refer to last sub-section.

Scenario Description

The NMS server can monitor and configure the managed devices by using SNMP protocol, and those devices are located at where UDP packets can reach from NMS.

The managed devices report urgent trap events to the NMS servers.

Use SNMPv3 version of protocol can protected the transmitting of SNMP commands and responses.

The remote NMS with privilege IP address can manage the devices, but other remote NMS can't.

Parameter Setup Example

Following tables list the parameter configuration as an example for the Gateway 1 in above diagram with "SNMP" enabling at LAN and WAN interfaces.

Use default value for those parameters that are not mentioned in the tables.

Configuration Path	[SNMP]-[Configuration]
SNMP Enable	■ *LAN* ■ *WAN*
Supported Versions	■ *v1* ■ *v2c* ■ *v3*
Get / Set Community	*ReadCommunity / WriteCommunity*
Trap Event Receiver 1	*118.18.81.11*
WAN Access IP Address	*118.18.81.11*

Configuration Path	[SNMP]-[User Privacy Definition]		
ID	1	2	3
User Name	*UserName1*	*UserName2*	*UserName3*
Password	*Password1*	*Password2*	*Disable*
Authentication	*MD5*	*SHA-1*	*Disable*
Encryption	*DES*	*Disable*	*Disable*
Privacy Mode	*authPriv*	*authNoPriv*	*noAuthNoPriv*
Privacy Key	*12345678*	*Disable*	*Disable*
Authority	*Read/Write*	*Read*	*Read*
Enable	■ *Enable*	■ *Enable*	■ *Enable*

Scenario Operation Procedure

In above diagram, the NMS server can manage multiple devices in the Intranet or a UDP-reachable network. The "Gateway 1" is one of the managed devices, and it has the IP address of 10.0.75.2 for

Modbus Cellular Gateway

LAN interface and 118.18.81.33 for WAN-1 interface. It serves as a NAT router.

At first stage, the NMS manager prepares related information for all managed devices and records them in the NMS system. Then NMS system gets the status of all managed devices by using SNMP get commands.

When the manager wants to configure the managed devices, the NMS system allows him to do that by using SNMP set commands. The "UserName1" account is used if the manager uses SNMPv3 protocol for configuring the "Gateway 1". Only the "UserName1" account can let the "Gateway 1" accept the configuration from the NMS since the authority of the account is "Read/Write".

Once a managed device has an urgent event to send, the device will issue a trap to the Trap Event Receivers. The NMS itself could be one among them.

If you want to secure the transmitted SNMP commands and responses between the NMS and the managed devices, use SNMPv3 version of protocol.

The remote NMS without privilege IP address can't manage the "Gateway 1", since "Gateway 1" allows only the NMS with privilege IP address can manage it via its WAN interface.

Modbus Cellular Gateway

SNMP Setting

The SNMP allows user to configure SNMP relevant setting which includes interface, version, access control and trap receiver.

Go to **Administration > Configure & Manage > SNMP** tab.

Enable SNMP

SNMP Item	Value setting	Description
SNMP Enable	1.The boxes are unchecked by default	Select the interface for the SNMP and enable SNMP functions. When Check the **LAN** box, it will activate SNMP functions and you can access SNMP from LAN side; When Check the **WAN** box, it will activate SNMP functions and you can access SNMP from WAN side.
Supported Versions	1.The **v1** box is checked by default 2.The **v2c** box is checked by default	Select the version for the SNMP When Check the **v1** box. It means you can access SNMP by version 1. When Check the **v2c** box. It means you can access SNMP by version 2c. When Check the **v3** box. It means you can access SNMP by version 3.
Remote Aceess IP	1. String format: any Ipv4 address 2. It is an optional item.	Specify the **Remote Access IP** for WAN. If you filled in a certain IP address. It means only this IP address can access SNMP from WAN side. If you left it as blank, it means any IP address can access SNMP from WAN side.
SNMP Port	1. String format: any port number 2. The default SNMP port is **161**. 3. A Must filled setting	Specify the **SNMP Port**. You can fill in any port number. But you must ensure the port number is not to be used. *Value Range*: 1 ~ 65535.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Modbus Cellular Gateway

Create/Edit Multiple Community

The SNMP allows you to custom your access control for version 1 and version 2 user. The router supports up to a maximum of 10 community sets.

When **Add** button is applied, **Multiple Community Rule Configuration** screen will appear.

Multiple Community Rule Configuration		
Item	**Value setting**	**Description**
Community	1. Read Only is selected by default 2. A Must filled setting 3. String format: any text	Specify this version 1 or version v2c user's community that will be allowed Read Only (GET and GETNEXT) or Read-Write (GET, GETNEXT and SET) access respectively. The maximum length of the community is 32.
Enable	1.The box is checked by default	Click Enable to enable this version 1 or version v2c user.
Save	N/A	Click the **Save** button to save the configuration. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show "Click on save button to apply your changes" remind user to click main page Save button.
Undo	N/A	Click the **Undo** button to cancel the settings.
Back	N/A	Click the **Back** button to return to last page.

Modbus Cellular Gateway

Create/Edit User Privacy

The SNMP allows you to custom your access control for version 3 user. The router supports up to a maximum of 128 User Privacy sets.

ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	OID Filter Prefix	Enable	Actions

When **Add** button is applied, **User Privacy Rule Configuration** screen will appear.

Item	Setting
▶ User Name	
▶ Password	
▶ Authentication	None ▼
▶ Encryption	None ▼
▶ Privacy Mode	noAuthNoPriv ▼
▶ Privacy Key	
▶ Authority	Read ▼
▶ OID Filter Prefix	1
▶ Enable	☑ Enable

User Privacy Rule Configuration		
Item	**Value setting**	**Description**
User Name	1. A Must filled setting 2. String format: any text	Specify the **User Name** for this version 3 user. ***Value Range***: 1 ~ 32 characters.
Password	1. String format: any text	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Password** for this version 3 user. ***Value Range***: 8 ~ 64 characters.
Authentication	1. **None** is selected by default	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Authentication** types for this version 3 user. Selected the authentication types **MD5/ SHA-1** to use.
Encryption	1. **None** is selected by default	When your **Privacy Mode** is **authPriv**, you must specify the **Encryption** protocols for this version 3 user. Selected the encryption protocols **DES / AES** to use.
Privacy Mode	1. **noAuthNoPriv** is	Specify the **Privacy Mode** for this version 3 user.

Modbus Cellular Gateway

	selected by default	Selected the **noAuthNoPriv**. You do not use any authentication types and encryption protocols. Selected the **authNoPriv**. You must specify the **Authentication** and **Password**. Selected the **authPriv**. You must specify the Authentication, Password, Encryption and Privacy Key.
Privacy Key	1. String format: any text	When your **Privacy Mode** is **authPriv**, you must specify the **Privacy Key** (8 ~ 64 characters) for this version 3 user.
Authority	1. **Read** is selected by default	Specify this version 3 user's **Authority** that will be allowed **Read Only** (GET and GETNEXT) or **Read-Write** (GET, GETNEXT and SET) access respectively.
OID Filter Prefix	1. The default value is 1 2. A Must filled setting 3. String format: any legal OID	The **OID Filter Prefix** restricts access for this version 3 user to the sub-tree rooted at the given OID. **_Value Range_**: 1 ~2080768.
Enable	1.The box is checked by default	Click **Enable** to enable this version 3 user.
Save	N/A	Click the **Save** button to save the configuration. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show "Click on save button to apply your changes" remind user to click main page **Save** button.
Undo	N/A	Click the **Undo** button to cancel the settings
Back	N/A	Click the **Back** button to return the last page.

Create/Edit Trap Event Receiver

The SNMP allows you to custom your trap event receiver. The router supports up to a maximum of 4 Trap Event Receiver sets.

When **Add** button is applied, **Trap Event Receiver Rule Configuration** screen will appear. The default SNMP Version is v1. The configuration screen will provide the version 1 must filled items.

Modbus Cellular Gateway

When you selected v2c, the configuration screen is exactly the same as that of v1, except the version.

When you selected v3, the configuration screen will provide more setting items for the version 3 Trap.

Trap Event Receiver Rule Configuration		
Item	**Value setting**	**Description**
Server IP	1. A Must filled setting 2. String format: any Ipv4 address	Specify the trap **Server IP**. The DUT will send trap to the server IP.
Server Port	1. String format: any port number 2. The default SNMP trap port is 162 3. A Must filled setting	Specify the trap **Server Port**. You can fill in any port number. But you must ensure the port number is not to be used. *Value Range*: 1 ~ 65535.
SNMP Version	1. **v1** is selected by	Select the version for the trap

Modbus Cellular Gateway

	default	Selected the **v1**. The configuration screen will provide the version 1 must filled items. Selected the **v2c**. The configuration screen will provide the version 2c must filled items. Selected the **v3**. The configuration screen will provide the version 3 must filled items.
Community Name	1. A **v1** and **v2c** Must filled setting 2. String format: any text	Specify the **Community Name** for this version 1 or version v2c trap. ***Value Range***: 1 ~ 32 characters.
User Name	1. A **v3** Must filled setting 2. String format: any text	Specify the **User Name** for this version 3 trap. ***Value Range***: 1 ~ 32 characters.
Password	1. A **v3** Must filled setting 2. String format: any text	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Password** for this version 3 trap. ***Value Range***: 8 ~ 64 characters.
Privacy Mode	1. A **v3** Must filled setting 2. **noAuthNoPriv** is selected by default	Specify the **Privacy Mode** for this version 3 trap. Selected the **noAuthNoPriv**. You do not use any authentication types and encryption protocols. Selected the **authNoPriv**. You must specify the **Authentication** and **Password**. Selected the **authPriv**. You must specify the Authentication, Password, Encryption and Privacy Key.
Authentication	1. A **v3** Must filled setting 2. **None** is selected by default	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Authentication** types for this version 3 trap. Selected the authentication types **MD5/ SHA-1** to use.
Encryption	1. A **v3** Must filled setting 2. **None** is selected by default	When your **Privacy Mode** is **authPriv**, you must specify the **Encryption** protocols for this version 3 trap. Selected the encryption protocols **DES / AES** to use.
Privacy Key	1. A **v3** Must filled setting 2. String format: any text	When your **Privacy Mode** is **authPriv**, you must specify the **Privacy Key** (8 ~ 64 characters) for this version 3 trap.
Enable	1.The box is checked by default	Click **Enable** to enable this trap receiver.
Save	N/A	Click the **Save** button to save the configuration. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show "Click on save button to apply your changes" remind user to click main page **Save** button.
Undo	N/A	Click the **Undo** button to cancel the settings.
Back	N/A	Click the **Back** button to return the last page.

Modbus Cellular Gateway

Edit SNMP Options

If you use some particular private MIB, you must fill the enterprise name, number and OID.

Options	
Item	**Setting**
▶ Enterprise Name	AMIT
▶ Enterprise Number	12823
▶ Enterprise OID	1.3.6.1.4.1. 12823.4.4.9

Options		
Item	**Value setting**	**Description**
Enterprise Name	1. The default value is AMIT 2. A Must filled setting 3. String format: any text	Specify the **Enterprise Name** for the particular private MIB. ***Value Range***: 1 ~ 10 characters, and only string with A~Z, a~z, 0~9, '–', '_'.
Enterprise Number	The default value is 12823 (AMIT Enterprise Number) 2. A Must filled setting 3. String format: any number	Specify the **Enterprise Number** for the particular private MIB. ***Value Range***: 1 ~2080768.
Enterprise OID	1. The default value is 1.3.6.1.4.1.12823.4.4.9 (AMIT Enterprise OID) 2. A Must filled setting 3. String format: any legal OID	Specify the **Enterprise OID** for the particular private MIB. The range of the each OID number is 1-2080768. The maximum length of the enterprise OID is 31. The seventh number must be identical with the enterprise number.
Save	N/A	Click the **Save** button to save the configuration and apply your changes to SNMP functions.
Undo	N/A	Click the **Undo** button to cancel the settings.

Modbus Cellular Gateway

6.1.4 Telnet with CLI

A command-line interface (CLI), also known as command-line user interface, and console user interface are means of interacting with a computer program where the user (or client) issues commands to the program in the form of successive lines of text (command lines). The interface is usually implemented with a command line shell, which is a program that accepts commands as text input and converts commands to appropriate operating system functions. Programs with command-line interfaces are generally easier to automate via scripting. The device supports both Telnet and SSH (Secure Shell) CLI with default service port 23 and 22, respectively.

Telnet & SSH Scenario
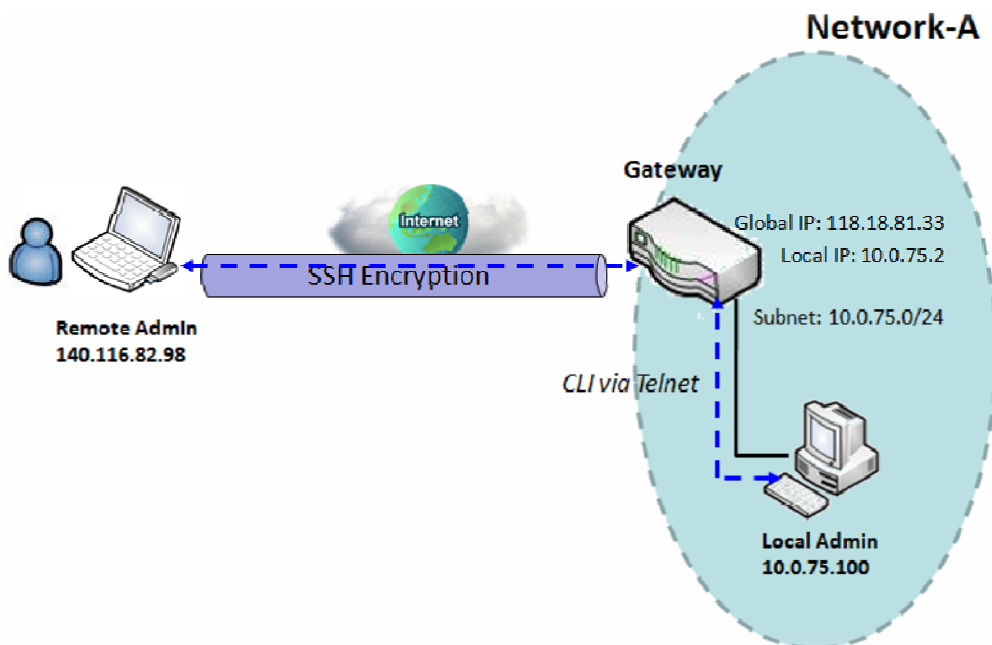
Scenario Application Timing

When the administrator of the gateway wants to manage it from remote site in the Intranet or Internet, he may use "Telnet with CLI" function to do that by using "Telnet" or "SSH" utility.

Scenario Description

The Local Admin or the Remote Admin can manage the Gateway by using "Telnet" or "SSH" utility with privileged user name and password.

The data packets between the Local Admin and the Gateway or between the Remote Admin and the Gateway can be plain texts or encrypted texts. Suggest they are plain texts in the Intranet for Local Admin to use "Telnet" utility, and encrypted texts in the Internet for Remote Admin to use "SSH" utility.

Modbus Cellular Gateway

Parameter Setup Example

Following table lists the parameter configuration as an example for the Gateway in above diagram with "Telnet with CLI" enabling at LAN and WAN interfaces.

Use default value for those parameters that are not mentioned in the table.

Configuration Path	[Telnet with CLI]-[Configuration]
Telnet with CLI	LAN: ■ *Enable* WAN: ■ *Enable*
Connection Type	Telnet: Service Port *23* ■ *Enable* SSH: Service Port *22* ■ *Enable*

Scenario Operation Procedure

In above diagram, "Local Admin" or "Remote Admin" can manage the "Gateway" in the Intranet or Internet. The "Gateway" is the gateway of Network-A, and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. It serves as a NAT gateway.

The "Local Admin" in the Intranet uses "Telnet" utility with privileged account to login the Gateway.

Or the "Remote Admin" in the Internet uses "SSH" utility with privileged account to login the Gateway.

The administrator of the gateway can control the device as like he is in front of the gateway.

Modbus Cellular Gateway

Telnet with CLI Setting

Go to Administration > Configure & Manage > Telnet with CLI tab.

The Telnet with CLI setting allows administrator to access this device through the traditional Telnet program. Before you can telnet (login) to the device, please configure the related settings and password with care. The password management part allows you to set root password for logging telnet and SSH.

Configuration Item	Value setting	Description
Telnet with CLI	1. The LAN Enable box is checked by default. 2. The WAN Enable box is unchecked by default.	Check the **Enable** box to activate the Telnet with CLI function for connecting from WAN/LAN interfaces.
Connection Type	1. The Telnet Enable box is checked by default. By default **Service Port** is 23. 2. The SSH Enable box is unchecked by default. By default **Service Port** is 22.	Check the Telnet **Enable** box to activate telnet service. Check the SSH **Enable** box to activate SSH service. You can set which number of **Service Port** you want to provide for the corresponding service. *Value Range*: 1 ~65535.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Modbus Cellular Gateway

Configuration Item	Value setting	Description
root	1. String: any text but no blank character 2. The default password for telnet is 'm2mamit'.	Type old password and specify new password to change root password. ***Note: You are highly recommended to change the default telnet password with yours before the device is deployed.***
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

6.2 System Operation

System Operation allows the network administrator to manage system, settings such as web-based utility access password change, system information, system time, system log, firmware/configuration backup & restore, and reset & reboot.

6.2.1 Password & MMI

Go to **Administration > System Operation > Password & MMI** tab.

Change Password

Change password screen allows network administrator to change the web-based MMI login password to access gateway.

Password	[Help]
Item	**Setting**
▸ Old Password	
▸ New Password	
▸ New Password Confirmation	

Change Password		
Item	**Value Setting**	**Description**
Old Password	1. String: any text **2. The default password for web-based MMI is 'admin'.**	Enter the current password to enable you unlock to change password.
New Password	String: any text	Enter new password
New Password Confirmation	String: any text	Enter new password again to confirm
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

Change MMI Setting for Accessing

This is the gateway's web-based MMI access which allows administrator to access the gateway for management. The gateway's web-based MMI will automatically logout when the idle time has elapsed. The

Modbus Cellular Gateway

setting allows administrator to enable automatic logout and set the logout idle time. When the login timeout is disabled, the system won't logout the administrator automatically.

Web UI		
Item	Value Setting	Description
Login	3 times is set by default	Enter the login trial counting value. *Value Range*: 3 ~ 10. If someone tried to login the web GUI with incorrect password for more than the counting value, an warning message "***Already reaching maximum Password-Guessing times, please wait a few seconds!***" will be displayed and ignore the following login trials.
Login Timeout	The Enable box is unchecked by default	Check the Enable box to activate the auto logout function, and specify the maximum idle time as well. *Value Range*: 30 ~ 65535.
GUI Access Protocol	http/https is selected by default.	Select the protocol that will be used for GUI access. It can be **http/https**, **http only**, or **https only**.
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

Modbus Cellular Gateway

6.2.2 System Information

System Information screen gives network administrator a quick look up on the type of WAN connection being used. The display also shows the current System time. It is particularly useful when firmware has been upgraded and system configuration file has been loaded.

Go to **Administration > System Operation > System Information** tab.

System Name	
Item	**Setting**
▶ System Name	AMIT

System Name		
Item	**Value Setting**	**Description**
System Name	1. an optional item 2. AMIT is set by default.	Enter the system name for identification purpose. It can be the manufacture, or any name for a device deployment.

System Information	
Item	**Setting**
▶ WAN Type	3G/4G
▶ Display Time	Fri, 01 Jan 2010 02:51:22 +0000
▶ Host Name	Cellular_Gateway

System Information		
Item	**Value Setting**	**Description**
WAN Type	N/A	It displays the WAN Type of WAN-1 Interface Internet connection configured.
Display Time	N/A	It displays the current system time that you browsed this web page.
Host Name	1. It is an optional item 2. **Cellular_Gayeway** is set by default.	Enter the host name for the gateway. It can be used to interact with external network servers for identifying the name of requesting device.
Save	N/A	Click the **Save** button to save the settings.
Refresh	N/A	Click the **Refresh** button to update the system Information immediately.

Modbus Cellular Gateway

6.2.3 System Time

The gateway provides manually setup and auto-synchronized approaches for the administrator to setup the system time for the gateway.

Go to **Administration > System Operation > System Time** tab.

System Time Information		
Item	**Value Setting**	**Description**
Time Zone	1. It is an optional item. 2. **GMT+00 :00** is selected by default.	Select a time zone where this device locates.
Auto-synchronization	1. Checked by default. 2. Auto is selected by default.	Check the **Enable** button to activate the time auto-synchronization function with a certain NTP server. You can enter the IP or FQDN for the NTP server you expected, or leave it as auto mode so that the available server will be used for time synchronization one by one.
Daylight Saving Time	1. It is an optional item. 2. Un-checked by default	Check the **Enable** button to activate the daylight saving function. When you enabled this function, you have to specify the start date and end date for the daylight saving time duration.
Set Date & Time	1. It is an optional item.	If you do not enable the time auto-synchronization function, you can also manually set the date (Year/Month/Day) and time (Hour:Minute:Second).
Save	N/A	Click the **Save** button to save the settings.
Refresh	N/A	Click the **Refresh** button to update the system time immediately.

Instead of manually configuring the system time for the gateway, there are two simple and quick solutions for you to set the correct time information and set it as the system time for the gateway.

Modbus Cellular Gateway

The first one is "Sync with Timer Server". Based on your selection of time zone and time server in above time information configuration window, system will communicate with time server by NTP Protocol to get system date and time after you click on the **Sync with Timer Server** button.

Note: Remember to select a correct time zone for the device, otherwise, you will just get the UTC (Coordinated Universal Time) time, not the local time for the device.

The second one is "Sync with my PC". Click on the **Sync with my PC** button to let system synchronize its date and time to the time of the administration PC.

Modbus Cellular Gateway

6.2.4 System Log

System Log screen contains various event log tools facilitating network administrator to perform local event logging and remote reporting.

Go to **Administration > System Operation > System Log** tab.

View & Email Log History

View button is provided for network administrator to view log history on the gateway. **Email Now** button enables administrator to send instant Email for analysis.

View & Email Log History		
Item	**Value setting**	**Description**
View button	N/A	Click the **View** button to view Log History in Web Log List Window.
Email Now	N/A	Click the **Email Now** button to send Log History via Email instantly.

Modbus Cellular Gateway

button

Web Log List Window

Item	Value Setting	Description
Time column	N/A	It displays event time stamps
Log column	N/A	It displays Log messages

Web Log List Button Description

Item	Value setting	Description
Previous	N/A	Click the **Previous** button to move to the previous page.
Next	N/A	Click the **Next** button to move to the next page.
First	N/A	Click the **First** button to jump to the first page.
Last	N/A	Click the **Last** button to jump to the last page.
Download	N/A	Click the **Download** button to download log to your PC in tar file format.
Clear	N/A	Click the **Clear** button to clear all log.
Back	N/A	Click the **Back** button to return to the previous page.

Web Log Type Category

Web Log Type Category screen allows network administrator to select the type of events to log and be displayed in the Web Log List Window as described in the previous section. Click on the View button to view Log History in the Web Log List window.

248

Modbus Cellular Gateway

Web Log Type Category Setting Window		
Item	**Value Setting**	**Description**
System	Checked by default	Check to log system events and to display in the Web Log List window.
Attacks	Checked by default	Check to log attack events and to display in the Web Log List window.
Drop	Checked by default	Check to log packet drop events and to display in the Web Log List window.
Login message	Checked by default	Check to log system login events and to display in the Web Log List window.
Debug	Un-checked by default	Check to log debug events and to display in the Web Log List window.

Email Alert

Email Alert screen allows network administrator to select the type of event to log and be sent to the destined Email account.

Email Alert Setting Window		
Item	**Value Setting**	**Description**
Enable	Un-checked by default	Check **Enable** box to enable sending event log messages to destined Email account defined in the E-mail Addresses blank space.
Server	N/A	Select one email server from the Server dropdown box to send Email. If none has been available, click the **Add Object** button to create an outgoing Email server. You may also add an outgoing Email server from Object Definition > External Server > External Server tab.
E-mail address	String : email format	Enter the recipient's Email address. Separate Email addresses with comma ',' or semicolon ' ;' Enter the Email address in the format of '*myemail@domain.com*'
Subject	String : any text	Enter an Email subject that is easy for you to identify on the Email client.
Log type category	Default unchecked	Select the type of events to log and be sent to the designated Email account. Available events are System, Attacks, Drop, Login message, and Debug.

Modbus Cellular Gateway

Syslogd

Syslogd screen allows network administrator to select the type of event to log and be sent to the designated Syslog server.

Syslogd Setting Window		
Item	**Value Setting**	**Description**
Enable	Un-checked by default	Check Enable box to activate the Syslogd function, and send event logs to a syslog server
Server	N/A	Select one syslog server from the Server dropdown box to sent event log to. If none has been available, click the **Add Object** button to create a system log server. You may also add an system log server from the Object Definition > External Server > External Server tab.
Log type category	Un-checked by default	Select the type of event to log and be sent to the destined syslog server. Available events are System, Attacks, Drop, Login message, and Debug.

Log to Storage

Log to Storage screen allows network administrator to select the type of events to log and be stored at an internal or an external storage.

Log to Storage Setting Window		
Item	**Value Setting**	**Description**
Enable	Un-checked by default	Check to enable sending log to storage.
Select Device	Internal is selected by default	Select internal or external storage.
Log file name	Un-checked by default	Enter log file name to save logs in designated storage.
Split file Enable	Un-checked by default	Check **enable** box to split file whenever log file reaching the specified limit.
Split file Size	**200 KB** is set by default	Enter the file size limit for each split log file. ***Value Range***: 10 ~1000.
Log type category	Un-checked by default	Check which type of logs to send: System, Attacks, Drop, Login message, Debug

Log to Storage Button Description		
Item	**Value setting**	**Description**
Download log file	N/A	Click the **Download log file** button to download log files to a log.tar file.

Modbus Cellular Gateway

6.2.5 Backup & Restore

In the Backup & Restore window, you can upgrade the device firmware when new firmware is available and also backup / restore the device configuration.

In addition to the factory default settings, you can also customize a special configuration setting as a customized default value. With this customized default value, you can reset the device to the expected default setting if needed.

Go to **Administration > System Operation > Backup & Restore** tab.

FW Backup & Restore		
Item	**Value Setting**	**Description**
FW Upgrade	Via Web UI is selected by default	If new firmware is available, click the **FW Upgrade** button to upgrade the device firmware **via Web UI**, or **Via Storage**. After clicking on the "FW Upgrade" command button, you need to specify the file name of new firmware by using "Browse" button, and then click "Upgrade" button to start the FW upgrading process on this device. If you want to upgrade a firmware which is from GPL policy, please check "Accept unofficial firmware"
Backup Configuration Settings	Download is selected by default	You can backup or restore the device configuration settings by clicking the *Via Web UI* button. **Download**: for backup the device configuration to a config.bin file. **Upload**: for restore a designated configuration file to the device. **Via Web UI**: to retrieve the configuration file via Web GUI.
Auto Restore Configuration	The Enable box is unchecked by default	Chick the **Enable** button to activate the customized default setting function. Once the function is activated, you can save the expected setting as a customized default setting by clicking the **Save Conf.** button, or clicking the **Clean Conf.** button to erase the stored customized configuration.

Modbus Cellular Gateway

6.2.6 Reboot & Reset

For some special reason or situation, you may need to reboot the gateway or reset the device configuration to its default value. In addition to perform these operations through the Power ON/OFF, or pressing the reset button on the device panel, you can do it through the web GUI too.

Go to **Administration > System Operation > Reboot & Reset** tab.

In the Reboot & Reset window, you can reboot this device by clicking the "Reboot" button, and reset this device to default settings by clicking the "Reset" button.

System Operation	
Item	**Setting**
▶ Reboot	Now ▼ Reboot
▶ Reset to Default	Reset

System Operation Window		
Item	**Value Setting**	**Description**
Reboot	Now is selected by default	Chick the **Reboot** button to reboot the gateway immediately or on a pre-defined time schedule. **Now**: Reboot immediately **Time Schedule**: Select a pre-defined auto-reboot time schedule rule to reboot the auto device on a designated tim. To define a time schedule rule, go to **Object Definition > Scheduling > Configuration** tab.
Reset to Default	N/A	Click the **Reset** button to reset the device configuration to its default value.

6.3 FTP

The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files between a client and server on a computer network. FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it.

For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). Besides, SSH File Transfer Protocol (SFTP) is sometimes also used instead, but is technologically different.

This gateway embedded FTP / SFTP server for administrator to download the log files to his computer or database. In the following two sections, you can configure the FTP server and create the user accounts that can login to the server. After login to the FTP server, you can browse the log directory and have the permission to download the stored log files and delete the files you have downloaded to make more storage space for further data logs.

The available log files can be system logs (refer to Administration > System Operation > System Log), Network Packets (refer to Administrator > Diagnostic > Packet Analyzer), Data Log (refer to Field Communication > Data Logging > Log File Management), and GNSS Log (refer to Service > Location Tracking > GNSS). With proper configuration for the various log functions that supported on your purchased product, you can download the log via FTP / SFTP connections.
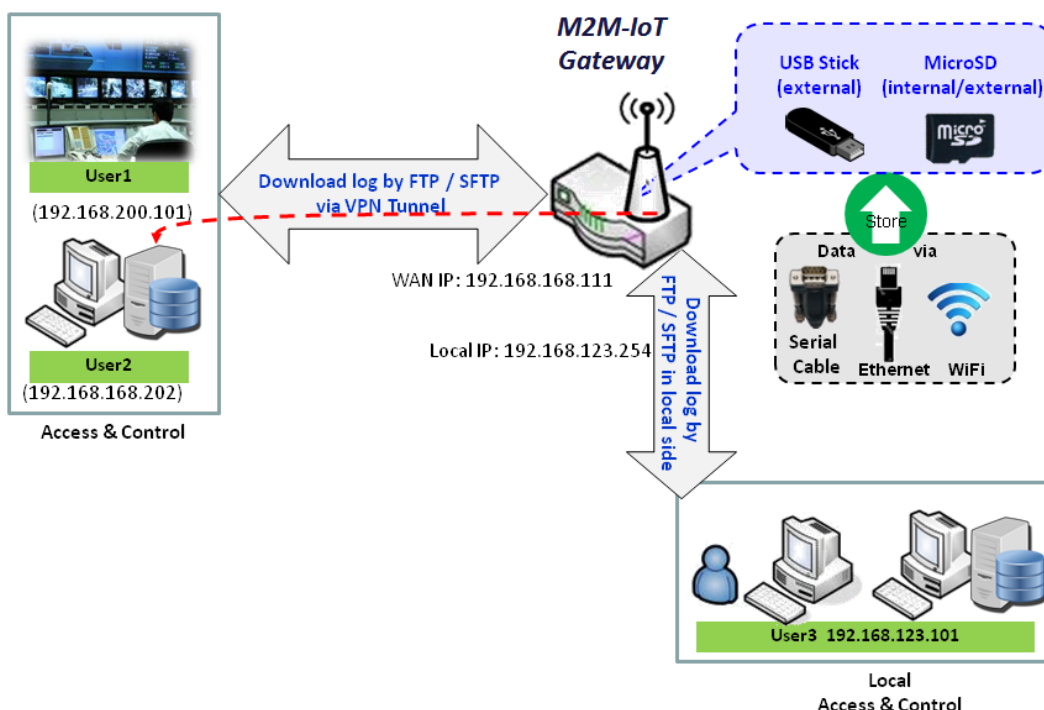
Modbus Cellular Gateway

6.3.1 Server Configuration

This section allows user to setup the embedded FTP and SFTP server for retrieving the interested fog files.

Go to Administration > FTP > Server Configuration tab.

Enable FTP Server

Item	Setting
FTP Server Configuration	Save
▶ FTP	☐ Enable
▶ FTP Port	21
▶ Timeout	300 secend(s)(60-7200)
▶ Max. Connections per IP	2 ▼
▶ Max. FTP Clients	5 ▼
▶ PASV Mode	☐ Enable
▶ Port Range of PASV Mode	50000 ~ 50031
▶ Auto Report External IP in PASV Mode	☐ Enable
▶ ASCII Transfer Mode	☐ Enable
▶ FTPS(FTP over SSL/TLS)	☐ Enable

Configuration Item	Value setting	Description
FTP	The box is unchecked by default.	Check **Enable** box to activate the embedded FTP Server function. With the FTP Server enabled, you can retrieve or delete the stored log files via FTP connection. Note: The embedded FTP Server is only for log downloading, so no any write permission is implemented for user file upload to the storage.
FTP Port	Port **21** is set by default	Specify a port number for FTP connection. The gateway will listen for incoming FTP connections on the specified port. ***Value Range*: 1 ~ 65535.**
Timeout	**300** seconds is set by default.	Specify the maximum timeout interval for the FTP connection. Supported range is 60 to 7200 seconds.
Max. Connections per IP	**2** Clients are set by default.	Specify the maximum number of clients from the same IP address for the FTP connection. Up to 5 clients from the same IP address is supported.
Max. FTP Clients	**5** Clients are set by	Specify the maximum number of clients for the FTP connection. Up to 32 clients

	default.	is supported.
PASV Mode	Optional setting	Check the **Enable** box to activate the support of PASV mode for a FTP connection from FTP clients.
Port Range of PASV Mode	Port **50000** ~ **50031** is set by default.	Specify the port range to allocate for PASV style data connection. ***Value Range***: 1024 ~ 65535.
Auto Report External IP in PASV Mode	Optional setting	Check the **Enable** box to activate the support of overriding the IP address advertising in response to the PASV command.
ASCII Transfer Mode	Optional setting	Check the **Enable** box to activate the support of ASCII mode data transfers. Binary mode is supported by default.
FTPS (FTP over SSL/TLS)	Optional setting	Check the **Enable** box to activate the support of secure connections via SSL/TLS.

Enable SFTP Server

Configuration Item	Value setting	Description
SFTP	The box is unchecked by default.	Check **Enable** box to activate the embedded SFTP Server function. With the SFTP Server enabled, you can retrieve or delete the stored log files via secure SFTP connection.
SFTP Port	Default 22	Specify a port number for SFTP connection. The gateway will listen for incoming SFTP connections on the specified port. ***Value Range***: 1 ~ 65535.

Modbus Cellular Gateway

6.3.2 User Account

This section allows user to setup user accounts for logging to the embedded FTP and SFTP server to retrieve the interested fog files.

Go to Administration > FTP > User Account tab.

Create/Edit FTP User Accounts

ID	User Name	Password	Directory	Permission	Enable	Actions

When **Add** button is applied, **User Account Configuration screen** will appear.

Item	Setting
▸ User Name	
▸ Password	
▸ Directory	Browse
▸ Permission	Read/Write ▾
▸ Enable	☑

Configuration Item	Value setting	Description
User Name	String : non-blank string	Enter the user account for login to the FTP server. **Value Range:** 1 ~ 15 characters.
Password	String : no blank	Enter the user password for login to the FTP server.
Directory	N/A	Select a root directory after user login.
Permission	**Read/Write** is selected by default.	Select the Read/write permission. Note: The embedded FTP Server is only for log downloading, so no any write permission is implemented for user file upload to the storage, even **Read/Write** option is selected.
Enable	The box is checked by default.	Check the box to activate the FTP user account.

6.4 Diagnostic

This gateway supports simple network diagnosis tools for the administrator to troubleshoot and find the root cause of the abnormal behavior or traffics passing through the gateway. There can be a Packet Analyzer to help record the packets for a designated interface or specific source/destination host, and another Ping and Tracert tools for testing the network connectivity issues.

6.4.1 Diagnostic Tools

The Diagnostic Tools provide some frequently used network connectivity diagnostic tools (approaches) for the network administrator to check the device connectivity.

Go to **Administration > Diagnostic > Diagnostic Tools** tab.

Diagnostic Tools		
Item	**Value setting**	**Description**
Ping Test	Optional Setting	This allows you to specify an IP / FQDN and the test interface, so system will try to ping the specified device to test whether it is alive after clicking on the **Ping** button. A test result window will appear beneath it.
Tracert Test	Optional setting	Trace route (tracert) command is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Trace route proceeds until all (three) sent packets are lost for more than twice, then the connection is lost and the route cannot be evaluated. First, you need to specify an IP / FQDN, the test interface and the protocol (UDP or ICMP), and by default, it is **UDP**. Then, system will try to trace the specified host to test whether it is alive after clicking on **Tracert** button. A test result window will appear beneath it.
Wake on LAN	Optional setting	Wake on LAN (WOL) is an Ethernet networking standard that allows a computer to be turned on or awakened by a network message. You can specify the MAC address of the computer, in your LAN network, to be remotely turned on by clicking on the **Wake up** command button.
Save	N/A	Click the **Save** button to save the configuration.

6.4.2 Packet Analyzer

The Packet Analyzer can capture packets depend on user settings. User can specify interfaces to capture packets and filter by setting rule. Ensure the log storage is available (either embedded SD-Card or external USB Storage), otherwise **Packet Analyzer** cannot be enabled.

Go to **Administration > Diagnostic > Packet Analyzer** tab.

Configuration

Item	Value setting	Description
Packet Analyzer	The box is unchecked by default.	Check **Enable** box to activate the Packet Analyzer function. If you cannot enable the checkbox, please check if the storage is available or not. Plug in the USB storage and then enable the Package Analyzer function.
File Name	1. An optional setting 2. Blank is set by default, and the default file name is **<Interface>_<Date>_<index>.**	Enter the file name to save the captured packets in log storage. If **Split Files** option is also enabled, the file name will be appended with an index code "**_<index>**". The extension file name is **.pcap**.
Split Files	1. An optional setting 2. The default value of **File Size** is 200 KB.	Check **enable** box to split file whenever log file reaching the specified limit. If the **Split Files** option is enabled, you can further specify the **File Size** and **Unit** for the split files. *Value Range*: 10 ~ 99999. NOTE: **File Size** cannot be less than 10 KB
Packet Interfaces	An optional setting	Define the interface(s) that **Packet Analyzer** should work on. At least, one interface is required, but multiple selections are also accepted. The supported interfaces can be: ● **WAN**: When the WAN is enabled at **Physical Interface**, it can be selected here. ● **ASY**: This means the serial communication interface. It is used to capture packets appearing in the **Field Communication**. Therefore, it can only be selected when specific field communication protocol, like Modbus, is enabled.

Modbus Cellular Gateway

		● **VAP**: This means the virtual AP. When WiFi and VAP are enabled, it can be selected here.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.

Once you enabled the Packet Analyzer function on specific Interface(s), you can further specify some filter rules to capture the packets which matched the rules.

Capture Filters

Item	Setting
▶ Filter	☐ Enable
▶ Source MACs	
▶ Source IPs	
▶ Source Ports	
▶ Destination MACs	
▶ Destination IPs	
▶ Destination Ports	

Capture Fitters		
Item	**Value setting**	**Description**
Filter	Optional setting	Check **Enable** box to activate the Capture Filter function.
Source MACs	Optional setting	Define the filter rule with **Source MACs**, which means the source MAC address of packets. Packets which match the rule will be captured. Up to 10 MACs are supported, but they must be separated with "**;**", e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when match any one MAC in the rule.

Modbus Cellular Gateway

Source IPs	Optional setting	Define the filter rule with **Source IPs**, which means the source IP address of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with "**;**", e.g. 192.168.1.1; 192.168.1.2 The packets will be captured when match any one IP in the rule.
Source Ports	Optional setting	Define the filter rule with **Source Ports**, which means the source port of packets. The packets will be captured when match any port in the rule. Up to 10 ports are supported, but they must be separated with "**;**", e.g. 80; 53 ***Value Range***: 1 ~ 65535.
Destination MACs	Optional setting	Define the filter rule with **Destination MACs**, which means the destination MAC address of packets. Packets which match the rule will be captured. Up to 10 MACs are supported, but they must be separated with "**;**", e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when match any one MAC in the rule.
Destination IPs	Optional setting	Define the filter rule with **Destination IPs**, which means the destination IP address of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with "**;**", e.g. 192.168.1.1; 192.168.1.2 The packets will be captured when match any one IP in the rule.
Destination Ports	Optional setting	Define the filter rule with **Destination Ports**, which means the destination port of packets. The packets will be captured when match any port in the rule. Up to 10 ports are supported, but they must be separated with "**;**", e.g. 80; 53 ***Value Range***: 1 ~ 65535.

Chapter 7 Service

7.1 Cellular Toolkit
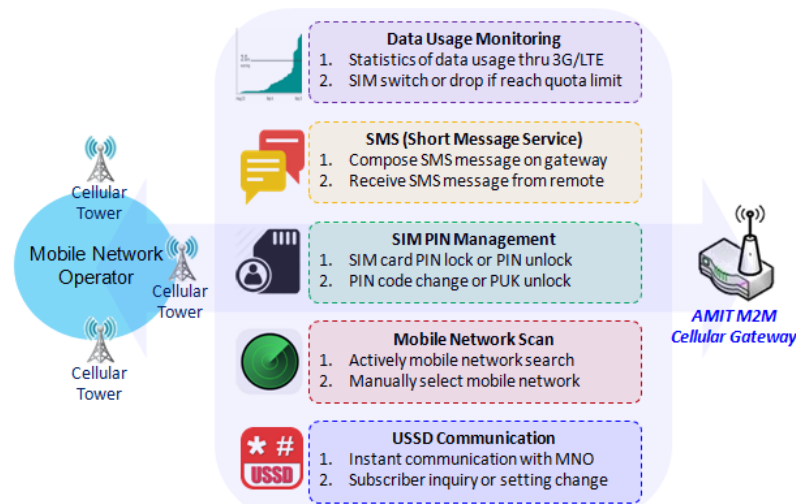
Besides cellular data connection, you may also like to monitor data usage of cellular WAN, sending text message through SMS, changing PIN code of SIM card, communicating with carrier/ISP by USSD command, or doing a cellular network scan for diagnostic purpose.

In Cellular Toolkit section, it includes several useful features that are related to cellular configuration or application. You can configure settings of Data Usage, SMS, SIM PIN, USSD, and Network Scan here. Please note at least a valid SIM card is required to be inserted to device before you continue settings in this section.
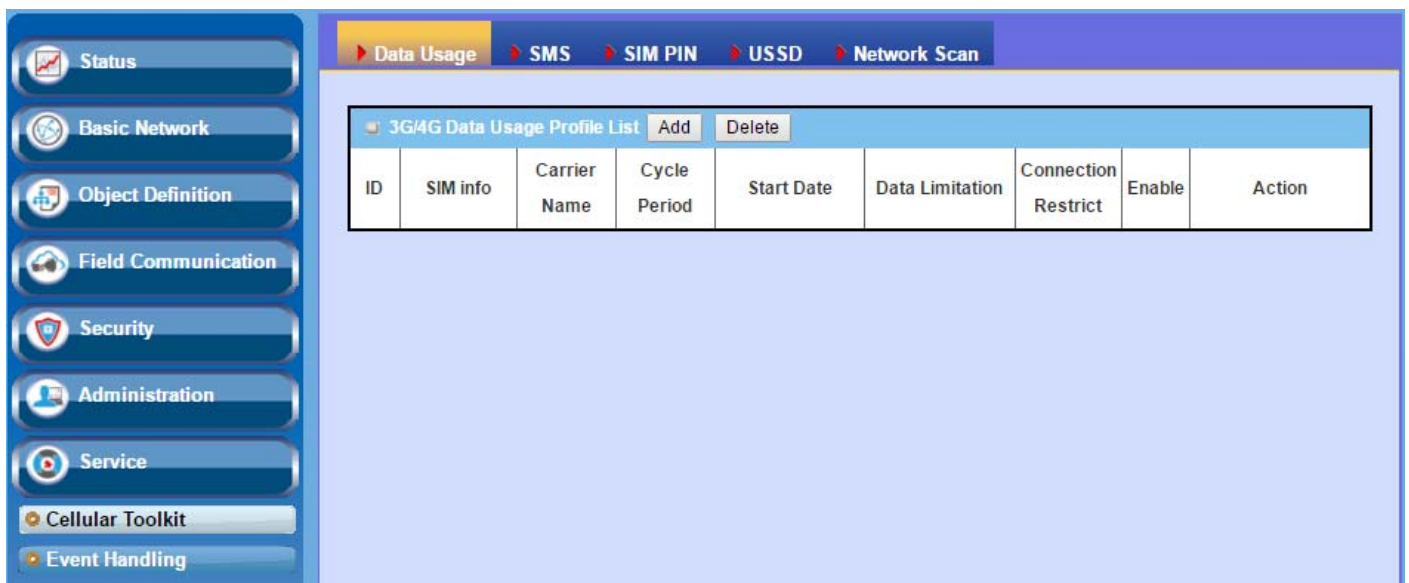
Modbus Cellular Gateway

7.1.1 Data Usage

Most of data plan for cellular connection is with a limited amount of data usage. If data usage has been over limited quota, either you will get much lower data throughput that may affect your daily operation, or you will get a 'bill shock' in the next month because carrier/ISP charges a lot for the over-quota data usage.

With help from Data Usage feature, device will monitor cellular data usage continuously and take actions. If data usage reaches limited quota, device can be set to drop the cellular data connection right away. Otherwise, if secondary SIM card is inserted, device will switch to secondary SIM and establish another cellular data connection with secondary SIM automatically.

If Data Usage feature is enabled, all history of cellular data usage can be viewed at **Status** > **Statistics & Reports** > **Cellular Usage** tab.

3G/4G Data Usage

SIM A Settings
-Cycle Period: monthly
-Start Date: 2017 / Feb / 20
-Data Limitation: 1Gb
-Connection Restrict: Enable
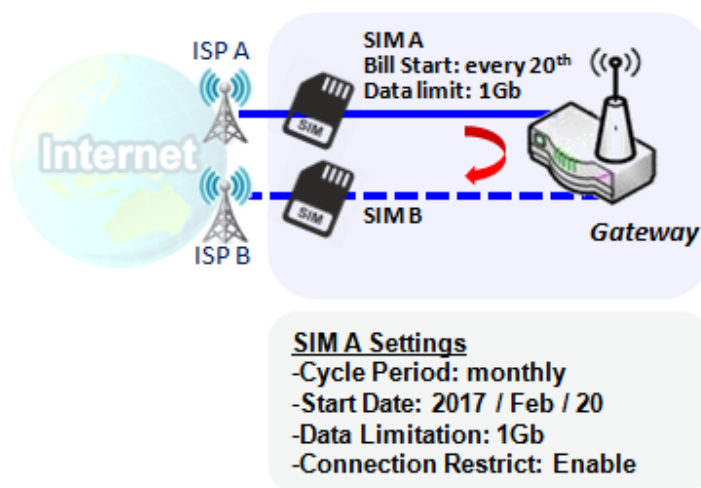
Data Usage feature enabling gateway device to continuously monitor cellular data usage and take actions. In the diagram, quota limit of SIM A is **1Gb** per month and bill start date is **20**th of every month. The device is smart to start a new calculation of data usage on every 20th of month. Enable Connection Restrict will force gateway device to drop cellular connection of SIM A when data usage reaches quota limit (1Gb in this case). If SIM failover feature is configured in **Internet Setup**, then gateway will switch to SIM B and establish a new cellular data connection automatically.

Modbus Cellular Gateway

Data Usage Setting

Go to **Service** > **Cellular Toolkit** > **Data Usage** tab.

Before finished settings for Data Usage, you need to know bill start date, bill period, and quota limit of data usage according to your data plan. You can ask this information from your carrier or ISP.

Create / Edit 3G/4G Data Usage Profile

When **Add** button is applied, 3G/4G Data Usage Profile Configuration screen will appear. You can create up to four data usage profiles, one profile for each SIM card used in the Gateway.

3G/4G Data Usage Profile Configuration		
Item Setting	**Value setting**	**Description**
SIM Select	3G/4G-1 and SIM A by default.	Choose a cellular interface (**3G/4G-**1 or **3G/4G-2**), and a SIM card bound to the selected cellular interface to configure its data usage profile.
Carrier Name	It is an optional item.	Fill in the Carrier Name for the selected SIM card for identification.
Cycle Period	Days by default	The first box has three types for cycle period. They are **Days**, **Weekly** and **Monthly**. **Days**: For per Days cycle periods, you have to further specify the number of days in the second box. *Value Range*: 1 ~ 90 days. **Weekly**, **Monthly**: The cycle period is one week or one month.
Start Date	N/A	Specify the date to start measure network traffic. Please don't select the day before now, otherwise, the traffic statistics will be

		incorrect.
Data Limitation	N/A	Specify the allowable data limitation for the defined cycle period.
Connection Restrict	Un-Checked by default.	Check the **Enable** box to activate the connection restriction function. During the specified cycle period, if the actual data usage exceeds the allowable data limitation, the cellular connection will be forced to disconnect.
Enable	Un-Checked by default.	Check the **Enable** box to activate the data usage profile.

Modbus Cellular Gateway

7.1.2 SMS

Short Message Service (SMS) is a text messaging service, which is used to be widely-used on mobile phones. It uses standardized communications protocols to allow mobile phones or cellular devices to exchange short text messages in an instant and convenient way.

SMS Setting

Go to **Service** > **Cellular Toolkit** > **SMS** tab

With this gateway device, you can send SMS text messages or browse received SMS messages as you usually do on a cellular phone.

Setup SMS Configuration

Configuration		
Item		**Setting**
▸ Physical Interface		3G/4G-1 ▾
▸ SMS		☑ Enable SIM Status: SIM_A
▸ SMS Storage		SIM Card Only ▾

Configuration Item	Value setting	Description
Physical Interface	The box is 3G/4G-1 by default	Choose a cellular interface (**3G/4G-1** or **3G/4G-2**) for the following SMS function configuration.
SMS	The box is checked by default	This is the SMS switch. If the box checked that the SMS function enable, if the box unchecked that the SMS function disable.
SIM Status	N/A	Depend on currently SIM status. The possible value will be **SIM_A** or **SIM_B**.
SMS Storage	The box is SIM Card Only by default	This is the SMS storage location. Currently the option only **SIM Card Only.**
Save	N/A	Click the **Save** button to save the settings

Modbus Cellular Gateway

SMS Summary

Show **Unread SMS**, **Received SMS**, **Remaining SMS**, and edit SMS context to send, read SMS from SIM card.

Item	Setting
▶ Unread SMS	1
▶ Received SMS	7
▶ Remaining SMS	12

SMS Summary — New SMS — SMS Inbox

SMS Summary		
Item	**Value setting**	**Description**
Unread SMS	N/A	If SIM card insert to router first time, unread SMS value is zero. When received the new SMS but didn't read, this value plus one.
Received SMS	N/A	This value record the existing SMS numbers from SIM card, When received the new SMS, this value plus one.
Remaining SMS	N/A	This value is SMS capacity minus received SMS, When received the new SMS, this value minus one.
New SMS	N/A	Click **New SMS** button, a **New SMS** screen appears. User can set the SMS setting from this screen. Refer to New SMS in the next page.
SMS Inbox	N/A	Click **SMS Inbox** button, a **SMS Inbox List** screen appears. User can read or delete SMS, reply SMS or forward SMS from this screen. Refer to SMS Inbox List in the next page.
Refresh	N/A	Click the **Refresh** button to update the SMS summary immediately.

New SMS
You can set the SMS setting from this screen.

Item	Setting
▶ Receivers	(Use '+' for International Format and ';' to Compose Multiple Receivers)
▶ Text Message	Length of Current Input : 0
▶ Result	

New SMS — Send

Modbus Cellular Gateway

New SMS		
Item	**Value setting**	**Description**
Receivers	N/A	Write the receivers to send SMS. User need to add the semicolon and compose multiple receivers that can group send SMS.
Text Message	N/A	Write the SMS context to send SMS. The router supports up to a maximum of 1023 character for SMS context length.
Send	N/A	Click the **Send** button, above text message will be sent as a SMS.
Result	N/A	If SMS has been sent successfully, it will show **Send OK**, otherwise **Send Failed** will be displayed.

SMS Inbox List

You can read or delete SMS, reply SMS or forward SMS from this screen.

SMS Inbox List		
Item	**Value setting**	**Description**
ID	N/A	The number or SMS.
From Phone Number	N/A	What the phone number from SMS
Timestamp	N/A	What time receive SMS
SMS Text Preview	N/A	Preview the SMS text. Click the **Detail** button to read a certain message.
Action	The box is unchecked by default	Click the **Detail** button to read the SMS detail; Click the **Reply / Forward** button to reply/forward SMS. Besides, you can check the box(es), and then click the **Delete** button to delete the checked SMS(s).
Refresh	N/A	Refresh the SMS Inbox List.
Delete	N/A	Delete the SMS for all checked box from Action.
Close	N/A	Close the Detail SMS Message screen.

Modbus Cellular Gateway

7.1.3 SIM PIN

With most cases in the world, users need to insert a SIM card (a.k.a. UICC) into end devices to get on cellular network for voice service or data surfing. The SIM card is usually released by mobile operators or service providers. Each SIM card has a unique number (so-called ICCID) for network owners or service providers to identify each subscriber. As SIM card plays an important role between service providers and subscribers, some security mechanisms are required on SIM card to prevent any unauthorized access.

Enabling a PIN code in SIM card is an easy and effective way of protecting cellular devices from unauthorized access. This gateway device allows you to activate and manage PIN code on a SIM card through its web GUI.

Activate PIN code on SIM Card
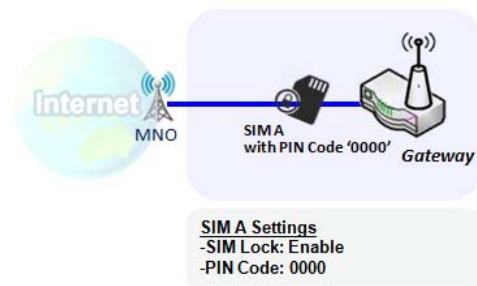
This gateway device allows you to activate PIN code on SIM card. This example shows how to activate PIN code on SIM-A for 3G/4G-1 with default PIN code "**0000**".

Change PIN code on SIM Card
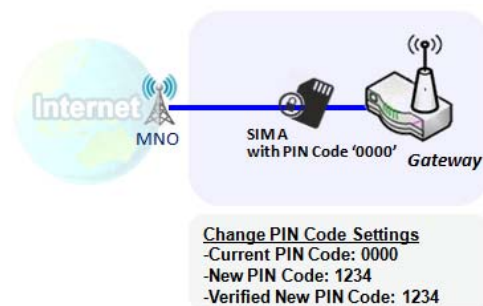
This gateway device allows you to change PIN code on SIM card. Following the example above, you need to type original PIN code "**0000**", and then type new PIN code with '**1234**' if you like to set new PIN code as '**1234**'. To confirm the new PIN code you type is what you want, you need to type new PIN code '**1234**' in Verified New PIN Code again.

Unlock SIM card by PUK Code
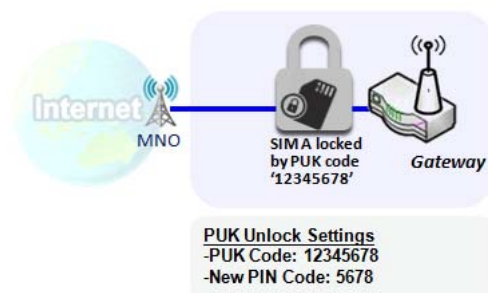
If you entered incorrect PIN code at configuration page for 3G/4G-1 WAN over three times, and then it will cause SIM card to be locked by PUK code. Then you have to call service number to get a PUK code to unlock SIM card. In the diagram, the PUK code is "**12345678**" and new PIN code is "**5678**".

Modbus Cellular Gateway

SIM PIN Setting

Go to **Service** > **Cellular Toolkit** > **SIM PIN** Tab

With the SIM PIN Function window, it allows you to enable or disable SIM lock (which means protected by PIN code), or change PIN code. You can also see the information of remaining times of failure trials as we mentioned earlier. If you run out of these failure trials, you need to get a PUK code to unlock SIM card.

Select a SIM Card

Configuration	
Item	**Setting**
▶ Physical Interface	3G/4G-1 ▼
▶ SIM Status	SIM-A Ready
▶ SIM Selection	SIM-A ▼ Switch

Configuration Window		
Item	**Value setting**	**Description**
Physical Interface	The box is 3G/4G-1 by default	Choose a cellular interface (**3G/4G**-1 or **3G/4G-2**) to change the SIM PIN setting for the selected SIM Card. The number of physical modems depends on the gateway model you purchased.
SIM Status	N/A	Indication for the selected SIM card and the SIM card status. The status could be **Ready**, **Not Insert**, or **SIM PIN**. **Ready** -- SIM card is inserted and ready to use. It can be a SIM card without PIN protection or that SIM card is already unlocked by correct PIN code. **Not Insert** -- No SIM card is inserted in that SIM slot. **SIM PIN** -- SIM card is protected by PIN code, and it's not unlocked by a correct PIN code yet. That SIM card is still at locked status.
SIM Selection	N/A	Select the SIM card for further SIM PIN configuration. Press the **Switch** button, then the Gateway will switch SIM card to another one. After that, you can configure the SIM card.

Modbus Cellular Gateway

Enable / Change PIN Code

Enable or Disable PIN code (password) function, and even change PIN code function.

SIM function Window		
Item Setting	**Value setting**	**Description**
SIM lock	Depend on SIM card	Click the **Enable** button to activate the SIM lock function. For the first time you want to enable the SIM lock function, you have to fill in the PIN code as well, and then click **Save** button to apply the setting.
Remaining times	Depend on SIM card	Represent the remaining trial times for the SIM PIN unlocking.
Save	N/A	Click the **Save** button to apply the setting.
Change PIN Code	N/A	Click the **Change PIN code** button to change the PIN code (password). If the **SIM Lock** function is not enabled, the **Change PIN code** button is disabled. In the case, if you still want to change the PIN code, you have to enable the SIM Lock function first, fill in the PIN code, and then click the **Save** button to enable. After that, You can click the **Change PIN code** button to change the PIN code.

When **Change PIN Code** button is clicked, the following screen will appear.

Item	Value Setting	Description
Current PIN Code	A Must filled setting	Fill in the current (old) PIN code of the SIM card.
New PIN Code	A Must filled setting	Fill in the new PIN Code you want to change.
Verified New PIN Code	A Must filled setting	Confirm the new PIN Code again.
Apply	N/A	Click the **Apply** button to change the PIN code with specified new PIN code.
Cancel	N/A	Click the **Cancel** button to cancel the changes and keep current PIN code.

Modbus Cellular Gateway

Note: If you changed the PIN code for a certain SIM card, you must also change the corresponding PIN code specified in the **Basic Network** > **WAN & Uplink** > **Internet Setup** > **Connection with SIM Card** page. Otherwise, it may result in wrong SIM PIN trials with invalid (old) PIN code.

Unlock with a PUK Code

The PUK Function window is only available for configuration if that SIM card is locked by PUK code. It means that SIM card is locked and needs additional PUK code to unlock. Usually it happens after too many trials of incorrect PIN code, and the remaining times in SIM Function table turns to 0. In this situation, you need to contact your service provider and request a PUK code for your SIM card, and try to unlock the locked SIM card with the provided PUK code. After unlocking a SIM card by PUK code successfully, the SIM lock function will be activated automatically.

Item	Setting
▸ PUK status	PUK unlock.
▸ Remaining times	N/A
▸ PUK Code	[ ] (8 digits)
▸ New PIN Code	[ ] (4~8 digits)

PUK function — Save

PUK Function Window		
Item	**Value setting**	**Description**
PUK status	**PUK Unlock / PUK Lock**	Indication for the PUK status. The status could be **PUK Lock** or **PUK Unlock**. As mentioned earlier, the SIM card will be locked by PUK code after too many trials of failure PIN code. In this case, the PUK Status will turns to **PUK Lock**. In a normal situation, it will display **PUK Unlock**.
Remaining times	Depend on SIM card	Represent the remaining trial times for the PUK unlocking. Note : **DO NOT make the remaining times down to zero, it will damage the SIM card FOREVER !** Call for your ISP's help to get a correct PUK and unlock the SIM if you don't have the PUK code.
PUK Code	A Must filled setting	Fill in the PUK code (8 digits) that can unlock the SIM card in PUK unlock status.
New PIN Code	A Must filled setting	Fill in the New PIN Code (4~8 digits) for the SIM card. You have to determine your new PIN code to replace the old, forgotten one. Keep the PIN code (password) in mind with care.
Save	N/A	Click the **Save** button to apply the setting.

Note: If you changed the PUK code and PIN code for a certain SIM card, you must also change the corresponding PIN code specified in the **Basic Network** > **WAN & Uplink** > **Internet Setup** > **Connection with SIM Card** page. Otherwise, it may result in wrong SIM PIN trials with invalid (old) PIN code.

Modbus Cellular Gateway

7.1.4 USSD

Unstructured Supplementary Service Data (USSD) is a protocol used by GSM cellular telephones to communicate with the service provider's computers. USSD can be used for WAP browsing, prepaid callback service, mobile-money services, location-based content services, menu-based information services, and as part of configuring the phone on the network.

An USSD message is up to 182 alphanumeric characters in length. Unlike Short Message Service (SMS) messages, USSD messages create a real-time connection during an USSD session. The connection remains open, allowing a two-way exchange of a sequence of data. This makes USSD more responsive than services that use SMS.

Configuration	
Item	**Setting**
▸ Physical Interface	3G/4G-1 ⌄ SIM Status: SIM_A

USSD Profile List Add Delete				
ID	**Profile Name**	**USSD Command**	**Comments**	**Actions**
1	roaming setting	*135#	Roaming function	Edit ☐ Select

USSD Profile Configuration Save	
Item	**Setting**
▸ Profile Name	roaming setting
▸ USSD Command	*135#
▸ Comments	Roaming function

USSD Request Send Clear	
Item	**Setting**
▸ USSD Profile	roaming setting ⌄
▸ USSD Command	*135#
▸ USSD Response	< ChungHwa Data Roaming Services> 1 Order 2 Query 3 Setting 4 使用中文

USSD Scenario
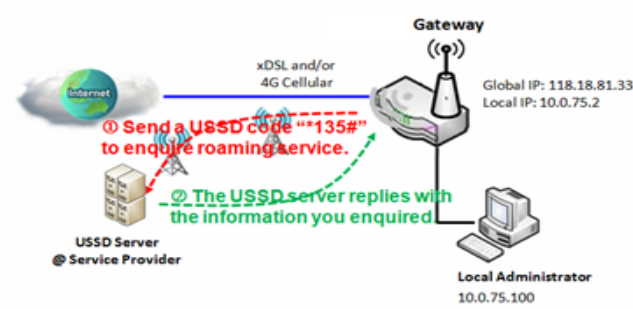
USSD allows you to have an instant bi-directional communication with carrier/ISP. In the diagram, the USSD command '***135#**' is referred to data roaming services. After sending that USSD command to carrier, you can get a response at window USSD Response. Please note the USSD command varies for different carriers/ISP.

272

Modbus Cellular Gateway

USSD Setting

Go to **Service** > **Cellular Toolkit** > **USSD** tab.

In "USSD" page, there are four windows for the USSD function. The "Configuration" window can let you specify which 3G/4G module (physical interface) is used for the USSD function, and system will show which SIM card in the module is the current used one. The second window is the "USSD Profile List" and it shows all your defined USSD profiles that store pre-commands for activating an USSD session. An "Add" button in the window can let you add one new USSD profile and define the command for the profile in the third window, the "USSD Profile Configuration". When you want to start the activation of an USSD connection session to the USSD server, select the USSD profile or type in the correct pre-command, and then click on the "Send" button for the session. The responses from the USSD server will be displayed beneath the "USSD Command" line. When commands typed in the "USSD Command" field are sent, received responses will be displayed in the "USSD Response" blank space. User can communicate with the USSD server by sending USSD commands and getting USSD responses via the gateway.

USSD Configuration

Configuration	
Item	Setting
▸ Physical Interface	3G/4G-1 ▾ SIM Status: SIM_A

Configuration Item	Value setting	Description
Physical Interface	The box is **3G/4G-1** by default.	Choose a cellular interface (**3G/4G**-1 or **3G/4G**-2) to configure the USSD setting for the connected cellular service (identified with **SIM_A** or **SIM_B**).
SIM Status	N/A	Show the connected cellular service (identified with **SIM_A** or **SIM_B**).

Create / Edit USSD Profile

The cellular gateway allows you to custom your USSD profile. It supports up to a maximum of 35 USSD profiles.

USSD Profile List Add Delete				
ID	Profile Name	USSD Command	Comments	Actions

When **Add** button is applied, **USSD Profile Configuration** screen will appear.

Modbus Cellular Gateway

USSD Profile Configuration	Save
Item	**Setting**
▶ Profile Name	[ ]
▶ USSD Command	[ ]
▶ Comments	[ ]

USSD Profile Configuration		
Item	**Value setting**	**Description**
Profile Name	N/A	Enter a name for the USSD profile.
USSD Command	N/A	Enter the USSD command defined for the profile. Normally, it is a command string composed with numeric keypad "0~9", "*", and "#". The USSD commands are highly related to the cellular service, please check with your service provider for the details.
Comments	N/A	Enter a brief comment for the profile.

Send USSD Request

When **send** the USSD command, the USSD Response screen will appear.
When click the **Clear** button, the USSD Response will disappear.

USSD Request	Send	Clear
Item	**Setting**	
▶ USSD Profile	--- Option --- ▼	
▶ USSD Command	[ ]	

USSD Request		
Item	**Value setting**	**Description**
USSD Profile	N/A	Select a USSD profile name from the dropdown list.
USSD Command	N/A	The USSD Command string of the selected profile will be shown here.
USSD Response	N/A	Click the **Send** button to send the USSD command, and the **USSD Response** screen will appear. You will see the response message of the corresponding service, receive the service SMS.

Modbus Cellular Gateway

7.1.5 Network Scan

"Network Scan" function can let administrator specify the device how to connect to the mobile system for data communication in each 3G/4G interface. For example, administrator can specify which generation of mobile system is used for connection, 2G, 3G or LTE. Moreover, he can define their connection sequence for the gateway device to connect to the mobile system automatically. Administrator also can scan the mobile systems in the air manually, select the target operator system and apply it. The manual scanning approach is used for problem diagnosis.

Network Scan Setting

Go to **Service** > **Cellular Toolkit** > **Network Scan** tab.

In "Network Scan" page, there are two windows for the Network Scan function. The "Configuration" window can let you select which 3G/4G module (physical interface) is used to perform Network Scan, and system will show the current used SIM card in the module. You can configure each 3G/4G WAN interface by executing the network scanning one after another. You can also specify the connection sequence of the targeted generation of mobile system, 2G/3G/LTE.

Network Scan Configuration

Configuration		
Item		**Setting**
▶ Physical Interface	3G/4G-1 ▾	SIM Status: SIM_A
▶ Network Type	Auto ▾	
▶ Scan Approach	Auto ▾	

Configuration Item	Value setting	Description
Physical Interface	The box is **3G/4G-1** by default	Choose a cellular interface (**3G/4G**-1 or **3G/4G**-2) for the network scan function.
SIM Status	N/A	Show the connected cellular service (identified with **SIM_A** or **SIM_B**).
Network Type	**Auto** is selected by default.	Specify the network type for the network scan function. It can be Auto, 2G Only, 2G prefer, 3G Only, 3G prefer, or 4G Only. When **Auto** is selected, the network will be register automatically; If the **prefer** option is selected, network will be register for your option first; If the **only** option is selected, network will be register for your option only.
Scan Approach	Auto is selected by default.	When **Auto** selected, cellular module register automatically. If the **Manually** option is selected, a **Network Provider List** screen appears. Press **Scan** button to scan for the nearest base stations. Select (check the box)

Modbus Cellular Gateway

		the preferred base stations then click **Apply** button to apply settings.
Save	N/A	Click **Save** to save the settings

The second window is the "Network Provider List" window and it appears when the **Manually** Scan Approach is selected in the Configuration window. By clicking on the "Scan" button and wait for 1 to 3 minutes, the found mobile operator system will be displayed for you to choose. Click again on the "Apply" button to drive system to connect to that mobile operator system for the dedicated 3G/4G interface.

Network Provider List	Scan	Apply			
Provider Name	**Mobile System**	**Network Status**	**Action**
Chunghwa Telecom	4G	Current	☐ Select
Far EasTone	3G	Forbidden	☐ Select

Modbus Cellular Gateway

7.2 Event Handling

Event handling is the application that allows administrator to setup the pre-defined events, handlers, or response behavior with individual profiles. With properly configuring the event handling function, administrator can easily and remotely obtain the status and information via the purchased gateway. Moreover, he can also handle and manage some important system related functions, even the field bus devices and D/O devices which are already well connected to.

The supported events are categorized into two groups: the **managing events** and **notifying events**.

The **managing events** are the events that are used to manage the gateway or change the setting / status of the specific functionality of the gateway. On receiving the managing event, the gateway will take action to change the functionality, collect the required status for administration, and also change the status of a certain connected field bus device simultaneously.

The **notifying events** are the events that some related objects have been triggered and take corresponding actions on the occurrence of the events. It could be an event generated from the connected sensor, or a certain connected field bus device for alerting the administrator something happened with SMS message, Email, and SNMP Trap, etc...
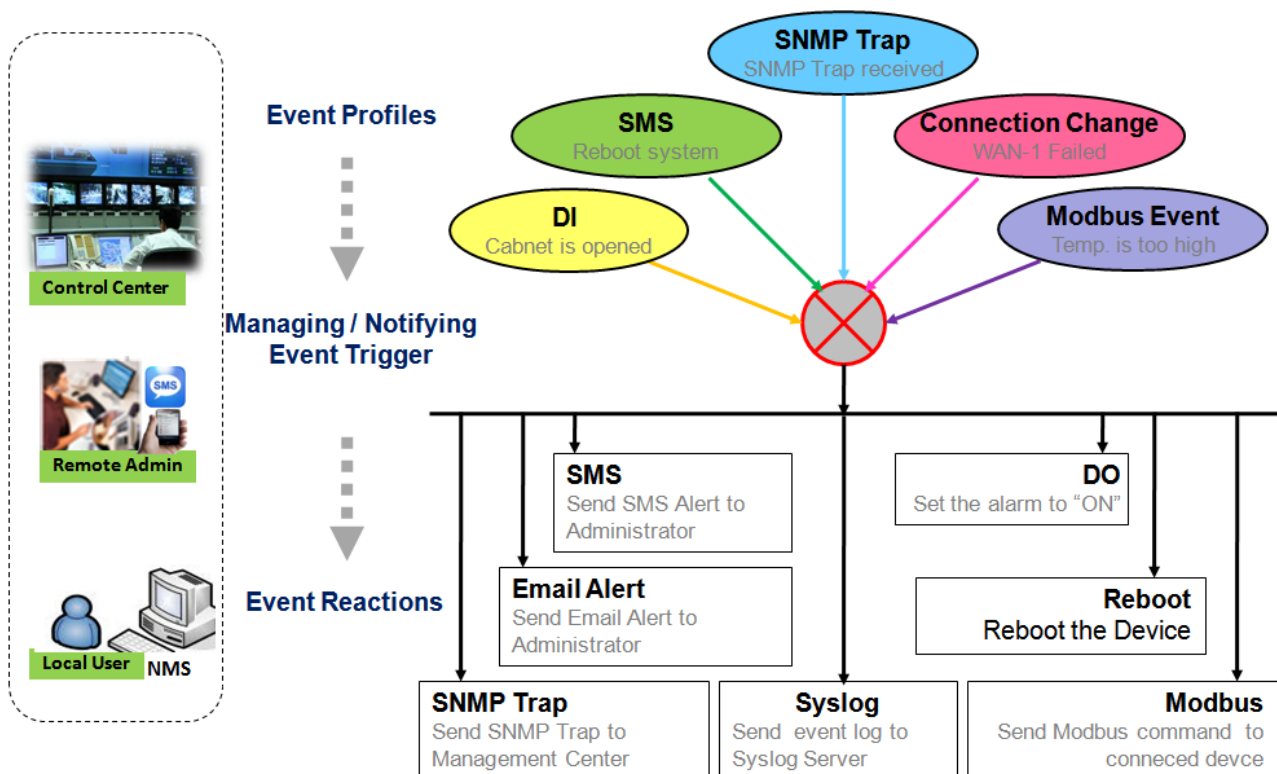
For ease of configuration, administrator can create and edit the common pre-defined managing / notifying event profiles for taking instant reaction on a certain event or managing the devices for some advanced useful purposes. For example, sending/receiving remote managing SMS for the gateway's routine maintaining, the

Modbus Cellular Gateway

field bus device status monitoring, digital sensors detection controlling, and so on. All of such management and notification function can be realized effectively via the Event Handling feature.

The following is the summary lists for the provided profiles, and events:

(**Note**: The available profiles and events could be different for the purchased product.)

- Profiles (Rules):
  - SMS Configuration and Accounts
  - Email Accounts
  - Digital Input (DI) profiles
  - Digital Output (DO) profiles
  - Modbus Managing Event profiles
  - Modbus Notifying Event profiles

- Managing Events:
  - Trigger Type: SMS, SNMP Trap, and Digital Input (DI).
  - Actions: Get the Network Status; or Configure the LAN/VLAN behavior, WIFI behavior, NAT behavior, Firewall behavior, VPN behavior, System Management, Administration, Digital Output behavior, and connected Modbus devices.

- Notifying Events:
  - Trigger Type: Digital Input, Power Change, Connection Change (WAN, LAN & VLAN, WiFi, DDNS), Administration, Modbus, and Data Usage.
  - Actions: Notify the administrator with SMS, Syslog, SNMP Trap or Email Alert; Change the status of connected Digital Output or Modbus devices.

To use the event handling function, First of all, you have to enable the event management setting and configure the event details with the provided profile settings. You can create or edit pre-defined profiles for individual managing / notifying events. The profile settings are separated into several items; they are the SMS Account Definition, Email Service Definition, Digital Input (DI) Profile Configuration, Digital Output (DO) Profile Configuration, and Modbus Definition.

Then, you have to configure each managing / notifying event with identifying the event's trigger condition, and the corresponding actions (reaction for the event) for the event. For each event, more than one action can be activated simultaneously.

Modbus Cellular Gateway

7.2.1 Configuration

Go to **Service** > **Event Handling** > **Configuration** Tab.

Event handling is the service that allows administrator to setup the pre-defined events, handlers, or response behavior with individual profiles.

Enable Event Management

Configuration	
Item	**Setting**
▸ Event Management	☐ Enable

Configuration		
Item	**Value setting**	**Description**
Event Management	The box is unchecked by default	Check the **Enable** box to activate the Event Management function.

Enable SMS Management

To use the SMS management function, you have to configure some important settings first.

SMS Configuration	
Item	**Setting**
▸ Message Prefix	☐ Enable & [_____]
▸ Physical Interface	3G/4G-1 ▾ SIM Status: SIM_A
▸ Delete Managed SMS after Processing	☐ Enable

SMS Configuration		
Item	**Value setting**	**Description**
Message Prefix	The box is unchecked by default	Click the **Enable** box to enable the SMS prefix for validating the received SMS. Once the function is enabled, you have to enter the prefix behind the checkbox. The received managing events SMS must have the designated prefix as an initial identifier, then corresponding handlers will become effective for further processing.

Modbus Cellular Gateway

Physical Interface	The box is 3G/4G-1 by default.	Choose a cellular interface (**3G/4G**-1 or **3G/4G-2**) to configure the SMS management setting.
SIM Status	N/A	Show the connected cellular service (identified with **SIM_A** or **SIM_B**).
Delete Managed SMS after Processing	The box is unchecked by default	Check the **Enable** box to delete the received managing event SMS after it has been processed.

Create / Edit SMS Account

Setup the SMS Account for managing the gateway through the SMS. It supports up to a maximum of 5 accounts.

You can click the **Add / Edit** button to configure the SMS account.

SMS Account Configuration		
Item	**Value setting**	**Description**
Phone Number	1. Mobile phone number format 2. A Must filled setting	Specify a mobile phone number as the SMS account identifier. ***Value Range***: -1 ~ 32 digits.
Phone Description	1. Any text 2. An Optional setting	Specify a brief description for the SMS account.
Application	A Must filled setting	Specify the application type. It could be **Event Trigger, Notify Handle,** or **both**.
Enable	The box is unchecked by default.	Click **Enable** box to activate this account.
Save	NA	Click the **Save** button to save the configuration.

Modbus Cellular Gateway

Create / Edit Email Service Account

Setup the Email Service Account for event notification. It supports up to a maximum of 5 accounts.

ID	Email Server	Email Addresses	Enable	Actions

Email Service List **Add** **Delete**

You can click the **Add / Edit** button to configure the Email account.

Email Service Configuration

Item	Setting
▶ Email Server	--- Option --- ▼
▶ Email Addresses	
▶ Enable	☑ Enable
	Save

Email Service Configuration		
Item	**Value setting**	**Description**
Email Server	--- Option ---	Select an Email Server profile from **External Server** setting for the email account setting.
Email Addresses	1. Internet E-mail address format 2. A Must filled setting	Specify the Destination Email Addresses.
Enable	The box is unchecked by default.	Click **Enable** box to activate this account.
Save	*NA*	Click the **Save** button to save the configuration

Modbus Cellular Gateway

Create / Edit Digital Input (DI) Profile Rule (DI/DO support required)

Setup the Digital Input (DI) Profile rules. It supports up to a maximum of 10 profiles.

☐ **Digital Input (DI) Profile List** [Add] [Delete]							
ID	DI Profile Name	Description	DI Source	Normal Level	Signal Active Time (s)	Enable	Actions

When **Add** button is applied, the **Digital Input (DI) Profile Configuration** screen will appear.

☐ **Digital Input (DI) Profile Configuration**	
Item	**Setting**
▶ DI Profile Name	[ ]
▶ Description	[ ]
▶ DI Source	[ID1 ▼]
▶ Normal Level	[Low ▼]
▶ Signal Active Time	[1] (seconds)
▶ Profile	☑ Enable
	[Save]

Digital Input (DI) Profile Configuration		
Item	**Value setting**	**Description**
DI Profile Name	1. String format 2. A Must filled setting	Specify the DI Profile Name. ***Value Range*: -1 ~ 32 characters.**
Description	1. Any text 2. An Optional setting	Specify a brief description for the profile.
DI Source	**ID1** by default	Specify the DI Source. It could be **ID1** or **ID2**. The number of available DI source could be different for the purchased product.
Normal Level	Low by default	Specify the Normal Level. It could be **Low** or **High**.
Signal Active Time	1. Numberic String format 2. A Must filled setting	Specify the Signal Active Time. It could be from 1 to 10 seconds. ***Value Range*: 1 ~ 10 seconds.**
Profile	The box is unchecked by default.	Click **Enable** box to activate this profile setting.
Save	*NA*	Click the **Save** button to save the configuration.

Modbus Cellular Gateway

Create / Edit Digital Output (DO) Profile Rule (DI/DO support required)

Setup the Digital Output (DO) Profile rules. It supports up to a maximum of 10 profiles.

ID	DO Profile Name	Description	DO Source	Normal Level	Total Signal Period (ms)	Repeat & Counter	Duty Cycle(%)	Enable	Actions

When **Add** button is applied, the **Digital Output (DO) Profile Configuration** screen will appear.

Digital Output (DO) Profile Configuration

Item	Setting
▶ DO Profile Name	
▶ Description	
▶ DO Source	ID1 ▾
▶ Normal Level	Low ▾
▶ Total Signal Period	10 (ms)
▶ Repeat & Counter	☐ Enable & Counter: 0
▶ Duty Cycle	(%)
▶ Profile	☑ Enable
	Save

Digital Output (DO) Profile Configuration		
Item	**Value setting**	**Description**
DO Profile Name	1. String format 2. A Must filled setting	Specify the DO Profile Name. ***Value Range***: -1 ~ 32 characters.
Description	1. Any text 2. An Optional setting	Specify a brief description for the profile.
DO Source	**ID1** by default	Specify the DO Source. It could be **ID1**.
Normal Level	Low by default	Specify the Normal Level. It could be **Low** or **High**.
Total Signal Period	1. Numberic String format 2. A Must filled setting	Specify the Total Signal Period. ***Value Range***: 10 ~ 10000 ms.
Repeat & Counter	The box is unchecked by default.	Check the Enable box to activate the repeated Digital Output, and specify the Repeat times. ***Value Range***: 0 ~ 65535.
Duty Cycle	1. Numberic String format 2. A Must filled setting	Specify the Duty Cycle for the Digital Output. ***Value Range***: 1 ~100 %.
Profile	The box is unchecked by default.	Click **Enable** box to activate this profile setting.
Save	N/A	Click the **Save** button to save the configuration.

Modbus Cellular Gateway

Create / Edit Modbus Notifying Events Profile (Modbus support required)

Setup the Modbus Notifying Events Profile. It supports up to a maximum of 10 profiles.

ID	Modbus Name	Description	Read Function	Modbus Mode	IP	Port	Device ID	Register	Logic Comparator	Value	Enable	Actions
1	co2_level	read co2 level to check if it bigger than 60	Read Holding Registers (0x03)	TCP	122.22.33.44	987	78	3	>	60	☑	Edit ☐ Select

You can click the **Add / Edit** button to configure the profile.

Modbus Notifying Events Profile Configuration

Item	Setting
▶ Modbus Name	[ ]
▶ Description	[ ]
▶ Read Function	Read Coils (0x01) ▼
▶ Modbus Mode	Serial ▼
▶ IP	[ ]
▶ Port	[ ]
▶ Device ID	[ ]
▶ Register	[ ]
▶ Logic Comparator	> ▼
▶ Value	0
▶ Enable	☑ Enable
	Save

Modbus Notifying Events Profile		
Item	**Value setting**	**Description**
Modbus Name	1. String format 2. A Must filled setting	Specify the Modbus profile name. ***Value Range*: -1 ~ 32 characters.**
Description	1. Any text 2. An Optional setting	Specify a brief description for the profile.
Read Function	Read Holding Registers by default	Specify the Read Function for **Notifying Events**.

Modbus Cellular Gateway

Modbus Mode	Serial by default	Specify the Modbus Mode. It could be Serial or TCP.
IP	1. NA for Serial on Modbus Mode. 2. A Must filled setting for TCP on Modbus Mode.	Specify the IP for TCP on Modbus Mode. IPv4 Format.
Port	1. NA for Serial on Modbus Mode. 2. A Must filled setting for TCP on Modbus Mode.	Specify the Port for TCP on Modbus Mode. ***Value Range*: 1 ~ 65535.**
Device ID	1. Numberic String format 2. A Must filled setting	Specify the Device ID of the modbus device. It could be from 1 to 247.
Register	1. Numberic String format 2. A Must filled setting	Specify the Register number of the modbus device. ***Value Range*: 0 ~ 65535.**
Logic Comparator	Logic Comparator '>' by default.	Specify the Logic Comparator for **Notifying Events**. It could be '>', '<', '=', '>=', or '<='.
Value	1. Numberic String format 2. A Must filled setting	Specify the Value. ***Value Range*: 0 ~ 65535.**
Enable	The box is unchecked by default.	Click **Enable** box to activate this profile setting.
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore what you just configured back to the previous setting.

Modbus Cellular Gateway

Create / Edit Modbus Managing Events Profile (Modbus support required)

Setup the Modbus Managing Events Profile. It supports up to a maximum of 10 profiles.

ID	Modbus Name	Description	Write Function	Modbus Mode	IP	Port	Device ID	Register	Value	Enable	Actions
1	water_pump	write water pump to control the motor speed high-low	Write Single Register (0x06)	TCP	233.44.55.66	876	247	44	5678	✔	Edit ☐ Select

You can click the **Add / Edit** button to configure the profile.

Item	Setting
▶ Modbus Name	
▶ Description	
▶ Write Function	Write Single Coil (0x05) ▼
▶ Modbus Mode	Serial ▼
▶ IP	
▶ Port	
▶ Device ID	
▶ Register	
▶ Value	0
▶ Enable	✔ Enable
	Save

Modbus Managing Events Profile		
Item	**Value setting**	**Description**
Modbus Name	1. String format 2. A Must filled setting	Specify the Modbus profile name. *Value Range*: -1 ~ 32 characters.
Description	1. Any text 2. An Optional setting	Specify a brief description for the profile.
Write Function	Write Single Registers by default	Specify the Write Function for **Managing Events**.
Modbus Mode	**Serial** by default	Specify the Modbus Mode. It could be **Serial or TCP**.
IP	1. NA for Serial on Modbus	Specify the IP for TCP on Modbus Mode. IPv4 Format.

	Mode. 2. A Must filled setting for TCP on Modbus Mode.	
Port	1. NA for Serial on Modbus Mode. 2. A Must filled setting for TCP on Modbus Mode.	Specify the Port for TCP on Modbus Mode. *Value Range*: 1 ~ 65535.
Device ID	1. Numberic String format 2. A Must filled setting	Specify the Device ID of the modbus device. *Value Range*: 1 ~ 247.
Register	1. Numberic String format 2. A Must filled setting	Specify the Register number of the modbus device. *Value Range*: 0 ~ 65535.
Value	1. Numberic String format 2. A Must filled setting	Specify the Value. *Value Range*: 0 ~ 65535.
Enable	The box is unchecked by default.	Click **Enable** box to activate this profile setting.
Save	*NA*	Click the **Save** button to save the configuration
Undo	*NA*	Click the **Undo** button to restore what you just configured back to the previous setting.

Modbus Cellular Gateway

7.2.2 Managing Events

Managing Events allow administrator to define the relationship (rule) among event trigger, handlers and response.

Go to **Service** > **Event Handling** > **Managing Events** Tab.

Enable Managing Events

Configuration	
Item	**Setting**
▶ Managing Events	☐ Enable

Configuration		
Item	**Value setting**	**Description**
Managing Events	The box is unchecked by default	Check the **Enable** box to activate the Managing Events function.

Create / Edit Managing Event Rules

Setup the Managing Event rules. It supports up to a maximum of 128 rules.

Managing Event List	Add	Delete			
ID	Event	Description		Enable	Actions

When **Add** button is applied, the **Managing Event Configuration** screen will appear.

Managing Event Configuration	
Item	**Setting**
▶ Event	SMS ▼ [_____]
▶ Description	[_____]
▶ Action	☐ Network Status /(☐ LAN&VLAN ☐ WiFi ☐ NAT ☐ Firewall ☐ VPN ☐ GRE ☐ System Manage ☐ Administration ☐ Digital Output ☐ Modbus)
▶ Managing Event	☑ Enable
	Save

Managing Event Configuration		
Item	**Value setting**	**Description**
Event	**SMS** (or **SNMP Trap**) by default	Specify the Event type (**SMS**, **SNMP Trap**, or **DI**) and an event identifier / profile. **SMS**: Select **SMS** and fill the message in the textbox to as the trigger condition for the event; **SNMP**: Select **SNMP Trap** and fill the message in the textbox to specify SNMP Trap Event;

		Digital Input: Select Digital Input and a DI profile you defined to specify a certain Digital Input Event; *Note: The available Event Type could be different for the purchased product.*
Description	String format : any text.	Enter a brief description for the Managing Event.
Action	All box is unchecked by default.	Specify Network Status, or at least one rest action to take when the expected event is triggered. Network Status: Select Network Status Checkbox to get the network status as the action for the event; LAN&VLAN: Select LAN&VLAN Checkbox and the interested sub-items (Port link On/Off), the gateway will change the settings as the action for the event; WiFi: Select WiFi Checkbox and the interested sub-items (WiFi radio On/Off), the gateway will change the settings as the action for the event; NAT: Select NAT Checkbox and the interested sub-items (Virtual Server Rule On/Off, DMZ On/Off), the gateway will change the settings as the action for the event; Firewall: Select Firewall Checkbox and the interested sub-items (Remote Administrator Host ID On/Off), the gateway will change the settings as the action for the event; VPN: Select VPN Checkbox and the interested sub-items (IPSec Tunnel ON/Off, PPTP Client On/Off, L2TP Client On/Off, OpenVPN Client On/Off), the gateway will change the settings as the action for the event; GRE: Select GRE Checkbox and the interested sub-items (GRE Tunnel On/Off), the gateway will change the settings as the action for the event; System Manage: Select System Manage Checkbox and the interested sub-items (WAN SSH Service On/Off, TR-069 On/Off), the gateway will change the settings as the action for the event; Administration: Select Administration Checkbox and the interested sub-items (Backup Config, Restore Config, Reboot, Save Current Setting as Default), the gateway will change the settings as the action for the event; Digital Output: Select Digital Output checkbox and a DO profile you defined as the action for the event; Modbus: Select Modbus checkbox and a Modbus Managing Event profile you defined as the action for the event; *Note: The available Event Type could be different for the purchased product.*
Managing Event	The box is unchecked by default.	Click Enable box to activate this Managing Event setting.
Save	*NA*	Click the Save button to save the configuration
Undo	*NA*	Click the Undo button to restore what you just configured back to the previous setting.

Modbus Cellular Gateway

7.2.3 Notifying Events

Go to **Service** > **Event Handling** > **Notifying Events** Tab.

Notifying Events Setting allows administrator to define the relationship (rule) between event trigger and handlers.

Enable Notifying Events

Item	Setting
▶ Notifying Events	☑ Enable

Configuration Item	Value setting	Description
Notifying Events	The box is unchecked by default	Check the **Enable** box to activate the Notifying Events function.

Create / Edit Notifying Event Rules

Setup your Notifying Event rules. It supports up to a maximum of 128 rules.

Notifying Event List	Add	Delete				
ID	Event	Description	Action	Enable	Actions

When **Add** button is applied, the **Notifying Event Configuration** screen will appear.

Item	Setting
▶ Event	Digital Input ▼ On-->Off ▼
▶ Description	
▶ Action	☐ Digital Output ☐ SMS ☐ Syslog ☐ SNMP Trap ☐ Email Alert
▶ Time Schedule	(0) Always ▼
▶ Notifying Events	☑ Enable
Save	

Modbus Cellular Gateway

Notifying Event Configuration		
Item	**Value setting**	**Description**
Event	**Digital Input** (or **WAN**) by default	Specify the Event type and corresponding event configuration. The supported Event Type could be: **Digital Input**: Select **Digital Input** and a DI profile you defined to specify a certain Digital Input Event; **WAN**: Select **WAN** and a trigger condition to specify a certain WAN Event; **LAN&VLAN**: Select **LAN&VLAN** and a trigger condition to specify a certain LAN&VLAN Event; **WiFi**: Select **WiFi** and a trigger condition to specify a certain WiFi Event; **DDNS**: Select **DDNS** and a trigger condition to specify a certain DDNS Event; **Administration**: Select **Administration** and a trigger condition to specify a certain Administration Event; **Modbus**: Select **Modbus** and a Modbus Notifying Event profile you defined to specify a certain Modbus Event; **Data Usage**: Select **Data Usage**, the SIM Card (Cellular Service) and a trigger condition to specify a certain Data Usage Event; *Note: The available Event Type could be different for the purchased product.*
Description	String format : any text.	Enter a brief description for the Notifying Event.
Action	All box is unchecked by default.	Specify at least one action to take when the expected event is triggered. **Digital Output**: Select **Digital Output** checkbox and a DO profile you defined as the action for the event; **SMS**: Select **SMS**, and the gateway will send out a SMS to all the defined SMS accounts as the action for the event; **Syslog**: Select **Syslog** and select/unselect the Enable Checkbox to as the action for the event; **SNMP Trap**: Select **SNMP Trap**, and the gateway will send out SNMP Trap to the defined SNMP Event Receivers as the action for the event; **Email Alert**: Select **Email Alert**, and the gateway will send out an Email to the defined Email accounts as the action for the event; *Note: The available Event Type could be different for the purchased product.*
Time Schedule	**(0) Always** is selected by default	Select a time scheduling rule for the Notifying Event.
Notifying Events	The box is unchecked by default.	Click **Enable** box to activate this Notifying Event setting.
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore what you just configured back to the previous setting.

Chapter 8 Status

8.1 ~~Dashboard~~ (not supported)

Not supported feature for the purchased product, leave it as blank.

8.2 Basic Network

8.2.1 WAN & Uplink Status

Go to **Status > Basic Network > WAN & Uplink** tab.

The **WAN & Uplink Status** window shows the current status for different network type, including network configuration, connecting information, modem status and traffic statistics.

WAN interface IPv4 Network Status

WAN interface IPv4 Network Status screen shows status information for IPv4 network.

ID	Interface	WAN Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Action
WAN-1	3G/4G	3G/4G	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	N/A	Disconnected	Edit

WAN interface IPv4 Network Status		
Item	**Value setting**	**Description**
ID	N/A	It displays corresponding WAN interface WAN IDs.
Interface	N/A	It displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, 3G/4G, etc...
WAN Type	N/A	It displays the method which public IP address is obtained from your ISP. Depending on the model purchased, it can be Static IP, Dynamic IP, PPPoE, PPTP, L2TP, 3G/4G.
IP Addr.	N/A	It displays the public IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
Subnet Mask	N/A	It displays the Subnet Mask for public IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
Gateway	N/A	It displays the Gateway IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
DNS	N/A	It displays the IP address of DNS server obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
MAC Address	N/A	It displays the MAC Address for your ISP to allow you for Internet access. Note: Not all ISP may require this field.
Conn. Status	N/A	It displays the connection status of the device to your ISP. Status are Connected or disconnected.
Action	N/A	This area provides functional buttons. **Renew** button allows user to force the device to request an IP address from

Modbus Cellular Gateway

the DHCP server. Note: **Renew** button is available when DHCP WAN Type is used and WAN connection is disconnected.

Release button allows user to force the device to clear its IP address setting to disconnect from DHCP server. Note: **Release** button is available when DHCP WAN Type is used and WAN connection is connected.

Connect button allows user to manually connect the device to the Internet. Note: Connect button is available when Connection Control in WAN Type setting is set to Connect Manually (Refer to **Edit** button in **Basic Network > WAN & Uplink > Internet Setup**) and WAN connection status is disconnected.

Disconnect button allows user to manually disconnect the device from the Internet. Note: **Connect** button is available when Connection Control in WAN Type setting is set to Connect Manually (Refer to **Edit** button in **Basic Network > WAN & Uplink > Internet Setup**) and WAN connection status is connected.

WAN interface IPv6 Network Status

WAN interface IPv6 Network Status screen shows status information for IPv6 network.

ID	Interface	WAN Type	Link-local IP Address	Global IP Address	Conn. Status	Action
WAN-1	Ethernet	DHCPv6	fe80::250:18ff:fe16:1121	/64	Disconnected	Connect	Edit

WAN interface IPv6 Network Status		
Item	**Value setting**	**Description**
ID	N/A	It displays corresponding WAN interface WAN IDs.
Interface	N/A	It displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, 3G/4G, etc...
WAN Type	N/A	It displays the method which public IP address is obtained from your ISP. WAN type setting can be changed from **Basic Network > IPv6 > Configuration**.
Link-local IP Address	N/A	It displays the LAN IPv6 Link-Local address.
Global IP Address	N/A	It displays the IPv6 global IP address assigned by your ISP for your Internet connection.
Conn. Status	N/A	It displays the connection status. The status can be connected, disconnected and connecting.
Action	N/A	This area provides functional buttons. **Edit Button** when pressed, web-based utility will take you to the IPv6 configuration page. (**Basic Network > IPv6 > Configuration**.)

Modbus Cellular Gateway

LAN Interface Network Status

LAN Interface Network Status screen shows IPv4 and IPv6 information of LAN network.

LAN Interface Network Status				
IPv4 Address	IPv4 Subnet Mask	IPv6 Link-local Address	IPv6 Global Address	Action
192.168.123.254	255.255.255.0	fe80::250:18ff:fe21:e949	/64	Edit IPv4 Edit IPv6

LAN Interface Network Status		
Item	**Value setting**	**Description**
IPv4 Address	N/A	It displays the current IPv4 IP Address of the gateway This is also the IP Address user use to access Router's Web-based Utility.
IPv4 Subnet Mask	N/A	It displays the current mask of the subnet.
IPv6 Link-local Address	N/A	It displays the current LAN IPv6 Link-Local address. This is also the IPv6 IP Address user use to access Router's Web-based Utility.
IPv6 Global Address	N/A	It displays the current IPv6 global IP address assigned by your ISP for your Internet connection.
Action	N/A	This area provides functional buttons. **Edit IPv4 Button** when press, web-based utility will take you to the Ethernet LAN configuration page. (**Basic Network > LAN & VLAN > Ethernet LAN** tab). **Edit IPv6 Button** when press, web-based utility will take you to the IPv6 configuration page. (**Basic Network > IPv6 > Configuration**.)

3G/4G Modem Status

3G/4G Modem Status List screen shows status information for 3G/4G WAN network(s).

3G/4G Modem Status List					
Interface	Card Information	Link Status	Signal Strength	Network Name	Action
3G/4G	ME3620-J	Disconnected	N/A		Detail

3G/4G Modem Status List		
Item	**Value setting**	**Description**
Physical Interface	N/A	It displays the type of WAN physical interface. Note: Some device model may support two 3G/4G modules. Their physical interface name will be **3G/4G-1** and **3G/4G-2**.
Card Information	N/A	It displays the vendor's 3G/4G modem model name.
Link Status	N/A	It displays the 3G/4G connection status. The status can be Connecting, Connected, Disconnecting, and Disconnected.

Modbus Cellular Gateway

Signal Strength	N/A	It displays the 3G/4G wireless signal level.
Network Name	N/A	It displays the name of the service network carrier.
Refresh	N/A	Click the **Refresh** button to renew the information.
Action	N/A	This area provides functional buttons. **Detail Button** when press, windows of detail information will appear. They are the Modem Information, SIM Status, and Service Information. Refer to next page for more.

When the **Detail** button is pressed, 3G/4G modem information windows such as Modem Information, SIM Status, Service Information, and Signal Strength / Quality will appear.

Interface Traffic Statistics

Interface Traffic Statistics screen displays the Interface's total transmitted packets.

ID	Interface	Received Packets	Transmitted Packets
WAN-1	3G/4G	0	0

Interface Traffic Statistics		
Item	**Value setting**	**Description**
ID	N/A	It displays corresponding WAN interface WAN IDs.
Interface	N/A	It displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, 3G/4G, etc...
Received Packets	N/A	It displays the downstream packets. It is reset when the device is rebooted.
Transmitted Packets	N/A	It displays the upstream packets. It is reset when the device is rebooted.

Modbus Cellular Gateway

8.2.2 LAN & VLAN Status

Go to **Status > Basic Network > LAN & VLAN** tab.

Client List

The **Client List** shows you the LAN Interface, IP address, Host Name, MAC Address, and Remaining Lease Time of each device that is connected to this gateway.

LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time
Ethernet	Dynamic / 192.168.1.100	amit-25611230-1	00-01-0A-10-0F-17	23:59:51

LAN Client List		
Item	**Value setting**	**Description**
LAN Interface	N/A	Client record of LAN Interface. String Format.
IP Address	N/A	Client record of IP Address Type and the IP Address. Type is String Format and the IP Address is IPv4 Format.
Host Name	N/A	Client record of Host Name. String Format.
MAC Address	N/A	Client record of MAC Address. MAC Address Format.
Remaining Lease Time	N/A	Client record of Remaining Lease Time. Time Format.

8.2.3 ~~WiFi Status~~ (not supported)

Not supported feature for the purchased product, leave it as blank.

Modbus Cellular Gateway

8.2.4 DDNS Status

Go to **Status > Basic Network > DDNS** tab.

The **DDNS Status** window shows the current DDNS service in use, the last update status, and the last update time to the DDNS service server.

DDNS Status

Host Name	Provider	Effective IP	Last Update Status	Last Update Time

DDNS Status Item	Value Setting	Description
Host Name	N/A	It displays the name you entered to identify DDNS service provider
Provider	N/A	It displays the DDNS server of DDNS service provider
Effective IP	N/A	It displays the public IP address of the device updated to the DDNS server
Last Update Status	N/A	It displays whether the last update of the device public IP address to the DDNS server has been successful (Ok) or failed (Fail).
Last Update Time	N/A	It displays time stamp of the last update of public IP address to the DDNS server.
Refresh	N/A	The **refresh** button allows user to force the display to refresh information.

Modbus Cellular Gateway

8.3 Security
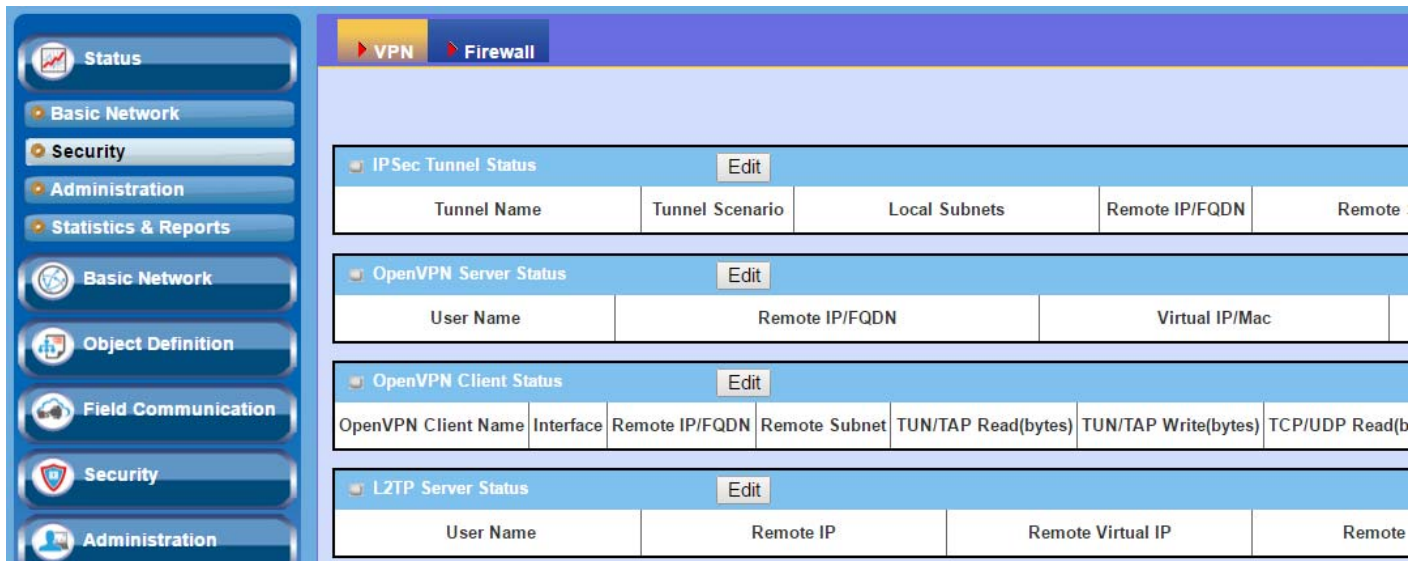
8.3.1 VPN Status

Go to **Status > Security > VPN** tab.

The **VPN Status** widow shows the overall VPN tunnel status.

IPSec Tunnel Status

IPSec Tunnel Status windows show the configuration for establishing IPSec VPN connection and current connection status.

IPSec Tunnel Status		
Item	**Value setting**	**Description**
Tunnel Name	N/A	It displays the tunnel name you have entered to identify.
Tunnel Scenario	N/A	It displays the Tunnel Scenario specified.
Local Subnets	N/A	It displays the Local Subnets specified.
Remote IP/FQDN	N/A	It displays the Remote IP/FQDN specified.
Remote Subnets	N/A	It displays the Remote Subnets specified.
Conn. Time	N/A	It displays the connection time for the IPSec tunnel.
Status	N/A	It displays the Status of the VPN connection. The status displays are Connected, Disconnected, Wait for traffic, and Connecting.
Edit Button	N/A	Click on Edit Button to change IPSec setting, web-based utility will take you to the IPSec configuration page. (**Security > VPN > IPSec** tab)

Modbus Cellular Gateway

OpenVPN Server Status

According to OpenVPN configuration, the **OpenVPN Server/Client Status** shows the status and statistics for the OpenVPN connection from the server side or client side.

OpenVPN Server Status	Edit			
User Name	Remote IP/FQDN	Virtual IP/Mac	Conn. Time	Status

OpenVPN Server Status		
Item	**Value setting**	**Description**
User Name	N/A	It displays the Client name you have entered for identification.
Remote IP/FQDN	N/A	It displays the public IP address (the WAN IP address) of the connected OpenVPN Client
Virtual IP/MAC	N/A	It displays the virtual IP/MAC address assigned to the connected OpenVPN client.
Conn. Time	N/A	It displays the connection time for the corresponding OpenVPN tunnel.
Status	N/A	It displays the connection status of the corresponding OpenVPN tunnel. The status can be Connected, or Disconnected.

OpenVPN Client Status

OpenVPN Client Status	Edit								
OpenVPN Client Name	Interface	Remote IP/FQDN	Remote Subnet	TUN/TAP Read(bytes)	TUN/TAP Write(bytes)	TCP/UDP Read(bytes)	TCP/UDP Write(bytes)	Conn. Time	Conn. Status

OpenVPN Client Status		
Item	**Value setting**	**Description**
OpenVPN Client Name	N/A	It displays the Client name you have entered for identification.
Interface	N/A	It displays the WAN interface specified for the OpenVPN client connection.
Remote IP/FQDN	N/A	It displays the peer OpenVPN Server's Public IP address (the WAN IP address) or FQDN.
Remote Subnet	N/A	It displays the Remote Subnet specified.
TUN/TAP Read(bytes)	N/A	It displays the TUN/TAP Read Bytes of OpenVPN Client.
TUN/TAP Write(bytes)	N/A	It displays the TUN/TAP Write Bytes of OpenVPN Client.
TCP/UDP Read(bytes)	N/A	It displays the TCP/UDP Read Bytes of OpenVPN Client.
TCP/UDP Write(bytes)	N/A	It displays the TCP/UDP Write Bytes of OpenVPN Client. Connection
Conn. Time	N/A	It displays the connection time for the corresponding OpenVPN tunnel.
Conn. Status	N/A	It displays the connection status of the corresponding OpenVPN tunnel. The status can be Connected, or Disconnected.

Modbus Cellular Gateway

L2TP Server/Client Status

LT2TP **Server/Client Status** shows the configuration for establishing LT2TP tunnel and current connection status.

☐ L2TP Server Status	Edit				
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Conn. Time	Status

L2TP Server Status		
Item	**Value setting**	**Description**
User Name	N/A	It displays the login name of the user used for the connection.
Remote IP	N/A	It displays the public IP address (the WAN IP address) of the connected L2TP client.
Remote Virtual IP	N/A	It displays the IP address assigned to the connected L2TP client.
Remote Call ID	N/A	It displays the L2TP client Call ID.
Conn. Time	N/A	It displays the connection time for the L2TP tunnel.
Status	N/A	It displays the Status of each of the L2TP client connection. The status displays Connected, Disconnect, Connecting
Edit	N/A	Click on **Edit** Button to change L2TP server setting, web-based utility will take you to the L2TP server page. (**Security > VPN > L2TP** tab)

☐ L2TP Client Status	Edit					
L2TP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Conn. Time	Status

L2TP Client Status		
Item	**Value setting**	**Description**
Client Name	N/A	It displays Name for the L2TP Client specified.
Interface	N/A	It displays the WAN interface with which the gateway will use to request PPTP tunneling connection to the PPTP server.
Virtual IP	N/A	It displays the IP address assigned by Virtual IP server of L2TP server.
Remote IP/FQDN	N/A	It displays the L2TP Server's Public IP address (the WAN IP address) or FQDN.
Default Gateway/Remote Subnet	N/A	It displays the specified IP address of the gateway device used to connect to the internet to connect to the L2TP server –the default gateway. Or other specified subnet if the default gateway is not used to connect to the L2TP server –the remote subnet.
Conn. Time	N/A	It displays the connection time for the L2TP tunnel.
Status	N/A	It displays the Status of the VPN connection. The status displays Connected, Disconnect, and Connecting.
Edit	N/A	Click on **Edit** Button to change L2TP client setting, web-based utility will take you to the L2TP client page. (**Security > VPN > L2TP** tab)

Modbus Cellular Gateway

PPTP Server/Client Status

PPTP Server/Client Status shows the configuration for establishing PPTP tunnel and current connection status.

PPTP Server Status	Edit				
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Conn. Time	Status

PPTP Server Status Item	Value setting	Description
User Name	N/A	It displays the login name of the user used for the connection.
Remote IP	N/A	It displays the public IP address (the WAN IP address) of the connected PPTP client.
Remote Virtual IP	N/A	It displays the IP address assigned to the connected PPTP client.
Remote Call ID	N/A	It displays the PPTP client Call ID.
Conn. Time	N/A	It displays the connection time for the PPTP tunnel.
Status	N/A	It displays the Status of each of the PPTP client connection. The status displays Connected, Disconnect, and Connecting.
Edit Button	N/A	Click on **Edit** Button to change PPTP server setting, web-based utility will take you to the PPTP server page. (**Security > VPN > PPTP** tab)

PPTP Client Status	Edit					
PPTP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Conn. Time	Status

PPTP Client Status Item	Value setting	Description
Client Name	N/A	It displays Name for the PPTP Client specified.
Interface	N/A	It displays the WAN interface with which the gateway will use to request PPTP tunneling connection to the PPTP server.
Virtual IP	N/A	It displays the IP address assigned by Virtual IP server of PPTP server.
Remote IP/FQDN	N/A	It displays the PPTP Server's Public IP address (the WAN IP address) or FQDN.
Default Gateway / Remote Subnet	N/A	It displays the specified IP address of the gateway device used to connect to the internet to connect to the PPTP server –the default gateway. Or other specified subnet if the default gateway is not used to connect to the PPTP server –the remote subnet.
Conn. Time	N/A	It displays the connection time for the PPTP tunnel.
Status	N/A	It displays the Status of the VPN connection. The status displays Connected, Disconnect, and Connecting.
Edit Button	N/A	Click on **Edit** Button to change PPTP client setting, web-based utility will take you to the PPTP server page. (**Security > VPN > PPTP** tab)

Modbus Cellular Gateway

8.3.2 Firewall Status

Go to **Status > Security > Firewall Status** Tab.

The **Firewall Status** provides user a quick view of the firewall status and current firewall settings. It also keeps the log history of the dropped packets by the firewall rule policies, and includes the administrator remote login settings specified in the Firewall Options.

By clicking the icon [+], the status table will be expanded to display log history. Clicking the **Edit** button the screen will be switched to the configuration page.

Packet Filter Status

Packet Filters	Edit		[+]
Activated Filter Rule	Detected Contents	IP	Time

Packet Filter Status		
Item	**Value setting**	**Description**
Activated Filter Rule	N/A	This is the Packet Filter Rule name.
Detected Contents	N/A	This is the logged packet information, including the source IP, destination IP, protocol, and destination port –the TCP or UDP. String format: Source IP to Destination IP : Destination Protocol (TCP or UDP)
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure Packet Filter Log Alert is enabled.
*Refer to **Security > Firewall > Packet Filter** tab. Check Log Alert and save the setting.*

URL Blocking Status

URL Blocking	Edit		[+]
Activated Blocking Rule	Blocked URL	IP	Time

URL Blocking Status		
Item	**Value setting**	**Description**
Activated Blocking Rule	N/A	This is the URL Blocking Rule name.
Blocked URL	N/A	This is the logged packet information.

IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure URL Blocking Log Alert is enabled.

*Refer **to Security > Firewall > URL Blocking** tab. Check Log Alert and save the setting.*

Web Content Filter Status

Web Content Filters	Edit			[+]
Activated Filter Rule	Detected Contents		IP	Time

Web Content Filter Status		
Item	**Value setting**	**Description**
Activated Filter Rule	N/A	Logged packet of the rule name. String format.
Detected Contents	N/A	Logged packet of the filter rule. String format.
IP	N/A	Logged packet of the Source IP. IPv4 format.
Time	N/A	Logged packet of the Date Time. Date time format ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure Web Content Filter Log Alert is enabled.

*Refer to **Security > Firewall > Web Content Filter** tab. Check Log Alert and save the setting.*

Modbus Cellular Gateway

MAC Control Status

MAC Control	Edit			[+]
Activated Control Rule	Blocked MAC Addresses		IP	Time

MAC Control Status		
Item	**Value setting**	**Description**
Activated Control Rule	N/A	This is the MAC Control Rule name.
Blocked MAC Addresses	N/A	This is the MAC address of the logged packet.
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure MAC Control Log Alert is enabled.

*Refer to **Security > Firewall > MAC Control** tab. Check Log Alert and save the setting.*

Application Filters Status

Application Filters	Edit			[+]
Filtered Application Category	Filtered Application Name		IP	Time

Application Filters Status		
Item	**Value setting**	**Description**
Filtered Application Category	N/A	The name of the Application Category being blocked.
Filtered Application Name	N/A	The name of the Application being blocked.
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure Application Filter Log Alert is enabled.

*Refer to **Security > Firewall > Application Filter** tab. Check Log Alert and save the setting.*

Modbus Cellular Gateway

IPS Status

IPS	Edit			[+]
	Detected Intrusion		IP	Time

IPS Firewall Status		
Item	**Value setting**	**Description**
Detected Intrusion	N/A	This is the intrusion type of the packets being blocked.
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure IPS Log Alert is enabled.
Refer to **Security > Firewall > IPS** tab. Check Log Alert and save the setting.

Firewall Options Status

Options	Edit			[+]
Stealth Mode	SPI	Discard Ping from WAN	Remote Administrator Management	

Firewall Options Status		
Item	**Value setting**	**Description**
Stealth Mode	N/A	Enable or Disable setting status of Stealth Mode on Firewall Options. String Format: Disable or Enable
SPI	N/A	Enable or Disable setting status of SPI on Firewall Options. String Format : Disable or Enable
Discard Ping from WAN	N/A	Enable or Disable setting status of Discard Ping from WAN on Firewall Options. String Format: Disable or Enable
Remote Administrator Management	N/A	Enable or Disable setting status of Remote Administrator. If Remote Administrator is enabled, it shows the currently logged in administrator's source IP address and login user name and the login time. Format: IP : "Source IP", User Name: "Login User Name", Time: "Date time" Example: IP: 192.168.127.39, User Name: admin, Time: Mar 3 01:34:13

Note: Ensure Firewall Options Log Alert is enabled.
Refer to **Security > Firewall > Options** tab. Check Log Alert and save the setting.

Modbus Cellular Gateway

8.4 Administration

8.4.1 Configure & Manage Status

Go to **Status > Administration > Configure & Manage** tab.
The **Configure & Manage Status** window shows the status for managing remote network devices. The type of management available in your device is depended on the device model purchased. The commonly used ones are the SNMP, TR-069, and UPnP.

SNMP Linking Status

SNMP Link Status screen shows the status of current active SNMP connections.

User Name	IP Address	Port	Community	Auth. Mode	Privacy Mode	SNMP Version

SNMP Link Status		
Item	**Value setting**	**Description**
User Name	N/A	It displays the user name for authentication. This is only available for SNMP version 3.
IP Address	N/A	It displays the IP address of SNMP manager.
Port	N/A	It displays the port number used to maintain connection with the SNMP manager.
Community	N/A	It displays the community for SNMP version 1 or version 2c only.
Auth. Mode	N/A	It displays the authentication method for SNMP version 3 only.
Privacy Mode	N/A	It displays the privacy mode for version 3 only.
SNMP Version	N/A	It displays the SNMP Version employed.

SNMP Trap Information

SNMP Trap Information screen shows the status of current received SNMP traps.

Trap Level	Time	Trap Event

SNMP Trap Information		
Item	**Value setting**	**Description**
Trap Level	N/A	It displays the trap level.
Time	N/A	It displays the timestamp of trap event.
Trap Event	N/A	It displays the IP address of the trap sender and event type.

Modbus Cellular Gateway

TR-069 Status

TR-069 Status screen shows the current connection status with the TR-068 server.

TR-069 Status
Link Status
Off

TR-069 Status		
Item	**Value setting**	**Description**
Link Status	N/A	It displays the current connection status with the TR-068 server. The connection status is either On when the device is connected with the TR-068 server or Off when disconnected.

Modbus Cellular Gateway

8.4.2 Log Storage Status

Go to **Status > Administration > Log Storage** tab.

The **Log Storage Status** screen shows the status for selected device storage.

Log Storage Status

Log Storage Status screen shows the status of current the selected device storage. The status includes Device Select, Device Description, Usage, File System, Speed, and status
.

Storage Information					
Device Select	**Device Description**	**Usage**	**File System**	**Speed**	**Status**
Storage 1 ▾	USB Storage	0 / 3788 MB	FAT/FAT32	USB 2.0	Ready

Modbus Cellular Gateway

8.5 Statistics & Report

8.5.1 Connection Session

Go to **Status > Statistics & Reports > Connection Session** tab.

Internet Surfing Statistic shows the connection tracks on this router.

Internet Surfing Statistic		
Item	**Value setting**	**Description**
Previous	N/A	Click the **Previous** button; you will see the previous page of track list.
Next	N/A	Click the **Next** button; you will see the next page of track list.
First	N/A	Click the **First** button; you will see the first page of track list.
Last	N/A	Click the **Last** button; you will see the last page of track list.
Export (.xml)	N/A	Click the **Export (.xml)** button to export the list to xml file.
Export (.csv)	N/A	Click the **Export (.csv)** button to export the list to csv file.
Refresh	N/A	Click the **Refresh** button to refresh the list.

8.5.2 ~~Network Traffic~~ (not supported)

Not supported feature for the purchased product, leave it as blank.

Modbus Cellular Gateway

8.5.3 Device Administration

Go to **Status > Statistics & Reports > Device Administration** tab.

Device Administration shows the login information.

Device Manager Login Statistics	Previous	Next	First	Last	Export (.xml)	Export (.csv)	Refresh
User Name	**Protocol Type**		**IP Address**		**User Level**	**Duration Time**	
admin	http/https		192.168.123.100		Admin	2017/03/22 03:31~	

Device Manager Login Statistic		
Item	**Value setting**	**Description**
Previous	N/A	Click the **Previous** button; you will see the previous page of login statistics.
Next	N/A	Click the **Next** button; you will see the next page of login statistics.
First	N/A	Click the **First** button; you will see the first page of login statistics.
Last	N/A	Click the **Last** button; you will see the last page of login statistics.
Export (.xml)	N/A	Click the **Export (.xml)** button to export the login statistics to xml file.
Export (.csv)	N/A	Click the **Export (.csv)** button to export the login statistics to csv file.
Refresh	N/A	Click the **Refresh** button to refresh the login statistics.

Modbus Cellular Gateway

8.5.4 Cellular Usage

Go to **Status > Statistics & Reports > Cellular Usage** tab.

Cellular Usage screen shows data usage statistics for the selected cellular interface. The cellular data usage can be accumulated per hour or per day.
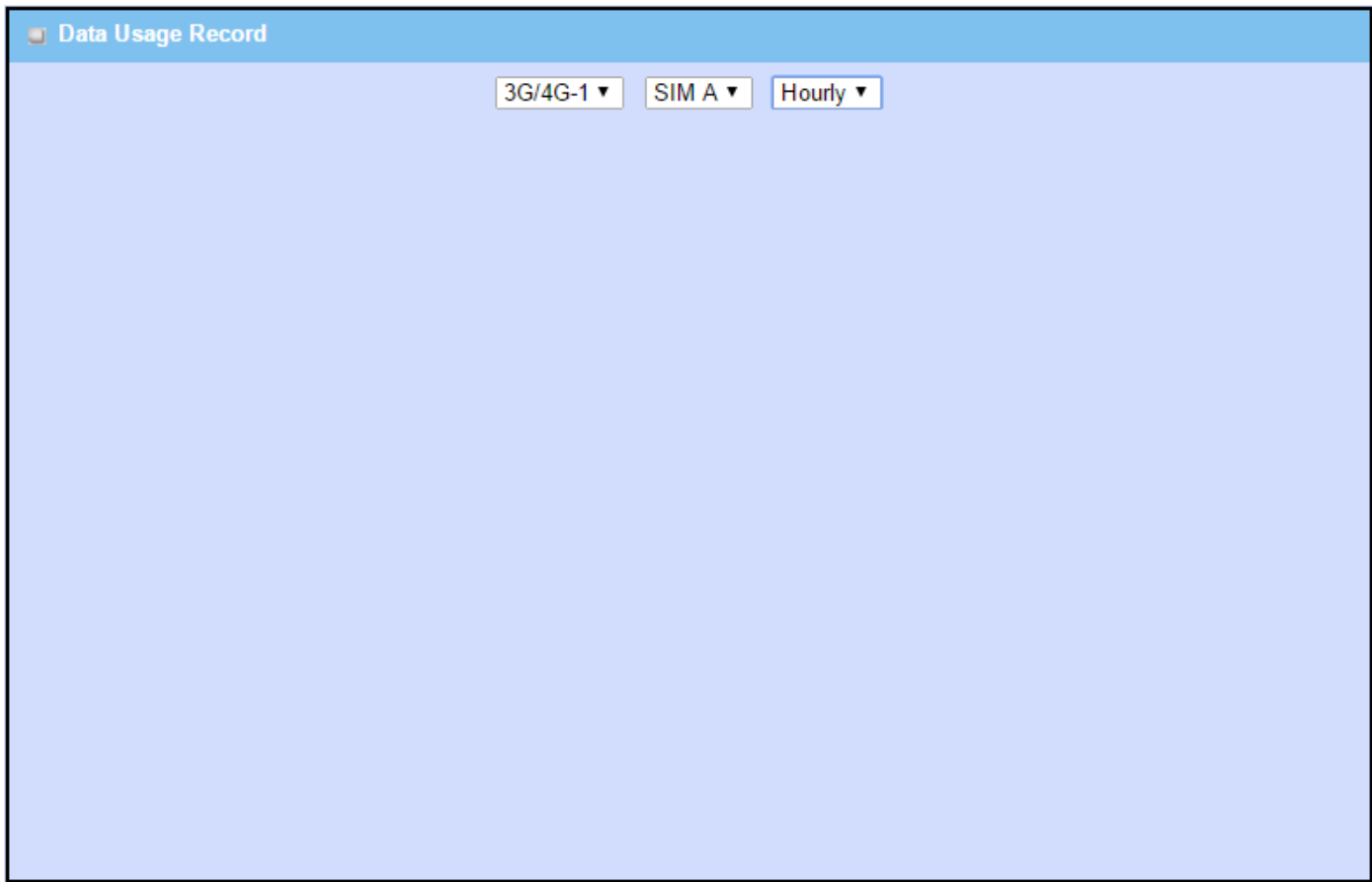
Appendix A GPL WRITTEN OFFER

This product incorporates open source software components covered by the terms of third party copyright notices and license agreements contained below.

GPSBabel
Version 1.4.4
Copyright (C) 2002-2005 Robert Lipe<robertlipe@usa.net>
GPL License: https://www.gpsbabel.org/

Curl
Version 7.19.6
Copyright (c) 1996-2009, Daniel Stenberg, <daniel@haxx.se>.
MIT/X derivate License: https://curl.haxx.se/

OpenSSL
Version 1.0.2c
Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
GPL License: https://www.openssl.org/

brctl - ethernet bridge administration
Stephen Hemminger <shemminger@osdl.org>
Lennert Buytenhek <buytenh@gnu.org>
version 1.1
GNU GENERAL PUBLIC LICENSE Version 2, June 1991

tc - show / manipulate traffic control settings
Stephen Hemminger<shemminger@osdl.org>
Alexey Kuznetsov<kuznet@ms2.inr.ac.ru>
version iproute2-ss050330
GNU GENERAL PUBLIC LICENSE Version 2, June 1991

dhcp-fwd — starts the DHCP forwarding agent
Enrico Scholz <enrico.scholz@informatik.tu-chemnitz.de>
version 0.7
GNU GENERAL PUBLIC LICENSE Version 2, June 1991

lftp - Sophisticated file transfer program
Alexander V. Lukyanov <lav@yars.free.net>

Modbus Cellular Gateway

version:4.5.x
Copyright (c) 1996-2014 by Alexander V. Lukyanov (lav@yars.free.net)

dnsmasq - A lightweight DHCP and caching DNS server.
Simon Kelley <simon@thekelleys.org.uk>
version:2.72
dnsmasq is Copyright (c) 2000-2014 Simon Kelley

socat - Multipurpose relay
Version: 2.0.0-b8
GPLv2
http://www.dest-unreach.org/socat/

LibModbus
Version: 3.0.3
LGPL v2
http://libmodbus.org/news/

LibIEC60870
GPLv2
Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston,
MA 02111-1307 USA
https://sourceforge.net/projects/mrts/

Openswan
Version: v2.6.38 GNU GENERAL PUBLIC LICENSE Version 2, June 1991
 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston,
MA 02111-1307 USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.
https://www.openswan.org/

Opennhrp
Version: v0.14.1
OpenNHRP is an NHRP implementation for Linux. It has most of the RFC2332
and Cisco IOS extensions.
Project homepage: http://sourceforge.net/projects/opennhrp
Git repository: git://opennhrp.git.sourceforge.net/gitroot/opennhrp
 LICENSE
OpenNHRP is licensed under the MIT License. See MIT-LICENSE.txt for

additional details.

OpenNHRP embeds libev. libev is dual licensed with 2-clause BSD and GPLv2+ licenses. See libev/LICENSE for additional details.

OpenNHRP links to c-ares. c-ares is licensed under the MIT License.

https://sourceforge.net/projects/opennhrp/

IPSec-tools

Version: v0.8

No GPL be written

http://ipsec-tools.sourceforge.net/

PPTP

Version: pptp-1.7.1

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA

 Everyone is permitted to copy and distribute verbatim copies

 of this license document, but changing it is not allowed.

http://pptpclient.sourceforge.net/

PPTPServ

Version: 1.3.4

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA

 Everyone is permitted to copy and distribute verbatim copies

 of this license document, but changing it is not allowed. http://poptop.sourceforge.net/

L2TP

Version: 0.4

Copying All software included in this package is Copyright 2002 Roaring Penguin Software Inc. You may distribute it under the terms of the GNU General Public License (the "GPL"), Version 2, or (at your option) any later version.

http://www.roaringpenguin.com/

L2TPServ

Version: v 1.3.1 GNU GENERAL PUBLIC LICENSEVersion 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

 Everyone is permitted to copy and distribute verbatim copies

 of this license document, but changing it is not allowed.

Modbus Cellular Gateway

http://www.xelerance.com/software/xl2tpd/

Mpstat: from sysstat, system performance tools for Linux
Version: 10.1.6
Copyright: (C) 1999-2013 by Sebastien Godard (sysstat <at> orange.fr)

SSHD: dropbear, a SSH2 server
Version: 0.53.1
Copyright: (c) 2002-2008 Matt Johnston

Libncurses: The ncurses (new curses) library is a free software emulation of curses in System V Release 4.0 (SVr4), and more.
Version: 5.9
Copyright: (c) 1998,2000,2004,2005,2006,2008,2011,2015 Free Software Foundation, Inc., 51 Franklin Street, Boston, MA 02110-1301, USA

MiniUPnP: The miniUPnP daemon is an UPnP IGD (internet gateway device) which provide NAT traversal services to any UPnP enabled client on the network.
Version: 1.7
Copyright: (c) 2006-2011, Thomas BERNARD

CoovaChilli is an open-source software access controller for captive portal (UAM) and 802.1X access provisioning.
Version: 1.3.0
Copyright: (C) 2007-2012 David Bird (Coova Technologies) <support@coova.com>

Krb5: Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.
Version: 1.11.3
Copyright: (C) 1985-2013 by the Massachusetts Institute of Technology and its contributors

OpenLDAP: a suite of the Lightweight Directory Access Protocol (v3) servers, clients, utilities, and development tools.
Version: 2.4
Copyright: 1998-2014 The OpenLDAP Foundation

Samba3311: the free SMB and CIFS client and server for UNIX and other operating systems
Version: 3.3.11
Copyright: (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>

Modbus Cellular Gateway

NTPClient: an NTP (RFC-1305, RFC-4330) client for unix-alike computers
Version: 2007_365
Copyright: 1997, 1999, 2000, 2003, 2006, 2007 Larry Doolittle

exFAT: FUSE-based exFAT implementation
Version: 0.9.8
Copyright: (C) 2010-2012 Andrew Nayenko

ONTFS_3G: The NTFS-3G driver is an open source, freely available read/write NTFS driver for Linux, FreeBSD, Mac OS X, NetBSD, Solaris and Haiku.
Version: 2009.4.4
Copyright: (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

mysql-5_1_72: a release of MySQL, a dual-license SQL database server
Version: 5.1.72
Copyright: (c) 2000, 2013, Oracle and/or its affiliates
FreeRadius: a high performance and highly configurable RADIUS server
Version: 2.1.12
Copyright: (C) 1999-2011 The FreeRADIUS server project and contributors

Linux IPv6 Router Advertisement Daemon – radvd
Version: V 1.15
Copyright (c) 1996,1997 by Lars Fenneberg<lf@elemental.net>
BSD License: http://www.litech.org/radvd/

WIDE-DHCPv6
Dynamic Host Configuration Protocol for IPv6 (DHCPv6) clients, servers, and relay agents.
Version: 20080615
Copyright (C) 1998-2004 WIDE Project.
BSD License: https://sourceforge.net/projects/wide-dhcpv6/