



# Industrial Cellular Gateway

## EW200

User Manual

**All Rights Reserved**

Dissemination or reproduction of this document, or its contents, is not authorized except where expressly permitted. Violators are liable for damages. All rights reserved, for the purposes of patent application or trademark registration.

**Disclaimer of Liability**

The information contained in this document is subject to change without notice. EtherWAN is not liable for any errors or omissions contained herein or for resulting damage in connection with the information provided in this manual.

All other trademarks are property of their respective owners.

**Warranty**

For details on the EtherWAN warranty replacement policy, please visit our web site at:

[www.etherwan.com](http://www.etherwan.com)

**Products Supported by this Manual:**

EW200

# Preface

## Audience

This guide is designed for the person who installs, configures, deploys, and maintains the Ethernet network. This document assumes the reader has moderate hardware, computer, and Internet skills.

## Document Revision Level

This section provides a history of the revision changes to this document.

Revision	Document Version	Date	Description
A	Version 2	1/15/2018	Fixed several spelling and grammar errors
A	3	2/9/2018	Text revisions
B	1	07/05/2019	Added TR-069 & LLDP function description
C	1	09/03/2019	Added MQTT and Azure info
C	2	12/19/2019	Added max connections for TCP client and server
D	1	09/24/2020	Revised for new firmware

## Contents

Preface.....	3
Contents .....	4
Chapter 1 Introduction .....	9
1.1 Introduction.....	9
1.2 Contents List .....	10
1.2.1 Package Contents .....	10
1.3 Hardware Configuration .....	11
1.4 LED Indicators.....	13
1.5 Installation & Maintenance.....	14
1.5.1 SYSTEM REQUIREMENTS .....	14
1.5.2 WARNING.....	14
1.5.3 HOT SURFACE CAUTION.....	15
1.5.4 Product Information for CE RED Requirements .....	16
1.6 Hardware Installation.....	18
1.6.1 Mount the Unit.....	18
1.6.2 Insert the SIM Card.....	18
1.6.3 Connecting Power .....	19
1.6.4 Power Supply Installation .....	19
1.6.5 Connecting DI/DO Devices .....	22
1.6.6 Connecting Serial Devices .....	23
1.6.7 Connecting to the Network or a Host .....	23
1.6.8 Setup by Configuring WEB UI.....	24
Chapter 2 Basic Network .....	25
2.1 WAN & Uplink .....	25
2.1.1 Physical Interface.....	26
2.1.2 Internet Setup .....	31
2.1.3 Load Balance .....	51
2.2 LAN & VLAN .....	56
2.2.1 Ethernet LAN.....	56
2.2.2 VLAN .....	59
2.2.3 DHCP Server.....	72



# EW200 Industrial Cellular Gateway

---

2.3	Wi-Fi .....	80
2.3.1	Wi-Fi Configuration.....	81
2.3.2	Wireless Client List.....	93
2.3.3	Advanced Configuration .....	95
2.4	IPv6.....	97
2.4.1	IPv6 Configuration.....	97
2.5	Port Forwarding .....	104
2.5.1	Configuration .....	105
2.5.2	Virtual Server & Virtual Computer .....	106
2.5.3	DMZ & Pass Through.....	112
2.5.4	Special AP & ALG.....	114
2.6	Routing.....	118
2.6.1	Static Routing.....	119
2.6.2	Dynamic Routing.....	122
2.6.3	Routing Information.....	130
2.7	DNS & DDNS.....	131
2.7.1	DNS & DDNS Configuration .....	131
2.8	QoS .....	135
2.8.1	QoS Configuration .....	135
2.9	Redundancy.....	144
2.9.1	VRRP .....	144
Chapter 3	Object Definition.....	147
3.1	Scheduling.....	147
3.1.1	Scheduling Configuration .....	147
3.2	Grouping .....	149
3.2.1	Host Grouping.....	149
3.3	External Server.....	151
3.4	Certificates .....	154
3.4.1	Configuration .....	154
3.4.2	My Certificate .....	157
3.4.3	Trusted Certificate.....	164
3.4.4	Issue Certificate .....	169

# EW200 Industrial Cellular Gateway

---

Chapter 4 Field Communication .....	172
4.1 Bus & Protocol.....	172
4.1.1 Port Configuration .....	172
4.1.2 Virtual COM .....	174
4.1.3 Modbus .....	185
4.2 Data Logging .....	196
4.2.1 Data Logging Configuration .....	199
4.2.2 Scheme Setup.....	201
4.2.3 Log File Management .....	203
4.3 Data Interchange .....	204
4.3.1 MQTT .....	204
Chapter 5 Security.....	215
5.1 VPN.....	215
5.1.1 IPsec .....	216
5.1.2 OpenVPN.....	224
5.1.3 L2TP .....	238
5.1.4 PPTP .....	245
5.1.5 GRE.....	252
5.2 Firewall .....	256
5.2.1 Packet Filter .....	256
5.2.2 URL Blocking .....	261
5.2.3 MAC Control .....	265
5.2.4 IPS.....	268
5.2.5 Options.....	272
Chapter 6 Administration.....	276
6.1 Configure & Manage .....	276
6.1.1 Command Script .....	277
6.1.2 TR-069 .....	280
6.1.3 SNMP.....	285
6.1.4 Telnet with CLI .....	296
6.1.5 LLDP.....	300
6.2 System Operation.....	301

# EW200 Industrial Cellular Gateway

---

6.2.1 Password & MMI.....	301
6.2.2 System Information.....	304
6.2.3 System Time.....	305
6.2.4 System Log .....	309
6.2.5 Backup & Restore .....	314
6.2.6 Reboot & Reset .....	315
6.3 FTP.....	316
6.3.1 Server Configuration.....	317
6.3.2 User Account.....	319
6.4 Diagnostics.....	320
6.4.1 Diagnostic Tools .....	320
6.4.2 Packet Analyzer .....	321
Chapter 7 Service.....	324
7.1 Cellular Toolkit .....	324
7.1.1 Data Usage .....	325
7.1.2 SMS.....	327
7.1.3 SIM PIN .....	331
7.1.4 USSD .....	335
7.1.5 Network Scan.....	338
7.2 SMS & Event .....	340
7.2.1 Configuration .....	342
7.2.2 Managing Events .....	353
7.2.3 Notifying Events .....	356
7.3 Azure Agent .....	359
7.3.1 Azure Configuration.....	359
7.3.2 EW-200 Azure Configuration .....	361
Chapter 8 Status .....	366
8.1 Dashboard .....	366
8.1.1 Device Dashboard.....	366
8.2 Basic Network.....	369
8.2.1 WAN & Uplink Status .....	369
8.2.2 LAN & VLAN Status .....	373

# EW200 Industrial Cellular Gateway

---

- 8.2.3 Wi-Fi Status ..... 374
  - 8.2.4 DDNS Status..... 377
- 8.3 Security ..... 378
  - 8.3.1 VPN Status..... 378
  - 8.3.2 Firewall Status ..... 382
- 8.4 Administration..... 386
  - 8.4.1 Configure & Manage Status..... 386
  - 8.4.2 Log Storage Status ..... 388
- 8.5 Statistics & Reports..... 389
  - 8.5.1 Connection Session..... 389
  - 8.5.2 Network Traffic..... 390
  - 8.5.3 Device Administration ..... 391
  - 8.5.4 Cellular Usage..... 392
  - 8.5.4 Cellular Signal ..... 393
- Specifications..... 394
- Contact Information ..... 397

## Chapter 1 Introduction

### 1.1 Introduction

Congratulations on your purchase of this product: Industrial Cellular Gateway. For M2M (Machine-to-Machine) applications, EtherWAN Cellular Gateway is the right choice.

With a built-in world-class 4G LTE module, just insert a SIM card from local mobile carrier to access the Internet. The dual SIM design provides redundancy and a reliable WAN connection for critical applications. Through VPN tunneling technology, remote sites easily become a part of the local Intranet, and all data is transmitted in a secure (256-bit AES encryption) link. The DI/DO feature allows the gateway to respond in real time to events detected by sensors.

This EW200 is equipped with a host of security features including VPN, firewall, NAT, port forwarding, DHCP server and other features for outdoor IP surveillance applications. Redundant 12-48 VDC power terminals and dual SIM cards ensure data transmission and network connection without loss.

Main Features:

- Built-in high speed LTE modem with dual SIMs for uplink traffic failover.
- Equipped with gigabit Ethernet ports to connect other IP-based devices.
- RS-232 serial port for controlling legacy serial devices or Modbus devices.
- Digital I/O ports for integrating sensors, switch, or other alarm devices.
- Equipped with 802.11a/b/g/n/ac 2T2R 2.4G/5GHz selectable Wi-Fi access point.
- Designed with solid and easy-to-mount metal body for industrial environments to work with a variety M2M (Machine-to-Machine) applications.

Before you install and use this product, please read this manual in detail.





# EW200 Industrial Cellular Gateway

---

## 1.2 Contents List

### 1.2.1 Package Contents

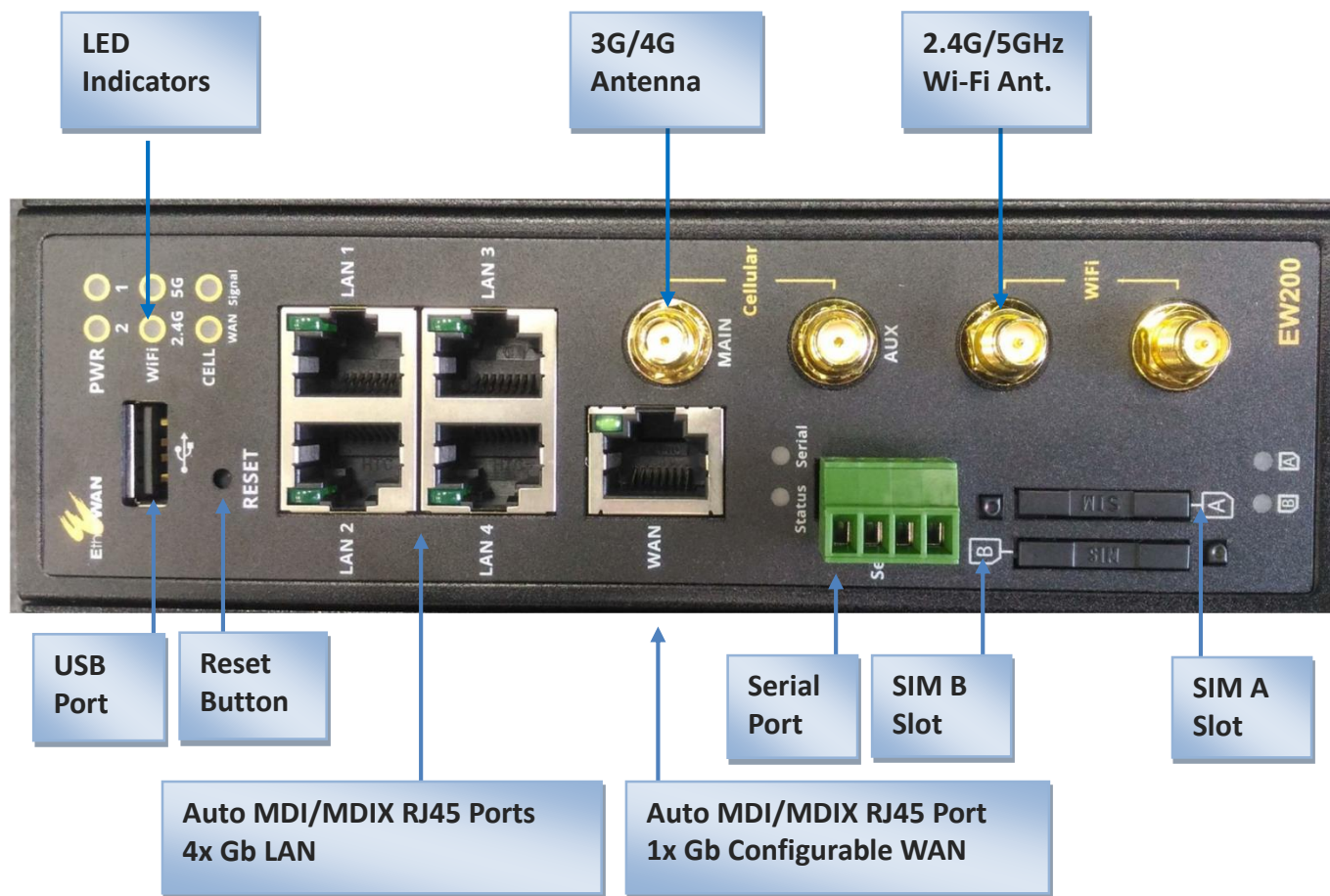
#### #Standard Package

Items	Description	Contents	Quantity
1	EW200 Industrial Cellular Gateway		1pcs
2	8 pin Terminal Block		1pcs
3	4 pin Terminal Block		1pcs
4	DIN-Rail Bracket		1pcs

# EW200 Industrial Cellular Gateway

## 1.3 Hardware Configuration

### ➤ Front View



#### ※ Reset Button

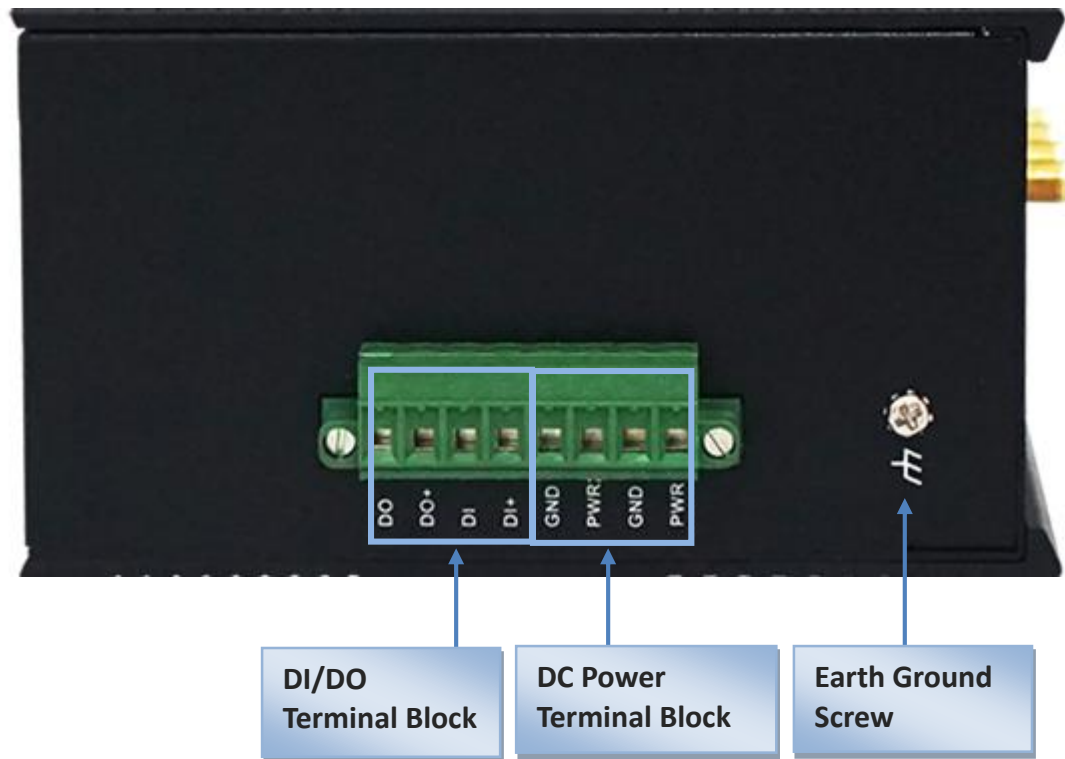
The RESET button provides a quick and easy way to restore the default settings. Press the RESET button continuously for 6 seconds, and then release it. The device will reset to factory default settings.

#### ※ 3G/4G, Wi-Fi Antenna

All the 3G/4G and 2.4G/5GHz Wi-Fi antennas are optional accessories, and are not included in the standard package. Purchase suitable antennas and required RF cables to fit your application.

# EW200 Industrial Cellular Gateway

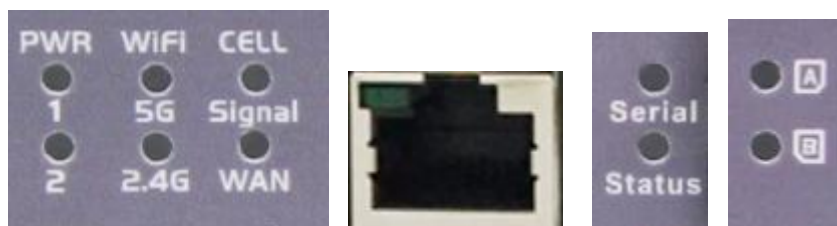
## ➤ Left View









# EW200 Industrial Cellular Gateway

## 1.4 LED Indicators



LED Icon	Indication	LED Color	Description
	Power Source 1	Blue	<b>Steady ON:</b> Device is powered on by power source 1
	Power Source 2	Blue	<b>Steady ON:</b> Device is powered on by power source 2
<b>Wi-Fi</b>	Wi-Fi 2.4G/5GHz	Blue	<b>OFF:</b> Wi-Fi is disabled <b>Steady ON:</b> Wi-Fi is enabled
<b>Signal</b>	Signal (Cellular)	Blue	<b>Steady On:</b> Signal Strength is 61~100% <b>Slow Flash (per Second):</b> Signal Strength is 31~60% <b>Fast Flash (per 0.5 second):</b> Signal Strength is 0~30%
<b>WAN</b>	WAN (Cellular)	Blue	<b>OFF:</b> No data packets transferred via Cellular interface <b>Flashing:</b> Data packets being transferred via Cellular interface
	LAN 1 ~ LAN 4/WAN	Green	<b>Steady ON:</b> Ethernet connection of LAN or WAN is established. <b>Flash:</b> Data packets are being transferred. <b>OFF:</b> No Ethernet cable attached or Device not linked.
<b>Serial</b>	Serial	Blue	<b>OFF:</b> No Serial data transferred via serial port <b>Flashing:</b> Data packets being transferred via Serial port
<b>Status</b>	Status	Blue	<b>Slow Flash (per Second):</b> Device working normally <b>Very Fast Flash:</b> Device is in Recovery Mode or abnormal state
	SIM A/B	Blue	<b>OFF:</b> SIM not detected <b>Slow Flash (per Second):</b> SIM A/B was chosen for the connection <b>Steady ON:</b> Cellular connection successfully established (under SIM A/B)

## 1.5 Installation & Maintenance

### 1.5.1 SYSTEM REQUIREMENTS

Network Requirements	<ul style="list-style-type: none"><li>• A gigabit Ethernet RJ45 cable</li><li>• 3G/4G cellular service subscription</li><li>• IEEE 802.11 a/b/g/n/ac wireless clients</li><li>• 10/100/1000 Ethernet adapter on PC</li></ul>
Web-based Configuration Utility Requirements	<p><b>Computer with the following:</b></p> <ul style="list-style-type: none"><li>• Windows®, Macintosh, or Linux-based operating system</li><li>• An installed Ethernet adapter</li></ul> <p><b>Browser Requirements:</b></p> <ul style="list-style-type: none"><li>• Internet Explorer 6.0 or higher</li><li>• Chrome 2.0 or higher</li><li>• Firefox 3.0 or higher</li><li>• Safari 3.0 or higher</li></ul>

### 1.5.2 WARNING



#### *Attention*

- Only use the power supply that complies with the power specification of the gateway. Using an out-of-spec voltage rating power source 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.

### 1.5.3 HOT SURFACE CAUTION



**CAUTION:** The surface temperature for the metallic enclosure can be very high! Especially after long periods of operation, when installed in a closed cabinet without air conditioning, or in a location with a high ambient temperature.

**DO NOT touch the hot surface!!**

# EW200 Industrial Cellular Gateway

## 1.5.4 Product Information for CE RED Requirements

The following product information is required to be presented in product User Manual for latest CE RED requirements.<sup>1</sup>

### (1) Frequency Band & Maximum Power

#### 1.a Frequency Band for Cellular Connection

Band number	Operating Frequency	Max output power
LTE FDD BAND 1	Uplink: 1920-1980 MHz Downlink: 2110-2170 MHz	23 ±2.7 dBm
LTE FDD BAND 3	Uplink: 1710-1785 MHz Downlink: 1805-1880 MHz	
LTE FDD BAND 7	Uplink: 2500-2570 MHz Downlink: 2620-2690 MHz	
LTE FDD BAND 8	Uplink: 880-915 MHz Downlink: 925-960 MHz	
LTE FDD BAND 20	Uplink: 832-862 MHz Downlink: 791-821 MHz	
WCDMA BAND 1	Uplink: 1920-1980 MHz Downlink: 2110-2170 MHz	24 +1/-3 dBm
WCDMA BAND 8	Uplink: 880-915 MHz Downlink: 925-960 MHz	
E-GSM	Uplink: 880-915 MHz Downlink: 925-960 MHz	33 ±2 dBm
DCS	Uplink: 1710-1785 MHz Downlink: 1805-1880 MHz	30 ±2 dBm

#### 1.b Frequency Band for Wi-Fi Connection

Band	Operating Frequency	Max. Output Power (EIRP)
2.4G	2.4 – 2.4835 GHz	100 mW
5G	5.15 – 5.25 GHz	200 mW

### (2) 5150 ~ 5350MHz Indoor Use Statements

This product is equipped with IEEE 802.11ac compliant 5GHz wireless radio module. According to RED requirements, the channels covered in the 5150 ~ 5350 MHz frequency band are for Indoor Use Only.

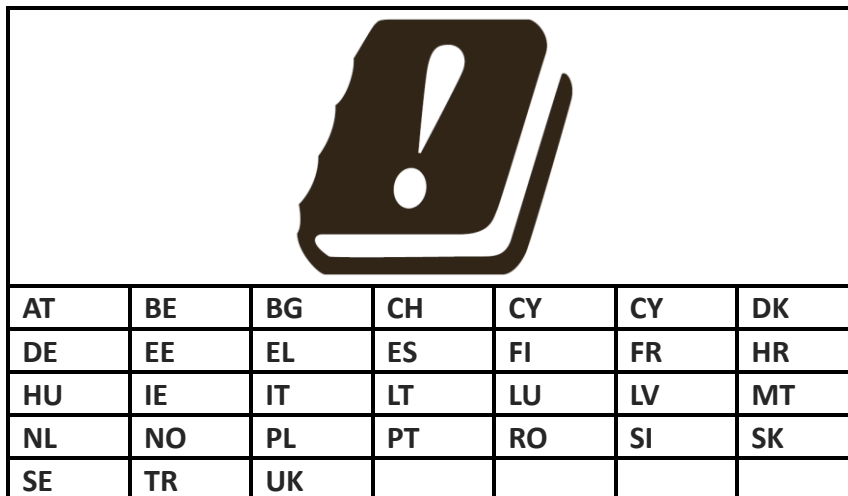
---

<sup>1</sup> The information presented in this section is ONLY valid for the EU/EFTA regional version. For non-CE/EFTA versions, please refer to the corresponding product specification.

# EW200 Industrial Cellular Gateway

## (3) Country List for Restrictions (for products with 5GHz radio)

For EU/EFTA, this product can be used in all EU member states and EFTA countries.



## (4) RF Exposure Statements

The antenna of the product, under normal use condition, should be at least 20 cm away from the body of user.

## (5) Unit Mounting Notice

The product is suitable for mounting at heights  $\leq 2\text{m}$  (approx. 6 ft), or in a cabinet. Ensure the unit is fixed tightly to reduce the chance of injury due to exposure to mechanical hazards if dropped.

# EW200 Industrial Cellular Gateway

## 1.6 Hardware Installation

This chapter describes how to install and configure the hardware

### 1.6.1 Mount the Unit

The EW200 series product can be mounted on a wall, horizontal plane, or DIN Rail in a cabinet with the mounting accessories (brackets or DIN-rail kit). The mounting accessories are not screwed on the product when shipped from factory. Screw the wall-mount kits or DIN-rail bracket on the product first.

### 1.6.2 Insert the SIM Card

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

The SIM card slots are located at the front side of the device housing. Push the button and pull the SIM card loader to install or remove the SIM card. After the SIM card is placed in the loader, push the SIM card loader into its slot.

#### Step 1:

Push the button with a pin to unlock and eject SIM socket.



#### Step 2:

Put SIM card in the socket firmly.



#### Step 3:

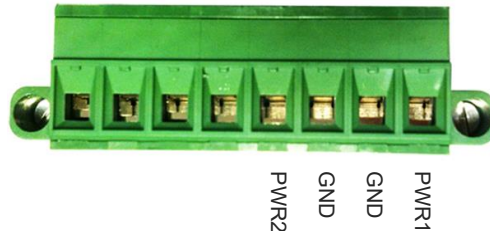
Put SIM socket back into the SIM slot.



# EW200 Industrial Cellular Gateway

## 1.6.3 Connecting Power

The EW200 series product can be powered by connecting one or two power sources to the terminal block. **It supports dual 12 to 48V DC power inputs.** The following picture indicates the power terminal block pin assignments. Please check carefully and connect to the right power requirements and polarity.



The dual power supplies PWR1 and PWR2 can be used in either primary/backup or concurrent modes, depending on the voltage for PWR1 and PWR2.

If the voltage difference between PWR1 and PWR2 is greater than 5.0 volts (this is the case for using two power supplies with the different external spec., such as 48V and 24V), the power control circuit works in primary / backup power mode. The one with higher voltage is treated as the primary power, and the other one is backup power. Normally, only the primary power supplies power to the gateway and connected PoE devices; the backup power supply will supply the power to the gateway and connected PoE devices only when the primary power fails.

If the voltage difference between PWR1 and PWR2 is less than 0.5 volts (this is the case for using two power supply with the same external spec., such as 48V), the power control circuit works in concurrent mode. Both PWR1 and PWR2 supply required power to the gateway and connected PoE devices simultaneously.

Make sure that the external power supply can supply the amount of power that the system requires. Failure to do so may result in a situation in which the power control circuit switches to concurrent mode so that PWR1 and PWR2 supply power at the same time.

## 1.6.4 Power Supply Installation

The power supply is an optional unit, and is not included in the standard package. You must purchase or prepare an external power supply for providing power to the gateway. Following is an example of the industrial power supply installation.


### ➤ AC Power Cable Installation

The power supply unit should be 100-240V AC, 50/60Hz with power input lines. AWG 18 power cable is recommended.

# EW200 Industrial Cellular Gateway



The terminal pin number assignment is shown below

Pin No.	Assignment
1	FG 
2	AC/N
3	AC/L

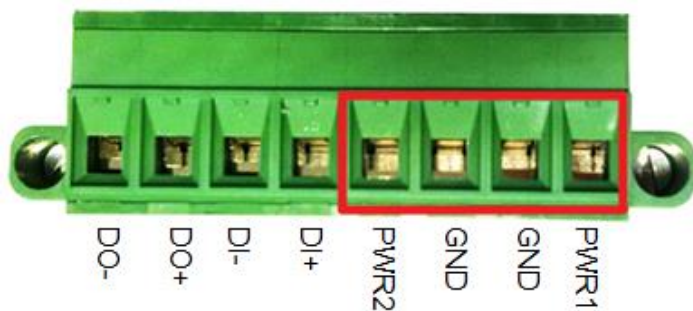
Connect the live line, neutral line and earth line to the corresponding locations.

## ➤ DC Power Terminal Block Installation

The Power Supply unit may consist of one set or two sets of DC power output contacts.



You can connect the DC power supply and the terminal block power pins, as shown below, of the gateway with a power cable. AWG 18 power cable is recommended.

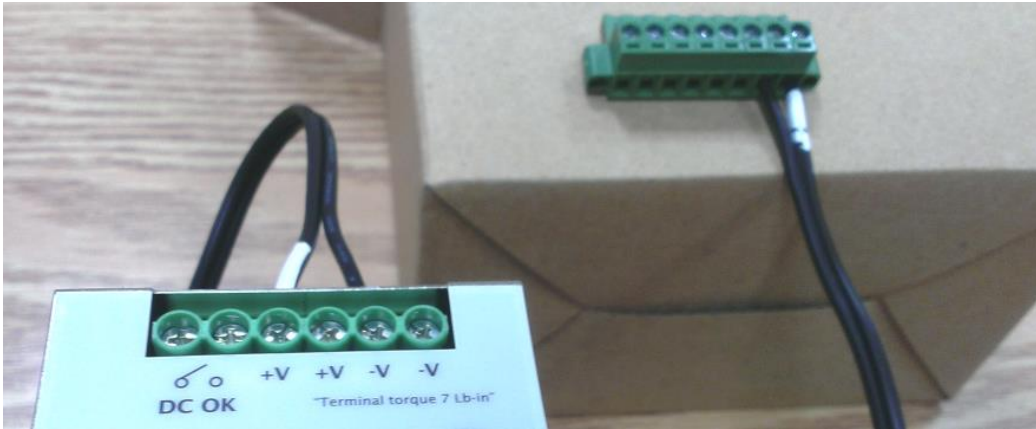


Insert DC power wires into the contacts PWR1 or PWR2. The +V connect to PWR and then -V connect to GND. After that, plug in the terminal block to the socket at the side of the gateway.



## EW200 Industrial Cellular Gateway

---



Finally, connect the power plug of the power supply cable to an outlet. The power supply units will turn on and provide DC power to the connected device.

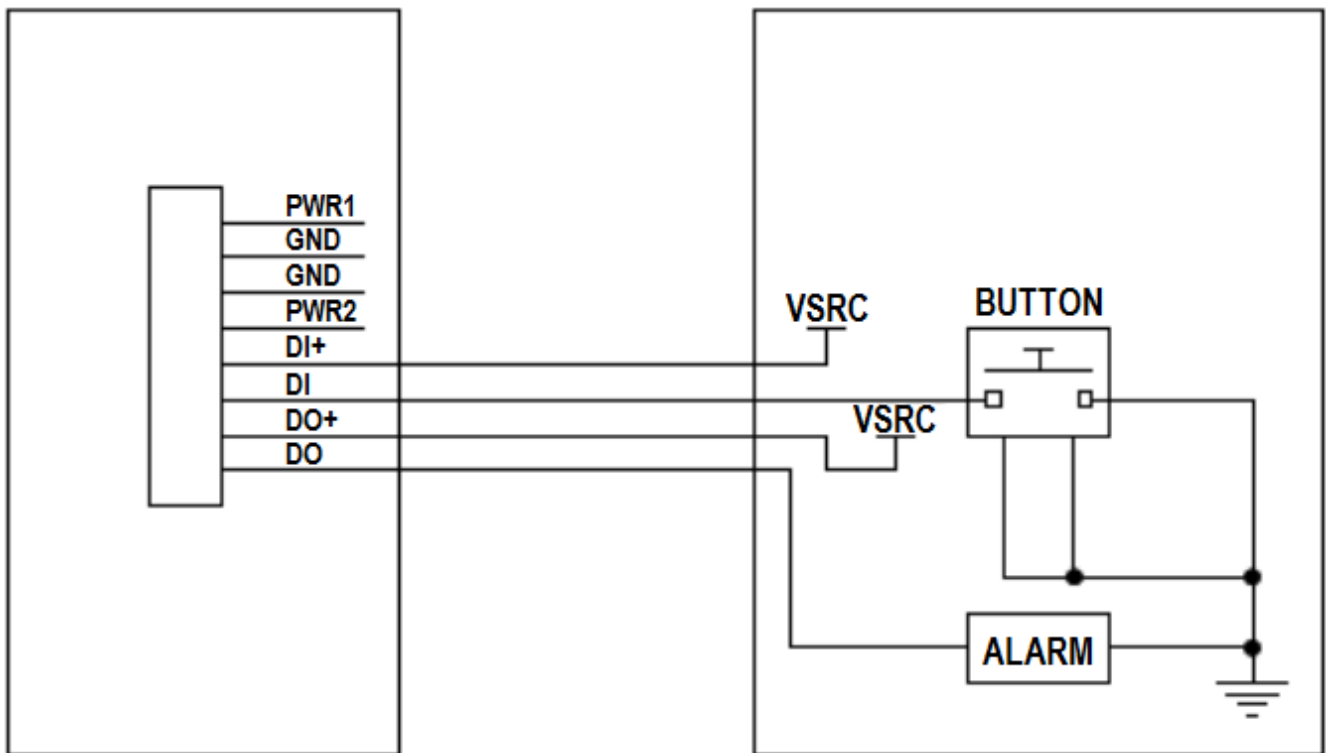
# EW200 Industrial Cellular Gateway

## 1.6.5 Connecting DI/DO Devices

There is one DI (digital input) and one DO (digital output) port next to the power terminal block. Refer to the following specification for connection of DI and DO devices.

Mode	Specification	
Digital Input	Trigger Voltage (high)	Logic level 1: 5V~30V
	Normal Voltage (low)	Logic level 0: 0V~2V
Digital Output	Voltage (Relay Mode)	Depends on external device Maximum voltage is 30V
	Maximum Current	1A

### Connection Diagram



# EW200 Industrial Cellular Gateway

---

## 1.6.6 Connecting Serial Devices

The EW200 has a 4-pin Terminal Block serial port for connecting to your serial device. Connect the serial device to the terminal block with the right pin assignments of RS-232/485 (shown below).



Pin 1   2   3   4

	Pin1	Pin2	Pin3	Pin4
RS-232	GND	RXD	TXD	GND
RS-485	GND	DATA-	DATA+	GND

## 1.6.7 Connecting to the Network or a Host

The EW200 provides RJ45 ports to connect 10/100/1000Mbps Ethernet. It can auto detect the transmission speed on the network and configure itself automatically. Connect one Ethernet cable to the RJ45 port (LAN) of the device and plug another end of the Ethernet cable into your computer's network port. In this way, you can use the RJ45 Ethernet cable to connect to the host PC's Ethernet port for configuring the device.

# EW200 Industrial Cellular Gateway

---

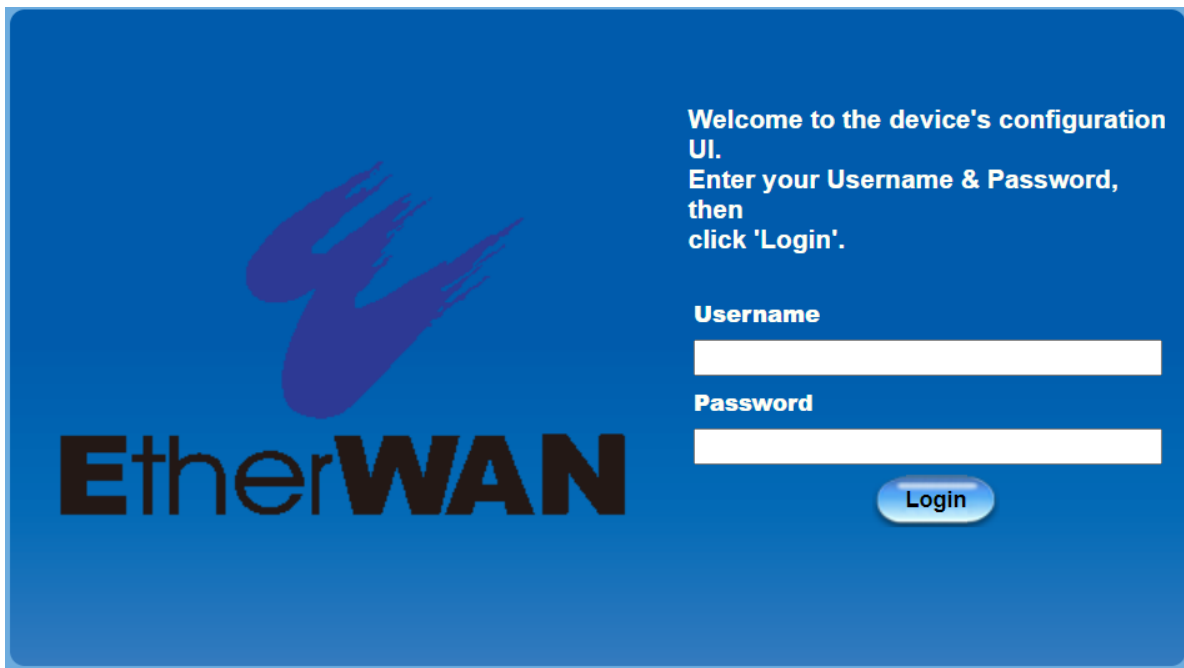
## 1.6.8 Setup by Configuring WEB UI

You can use the web UI to configure the device.

The IP Address is (<http://192.168.123.254>)<sup>2</sup>



When you see the login page, enter the default username and password '**admin**'<sup>3</sup> and then click the '**Login**' button.



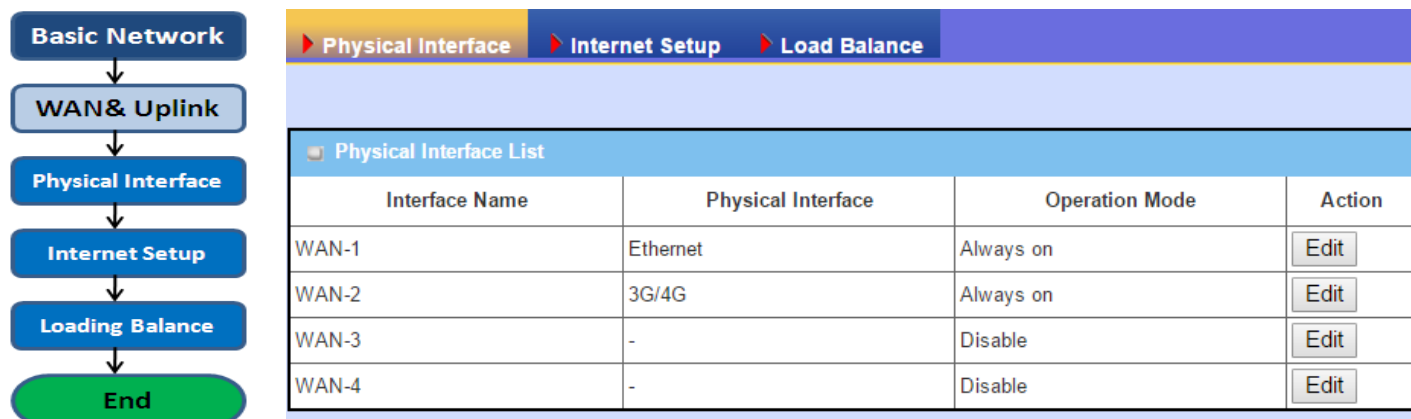
---

<sup>2</sup> The default LAN IP address of this gateway is 192.168.123.254. If you change it, you will need to log in using the new IP address.

<sup>3</sup> You will be requested by the system to change this login password from the default value.

## Chapter 2 Basic Network

### 2.1 WAN & Uplink

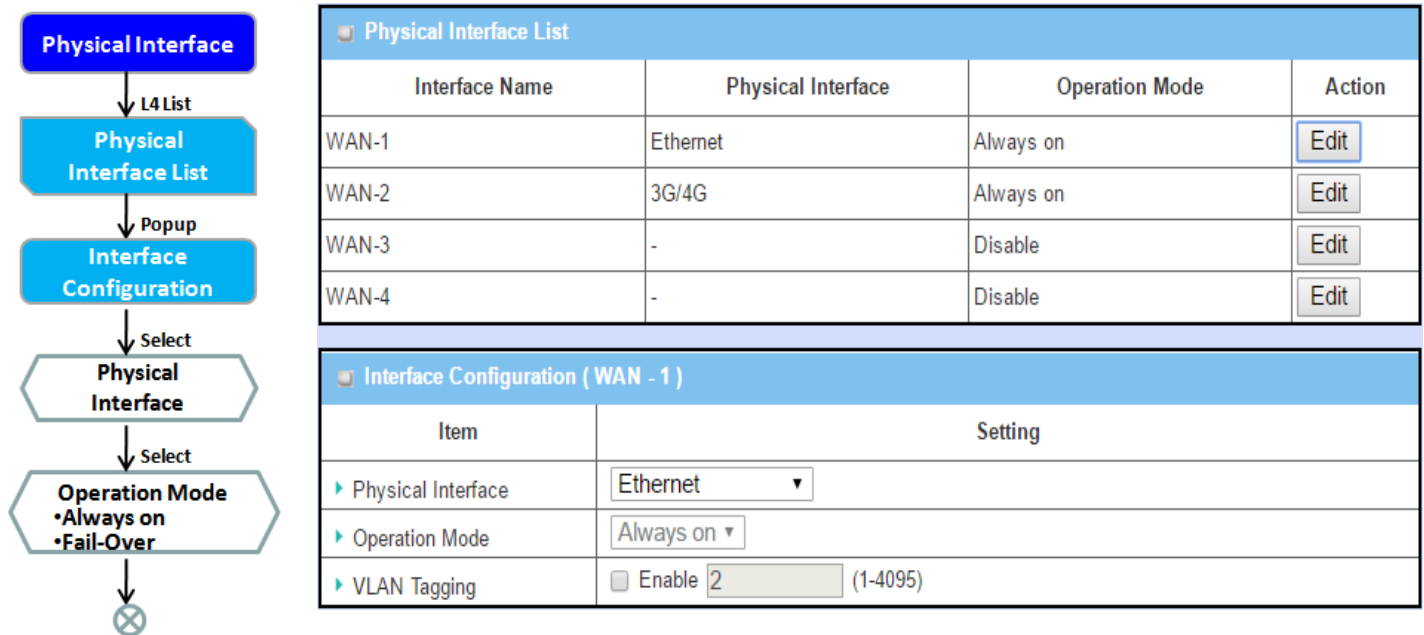


The gateway provides multiple WAN interfaces to let client hosts in the Intranet of the gateway access the Internet via ISP. But ISPs in the world apply various connection protocols to let gateways or user's devices dial in to ISPs and then link to the Internet via different kinds of media.

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. Since the gateway has multiple WAN interfaces, you can assign a physical interface to participate in the Load Balance function.

# EW200 Industrial Cellular Gateway

## 2.1.1 Physical Interface



M2M gateways are usually equipped with various WAN interfaces to support different WAN connection scenarios. You can configure the WAN interfaces one by one to get a proper internet connection setup. **Refer to the product specification for the available WAN interfaces in your model.**

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

In the "Physical Interface" page, there are two configuration windows, "Physical Interface List" and "Interface Configuration". The "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.

### Physical Interface:

- **Ethernet WAN:** The gateway has one or more RJ45 WAN ports that can be configured to be WAN connections. You can directly connect to external DSL modem or setup behind a firewall device.
- **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 card slots.

# EW200 Industrial Cellular Gateway



## Attention

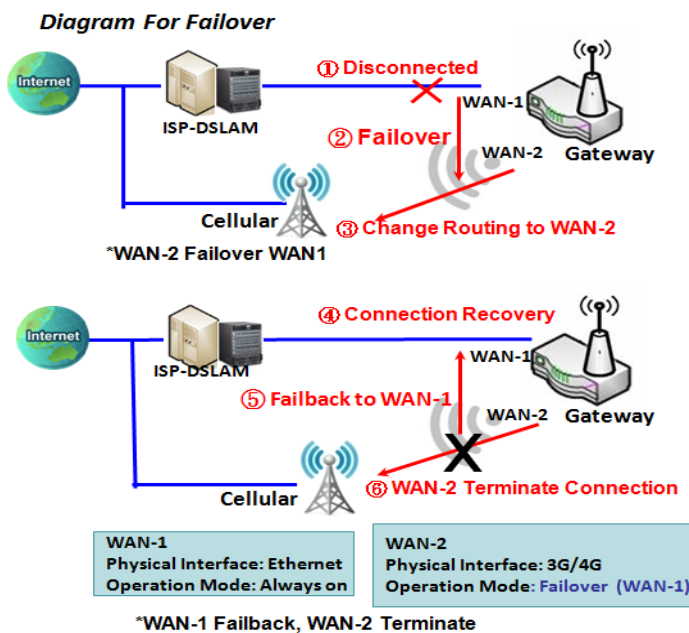
- POWER OFF the gateway before you insert or remove a SIM card.
- The SIM card can be damaged if you insert or remove SIM card while the gateway is in operation.

## Operation Mode:

There are three option items "Always on", "Failover", and "Disable" for the operation mode setting.

**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 pass through these WAN connections based on load balance policies.

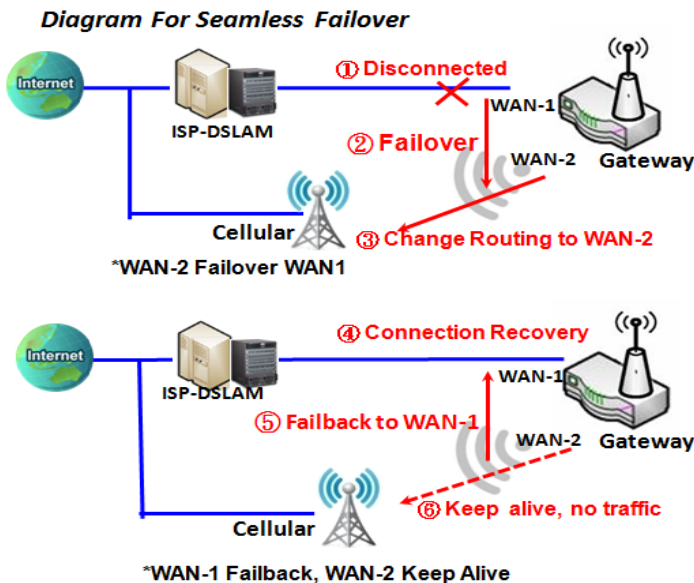
## Failover:



A failover interface is a backup connection to the primary. That means only when the primary WAN connection is broken, the backup connection will be started up to substitute the primary connection. As shown in the diagram, WAN-2 is backup WAN for WAN-1. WAN-1 serves as the primary connection with operation mode "Always on". WAN-2 won't be activated until WAN-1 is disconnected. When WAN-1 connection is recovered, it will take over data traffic again. At that time, WAN-2 connection will be terminated.

# EW200 Industrial Cellular Gateway

## Seamless Failover:



In addition, there is a "Seamless" option for Failover operation mode. When seamless option is activated by checking the "Seamless" box in the configuration window, both the primary connection and the failover connection are started up after system rebooting. But only the primary connection executes data transfer, while the failover one just keeps the connection alive. As soon as the primary connection is lost, the system will switch to the failover connection.

When the "Seamless" enable checkbox is activated, it can allow the Failover interface to be connected continuously from the time the system boots up. The failover WAN interface maintains the connection without transferring data traffic. This is to shorten the switch time during failover process. When the primary connection is disconnected, failover interface will

take over the data transfer mission instantly by only changing the routing path to the failover interface. The dialing-up time of failover connection is reduced since it has been connected beforehand.

## VLAN Tagging

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



# EW200 Industrial Cellular Gateway

---

## Physical Interface Setting

---

Go to **Basic Network > WAN > Physical Interface** tab.

The Physical Interface allows for the setup of the physical WAN interface and adjustment of WAN's behavior.

Note: Number of available WAN Interfaces varies by model.

Physical Interface List			
Interface Name	Physical Interface	Operation Mode	Action
WAN-1	Ethernet	Always on	<input type="button" value="Edit"/>
WAN-2	3G/4G	Always on	<input type="button" value="Edit"/>
WAN-3	-	Disable	<input type="button" value="Edit"/>
WAN-4	-	Disable	<input type="button" value="Edit"/>

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

# EW200 Industrial Cellular Gateway

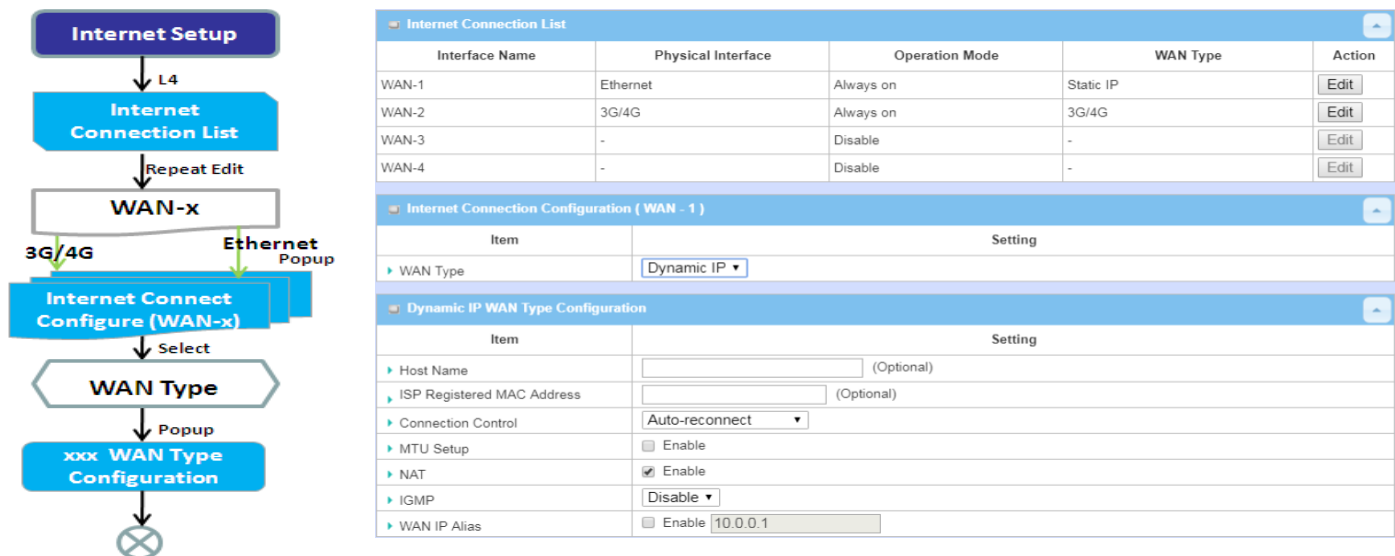
## Interface Configuration:

Interface Configuration ( WAN - 1 )	
Item	Setting
▶ Physical Interface	Ethernet ▼
▶ Operation Mode	Always on ▼
▶ VLAN Tagging	<input type="checkbox"/> Enable 2 (1-4095)

Interface Configuration		
Item	Value setting	Description
Physical Interface	1. Required setting 2. WAN-1 is the primary interface and is factory set to <b>Always on</b> .	Select one expected interface from the available interface dropdown list. Depending on the gateway model, <b>Disable</b> and <b>Failover</b> options will be available only to multiple WAN gateways. WAN-2 ~ WAN-4 interfaces are only available to multiple WAN gateways.
Operation Mode	Required setting	<p>Define the operation mode of the interface.</p> <p>Select <b>Always on</b> to make this WAN always active.</p> <p>Select <b>Disable</b> to disable this WAN interface.</p> <p>Select <b>Failover</b> to make this WAN a Failover WAN when the primary or the secondary WAN link fails. Then select the primary or the existing secondary WAN interface to switch Failover from.</p> <p>(Note: for WAN-1, only <b>Always on</b> option is available.)</p>
VLAN Tagging	Optional setting	<p>Check <b>Enable</b> box to enter tag value provided by your ISP. Otherwise uncheck the box.</p> <p><u>Value Range</u>: 1 ~ 4095.</p> <p>Note: This feature is NOT available for 3G/4G WAN connection.</p>

# EW200 Industrial Cellular Gateway

## 2.1.2 Internet Setup



After specifying the physical interface for each WAN connection, the connection profile must be configured to satisfy the dial-in process of the ISP, so that all client hosts in the Intranet of the gateway can access the Internet.

On the "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 the 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.

# EW200 Industrial Cellular Gateway

## Internet Connection List - Ethernet WAN

The diagram illustrates the configuration process for an Ethernet WAN connection. It starts with an 'Edit' button leading to 'Internet Connection List Physical Interface= Ethernet'. This leads to 'Internet Connect Configure', then 'Select one' to 'WAN Type='. A dropdown menu shows options: Dynamic IP, Static IP, PPPoE, L2TP, and PPTP. An arrow labeled 'L4 Setup' points to 'XXX WAN Type Configuration', which then leads to 'Ethernet Connection Common Configure' via another 'L4 Setup' arrow, ending at a save icon.

Internet Connection Configuration ( WAN - 1 )	
Item	Setting
WAN Type	Dynamic IP ▼ Static IP
Dynamic IP WAN Type Configuration	
Item	Setting
Host Name	(Optional)
ISP Registered MAC Address	<input type="text"/> Clone (Optional)
Connection Control	Auto-reconnect ▼
MTU Setup	<input type="checkbox"/> Enable
NAT	<input checked="" type="checkbox"/> Enable
IGMP	Disable ▼
WAN IP Alias	<input type="checkbox"/> Enable 10.0.0.1

Network Monitoring Configuration	
Item	Setting
Network Monitoring Configuration	<input checked="" type="checkbox"/> Enable
Checking Method	DNS Query ▼
Loading Check	<input checked="" type="checkbox"/> Enable
Query Interval	5 (seconds)
Latency Threshold	3000 (ms)

### WAN Type for Ethernet Interface:

Ethernet is the most common WAN and uplink interface for M2M gateways. Usually it is connected with xDSL or cable modem for you to setup the WAN connection. There are various WAN types for connection with an ISP.

- **Static IP:** Select this option if the ISP provides a fixed IP. This is usually is more expensive, but important for cooperate requirements.
- **Dynamic IP:** The assigned IP address for the WAN by a DHCP server is different every time. This is cheaper and usually for consumer use.
- **PPP over Ethernet:** As known as PPPoE. This WAN type is widely used for ADSL connection. IP is usually different for every dial up.
- **PPTP:** This WAN type is popular in some countries, like Russia.
- **L2TP:** This WAN type is popular in some countries, like Israel.

### Configure Ethernet WAN Setting

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

# EW200 Industrial Cellular Gateway

## WAN Type = Dynamic IP

Internet Connection Configuration ( WAN - 1 )	
Item	Setting
▶ WAN Type	Dynamic IP ▼

When selected, "Dynamic IP WAN Type Configuration" will appear. Items and settings are explained below

Dynamic IP WAN Type Configuration	
Item	Setting
▶ Host Name	<input type="text"/> (Optional)
▶ ISP Registered MAC Address	<input type="text"/> <input type="button" value="Clone"/> (Optional)

Dynamic IP WAN Type Configuration		
Item	Value setting	Description
Host Name	Optional setting	Enter the host name provided by your service provider.
ISP Registered MAC Address	Optional setting	Enter the MAC address that you have registered with your service provider. Or Click the <b>Clone</b> button to clone your PC's MAC to this field. Usually this is the PC's MAC address assigned to allow you to connect to the Internet.

## WAN Type= Static IP

Internet Connection Configuration ( WAN - 1 )	
Item	Setting
▶ WAN Type	Static IP ▼

When selected, "Static IP WAN Type Configuration" will appear. Items and settings are explained below

Static IP WAN Type Configuration	
Item	Setting
▶ WAN IP Address	<input type="text"/>
▶ WAN Subnet Mask	255.255.255.0 (/24) ▼
▶ WAN Gateway	<input type="text"/>
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/> (Optional)

# EW200 Industrial Cellular Gateway

Static IP WAN Type Configuration		
Item	Value setting	Description
<b>WAN IP Address</b>	Required setting	Enter the WAN IP address given by your service provider
<b>WAN Subnet Mask</b>	Required setting	Enter the WAN subnet mask given by your service provider
<b>WAN Gateway</b>	Required setting	Enter the WAN gateway IP address given by your service provider
<b>Primary DNS</b>	Required setting	Enter the primary WAN DNS IP address given by your service provider
<b>Secondary DNS</b>	Optional setting	Enter the secondary WAN DNS IP address given by your service provider

## WAN Type= PPPoE

Internet Connection Configuration ( WAN - 1 )	
Item	Setting
▶ WAN Type	PPPoE ▼

When selected, "PPPoE WAN Type Configuration" will appear. Items and settings are explained below

PPPoE WAN Type Configuration	
Item	Setting
▶ IP Type	IPv4 ▼
▶ PPPoE Account	<input type="text"/>
▶ PPPoE Password	<input type="text"/>
▶ Primary DNS	<input type="text"/> (Optional)
▶ Secondary DNS	<input type="text"/> (Optional)
▶ Service Name	<input type="text"/> (Optional)
▶ Assigned IP Address	<input type="text"/> (Optional)

PPPoE WAN Type Configuration		
Item	Value setting	Description
<b>PPPoE Account</b>	Required setting	Enter the PPPoE User Name provided by your service provider.
<b>PPPoE Password</b>	Required setting	Enter the PPPoE password provided by your service provider.
<b>Primary DNS</b>	Optional setting	Enter the IP address of Primary DNS server.
<b>Secondary DNS</b>	Optional setting	Enter the IP address of Secondary DNS server.
<b>Service Name</b>	Optional setting	Enter the service name if your ISP requires it
<b>Assigned IP Address</b>	Optional setting	Enter the IP address assigned by your service provider.

# EW200 Industrial Cellular Gateway

## WAN Type= PPTP

Internet Connection Configuration ( WAN - 1 )	
Item	Setting
▶ WAN Type	PPTP ▼

When selected, "PPTP WAN Type Configuration" will appear. Items and settings are explained below

PPTP WAN Type Configuration	
Item	Setting
▶ IP Mode	Dynamic IP Address ▼
▶ Server IP Address / Name	<input type="text"/>
▶ PPTP Account	<input type="text"/>
▶ PPTP Password	<input type="text"/>
▶ Connection ID	<input type="text"/> (Optional)
▶ MPPE	<input type="checkbox"/> Enable

PPTP WAN Type Configuration		
Item	Value setting	Description
IP Mode	Required setting	<p>Select either Static or Dynamic IP address for PPTP Internet connection.</p> <ul style="list-style-type: none"> <li>When <b>Static IP Address</b> is selected, you will need to enter the <b>WAN IP Address</b>, <b>WAN Subnet Mask</b>, and <b>WAN Gateway</b>. <ul style="list-style-type: none"> <li><b>WAN IP Address</b> (Required setting): Enter the WAN IP address given by your service provider.</li> <li><b>WAN Subnet Mask</b> (Required setting): Enter the WAN subnet mask given by your service provider.</li> <li><b>WAN Gateway</b> (Required setting): Enter the WAN gateway IP address given by your service provider.</li> </ul> </li> <li>When <b>Dynamic IP</b> is selected, the above settings are not required.</li> </ul>
Server IP Address/Name	Required setting	Enter the PPTP server name or IP Address.
PPTP Account	Required setting	Enter the PPTP username provided by your service provider.
PPTP Password	Required setting	Enter the PPTP connection password provided by your service provider.
Connection ID	Optional setting	Enter a name to identify the PPTP connection.
MPPE	Optional setting	Select <b>Enable</b> to enable MPPE (Microsoft Point-to-Point Encryption) security for PPTP connection.

# EW200 Industrial Cellular Gateway

## WAN Type= L2TP

Internet Connection Configuration ( WAN - 1 )	
Item	Setting
▶ WAN Type	L2TP ▼

When selected, "L2TP WAN Type Configuration" will appear. Items and settings are explained below

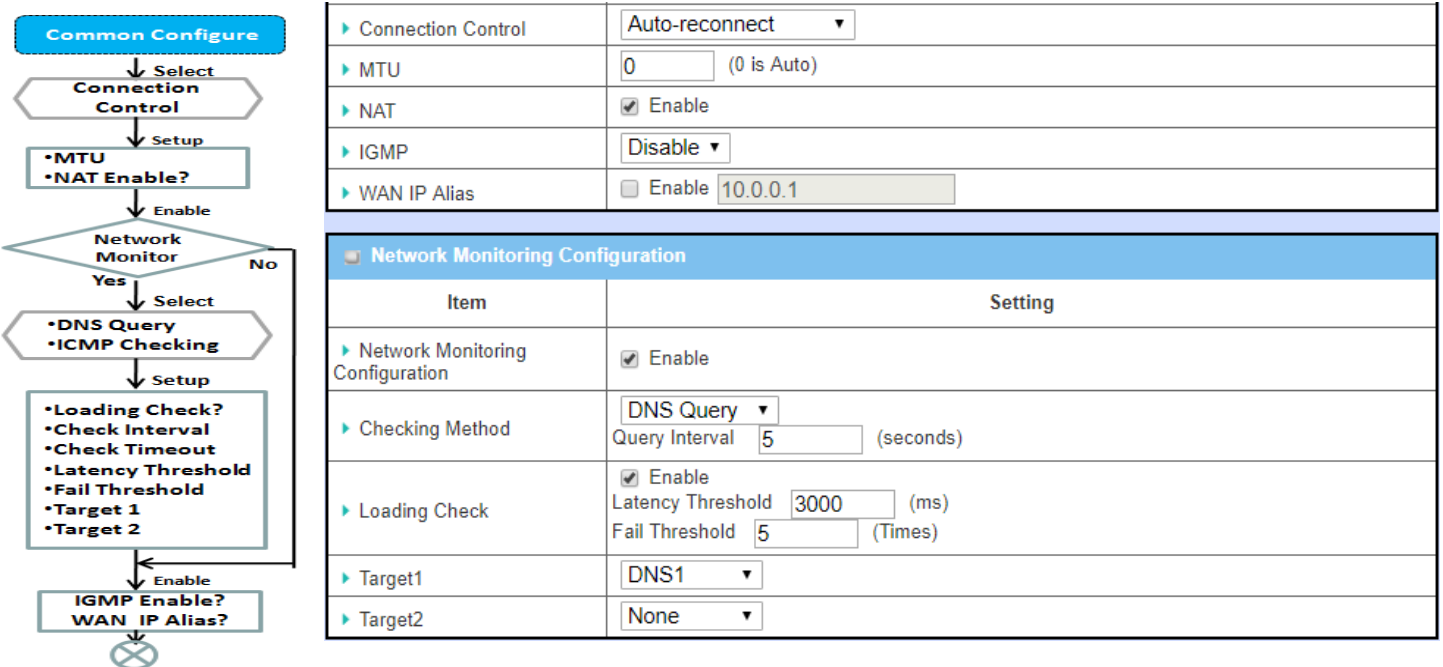
L2TP WAN Type Configuration	
Item	Setting
▶ IP Mode	Dynamic IP Address ▼
▶ Server IP Address / Name	<input type="text"/>
▶ L2TP Account	<input type="text"/>
▶ L2TP Password	<input type="text"/>
▶ Service Port	User-defined ▼ <input type="text" value="1702"/>
▶ MPPE	<input type="checkbox"/> Enable

L2TP WAN Type Configuration		
Item	Value setting	Description
IP Mode	Required setting	<p>Select either Static or Dynamic IP address for L2TP Internet connection.</p> <ul style="list-style-type: none"> <li>When <b>Static IP Address</b> is selected, you will need to enter the <b>WAN IP Address</b>, <b>WAN Subnet Mask</b>, and <b>WAN Gateway</b>. <ul style="list-style-type: none"> <li><b>WAN IP Address</b> (Required setting): Enter the WAN IP address given by your service provider.</li> <li><b>WAN Subnet Mask</b> (Required setting): Enter the WAN subnet mask given by your service provider.</li> <li><b>WAN Gateway</b> (Required setting): Enter the WAN gateway IP address given by your service provider.</li> </ul> </li> <li>When <b>Dynamic IP</b> is selected, the above settings are not required.</li> </ul>
Server IP Address/Name	Required setting	Enter the L2TP server name or IP Address.
L2TP Account	Required setting	Enter the L2TP username provided by your service provider.
L2TP Password	Required setting	Enter the L2TP connection password provided by your service provider.
Service Port	Required setting	<p>Enter the service port for the Internet service.</p> <p>There are three options:</p> <ul style="list-style-type: none"> <li><b>Auto:</b> Port will be automatically assigned.</li> <li><b>1701 (For Cisco):</b> Set service port to port 1701 to connect to CISCO server.</li> <li><b>User-defined:</b> enter a service port provided by your service provider.</li> </ul>
MPPE	Optional setting	Select <b>Enable</b> to enable MPPE (Microsoft Point-to-Point Encryption) security for PPTP connection.



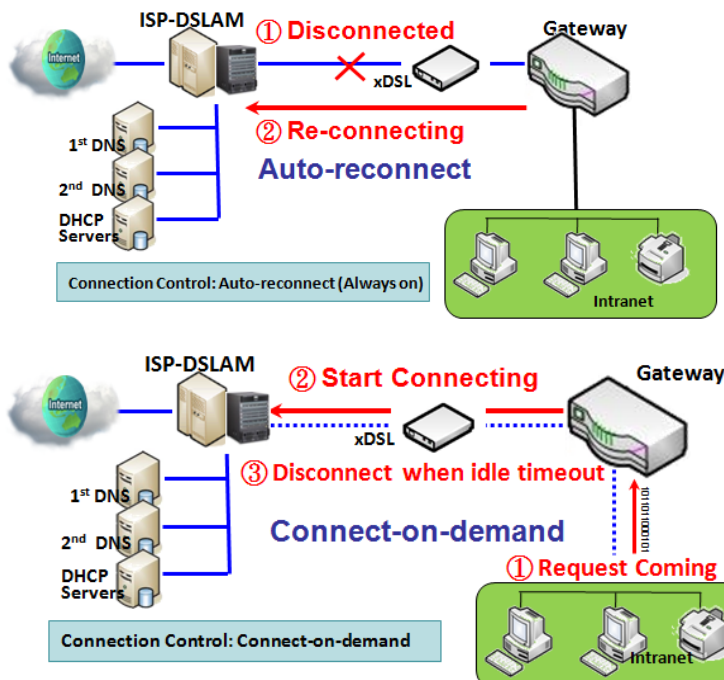
# EW200 Industrial Cellular Gateway

## Ethernet Connection Common Configuration



There are some important parameters to be set up no matter which type of WAN is selected.

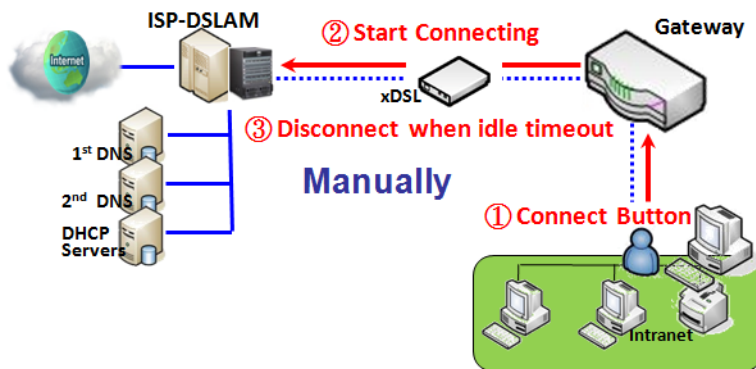
## Connection Control



**Auto-reconnect:** The gateway will establish an Internet connection automatically once it has been booted up, and try to reconnect once the connection is down. It is recommended to choose this scheme for mission critical applications to ensure full-time Internet connection.

**Connect-on-demand:** The gateway will not start to establish an Internet connection until local data is going to be sent to the WAN side. After normal data transfer between LAN and WAN sides, this gateway will disconnect the WAN connection if idle time reaches value of **Maximum Idle Time**.

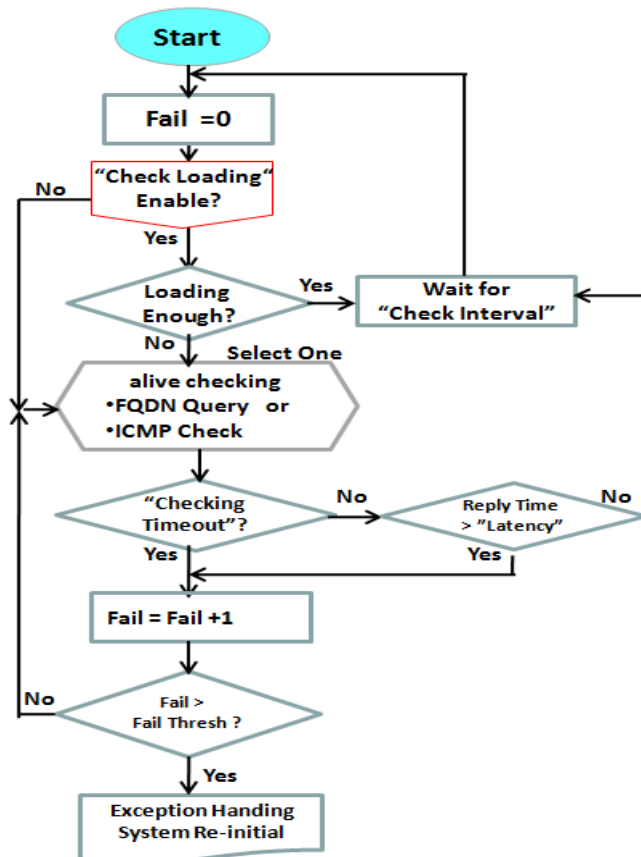
# EW200 Industrial Cellular Gateway



**Manually:** This gateway will not start to establish a WAN connection until the “Connect” button in web UI is pressed. After normal data transfer between LAN and WAN sides, this gateway will disconnect if idle time reaches value of **Maximum Idle Time**.

Note: If the WAN interface serves as the primary one for another WAN interface in Failover role, the Connection Control parameter will not be available on both WANs as the system must set it to “Auto-reconnect”.

## Network Monitoring



When it is necessary to monitor connection status continuously, "ICMP Check" and "FQDN Query" are used. When there is high connection traffic, checking packets will waste bandwidth, and the response time of replied packets may also increase. To prevent "Network Monitoring" from working abnormally, enabling the "Checking Loading" option will stop connection checking when there is high traffic. It will wait for another "Check Interval" and then check loading again.

When you do "Network Monitoring", if the reply time is longer than "Latency" or no response time is longer than "Checking Timeout", the "Fail" count will be increased. If it is continuous and "Fail" count is more than the configured "Fail Threshold", the gateway will do an exception handling process and re-initialize the connection again. Otherwise, network monitoring process will restart.

# EW200 Industrial Cellular Gateway

## Set up “Ethernet Common Configuration”

Ethernet WAN Common Configuration		
Item	Value setting	Description
Connection Control	Required setting	<p>There are three connection modes.</p> <ul style="list-style-type: none"><li>• <b>Auto-reconnect</b> enables the router to always keep the Internet connection on.</li><li>• <b>Connect-on-demand</b> enables the router to automatically re-establish Internet connection as soon as user attempts to access the Internet. Internet connection will be disconnected when it has been inactive for a specified idle time.</li><li>• <b>Connect Manually</b> allows user to connect to Internet manually. Internet connection will be inactive after it has been inactive for specified idle time.</li></ul> <p><b>Note:</b> If the WAN interface serves as the primary one for another WAN interface in Failover role (and vice versa), the Connection Control parameter will not be available on both WANs as the system must set it to “Auto-reconnect”</p>
Maximum Idle Time	1. Optional setting 2. <b>600</b> seconds is default	<p>Specify the Maximum Idle Time setting to disconnect the internet connection when the connection idle times out.</p> <p><b>Value Range:</b> 300 ~ 86400.</p> <p><b>Note:</b> This field is available only when <b>Connect-on-demand</b> or <b>Connect Manually</b> is selected as the connection control scheme.</p>
MTU	1. Required setting 2. <b>Auto(0)</b> is set by default 3. Manual set range 1200~1500	<p><b>MTU</b> refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission.</p> <p>When set to <b>Auto</b> (value '0'), the router selects the best MTU for best Internet connection performance.</p>
NAT	1. Optional setting 2. NAT is enabled by default	<p>Enable NAT (Network Address Translation) on the WAN connection.</p> <p>Uncheck the box to disable NAT.</p>
IGMP	1. Required setting 2. Disable is set by default	<p>Enable IGMP (Internet Group Management Protocol) to enable the router to listen to IGMP packets to discover which interfaces are connected to which device. The router uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.</p>
WAN IP Alias	1. Optional setting 2. Box is unchecked by default	<p>Enable <b>WAN IP Alias</b> then enter the IP address provided by your service provider.</p> <p><b>WAN IP Alias</b> is used by the device router and is treated as a second set of WAN IP to provide dual WAN IP address to your LAN network.</p>
Save	N/A	Click <b>Save</b> to save the settings.
Undo	N/A	Click <b>Undo</b> to cancel the settings.

# EW200 Industrial Cellular Gateway

Network Monitoring Configuration	
Item	Setting
▶ Network Monitoring Configuration	<input checked="" type="checkbox"/> Enable
▶ Checking Method	DNS Query ▼
▶ Loading Check	<input checked="" type="checkbox"/> Enable
▶ Query Interval	5 (seconds)
▶ Latency Threshold	3000 (ms)
▶ Fail Threshold	5 (Times)
▶ Target1	DNS1 ▼
▶ Target2	None ▼

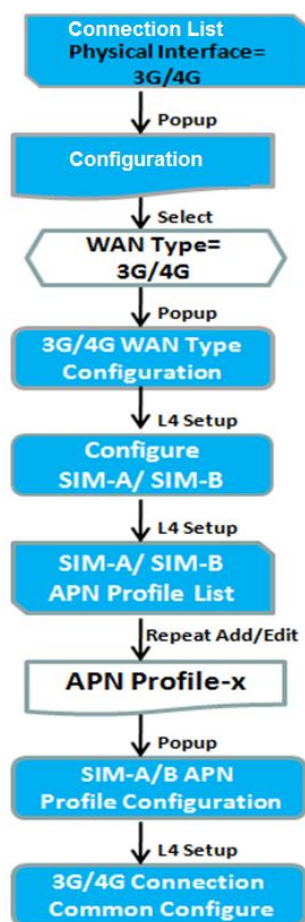
Network Monitoring Configuration		
Item	Value setting	Description
Network Monitoring Configuration	1. Optional setting 2. Box is checked by default	Check the <b>Enable</b> box to activate the network monitoring function.
Checking Method	1. Optional setting 2. <b>DNS Query</b> is set by default	<p>Choose either <b>DNS Query</b> or <b>ICMP Checking</b> to detect WAN link. With <b>DNS Query</b>, the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. With <b>ICMP Checking</b>, the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2.</p> <p><b>Query Interval</b> defines the transmitting interval between two DNS Query or ICMP checking packets.</p>
Loading Check	1. Optional setting 2. Box is checked by default	<p>Check the <b>Enable</b> box to activate the loading check function. Enable Loading Check allows the gateway to ignore unreturned DNS queries or ICMP requests when WAN bandwidth is fully occupied. This is to prevent false link-down status.</p> <p><b>Latency Threshold</b> defines the tolerance threshold of responding time. <b>Fail Threshold</b> specifies the number of detected disconnections before the router recognizes the WAN link down status. Enter a number of detected disconnection times as the threshold for disconnection.</p>
Query Interval	1. Optional setting 2. 5 seconds is selected by default.	<p>Specify a time interval as the <b>DNS Query Interval</b>. <b>Query Interval</b> defines the transmitting interval between two DNS Query or ICMP checking packets. With <b>DNS Query</b>, the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. <b>Value Range:</b> 2 ~ 14400.</p>
Check Interval	1. Optional setting 2. 5 seconds is selected by default.	<p>Specify a time interval as the <b>ICMP Checking Interval</b>. <b>Query Interval</b> defines the transmitting interval between two DNS Query or ICMP checking packets. With <b>ICMP Checking</b>, the system will check connection by sending ICMP</p>

# EW200 Industrial Cellular Gateway

		request packets to the destination specified in Target 1 and Target 2. <b>Value Range:</b> 2 ~ 14400.
<b>Latency Threshold</b>	1. Optional setting 2. 3000 ms is set by default	Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged. <b>Latency Threshold</b> defines the tolerance threshold of responding time. <b>Value Range:</b> 2000 ~ 3000 seconds.
<b>Fail Threshold</b>	1. Optional setting 2. 5 times is set by default	Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged. <b>Fail Threshold</b> specifies the detected disconnection before the router recognize the WAN link down status. <b>Value Range:</b> 1 ~ 10 times.
<b>Target 1</b>	1. Optional setting 2. <b>DNS1</b> is selected by default	<b>Target1</b> specifies the first target of sending DNS query/ICMP request. <b>DNS1:</b> set the primary DNS to be the target. <b>DNS2:</b> set the secondary DNS to be the target. <b>Gateway:</b> set the Current gateway to be the target. <b>Other Host:</b> enter an IP address to be the target.
<b>Target 2</b>	1. Optional setting 2. <b>None</b> is selected by default	<b>Target1</b> specifies the second target of sending DNS query/ICMP requests. <b>None:</b> no second target is required. <b>DNS1:</b> set the primary DNS to be the target. <b>DNS2:</b> set the secondary DNS to be the target. <b>Gateway:</b> set the Current gateway to be the target. <b>Other Host:</b> enter an IP address to be the target.
<b>Save</b>	N/A	Click <b>Save</b> to save the settings.
<b>Undo</b>	N/A	Click <b>Undo</b> to cancel the settings.

# EW200 Industrial Cellular Gateway

## Internet Connection – 3G/4G WAN



Internet Connection Configuration ( WAN - 2 )	
Item	Setting
WAN Type	3G/4G ▼
3G/4G WAN Type Configuration	
Preferred SIM Card	SIM-A First ▼ Failback : <input type="checkbox"/> Enable
Auto Flight Mode	<input type="checkbox"/> Enable
SIM Switch Policy	Policy Setting
Connection with SIM-A Card	
Connection with SIM-B Card	
3G/4G Connection Common Configuration	
Item	Setting
Connection Control	Auto-reconnect ▼
Time Schedule	(0) Always ▼
MTU Setup	<input type="checkbox"/> Enable

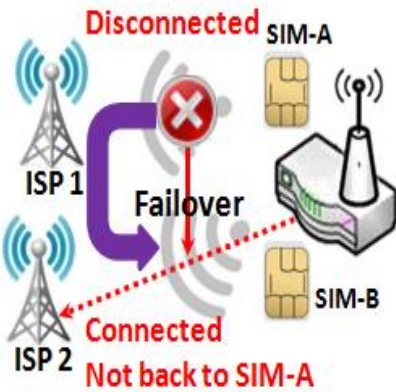
### Preferred SIM Card – Dual SIM Failover

For 3G/4G embedded devices, one embedded cellular module can create only one WAN interface. This device features 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”.

# EW200 Industrial Cellular Gateway

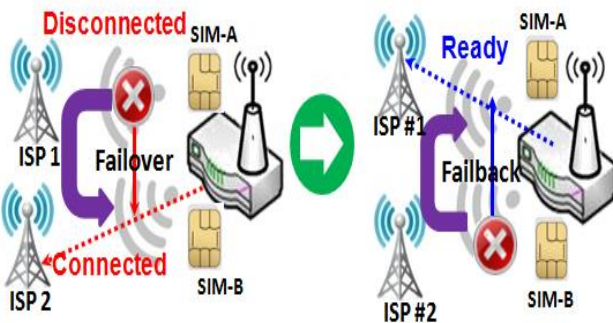
**SIM-A/SIM-B only:** When “SIM-A Only” or “SIM-B Only” is used, the specified SIM slot card is the only one to be used for negotiation parameters between gateway device and cellular ISP.

## SIM-A / SIM-B first without Failback enabled



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. If the connection is broken, the gateway will automatically switch to use the other SIM card as an alternate and **will not switch back** to use original SIM card except when the 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 enabled



With Failback option enabled, “SIM-A First” scenario is used to connect when the connection is broken, and the 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

## Configure 3G/4G WAN Setting

When **Edit** button is applied, **Internet Connection Configuration**, and **3G/4G WAN Configuration** screens will appear. WAN-2 interface is used in this example.

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 : <input type="checkbox"/> Enable
▶ Auto Flight Mode	<input type="checkbox"/> Enable
▶ SIM Switch Policy	Policy Setting



# EW200 Industrial Cellular Gateway

3G/4G Connection Configuration		
Item	Value setting	Description
<b>WAN Type</b>	1. Required setting 2. <b>3G/4G</b> is set by default.	From the dropdown box, select the Internet connection method for 3G/4G WAN Connection. Only <b>3G/4G</b> is available.
<b>Preferred SIM Card</b>	1. Required setting 2. By default <b>SIM-A First</b> is selected 3. <b>Failback</b> is unchecked by default	<p>Choose which SIM card you want to use for the connection.</p> <p>When <b>SIM-A First</b> or <b>SIM-B First</b> is selected, it means the connection is built first by using SIM A/SIM B. If the connection fails, it will switch to the other SIM card and try to dial again, until the connection is up.</p> <p>When <b>SIM-A only</b> or <b>SIM-B only</b> is selected, it will try to dial up only using the SIM card you selected.</p> <p>When <b>Failback</b> 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.</p> <p><b>Note_1:</b> For product with a single SIM design, only <b>SIM-A Only</b> option is available.</p> <p><b>Note_2:</b> <b>Failback</b> is available only when <b>SIM-A First</b> or <b>SIM-B First</b> is selected.</p>
<b>Auto Flight Mode</b>	Unchecked by default	<p>Check the <b>Enable</b> box to activate the function.</p> <p>By default, if you disabled the <b>Auto Flight Mode</b>, the cellular module will always occupy a physical channel with cellular tower. It can get data connection instantly, and receive managing SMS all the time on required.</p> <p>If you enable the <b>Auto Flight Mode</b>, the gateway will pop up a message "Flight mode will cause cellular function to be malfunctioned when the data session is offline." , and it will make the cellular module into flight mode and disconnected with cellular tower physically. In addition, whenever the cellular module is going to be used for data connection to backup the failed primary connection, the cellular module will be active to connect with cellular tower and get the data connection for use, It takes few more seconds.</p> <p><b>Note:</b> Keep it unchecked unless your cellular ISP asked the connected gateway to enable the Auto Flight Mode.</p>
<b>SIM Switch Policy</b>		Click the <b>Policy Setting</b> button to define the SIM switch policy or browse the current policy settings.

## SIM Switch Policy Settings

Policy Setting	
Item	Setting
▶ Failed connection	<input type="text" value="0"/> (1-10) times
▶ RSSI Monitor	<input type="checkbox"/> Enable Threshold: - <input type="text" value="0"/> (-90~-113 dBm)
▶ Network Service	<input type="checkbox"/> Enable Loss LTE signal: <input type="text" value="0"/> (1~30 minutes)
▶ Roaming Service	<input type="checkbox"/> Enable Timeout: <input type="text" value="0"/> (1~30 minutes)

Policy Setting		
Item	Value setting	Description
<b>Failed connection</b>	1. Required setting 2. <b>0</b> is set by default.	When the number of disconnections reaches the set value, it will switch to another sim card.



# EW200 Industrial Cellular Gateway

		For example, if a value of 2 is entered, and the system cannot connect for two times in a row, then it will switch to the other sim card.
<b>RSSI Monitor</b>	1. Unchecked by default	Click to enable, and set a value between -90~-113 dBm. When the signal strength goes below the set value, it will switch to the other sim card.
<b>Network Service</b>	Unchecked by default	Click to enable, and enter a time in minutes between 1 and 30. When the time of lost LTE signal reaches the set value, it will switch to the other sim card.
<b>Roaming Service</b>	Unchecked by default	Click to enable, and enter a time in minutes between 1 and 30. When the time of roaming service reaches the set value, it will switch to the other SIM card to connect.

## Configure SIM-A / SIM-B Card

Here you can set configurations for the cellular connection according to your requirements.

Connection with SIM-A Card

Item	Setting
▶ Network Type	Auto ▾
▶ Dial-Up Profile	Manual-configuration ▾
▶ APN	<input type="text"/>
▶ IP Type	IPv4 ▾
▶ PIN Code	<input type="text"/> (Optional)
▶ Dial Number	<input type="text"/> (Optional)
▶ Account	<input type="text"/> (Optional)
▶ Password	<input type="text"/> (Optional)
▶ Authentication	Auto ▾
▶ IP Mode	Dynamic IP ▾
▶ Primary DNS	<input type="text"/> (Optional)
▶ Secondary DNS	<input type="text"/> (Optional)
▶ Roaming	<input type="checkbox"/> Enable

Note\_1: Configurations of SIM-B Card follow 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 only one will pop up.

Connection with SIM-A/-B Card		
Item	Value setting	Description
<b>Network Type</b>	1. Required setting 2. By default <b>Auto</b> is selected	Select <b>Auto</b> to register a network automatically, regardless of the network type. Select <b>2G Only</b> to register 2G networks only. Select <b>2G Prefer</b> to register 2G networks first if available. Select <b>3G only</b> to register 3G networks only. Select <b>3G Prefer</b> to register 3G networks first if available. Select <b>LTE only</b> to register LTE networks only.

# EW200 Industrial Cellular Gateway

<p><b>Note:</b> Options may vary by model.</p>		
<b>Dial-Up Profile</b>	<p>1. Required setting 2. By default <b>Manual-configuration</b> is selected</p>	<p>Specify the type of dial-up profile for your 3G/4G network. It can be <b>Manual-configuration</b>, <b>APN Profile List</b>, or <b>Auto-detection</b>.</p> <p>Select <b>Manual-configuration</b> to set <b>APN</b> (Access Point Name), <b>Dial Number</b>, <b>Account</b>, and <b>Password</b> to what your carrier provides. Select <b>APN Profile List</b> to set more than one profile to dial up in turn, until the connection is established. A new field will pop up. Go to <b>Basic Network &gt; WAN &amp; Uplink &gt; Internet Setup &gt; SIM-A APN Profile List</b> for details. Select <b>Auto-detection</b> to automatically bring out all configurations needed while dialing-up, by comparing the IMSI of the SIM card to the record listed in the manufacturer's database.</p> <p><b>Note_1:</b> It is highly recommended to select the <b>Manual</b> or <b>APN Profile List</b> to specify the network for your subscription. Your ISP should provide such network settings. <b>Note_2:</b> If you select <b>Auto-detection</b>, it is likely to connect to an improper network, or fail to find a valid APN for your ISP.</p>
<b>APN</b>	<p>1. Required setting 2. String format: any text</p>	<p>Enter the <b>APN</b> you want to use to establish the connection. This is a required setting if you selected <b>Manual-configuration</b> as dial-up profile scheme.</p>
<b>IP Type</b>	<p>1. Required setting 2. <b>IPv4</b> is selected by default</p>	<p>Specify the IP type of the network service provided by your 3G/4G network. It can be <b>IPv4</b>, <b>IPv6</b>, or <b>IPv4/6</b>.</p>
<b>PIN code</b>	<p>1. Optional setting 2. String format: integer</p>	<p>Enter the PIN (Personal Identification Number) code if needed to unlock your SIM card.</p>
<b>Dial Number, Account, Password</b>	<p>1. Optional setting 2. String format: any text</p>	<p>Enter the optional <b>Dial Number</b>, <b>Account</b>, and <b>Password</b> settings if your ISP provided these settings. Note: These settings are only displayed when <b>Manual-configuration</b> is selected.</p>
<b>Authentication</b>	<p>1. Required setting 2. By default <b>Auto</b> is selected</p>	<p>Select <b>PAP</b> (Password Authentication Protocol) and use such protocol to be authenticated with the carrier's server. Select <b>CHAP</b> (Challenge Handshake Authentication Protocol) and use such protocol to be authenticated with the carrier's server. When <b>Auto</b> is selected, it means it will authenticate with the server using either <b>PAP</b> or <b>CHAP</b>.</p>
<b>IP Mode</b>	<p>1. Required setting 2. By default <b>Dynamic IP</b> is selected</p>	<p>When <b>Dynamic IP</b> 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 <b>Static IP</b> mode and fill in all parameters that required, such as IP address, subnet mask and gateway. <b>Note:</b> <b>IP Subnet Mask</b> is Required setting. Make sure you have the right configuration.</p>
<b>Primary DNS</b>	<p>1. Optional setting 2. String format: IP address (IPv4 type)</p>	<p>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.</p>
<b>Secondary DNS</b>	<p>1. Optional setting 2. String format: IP address (IPv4 type)</p>	<p>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.</p>
<b>Roaming</b>	<p>Unchecked by default</p>	<p>Check the box to establish the connection even if the registration status is</p>

# EW200 Industrial Cellular Gateway

roaming, not in home network.

**Note:** Additional charges may be incurred if the connection is set to roaming.

## 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.

SIM-A APN Profile List <span>Add</span> <span>Delete</span>								
ID	Profile Name	APN	Account	Password	Authentication	Priority	Enable	Actions

This lists all the APN profiles you created, making it easy to check and modify. It is available only when you select Dial-Up Profile as APN Profile List.

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

SIM-A APN Profile Configuration	
Item	Setting
▶ Profile Name	<input type="text" value="Profile-1"/>
▶ APN	<input type="text"/>
▶ IP Type	<input type="text" value="IPv4"/> ▼
▶ Account	<input type="text"/> (Optional)
▶ Password	<input type="text"/> (Optional)
▶ Authentication	<input type="text" value="Auto"/> ▼
▶ Priority	<input type="text"/>
▶ Profile	<input type="checkbox"/> Enable

SIM-A/-B APN Profile Configuration		
Item	Value setting	Description
Profile Name	1. By default <b>Profile-x</b> is listed 2. String format: any text	Enter the profile name you want to describe for this profile.
APN	String format: any text	Enter the <b>APN</b> you want to use to establish the connection.
IP Type	1. Required setting 2. <b>IPv4</b> is selected by default	Specify the IP type of the network service provided by your 3G/4G network. It can be <b>IPv4</b> , <b>IPv6</b> , or <b>IPv4/6</b> .
Account	String format: any text	Enter the <b>Account</b> you want to use for the authentication. <b>Value Range:</b> 0 ~ 53 characters.
Password	String format: any text	Enter the <b>Password</b> you want to use for the authentication.
Authentication	1. Required setting 2. <b>Auto</b> is selected by default	Select the Authentication method for the 3G/4G connection. It can be <b>Auto</b> , <b>PAP</b> , <b>CHAP</b> , or <b>None</b> .

# EW200 Industrial Cellular Gateway

<b>Priority</b>	1. Required setting 2. String format: integer	Enter the value for the dial-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. <b>Value Range: 1 ~ 16.</b>
<b>Profile</b>	The box is checked by default	Check the box to enable this profile. Uncheck the box to disable this profile in dialing-up action.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the configuration.
<b>Undo</b>	N/A	Click the <b>Undo</b> button to restore what you just configured back to the previous setting.
<b>Back</b>	N/A	When the <b>Back</b> button is clicked, the screen will return to the previous page.

## 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 ▼
▶ Time Schedule	(0) Always ▼
▶ MTU Setup	<input type="checkbox"/> Enable
▶ IP Passthrough (Cellular Bridge)	<input type="checkbox"/> Enable Fixed MAC : <input type="text"/>
▶ NAT	<input checked="" type="checkbox"/> Enable
▶ IGMP	Disable ▼
▶ WAN IP Alias	<input type="checkbox"/> Enable <input type="text" value="10.0.0.1"/>

3G/4G Connection Common Configuration		
Item	Value setting	Description
<b>Connection Control</b>	By default <b>Auto-reconnect</b> is selected	<p>When <b>Auto-reconnect</b> is selected, it means the device will try to keep the Internet connection on at all times whenever the physical link is connected.</p> <p>When <b>Connect-on-demand</b> is selected, it means the Internet connection will be established only when data traffic is detected.</p> <p>When <b>Connect Manually</b> is selected, it means the <b>Connect</b> button must be clicked to dial up the connection manually. Please go to <b>Status &gt; Basic Network &gt; WAN &amp; Uplink</b> tab for details.</p> <p><b>Note:</b> If the WAN interface serves as the primary one for another WAN interface in Failover role( and vice versa), the Connection Control parameter will not be available on both WANs as the system must set it to "Auto-reconnect"</p>
<b>Maximum Idle Time</b>	1. Optional setting 2. By default <b>600</b> seconds is filled-in	<p>Specify the maximum Idle time setting to disconnect the internet connection when the connection has idle timed out.</p> <p><b>Value Range: 300 ~ 86400.</b></p>

# EW200 Industrial Cellular Gateway

		<b>Note:</b> This field is available only when <b>Connect-on-demand</b> or <b>Connect Manually</b> is selected as the connection control scheme.
<b>Time Schedule</b>	1. Required setting 2. By default <b>(0) Always</b> is selected	When <b>(0) Always</b> is selected, it means this WAN is operating all the time. Once you have set other schedule rules, there will be other options to select. Please go to <b>Object Definition &gt; Scheduling</b> for details.
<b>MTU</b>	1. Required setting 2. By default <b>0</b> is filled-in	Specify the <b>MTU</b> (Maximum Transmission Unit) for the 3G/4G connection. <b>Value Range:</b> 512 ~ 1500, 0 is for auto.
<b>IP Pass-through (Cellular Bridge)</b>	1. Unchecked by default 2. String format for <b>Fixed MAC:</b> MAC address, e.g. 00:50:18:aa:bb:cc	When <b>Enable</b> box is checked, it means the device will directly assign the WAN IP to the first connected local LAN client. However, when an optional <b>Fixed MAC</b> is a non-zero value, it means only the client with this MAC address can get the WAN IP address.  <b>Note:</b> When the <b>IP Pass-through</b> is on, <b>NAT</b> and <b>WAN IP Alias</b> will be unavailable until the function is disabled again.
<b>NAT</b>	Checked by default	Uncheck the box to disable <b>NAT</b> (Network Address Translation) function.
<b>IGMP</b>	By default <b>Disable</b> is selected	Select <b>Auto</b> to enable <b>IGMP</b> function. Check the <b>Enable</b> box to enable <b>IGMP Proxy</b> .
<b>WAN IP Alias</b>	1. Unchecked by default 2. String format: IP address (IPv4 type)	Check the box to enable <b>WAN IP Alias</b> , and fill in the IP address you want to assign.

**Network Monitoring Configuration**

Item	Setting
▶ Network Monitoring Configuration	<input checked="" type="checkbox"/> Enable
▶ Checking Method	DNS Query ▼
▶ Loading Check	<input checked="" type="checkbox"/> Enable
▶ Query Interval	5 (seconds)
▶ Latency Threshold	3000 (ms)
▶ Fail Threshold	5 (Times)
▶ Target1	DNS1 ▼
▶ Target2	None ▼

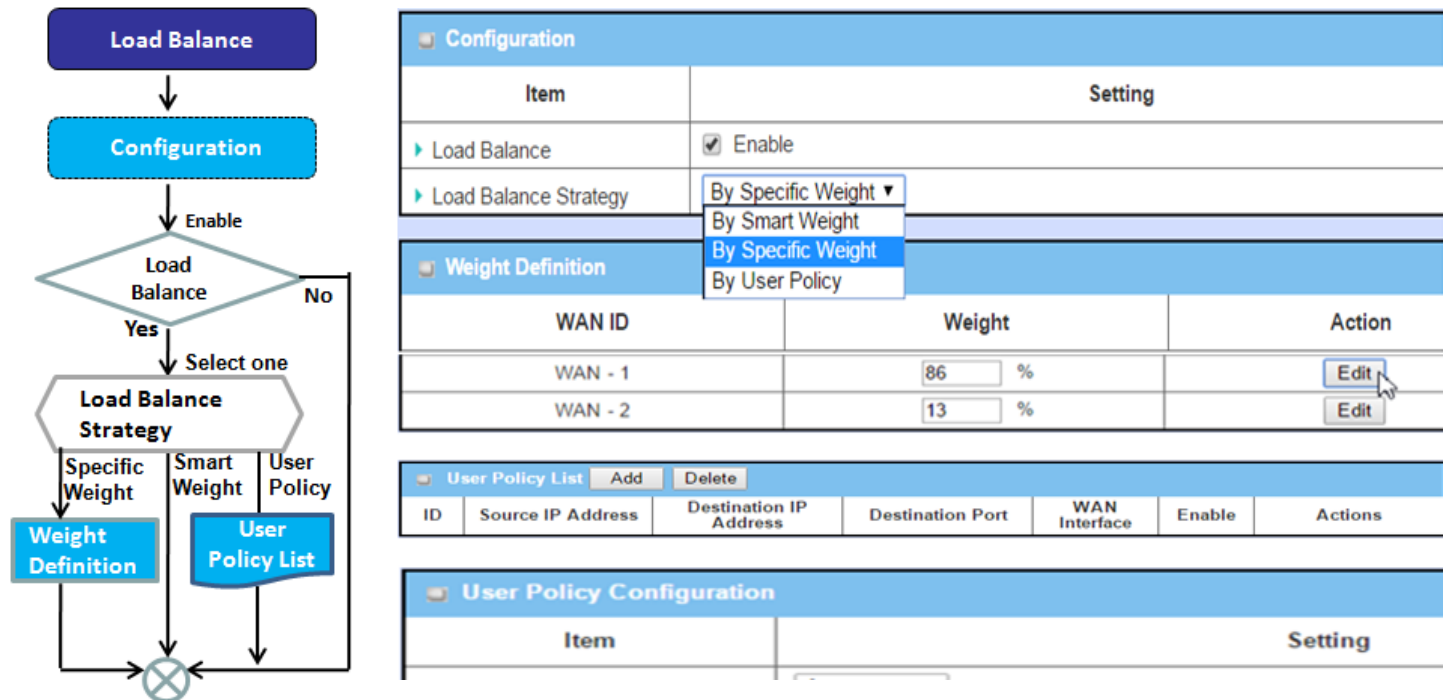
Network Monitoring Configuration		
Item	Value setting	Description
<b>Network Monitoring Configuration</b>	1. Optional setting 2. Box is checked by default	Check the <b>Enable</b> box to activate the network monitoring function.
<b>Checking Method</b>	1. Optional setting 2. <b>DNS Query</b> is set by default	Choose either <b>DNS Query</b> or <b>ICMP Checking</b> to detect WAN link. With <b>DNS Query</b> , the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. With <b>ICMP Checking</b> , the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2.

# EW200 Industrial Cellular Gateway

		<b>Query Interval</b> defines the transmitting interval between two DNS Query or ICMP checking packets.
<b>Loading Check</b>	1. Optional setting 2. Box is checked by default	Check the <b>Enable</b> box to activate the loading check function. Enable Loading Check allows the gateway to ignore unreturned DNS queries or ICMP requests when WAN bandwidth is fully occupied. This is to prevent false link-down status.  <b>Latency Threshold</b> defines the tolerance threshold of responding time. <b>Fail Threshold</b> specifies the detected disconnection before the router recognize the WAN link down status. Enter a number of detected disconnection times to be the threshold before disconnection is acknowledged.
<b>Query Interval</b>	1. Optional setting 2. 5 seconds is selected by default.	Specify a time interval as the DNS <b>Query Interval</b> . <b>Query Interval</b> defines the transmitting interval between two DNS Query or ICMP checking packets. With DNS Query, the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. <b>Value Range:</b> 2 ~ 14400.
<b>Latency Threshold</b>	1. Optional setting 2. 3000 ms is set by default	Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged. <b>Latency Threshold</b> defines the tolerance threshold of responding time. <b>Value Range:</b> 2000 ~ 3000 seconds.
<b>Fail Threshold</b>	1. Optional setting 2. 5 times is set by default	Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged. <b>Fail Threshold</b> specifies the detected disconnection before the router recognize the WAN link down status. <b>Value Range:</b> 1 ~ 10 times.
<b>Target 1</b>	1. Optional setting 2. <b>DNS1</b> is selected by default	<b>Target1</b> specifies the first target of sending DNS query/ICMP request. <b>DNS1:</b> set the primary DNS to be the target. <b>DNS2:</b> set the secondary DNS to be the target. <b>Gateway:</b> set the current gateway to be the target. <b>Other Host:</b> enter an IP address to be the target.
<b>Target 2</b>	1. Optional setting 2. <b>None</b> is selected by default	<b>Target1</b> specifies the second target of sending DNS query/ICMP request. <b>None:</b> no second target is required. <b>DNS1:</b> set the primary DNS to be the target. <b>DNS2:</b> set the secondary DNS to be the target. <b>Gateway:</b> set the Current gateway to be the target. <b>Other Host:</b> enter an IP address to be the target.
<b>Save</b>	N/A	Click <b>Save</b> to save the settings.
<b>Undo</b>	N/A	Click <b>Undo</b> to cancel the settings.

# EW200 Industrial Cellular Gateway

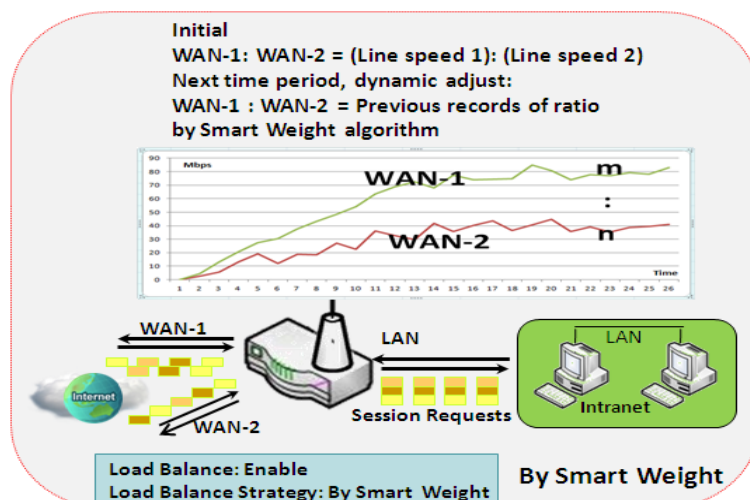
## 2.1.3 Load Balance



When there are multiple WAN interfaces, and when the bandwidth of one WAN connection is not enough for the traffic loads from the Intranet to the Internet, the WAN load balance function can be used to enlarge the total WAN bandwidth.

### Load Balance Strategy

There are three optional strategies for load balance: **"By Smart Weight"**, **"By Specific Weight"**, and **"By User Policy"**. Select a strategy according to application requirements and environment. The strategies are explained as below.

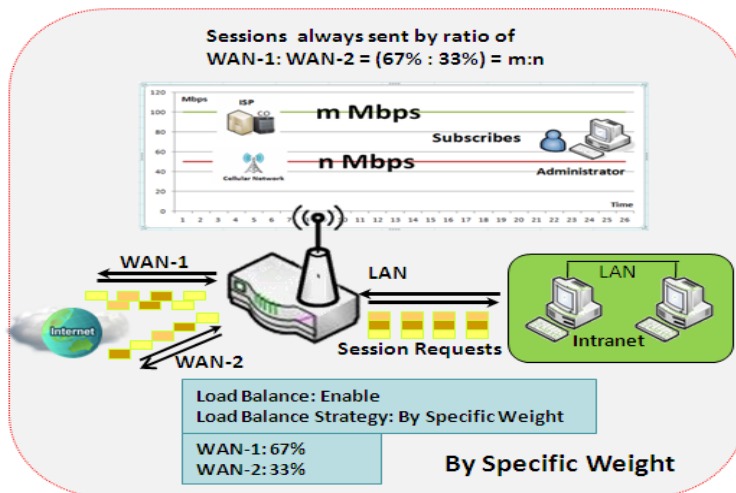


### **By Smart Weight**

If based on "By Smart Weight", the gateway will take the line speed settings of all WAN interfaces specified in "Physical Interface" configuration page as default ratio for data transfer. Based on the ratio of packet bytes via these WAN interfaces in past period (maybe 5 minutes), the system decides how many sessions will be transferred via each WAN interface for next period. The administrator may take it as a fast approach to maximizing bandwidth utilization of multiple WAN interfaces in a gateway.

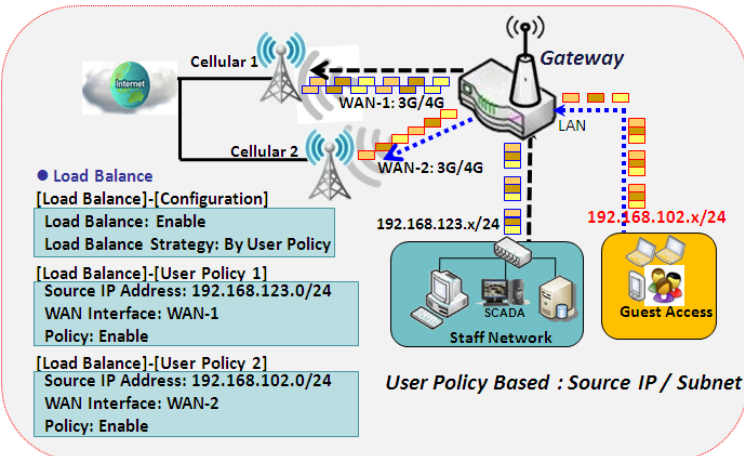


# EW200 Industrial Cellular Gateway



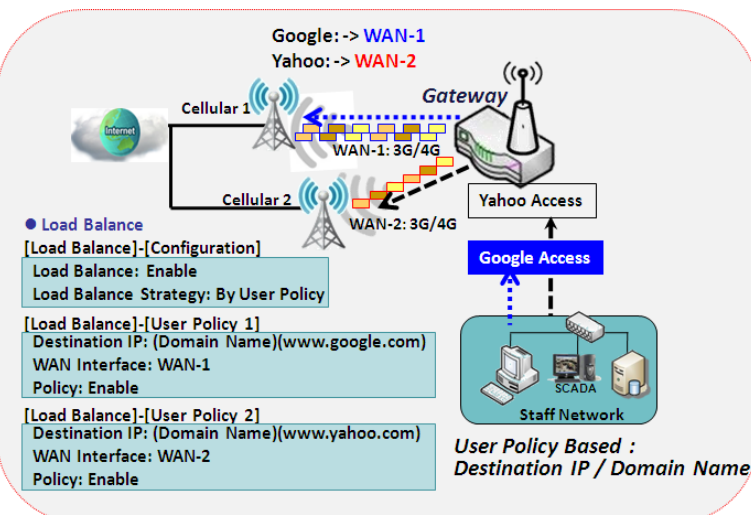
## By Specific Weight

When "By Specific Weight" is selected, you need to set up the ratio of WAN-1/WAN-2 to decide the sessions sent ratio. Total ratio should be 100%. The ratio is usually defined based on the practical WAN speed of the environment. The gateway's traffic control process will operate routing based on the dedicated weight ratio on all WAN interfaces.



## By User Policy

If "By User Policy" load balance strategy is selected, you can map Source IP, Destination IP, or Destination Port to an assigned WAN interface. This IP address is not necessarily a single IP; it can also be a subnet or IP range. The destination port can be a single port or port range. You can select one target for one mapping to setup IP address and leave others as "any"/ "All". Besides this, you can also set protocols as TCP, UDP or both.



The diagrams shown on the left are user policy examples. The first diagram illustrates an example for mapping various source IP subnets to different WAN interfaces. All packets from different subnets will be routed to the assigned WAN interface. The administrator can manage and balance the loading among available WAN interfaces accordingly.

The second diagram illustrates another example for routing packets with designated destination IP or domain names to a specific WAN interface.

If packets do not belong to user policy rule, the gateway just routes those packets based on the smart weight algorithm.



# EW200 Industrial Cellular Gateway

## Load Balance Setting

Go to **Basic Network > WAN & Uplink > Load Balance** Tab.

The Load Balance function is used to manage balanced bandwidth usage among multiple WAN connections. When "By Smart Weight" is chosen, the system will operate load balancing automatically based on the embedded Smart Weight algorithm. However, when "By Specific Weight" is selected, the subsequent "Weight Definition" configuration window will let you define the ratio of transferred sessions between all WAN interfaces for data transfer. Finally, when "By User Policy" is chosen, the "User Policy List" will show all defined user policy entries, and the "User Policy Configuration" window will let you create and define one user policy for routing dedicated packet flow via one WAN interface.

### Enable/Select Load Balance Strategy

Configuration	
Item	Setting
▶ Load Balance	<input type="checkbox"/> Enable
▶ Load Balance Strategy	By Smart Weight ▼

Configuration Item	Value setting	Description
Load Balance	Unchecked by default	Check the <b>Enable</b> box to activate Load Balance function.
Load Balance Strategy	1. Required setting 2. <b>By Smart Weight</b> is selected by default.	There are three load balance strategies: <b>By Smart Weight:</b> System will operate load balance function automatically based on the embedded Smart Weight algorithm. <b>By Specific Weight:</b> System will adjust the ratio of transferred sessions among all WANs based on the specified weights for each WAN. <b>By User Policy:</b> System will route traffic through available WAN interface based on user defined rules.
Save	NA	Click the <b>Save</b> button to save the configuration
Undo	NA	Click the <b>Undo</b> button to restore previous settings.

When **By Specific Weight** is selected, you need to adjust the percentage of WAN loading. The system will give a value according to the bandwidth ratio of each WAN initially, and retain the value after the **Save** button is clicked.

Weight Definition		
WAN ID	Weight	Action
WAN - 1	86 %	Edit
WAN - 2	13 %	Edit

# EW200 Industrial Cellular Gateway

Weight Definition		
Item	Value setting	Description
WAN ID	NA	The Identifier for each available WAN interface
Weight	1. Required setting 2. Set with bandwidth ratio of each WAN by default.	Enter the weight ratio for each WAN interface. Initially, the bandwidth ratio of each WAN is set by default. <b>Value Range: 1 ~ 99.</b>  Note: The sum of all weights can't be greater than 100%.
Save	NA	Click the <b>Save</b> button to save the configuration
Undo	NA	Click the <b>Undo</b> button to restore previous settings.

When **By User Policy** is selected, a **User Policy List** screen will appear. With properly configured policy rules, the system will route traffic through available WAN interfaces based on those rules

## Create User Policy

<input type="checkbox"/> User Policy List <input type="button" value="Add"/> <input type="button" value="Delete"/>						
ID	Source IP Address	Destination IP Address	Destination Port	WAN Interface	Enable	Actions

When Add button is applied, User Policy Configuration screen will appear.

<input type="checkbox"/> User Policy Configuration	
Item	Setting
▶ Source IP Address	<input type="text" value="Any"/>
▶ Destination IP Address	<input type="text" value="Any"/>
▶ Destination Port	<input type="text" value="All"/>
▶ Protocol	<input type="text" value="Both"/>
▶ WAN Interface	<input type="text" value="WAN - 1"/>
▶ Policy	<input type="checkbox"/> Enable

User Policy Configuration		
Item	Value setting	Description
Source IP Address	1. Required setting 2. <b>Any</b> is selected by default.	There are four options: <b>Any:</b> No specific Source IP is provided. The traffic may come from any source <b>Subnet:</b> Specify the subnet for the traffic source. Input format is: xxx.xxx.xxx.xxx/xx e.g. 192.168.123.0/24. <b>IP Range:</b> Specify the IP Range for the traffic source

# EW200 Industrial Cellular Gateway

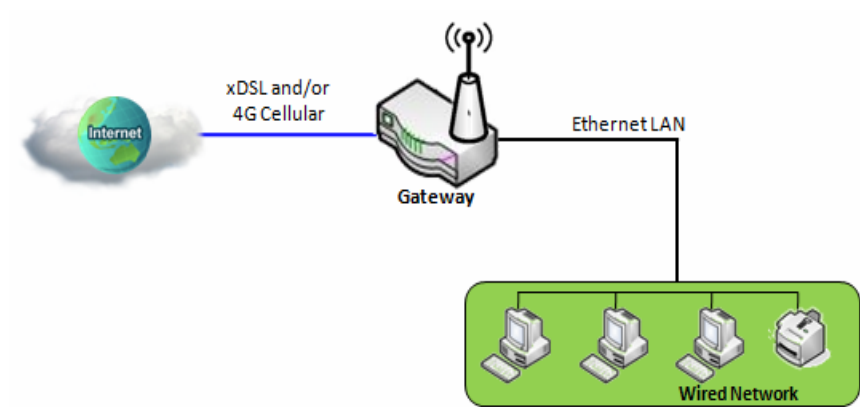
		<b>Single IP:</b> Specify a unique IP Address for the traffic source. Input format is: xxx.xxx.xxx.xxx e.g. 192.168.123.101.
<b>Destination IP Address</b>	1. Required setting 2. <b>Any</b> is selected by default.	<p>There are five options:</p> <p><b>Any:</b> No specific destination IP is provided. The traffic may go to any destination.</p> <p><b>Subnet:</b> Specify the subnet for the traffic destination. Input format is: xxx.xxx.xxx.xxx/xx e.g. 192.168.123.0/24.</p> <p><b>IP Range:</b> Specify the IP Range for the traffic destination</p> <p><b>Single IP:</b> Specify a unique IP Address for the traffic destination. Input format is: xxx.xxx.xxx.xxx e.g. 192.168.123.101.</p> <p><b>Domain Name:</b> Specify the domain name for the traffic destination</p>
<b>Destination Port</b>	1. Required setting 2. <b>All</b> is selected by default.	<p>There are four options:</p> <p><b>All:</b> No specific destination port is provided.</p> <p><b>Port Range:</b> Specify the Destination Port Range for the traffic</p> <p><b>Single Port:</b> Specify a unique destination Port for the traffic</p> <p><b>Well-known Applications:</b> Select the service port of well-known applications defined in dropdown list.</p>
<b>Protocol</b>	1. Required setting 2. <b>Both</b> is selected by default.	There are three options. They are <b>Both</b> , <b>TCP</b> , and <b>UDP</b> .
<b>WAN Interface</b>	1. Required setting 2. <b>WAN-1</b> is selected by default.	Select the interface that traffic should pass through. Note that the WAN interface dropdown list will only show the available WAN interfaces.
<b>Policy</b>	Unchecked by default	Check the <b>Enable</b> checkbox to activate the policy rule.
<b>Save</b>	NA	Click the <b>Save</b> button to save the configuration
<b>Undo</b>	NA	Click the <b>Undo</b> button to restore what you just configured back to the previous setting.

# EW200 Industrial Cellular Gateway

## 2.2 LAN & VLAN

This section describes the configuration of LAN and VLAN. VLAN is an optional feature, and its presence depends on the gateway model.

### 2.2.1 Ethernet LAN



The Local Area Network (LAN) can be used to share data or files among computers attached to a network. The following diagram illustrates a network of wired and interconnected computers.

Follow the following instructions to set up an IPv4 Ethernet LAN.

Configuration	
Item	Setting
IP Mode	Static IP
LAN IP Address	192.168.123.254
Subnet Mask	255.255.255.0 (/24)

Configuration		
Item	Value setting	Description
IP Mode	N/A	It shows the LAN IP mode for the gateway according the related configuration. <b>Static IP:</b> If there is at least one WAN interface activated, the LAN IP mode is fixed in Static IP mode. <b>Dynamic IP:</b> If all the available WAN inferfaces are disabled, the LAN IP mode can be Dynamic IP mode.
LAN IP Address	1. Required 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. <b>Note:</b> This is also the IP address of the web UI. If you change it, you will need to enter the new IP address in the browser in order to see the web UI.
Subnet Mask	1. Required setting 2. 255.255.255.0 (/24) is set	Select the subnet mask for this gateway from the dropdown list.

# EW200 Industrial Cellular Gateway

	by default	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 the LAN IP address of this gateway, so there are a maximum of 253 clients allowed in LAN network. <b>Value Range:</b> 255.0.0.0 (/8) ~ 255.255.255.252 (/30).
Save	N/A	Click the <b>Save</b> button to save the configuration
Undo	N/A	Click the <b>Undo</b> button to restore previous settings.

## Create / Edit Additional IP

This gateway provides the LAN IP alias function for special management considerations. You can add additional LAN IPs for this gateway, and access this gateway through the additional IPs.

Additional IP <span>Add</span> <span>Delete</span>						
ID	Name	Interface	IP Address	Subnet Mask	Enable	Action

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

Additional IP Configuration	
Item	Setting
▶ Name	<input type="text"/>
▶ Interface	<input type="text" value="lo"/>
▶ IP Address	<input type="text"/>
▶ Subnet Mask	<input type="text" value="255.255.255.0 (/24)"/>
▶ Enable	<input type="checkbox"/>
<span>Save</span>	

Configuration Item	Value setting	Description
Name	1. Optional setting	Enter the name for the alias IP address.
Interface	1. Required setting 2. <b>lo</b> is set by default	Specify the Interface type. It can be <b>lo</b> or <b>br0</b> .
IP Address	1. Optional setting 2. <b>192.168.123.254</b> is set by default	Enter the additional IP address for this device.
Subnet Mask	1. Required setting 2. <b>255.255.255.0 (/24)</b> 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

# EW200 Industrial Cellular Gateway

---

		LAN IP address of this gateway, so there are a maximum of 253 clients allowed in the LAN network. <i><b>Value Range:</b> 255.0.0.0 (/8) ~ 255.255.255.255 (/32).</i>
<b>Save</b>	NA	Click the <b>Save</b> button to save the configuration

# EW200 Industrial Cellular Gateway

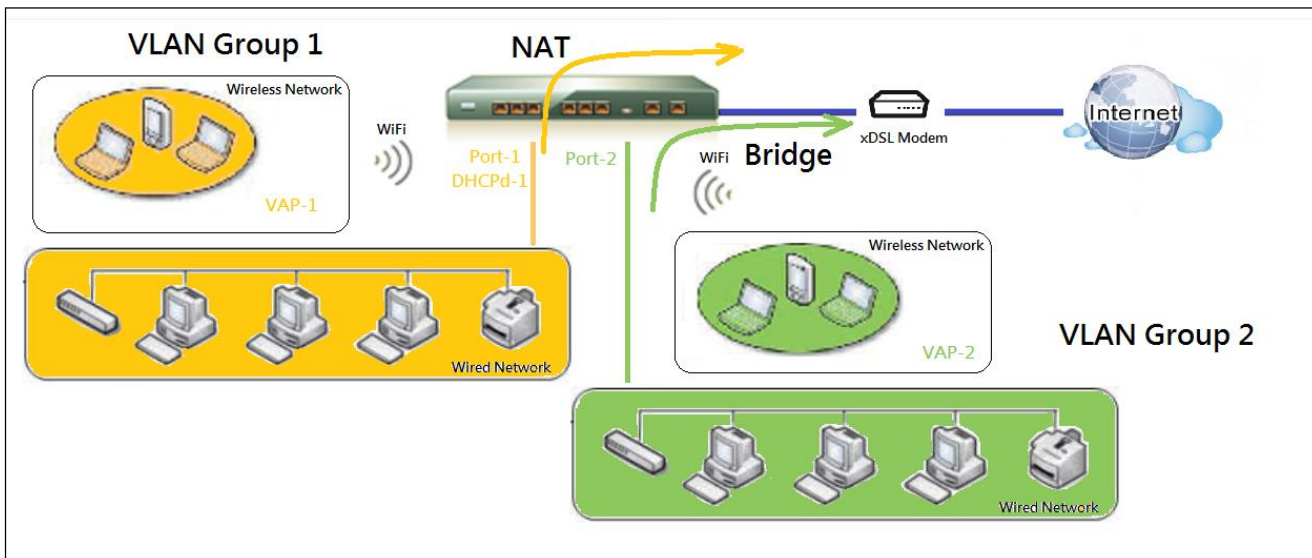
## 2.2.2 VLAN

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 scenarios. For example, if there are various departments within an 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 as needed. In some cases, the ISP may need the router to support “VLAN tags” for certain kinds of services (e.g. IPTV). You can group all devices requiring this service in one tag-based VLAN.

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

### ➤ Port-based VLAN

Port-based VLANs can group Ethernet ports, Port-1 ~ Port-4, and Wi-Fi Virtual Access Points, VAP-1 ~ VAP-8, together for differentiated services like Internet surfing, multimedia enjoyment, VoIP, 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 members obtain IP addresses. Thus, each host can access 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.

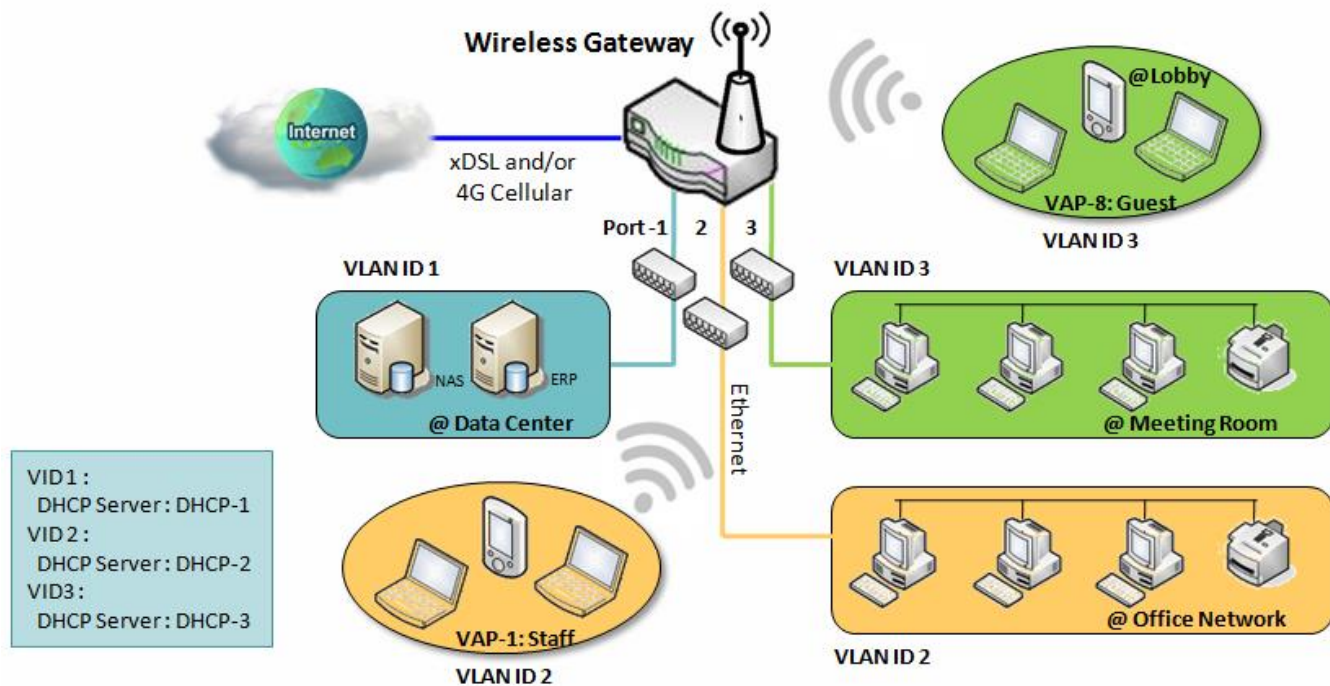


A port-based VLAN is a group of ports on an Ethernet or Virtual APs of Wired or Wireless Gateway that form a logical LAN segment. The following is an example.

In a company, the administrator designs 3 network segments: Lobby/Meeting Room, Office, and Data Center. In a Wireless Gateway, the 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. The office segment is configured with VLAN ID 2. The VLAN group includes Port-2 and VAP-1 (SSID: Staff) with NAT mode

# EW200 Industrial Cellular Gateway

and DHCP-2 server equipped. Finally, the administrator also configures the Data Center segment with VLAN ID 1. The VLAN group includes Port-1 with NAT mode to WAN interface as shown in following diagram.



The above shows a general case for a gateway with 3 Ethernet LAN ports. If the device has only one Ethernet LAN port, there will be only one VLAN group for the device. Under such a situation, it still supports both the NAT and Bridge mode for the Port-based VLAN configuration.

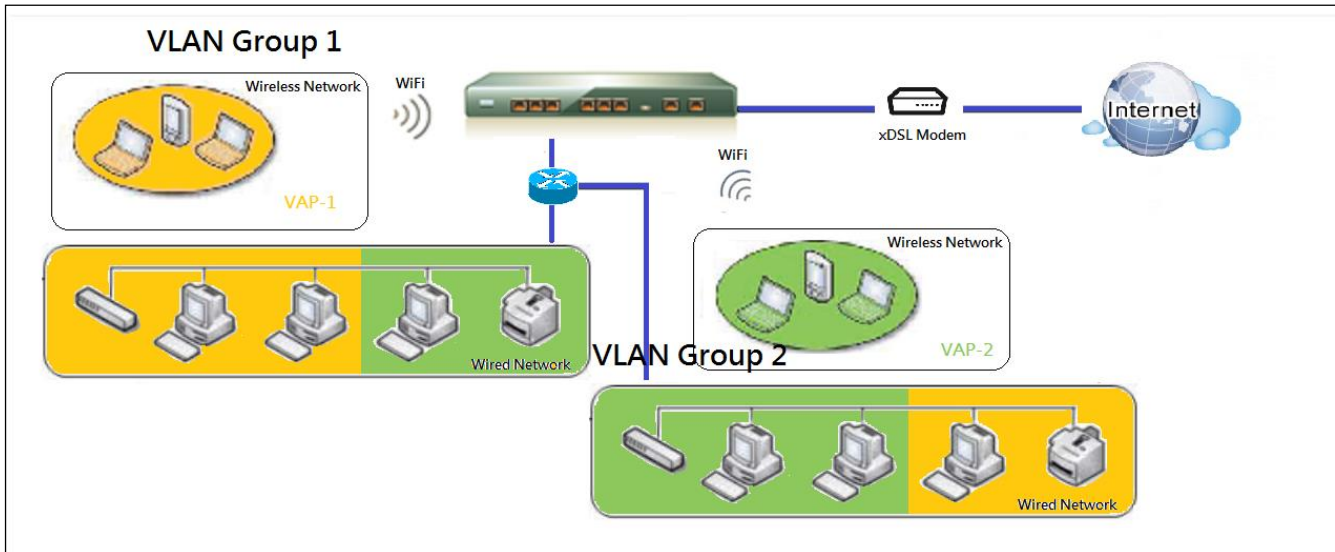
## ➤ Tag-based VLAN

The tag-based VLAN function can group Ethernet ports, Port-1 ~ Port-4, and Wi-Fi Virtual Access Points, VAP-1 ~ VAP-8, together with different VLAN tags for deployment in subnets. All packet flows can carry different VLAN tags even at the same physical Ethernet port. These flows can be directed to different destinations because they have differentiated tags. The approach is very useful to group hosts at different geographic locations into the same workgroup.

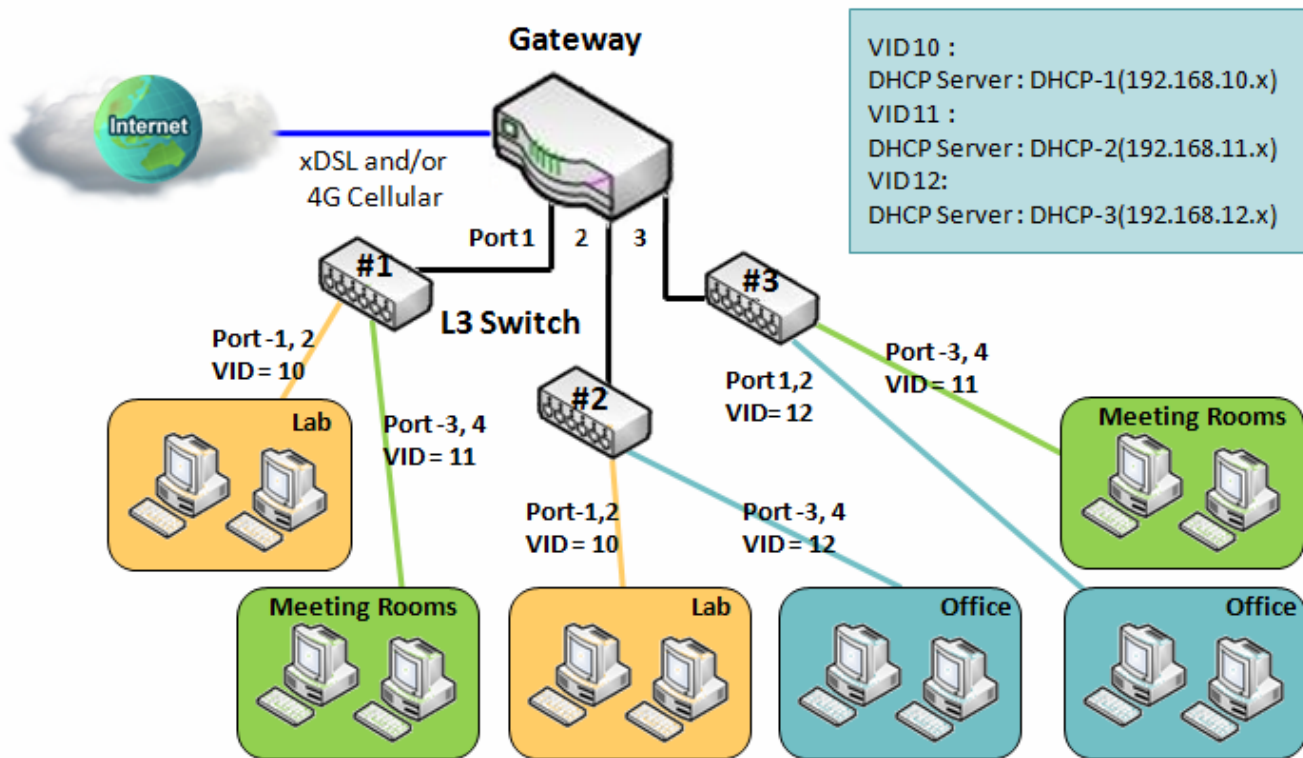
Tag-based VLANs are also called VLAN Trunks. The VLAN Trunk collects all packet flows with different VLAN IDs from the router and delivers them in the Intranet. VLAN membership in a tagged VLAN is determined by VLAN ID information within the packet frames that are received on a port. The administrator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



# EW200 Industrial Cellular Gateway



The administrator designs 3 network segments, Lab, Meeting Rooms, and Office. In a Secure VPN Gateway, the administrator can configure the 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 configures the 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, client hosts in VLAN 11 group cannot access the Internet. At last, he configures the Lab segment with VLAN ID 10. The VLAN group is equipped with DHCP-1 server to construct a 192.168.10.x subnet.



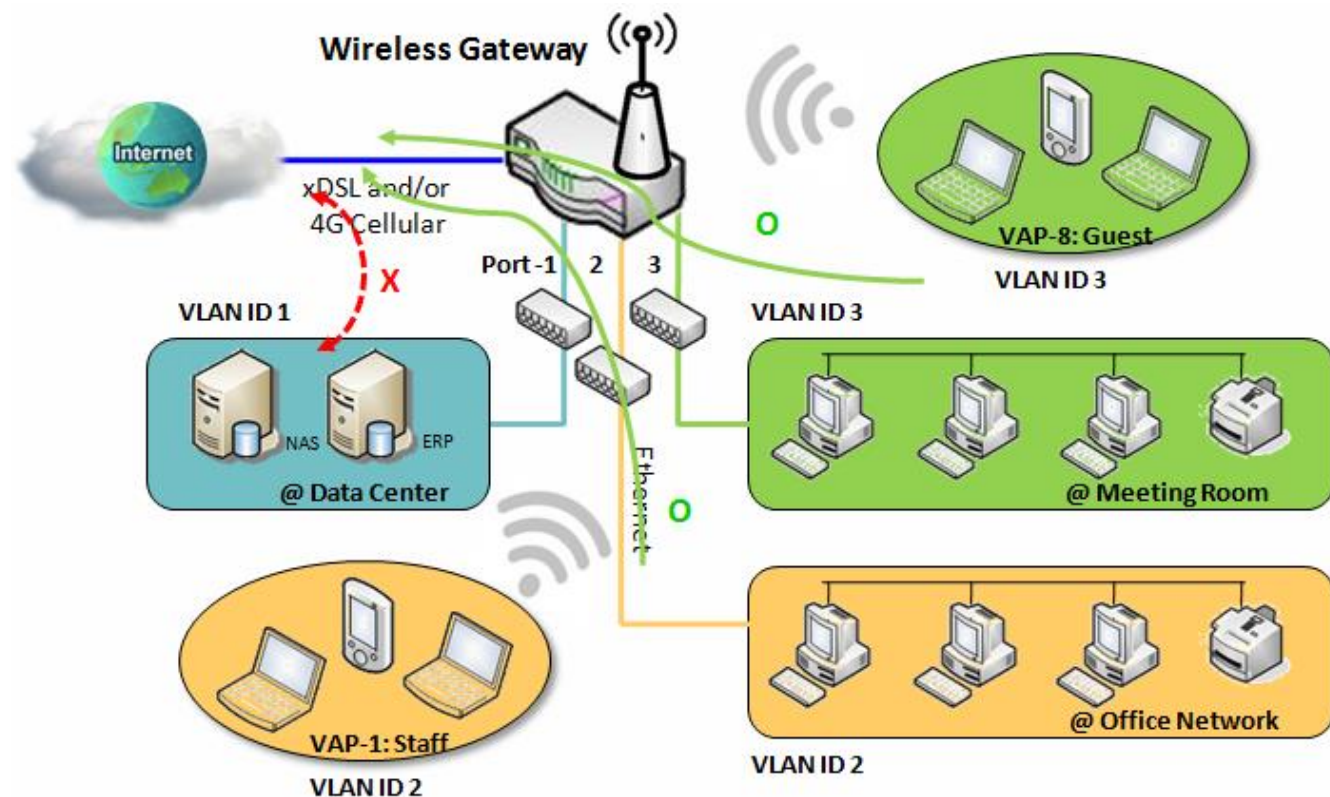
# EW200 Industrial Cellular Gateway

## ➤ VLAN Groups Access Control

The 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

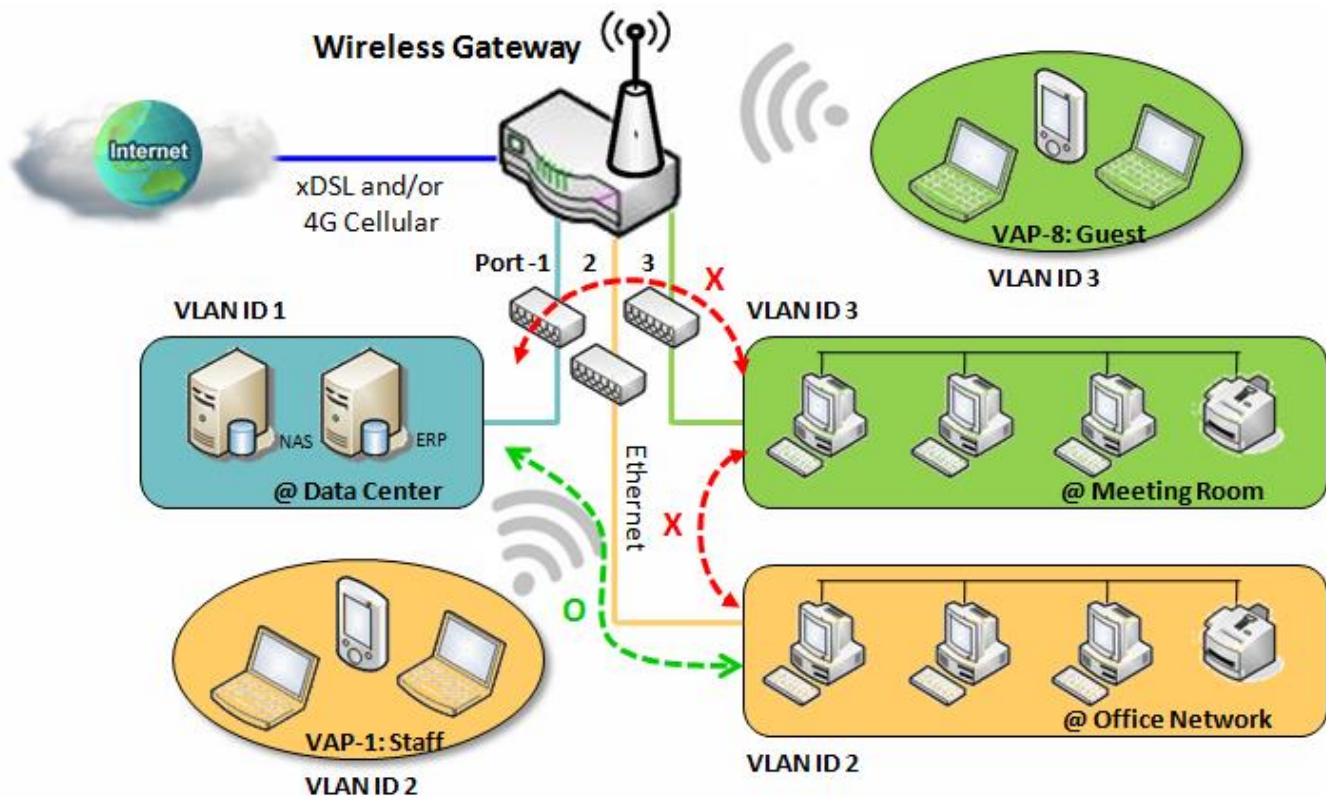
The administrator can specify members of one VLAN group to be able to access Internet or not. Following is an example that VLAN groups of VID is 2 and 3 can access Internet but the one with VID 1 cannot access Internet. That is, visitors in the meeting room and staff in the office network can access Internet. But the computers/servers in data center cannot access Internet due to security considerations. The servers in the data center are only for trusted staff or are accessed through secure tunnels.



# EW200 Industrial Cellular Gateway

## Inter VLAN Group Routing:

In Port-based tagging, the administrator can specify member hosts of one VLAN group to be able or not able to communicate with another VLAN group. This is a communication pair, and one VLAN group can join many communication pairs. But communication pairs do not have a transitive property. That is, if 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 in the following diagram. VLAN groups of VID 1 and 2 can access each other but the ones between VID 1 and VID 3 and between VID 2 and VID 3 cannot.



# EW200 Industrial Cellular Gateway

## VLAN Setting

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

The VLAN function allows you to divide a local network into different virtual LANs, either port-based or tag-based.

Configuration

Item	Setting
VLAN Types	Port-based ▼
System Reserved VLAN ID	Start ID <input type="text" value="1"/> (1-4091) ~ End ID <input type="text" value="5"/>

Configuration

Item	Value setting	Description
<b>VLAN Type</b>	<b>Port-based</b> is selected by default	Select the VLAN type that you want to use. <b>Port-based:</b> Port-based VLAN allows you to add rules for each LAN port, and you can implement advanced controls with the VLAN ID. <b>Tag-based:</b> Tag-based VLAN allows you to add VLAN ID, and select members and DHCP Server for this VLAN ID. Go to <b>Tag-based VLAN List</b> table.
<b>System Reserved VLAN ID</b>	<b>1 ~ 5</b> are reserved by default	Specify the VLAN ID range that is reserved for the system operation. For the Port-based/Tag-based VLAN grouping, only use the ID outside the reserved range. <b>Value Range:</b> 1 ~ 4091.
<b>Save</b>	NA	Click the <b>Save</b> button to save the configuration

## Port-based VLAN – Create/Edit VLAN Rules

The port-based VLAN allows you to customize each LAN port. There is a default rule that shows the configuration of all LAN ports. If your device has a DMZ port, you will see DMZ configuration too. The maximum number of rules is based on the number of LAN ports.

Port-based VLAN List

AddDelete

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	<input checked="" type="checkbox"/>	Edit
LAN	Native VLAN	X	NAT	Detail	192.168.123.254	255.255.255.0	All WANs	0	<input checked="" type="checkbox"/>	Edit

ApplyInter VLAN Group Routing

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

# EW200 Industrial Cellular Gateway

## Port-based VLAN – Configuration

Port-based VLAN Configuration	
Item	Setting
▶ Name	VLAN - 1
▶ VLAN ID	
▶ VLAN Tagging	Disable ▼
▶ NAT / Bridge	NAT ▼
▶ Port Members	Port: <input type="checkbox"/> PORT-1 <input type="checkbox"/> PORT-2 <input type="checkbox"/> PORT-3 <input type="checkbox"/> PORT-4 2.4G: <input type="checkbox"/> VAP-1 <input type="checkbox"/> VAP-2 <input type="checkbox"/> VAP-3 <input type="checkbox"/> VAP-4 <input type="checkbox"/> VAP-5 <input type="checkbox"/> VAP-6 <input type="checkbox"/> VAP-7 <input type="checkbox"/> VAP-8
▶ LAN to Join	<input type="checkbox"/> Enable <input type="button" value="DHCP 1 ▼"/>

Port-based VLAN Configuration		
Item	Value setting	Description
<b>Name</b>	1. Required setting 2. String format: already has default text	Define the <b>Name</b> of this rule. It has default text and cannot be modified.
<b>VLAN ID</b>	Required setting	Define the VLAN ID number, range is 1~4094.
<b>VLAN Tagging</b>	<b>Disable</b> is selected by default.	The rule is activated according to <b>VLAN ID</b> and <b>Port Members</b> configuration when <b>Enable</b> is selected.  The rule is activated according <b>Port Members</b> configuration when <b>Disable</b> is selected.
<b>NAT / Bridge</b>	<b>NAT</b> is selected by default.	Select <b>NAT</b> mode or <b>Bridge</b> mode for the rule.
<b>Port Members</b>	Unchecked by default.	Select which LAN port(s) and VAP(s) that you want to add to the rule. Note: The available member list will depend on product model.
<b>LAN to Join</b>	Unchecked by default.	Check the Enable box and select one of the defined DHCP Server for the List to define the DHCP server for the VLAN group. If you enabled this function, all the rest settings will be greyed out, not required to configured manually.

If you don't bind the VLAN group to a pre-defined DHCP server, you have to further specify the following settings.



# EW200 Industrial Cellular Gateway

▶ 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	<input type="checkbox"/>

<b>WAN &amp; WAN VID to Join</b>	All WANs is selected by default.	Select which <b>WAN</b> or <b>All WANs</b> that allow accessing Internet. Note: If Bridge mode is selected, you need to select a WAN and enter a VID.
<b>LAN IP Address</b>	Required setting	Assign an <b>IP Address</b> for the DHCP Server that the rule used, this IP address is a gateway IP.
<b>Subnet Mask</b>	255.255.255.0(/24) is selected by default.	Select a <b>Subnet Mask</b> for the DHCP Server.
<b>DHCP Server /Relay</b>	<b>Server</b> is selected by default.	Define the <b>DHCP Server</b> type. There are three types: <b>Server</b> , <b>Relay</b> , and <b>Disable</b> . <b>Relay</b> : Select <b>Relay</b> to enable DHCP Relay function for the VLAN group. You only need to fill the <b>DHCP Server IP Address</b> field. <b>Server</b> : Select <b>Server</b> to enable DHCP Server function for the VLAN group. You need to specify the DHCP Server settings. <b>Disable</b> : Select <b>Disable</b> to disable the DHCP Server function for the VLAN group.
<b>DHCP Server IP Address (for DHCP Relay only)</b>	Required setting	If you select <b>Relay</b> type of DHCP Server, assign a <b>DHCP Server IP Address</b> that the gateway will relay the DHCP requests to the assigned DHCP server.
<b>DHCP Server Name</b>	Required setting	Define name of the DHCP Server.
<b>IP Pool</b>	Required setting	Define the IP Pool range. There are <b>Starting Address</b> and <b>Ending Address</b> fields. If a client requests an IP address from this DHCP Server, it will assign an IP address in the range of <b>IP pool</b> .
<b>Lease Time</b>	Required setting	Define a period of time for an IP Address that the DHCP Server leases to a new

## EW200 Industrial Cellular Gateway

---

		device. By default, the <b>lease time</b> is 86400 seconds.
<b>Domain Name</b>	String format, any text	The Domain Name of this DHCP Server. <b><u>Value Range:</u></b> 0 ~ 31 characters.
<b>Primary DNS</b>	IPv4 format	The Primary DNS of this DHCP Server.
<b>Secondary DNS</b>	IPv4 format	The Secondary DNS of this DHCP Server.
<b>Primary WINS</b>	IPv4 format	The Primary WINS of this DHCP Server.
<b>Secondary WINS</b>	IPv4 format	The Secondary WINS of this DHCP Server.
<b>Gateway</b>	IPv4 format	The Gateway of this DHCP Server.
<b>Enable</b>	Unchecked by default	Click <b>Enable</b> box to activate this rule.
<b>Save</b>	NA	Click the <b>Save</b> button to save the configuration
<b>Undo</b>	NA	Click the <b>Undo</b> button to restore previous settings.

# EW200 Industrial Cellular Gateway

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

IP Fixed Mapping Rule List

MAC Address	IP Address	Enable	Actions
-------------	------------	--------	---------

Mapping Rule Configuration

Item	Setting
▶ MAC Address	<input type="text"/>
▶ IP Address	<input type="text"/>
▶ Enable	<input type="checkbox"/>

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

Mapping Rule Configuration		
Item	Value setting	Description
MAC Address	Required setting	Define the <b>MAC Address</b> target that the DHCP Server wants to match.
IP Address	Required setting	Define the <b>IP Address</b> 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 <b>IP Address</b> to the client whose <b>MAC Address</b> matched the rule.
Enable	Unchecked by default	Click <b>Enable</b> box to activate this rule.
Save	NA	Click the <b>Save</b> button to save the configuration

Note: Always click on the **Apply** button to apply the changes after the web browser refresh has taken you back to the VLAN page.

Port-based VLAN List

Name	VLAN ID	VLAN Tagging	NAT / Bridge	Port Members	LAN IP Address	Subnet Mask	Joined WAN	WAN VID	Enable	Actions
LAN	Native VLAN Tag 1	X	NAT	<input type="button" value="Detail"/>	192.168.66.1	255.255.254.0	All WANs	0	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/>



# EW200 Industrial Cellular Gateway

## Port-based VLAN – Inter VLAN Group Routing

Click the **VLAN Group Routing** button, and 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 2.4G VAP: 1,2,3,4,5,6,7,8 5G VAP: 1,2,3,4,5,6,7,8	Allow <input type="button" value="Edit"/>

Inter VLAN Group Routing		
VLAN IDs	Members	Action
		<input type="button" value="Edit"/>
		<input type="button" value="Edit"/>
		<input type="button" value="Edit"/>
		<input type="button" value="Edit"/>

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

VLAN Group Internet Access Definition		
VLAN IDs	Members	Internet Access(WAN)
<input checked="" type="checkbox"/> 1	Port : 2,3 2.4G VAP: 1,2,3,4,5,6,7,8 5G VAP: 1,2,3,4,5,6,7,8	Allow <input type="button" value="Edit"/>

Inter VLAN Group Routing		
VLAN IDs	Members	Action
<input type="checkbox"/> 1		<input type="button" value="Edit"/>
		<input type="button" value="Edit"/>
		<input type="button" value="Edit"/>
		<input type="button" value="Edit"/>

Inter VLAN Group Routing		
Item	Value setting	Description
VLAN Group Internet Access Definition	All boxes are checked by default.	By default, all boxes are checked, meaning all <b>VLAN ID</b> members are allowed to access WAN interface. If a <b>VLAN ID</b> box is unchecked, it means the VLAN ID member can't access the Internet.

# EW200 Industrial Cellular Gateway

		Note: <b>VLAN ID 1</b> is always available; it is the default VLAN ID of the <b>LAN</b> . Other <b>VLAN IDs</b> are available only when they are enabled.
<b>Inter VLAN Group Routing</b>	Unchecked by default	Click the 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 <b>Inter VLAN Group Routing</b> . 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.
<b>Save</b>	N/A	Click the <b>Save</b> 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 that shows the configuration of all LAN ports and all VAPs. 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 <span>Add</span> <span>Delete</span>						
VLAN ID	Internet	Port Members	Bridge Interface	IP Address	Subnet Mask	Actions
Native VLAN	<input checked="" type="checkbox"/>	Port: <input checked="" type="checkbox"/> Port-2 <input checked="" type="checkbox"/> Port-3 2.4G: <input checked="" type="checkbox"/> VAP-1 <input checked="" type="checkbox"/> VAP-2 <input checked="" type="checkbox"/> VAP-3 <input checked="" type="checkbox"/> VAP-4 <input checked="" type="checkbox"/> VAP-5 <input checked="" type="checkbox"/> VAP-6 <input checked="" type="checkbox"/> VAP-7 <input checked="" type="checkbox"/> VAP-8 5G: <input checked="" type="checkbox"/> VAP-1 <input checked="" type="checkbox"/> VAP-2 <input checked="" type="checkbox"/> VAP-3 <input checked="" type="checkbox"/> VAP-4 <input checked="" type="checkbox"/> VAP-5 <input checked="" type="checkbox"/> VAP-6 <input checked="" type="checkbox"/> VAP-7 <input checked="" type="checkbox"/> VAP-8	DHCP 1			<span>Edit</span> <span>Select</span>

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

Tag-based VLAN Configuration	
Item	Setting
VLAN ID	0
Internet Access	<input checked="" type="checkbox"/> Enable
Port Members	Port: <input type="checkbox"/> Port-2 <input type="checkbox"/> Port-3 2.4G: <input type="checkbox"/> VAP-1 <input type="checkbox"/> VAP-2 <input type="checkbox"/> VAP-3 <input type="checkbox"/> VAP-4 <input type="checkbox"/> VAP-5 <input type="checkbox"/> VAP-6 <input type="checkbox"/> VAP-7 <input type="checkbox"/> VAP-8 5G: <input type="checkbox"/> VAP-1 <input type="checkbox"/> VAP-2 <input type="checkbox"/> VAP-3 <input type="checkbox"/> VAP-4 <input type="checkbox"/> VAP-5 <input type="checkbox"/> VAP-6 <input type="checkbox"/> VAP-7 <input type="checkbox"/> VAP-8
Bridge Interface	DHCP 1

Tag-based VLAN Configuration (Part-1)		
Item	Value setting	Description
<b>VLAN ID</b>	Required setting	Define the <b>VLAN ID</b> number, range is 6~4094.
<b>Internet Access</b>	The box is checked by default.	Click <b>Enable</b> box to allow the members in the VLAN group access to internet.
<b>Port Members</b>	Unchecked by default	Check the LAN port box(es) to join the VLAN group. Check the VAP box(es) to join the VLAN group. Note: Only the wireless gateway has the VAP list.
<b>Bridge Interface</b>	<b>DHCP 1</b> is selected by default.	Select a predefined <b>DHCP Server</b> , <b>New</b> to define a new DHCP server for these members of this VLAN group.
<b>Save</b>	N/A	Click <b>Save</b> button to save the configuration Note: After clicking the <b>Save</b> button, always click the <b>Apply</b> button to apply the settings.

If you select New to create a new DHCP server setting for the VLAN group, you have to further specify the

# EW200 Industrial Cellular Gateway

following configuration.

▶ IP Address	<input type="text"/>
▶ Subnet Mask	255.255.255.0 (/24) ▼
▶ DHCP Relay	<input type="checkbox"/> Enable & Server IP : <input type="text"/>
▶ WAN Interface	WAN - 1 ▼
▶ DHCP Relay Option 82	<input type="checkbox"/> Enable
<input type="button" value="Save"/>	

Tag-based VLAN Configuration (part II)		
Item	Value setting	Description
IP Address	Required 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 Relay	Unchecked by default	Check the box to enable the DHCP Relay function for the VLAN group, and you only need to fill the DHCP Server IP Address field.
WAN Interface	WAN-1 is selected by default	Select which WAN interface allows accessing the Internet.
DHCP Option 82	Optional setting	If you select Relay type of DHCP Server, you can further enable the DHCP Option 82 setting if the DHCP server support it.
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.

## Tag-based VLAN Summary

The configured tag-based VLAN group information will be displayed in the following screen.

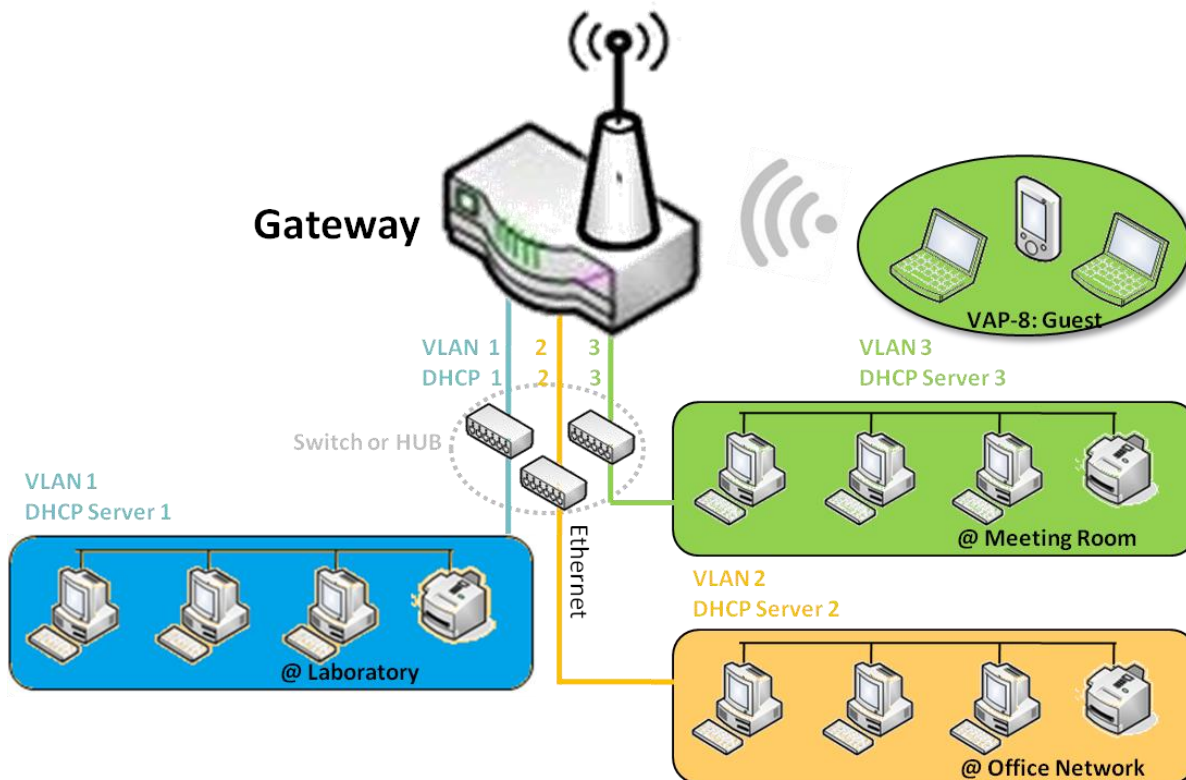
Tag-based VLAN Summary	
Port	VLAN IDs
Port1	Native VLAN
Port2	Native VLAN
Port3	Native VLAN
Port4	Native VLAN

# EW200 Industrial 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 (refer to VLAN section for details). There is one default setting for whose LAN IP Address is the same as the gateway LAN interface, with its default Subnet Mask setting as “255.255.255.0”, and its default IP Pool range is from “.100” to “.200” as shown at the DHCP Server List page on gateway’s Web UI.

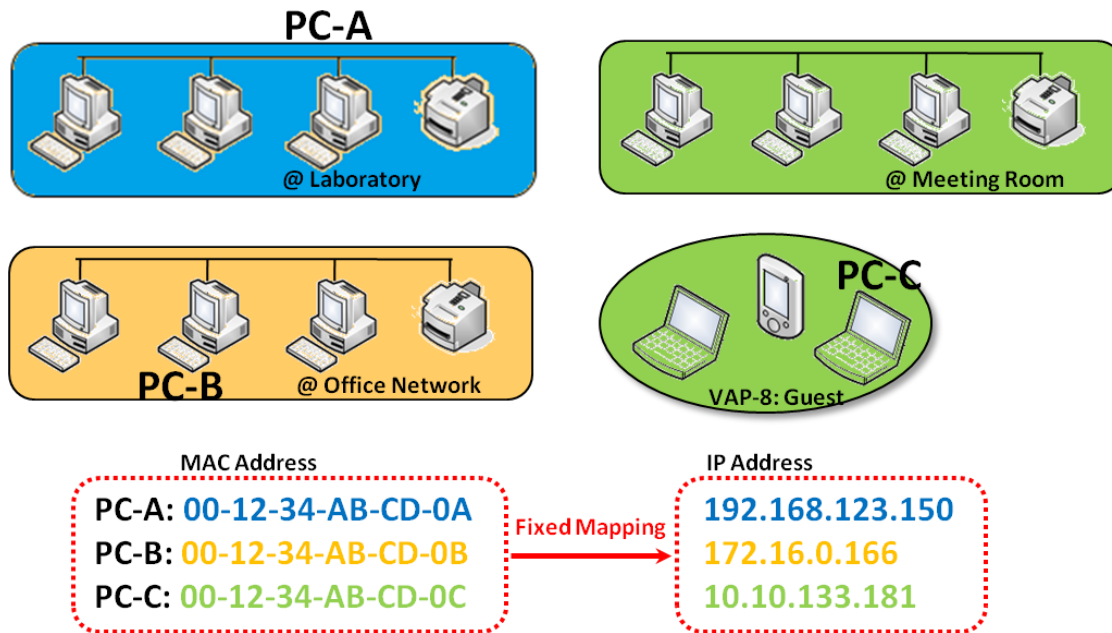


More DHCP server configurations can be added by clicking on the “Add” button behind “DHCP Server List”, or clicking on the “Edit” button at the end of each DHCP Server on list to edit the current settings. Additionally, you can select a DHCP Server and delete it by clicking on the “Select” check-box and the “Delete” button.

# EW200 Industrial Cellular Gateway

## ➤ Fixed Mapping

User can assign fixed IP address to a specific client MAC address, when targets already exist in the **DHCP Client List**, or add other Mapping Rules manually in advance.



# EW200 Industrial 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 customize your DHCP Server Policy. If multiple LAN ports are available, you can define one policy for each LAN (or VLAN group). A maximum of 4 policy sets are supported.

DHCP Server List <span>Add</span> <span>Delete</span> <span>DHCP Client List</span> <span>[ Help ]</span>												
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	<input checked="" type="checkbox"/>	<span>Edit</span> <span>Fixed Mapping</span>

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

DHCP Server Configuration	
Item	Setting
▶ DHCP Server Name	<input type="text" value="DHCP 2"/>
▶ LAN IP Address	<input type="text" value="192.168.2.254"/>
▶ Subnet Mask	<input type="text" value="255.0.0.0 (/8)"/>
▶ IP Pool	Starting Address: <input type="text"/> Ending Address: <input type="text"/>
▶ Lease Time	<input type="text" value="86400"/> seconds
▶ Domain Name	<input type="text"/> (Optional)
▶ Primary DNS	<input type="text"/> (Optional)
▶ Secondary DNS	<input type="text"/> (Optional)
▶ Primary WINS	<input type="text"/> (Optional)
▶ Secondary WINS	<input type="text"/> (Optional)
▶ Gateway	<input type="text"/> (Optional)
▶ Server	<input type="checkbox"/> Enable

# EW200 Industrial Cellular Gateway

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

## Create / Edit Mapping Rule List on DHCP Server

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

Mapping Rule List <input type="button" value="Add"/> <input type="button" value="Delete"/> <span>[ Help ]</span>			
MAC Address	IP Address	Enable	Actions

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

# EW200 Industrial Cellular Gateway

Mapping Rule Configuration	
Item	Setting
▶ MAC Address	<input type="text"/>
▶ IP Address	<input type="text"/>
▶ Rule	<input type="checkbox"/> Enable

Mapping Rule Configuration		
Item	Value setting	Description
MAC Address	1. MAC Address string format 2. Required setting	The MAC Address of this mapping rule.
IP Address	1. IPv4 format. 2. Required setting	The IP Address of this mapping rule.
Rule	Unchecked by default	Click <b>Enable</b> box to activate this rule.
Save	N/A	Click the <b>Save</b> button to save the configuration
Undo	N/A	Click the <b>Undo</b> button to restore previous settings.
Back	N/A	When the <b>Back</b> button is clicked the screen will return to the <b>DHCP Server Configuration</b> page.

## View / Copy DHCP Client List

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

DHCP Client List <span>Copy to Fixed Mapping</span>					
LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time	Actions
Ethernet	Dynamic /192.168.123.100	James-P45V	74:D0:2B:62:8D:42	00:49:07	<input type="checkbox"/> Select

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.



# EW200 Industrial Cellular Gateway

Option	Meaning	RFC
66	TFTP server name	<a href="#">[RFC 2132]</a>
72	Default World Wide Web Server	<a href="#">[RFC 2132]</a>
114	URL	<a href="#">[RFC 3679]</a>

Configuration	
Item	Setting
▶ DHCP Server Options	<input type="checkbox"/> Enable

## Create / Edit DHCP Server Options

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

DHCP Server Option List <span>Add</span> <span>Delete</span>							
ID	Option Name	DHCP Server Select	Option Select	Type	Value	Enable	Actions

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

DHCP Server Option Configuration <span>Save</span> <span>Undo</span>	
Item	Setting
Option Name	<input type="text" value="Option 1"/>
DHCP Server Select	<span>DHCP 1 ▼</span>
Option Select	<span>DHCP OPTION 66 ▼</span>
Type	<span>Single IP Address ▼</span>
Value	<input type="text"/>
Enable	<input type="checkbox"/> Enable

# EW200 Industrial Cellular Gateway

DHCP Server Option Configuration			
Item	Value setting		Description
Option Name	1. String format, any text 2. Required setting.		Enter a DHCP Server Option name.
DHCP Server Select	Dropdown list of all available DHCP servers.		Choose the DHCP server this option should apply to.
Option Select	1. Required setting. 2. Option 66 is selected by default.		Choose the specific option from the dropdown list. It can be <b>Option 66, Option 72, Option 144, Option 42, Option 150, or Option 160.</b> <b>Option 42</b> for ntp server; <b>Option 66</b> for TFTP; <b>Option 72</b> for www; <b>Option 144</b> for URL.
Type Dropdown list of DHCP server option value type	Each option has different value types.		
	66	Single IP address	
		Single FQDN	
	72	IP address list, separated by “,”	
	114	Single URL	
	42	IP address list, separated by “,”	
	150	IP address list, separated by “,”	
	160	Single IP address, Single FQDN	
Value 1. IPv4 format 2. FQDN format 3. IP list 4. URL format 5. Required setting	Should conform to Type:		
	Type		Value
	66	Single IP address	
		Single FQDN	
	72	IP address list, separated by “,”	
	114	Single URL	
Enable	Unchecked by default	Click <b>Enable</b> box to activate this setting.	
Save	NA	Click the <b>Save</b> button to save the setting.	
Undo	NA	When the <b>Undo</b> button is clicked the screen will return back with nothing changed.	

## Create / Edit DHCP Relay

The gateway supports up to a maximum of 6 DHCP Relay configurations.

DHCP Relay Configuration List <span>Add</span> <span>Delete</span>						
ID	Agent Name	LAN interface	WAN interface	Server IP	Enable	Actions

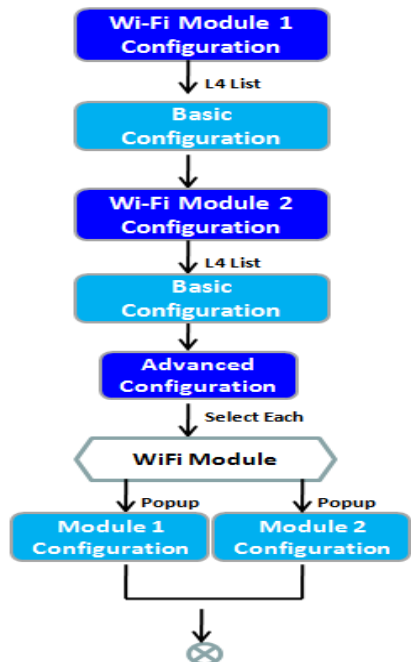
When **Add/Edit** button is applied, the **DHCP Relay Configuration** screen will appear.

# EW200 Industrial Cellular Gateway

DHCP Relay Configuration <span>Save</span> <span>Undo</span>	
Item	Setting
Agent Name	<input type="text"/>
LAN interface	LAN ▼
WAN interface	WAN - 1 ▼
Server IP	<input type="text"/>
DHCP OPTION 82	<input type="checkbox"/>
Enable	<input type="checkbox"/>

DHCP Relay Configuration		
Item	Value setting	Description
<b>Agent Name</b>	1. String format, any text. 2. Required setting.	Enter a DHCP Relay name. Enter a name that is easy for you to understand. <b>Value Range:</b> 1~64 characters.
<b>LAN Interface</b>	1. Required setting. 2. <b>LAN</b> is selected by default.	Choose a LAN Interface for the dropdown list to apply with the DHCP Relay function.
<b>WAN Interface</b>	1. Required setting. 2. <b>WAN-1</b> is selected by default.	Choose a WAN Interface for the dropdown list to apply with the DHCP Relay function. It can be the available WAN interface(s), and L2TP connection.
<b>Server IP</b>	1. Required setting. 2. <b>null</b> by default	Assign a <b>DHCP Server IP Address</b> that the gateway will relay the DHCP requests to the assigned DHCP server via specified WAN interface.
<b>DHCP OPTION 82</b>	Unchecked by default.	Click <b>Enable</b> box to activate DHCP OPTION 82 function. Option 82 is organized as a single DHCP option that contains circuit-ID information known by the relay agent. If the relayed DHCP server required the such information, you have to enable it, otherwise, just leave it as unchecked.
<b>Enable</b>	Unchecked by default.	Click <b>Enable</b> box to activate this setting.
<b>Save</b>	NA	Click the <b>Save</b> button to save the setting.
<b>Undo</b>	NA	When the <b>Undo</b> button is clicked the screen will return back with nothing changed.

## 2.3 Wi-Fi



```
graph TD; A[Wi-Fi Module 1 Configuration] -->|L4 List| B[Basic Configuration]; B --> C[Wi-Fi Module 2 Configuration]; C -->|L4 List| D[Basic Configuration]; D --> E[Advanced Configuration]; E -->|Select Each| F{{WiFi Module}}; F -->|Popup| G[Module 1 Configuration]; F -->|Popup| H[Module 2 Configuration]; G --> I(( )); H --> I;
```

The flowchart illustrates the configuration process for the Wi-Fi module. It starts with 'Wi-Fi Module 1 Configuration', leading to a 'Basic Configuration' screen via an 'L4 List'. This is followed by 'Wi-Fi Module 2 Configuration', which also leads to a 'Basic Configuration' screen via an 'L4 List'. From there, it proceeds to 'Advanced Configuration', which then leads to a 'WiFi Module' selection screen via 'Select Each'. This selection screen branches into 'Module 1 Configuration' and 'Module 2 Configuration' via 'Popup' actions. Both module configuration screens then lead to a final output point, represented by a circle with an 'X'.

Basic Configuration		[ Help ]
Item	Setting	
▶ Operation Band	2.4G Single Band ▼	

2.4G WiFi Configuration	
Item	Setting
▶ WiFi Module	<input checked="" type="checkbox"/> Enable
▶ Channel	Auto ▼ <input checked="" type="radio"/> By AP Numbers <input type="radio"/> By Less Interference
▶ WiFi System	802.11b/g/n Mixed ▼
▶ WiFi Operation Mode	AP Router Mode ▼
▶ Green AP	<input type="checkbox"/> Enable
▶ VAP Isolation	<input checked="" type="checkbox"/> Enable
▶ Time Schedule	(0) Always ▼

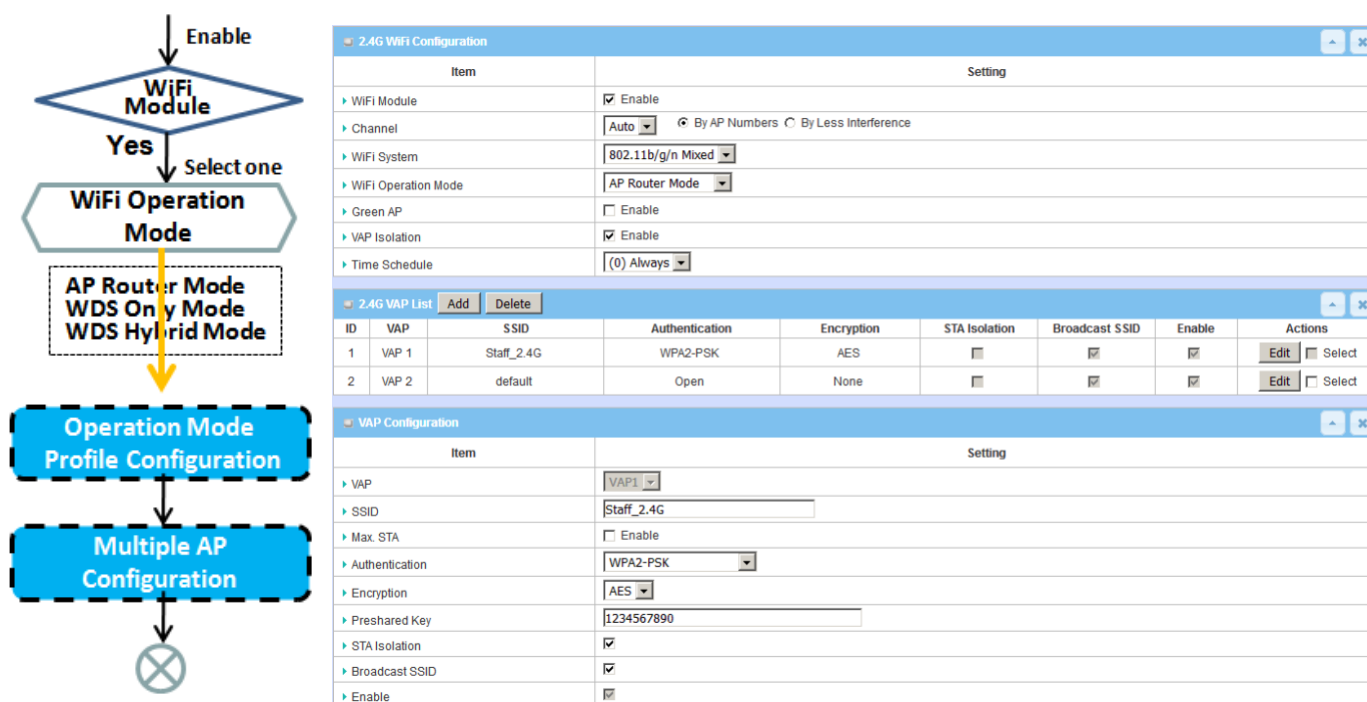
2.4G VAP List		Add	Delete					
ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions

The gateway provides Wi-Fi interface for mobile devices or BYOD devices to access Internet/Intranet. The Wi-Fi function is usually modularized design in the gateway, and there can be single or dual modules within a gateway. The Wi-Fi system in the gateway complies with the IEEE 802.11ac/11n/11g/11b standard in 2.4GHz or 5GHz single band or 2.4G/5GHz concurrent dual bands of operation. There are several wireless operation modes provided by this device. They are: “AP Router Mode”, “WDS Only Mode”, and “WDS Hybrid Mode”.

There are some sub-sections for Wi-Fi configuration, including “Basic Configuration” and “Advanced Configuration”. In the Basic Configuration section, all the settings must be entered for Wi-Fi to be used. The Advanced Configuration section provides more parameters for advanced users to fine tune the connectivity performance for the Wi-Fi function.

# EW200 Industrial Cellular Gateway

## 2.3.1 Wi-Fi Configuration

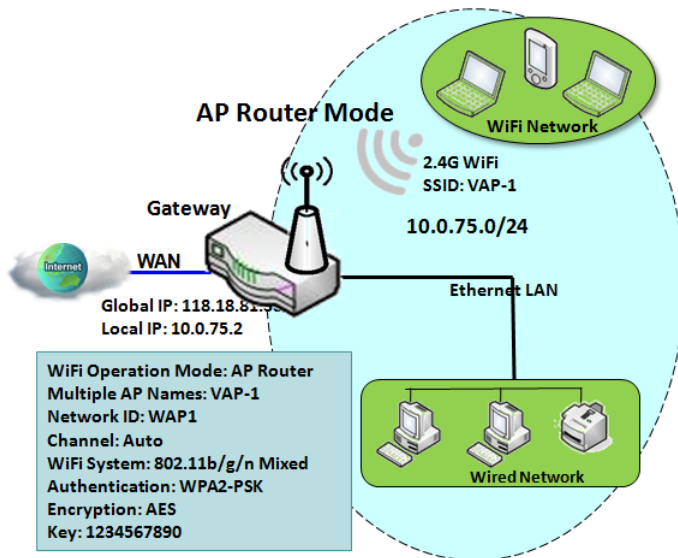


Due to optional module(s) and frequency band, you need to set up modules one by one. For each module, you need to specify the operation mode, and then set up the virtual APs for wireless access.

Following are the scenarios for each wireless operation mode. To connect your wireless devices with the wireless gateway, make sure of your application scenario for Wi-Fi network and choose the most suitable operation mode.

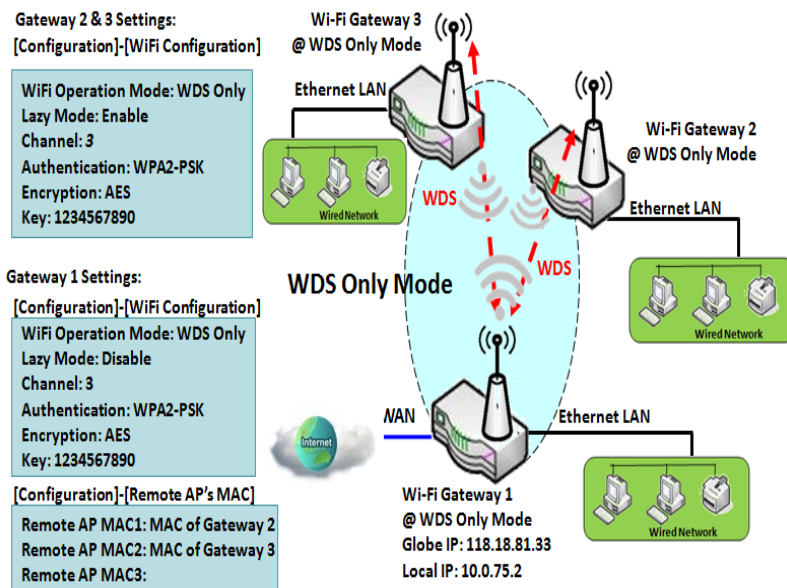
# EW200 Industrial Cellular Gateway

## AP Router Mode



This mode allows connected wired and wireless devices to form the Intranet of the wireless gateway, and the Intranet will link to the Internet with the gateway's NAT mechanism. So, this gateway is working as a Wi-Fi AP, but also a Wi-Fi hotspot for Internet access. It means local Wi-Fi clients can associate to it, and the Internet. With its NAT mechanism, wireless clients don't need to obtain a public IP addresses from ISP.

## WDS Only Mode



WDS (Wireless Distributed System) Only mode drives a Wi-Fi gateway to be a bridge for its wired Intranet and a repeater to extend distance. You can use multiple Wi-Fi gateways as a Wi-Fi repeater chain with all gateways setup as "WDS Only" mode. All gateways can communicate with each other through Wi-Fi. All wired client hosts within each gateway can also communicate each other. Only one gateway within a repeater chain can be a DHCP server to provide IP addresses for all wired client hosts of every gateway. This gateway can be a NAT router to provide internet access.

The diagram illustrates that there are two wireless gateways 2, 3 running in "WDS Only" mode. They both use channel 3 to link to local

Gateway 1 through WDS. Both gateways connected by WDS need to have remote AP MAC set up for each other. All client hosts under gateways 2, 3 can request IP address from the DHCP server at gateway 1. Wireless Gateway 1 also executes the NAT mechanism for all client hosts Internet access.

# EW200 Industrial Cellular Gateway

## WDS Hybrid Mode

### Gateway 2 / AP 1 Settings:

#### [Configuration]-[WiFi Configuration]

WiFi Operation Mode: WDS Hybrid  
Lazy Mode: Enable  
Multiple AP Names: VAP1  
Network ID: Extended-WiFi  
Channel: same as Router 1  
Authentication: same as Router 1  
Encryption: same as Router 1  
Key: same as Router 1

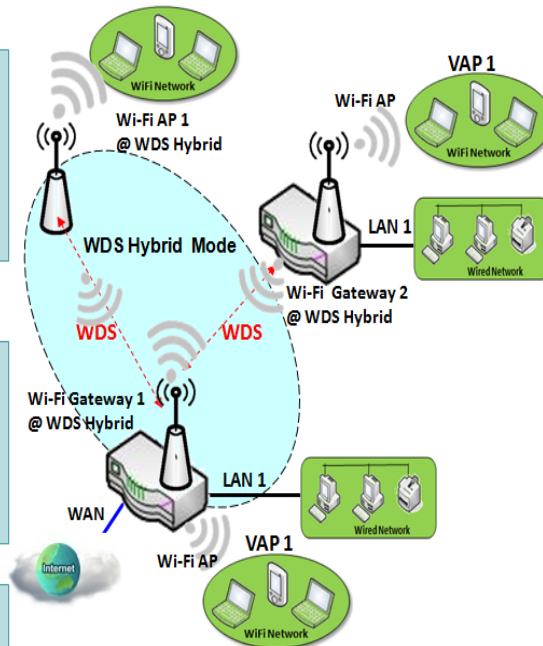
### Gateway 1 Settings:

#### [Configuration]-[WiFi Configuration]

WiFi Operation Mode: WDS Hybrid  
Lazy Mode: Disable  
Multiple AP Names: VAP1  
Network ID: Extended-WiFi  
Channel: 3  
Authentication: WPA2-PSK  
Encryption: AES  
Key: 1234567890

#### [Configuration]-[Remote AP's MAC]

Remote AP MAC1: MAC of Router 2  
Remote AP MAC2: MAC of AP 1  
Remote AP MAC3:



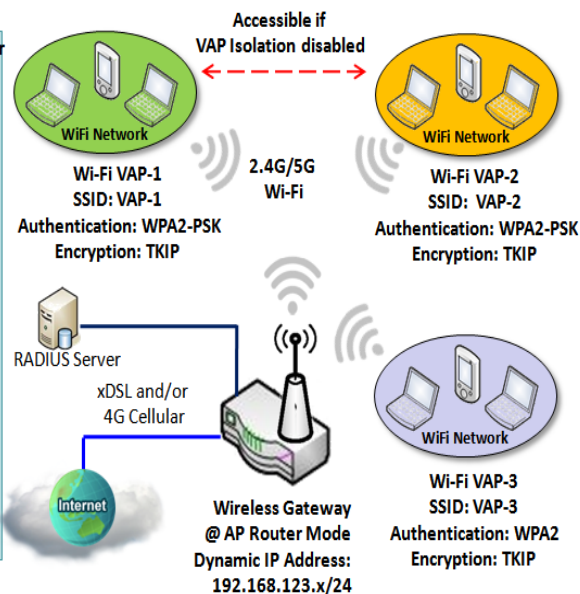
WDS hybrid mode includes both WDS and AP Router mode. WDS Hybrid mode can act as an access point for its Wi-Fi Intranet and a Wi-Fi bridge for its wired and Wi-Fi Intranets at the same time. Users can thus use the features to build up a large wireless network in a large space like airports, hotels or campus.

The diagram illustrates Gateway 1, Gateway 2 and AP 1 connected by WDS. Each gateway has access point function for Wi-Fi client access. Gateway 1 has DHCP server to assign IP to client hosts. All gateways and AP are under WDS hybrid mode. To setup WDS hybrid mode, fill out all configuration items similar to that of AP-router and WDS modes.

## Multiple VAPs

### Gateway Settings:

WiFi Operation Mode: AP Router  
VAP1  
SSID: VAP-1  
Authentication: WPA2-PSK  
Encryption: TKIP  
Key: 1234567890  
  
VAP2  
SSID: VAP-2  
Authentication: WPA2-PSK  
Encryption: TKIP  
Key: 1234567890  
  
VAP3  
SSID: VAP-3  
Authentication: WPA2  
Encryption: TKIP  
RADIUS Server IP: 192.168.168.  
RADIUS Server Port: 1812  
RADIUS Shared Key

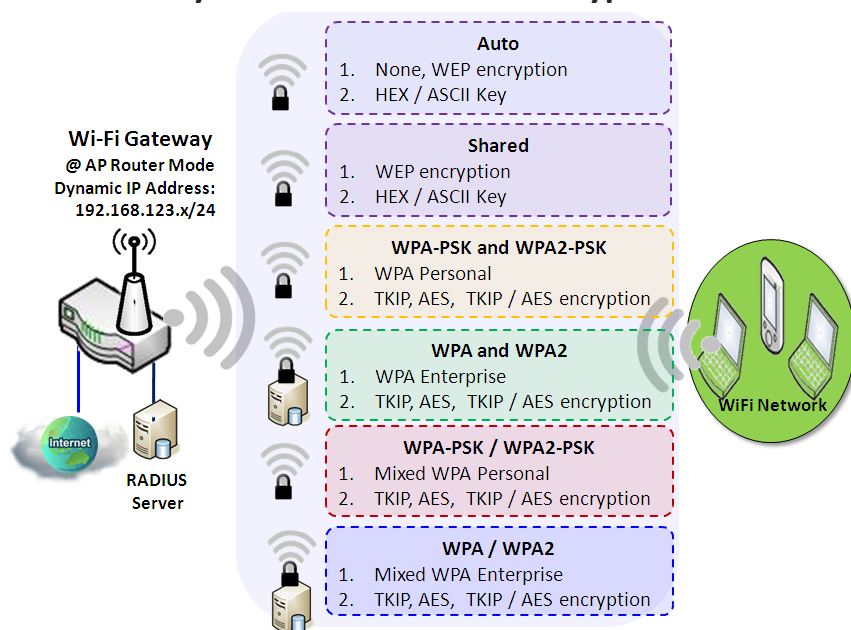


VAP (Virtual Access Point) is a function to partition a wireless network into multiple broadcast domains. It can simulate multiple APs in one physical AP. This wireless gateway supports up to 8 VAPs. For each VAP, you need to setup SSID, authentication and encryption to control Wi-Fi client access.

There is a VAP isolation option to manage access among VAPs. You can allow or block communication for the wireless clients connected to different VAPs. As shown in the diagram, the clients in VAP-1 and VAP-2 can communicate to each other when VAP Isolation is disabled.

# EW200 Industrial Cellular Gateway

## Wi-Fi Security – Authentication & Encryption



Wi-Fi security provides complete authentication and encryption mechanisms to enhance data security while data is transferred wirelessly. The wireless gateway supports Shared, WPA-PSK / WPA2-PSK and WPA / WPA2 authentication. You can select one authentication scheme to validate the wireless clients while they are connecting to the AP. For data encryption, the gateway supports WEP, TKIP and AES. The selected encryption algorithm will be applied to the data while the wireless connection is established.



# EW200 Industrial Cellular Gateway

## Wi-Fi Configuration Setting

The Wi-Fi configuration allows user to configure 2.4GHz or 5GHz Wi-Fi settings.

Go to **Basic Network > Wi-Fi > Wi-Fi Module One** Tab. If the gateway is equipped with two Wi-Fi modules, there will also be a **Wi-Fi Module Two**. You can do similar configurations on both Wi-Fi modules.

### Basic Configuration

Basic Configuration [ Help ]	
Item	Setting
▶ Operation Band	2.4G Single Band ▼

Basic Configuration		
Item	Value setting	Description
Operation Band	Required setting	Specify the intended operation band for the Wi-Fi module. Usually, this setting is fixed and cannot be changed once the module is integrated into the product. However, there are some modules with selectable bands that can be chosen. Under such situation, you can specify which operation band is suitable for the application.

### Configure Wi-Fi Setting

2.4G WiFi Configuration	
Item	Setting
▶ WiFi Module	<input checked="" type="checkbox"/> Enable
▶ Channel	Auto ▼ <input checked="" type="radio"/> By AP Numbers <input type="radio"/> By Less Interference
▶ WiFi System	802.11b/g/n Mixed ▼
▶ WiFi Operation Mode	AP Router Mode ▼

Configuring Wi-Fi Settings		
Item	Value setting	Description
Wi-Fi Module	Box is checked by default	Check the <b>Enable</b> box to activate Wi-Fi function.
Channel	1. Required setting. 2. <b>Auto</b> is selected by default.	Select a radio channel for the VAP. Each channel corresponds to a different radio band. The permissible channels depend on the local <b>Regulatory Domain</b> . There are two options when <b>Auto</b> is selected: ● <b>By AP Numbers</b>

# EW200 Industrial Cellular Gateway

		<p>The channel will be selected according to AP numbers (The less, the better).</p> <ul style="list-style-type: none"> <li>● <b>By Less Interference</b></li> </ul> <p>The channel will be selected according to interference. (The lower, the better).</p>
<b>Wi-Fi System</b>	Required setting	<p>Specify the preferred Wi-Fi System. The dropdown list of <b>Wi-Fi system</b> is based on <b>IEEE 802.11</b> standard.</p> <ul style="list-style-type: none"> <li>● <b>2.4G Wi-Fi</b> Select b, g and n only or mixed.</li> <li>● <b>5G Wi-Fi</b> Select a, n and ac only or mixed.</li> </ul>
<b>Wi-Fi Operation Mode</b>		<p>Specify the <b>Wi-Fi Operation Mode</b> according to your application. Go to the following table for <b>AP Router Mode</b>, <b>WDS Only Mode</b>, and <b>WDS Hybrid Mode</b> settings.</p> <p>Note: The available operation modes depend on the product specification.</p>

In the following, the specific configuration description for each Wi-Fi operation mode is given.

## AP Router Mode & VAPs Configuration

For the AP Router mode, the device not only supports **stations connection** but also the **router function**. The **WAN** port and the **NAT** function are **enabled**.

▶ Wi-Fi Operation Mode	AP Router Mode ▼
▶ Green AP	<input type="checkbox"/> Enable
▶ VAP Isolation	<input checked="" type="checkbox"/> Enable
▶ Time Schedule	(0) Always ▼

AP Router Mode		
Item	Value setting	Description
<b>Green AP</b>	Unchecked by default.	Check the <b>Enable</b> box to activate <b>Green AP</b> function.
<b>VAP Isolation</b>	The box is checked by default.	Check the <b>Enable</b> box to activate this function. By default, the box is checked; it means that stations that are associated to different VAPs cannot communicate with each other.
<b>Time Schedule</b>	Required setting	Apply a specific <b>Time Schedule</b> to this rule; otherwise leave it as <b>(0) Always</b> . If the dropdown list is empty ensure <b>Time Schedule</b> is pre-configured. Refer to <b>Object Definition &gt; Scheduling &gt; Configuration</b> tab.

2.4G VAP List									
ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions	
1	VAP 1	Staff_2.4G	WPA2-PSK	AES	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit	Select

By default, VAP 1 is enabled and security key is required to connect to the gateway wirelessly to enhance the security level and prevent unexpected access of un-authorized devices.

The default wifi key is printed on both the device label and the Security Card. It is created randomly and

# EW200 Industrial Cellular Gateway

differs from devices. So, you can connect to the VAP1 (SSID: Staff\_2.4G) with the provided key. However, it is strongly recommended that you change the security key to an easy-to-remember one by clicking the **Edit** button.

Click **Add / Edit** button in the VAL List screen to create or edit the settings for a VAP. a **VAP Configuration** screen will appear.

VAP Configuration	
Item	Setting
VAP	VAP1 ▾
SSID	Staff_2.4G
Max. STA	<input type="checkbox"/> Enable
Authentication	Auto ▾ 802.1x <input type="checkbox"/> Enable
Encryption	None ▾
STA Isolation	<input checked="" type="checkbox"/>
Broadcast SSID	<input checked="" type="checkbox"/>
Enable	<input checked="" type="checkbox"/>

For others:

VAP Configuration	
Item	Setting
VAP	VAP2 ▾
SSID	default
Max. STA	<input type="checkbox"/> Enable
Authentication	Open ▾
Encryption	None ▾
STA Isolation	<input type="checkbox"/>
Broadcast SSID	<input type="checkbox"/>
Enable	<input type="checkbox"/>

VAP Configuration		
Item	Value setting	Description
SS ID	1. String format: Any text	Enter the SSID for the VAP, and decide whether to broadcast the SSID. The <b>SSID</b> is used for identifying from another AP, and client stations will associate with AP according to SSID.
Max. STA	Unchecked by default	Check this box and enter a limit for the maximum number of client stations. Unchecked by default, meaning no special limitation on the number of connected STAs.

# EW200 Industrial Cellular Gateway

Authentication	1. Required setting 2. <b>Auto</b> is selected by default.	For security, there are several authentication methods supported. Client stations should provide the key when associating with this device.
		<p>When <b>Open</b> is selected</p> <p>The <b>802.1x</b> check box shows up next to the dropdown list.</p> <ul style="list-style-type: none"> <li>● <b>802.1x</b> (Unchecked by default)</li> </ul> <p>When <b>802.1x</b> is enabled, it means the client stations will be authenticated by RADIUS server.</p> <p><b>RADIUS Server IP</b> (The default IP is 0.0.0.0)</p> <p><b>RADIUS Server Port</b> (The default value is 1812)</p> <p><b>RADIUS Shared Key</b></p>
		<p>When <b>Shared</b> is selected</p> <p>The pre-shared WEP key should be set for authenticating.</p>
		<p>When <b>Auto</b> is selected</p> <p>The device will select <b>Open</b> or <b>Shared</b> by requesting of client automatically.</p> <p>The check box named <b>802.1x</b> shows up next to the dropdown list.</p> <ul style="list-style-type: none"> <li>● <b>802.1x</b> (Unchecked by default)</li> </ul> <p>When <b>802.1x</b> is enabled, it means the client stations will be authenticated by RADIUS server.</p> <p><b>RADIUS Server IP</b> (The default IP is 0.0.0.0)</p> <p><b>RADIUS Server Port</b> (The default value is 1812)</p> <p><b>RADIUS Shared Key</b></p>
		<p>When <b>WPA</b> or <b>WPA2</b> is selected</p> <p>They are implemented as per IEEE 802.11i. <b>WPA</b> has only implemented a part of IEEE 802.11i, but has better <b>compatibility</b>.</p> <p><b>WPA2</b> has fully implemented the 802.11i standard, and has the highest <b>security</b>.</p> <ul style="list-style-type: none"> <li>● <b>RADIUS Server</b></li> </ul> <p>The client stations will be authenticated by RADIUS server.</p> <p><b>RADIUS Server IP</b> (The default IP is 0.0.0.0)</p> <p><b>RADIUS Server Port</b> (The default value is 1812)</p> <p><b>RADIUS Shared Key</b></p>
		<p>When <b>WPA / WPA2</b> is selected</p> <p>It has the same settings as <b>WPA</b> or <b>WPA2</b>. The client stations can associate with this device via <b>WPA</b> or <b>WPA2</b>.</p>
		<p>When <b>WPA-PSK</b> or <b>WPA2-PSK</b> is selected</p> <p>It has the same encryption system as WPA or WPA2. The authentication uses pre-shared key instead of RADIUS server.</p>
Encryption	1. Required setting. 2. <b>None</b> is selected be default.	<p>When <b>WPA-PSK / WPA2-PSK</b> is selected</p> <p>It has the same settings as <b>WPA-PSK</b> or <b>WPA2-PSK</b>. The client stations can associate with this device via <b>WPA-PSK</b> or <b>WPA2-PSK</b>.</p>
		<p>Select a suitable encryption method and enter the required key(s).</p> <p>The available method in the dropdown list depends on the Authentication selected.</p> <p><b>None</b></p> <p>It means that the device is open system without encryption.</p> <p><b>WEP</b></p> <p>Up to 4 WEP keys can be set, and one must be selected as the current key. The key type can be set to <b>HEX</b> or <b>ASCII</b>.</p> <p>If <b>HEX</b> is selected, the key should consist of (0 to 9) and (A to F).</p> <p>If <b>ASCII</b> is selected, the key should consist of characters in the ASCII table.</p> <p><b>TKIP</b></p> <p>TKIP was proposed instead of WEP without upgrading hardware. Enter a Pre-shared Key for it. Key length is from 8 to 63 characters.</p>

# EW200 Industrial Cellular Gateway

		<b>AES</b> The newest encryption system in Wi-Fi, designed for the fast 802.11n high bitrate schemes. Enter a Pre-shared Key for it. Key length is from 8 to 63 characters. It is recommended to use <b>AES</b> encryption instead of any others for security. <b>TKIP / AES</b> <b>TKIP / AES</b> mixed mode. It means that the client stations can associate with this device via <b>TKIP</b> or <b>AES</b> . Enter a Pre-shared Key for it. Key length is from 8 to 63 characters.
<b>STA Isolation</b>	The box is checked by default.	Check the <b>Enable</b> box to activate this function. By default, the box is checked; it means that stations associated to the same VAP cannot communicate with each other.
<b>Broadcast SSID</b>	The box is checked by default.	Check the <b>Enable</b> box to activate this function. If the broadcast SSID option is enabled, it means the SSID will be broadcasted, and stations can associate with this device by scanning SSID.
<b>Enable</b>	VAP1: The box is checked by default; Others: unchecked by default.	Check the <b>Enable</b> box to activate this VAP.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the current configuration.
<b>Undo</b>	N/A	Click the <b>Undo</b> button to restore configuration to previous setting before saving.
<b>Apply</b>	N/A	Click the <b>Apply</b> button to apply the saved configuration.

## WDS Only Mode

For the WDS Only mode, the device only bridges the connected wired clients to another WDS-enabled Wi-Fi device that the device is associated with.

► WiFi Operation Mode	WDS Only Mode ▼
► Green AP	<input type="checkbox"/> Enable
► Time Schedule	(0) Always ▼
► Scan Remote AP's MAC List	<input type="button" value="Scan"/>
Remote AP MAC 1	<input type="text"/>
Remote AP MAC 2	<input type="text"/>
Remote AP MAC 3	<input type="text"/>
Remote AP MAC 4	<input type="text"/>

WDS Only Mode		
Item	Value setting	Description
<b>Green AP</b>	Unchecked by default	Check the <b>Enable</b> box to activate <b>Green AP</b> function.
<b>Time Schedule</b>	Required setting	Apply a specific <b>Time Schedule</b> to this rule; otherwise leave it as <b>(0) Always</b> . If the dropdown list is empty ensure <b>Time Schedule</b> is pre-configured. Refer to <b>Object</b>

# EW200 Industrial Cellular Gateway

Definition > Scheduling > Configuration tab.		
Scan Remote AP's MAC List	N/A	Press the <b>Scan</b> button to scan the spatial AP information, and then select one from the AP list, the MAC of selected AP will be auto filled in the following Remote AP MAC table.
Remote AP MAC 1~4	Required setting	Enter the remote AP's MAC manually, or via auto-scan approach, The device will bridge the traffic to the remote AP when associated successfully.

2.4G VAP List <span>Add</span> <span>Delete</span> <span>↑</span> <span>×</span>								
ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	Staff_2.4G	WPA2-PSK	AES	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<span>Edit</span> <input type="checkbox"/> Select

By default, VAP 1 is enabled and security key is required to connect to the gateway wirelessly to enhance the security level and prevent unexpected access of un-authorized devices.

The default wifi key is printed on both the device label and the Security Card. It is created randomly and differs from devices. So, you can connect to the VAP1 (SSID: Staff\_2.4G) with the provided key.

However, it is strongly recommended that you change the security key to an easy-to-remember one by clicking the **Edit** button.

Under **WDS Only** mode, only VAP1 is available for further specifying the required authentication and Encryption settings. Click **Edit** button in the VAL List screen and a VAP Configuration screen will appear for you to configure the required settings

VAP Configuration <span>↑</span> <span>×</span>	
Item	Setting
▶ VAP	VAP1
▶ SSID	Staff_2.4G
▶ Max. STA	<input type="checkbox"/> Enable
▶ Authentication	WPA2-PSK
▶ Encryption	AES
▶ Preshared Key	1234567890
▶ STA Isolation	<input checked="" type="checkbox"/>
▶ Broadcast SSID	<input checked="" type="checkbox"/>
▶ Enable	<input checked="" type="checkbox"/>

For a detailed description of VAP configuration, please refer to the description stated in AP-Router section.

## WDS Hybrid Mode

For WDS Hybrid mode, the device bridges all the wired **LAN** and **WLAN** clients to another WDS or WDS hybrid enabled Wi-Fi devices with which the device associated with.

# EW200 Industrial Cellular Gateway

▶ WiFi Operation Mode	WDS Hybrid Mode ▾
▶ Lazy Mode	<input type="checkbox"/> Enable
▶ Green AP	<input type="checkbox"/> Enable
▶ VAP Isolation	<input checked="" type="checkbox"/> Enable
▶ Time Schedule	(0) Always ▾
▶ Scan Remote AP's MAC List	Scan
Remote AP MAC 1	<input type="text"/>
Remote AP MAC 2	<input type="text"/>
Remote AP MAC 3	<input type="text"/>
Remote AP MAC 4	<input type="text"/>

WDS Hybrid Mode		
Item	Value setting	Description
<b>Lazy Mode</b>	The box is checked by default.	Check the <b>Enable</b> box to activate this function. With the function enabled, the device can auto-learn WDS peers without manually entering the other AP's MAC address. But at least one of the APs has to fill remote AP MAC addresses.
<b>Green AP</b>	Unchecked by default	Check the <b>Enable</b> box to activate <b>Green AP</b> function.
<b>VAP Isolation</b>	The box is checked by default.	Check the <b>Enable</b> box to activate this function. By default, the box is checked; it means that stations which associated to different VAPs cannot communicate with each other.
<b>Time Schedule</b>	Required setting	Apply a specific <b>Time Schedule</b> to this rule; otherwise leave it as <b>(0) Always</b> . If the dropdown list is empty ensure <b>Time Schedule</b> is pre-configured. Refer to <b>Object Definition &gt; Scheduling &gt; Configuration</b> tab.
<b>Scan Remote AP's MAC List</b>	Available when Lazy Mode disabled.	Press the <b>Scan</b> button to scan the spatial AP information, and then select one from the AP list, the MAC of selected AP will be auto filled in the following Remote AP MAC table.
<b>Remote AP MAC 1~4</b>	Available when Lazy Mode disabled.	Enter the remote AP's MAC manually, or via auto-scan approach, The device will bridge the traffic to the remote AP when associated successfully.

2.4G VAP List <span>Add</span> <span>Delete</span> <span>↑</span> <span>×</span>								
ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	Staff_2.4G	WPA2-PSK	AES	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<span>Edit</span> <input type="checkbox"/> Select

By default, VAP 1 is enabled and security key is required to connect to the gateway wirelessly to enhance the security level and prevent unexpected access of un-authorized devices.

The default wifi key is printed on both the device label and the Security Card. It is created randomly and differs from devices. So, you can connect to the VAP1 (SSID: Staff\_2.4G) with the provided key.




However, it is strongly recommended that you change the security key to an easy-to-remember one by clicking the **Edit** button.

# EW200 Industrial Cellular Gateway

Under **WDS Hybrid** mode, the VAP function is available and you can further specify the required VAP settings for connecting with wireless client devices.




Click **Add** / **Edit** button in the VAL List screen to create or edit the settings for a VAP. A VAP Configuration screen will appear.

For VAP 1:

 VAP Configuration  

Item	Setting
▶ VAP	VAP1
▶ SSID	Staff_2.4G
▶ Max. STA	<input type="checkbox"/> Enable
▶ Authentication	WPA2-PSK
▶ Encryption	AES
▶ Preshared Key	1234567890
▶ STA Isolation	<input checked="" type="checkbox"/>
▶ Broadcast SSID	<input checked="" type="checkbox"/>
▶ Enable	<input checked="" type="checkbox"/>

For Others:

 VAP Configuration  

Item	Setting
▶ VAP	VAP2
▶ SSID	default
▶ Max. STA	<input type="checkbox"/> Enable
▶ Authentication	Open
▶ Encryption	None
▶ STA Isolation	<input type="checkbox"/>
▶ Broadcast SSID	<input type="checkbox"/>
▶ Enable	<input type="checkbox"/>

For a detailed description of VAP configuration, refer to the description stated in AP-Router section.



# EW200 Industrial Cellular Gateway

## 2.3.2 Wireless Client List

The **Wireless Client List** page shows the information of wireless clients which are associated with this device.

Go to **Basic Network > Wi-Fi > Wireless Client List** Tab.

### Select Target Wi-Fi

Target WiFi [ Help ]	
Item	Setting
▶ Module Select	One ▼
▶ Operation Band	2.4G ▼
▶ Multiple AP Names	All ▼

Target Configuration		
Item	Value setting	Description
<b>Module Select</b>	Required setting.	Select the Wi-Fi module to check the information of connected clients. For single Wi-Fi module products, this option is hidden.
<b>Operation Band</b>	Required setting.	Specify the intended operation band for the Wi-Fi module. Usually this setting is fixed and cannot be changed once the module is integrated into the product. However, there are some modules with selectable band. Under such situation, you can specify which operation band is suitable for the application.
<b>Multiple AP Names</b>	1. Required setting. 2. All is selected by default.	Specify the VAP to show the associated clients information in the following Client List. By default, All VAP is selected.

### Show Client List

The following Client List shows the information for wireless clients that is associated with the selected VAP(s).

Client List								
IP Address Configuration & Address	Host Name	MAC Address	Mode	Rate	RSSI0	RSSI1	Signal	Interface

Target Configuration		
Item	Value setting	Description
<b>IP Address Configuration &amp; Address</b>	N/A	It shows the Client's IP address and the deriving method. <b>Dynamic</b> means the IP address is derived from a DHCP server. <b>Static</b> means the IP address is a fixed one that is self-filled by client.
<b>Host Name</b>	N/A	It shows the host name of client.
<b>MAC Address</b>	N/A	It shows the MAC address of client.
<b>Mode</b>	N/A	It shows what kind of <b>Wi-Fi system</b> the client used to associate with this device.

## EW200 Industrial Cellular Gateway

---

<b>Rate</b>	N/A	It shows the <b>data rate</b> between client and this device.
<b>RSSI0, RSSI1</b>	N/A	It shows the RX sensitivity (RSSI) value for each radio path.
<b>Signal</b>	N/A	The <b>signal strength</b> between client and this device.
<b>Interface</b>	N/A	It shows the VAP ID that the client is associated with.
<b>Refresh</b>	N/A	Click the <b>Refresh</b> button to update the Client List immediately.

# EW200 Industrial Cellular Gateway

## 2.3.3 Advanced Configuration

This device provides advanced wireless configuration for professional users to optimize wireless performance under specific installation environments. Please note that if you are not familiar with Wi-Fi technology, just leave the advanced configuration at the default values.

Go to **Basic Network > Wi-Fi > Advanced Configuration** Tab.

### Select Target Wi-Fi

Target WiFi [ Help ]	
Item	Setting
▶ Module Select	One ▼
▶ Operation Band	2.4G ▼

Target Configuration		
Item	Value setting	Description
Module Select	Required setting.	Select the Wi-Fi module to check the information of connected clients. For single Wi-Fi module products, this option is hidden.
Operation Band	Required setting.	Specify the intended operation band for the Wi-Fi module. Usually this setting is fixed and cannot be changed once the module is integrated into the product. However, there are some modules with selectable band.

### Setup Advanced Configuration

Advanced Configuration	
Item	Setting
▶ Regulatory Domain	(1-11)
▶ Beacon Interval	100 Range: (1~1000 msec)
▶ DTIM Interval	3 Range: (1~255)
▶ RTS Threshold	2347 Range: (1~2347)
▶ Fragmentation	2346 Range: (256~2346)
▶ WMM	<input checked="" type="checkbox"/> Enable
▶ Short GI	400ns ▼
▶ TX Rate	Best ▼
▶ RF Bandwidth	Auto ▼
▶ Transmit Power	100% ▼
▶ WIDS	<input type="checkbox"/> Enable

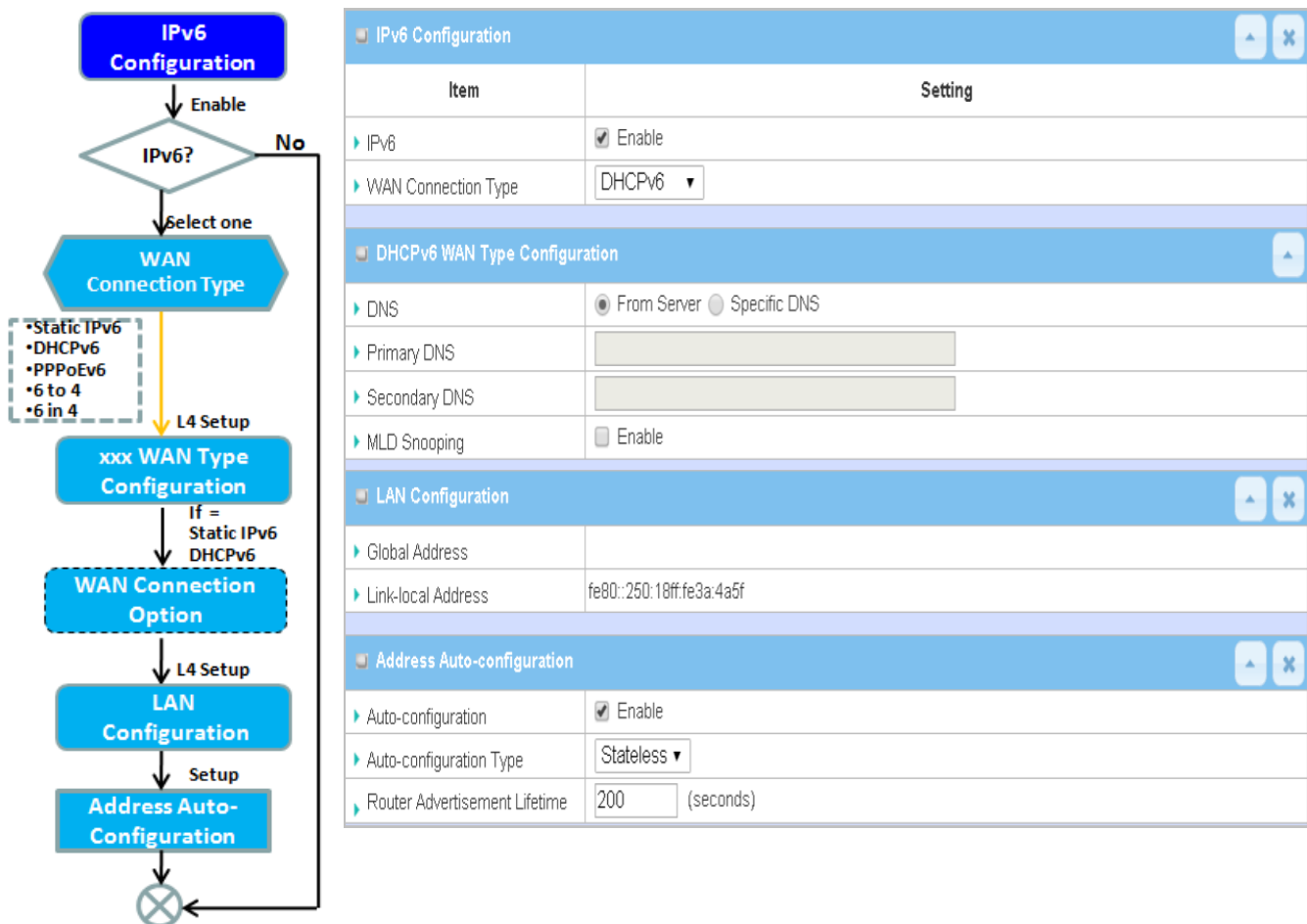
# EW200 Industrial Cellular Gateway

Advanced Configuration		
Item	Value setting	Description
<b>Regulatory Domain</b>	The default setting depends on location where product is sold	It limits the available radio channels of this device. The permissible channels depend on the local <b>Regulatory Domain</b> .
<b>Beacon Interval</b>	100	It shows the time interval between each beacon packet broadcasted. The beacon packet contains <b>SSID</b> , <b>Channel ID</b> and <b>Security setting</b> .
<b>DTIM Interval</b>	3	A <b>DTIM (Delivery Traffic Indication Message)</b> is a countdown informing clients of the next window for listening to broadcast message. When the device has buffered broadcast message for associated client, it sends the next DTIM with a DTIM value.
<b>RTS Threshold</b>	2347	<b>RTS (Request to send) Threshold</b> means when the packet size is over the setting value, then <b>RTS</b> is activated. RTS/CTS is a <b>collision avoidance</b> technique. RTS is <b>never</b> activated when the threshold is set to <b>2347</b> .
<b>Fragmentation</b>	2346	Wireless frames can be divided into smaller units (fragments) to <b>improve performance</b> in the presence of RF interference at the limits of RF coverage.
<b>WMM</b>	The box is checked by default	<b>WMM (Wi-Fi Multimedia)</b> can help control <b>latency</b> and <b>jitter</b> when transmitting <b>multimedia content</b> over a wireless connection.
<b>Short GI</b>	By default <b>400ns</b> is selected	<b>Short GI (Guard Interval)</b> is defined to set the sending interval between each packet. Note that lower <b>Short GI</b> could <b>increase</b> not only the <b>transition rate</b> but also <b>error rate</b> .
<b>TX Rate</b>	By default <b>Best</b> is selected	<b>Data transmission rate</b> . When <b>Best</b> is selected, the device will choose a proper <b>data rate</b> according to <b>signal strength</b> .
<b>RF Bandwidth</b>	By default <b>Auto</b> is selected	The setting of RF bandwidth limits the maximum data rate.
<b>Transmit Power</b>	By default <b>100%</b> is selected	Normally the wireless transmitter operates at 100% power. Set the <b>transmit power</b> to control the Wi-Fi <b>coverage</b> .
<b>5G Band Steering</b>	Unchecked by default	When a client is connected to 2.4G Wi-Fi, the device will send the client to the less congested 5G band automatically. This option is only available on modules that supports 5GHz band.
<b>WIDS</b>	Unchecked by default	The WIDS (Wireless Intrusion Detection System) will analyze all packets and make a table of statistics showing Wi-Fi status. Go to <b>Status &gt; Basic Network &gt; Wi-Fi</b> tab for detailed WIDS status.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the current configuration.
<b>Undo</b>	N/A	Click the <b>Undo</b> button to restore configuration to previous setting before saving.

## 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, and PPPoEv6.

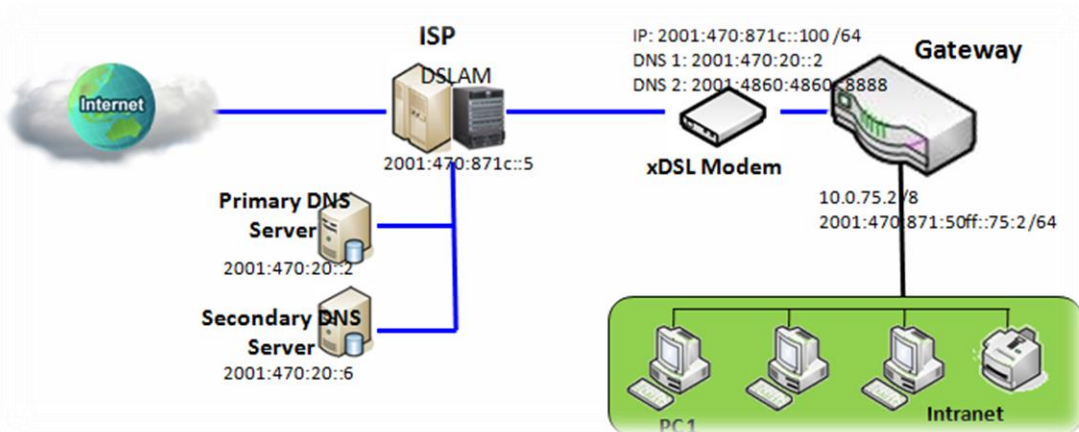
Note: The available WAN connection types can be different, depending on the Interface type of WAN-1.

# EW200 Industrial Cellular Gateway

## IPv6 WAN Connection Type

### Static IPv6

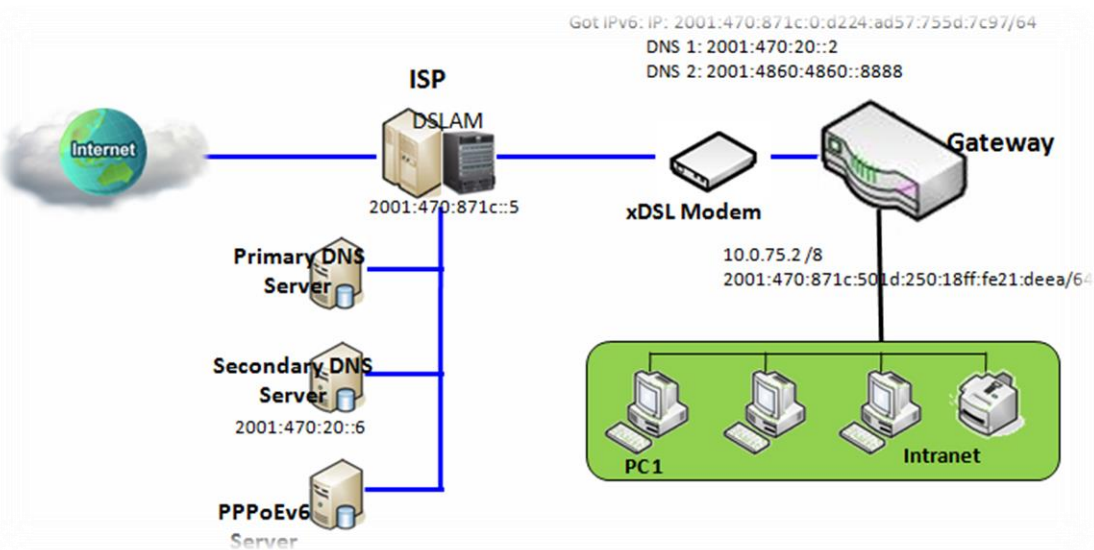
Static IPv6 does the same function as static IPv4. The static IPv6 provides manual setting of IPv6 address, IPv6 default gateway address, and IPv6 DNS.



Above diagram depicts IPv6 IP addressing. Use the information provided by your ISP to setup the IPv6 network.

### DHCPv6

DHCP in IPv6 performs 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 then has to resend a request to renew the IPv6 address.

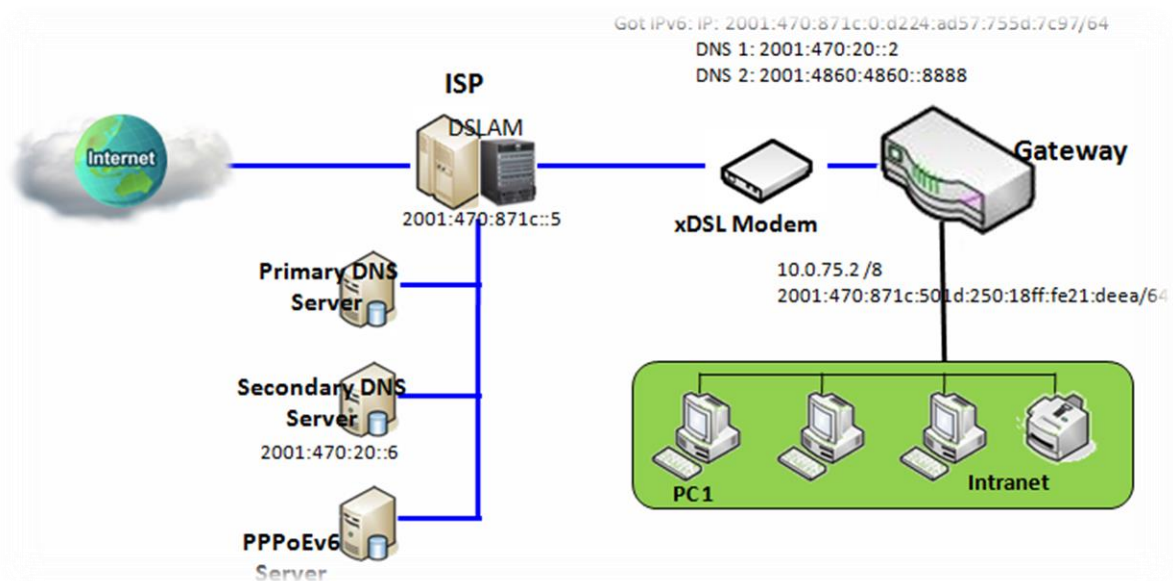


The above diagram depicts DHCP IPv6 IP addressing. The DHCPv6 server on the ISP side assigns IPv6 address, IPv6 default gateway address, and IPv6 DNS to client hosts automatically.

# EW200 Industrial Cellular Gateway

## PPPoEv6

PPPoEv6 in IPv6 performs the same function as PPPoE in IPv4. The PPPoEv6 server provides configuration parameters based on PPPoEv6 client requests. When a PPPoEv6 server gets a 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. A PPPoEv6 server (DSLAM) on the ISP side provides IPv6 configuration upon receiving a PPPoEv6 client request.

## 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	<input checked="" type="checkbox"/> Enable
▶ WAN Connection Type	DHCPv6 ▼

# EW200 Industrial Cellular Gateway

IPv6 Configuration		
Item	Value setting	Description
IPv6	Unchecked by default	Check the <b>Enable</b> box to activate the IPv6 function.
WAN Connection Type	1. Can only be selected when IPv6 Enabled 2. Required setting	Define the selected IPv6 WAN Connection Type to establish the IPv6 connectivity.  Select <b>Static IPv6</b> when your ISP provides you with a set IPv6 addresses. Then go to <b>Static IPv6 WAN Type Configuration</b> . Select <b>DHCPv6</b> when your ISP provides you with DHCPv6 services. Select <b>PPPoEv6</b> when your ISP provides you with PPPoEv6 account settings.  <b>Note:</b> The available WAN connection types can be different, depending on the Interface type of WAN-1.

## Static IPv6 WAN Type Configuration

Static IPv6 WAN Type Configuration	
▶ IPv6 Address	<input type="text"/>
▶ Subnet Prefix Length	<input type="text"/>
▶ Default Gateway	<input type="text"/>
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ MLD Snooping	<input type="checkbox"/> Enable

Static IPv6 WAN Type Configuration		
Item	Value setting	Description
IPv6 Address	Required setting	Enter the WAN <b>IPv6 Address</b> for the router.
Subnet Prefix Length	Required setting	Enter the WAN <b>Subnet Prefix Length</b> for the router.
Default Gateway	Required setting	Enter the WAN <b>Default Gateway</b> IPv6 address.
Primary DNS	Optional setting	Enter the WAN <b>primary DNS Server</b> .
Secondary DNS	Optional setting	Enter the WAN <b>secondary DNS Server</b> .
MLD Snooping	Unchecked by default	Enable/Disable the MLD Snooping function

## LAN Configuration

LAN Configuration	
▶ Global Address	<input type="text"/> /64
▶ Link-local Address	fe80::250:18ff:fe16:1123



## EW200 Industrial Cellular Gateway

---

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

Go to **Address Auto-configuration (summary)** to set up the LAN environment.

When the above settings are configured, click the **Save** button to save the configuration, and click the **Reboot** button to reboot the router.

# EW200 Industrial Cellular Gateway

## DHCPv6 WAN Type Configuration

DHCPv6 WAN Type Configuration	
▶ DNS	<input checked="" type="radio"/> From Server <input type="radio"/> Specific DNS
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ MLD Snooping	<input type="checkbox"/> Enable

DHCPv6 WAN Type Configuration		
Item	Value setting	Description
DNS	The option [From Server] is selected by default	Select the [Specific DNS] option to activate Primary DNS and Secondary DNS. Then fill in the DNS information.
Primary DNS	Cannot be modified by default	Enter the WAN <b>primary DNS Server</b> .
Secondary DNS	Cannot be modified by default	Enter the WAN <b>secondary DNS Server</b> .
MLD	Unchecked by default	Enable/Disable the MLD Snooping function

## LAN Configuration

LAN Configuration	
▶ Global Address	
▶ Link-local Address	fe80::250:18ff:fe16:1123

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

Go to **Address Auto-configuration (summary)** to set up the LAN environment.

When above settings are configured, click the **Save** button to save the configuration, and click **Reboot** button to reboot the router.

# EW200 Industrial Cellular Gateway

## PPPoEv6 WAN Type Configuration

PPPoEv6 WAN Type Configuration	
▶ Account	<input type="text"/>
▶ Password	<input type="text"/>
▶ Service Name	<input type="text"/>
▶ Connection Control	Auto-reconnect (Always on)
▶ MTU	<input type="text"/>
▶ MLD Snooping	<input type="checkbox"/> Enable

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

## LAN Configuration

LAN Configuration	
▶ Global Address	
▶ Link-local Address	fe80::250:18ff:fe16:1123

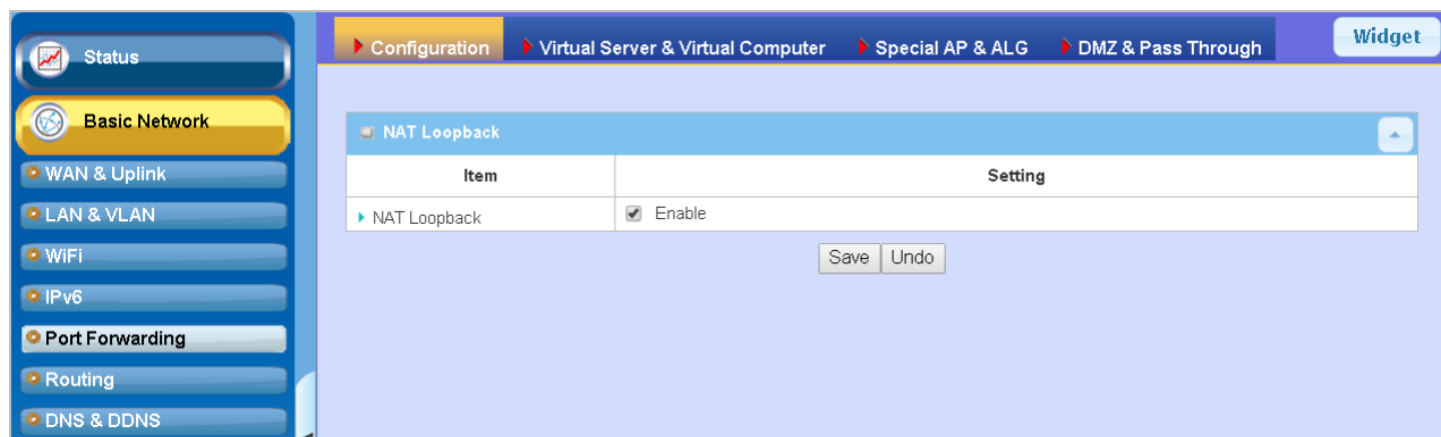
LAN Configuration Item	Value setting	Description
Global Address	Value auto-created	The LAN <b>IPv6 Address</b> for the router.
Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

Go to **Address Auto-configuration (summary)** to set up up the LAN environment.

When above settings are configured, click the **save button** to save the configuration and click **reboot button** to reboot the router.

## 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. This product 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.

# EW200 Industrial 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 NAT loopback feature is enabled. When accessing the email server from 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 <span>[ Help ]</span>	
Item	Setting
▶ NAT Loopback	<input checked="" type="checkbox"/> Enable

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

# EW200 Industrial Cellular Gateway

## 2.5.2 Virtual Server & Virtual Computer

Configuration

Item	Setting
Virtual Server	<input type="checkbox"/> Enable
Virtual Computer	<input checked="" type="checkbox"/> Enable

Virtual Server List

AddDelete

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

Virtual Computer List

AddDelete

ID	Global IP	Local IP	Enable	Actions
----	-----------	----------	--------	---------

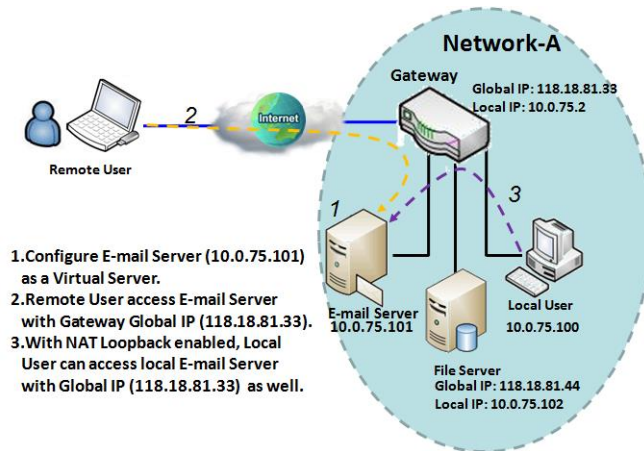
There are some important Port Forwarding functions implemented within the gateway, including "Virtual Server", "NAT loopback" and "Virtual Computer".

These allow personnel to access servers behind the gateway from outside the network. Those servers can be set up by using "Virtual Server" feature. NAT Loopback can allow access to servers from the LAN side with a global IP address and no change in settings.

"Virtual computer" is a host behind a 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, just map the local IP of the virtual computer to a global IP.

# EW200 Industrial Cellular Gateway

## Virtual Server & NAT Loopback

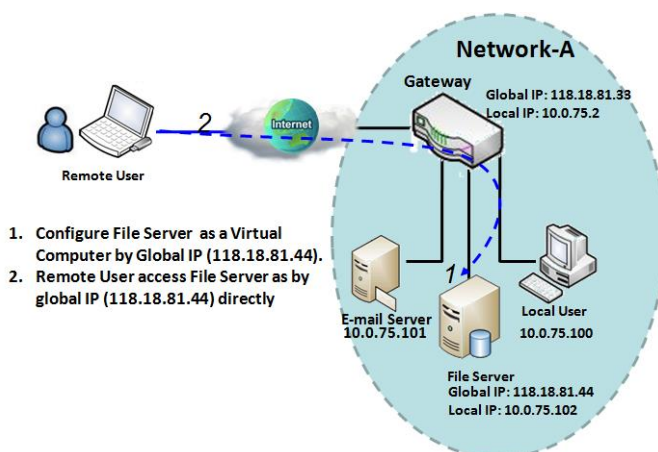


"Virtual Server" allows you to access servers with the global IP address or FQDN of the gateway as if they are servers existing in the Internet. But in fact, these servers are located in the Intranet and are physically behind the gateway. The gateway serves the service requests by port forwarding the requests to the LAN servers and transfers the replies from LAN servers to the requester on the WAN side. As shown in the 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.

# EW200 Industrial 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	<input checked="" type="checkbox"/> Enable
▶ Virtual Computer	<input checked="" type="checkbox"/> Enable

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

### Create / Edit Virtual Server

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

Virtual Server List <span>Add</span> <span>Delete</span>								
ID	WAN Interface	Server IP	Protocol	Public Port	Private Port	Time Schedule	Enable	Actions

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



# EW200 Industrial Cellular Gateway

Virtual Server Rule Configuration	
Item	Setting
▶ WAN Interface	<input checked="" type="checkbox"/> All <input type="checkbox"/> WAN-1 <input type="checkbox"/> WAN-2 <input type="checkbox"/> WAN-3
▶ Server IP	<input type="text"/>
▶ Source IP	Any ▼
▶ Protocol	TCP(6) & UDP(17) ▼
▶ Public Port	Single Port ▼ <input type="text"/>
▶ Private Port	Single Port ▼ <input type="text"/>
▶ Time Schedule	(0) Always ▼
▶ Rule	<input type="checkbox"/> Enable

Virtual Server Rule Configuration		
Item	Value setting	Description
<b>WAN Interface</b>	1. Required setting 2. Default is <b>ALL</b> .	<p>Define the selected interface to be the packet-entering interface of the gateway.</p> <p>If the packets to be filtered are coming from <b>WAN-x</b> then select <b>WAN-x</b> for this field.</p> <p>Select <b>ALL</b> for packets coming into the gateway from any interface.</p> <p><b>Note:</b> The available check boxes (<b>WAN-1 ~ WAN-4</b>) depend on the number of WAN interfaces for the product.</p>
<b>Server IP</b>	Required setting	<p>This field is to specify the IP address of the interface selected in the WAN Interface setting above.</p>
<b>Source IP</b>	1. Required setting 2. <b>Any is selected by default</b>	<p>This field is to specify the <b>Source IP</b> address.</p> <p>Select Any to allow the access coming from any IP addresses.</p> <p>Select Specific IP Address to allow the access coming from an IP address.</p> <p>Select IP Range to allow the access coming from a specified range of IP address.</p>
<b>Protocol</b>	Required setting	<p>When “<b>ICMPv4</b>” is selected, the protocol of packet filter rule is ICMPv4. Apply <b>Time Schedule</b> to this rule, otherwise leave it as <b>Always</b>. (Refer to <b>Scheduling setting</b> under <b>Object Definition</b>). Check <b>Enable</b> box to enable this rule.</p> <p>When “<b>TCP</b>” is selected, the protocol of packet filter rule is TCP.</p> <p><b>Public Port</b> is a predefined port from <b>Well-known Service</b>, and <b>Private Port</b> is the same as <b>Public Port</b> number.</p> <p><b>When Public Port</b> is set as <b>Single Port</b> and a port number specified, <b>Private Port</b> can be set as <b>Single Port</b> number.</p> <p>When Public Port is set as Port Range and a port range specified, Private Port can be set to Single Port or Port Range.</p> <p><u>Value Range:</u> 1 ~ 65535 for Public Port, Private Port.</p> <p>When “<b>UDP</b>” is selected, the protocol of packet filter rule is UDP.</p> <p><b>Public Port</b> is a predefined port from <b>Well-known Service</b>, and <b>Private Port</b> is the same as <b>Public Port</b> number.</p>

# EW200 Industrial Cellular Gateway

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

# EW200 Industrial Cellular Gateway

## Create / Edit Virtual Computer

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

Virtual Computer List <input type="button" value="Add"/> <input type="button" value="Delete"/>				
ID	Global IP	Local IP	Enable	Actions

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

Virtual Computer Rule Configuration <span>[ Help ]</span>		
Global IP	Local IP	Enable
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
<input type="button" value="Save"/>		

Virtual Computer Rule Configuration		
Item	Value setting	Description
Global IP	Required setting	Specify the IP address of the WAN IP.
Local IP	Required setting	Specify the IP address of the LAN IP.
Enable	N/A	Check <b>Enable</b> box to enable this rule.
Save	N/A	Click the <b>Save</b> button to save the settings.

# EW200 Industrial Cellular Gateway

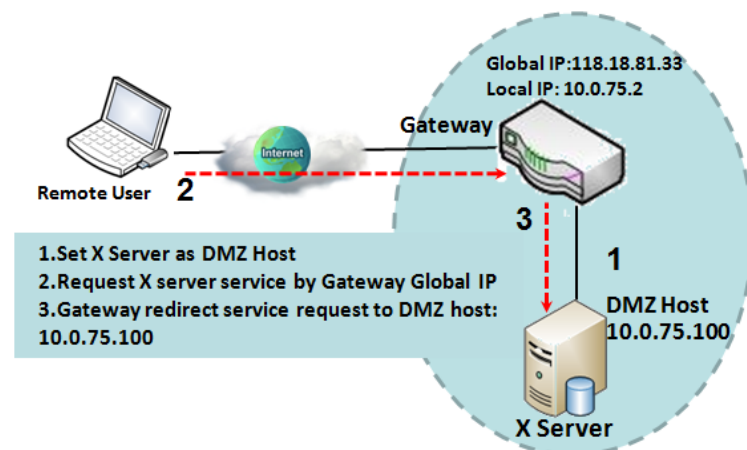
## 2.5.3 DMZ & Pass Through

A DMZ (Demilitarized Zone) Host is a host that is exposed to the Internet but still within the protection of a firewall by gateway device. This 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 set the LAN computer as a DMZ host to solve this problem.

The DMZ function allows you to ask the gateway to pass through all normal packets to the DMZ host behind the NAT gateway only when these packets are not expected to be received by applications in the gateway or by other client hosts in the Intranet. 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	
Item	Setting
DMZ	<input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> All <input type="checkbox"/> WAN-1 <input type="checkbox"/> WAN-2 <input type="checkbox"/> WAN-3 <input type="checkbox"/> WAN-4 DMZ Host : <input type="text" value="10.0.75.100"/>
Pass Through Enable	<input checked="" type="checkbox"/> IPSec <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP

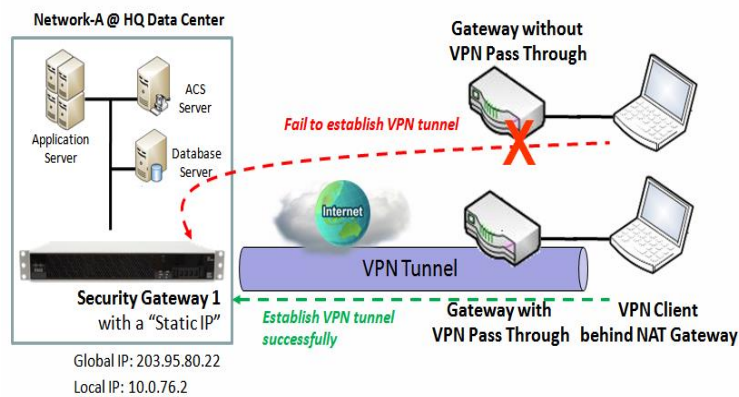
### DMZ Scenario



When the network administrator wants to set up service daemons in a host behind a NAT gateway to allow remote users to actively request services from the server, the host should be configured as a DMZ Host. As shown in the diagram, there is an X server installed as DMZ host, whose IP address is 10.0.75.100. A 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.

# EW200 Industrial 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 supports the pass through function for IPsec, PPTP, and L2TP connections.

## DMZ & Pass Through Setting

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

### Enable DMZ and Pass Through

Configuration [ Help ]	
Item	Setting
▶ DMZ	<input type="checkbox"/> Enable <input checked="" type="checkbox"/> All <input type="checkbox"/> WAN-1 <input type="checkbox"/> WAN-2 <input type="checkbox"/> WAN-3 <input type="checkbox"/> WAN-4 DMZ Host : <input type="text"/>
▶ Pass Through Enable	<input checked="" type="checkbox"/> IPsec <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP

Configuration Item	Value setting	Description
DMZ	1. Required setting 2. Default is <b>ALL</b> .	Check the <b>Enable</b> 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 <b>DMZ Host</b> field. If the packets to be filtered are coming from <b>WAN-x</b> then select <b>WAN-x</b> for this field. Select <b>ALL</b> for packets coming into the router from any interfaces. <b>Note:</b> The available check boxes ( <b>WAN-1 ~ WAN-4</b> ) depend on the number of WAN interfaces for the product.
Pass Through Enable	Boxes are checked by default	Check the box to enable pass through function for <b>IPsec</b> , <b>PPTP</b> , and <b>L2TP</b> . With the pass through function enabled, the VPN hosts behind the gateway can still connect to remote VPN servers.
Save	N/A	Click the <b>Save</b> button to save the settings.
Undo	N/A	Click the <b>Undo</b> button to cancel the settings

# EW200 Industrial Cellular Gateway

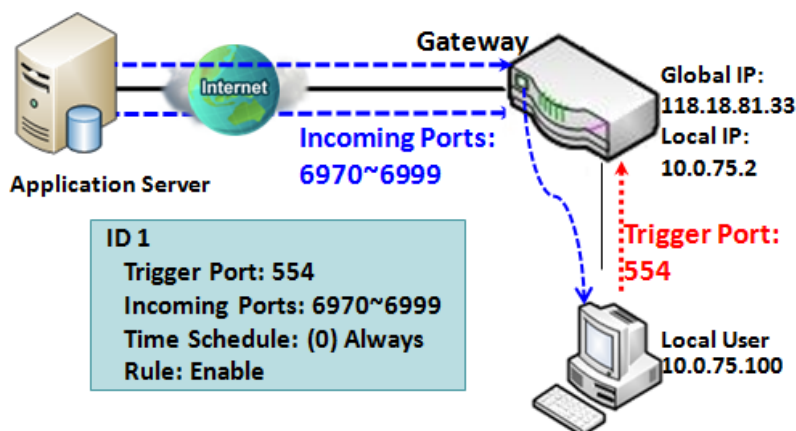
## 2.5.4 Special AP & ALG

A NAT gateway doesn't allow active connection requests from the outside world, they are ignored. But at the client hosts in the Intranet, users may use applications that need more service ports to be allowed for passing through the NAT gateway. The "Special AP (application)" feature in the gateway can solve this problem. That is, some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT gateway. The Special AP feature allows some of these applications to work with this product.

Application-level gateway (ALG) allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, BitTorrent, SIP, RTSP, file transfer in IM applications, etc. In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open up port mappings (firewall pinhole) dynamically as required. Legitimate application data can thus be passed through the security checks of the firewall or NAT that would have otherwise restricted the traffic for not meeting its limited filter criteria.

### Special AP

Special AP List <span>Add</span> <span>Delete</span>						
ID	WAN Interface	Trigger Port	Incoming Ports	Time Schedule	Enable	Actions
1	ALL	554	6970-6999	(0) Always	<input checked="" type="checkbox"/>	<span>Edit</span> <input type="checkbox"/> Select
2	ALL	47624	2300-2400,28800-29000	(0) Always	<input checked="" type="checkbox"/>	<span>Edit</span> <input type="checkbox"/> Select



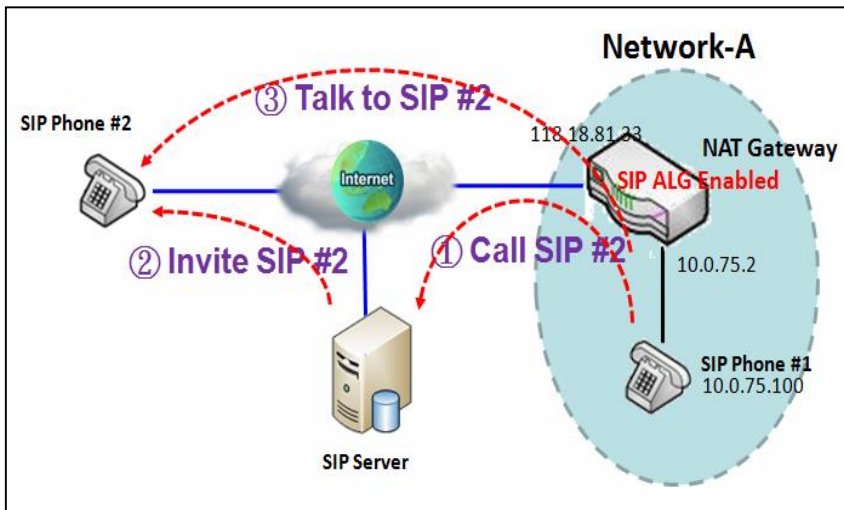
The Special AP feature allows you to request the gateway to open pre-defined service ports for incoming packets to pass through once the trigger port is activated by local hosts. As shown in the diagram, special AP rule define port **554** as trigger port and **6970~6999** as incoming ports. With this setting, a local user at host 10.0.75.100 can enjoy music by using the QuickTime application, whose media server is located in the Internet. When you open the application, it will activate the Trigger Port and then

incoming data packets from the remote application server will pass through incoming port 6970~6999.

# EW200 Industrial Cellular Gateway

## SIP ALG

This gateway supports the SIP ALG feature to allow one SIP phone behind the NAT gateway to call another SIP phone in the Internet, even if the gateway executes its NAT mechanism between the Intranet and the Internet. The NAT gateway monitors the control traffic and opens up port mappings (firewall pinhole) dynamically as required to know about an address/port number combination that allows incoming packets, so it will support address and port translation for SIP application layer "control/data" protocols as shown in following diagram. The NAT Gateway enables the SIP ALG feature, so it will monitor the SIP Phone #1 actions, open up the required ports and make the address and port translation in a SIP voice communication.



As shown in the diagram, the calling starts from the SIP Phone #1 to the SIP server via the NAT gateway. Then the SIP server invites the SIP Phone #2 and finally, the SIP Phone #1 talks to the SIP Phone #2. But for the NAT gateway, SIP Phone #2 is an unknown host, so the active access from the Phone #2 will be treated as unexpected traffic and will be blocked out. With the SIP ALG function enabled, the NAT gateway will monitor the control traffic for the SIP calls, and recognize the traffic from SIP Phone #2 is part of the connection sessions with SIP Phone #1.

# EW200 Industrial Cellular Gateway

## Special AP & ALG Setting

Go to **Basic Network > Port Forwarding > Special AP & ALG** tab.

The Special AP setting allows some applications require multiple connections. The ALG setting allows user to Support some SIP ALG, like STUN.

### Enable Special AP & ALG

Configuration	
Item	Setting
▶ Special AP	<input checked="" type="checkbox"/> Enable
▶ ALG Enable	<input checked="" type="checkbox"/> SIP ALG

Configuration Item	Value setting	Description
<b>Special AP</b>	The box is checked by default	Check the <b>Enable</b> box to activate the Special AP function.
<b>ALG Enable</b>	The box is checked by default	Check the <b>Enable</b> box to activate the SIP ALG function.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the settings.
<b>Undo</b>	N/A	Click the <b>Undo</b> button to cancel the settings

### Create / Edit Special AP Rule

The gateway allows you to customize Special AP rules. It supports up to a maximum of 8 rule-based Special AP sets.

Special AP List <span>Add</span> <span>Delete</span>						
ID	WAN Interface	Trigger Port	Incoming Ports	Time Schedule	Enable	Actions

When the **Add** button is applied, the **Special AP Rule Configuration** screen will appear.

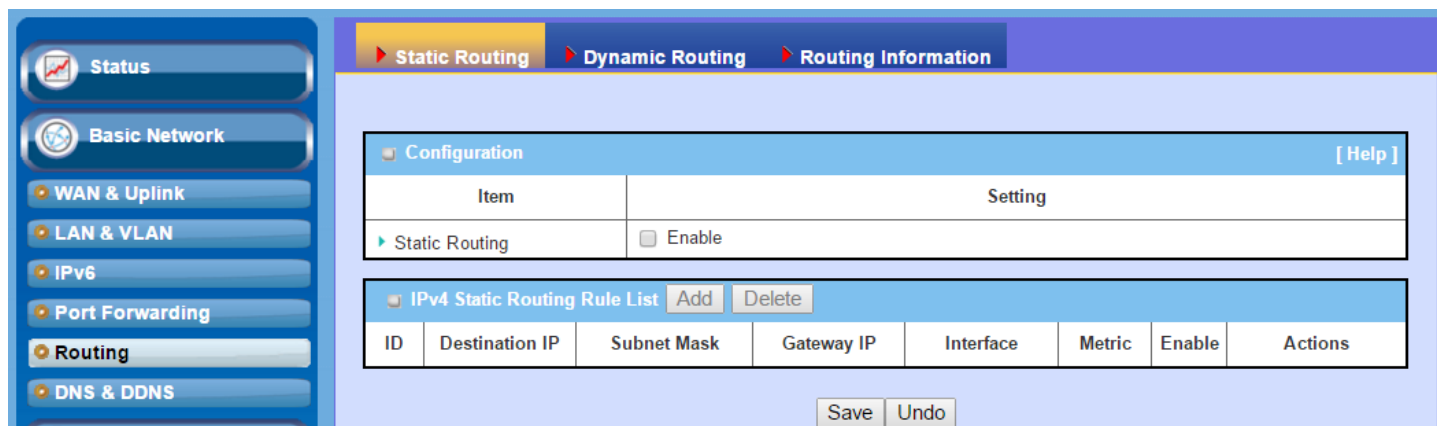


# EW200 Industrial Cellular Gateway

Special AP Rule Configuration [ Help ]	
Item	Setting
▶ WAN Interface	<input checked="" type="checkbox"/> ALL <input type="checkbox"/> WAN-1 <input type="checkbox"/> WAN-2 <input type="checkbox"/> WAN-3
▶ Trigger Port	Port : <input type="text"/> Popular Applications : <input type="text" value="User-defined"/> ▼
▶ Incoming Ports	<input type="text"/>
▶ Time Schedule	<input type="text" value="(0) Always"/> ▼
▶ Rule	<input type="checkbox"/>
<input type="button" value="Save"/>	

IP Translation Configuration		
Item	Value setting	Description
<b>WAN Interface</b>	1. Required setting 2. <b>All</b> is checked by default.	Check the interface box(es) for which the Special AP rule will be applied. By default, <b>All</b> is checked, and the Special AP rule will be applied to all WAN interfaces.
<b>Trigger Port</b>	1. Required setting 2. <b>User-defined</b> is selected by default.	Enter the expected trigger port (or port range) if <b>User-defined</b> is selected in the dropdown list. If you select another popular application from the dropdown list, the corresponding trigger port(s) and incoming ports will be defined automatically. <b>Value Range: 1 ~ 65535.</b>
<b>Incoming Ports</b>	1. Required setting	Enter the expected Incoming ports if <b>User-defined</b> is selected in the Trigger Port dropdown list. If you select another popular application from the dropdown list, the corresponding incoming ports will be defined automatically. <b>Value Range: 1 ~ 65535; It can be a single port, multiple ports separated by “,”. or port range.</b>
<b>Time Schedule</b>	1. Required setting 2. <b>(0) Always</b> is selected by default.	Apply <b>Time Schedule</b> to this rule, otherwise leave it as Always. If the dropdown list is empty ensure <b>Time Schedule</b> is pre-configured. Refer to <b>Object Definition &gt; Scheduling &gt; Configuration</b> tab.
<b>Rule</b>	Unchecked by default	Check the <b>Enable</b> box to activate the special AP rule.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the settings.
<b>Undo</b>	N/A	Click the <b>Undo</b> button to cancel the settings

## 2.6 Routing

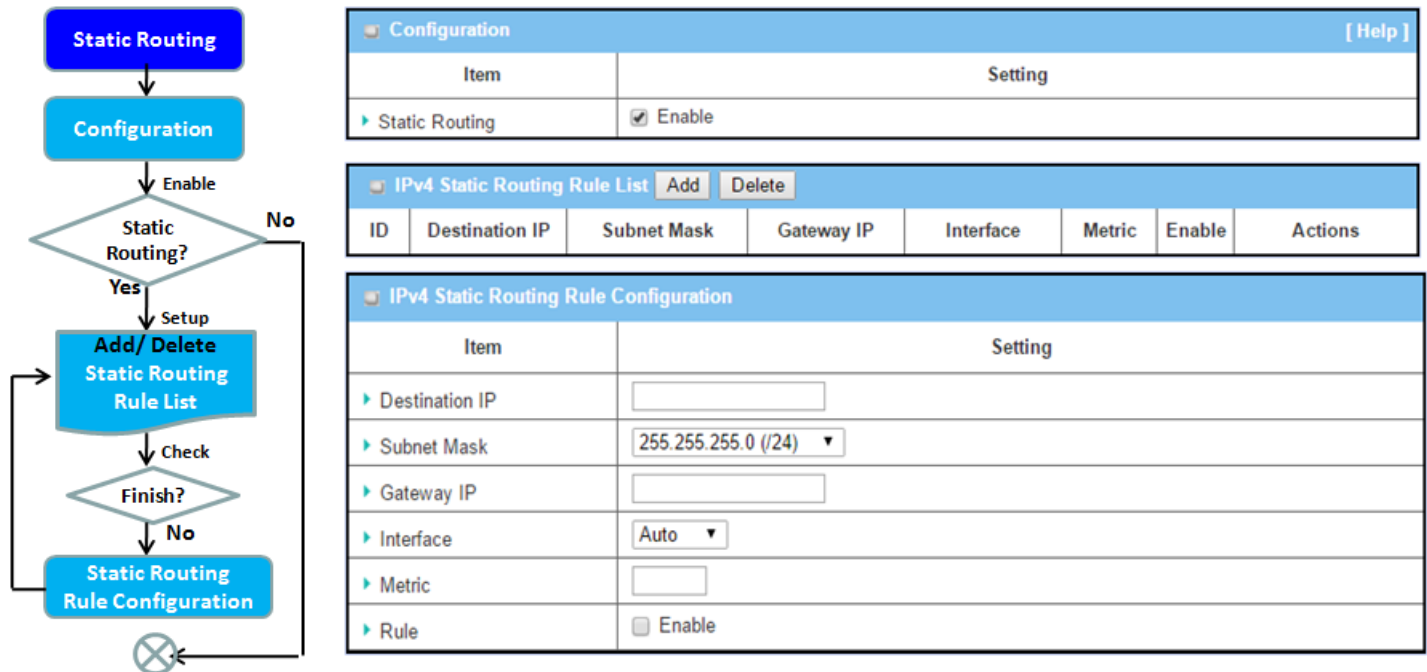


If you have more than one router and subnet, you will need to enable routing in order to allow packets to find a proper routing path and allow different subnets to communicate with each other. Routing is the process of selecting best paths in a network. It is performed for many kinds of networks, like 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.

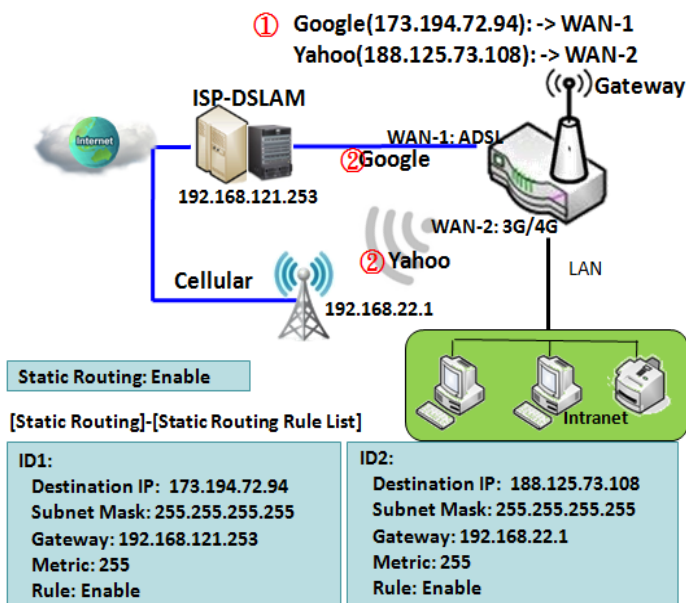
The routing tables can contain pre-defined routing paths for specific destinations. This is **static routing**. However, if the contents of routing tables record the obtained routing paths from neighbor routers by using protocols such as RIP, OSPF and BGP, this is **dynamic routing**. Both routing approaches will be illustrated. In addition, the gateway has advanced configurable routing software Quagga built-in for more complex routing applications. It can be configured via Telnet CLI.

# EW200 Industrial Cellular Gateway

## 2.6.1 Static Routing



"Static Routing" lets you define the routing paths for some dedicated hosts/servers or subnets to be stored 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 the gateway routing rule list.



When the administrator of the gateway wants to specify what kinds of packets will 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, rule 1 sets interface as ADSL, routing gateway as IP-DSLAM gateway 192.168.121.253. All packets to Google will go through WAN-1. The similar rule 2 sets 3G/4G as interface for traffic going to Yahoo.

# EW200 Industrial Cellular Gateway

## Static Routing Setting

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

There are three configuration windows for the static routing feature, including "Configuration", "Static Routing Rule List" and "Static Routing Rule Configuration". "Configuration" window lets you activate the global static routing feature. Even when there are existing routing rules, routing can be disabled temporarily by unchecking the Enable box. "Static Routing Rule List" window lists all your defined static routing rule entries. Use "Add" or "Edit" button to add and create one new static routing rule or to modify an existing 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

Check the **Enable** box to activate the "Static Routing" feature.

Configuration [ Help ]	
Item	Setting
Static Routing	<input checked="" type="checkbox"/> Enable

Static Routing		
Item	Value setting	Description
Static Routing	Unchecked by default	Check the <b>Enable</b> box to activate this function

### Create / Edit Static Routing Rules

The Static Routing Rule List shows the set up 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 <span>Add</span> <span>Delete</span>							
ID	Destination IP	Subnet Mask	Gateway IP	Interface	Metric	Enable	Actions

The gateway allows you to customize static routing rules. It supports up to a maximum of 64 rule sets. When the **Add** button is applied, the **Static Routing Rule Configuration** screen will appear, while the **Edit** button at the end of each static routing rule will let you modify the rule.

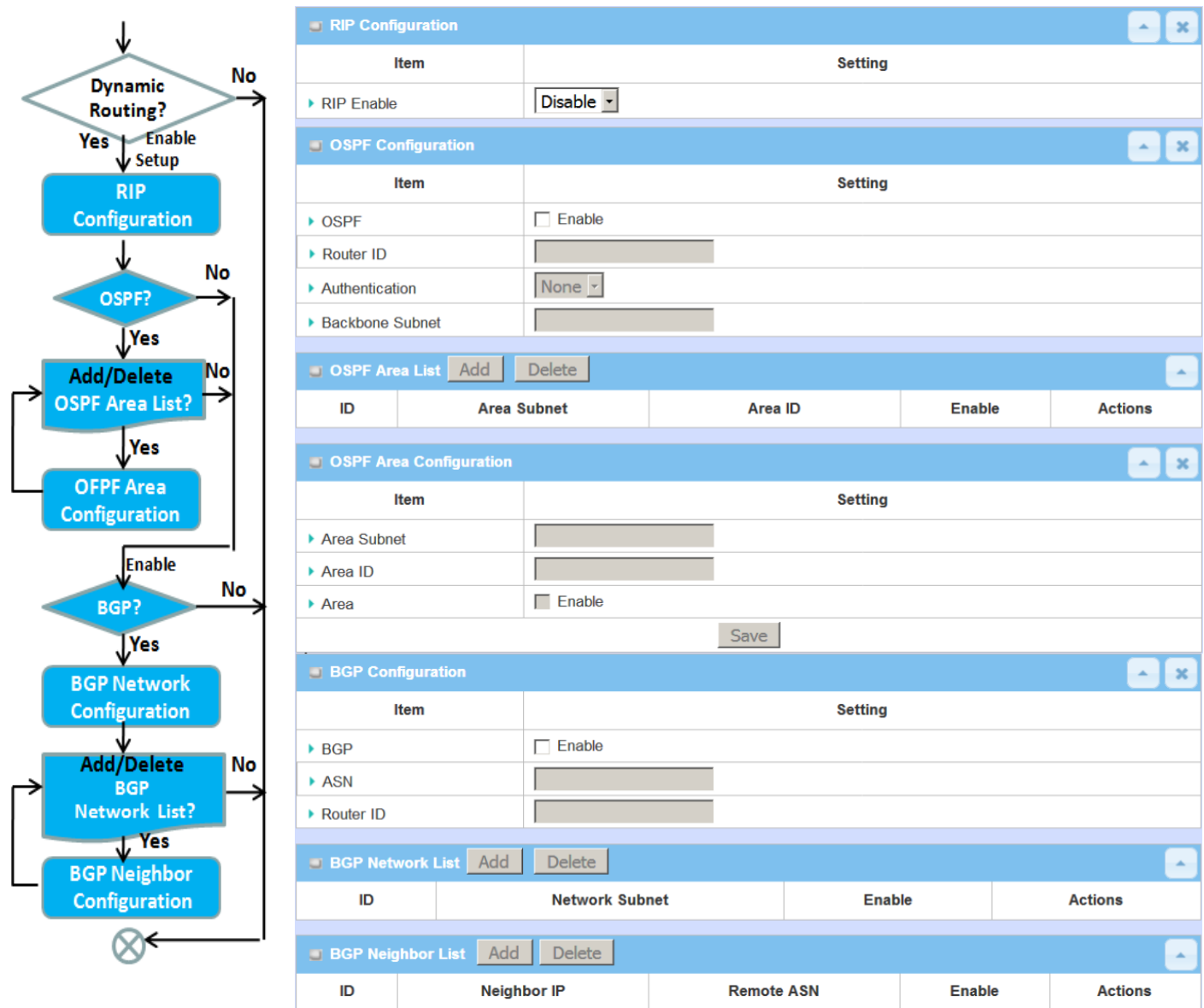
# EW200 Industrial Cellular Gateway

IPv4 Static Routing Rule Configuration	
Item	Setting
▶ Destination IP	<input type="text"/>
▶ Subnet Mask	255.255.255.0 (/24) ▼
▶ Gateway IP	<input type="text"/>
▶ Interface	Auto ▼
▶ Metric	<input type="text"/>
▶ Rule	<input type="checkbox"/> Enable

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

# EW200 Industrial Cellular Gateway

## 2.6.2 Dynamic Routing



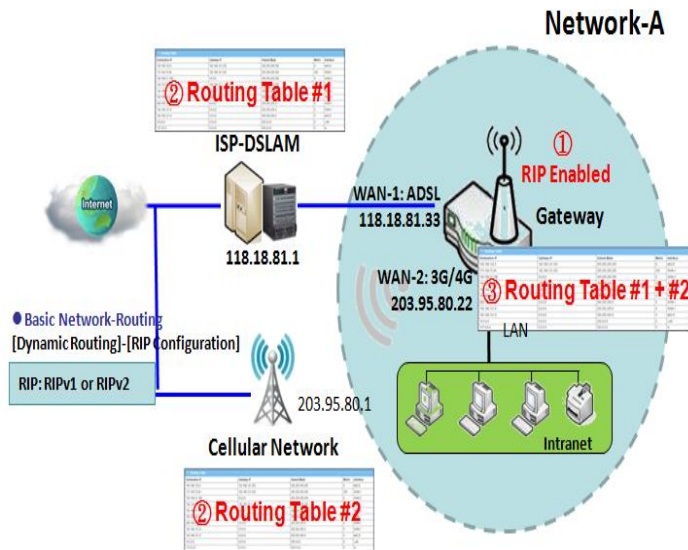
Dynamic Routing, also called adaptive routing, describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in network conditions.

This gateway supports dynamic routing protocols, including RIPv1/RIPv2 (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol), to establish the routing table automatically. Dynamic routing can be very useful when there are many subnets in your network. Generally speaking, RIP is suitable for small networks. OSPF is more suitable for medium networks. BGP is more used for large network infrastructure.

The supported dynamic routing protocols are described as follows.

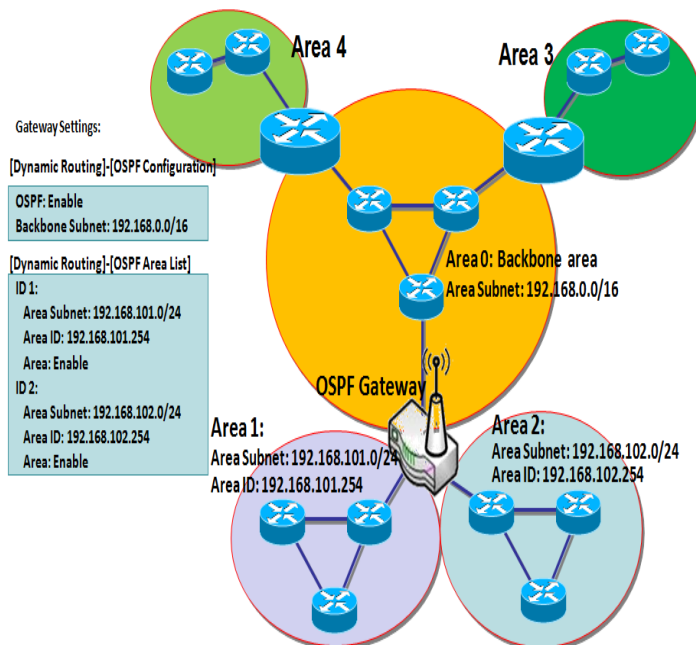
# EW200 Industrial Cellular Gateway

## RIP Scenario



The Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols. It 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



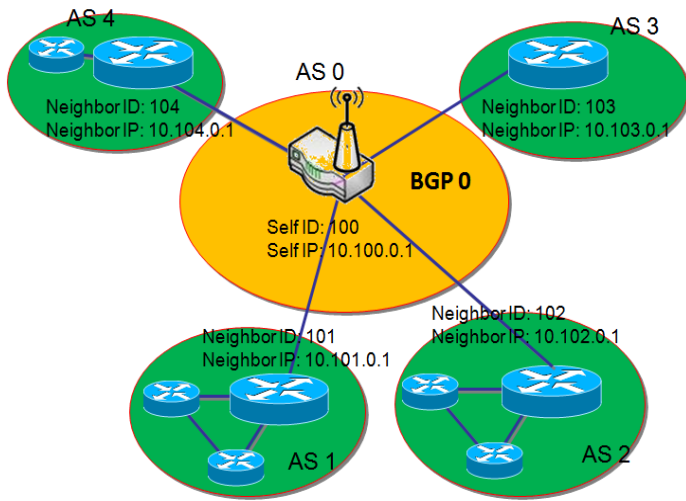
Open Shortest Path First (OSPF) is a routing protocol that uses link state routing algorithm. It is the most widely used interior gateway protocol (IGP) in large enterprise networks. It gathers link state information from available routers and constructs a topology map of the network. The topology is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

The network administrator can deploy an OSPF gateway in large enterprise network to get its routing table from the enterprise backbone, and forward routing information to other routers, which are not 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, the 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.

# EW200 Industrial 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 multihomed networks). Very large private IP networks also use BGP internally. The major BGP gateway within one AS will link with 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 a subnet in one ISP being linked with ones in other ISPs. By operating with BGP protocol, BGP 0 can gather routing information from other BGP gateways in the Internet. It then 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.



# EW200 Industrial Cellular Gateway

## Dynamic Routing Setting

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

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

In the "Dynamic Routing" page, there are seven configuration windows for dynamic routing feature. They are "RIP Configuration", "OSPF Configuration", "OSPF Area List", "OSPF Area Configuration", "BGP Configuration", "BGP Neighbor List" and "BGP Neighbor Configuration". 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 to disable it. The "OSPF Configuration" window lets 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. The "BGP Configuration" window will 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.

### RIP Configuration

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

RIP Configuration		
Item	Value setting	Description
RIP Enable	Disable is set by default	Select <b>Disable</b> to disable RIP protocol. Select <b>RIP v1</b> to enable RIPv1 protocol. Select <b>RIP v2</b> to enable RIPv2 protocol.

# EW200 Industrial Cellular Gateway

## OSPF Configuration

OSPF Configuration	
Item	Setting
▶ OSPF	<input type="checkbox"/> Enable
▶ Router ID	<input type="text"/>
▶ Authentication	<input type="text" value="None"/>
▶ Backbone Subnet	<input type="text"/>

OSPF Configuration		
Item	Value setting	Description
OSPF	Disable is set by default	Click <b>Enable</b> box to activate the OSPF protocol.
Router ID	1. IPv4 Format 2. Required setting	The Router ID of this router in OSPF protocol
Authentication	None is set by default	The Authentication method of this router in OSPF protocol. Select <b>None</b> to disable Authentication in OSPF protocol. Select <b>Text</b> to enable Text Authentication with entered the Key in this field in OSPF protocol. Select <b>MD5</b> to 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. Required setting	The Backbone Subnet of this router on OSPF protocol.

## Create / Edit OSPF Area Rules

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

OSPF Area List <input type="button" value="Add"/> <input type="button" value="Delete"/>				
ID	Area Subnet	Area ID	Enable	Actions

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

# EW200 Industrial Cellular Gateway

OSPF Area Configuration	
Item	Setting
▶ Area Subnet	<input type="text"/>
▶ Area ID	<input type="text"/>
▶ Area	<input type="checkbox"/> Enable
<input type="button" value="Save"/>	

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

# EW200 Industrial Cellular Gateway

## BGP Configuration

BGP Configuration	
Item	Setting
▶ BGP	<input type="checkbox"/> Enable
▶ ASN	<input type="text"/>
▶ Router ID	<input type="text"/>

BGP Network Configuration		
Item	Value setting	Description
BGP	Unchecked by default	Check the <b>Enable</b> box to activate the BGP protocol.
ASN	1. Numeric String Format 2. Required setting	The ASN Number of this router on BGP protocol. <b><u>Value Range:</u></b> 1 ~ 4294967295.
Router ID	1. IPv4 Format 2. Required setting	The Router ID of this router on BGP protocol.

## Create / Edit BGP Network Rules

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

BGP Network List <input type="button" value="Add"/> <input type="button" value="Delete"/>			
ID	Network Subnet	Enable	Actions

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

BGP Network Configuration	
Item	Setting
▶ Network Subnet	IP : <input type="text"/> <input type="text" value="255.255.255.0 (/24)"/> ▼
▶ Network	<input type="checkbox"/> Enable
<input type="button" value="Save"/>	

Item	Value setting	Description
Network Subnet	1. IPv4 Format 2. Required setting	The Network Subnet of this router in BGP Network List. Enter the IP address in this field and the selected subnet mask.
Network	Unchecked by default	Click <b>Enable</b> box to activate this rule.
Save	N/A	Click the <b>Save</b> button to save the configuration

# EW200 Industrial Cellular Gateway

## Create / Edit BGP Neighbor Rules

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

BGP Neighbor List <input type="button" value="Add"/> <input type="button" value="Delete"/>				
ID	Neighbor IP	Remote ASN	Enable	Actions

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

BGP Neighbor Configuration	
Item	Setting
▶ Neighbor IP	<input type="text"/>
▶ Remote ASN	<input type="text"/>
▶ Neighbor	<input type="checkbox"/> Enable
<input type="button" value="Save"/>	

BGP Neighbor Configuration		
Item	Value setting	Description
Neighbor IP	1. IPv4 Format 2. Required setting	The Neighbor IP of this router on BGP Neighbor List.
Remote ASN	1. Numeric String Format 2. Required setting	The Remote ASN of this router on BGP Neighbor List. <b><u>Value Range:</u></b> 1 ~ 4294967295.
Neighbor	Unchecked by default	Click <b>Enable</b> box to activate this rule.
Save	N/A	Click the <b>Save</b> button to save the configuration

# EW200 Industrial 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.

Routing Table				
Destination IP	Subnet Mask	Gateway IP	Metric	Interface
100.105.167.72	255.255.255.252	0.0.0.0	0	WAN-2
192.168.66.0	255.255.255.0	0.0.0.0	0	LAN
192.168.127.0	255.255.255.0	0.0.0.0	0	WAN-1
169.254.0.0	255.255.0.0	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 Information				
Policy Routing Source	Source IP	Destination IP	Destination Port	WAN Interface
Load Balance	-	-	-	-

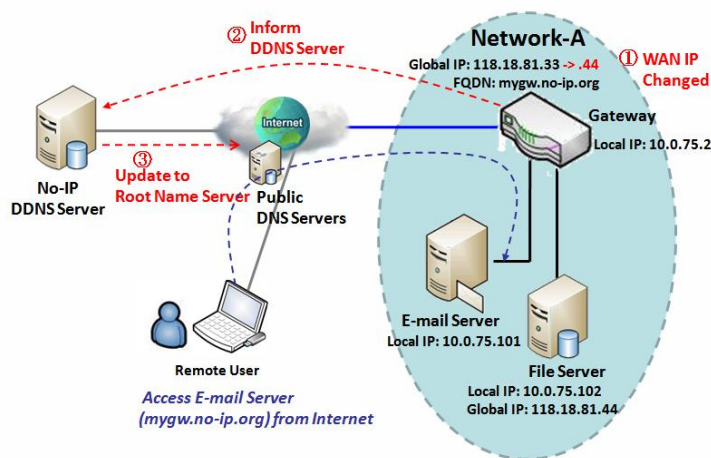
Policy Routing Information Item	Value setting	Description
Policy Routing Source	N/A	Policy Routing of Source. String Format.
Source IP	N/A	Policy Routing of Source IP. IPv4 Format.
Destination IP	N/A	Policy Routing of Destination IP. IPv4 Format.
Destination Port	N/A	Policy Routing of Destination Port.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

## 2.7 DNS & DDNS

How does a 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.

### 2.7.1 DNS & DDNS Configuration

#### 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, the 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 on the Internet are able to link to your gateway by using your domain name regardless of the changing global IP address.

# EW200 Industrial Cellular Gateway

## DNS & DDNS Setting

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

The DNS & DDNS setting allows user to set up dynamic DNS feature and DNS redirect rules.

### Set up Dynamic DNS

The gateway allows you to customize your dynamic DNS settings.

Item	Setting
▶ DDNS	<input type="checkbox"/> 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
<b>DDNS</b>	Unchecked by default	Check the Enable box to activate this function.
<b>WAN Interface</b>	WAN 1 is set by default	Select the WAN Interface IP Address of the gateway.
<b>Provider</b>	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...
<b>Host Name</b>	1. String format <b>2. Required setting</b>	Your registered host name of Dynamic DNS. Value Range: 0 ~ 63 characters.
<b>User Name / E-Mail</b>	1. String format <b>2. Required setting</b>	Enter your User name or E-mail addresss of Dynamic DNS.
<b>Password / Key</b>	1. String format 2. Required setting	Enter your Password or Key of Dynamic DNS.
<b>Save</b>	N/A	Click Save to save the settings
<b>Undo</b>	N/A	Click Undo to cancel the settings

### Set Up DNS Redirect

DNS redirect is a special function to redirect certain traffic to a specified host. Administator can manage the internet / intranet traffics that are going to access some restricted DNS and force those traffics to be redirected to a specified host.



# EW200 Industrial Cellular Gateway

DNS Redirect	
Item	Setting
▶ DNS Redirect	<input type="checkbox"/> Enable

DNS Redirect Configuration		
Item	Value setting	Description
<b>DNS Redirect</b>	Unchecked by default	Click the Enable box to activate this function.
<b>Save</b>	N/A	Click Save to save the settings
<b>Undo</b>	N/a	Click Undo to cancel the settings

If you **enable** the DNS Redirect function, you have to further specify the redirect rules. According to the rules, the gateway can redirect the traffic that matches the DNS to a corresponding pre-defined IP address.

Redirect Rule					
ID	Mapping Rule	Condition	Description	Enable	Action
<div> <div>Add</div> <div>Delete</div> </div>					

When the **Add** button is applied, the **Redirect Rule** screen will appear.

Redirect Rule					
Item	Setting				
Mapping Rule	<table border="1"> <thead> <tr> <th>Domain Name</th> <th>IP</th> </tr> </thead> <tbody> <tr> <td><input type="text"/> (* for Any)</td> <td><input type="text"/></td> </tr> </tbody> </table>	Domain Name	IP	<input type="text"/> (* for Any)	<input type="text"/>
Domain Name	IP				
<input type="text"/> (* for Any)	<input type="text"/>				
Condition	<div>Always</div>				
Description	<input type="text"/>				
Enable	<input type="checkbox"/> Enable				

Redirect Rule Configuration		
Item	Value setting	Description
<b>Domain Name</b>	1. String format, any text 2. <b>Required setting</b>	Enter a domain name to be redirect. The traffic to specified domain name will be redirect to the following IP address.
<b>IP</b>	1. IPv4 format 2. <b>Required setting</b>	Enter an IP Address as the target for the DNS redirect.
<b>Condition</b>	1. Required setting 2. <b>Always is selected by default</b>	Specify when will the DNS redirect action can be applied. It can be <b>Always</b> , or <b>WAN Block</b> . <b>Always</b> : The DNS redirect function can be applied to matched DNS all the time. <b>WAN Block</b> : The DNS redirect function can be applied to matched DNS only

## EW200 Industrial Cellular Gateway

---

		when the WAN connection is disconnected, or un-reachable.
<b>Description</b>	1. String format <b>2. Required setting</b>	Enter a brief description for this rule. Value Range: 0 ~ 63 characters.
<b>Enable</b>	Unchecked by default	Click the Enable button to activate this rule.
<b>Save</b>	N/A	Click <b>Save</b> to save the settings
<b>Undo</b>	N/A	Click <b>Undo</b> to cancel the settings

# EW200 Industrial Cellular Gateway

---

## 2.8 QoS

The total amount of data traffic is steadily increasing due to the higher demands of mobile applications such as games / chat / VoIP / P2P / video / web access.

The main goal of QoS (Quality of Service) is prioritizing incoming data, and preventing data loss due to factors such as jitter, delay and dropping. Another important aspect of QoS is ensuring that prioritizing one data flow doesn't interfere with other data flows. So, QoS helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based on priority. This is useful when there are certain types of data you want to give higher priority to, such as voice packets given higher priority than Web data packets.

To utilize your network throughput completely, the administrator must define bandwidth control rules carefully to balance the utilization of network bandwidth for all users to access. It is required that an access gateway satisfies the requirements of latency-critical applications, minimum access right guarantee, fair bandwidth usage for same subscribed condition and flexible bandwidth management.

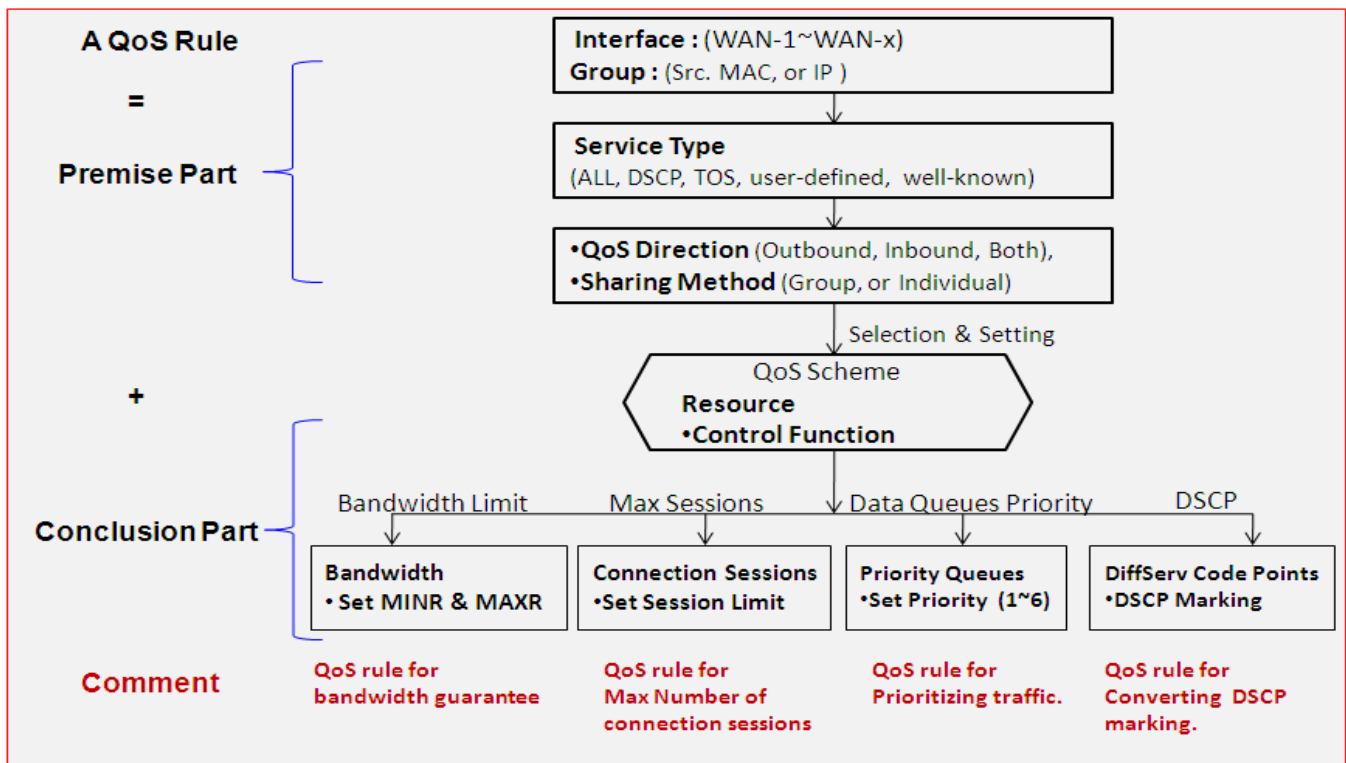
### 2.8.1 QoS Configuration

This gateway provides many flexible rules for you to set QoS policies. Basically, you need to know three pieces of information before you create your own policies. First, "who" needs to be managed? Second, "what" kind of service needs to be managed? The last part is "how" you prioritize. Once you have this information, you can continue to learn functions in this section in more detail.

#### [QoS Rule Configuration](#)

When you want to add a new QoS rule or edit an existing one, the "QoS Rule Configuration" window is used. The parameters in a rule include the applied WAN interfaces, the dedicated host group based on MAC address or IP address, the dedicated kind of service packets, the system resource to be distributed, the corresponding control function for your specified resource, the packet flow direction, the sharing method for the control function, the integrated time schedule rule and the rule activation. The following diagram illustrates how to organize a QoS rule.

# EW200 Industrial Cellular Gateway



In the above diagram, a QoS rule is organized by the premise part and the conclusion part. In the premise part, you must specify the WAN interface, host group, service type in the packets, packet flow direction to be watched and the sharing method of group control or individual control. In the conclusion part, you must make sure which kind of system resource to distribute and the control function based on the chosen system resource for the rule.

Rule-based QoS has the following features.

## Multiple Group Categories

Specify the group category in a QoS rule for the target objects to be applied on.

Group Category can be based on VLAN ID, MAC Address, IP Address, Host Name or Packet Length.

## Differentiated Services

Specify the service type in a QoS rule for the target packets to be applied on.

Differentiated services can be based on 802.1p, DSCP, TOS, VLAN ID, User-defined Services and Well-known Services. Well-known services include FTP(21), SSH(TCP:22), Telnet(23), SMTP(25), DNS(53), TFTP(UDP:69), HTTP(TCP:80), POP3(110), Auth(113), SFTP(TCP:115), SNMP&Traps(UDP:161-162), LDAP(TCP:389), HTTPS(TCP:443), SMTPs(TCP:465), ISAKMP(500), RTSP(TCP:554), POP3s(TCP:995), NetMeeting(1720), L2TP(UDP:1701) and PPTP(TCP:1723).

## Available Control Functions

There are 4 resources that can be applied in a QoS rule: bandwidth, connection sessions, priority queues and DiffServ Code Point (DSCP). Control function that acts on target objects for specific services of packet flow is based on these resources.

For bandwidth resources, control functions include guaranteeing bandwidth and limiting bandwidth. For priority

# EW200 Industrial Cellular Gateway

queue resources, control function is setting priority. For DSCP resource, control function is DSCP marking. The last resource is Connection Sessions; the related control function is limiting connection sessions.

## Individual / Group Control

One QoS rule can be applied to individual member or whole group in the target group. This feature depends on the model.

## Outbound / Inbound Control

One QoS rule can be applied to the outbound or inbound direction of packet flow, even them both. This feature depends on the model.

Two QoS rule examples are shown below.

## QoS Rule Example #1 - Connection Sessions

QoS Rule Configuration	
Item	Setting
▶ Interface	WAN - 1
▶ Group	IP 10.0.75.16 Subnet Mask : 255.255.255.240 (/28)
▶ Service	All
▶ Queue Outbound	N/A
▶ Queue Inbound	N/A
▶ Time Schedule	(0) Always
▶ Rule Enable	<input checked="" type="checkbox"/> Enable

When the administrator wants to limit maximum connection sessions from some client hosts (IP 10.0.75.16~31) to 20000 to avoid resources from becoming unbalanced, he/she can set up this rule as per the above configuration.

This rule defines that all client hosts whose IP address is in the range of 10.0.75.16~31, can access the Internet via "WAN-1" interface under the limitation of the maximum 20000 total connection sessions at any time.

# EW200 Industrial Cellular Gateway

## QoS Rule Example #2 – DifferServ Code Points

QoS Rule Configuration	
Item	Setting
▶ Interface	All WANs ▾
▶ Group	IP ▾ 10.0.75.196 Subnet Mask : 255.255.255.252 (/30) ▾
▶ Service	DSCP ▾ ▶ DiffServ CodePoint IP Precedence 4(CS4) ▾
▶ Queue Outbound	N/A
▶ Queue Inbound	N/A
▶ Time Schedule	(0) Always ▾
▶ Rule Enable	<input checked="" type="checkbox"/> Enable

When the administrator of the gateway wants to convert the code point value, "IP Precedence 4(CS4)", in the packets from some client hosts (IP 10.0.75.196~199) to the code value, "AF Class2(High Drop)", he/she can use the "Rule-based QoS" function to carry out this rule by defining an QoS rule as shown in the above configuration. Under such a configuration, all packets from WAN interfaces to LAN IP address 10.0.75.196 ~ 10.0.75.199 which have DiffServ code points with "IP Precedence 4(CS4)" value will be modified by "DSCP Marking" control function with "AF Class 2(High Drop)" value at any time.

# EW200 Industrial Cellular Gateway

## QoS Configuration Setting

Go to **Basic Network > QoS > Configuration** tab.

In "QoS Configuration" page, there are several configuration windows for QoS. They are "Configuration", "System Resource Configuration", "QoS Rule List", and "QoS Rule Configuration".

The "Configuration" window will let you activate the Rule-based QoS function. In addition, you can also enable the "Flexible Bandwidth Management" (FBM) feature for better utilization of system bandwidth by the FBM algorithm. Second, the "System Configuration" window will let you configure the total bandwidth and session of each WAN. Third, the "QoS Rule List" window lists all your defined QoS rules. At last, the "QoS Rule Configuration" window lets you define one QoS rule.

### Enable QoS Function

Configuration	
Item	Setting
▶ QoS Types	Software ▾ <input type="checkbox"/> Enable
▶ Flexible Bandwidth Management	<input type="checkbox"/> Enable

Configuration Item	Value Setting	Description
QoS Type	1. <b>Software</b> is selected by default. 2. Unchecked by default	Select the QoS Type from the dropdown list, and then click <b>Enable</b> box to activate the QoS function. The default QoS type is set to <b>Software</b> QoS. For some models, there is another option for <b>Hardware</b> QoS.
Flexible Bandwidth Management	Unchecked by default	Click <b>Enable</b> box to activate the Flexible Bandwidth Management function.
Save	N/A	Click the <b>Save</b> button to save the settings.

Check the "Enable" box to activate "Rule-based QoS". Also enable the Flexible Bandwidth Management (FBM) feature when needed. When FBM is enabled, the system adjusts the bandwidth distribution dynamically based on current bandwidth usage situation to reach maximum system network performance while transparent to all users. The bandwidth subscription profiles of all current users are considered in system's automatic adjusting algorithm.

# EW200 Industrial Cellular Gateway

## Set Up System Resource

System Resource Configuration		
Item	Setting	
▶ Type of System Queue	Bandwidth Queue ▼	6 (1~6)
▶ WAN Interface	WAN - 1 ▼	

WAN Interface Resource		
Item	Setting	
▶ Bandwidth of Upstream	100	Mbps ▼
▶ Bandwidth of Downstream	100	Mbps ▼
▶ Total Connection Sessions	30000	(1~100000)

System Resource Configuration		
Item	Value Setting	Description
Type of System Queue	1. Required setting. 2. <b>Bandwidth Queue</b> , and 6 are set by default.	Define the system queues that are available for the QoS settings. The supported type of system queues are <b>Bandwidth Queue</b> and <b>Priority Queues</b> . <b>Value Range:</b> 1 ~ 6.
WAN Interface	<b>WAN-1</b> is selected by default.	Select the WAN interface and then the following <b>WAN Interface Resource</b> screen will show the related resources for configuration. <ul style="list-style-type: none"> <li>● <b>Bandwidth of Upstream / Downstream</b> Specify total upload / download bandwidth of the selected WAN. Value Range: For Gigabit Ethernet: 1~1024000Kbps, or 1~1000Mbps; For Fast Ethernet: 1~102400Kbps, or 1~100Mbps; <b>For 3G/4G: 1~153600Kbps, or 1~150Mbps.</b></li> <li>● <b>Total Connection Sessions</b> Specify total connection sessions of the selected WAN. <b>Value Range:</b> 1 ~ 10000.</li> </ul>
Save	N/A	Click the <b>Save</b> button to save the settings.

Each WAN interface should be configured carefully for its upstream bandwidth, downstream bandwidth and maximum number of connection sessions.



# EW200 Industrial Cellular Gateway

## Create / Edit QoS Rules

After enabling QoS and configuring the system resources, you have to further specify some QoS rules to provide better service on the relevant traffic. The gateway supports up to a maximum of 128 rule-based QoS rule sets.

QoS Rule List <span>Add</span> <span>Delete</span> <span>Clear</span> <span>Restart</span>									
Interface	Group	Service	Resource	Control Function	Direction	Sharing Method	Time Schedule	Enable	Actions

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

QoS Rule Configuration	
Item	Setting
▶ Interface	All WANs ▼
▶ Group	Src. MAC Address ▼ <input type="text"/>
▶ Service	All ▼
▶ Resource	Bandwidth ▼
▶ Control Function	Set MINR & MAXR ▼ <input type="text"/> --- <input type="text"/> Mbps ▼
▶ QoS Direction	Outbound ▼
▶ Time Schedule	(0) Always ▼
▶ Rule Enable	<input type="checkbox"/> Enable

QoS Rule Configuration		
Item	Value setting	Description
Interface	1. Required setting. 2. <b>All WANs</b> are selected by default.	Specify the WAN interface to apply the QoS rule. Select <b>All WANs</b> or a certain <b>WAN-n</b> to filter the packets entering or leaving the interface(s).
Group	1. Required setting. 2. <b>Src. MAC Address</b> is selected by default.	<p>Specify the <b>Group</b> category for the QoS rule. It can be <b>Src. MAC Address</b>, <b>IP</b>, or <b>Host Name</b>.</p> <p>Select <b>Src. MAC Address</b> to prioritize packets based on MAC;</p> <p>Select <b>IP</b> to prioritize packets based on IP address and Subnet Mask;</p> <p>Select <b>Host Name</b> to prioritize packets based on a group of a pre-configured group of host from the dropdown list. If the dropdown list is empty, ensure that groups have been pre-configured.</p> <p><b>Note:</b> The required host groups must be created in advance and the corresponding QoS checkbox in the <b>Multiple Bound Services</b> field checked before the <b>Host Group</b> option becomes available. Refer to <b>Object Definition &gt; Grouping &gt; Host Grouping</b>.</p>

# EW200 Industrial Cellular Gateway

<b>Service</b>	<p>1. Required setting. 2. <b>All</b> is selected by default.</p>	<p>Specify the service type of traffic to have the QoS rule applied. It can be <b>All</b>, <b>DSCP</b>, <b>TOS</b>, <b>User-defined Service</b>, or <b>Well-known Service</b>.</p> <p>Select <b>All</b> for all packets.</p> <p>Select <b>DSCP</b> for DSCP type packets only.</p> <p>Select <b>TOS</b> for TOS type packets only. Select a service type (<b>Minimize-Cost</b>, <b>Maximize-Reliability</b>, <b>Maximize-Throughput</b>, or <b>Minimize-Delay</b>) from the dropdown list as well.</p> <p>Select <b>User-defined Service</b> for user-defined packets only. Define the port range and protocol as well.</p> <p>Select <b>Well-known Service</b> for specific application packets only. Select the required service from the dropdown list as well.</p>
<b>Resource, and Control Function</b>	Required setting	<p>Specify the Resource Type and corresponding Control function for the QoS rule. The available Resource options are <b>Bandwidth</b>, <b>Connection Sessions</b>, <b>Priority Queues</b>, and <b>DiffServ Codepoints</b>.</p> <p><b>Bandwidth:</b> Select <b>Bandwidth</b> as the resource type for the QoS Rule, and assign the min rate, max rate and rate unit as the bandwidth settings in the <b>Control Function / Set MINR &amp; MAXR</b> field.</p> <p><b>Connection Sessions:</b> Select <b>Connection Sessions</b> as the resource type for the QoS Rule, and assign supported session number in the <b>Control Function / Set Session Limitation</b> field.</p> <p><b>Priority Queues:</b> Select <b>Priority Queues</b> as the resource type for the QoS Rule, and specify a priority queue in the <b>Control Function / Set Priority</b> field.</p> <p><b>DiffServ Code Points:</b> Select <b>DiffServ Code Points</b> as the resource type for the QoS Rule, and select a DSCP marking from the <b>Control Function / DSCP Marking</b> dropdown list.</p>
<b>QoS Direction</b>	<p>1. Required setting. 2. <b>Outbound</b> is selected by default.</p>	<p>Specify the traffic flow direction for the packets to apply the QoS rule. It can be <b>Outbound</b>, <b>Inbound</b>, or <b>Both</b>.</p> <p><b>Outbound:</b> Select <b>Outbound</b> to prioritize the traffic going to the Internet via the specified interface. Under such situations, the hosts specified in the Group field are a source group.</p> <p><b>Inbound:</b> Select <b>Inbound</b> to prioritize the traffic coming from the Internet via the specified interface. Under such situations, the hosts specified in the Group field are a destination group.</p> <p><b>Both:</b> Select <b>both</b> to prioritize the traffic passing through the specified interface, both Inbound and Outbound are considered. Under such situation, the hosts specified in the Group field can be a source or destination group.</p>
<b>Sharing Method</b>	<p>1. Required setting. 2. <b>Group Control</b> is selected by default.</p>	<p>Specify the preferred sharing method for how to apply the QoS rule on the selected group. It can be <b>Individual Control</b> or <b>Group Control</b>.</p> <p><b>Individual Control:</b> If <b>Individual Control</b> is selected, each host in the group will have his own QoS service resource as specified in the rule.</p> <p><b>Group Control:</b> If <b>Group Control</b> is selected, all the group hosts share the same</p>

## EW200 Industrial Cellular Gateway

---

		QoS service resource.
<b>Time Schedule</b>	1. Required setting. 2. <b>(0) Always</b> is selected by default.	Apply <b>Time Schedule</b> to this rule; otherwise leave it as (0) <b>Always</b> . (refer to <b>Object Definition &gt; Scheduling &gt; Configuration</b> settings)
<b>Rule Enable</b>	Unchecked by default	Click <b>Enable</b> box to activate this QoS rule.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the settings.

## 2.9 Redundancy

In engineering, redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system, usually in the form of a backup or fail-safe. In an IP network, the access gateway is the critical part of the networking system. A redundant gateway is the backup to the master gateway and it will take over the data transmitting job if the master gateway fails.

The gateway can serve as the redundant gateway of core router in the enterprise by using the Virtual Router Redundancy Protocol (VRRP).

### 2.9.1 VRRP

Configuration	
Item	Setting
▶ VRRP	<input type="checkbox"/> Enable
▶ Virtual Server ID	<input type="text"/> (1-255)
▶ Priority of Virtual Server	<input type="text"/> (Lowest 1 ~ 254 Highest)
▶ Virtual Server IP Address	<input type="text"/>

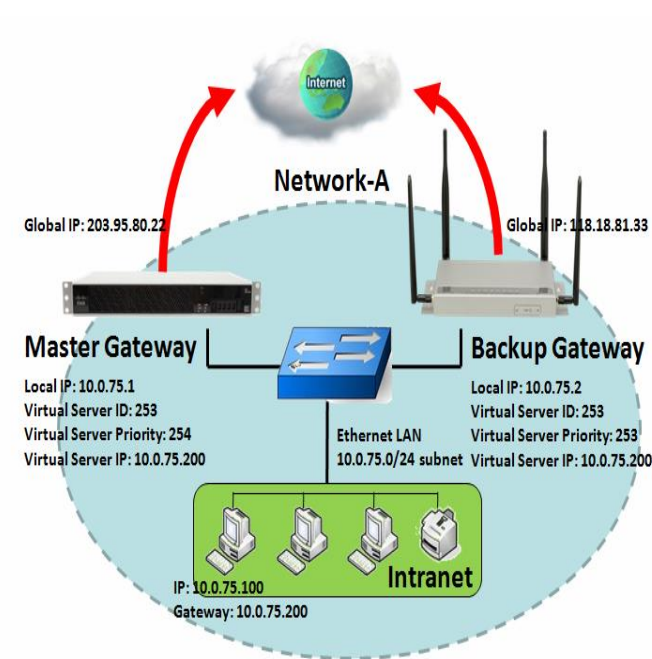
Virtual Router Redundancy Protocol (VRRP) is a networking protocol providing device redundancy. It allows a backup router or switch to automatically take over if the primary (master) router or switch fails. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP network.

The protocol achieves this by creation of virtual routers, which are an abstract representation of multiple routers, i.e. master and backup routers, acting as a group. The default gateway of a participating host is assigned to the virtual router instead of a physical router. If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected to automatically replace it. The physical router that is forwarding packets at any given time is called the master router.

A group of physical VRRP gateways combined together to play a virtual server with one unique virtual server ID and one unique virtual server IP address. These VRRP gateways have their own priority values to serve as the sequence for backing up the master gateway.

The gateway with VRRP function can join one group of redundant gateways to serve as the backup one for the master gateway. Enter the same values of virtual server ID and IP for these gateways, and each gateway will own its own priority as the sequence in the backup list. They construct a VRRP redundant gateway group. Following diagram illustrates the group example with two member gateways.

# EW200 Industrial Cellular Gateway



As shown in the diagram, a Master Gateway and Backup Gateway are a redundant gateway group of Network-A. Subnet of network-A is 10.0.75.0/24. Master gateway has a LAN IP of 10.0.75.1 and WAN IP of 203.95.80.22. Backup gateway has LAN IP 10.0.75.2 and 118.18.81.33 for WAN-1. They both serve as NAT routers.

Specify the ID of VRRP virtual server to be "253" and its IP address to be "10.0.75.200". The priority of the master gateway is 254 and it is larger than the one (253) of the backup gateway. At first stage, all data from the Intranet go through the master gateway that has the highest priority. Once the master Internet connection is broken, the backup gateway will take over the data transmitting job and serve as the master gateway.

When a gateway with higher priority recovers from broken connection, it will take over data transmitting again.

## VRRP Setting

Go to **Basic Network > Redundancy > VRRP** tab.

Configuration	
Item	Setting
▶ VRRP	<input type="checkbox"/> Enable
▶ Virtual Server ID	<input type="text"/> (1-255)
▶ Priority of Virtual Server	<input type="text"/> (Lowest 1 ~ 254 Highest)
▶ Virtual Server IP Address	<input type="text"/>

VRRP Item	Value setting	Description
VRRP	Unchecked by default	Check the <b>Enable</b> box to activate this VRRP function.
Virtual Server ID	1. Numeric String Format 2. Required setting	Specify the Virtual Server ID on VRRP of the gateway. Value Range: 1 ~ 255.
Priority of	1. Numeric String Format	Specify the Priority of Virtual Server on VRRP of the gateway.

## EW200 Industrial Cellular Gateway

---

<b>Virtual Server</b>	2. Required setting	<b><u>Value Range:</u></b> 1 ~ 254, and 254 is the highest priority.
<b>Virtual Server IP Address</b>	1. IPv4 Format 2. Required setting	Specify the Virtual Server IP Address on VRRP of the gateway.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the configuration.
<b>Undo</b>	N/A	Click the <b>Undo</b> button to restore what you just configured back to the previous setting.

## Chapter 3 Object Definition

### 3.1 Scheduling

Scheduling provides the ability to add/delete time schedule rules, which can be applied to other functions.

#### 3.1.1 Scheduling Configuration

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

Time Schedule List <span>Add</span> <span>Delete</span>		
ID	Rule Name	Actions

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

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

Time Schedule Configuration	
Item	Setting
▶ Rule Name	<input type="text"/>
▶ Rule Policy	<span>Inactivate ▼</span> the Selected Days and Hours Below.

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

## EW200 Industrial Cellular Gateway

Time Period Definition			
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
2	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
3	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
4	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
5	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
6	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
7	-- choose one -- ▼	<input type="text"/>	<input type="text"/>
8	-- choose one -- ▼	<input type="text"/>	<input type="text"/>

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



# EW200 Industrial Cellular Gateway

## 3.2 Grouping

The Grouping function allows the user to create groups for services.

### 3.2.1 Host Grouping

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

The Host Grouping function allows the user to make host groups for services, such as QoS, Firewall, and Communication Bus. The supported service types may differ by product type.

Host Group List <span>Add</span> <span>Delete</span>						
ID	Group Name	Group Type	Member List	Bound Services	Enable	Actions

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

Host Group Configuration	
Item	Setting
▶ Group Name	<input type="text"/>
▶ Group Type	<input type="text" value="IP Address-based"/>
▶ Member to Join	<input type="text"/> <span>Join</span>
▶ Member List	
▶ Bound Services	<input type="checkbox"/> Firewall <input type="checkbox"/> QoS <input type="checkbox"/> Field Communication
▶ Group	<input type="checkbox"/> Enable

Host Group Configuration		
Item	Value setting	Description
Group Name	1. String format, any text 2. Required setting	Enter a group name for the rule.
Group Type	1. <b>IP Address-based</b> is selected by default. 2. Required setting	Select the group type for the host group. It can be <b>IP Address-based</b> , <b>MAC Address-based</b> , or <b>Host Name-based</b> . When <b>IP Address-based</b> is selected, only IP addresses can be added in <b>Member to Join</b> .

## EW200 Industrial Cellular Gateway

		<p>When <b>MAC Address-based</b> is selected, only MAC addresses can be added in <b>Member to Join</b>.</p> <p>When <b>Host Name-based</b> is selected, only host names can be added in <b>Member to Join</b>.</p> <p>Note: The available Group Types will differ depending on the device model.</p>
<b>Member to Join</b>	N/A	<p>Add the members to the group in this field.</p> <p>You can enter the member information as specified in the Member Type above, and press the <b>Join</b> button to add.</p> <p>Only one member can be added at a time.</p>
<b>Member List</b>	NA	This field will indicate the hosts (members) contained in the group.
<b>Bound Services</b>	The boxes are unchecked by default	Binding services applied to the host group. If you enable the <b>Firewall</b> , the produced group can be used in firewall service. <b>Note:</b> The supported service type may differ depending on product model.
<b>Group</b>	Unchecked by default	Check the <b>Enable</b> checkbox to activate the host group rule. The group will be bound to the selected service(s) for further configuration.
<b>Save</b>	N/A	Click <b>Save</b> to save the settings
<b>Undo</b>	N/A	Click <b>Undo</b> to cancel the settings

# EW200 Industrial Cellular Gateway

## 3.3 External Server


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

The External Server setting allows user to add an external server.

### Create External Server

 External Server List <input type="button" value="Add"/> <input type="button" value="Delete"/>						
ID	Server Name	Server Type	Server IP/FQDN	Server Port	Server Enable	Actions

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

 External Server Configuration	
Item	Setting
▶ Server Name	<input type="text"/>
▶ Server Type	<div>Email Server ▼ User Name: <input type="text"/> Password: <input type="text"/></div>
▶ Server IP/FQDN	<input type="text"/>
▶ Server Port	<input type="text" value="25"/>
▶ Server	<input checked="" type="checkbox"/> Enable
<div><input type="button" value="Save"/> <input type="button" value="Undo"/></div>	

# EW200 Industrial Cellular Gateway

External Server Configuration		
Item	Value setting	Description
<b>Server Name</b>	1. String format, any text 2. Required setting	Enter a server name.
		Specify the Server Type of the external server, and enter the required settings for the accessing the server.
		<b>Email Server</b> (Required setting): When <b>Email Server</b> is selected, <b>User Name</b> , and <b>Password</b> are also required. <b>User Name</b> (String format: any text) <b>Password</b> (String format: any text)
		<b>RADIUS Server</b> (Required setting): When <b>RADIUS Server</b> is selected, the following settings are also required. Primary: <b>Shared Key</b> (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 15. Secondary: <b>Shared Key</b> (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 15.
		<b>Active Directory Server</b> (Required setting): When <b>Active Directory Server</b> is selected, <b>Domain</b> setting is also required. <b>Domain</b> (String format: any text)
		<b>LDAP Server</b> (Required setting): When <b>LDAP Server</b> is selected, the following settings are also required. <b>Base DN</b> (String format: any text) <b>Identity</b> (String format: any text) <b>Password</b> (String format: any text)
		<b>UAM Server</b> (Required setting): When <b>UAM Server</b> is selected, the following settings are also required. <b>Login URL</b> (String format: any text) <b>Shared Secret</b> (String format: any text) <b>NAS/Gateway ID</b> (String format: any text) <b>Location ID</b> (String format: any text) <b>Location Name</b> (String format: any text)
		<b>TACACS+ Server</b> (Required setting):
<b>Server Type</b>	Required setting	

# EW200 Industrial Cellular Gateway

		<p>When <b>TACACS+ Server</b> is selected, the following settings are also required.</p> <p><b>Shared Key</b> (String format: any text)</p> <p><b>Session Timeout</b> (String format: any number)</p> <p>The values must be between 1 and 60.</p>
		<p><b>SCEP Server</b> (Required setting):</p> <p>When <b>SCEP Server</b> is selected, the following settings are also required.</p> <p><b>Path</b> (String format: any text, By default <b>cgi-bin</b> is filled)</p> <p><b>Application</b> (String format: any text, By default <b>pkiclient.exe</b> is filled)</p>
		<p><b>FTP(SFTP) Server</b> (Required setting):</p> <p>When <b>FTP(SFTP) Server</b> is selected, the following settings are also required.</p> <p><b>User Name</b> (String format: any text)</p> <p><b>Password</b> (String format: any text)</p> <p>Protocol (Select FTP or SFTP)</p> <p>Encryption (Select Plain, Explicit FTPS or Implicit FTPS)</p> <p>Transfer mode (Select Passive or Active)</p>
<b>Server IP/FQDN</b>	Required setting	Specify the IP address or FQDN used for the external server.
<b>Server Port</b>	Required setting	<p>Specify the Port used for the external server. If you selected a certain server type, the default server port number will be set.</p> <p>For <b>Email Server</b> 25 will be set by default;</p> <p>For <b>Syslog Server</b>, port 514 will be set by default;</p> <p>For <b>RADIUS Server</b>, port 1812 will be set by default;</p> <p>For <b>Active Directory Server</b>, port 389 will be set by default;</p> <p>For <b>LDAP Server</b>, port 389 will be set by default;</p> <p>For <b>UAM Server</b>, port 80 will be set by default;</p> <p>For <b>TACACS+ Server</b>, port 49 will be set by default;</p> <p>For <b>SCEP Server</b>, port 80 will be set by default;</p> <p>For <b>FTP(SFTP) Server</b>, port 21 will be set by default;</p> <p><u>Value Range</u>: 1 ~ 65535.</p>
<b>Account Port</b>	<p>1. Required setting</p> <p>2. <b>1813 is set by default</b></p>	<p>Specify the accounting port used if you selected external RADIUS server.</p> <p><u>Value Range</u>: 1 ~ 65535.</p>
<b>Server</b>	The box is checked by default	Click <b>Enable</b> to activate this External Server.
<b>Save</b>	N/A	Click <b>Save</b> to save the settings
<b>Undo</b>	N/A	Click <b>Undo</b> to cancel the settings
<b>Refresh</b>	N/A	Click the <b>Refresh</b> button to refresh the external server list.

## 3.4 Certificates

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.

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.

### 3.4.1 Configuration

The configuration setting allows user to create Root Certificate Authority (CA) certificates and configure enabling 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

<div>Root CA</div> <div>Generate</div>					
ID	Name	Subject	Issuer	Vaild To	Action

When the **Generate** button is applied, the **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.

# EW200 Industrial Cellular Gateway

Root CA Certificate Configuration	
Item	Setting
▶ Name	<input type="text"/>
▶ Key	Key Type : <input type="text" value="RSA"/> Key Length : <input type="text" value="512-bits"/> Digest Algorithm : <input type="text" value="MD5"/>
▶ Subject Name	Country(C) : <input type="text"/> State(ST) : <input type="text"/> Location(L) : <input type="text"/> Organization(O) : <input type="text"/> Organization Unit(OU) : <input type="text"/> Common Name(CN) : <input type="text"/> Email : <input type="text"/>
▶ Validity Period	<input type="text" value="20-years"/>

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

# EW200 Industrial Cellular Gateway

## Setup SCEP

SCEP Configuration	
Item	Setting
▶ SCEP	<input type="checkbox"/> Enable
▶ Automatically re-enroll aging certificates	<input type="checkbox"/> Enable

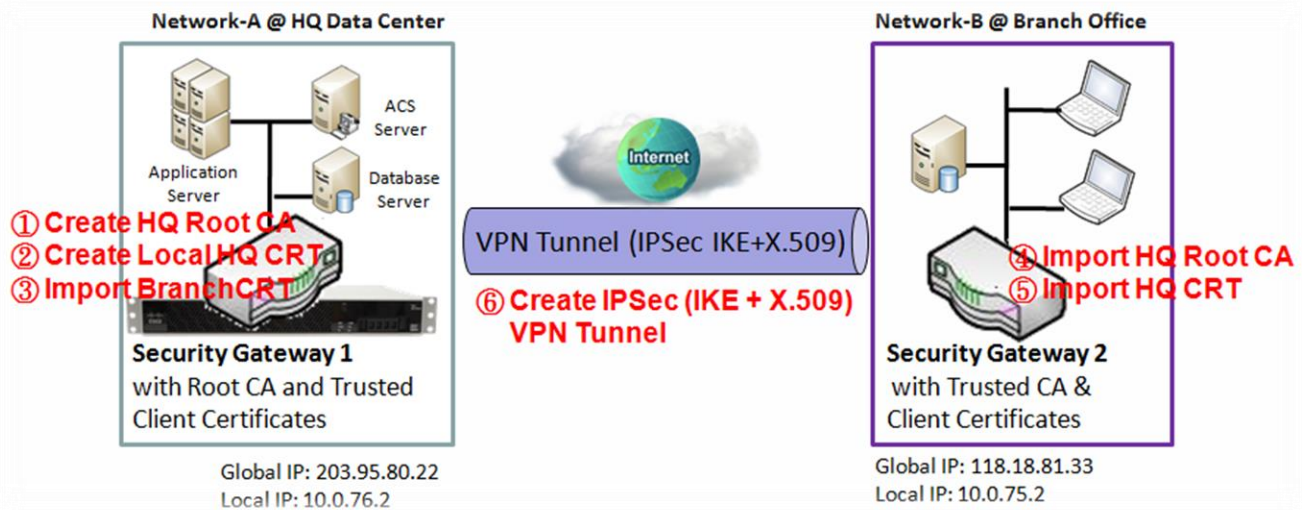
SCEP Configuration		
Item	Value setting	Description
<b>SCEP</b>	Unchecked by default	Check the <b>Enable</b> box to activate SCEP function.
<b>Automatically re-enroll aging certificates</b>	Unchecked by default	When <b>SCEP</b> is activated, check the <b>Enable</b> box to activate this function. It will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



## 3.4.2 My Certificate

My Certificate includes a Local Certificate List. Local Certificate List shows all generated certificates by the root CA for the gateway. 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. It can also import 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 of their identity when establishing a VPN tunnel.

### Scenario Description

Gateway 1 generates the root CA and a local certificate (HQCRT) signed by itself. It 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. It imports the certificate into the Gateway 2 as a local certificate. In addition, it also imports the certificates of the root CA of Gateway 1 into Gateway 2 as the trusted ones. (Refer to following two sub-sections)

An IPsec VPN tunnel is established 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.

# EW200 Industrial Cellular Gateway

## Parameter Setup Example

For Network-A at HQ

The 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 the 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 parameters that are not mentioned in the tables.

<b>Configuration Path</b>	[My Certificate]-[Root CA Certificate Configuration]
<b>Name</b>	<b>HQRootCA</b>
<b>Key</b>	Key Type: <b>RSA</b> Key Length: <b>1024-bits</b>
<b>Subject Name</b>	Country(C): <b>TW</b> State(ST): <b>Taiwan</b> Location(L): <b>Taipei</b> Organization(O): <b>EWANHQ</b> Organization Unit(OU): <b>HQRD</b> Common Name(CN): <b>HQRootCA</b> E-mail: <b>hqrootca@etherwan.com.tw</b>

<b>Configuration Path</b>	[My Certificate]-[Local Certificate Configuration]
<b>Name</b>	<b>HQCRT</b> Self-signed: <input checked="" type="checkbox"/>
<b>Key</b>	Key Type: <b>RSA</b> Key Length: <b>1024-bits</b>
<b>Subject Name</b>	Country(C): <b>TW</b> State(ST): <b>Taiwan</b> Location(L): <b>Taipei</b> Organization(O): <b>EWANHQ</b> Organization Unit(OU): <b>HQRD</b> Common Name(CN): <b>HQCRT</b> E-mail: <b>hqcert@etherwan.com.tw</b>

<b>Configuration Path</b>	[IPsec]-[Configuration]
<b>IPsec</b>	<input checked="" type="checkbox"/> <b>Enable</b>

<b>Configuration Path</b>	[IPsec]-[Tunnel Configuration]
<b>Tunnel</b>	<input checked="" type="checkbox"/> <b>Enable</b>
<b>Tunnel Name</b>	<b>s2s-101</b>
<b>Interface</b>	<b>WAN 1</b>
<b>Tunnel Scenario</b>	<b>Site to Site</b>
<b>Operation Mode</b>	<b>Always on</b>

<b>Configuration Path</b>	[IPsec]-[Local & Remote Configuration]
<b>Local Subnet</b>	<b>10.0.76.0</b>
<b>Local Netmask</b>	<b>255.255.255.0</b>
<b>Full Tunnel</b>	<b>Disable</b>
<b>Remote Subnet</b>	<b>10.0.75.0</b>
<b>Remote Netmask</b>	<b>255.255.255.0</b>
<b>Remote Gateway</b>	<b>118.18.81.33</b>

<b>Configuration Path</b>	[IPsec]-[Authentication]
---------------------------	--------------------------

# EW200 Industrial Cellular Gateway

Key Management	<i>IKE+X.509</i> Local Certificate: <i>HQCRT</i> Remote Certificate: <i>BranchCRT</i>
Local ID	<i>User Name Network-A</i>
Remote ID	<i>User Name Network-B</i>

Configuration Path	[IPsec]-[IKE Phase]
Negotiation Mode	<i>Main Mode</i>
X-Auth	<i>None</i>

## For Network-B at Branch Office

The 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 the above diagram. The configuration example must be combined with the ones in following two sections to complete the whole user scenario.

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

Configuration Path	[My Certificate]-[Local Certificate Configuration]
Name	<i>BranchCRT</i> Self-signed: <input type="checkbox"/>
Key	Key Type: <i>RSA</i> Key Length: <i>1024-bits</i>
Subject Name	Country(C): <i>TW</i> State(ST): <i>Taiwan</i> Location(L): <i>Taipei</i> Organization(O): <i>EWANBranch</i> Organization Unit(OU): <i>BranchRD</i> Common Name(CN): <i>BranchCRT</i> E-mail: <i>branchcrt@etherwan.com.tw</i>

Configuration Path	[IPsec]-[Configuration]
IPsec	■ <i>Enable</i>

Configuration Path	[IPsec]-[Tunnel Configuration]
Tunnel	■ <i>Enable</i>
Tunnel Name	<i>s2s-102</i>
Interface	<i>WAN 1</i>
Tunnel Scenario	<i>Site to Site</i>
Operation Mode	<i>Always on</i>

Configuration Path	[IPsec]-[Local & Remote Configuration]
Local Subnet	<i>10.0.75.0</i>
Local Netmask	<i>255.255.255.0</i>
Full Tunnel	<i>Disable</i>
Remote Subnet	<i>10.0.76.0</i>
Remote Netmask	<i>255.255.255.0</i>
Remote Gateway	<i>203.95.80.22</i>

# EW200 Industrial Cellular Gateway

<b>Configuration Path</b>	[IPsec]-[Authentication]
<b>Key Management</b>	<i>IKE+X.509</i> Local Certificate: <b>BranchCRT</b> Remote Certificate: <b>HQCRT</b>
<b>Local ID</b>	<i>User Name</i> <b>Network-B</b>
<b>Remote ID</b>	<i>User Name</i> <b>Network-A</b>

<b>Configuration Path</b>	[IPsec]-[IKE Phase]
<b>Negotiation Mode</b>	<i>Main Mode</i>
<b>X-Auth</b>	<i>None</i>

## Scenario Operation Procedure

In the 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. It imports 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 download 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.

# EW200 Industrial 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 lets you enter the required information necessary for corresponding certificate to be generated by itself, or corresponding CSR to be signed by other CAs.

### Create Local Certificate

Local Certificate List <span>Add</span> <span>Import</span> <span>Delete</span>					
ID	Name	Subject	Issuer	Vaild To	Actions

When the **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.

Local Certificate Configuration	
Item	Setting
▶ Name	<input type="text"/> Self-signed : <input type="checkbox"/>
▶ Key	Key Type : <span>RSA</span> Key Length : <span>1024-bits</span> Digest Algorithm : <span>SHA-1</span>
▶ Subject Name	Country(C) : <input type="text"/> State(ST) : <input type="text"/> Location(L) : <input type="text"/> Organization(O) : <input type="text"/> Organization Unit(OU) : <input type="text"/> Common Name(CN) : <input type="text"/> E-mail : <input type="text"/>
▶ Extra Attributes	Challenge Password: <input type="text"/> Unstructured Name: <input type="text"/>
▶ SCEP Enrollment	Enable: <input type="checkbox"/> SCEP Server: <span>--- Option ---</span> <span>Add Object</span> CA Certificate: <span>IDG761AM-JH.crt</span> CA Encryption Certificate: <span>--- Option ---</span> (Optional) CA Identifier: <input type="text"/> (Optional)

# EW200 Industrial Cellular Gateway

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

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

# EW200 Industrial Cellular Gateway

Import

Choose File

No file chosen

Apply

Cancel

PEM Encoded

Apply

Cancel

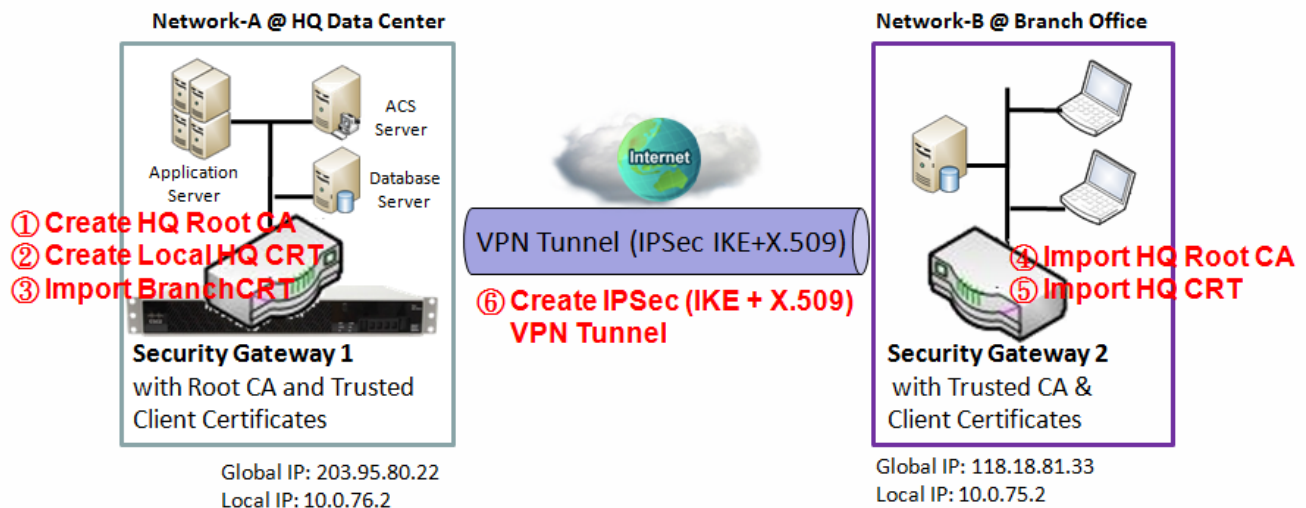
Import Item	Value setting	Description
Import	Required setting	Select a certificate file from user’s computer, and click the <b>Apply</b> button to import the specified certificate file to the gateway.
PEM Encoded	1. String format, any text 2. Required setting	This is an alternative approach to import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

# EW200 Industrial Cellular Gateway

## 3.4.3 Trusted Certificate

Trusted Certificate includes Trusted CA Certificate List, Trusted Client Certificate List, and Trusted Client Key List. The Trusted CA Certificate List contains the certificates of external trusted CAs. The Trusted Client Certificate List contains the others' certificates that you trust. The Trusted Client Key List contains the others' keys that you have trusted.

### Self-signed Certificate Usage Scenario



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

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

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

Gateway 1 generates the root CA and a local certificate (HQCRT) signed by itself. It 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 Gateway 1 sign it to be the BranchCRT certificate. It imports the certificate into the Gateway 2 as a local certificate. It also imports the certificates of the root CA of Gateway 1 into the Gateway 2 as trusted ones. (Refer to "My Certificate" and "Issue Certificate" sections).

An IPsec VPN tunnel can be established with IKE and X.509 protocols starting from either peer, so that all client hosts in these both subnets can communicate with each other.

Parameter Setup Example is the same as described in "My Certificate" section.

For Network-A at HQ



## EW200 Industrial Cellular Gateway

The 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 the 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.

<b>Configuration Path</b>	[Trusted Certificate]-[Trusted Client Certificate List]
<b>Command Button</b>	<i>Import</i>

<b>Configuration Path</b>	[Trusted Certificate]-[Trusted Client Certificate Import from a File]
<b>File</b>	<i>BranchCRT.crt</i>

For Network-B at Branch Office

<b>Configuration Path</b>	[Trusted Certificate]-[Trusted CA Certificate List]
<b>Command Button</b>	<i>Import</i>

<b>Configuration Path</b>	[Trusted Certificate]-[Trusted CA Certificate Import from a File]
<b>File</b>	<i>HQRootCA.crt</i>

<b>Configuration Path</b>	[Trusted Certificate]-[Trusted Client Certificate List]
<b>Command Button</b>	<i>Import</i>

<b>Configuration Path</b>	[Trusted Certificate]-[Trusted Client Certificate Import from a File]
<b>File</b>	<i>HQCRT.crt</i>

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

In the above diagram, "Gateway 1" is the gateway of Network-A located at 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 located at the 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 2 imports the certificates of the root CA and HQCRT that were generated and signed by Gateway 1 into the "Trusted CA Certificate List" and "Trusted Client Certificate List" of Gateway 2.

It imports 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.

# EW200 Industrial 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

Trusted CA Certificate List					
Import Delete Get CA					
ID	Name	Subject	Issuer	Vaild To	Actions

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

Trusted CA Certificate Import from a File

Choose File No file chosen

Apply Cancel

Trusted CA Certificate Import from a PEM

Apply Cancel

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

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

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

# EW200 Industrial Cellular Gateway

Get CA Configuration	
Item	Setting
▶ SCEP Server	<div>--- Option --- ▼</div> <div>Add Object</div>
▶ CA Identifier	<div></div> (Optional)

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

## Import Trusted Client Certificate

Trusted Client Certificate List <div>Import</div> <div>Delete</div>					
ID	Name	Subject	Issuer	Vaild To	Actions

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

Trusted Client Certificate Import from a File	
<div>Choose File No file chosen</div>	
<div>Apply Cancel</div>	

Trusted Client Certificate Import from a PEM	
<div></div>	
<div>Apply Cancel</div>	

## Trusted Client Certificate List

# EW200 Industrial Cellular Gateway

Item	Value setting	Description
<b>Import from a File</b>	Required setting	Select a certificate file from a connected computer, and click the <b>Apply</b> button to import the specified certificate file to the gateway.
<b>Import from a PEM</b>	1. String format, any text 2. Required setting	This is an alternative approach to importing a certificate. You can directly enter (Copy and Paste) the PEM encoded certificate string, and click the <b>Apply</b> button to import the specified certificate to the gateway.
<b>Apply</b>	N/A	Click the <b>Apply</b> button to import the certificate.
<b>Cancel</b>	N/A	Click the <b>Cancel</b> button to discard the import operation and the screen will return to the Trusted Certificates page.

## Import Trusted Client Key

Trusted Client Key List <input type="button" value="Import"/> <input type="button" value="Delete"/>		
ID	Name	Actions

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

Trusted Client Key Import from a File

Trusted Client Key Import from a PEM

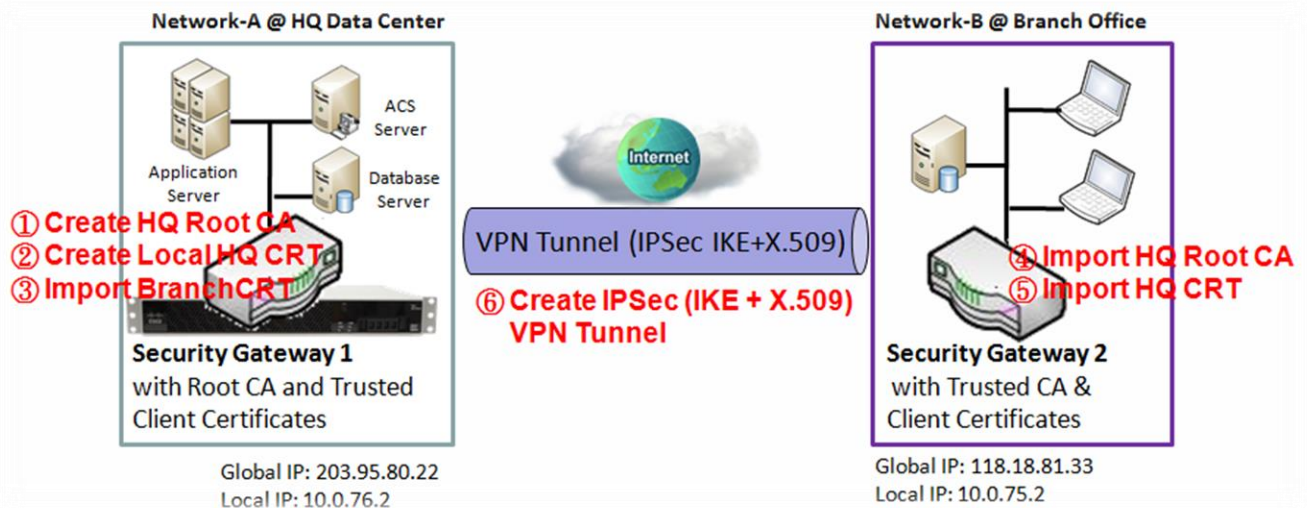
Trusted Client Key List		
Item	Value setting	Description
<b>Import from a File</b>	Required setting	Select a certificate key file from a connected computer, and click the <b>Apply</b> button to import the specified key file to the gateway.
<b>Import from a PEM</b>	1. String format, any text 2. Required setting	This is an alternative approach to importing a certificate key. You can directly enter (Copy and Paste) the PEM encoded certificate key string, and click the <b>Apply</b> button to import the specified certificate key to the gateway.
<b>Apply</b>	N/A	Click the <b>Apply</b> button to import the certificate key.
<b>Cancel</b>	N/A	Click the <b>Cancel</b> button to discard the import operation. The screen will return to the Trusted Certificates page.

## 3.4.4 Issue Certificate

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

If the gateway signs a CSR successfully, the "Signed Certificate View" window will show the resulting certificate contents. In addition, a "Download" button will be available for downloading the certificate to a file to the managing PC.

### Self-signed Certificate Usage Scenario



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

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

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

Gateway 1 generates the root CA and a local certificate (HQCRT) signed by itself. It 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 as the BranchCRT certificate. It imports the certificate into Gateway 2 as a local certificate. In addition, it also imports the certificates of the root CA of Gateway 1 into Gateway 2 as trusted ones. (Refer to "My Certificate" and "Trusted Certificate" sections).

# EW200 Industrial Cellular Gateway

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

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

For Network-A at HQ

The 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 the 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.

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

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

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

In the 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 the 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. It imports 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 download it). It takes the CSR to be signed by the root CA of Gateway 1 and obtains the BranchCRT certificate (which needs to be renamed). Import the certificate into the "Trusted Client Certificate List" of 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.

# EW200 Industrial 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

Sign

Choose File No file chosen

Certificate Signing Request (CSR) Import from a PEM

Sign

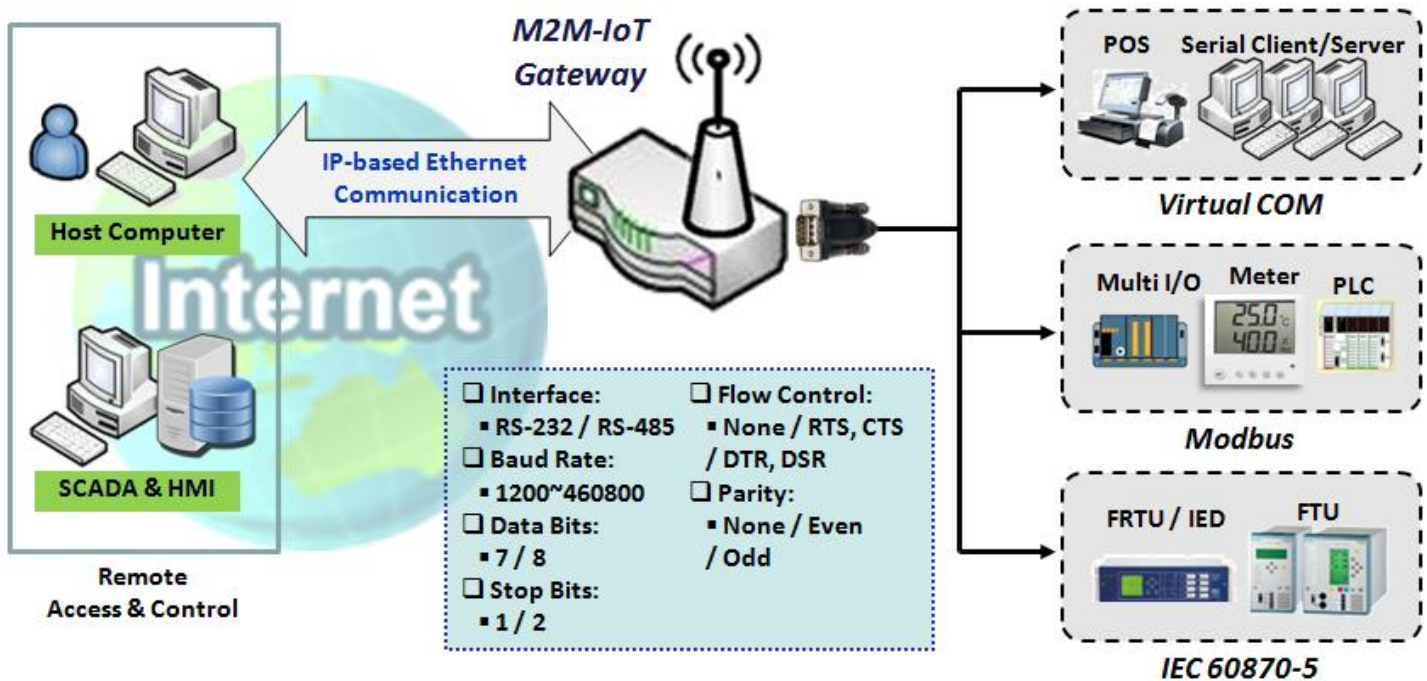
Certificate Signing Request (CSR) Import from a File		
Item	Value setting	Description
Certificate Signing Request (CSR) Import from a File	Required setting	Select a certificate signing request file from your computer for importing to the gateway.
Certificate Signing Request (CSR) Import from a PEM	1. String format, any text 2. Required setting	Enter (copy-paste) the certificate signing request PEM encoded certificate to the gateway.
Sign	N/A	When root CA exists, click the <b>Sign</b> button to sign and issue the imported certificate by root CA.



## Chapter 4 Field Communication

### 4.1 Bus & Protocol

The gateway may be equipped with a serial port for serial communication by connecting an RS-232 or RS-485 serial device to an IP-based Ethernet LAN. These communication protocols make allow for easy access to serial devices anywhere over a local LAN or the Internet. 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 quickly switch from one communication protocol to another for the serial port. The number of ports and type of the supported protocols will vary depending on gateway model.



# EW200 Industrial 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 lets 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	Displays the serial port ID. The number of serial ports will vary depending on gateway model.
Operation Mode	Disable is set by default	Displays the current selected operation mode for the serial interface. Depending on the 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 cable length and the installation environment.
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. Support for Flow Control depends on the model.
Parity	None is set by default	Select None / Even / Odd for Parity bit.
Action	N/A	Click <b>Edit</b> button to change the operation mode, or modify the parameters mentioned above for the serial interface communication.
Save	N/A	Click <b>Save</b> button to save the settings.
Undo	N/A	Click <b>Undo</b> button to cancel the settings.

# EW200 Industrial Cellular Gateway

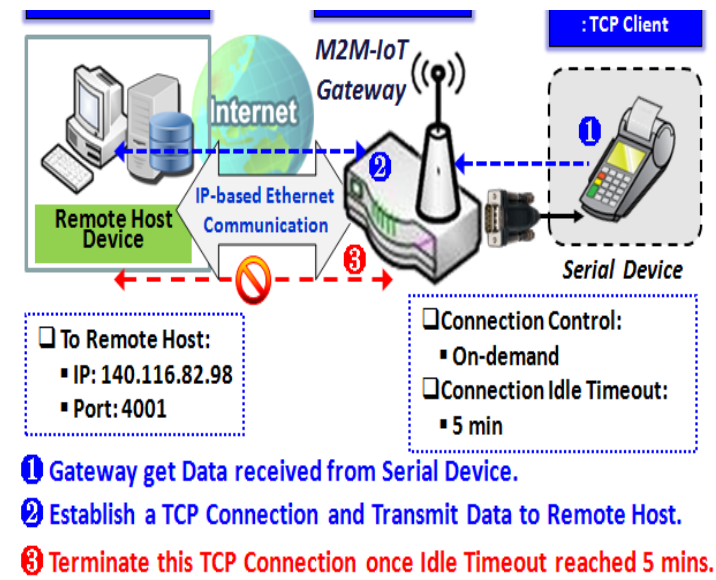
## 4.1.2 Virtual COM

Create a virtual COM port on user’s PC/Host to provide access to a serial device connected to the serial port on the gateway. This will allow access, control, and management of the connected serial device through the Internet (fixed line or cellular network). This is also known as Ethernet pass-through communication.

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	Disable	N/A	N/A	N/A	N/A	N/A	N/A	<input type="checkbox"/>	Edit

The Virtual COM setting screen enables user to connect a Virtual COM port based device to the Internet, so that serial data can be accessed remotely. There are Disable, TCP Client, TCP Server, UDP, and RFC2217 modes for remote accessing of the connected serial device. These operation modes are illustrated below.

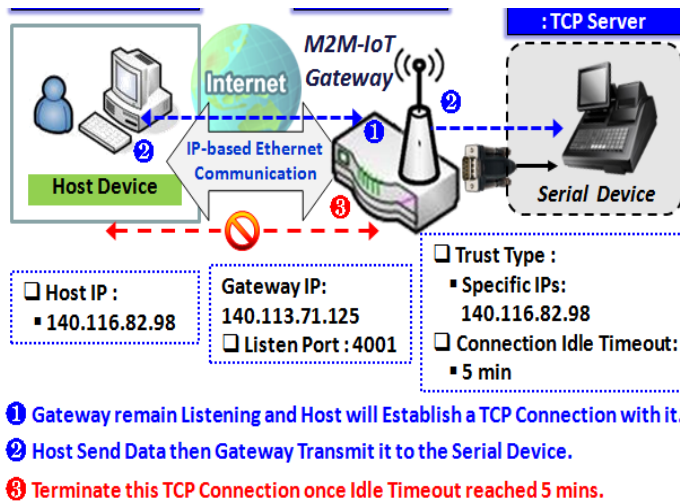
### TCP Client Mode



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. 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.

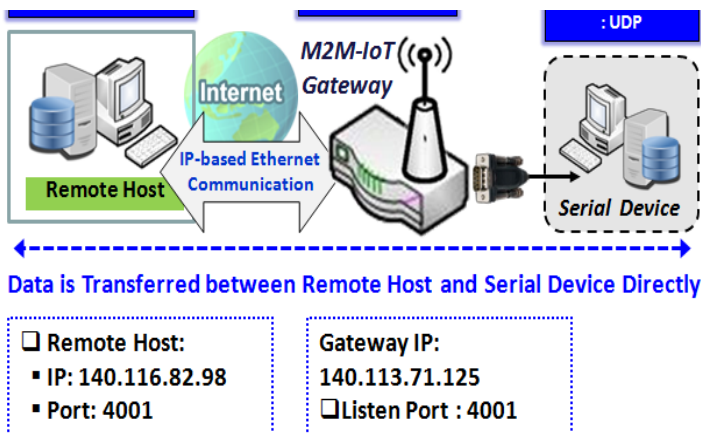
# EW200 Industrial Cellular Gateway

## TCP Server Mode



When the administrator expects the gateway to wait passively for the serial data requests from the Host Device, 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

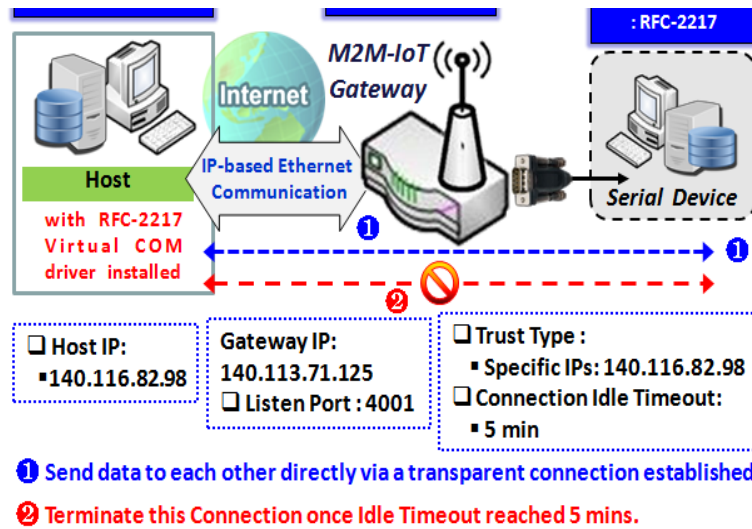


If both the Remote Host Computer and the serial device are expected to initiate a data transfer when required, the operation mode for the "Virtual COM" function in the gateway is required to be "UDP". In this mode, the UDP data can be transferred between the gateway and multiple host computers from either 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.

# EW200 Industrial Cellular Gateway

## RFC-2217 Mode



RFC-2217 defines general COM port control options based on the 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 RFC-2217 can be installed 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.

# EW200 Industrial Cellular Gateway

## Virtual COM Setting

The Virtual COM setting screen enables user to connect a Virtual COM port based device to the Internet, allowing users to access serial data remotely. There are Disable, TCP Client, TCP Server, UDP, and RFC2217 modes for remote accessing the connected serial device. By default, it is configured in Disable mode.

To use the Virtual COM function, 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

You can configure the gateway as the TCP (Transmission Control Protocol) Client. In TCP Client mode, the device initiates a TCP connection with a TCP server when there is data to transmit. The 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. TCP Client supports up to 4 server connections.

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 ▾	4001 (1-65535)	Allow All ▾	1	Always on ▾	0 (0-3600secs)	0 (0-3600secs)	<input type="checkbox"/>	Edit

Enable TCP Client Mode Window		
Item	Value setting	Description
Operation Mode	Required setting	Select <b>TCP Client</b> .
Connection Control	<b>Always on</b> is set by default	Choose <b>Always on</b> for a TCP full time connection. Otherwise, choose <b>On-Demand</b> to initiate TCP connection only when required to transmit, and to 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 the idle time has elapsed. Idle timeout is only available when <b>On-Demand</b> is selected in the <b>Connection Control</b> field.
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
Enable	Unchecked by default	Check the <b>Enable</b> box to activate the corresponding serial port in specified operation mode.
Save	N/A	Click the <b>Save</b> button to save the configuration

# EW200 Industrial Cellular Gateway

## Specify Data Packing Parameters

Data Packing (for TCP Client, TCP Server and UDP operation mode)				
Serial Port	Data Buffer Length	Delimiter Character 1	Delimiter Character 2	Data Timeout Transmit
SPort-0	<input type="text" value="0"/> (0~1024)	<input type="text" value="0"/> (Hex) <input type="checkbox"/> Enable	<input type="text" value="0"/> (Hex) <input type="checkbox"/> Enable	<input type="text" value="0"/> (0~1000ms)

Data Packing Configuration		
Item	Value setting	Description
<b>Data Buffer Length</b>	1. Optional setting 2. Default value is 0	Enter the data buffer length for the serial port. <b>Value Range:</b> 0 ~ 1024.
<b>Delimiter Character 1</b>	1. Optional setting 2. Default value is 0	Check the <b>Enable</b> box to activate the Delimiter character 1, and enter the Hex code for it. <b>Value Range:</b> 0x00 ~ 0xFF.
<b>Delimiter Character 2</b>	1. Optional setting 2. Default value is 0	Check the <b>Enable</b> box to activate the Delimiter character 2, and enter the Hex code for it. <b>Value Range:</b> 0x00 ~ 0xFF.
<b>Data Timeout Transmit</b>	1. Optional setting 2. Default value is 0	Enter the data timeout interval for transmitting serial data through the port. By default, it is set to 0 and the timeout function is disabled. <b>Value Range:</b> 0 ~ 1000ms.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the configuration

## Specify Remote TCP Server

Legal Host IP/ FQDN Definition (for TCP Client operation mode)					
ID	To Remote Host	Remote Port	Serial Port	Definition Enable	Action
1		4001	SPort-0	<input type="checkbox"/>	<input type="button" value="Edit"/>
2		4001	SPort-0	<input type="checkbox"/>	<input type="button" value="Edit"/>
3		4001	SPort-0	<input type="checkbox"/>	<input type="button" value="Edit"/>
4		4001	SPort-0	<input type="checkbox"/>	<input type="button" value="Edit"/>

Specify TCP Server Window		
Item	Value setting	Description
<b>To Remote Host</b>	Required setting	Press <b>Edit</b> button to enter IP address or FQDN of the remote TCP server to transmit serial data.
<b>Remote Port</b>	1. Required setting 2. Default value is 4001	Enter the TCP port number. This is the listening port of the remote TCP server. <b>Value Range:</b> 1 ~ 65535.
<b>Serial Port</b>	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.
<b>Definition Enable</b>	Unchecked by default	Check the <b>Enable</b> box to enable the TCP server configuration.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the configuration

# EW200 Industrial Cellular Gateway

## Enable TCP Server Mode

Configure the gateway as a 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 128 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 (1~65535)	Allow All ▼	1	Always on ▼	0 (0-3600secs)	0 (0-3600secs)	<input type="checkbox"/>	Edit

Enable TCP Server Mode Window		
Item	Value setting	Description
Operation Mode	Required setting	Select <b>TCP Server</b> mode.
Listen Port	4001 is set by default	Indicate the listening port of the TCP connection. <b>Value Range:</b> 1 ~ 65535.
Trust Type	<b>Allow All</b> is set by default	Choose <b>Allow All</b> to allow any TCP clients to connect. Otherwise choose <b>Specific IP</b> 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. <b>Value Range:</b> 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 the idle time has elapsed. Idle timeout is only available when <b>On-Demand</b> is selected in the <b>Connection Control</b> field. <b>Value Range:</b> 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. <b>Value Range:</b> 0 ~ 60 minutes.
Enable	Unchecked by default	Check the <b>Enable</b> box to activate the corresponding serial port in specified operation mode.
Save	N/A	Click <b>Save</b> button to save the settings.

# EW200 Industrial 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.

Trusted IP Definition (for TCP Server & RFC-2217 operation mode)				
ID	Host	Serial Port	Definition Enable	Action
1			<input type="checkbox"/>	Edit
2			<input type="checkbox"/>	Edit
3			<input type="checkbox"/>	Edit
4			<input type="checkbox"/>	Edit
5			<input type="checkbox"/>	Edit
6			<input type="checkbox"/>	Edit
7			<input type="checkbox"/>	Edit
8			<input type="checkbox"/>	Edit

Specify TCP Clients Window		
Item	Value setting	Description
Host	Required setting	Enter the IP address range of allowed TCP clients.
Serial Port	Unchecked by default	Check the box to specify the rule for selected Serial Port.
Definition Enable	Unchecked by default	Check the <b>Enable</b> box to enable the rule.
Save	N/A	Click <b>Save</b> to save the settings
Undo	N/A	Click <b>Undo</b> 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.

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	UDP ▼	4001 (1~65535)	Allow All ▼	1	Always on ▼	0 (0-3600secs)	0 (0-3600secs)	<input type="checkbox"/>	Edit



# EW200 Industrial Cellular Gateway

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

## Specify Remote UDP

Legal Host IP Definition (for UDP operation mode)					
ID	Remote Host	Remote Port	Serial Port	Definition Enable	Action
1		4001	SPort-0	<input type="checkbox"/>	Edit
2		4001	SPort-0	<input type="checkbox"/>	Edit
3		4001	SPort-0	<input type="checkbox"/>	Edit
4		4001	SPort-0	<input type="checkbox"/>	Edit

Specify Remote UDP hosts Window		
Item	Value setting	Description
<b>Host</b>	Required setting	Press <b>Edit</b> button to enter IP address range of remote UDP hosts.
<b>Remote Port</b>	4001 is set by default	Indicate the UDP port of peer UDP hosts. <b><u>Value Range:</u></b> 1 ~ 65535
<b>Serial Port</b>	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.
<b>Definition Enable</b>	Unchecked by default	Check the <b>Enable</b> box to enable the rule.
<b>Save</b>	N/A	Click <b>Save</b> to save the settings
<b>Undo</b>	N/A	Click <b>Undo</b> to cancel the settings

# EW200 Industrial Cellular Gateway

## Enable RFC-2217 Mode

RFC-2217 defines general COM port control options based on the Telnet protocol. With the RFC-2217 mode, a 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 (1~65535)	Allow All ▼	1	Always on ▼	0 (0-3600secs)	0 (0-3600secs)	<input type="checkbox"/>	Edit

Enable RFC-2217 Mode Window		
Item	Value setting	Description
Operation Mode	Required setting	Select <b>RFC-2217</b> mode.
Listen Port	4001 is set by default	Indicate the listening port of RFC-2217 connection. <b>Value Range:</b> 1 ~ 65535
Trust Type	Allow All is set by default	Choose <b>Allow All</b> to allow any clients to connect. Otherwise choose <b>Specific IP</b> 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 the idle time has elapsed. <b>Value Range:</b> 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 no response time of alive-check is longer than this timeout setting. <b>Value Range:</b> 0 ~ 60 minutes.
Enable	Unchecked by default	Check the <b>Enable</b> box to activate the corresponding serial port in specified operation mode.
Save	N/A	Click <b>Save</b> to save the settings
Undo	N/A	Click <b>Undo</b> to cancel the settings

# EW200 Industrial 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.

Trusted IP Definition (for TCP Server & RFC-2217 operation mode)				
ID	Host	Serial Port	Definition Enable	Action
1			<input type="checkbox"/>	Edit
2			<input type="checkbox"/>	Edit
3			<input type="checkbox"/>	Edit
4			<input type="checkbox"/>	Edit
5			<input type="checkbox"/>	Edit
6			<input type="checkbox"/>	Edit
7			<input type="checkbox"/>	Edit
8			<input type="checkbox"/>	Edit

Specify RFC-2217 Clients for Access Window		
Item	Value setting	Description
Host	Required setting	Enter the IP address range of allowed clients.
Serial Port	Unchecked by default	Check the box to specify the rule for selected Serial Port.
Definition Enable	Unchecked by default	Check the <b>Enable</b> box to enable the rule.
Save	N/A	Click <b>Save</b> to save the settings
Undo	N/A	Click <b>Undo</b> to cancel the settings

## Configure VirtualCOM Data Logging

If you intend to monitor the traffic of the serial port, you can configure the data logging settings and enable it to get the traffic log consequently.

COM Logging						
Serial Port	Storage Device	Remote Log Server(UDP)		Upload Server	Data Format	Max Record Day
SPort-0	External <input type="button" value="Download"/> <input type="checkbox"/> Enable	IP <input type="text"/>	TX Port <input type="text"/> RX Port <input type="text"/>	--- Option --- <input type="button" value="Add Object"/> <input type="checkbox"/> Enable	HEX <input type="button" value="v"/>	3 <input type="button" value="v"/>

# EW200 Industrial Cellular Gateway

COM Logging Configuration Window		
Item	Value setting	Description
<b>Storage Device</b>	Unchecked by default	Check the <b>Enable</b> box and use the attached available storage (USB or SD-card) device to keep the data log file under the folder “\virtual-com-log\SPort-n\Date\” . Click the <b>Download</b> button to get the log files (*.csv).
<b>Remote Log Server (UDP)</b>	Unchecked by default	Check the <b>Enable</b> box and use remote log server to keep the recorded traffic log over the serial port. You have to further specify the IP address and port number for the log server. Value Range: 1 ~ 65535, and 0 for disabled by default.
<b>Upload Server</b>	Unchecked by default	Check the <b>Enable</b> box and select a pre-defined FTP server from the dropdown list. You can also click the Add Object button to create a new entry for the server information. The device will auto-upload the logged traffic with a zipped file (*.csv.gz) per hour to the designated FTP server.
<b>Data Format</b>	<b>HEX</b> is set by default	Specify the data format for the logged traffic. It can be <b>HEX</b> or <b>ASCII</b> .
<b>Max Record Day</b>	<b>3</b> is set by default	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 Alive check timeout is only available when <b>On-Demand</b> is selected in the <b>Connection Control</b> field. Value Range: 1 ~ 30 days.
<b>Enable</b>	Unchecked by default	Check the Enable box to activate the data logging function for corresponding serial port with specified configuration.
<b>Save</b>	N/A	Click <b>Save</b> to save the settings
<b>Undo</b>	N/A	Click <b>Undo</b> to cancel the settings

# EW200 Industrial Cellular Gateway

## 4.1.3 Modbus

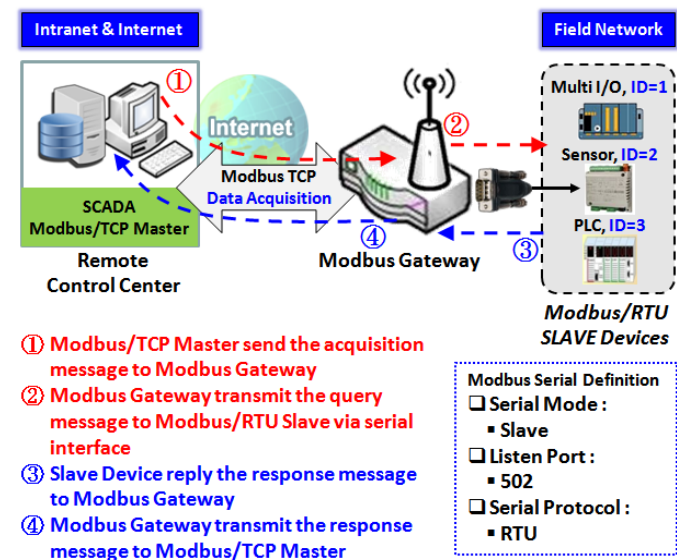
Modbus is one of the most popular automation protocols in the world, supporting traditional RS-232/422/485 devices and recently developed Ethernet devices. Many industrial devices, such as PLCs, DCSs, HMIs, instruments, and smart meters use the Modbus protocol as the communication standard. It is used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

However, the Ethernet-based Modbus protocol is 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



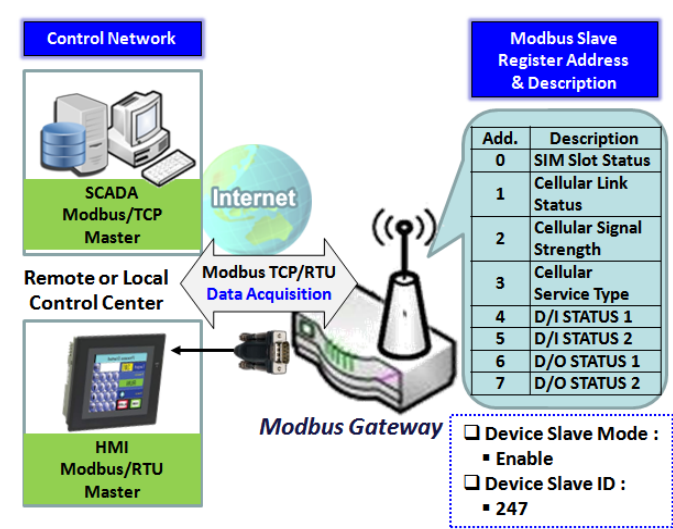
The IoT Gateway serves as a Modbus gateway to communicate with the Modbus TCP Master, the SCADA Server, located at a remote control center for Modbus device accessing.

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

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

# EW200 Industrial Cellular Gateway

## Modbus Slave Scenario



In addition to behaving as a Modbus Gateway, there is an integrated Modbus Slave option for providing device status, such as Cellular Network and DI/DO status, to remote Modbus Master via Modbus communication.

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

# EW200 Industrial 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 you have completed the Modbus settings in this section, select Modbus Operation Mode in the Port Configuration screen.

### Define Modbus Gateway function for each Serial Port

Modbus Gateway Definition						
Serial Port	Gateway Mode	Device Slave Mode	Listen Port	Serial Protocol	Enable	Action
▶ SPort-0	Disable	Slave Mode: Disable	502	RTU	<input type="checkbox"/>	Edit

Modbus Gateway Definition		
Item	Value setting	Description
Serial Port	N/A	Displays the name of the serial port used. E.g. SPort-0. The number of serial ports varies by model.
Gateway Mode	Disable is set by default	Specify the Modbus gateway mode for the selected serial port. It can be Disable, Serial as Slave or Serial as Master. A serial port can be attached with one Modbus Master, or daisy-chained in a group of Modbus Slave devices. <b>Disable:</b> Disable the Modbus gateway function for the selected serial port. <b>Serial as Slave:</b> For when attached serial device(s) are all Modbus Slave devices. <b>Serial as Master:</b> When the attached serial device is a Modbus Master device.
Device Slave Mode	Unchecked by default	Check the <b>Enable</b> box to activate the integrated Modbus Slave function, and enter the preferred ID for the integrated Modbus slave. 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. Value Range: 1 ~ 247.
Listen Port	1. 502 is set by default 2. Range 1 to 65535	Specify the Listening Port number if Slave device(s) is/are attached to the selected serial port. This setting is unneeded if a Master device is attached. <u>Value Range:</u> 1 ~ 65535. Note: Use different port numbers for the serial ports for products with multiple serial ports.
Serial Protocol	RTU is set by default	Select the serial protocol that is adopted by the attached Modbus device(s). It can be <b>RTU</b> or <b>ASCII</b> .
Enable	N/A	Displays whether the specific Modbus serial port is enabled or disabled. To enable or disable Modbus serial port, go to <b>Field Communication &gt; Bus &amp; Protocol &gt; Port Configuration</b> tab, and set the operation mode as <b>Modbus</b> .

# EW200 Industrial Cellular Gateway

## Specify Gateway Configuration

Gateway Mode Configuration for SPort-0	
Item	Setting
▶ Response Timeout	<input type="text" value="1000"/> ms (1~65535)
▶ Timeout Retries	<input type="text" value="0"/> times (0~5)
▶ 0Bh Exception	<input type="checkbox"/> Enable
▶ Tx Delay	<input type="checkbox"/> Enable
▶ TCP Connection Idle Time	<input type="text" value="300"/> sec (1~65535)
▶ Maximum TCP Connections	<input type="text" value="1"/> connections (1~4)
▶ TCP Keep-alive	<input type="checkbox"/> Enable
▶ Modbus Master IP Access	<input type="text" value="Allow All"/> ▼
▶ Message Buffering	<input type="checkbox"/> Enable

Gateway Mode Configuration for SPort-n		
Item	Value setting	Description
<b>Response Timeout</b>	1000 ms is set by default	Sets the response timeout of the slave after master request is sent. If the slave does not respond within the specified time, data will be discarded. This applies to the serially attached Master sent requests over to the remote Slave or requests send from the remote Master sent to the serially attached Slave. <b>Value Range:</b> 1 ~ 65535.
<b>Timeout Retries</b>	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 will not buffer Master requests. If a value other than zero is specified, the gateway will store the Master request in the buffer and retry sending the request the 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.
<b>0Bh Exception</b>	Unchecked by default	Check the <b>Enable</b> box to enable gateway to send a 0Bh exception code message to Modbus Master to indicate that the slave device did not respond within the timeout interval.
<b>Tx Delay</b>	Unchecked by default	Check the <b>Enable</b> box to activate the minimum amount of time after receiving a response before the next message can be sent out. When Tx Delay is enabled the Gateway will 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.



# EW200 Industrial Cellular Gateway

## Setup TCP/IP Connection for Receiving Modbus Master Request

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

Item	Value setting	Description
<b>TCP Connection Idle Time</b>	1. <b>300</b> 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 has elapsed, the TCP session will be terminated automatically. <u>Value Range:</u> 1 ~ 65535.
<b>Maximum TCP Connections</b>	1. 4 is set by default 2. Range 1 to 4	Enter the maximum number of allowed simultaneous TCP connections. Value Range: 1 ~ 4.
<b>TCP Keep-alive</b>	Unchecked by default	Check the <b>Enable</b> box to ensure to keep the TCP session connected.
<b>Modbus Master IP Access</b>	<b>Allow All</b> is selected by default.	Specify authorized masters on the TCP network. Select <b>Allow All</b> to allow any Modbus Master to reach the attached Slave(s). Otherwise, limit only specific Master to reach the Slave(s) by selecting <b>Specific IPs</b> . When <b>Specific IPs</b> is selected, a Trusted IP Definition dialog will appear.

## Specify Trusted Modbus Masters on the TCP network

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

▶ Modbus Master IP Access	Specific IPs ▼			
▶ Trusted IP Definition	ID	Source IP	Enable	Action
	1	Specific IP Address ▼ <input type="text"/>	<input type="checkbox"/>	Edit
	2		<input type="checkbox"/>	Edit
	3		<input type="checkbox"/>	Edit
	4		<input type="checkbox"/>	Edit

Item	Value setting	Description
<b>Source IP</b>	Required setting	Select <b>Specific IP Address</b> to only allow an IP address of the allowed Master to access the attached Slave(s). Select <b>IP Range</b> to only allow a set range of IP addresses of the allowed Master to access the attached Slave(s). Select <b>IP Address-based Group</b> 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 becomes available. Refer to <b>Object Definition &gt; Grouping &gt; Host grouping</b> . You may also access group

# EW200 Industrial Cellular Gateway

		creation through the Add Rule shortcut button. Settings configured through the Add Rule button will also appear in the Host grouping setting screen. Check the <b>Enable</b> box to enable this rule.
<b>Enable</b>	Unchecked by default	Check the <b>Enable</b> box to enable this rule.

## Modbus Priority Definition

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

▶ Message Buffering	<input checked="" type="checkbox"/> Enable			
▶ Modbus Priority Definition	<b>Modbus Priority</b>	<b>Priority Base</b>	<b>Enable</b>	<b>Action</b>
	▶ Modbus Priority 1	IP Address ▼ <input type="text"/>	<input type="checkbox"/>	<input type="button" value="Edit"/>
	▶ Modbus Priority 2		<input type="checkbox"/>	<input type="button" value="Edit"/>
	▶ Modbus Priority 3		<input type="checkbox"/>	<input type="button" value="Edit"/>
	▶ Modbus Priority 4		<input type="checkbox"/>	<input type="button" value="Edit"/>

Item	Value setting	Description
<b>Message Buffering</b>	1. Unchecked by default 2. Buffer up to 32 requests	Check the <b>Enable</b> box to buffer up to 32 requests from Modbus Master. If the <b>Enable</b> box is checked, a Modbus Priority Definition dialog will appear. Then the buffered Master requests can be further configured to prioritize the 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.
<b>Modbus Priority</b>	N/A	A Priority List for setting the priority of specified Modbus identity. Modbus Priority 1 ~ Modbus Priority 4.
<b>Priority Base</b>	IP Address by Default	Specify a Modbus identity with <b>IP Address</b> , <b>Slave ID</b> , or <b>Function Code</b> . The buffered Modbus message that matches 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 is issued by the Master.
<b>Enable</b>	Unchecked by default	Check the <b>Enable</b> box to enable the priority settings.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the settings.

# EW200 Industrial Cellular Gateway

## Specify Modbus TCP Slave device(s)

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

Modbus TCP Slave List for SPort-0 <span>Add</span> <span>Delete</span>					
ID	IP	Port	ID Range	Enable	Actions

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

Modbus TCP Slave Configuration for SPort-0	
Item	Setting
▶ IP	<input type="text"/>
▶ Port	<input type="text"/> (1~65535)
▶ ID Range	<input type="text"/> (1~247) ~ <input type="text"/> (1~247)
▶ Enable	<input type="checkbox"/>

Modbus Remote Slave Configuration		
Item	Value setting	Description
<b>IP</b>	Required setting	Enter the IP address of the remote Modbus TCP Slave device.
<b>Port</b>	1. Required 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). <u>Value Range:</u> 1 ~ 65535.
<b>ID Range</b>	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 specifying the Slave IP and Port, for accessing Remote Modbus RTU Slave(s) located behind another Modbus Gateway, user must specify the Modbus ID range of the Modbus RTU Slave(s). Value Range: 1 ~ 247.
<b>Enable</b>	Unchecked by default.	Check the <b>Enable</b> box to enable this rule.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the settings.

# EW200 Industrial Cellular Gateway

## Supported Function Code for Integrated Modbus Slave

This is for setting up 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.

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 ~ 9999

Register Address	Register Name	R / W	Register Range / Description
0	WAN-1 Connection Status	R	0 ~ 6, 0=Disconnected, 1=Connecting..., 2=Connected, 3=Disconnecting..., 5=Wait for Traffic..., 6=Disconnected
1	WAN-2 Connection Status	R	0 ~ 6, 0=Disconnected, 1=Connecting..., 2=Connected, 3=Disconnecting..., 5=Wait for Traffic..., 6=Disconnected
2	WAN-3 Connection Status	R	0 ~ 6, 0=Disconnected, 1=Connecting..., 2=Connected, 3=Disconnecting..., 5=Wait for Traffic..., 6=Disconnected
3	WAN-4 Connection Status	R	0 ~ 6, 0=Disconnected, 1=Connecting..., 2=Connected, 3=Disconnecting..., 5=Wait for Traffic..., 6=Disconnected
10	3G/4G_SERVICE_TYPE	R	0 ~ 7, 0=2G, 1=none, 2=3G, 3=3.5G, 4~6=3.75G, 7=LTE
11	3G/4G_LINK_STATUS	R	0 ~ 6, 0=Disconnected, 1=Connecting..., 2=Connected, 3=Disconnecting..., 5=Wait for Traffic..., 6=Disconnected
12	3G/4G_SIGNAL_STRENGTH	R	0 ~ 100
13	3G/4G_SIM_STATUS	R	0: SIM card with PIN code insert 1: SIM card ready 2: No SIM card
14	3G/4G_MCC	R	MCC Value
15	3G/4G_MNC	R	MNC Value
16	3G/4G_CS Register Status	R	0: Unregistered, 1: Registered
17	3G/4G_PS Register Status	R	0: Unregistered, 1: Registered
18	3G/4G_Roaming Status	R	0: Not Roaming, 1: Roaming
19	3G/4G_RSSI	R	RSSI Value
20	3G/4G_RSRP	R	RSRP Value
21	3G/4G_RSRQ	R	RSRQ Value
30	3G/4G_Module-2_SERVICE_TYPE	R	0 ~ 7, 0=2G, 1=none, 2=3G, 3=3.5G, 4~6=3.75G, 7=LTE
31	3G/4G_Module-2_LINK_STATUS	R	0 ~ 6, 0=Disconnected, 1=Connecting..., 2=Connected, 3=Disconnecting..., 5=Wait for Traffic..., 6=Disconnected
32	3G/4G_Module-2_SIGNAL_STRENGTH	R	0 ~ 100
33	3G/4G_Module-2_SIM_STATUS	R	0: SIM card with PIN code insert 1: SIM card

# EW200 Industrial Cellular Gateway

Register Address	Register Name	R / W	Register Range / Description
			ready 2: No SIM card
34	3G/4G_Module-2_MCC	R	MCC Value
35	3G/4G_Module-2_MNC	R	MNC Value
36	3G/4G_Module-2_CS Register Status	R	0: Unregistered, 1: Registered
37	3G/4G_Module-2_PS Register Status	R	0: Unregistered, 1: Registered
38	3G/4G_Module-2_Roaming Status	R	0: Not Roaming, 1: Roaming
39	3G/4G_Module-2_RSSI	R	RSSI Value
40	3G/4G_Module-2_RSRP	R	RSRP Value
41	3G/4G_Module-2_RSRQ	R	RSRQ Value
70	ADSL_Download_Data rate	R	ADSL Download Data rate value (kbps)
71	ADSL_Upload_Data rate	R	ADSL Upload Data rate value (kbps)
72	ADSL_SNR_Download	R	ADSL SNR Download value (dB)
73	ADSL_SNR_Upload	R	ADSL SNR Upload value (dB)
74	ADSL modem link status	R	0: Disconnected, 1: Connected
101	VPN IPsec tunnel 1 status	R	1: Connected, 2: Wait for traffic, 3: Disconnected, 9: Connecting
102	VPN IPsec tunnel 2 status	R	1: Connected, 2: Wait for traffic, 3: Disconnected, 9: Connecting
103	VPN IPsec tunnel 3 status	R	1: Connected, 2: Wait for traffic, 3: Disconnected, 9: Connecting
104	VPN IPsec tunnel 4 status	R	1: Connected, 2: Wait for traffic, 3: Disconnected, 9: Connecting
105	VPN IPsec tunnel 5 status	R	1: Connected, 2: Wait for traffic, 3: Disconnected, 9: Connecting
106	VPN IPsec tunnel 6 status	R	1: Connected, 2: Wait for traffic, 3: Disconnected, 9: Connecting
107	VPN IPsec tunnel 7 status	R	1: Connected, 2: Wait for traffic, 3: Disconnected, 9: Connecting
108	VPN IPsec tunnel 8 status	R	1: Connected, 2: Wait for traffic, 3: Disconnected, 9: Connecting
109	VPN IPsec tunnel 9 status	R	1: Connected, 2: Wait for traffic, 3: Disconnected, 9: Connecting
110	VPN IPsec tunnel 10 status	R	1: Connected, 2: Wait for traffic, 3: Disconnected, 9: Connecting
111	VPN IPsec tunnel 11 status	R	1: Connected, 2: Wait for traffic, 3: Disconnected, 9: Connecting
112	VPN IPsec tunnel 12 status	R	1: Connected, 2: Wait for traffic, 3: Disconnected, 9: Connecting
113	VPN IPsec tunnel 13 status	R	1: Connected, 2: Wait for traffic, 3: Disconnected, 9: Connecting
114	VPN IPsec tunnel 14 status	R	1: Connected, 2: Wait for traffic, 3: Disconnected, 9: Connecting
115	VPN IPsec tunnel 15 status	R	1: Connected, 2: Wait for traffic, 3: Disconnected, 9: Connecting
116	VPN IPsec tunnel 16 status	R	1: Connected, 2: Wait for traffic, 3: Disconnected, 9: Connecting
150	DI_STATUS_1	R	0: OFF, 1: ON

# EW200 Industrial Cellular Gateway

Register Address	Register Name	R / W	Register Range / Description
151	DO_STATUS_1	R/W	0: OFF, 1: ON
152	DI_STATUS_2	R	0: OFF, 1: ON
153	DO_STATUS_2	R/W	0: OFF, 1: ON
154	DI_STATUS_3	R	0: OFF, 1: ON
155	DO_STATUS_3	R/W	0: OFF, 1: ON
156	DI_STATUS_4	R	0: OFF, 1: ON
157	DO_STATUS_4	R/W	0: OFF, 1: ON
201	Serial Port-0_Interface	R	1: RS-232, 3: RS-485
202	Serial Port-0_Baud Rate	R	Baud Rate Value
203	Serial Port-0_Data Bits	R	7 or 8
204	Serial Port-0_Stop Bits	R	1 or 2
205	Serial Port-0_Flow Control	R	0: None, 2: RTS,CTS, 3: DTR,DSR
206	Serial Port-0_Parity	R	0: None, 1: Odd, 2: Even
211	Serial Port-1_Interface	R	1: RS-232, 3: RS-485
212	Serial Port-1_Baud Rate	R	Baud Rate Value
213	Serial Port-1_Data Bits	R	7 or 8
214	Serial Port-1_Stop Bits	R	1 or 2
215	Serial Port-1_Flow Control	R	0: None, 2: RTS,CTS, 3: DTR,DSR
216	Serial Port-1_Parity	R	0: None, 1: Odd, 2: Even
221	Serial Port-2_Interface	R	1: RS-232, 3: RS-485
222	Serial Port-2_Baud Rate	R	Baud Rate Value
223	Serial Port-2_Data Bits	R	7 or 8
224	Serial Port-2_Stop Bits	R	1 or 2
225	Serial Port-2_Flow Control	R	0: None, 2: RTS,CTS, 3: DTR,DSR
226	Serial Port-2_Parity	R	0: None, 1: Odd, 2: Even
231	Serial Port-3_Interface	R	1: RS-232, 3: RS-485
232	Serial Port-3_Baud Rate	R	Baud Rate Value
233	Serial Port-3_Data Bits	R	7 or 8
234	Serial Port-3_Stop Bits	R	1 or 2
235	Serial Port-3_Flow Control	R	0: None, 2: RTS,CTS, 3: DTR,DSR
236	Serial Port-3_Parity	R	0: None, 1: Odd, 2: Even
301	WiFi_Module_One Operation Band	R	2.4G=0, 5G=1
302	WiFi_Module_One Enable	R	Disable=0, Enable=1
303	WiFi_Module_One Channel	R	2.4G Auto=0, Channel = 1~14 5G Auto=0, Channel = 36~165
304	WiFi_Module_One System	R	2.4G, b Only=1, g Only=4, n Only=6, b/g Mixed=0, g/n Mixed=7, b/g/n Mixed=9 5G, n Only=11, a Only=2, a/n Mixed=8, a/n/ac Mixed=14
305	WiFi_Module_One Operation Mode	R	AP Router=0, WDS only=3, WDS Hybride=2
306	WiFi_Module_One WDS-1 RSSI0	R	RSSI=0~127
307	WiFi_Module_One WDS-1 RSSI1	R	RSSI=0~127
308	WiFi_Module_One WDS-2 RSSI0	R	RSSI=0~127
309	WiFi_Module_One WDS-2 RSSI1	R	RSSI=0~127
310	WiFi_Module_One WDS-3 RSSI0	R	RSSI=0~127
311	WiFi_Module_One WDS-3 RSSI1	R	RSSI=0~127
312	WiFi_Module_One WDS-4 RSSI0	R	RSSI=0~127

# EW200 Industrial Cellular Gateway

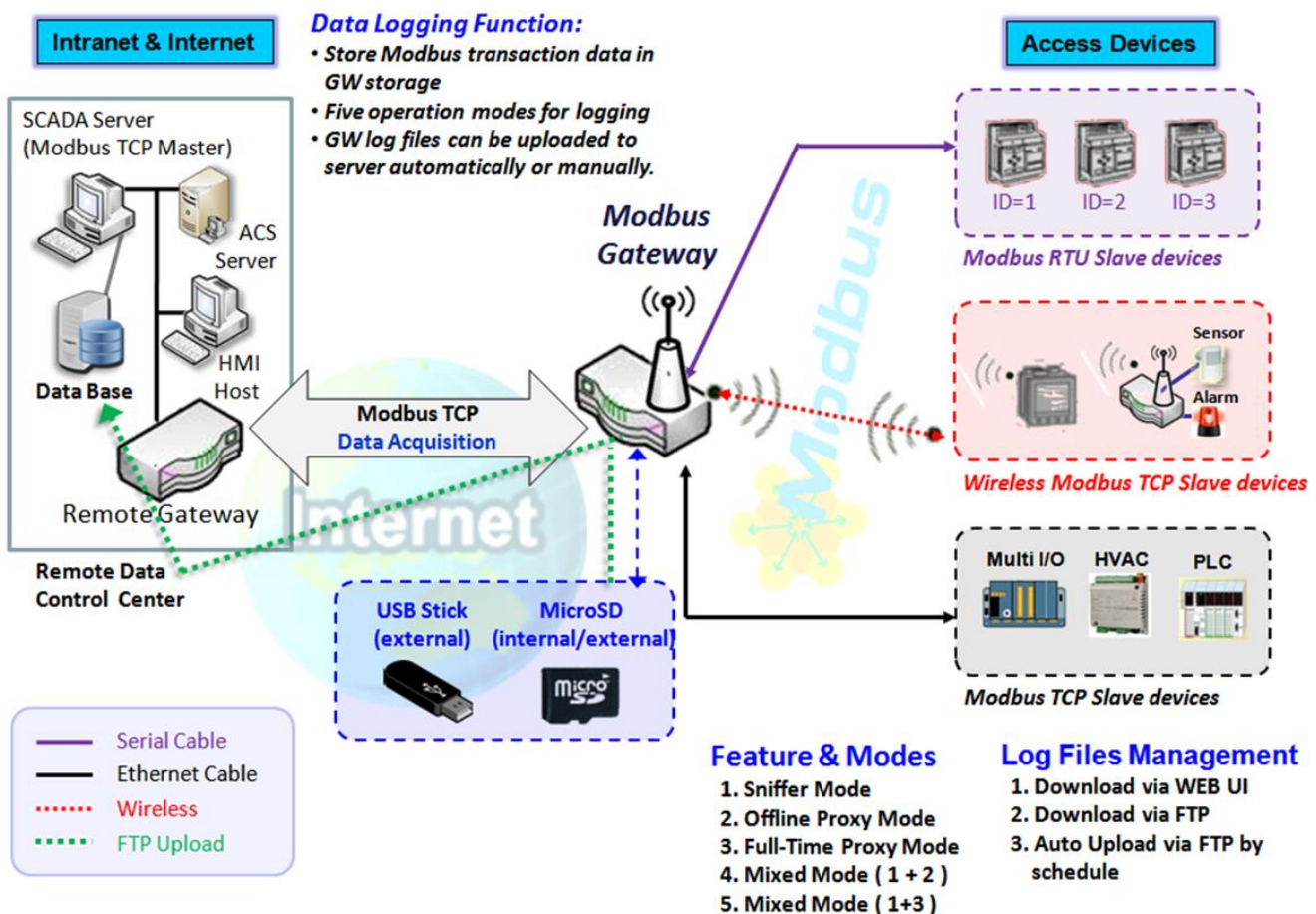
Register Address	Register Name	R / W	Register Range / Description
313	WiFi_Module_One WDS-4 RSSI1	R	RSSI=0~127
351	WiFi_Module_Two Operation Band	R	2.4G=0, 5G=1
352	WiFi_Module_Two Enable	R	Disable=0, Enable=1
353	WiFi_Module_Two Channel	R	2.4G Auto=0, Channel = 1~14 5G Auto=0, Channel = 36~165
354	WiFi_Module_Two System	R	2.4G, b Only=1, g Only=4, n Only=6, b/g Mixed=0, g/n Mixed=7, b/g/n Mixed=9 5G, n Only=11, a Only=2, a/n Mixed=8, a/n/ac Mixed=14
355	WiFi_Module_Two Operation Mode	R	AP Router=0, WDS only=3, WDS Hybride=2
306	WiFi_Module_Two WDS-1 RSSI0	R	RSSI=0~127
307	WiFi_Module_Two WDS-1 RSSI1	R	RSSI=0~127
308	WiFi_Module_Two WDS-2 RSSI0	R	RSSI=0~127
309	WiFi_Module_Two WDS-2 RSSI1	R	RSSI=0~127
310	WiFi_Module_Two WDS-3 RSSI0	R	RSSI=0~127
311	WiFi_Module_Two WDS-3 RSSI1	R	RSSI=0~127
312	WiFi_Module_Two WDS-4 RSSI0	R	RSSI=0~127
313	WiFi_Module_Two WDS-4 RSSI1	R	RSSI=0~127
1001	WiFi_Module_One Client-1 Rate	R	0~867(Mbps)
1002	WiFi_Module_One Client-1 RSSI0	R	RSSI=0~127
1003	WiFi_Module_One Client-1 RSSI1	R	RSSI=0~127
1004	WiFi_Module_One Client-1 Signal	R	Signal=0~100(%)
1097	WiFi_Module_One Client-25 Rate	R	0~867(Mbps)
1098	WiFi_Module_One Client-25 RSSI0	R	RSSI=0~127
1099	WiFi_Module_One Client-25 RSSI1	R	RSSI=0~127
1100	WiFi_Module_One Client-25 Signal	R	Signal=0~100(%)
2001	WiFi_Module_Two Client-1 Rate	R	0~867(Mbps)
2002	WiFi_Module_Two Client-1 RSSI0	R	RSSI=0~127
2003	WiFi_Module_Two Client-1 RSSI1	R	RSSI=0~127
2004	WiFi_Module_Two Client-1 Signal	R	Signal=0~100(%)
2097	WiFi_Module_Two Client-25 Rate	R	0~867(Mbps)
2098	WiFi_Module_Two Client-25 RSSI0	R	RSSI=0~127
2099	WiFi_Module_Two Client-25 RSSI1	R	RSSI=0~127
2100	WiFi_Module_Two Client-25 Signal	R	Signal=0~100(%)
9999	System_Reboot	W	Set 1 for System reboot.



## 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. The data logging function is a very useful and important feature for SCADA telemetry; it makes the monitoring and analyzing of tasks easier by checking the status and historical data during whole data acquisition period.

Even facing network connection problems with a remote NOC/SCADA side, you can enable the data logging proxy function provided by the gateway and continue doing data acquisition and storing of the collected data in local storage (in .CSV file format). When the network connection is 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 data logging schemes to meet different management requirements. They are Sniffer Mode, Offline Proxy Mode, Full-Time Proxy Mode, and mixed modes for sniffer and proxy combinations.

With 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 the administrator can check what Modbus communication went over the Modbus gateway, and if there is any communication loss among



# EW200 Industrial Cellular Gateway

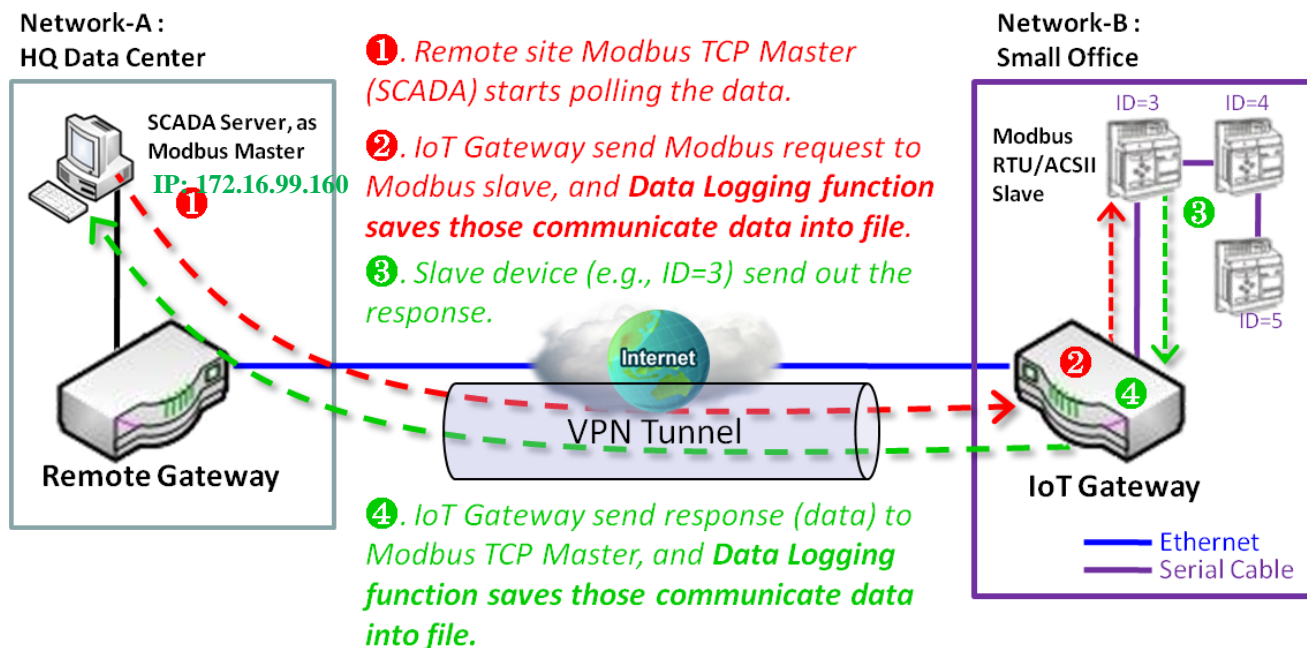
the Master and Slave sides.

However, if there is a network connection problem between the Modbus gateway and remote NOC/SCADA, the remote Modbus server won't be able to 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 loses 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 will stop the data log proxy function. The remote Modbus server can continue its data acquisition process, and if required, the administrator can also retrieve the stored data log files.

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

## ➤ Scenario for Sniffer Mode Data Logging



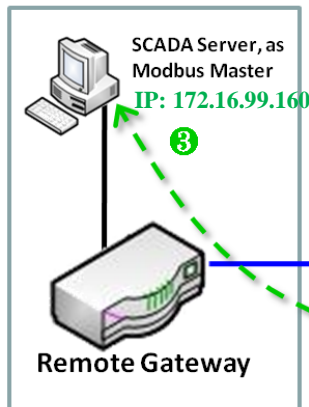
As Illustrated in the diagram, the Modbus gateway will store the following Modbus activities into a log file.

- The Modbus request sent from Remote Modbus TCP Master.
- The response (data) that is sent out from the polled Slave device (ID=3)

# EW200 Industrial Cellular Gateway

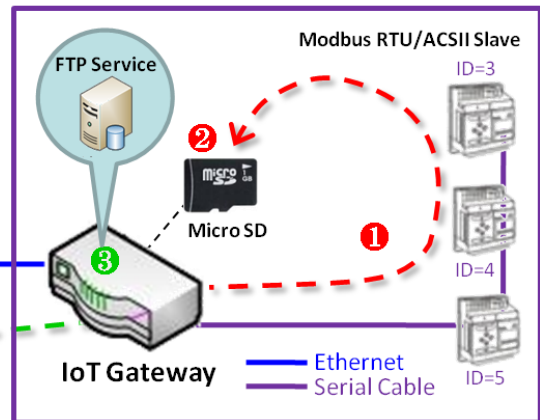
## Scenario for Off-Line Proxy Mode Data Logging

Network-A :  
HQ Data Center



- ❶ To do the Data-Acquisition by IoT Gateway itself automatically.
- ❷ Save those data as files to internal or external storage unit (e.g., Micro-SD card).
- ❸ Data Logging Files Downloading via FTP or WEB UI.

Network-B :  
Small Office



As illustrated, when the connection to a remote Modbus Master is 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) sent out from the polled Slave device (ID=3)

These data acquisition and data logging activities are repeated every 5 seconds until the connection is recovered.

# EW200 Industrial 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	<input type="checkbox"/> Enable
▶ Storage Device	External ▾

Configuration Item	Value setting	Description
Data Logging	Unchecked by default	Check the <b>Enable</b> box to activate to data logging function.
Storage Device	<b>External</b> is set by default	Choose the storage device to store the log files. It can be <b>External</b> or <b>Internal</b> , depending on the product specification.
Save	NA	Click the <b>Save</b> button to save the settings.

Note:

1. If there is no available storage device, the Enable checkbox will be grayed out, and can't be enabled. If you select External Storage, connect the storage device first, and then enable the function and also set 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 <input type="button" value="Add"/> <input type="button" value="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, the **Modbus Proxy Rule Configuration** screen will appear.

# EW200 Industrial Cellular Gateway

Modbus Proxy Rule List Configuration	
	<input type="button" value="Save"/> <input type="button" value="Undo"/>
Item	Setting
▶ Name	<input type="text"/>
▶ Modbus Slave Type	<input type="text" value="IP Address:Port"/> <input type="text"/> : <input type="text"/>
▶ Slave ID	<input type="text"/> (1~247) - <input type="text"/> (1~247)
▶ Function Code	<input type="text" value="Read Coils (0x01)"/>
▶ Start Address	<input type="text"/> (0~65535)
▶ Number of Coils/Registers	<input type="text"/> (1~125)
▶ Polling Rate (ms)	<input type="text" value="1000"/> (500~99999)

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

# EW200 Industrial Cellular Gateway

## 4.2.2 Scheme Setup

There are five data logging schemes to meet different management requirements. They are Sniffer Mode, Offline Proxy Mode, Full-Time Proxy Mode, and mixed modes for sniffer and proxy combinations. 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

Scheme List <span>Add</span> <span>Delete</span>							
ID	Name	Mode	Master Type	Master Query Timeout (sec)	Proxy Rules	Enable	Actions

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

Scheme Configuration <span>Save</span> <span>Undo</span>	
Item	Setting
▶ Name	<input type="text"/>
▶ Mode	<span>Sniffer</span> ▼
▶ Master Type	<span>IP Address</span> ▼ <input type="text"/>
▶ Enable	<input type="checkbox"/>

Scheme Configuration		
Item	Value setting	Description
<b>Name</b>	Required setting.	Specify a name as the identifier of the data logging rule. <b>Value Range:</b> 1 ~ 16 characters.
<b>Mode</b>	<b>Sniffer</b> is selected by default.	Select an expected data logging scheme for the data logging rule. There are five available schemes: <b>Sniffer:</b> The Modbus gateway will record all Modbus transactions between the Master and Slave devices. <b>Off-Line Proxy:</b> 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 the specified function code to collect and record the data / status from the slave devices. <b>Full-Time Proxy:</b> The pre-defined proxy rule will be triggered all the time and the Modbus gateway will issue the specified function code to collect and record the data / status from the slave devices. <b>Sniffer &amp; Off-Line Proxy:</b> This is a mixed mode for both Sniffer and Off-Line Proxy modes.

## EW200 Industrial Cellular Gateway

		<b>Sniffer &amp; Full-Time Proxy:</b> This is a mixed mode for both Sniffer and Full-Time Proxy modes.
<b>Master Type</b>	<b>IP Address</b> is selected by default.	Specify the Modbus master device to apply with the data logging rule. It can be <b>IP Address</b> for Modbus TCP master, or <b>Local Serial Port</b> for local attached Modbus RTU/ASCII master.
<b>Master Query Timeout (sec.)</b>	1. Optional setting. 2. <b>60</b> sec is set by default 3. Range 1 to 99999	Specify the timeout value for querying the Modbus Master. If there is no response from the master within the specified timeout setting, the 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, this value is not used.
<b>Proxy Rules</b>	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.
<b>Enable</b>	Unchecked by default.	Check the box to activate the data logging rule.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the settings.
<b>Undo</b>	N/A	Click the <b>Undo</b> button to cancel the changes.

# EW200 Industrial Cellular Gateway

## 4.2.3 Log File Management

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

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

If the user has 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 they have not been changed via the **Edit** button.

Log File List								
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	<div>Edit</div> <div>Download Log</div>

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

Log File List Configuration		Save	Undo
Item	Setting		
▶ File Content Format	Raw Data ▼		
▶ Split File by	Size ▼ 200 KB ▼		
▶ Auto Upload	<input checked="" type="checkbox"/> Enable --- Option --- ▼ <div>Add Object</div>		
▶ Log File Compression	<input type="checkbox"/> Enable		
▶ Delete File After Upload	<input type="checkbox"/> 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 'Name_yyyyMMddHHmmSS.csv'.
File Content Format	Raw Data is selected by default	Select the data format for the log files. It can be <b>Raw Data</b> , or <b>Modbus Type</b> .
Split File by	Size and 200 KB are set by default	Specify the split file methodology. It can be by <b>Size</b> , or by <b>Time Interval</b> . Specify a certain file size or time interval for splitting the data logs into a series of files. <b>Value Range:</b> 1 ~ 99999.
Auto Upload	1. Optional setting	Check the <b>Enable</b> box to activate the auto upload function for logged files.

# EW200 Industrial Cellular Gateway

	2. Unchecked by default	Once enabled, specify an external FTP server from the dropdown list for auto uploading the log files to the server. Refer to <b>Object Definition &gt; External Server &gt; External Server</b> tab, or create the FTP server with the <b>Add Object</b> button.
<b>Log File Compression</b>	1. Optional setting 2. Unchecked by default	If Auto Upload is activated, user can further specify whether to compress the log file prior to its being uploaded. Check the <b>Enable</b> button to activate the Log File Compression function.
<b>Delete File After Upload</b>	1. Optional setting 2. 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 <b>Enable</b> button to activate the function.
<b>When Storage Full</b>	<b>Remove the Oldest</b> is selected by default	Specify the operation to take when the storage is full. It can be <b>Remove the Oldest</b> log file, or <b>Stop Recording</b> . When <b>Remove the Oldest</b> is selected, the gateway will delete the oldest file once the storage is full, and continue with the data logging activity; When <b>Stop Recording</b> is selected, the gateway will stop the data logging activity once the storage is full.
<b>Save</b>	NA	Click the <b>Save</b> button to save the settings.
<b>Undo</b>	NA	Click the <b>Undo</b> 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.

## 4.3 Data Interchange

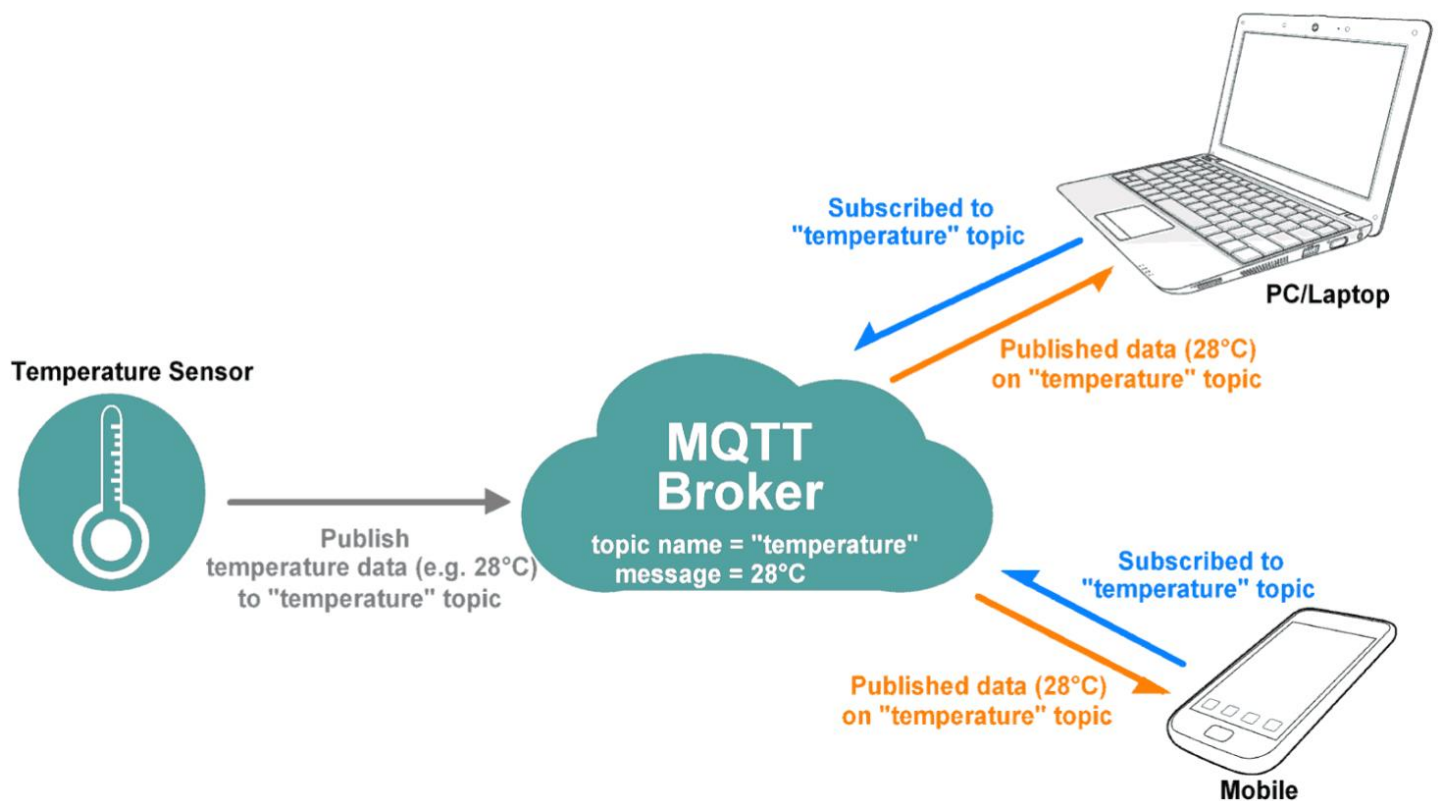
### 4.3.1 MQTT

MQTT (Message Queuing Telemetry Transport) is an ISO standard (ISO/IEC PRF 20922) publish-subscribe based messaging protocol. It works on top of the TCP/IP protocol. MQTT is a simple messaging protocol, designed for constrained devices with low-bandwidth. So, it is the perfect solution for IoT applications. An MQTT system consists of clients communicating with a server, often called a "broker". A client may be either a publisher of information or a subscriber. Each client can connect to the broker.

MQTT allows you to send commands to control outputs, read and publish data from sensor nodes, etc. Information is organized in a hierarchy of topics. When a publisher has a new item of data to distribute, it sends a control message with the data to the connected broker. The broker then distributes the information to any clients that have subscribed to that topic. The publisher does not need to have any data on the number or locations of subscribers, and subscribers in turn do not have to be configured with any data about the publishers. Therefore, it makes it really easy to establish a communication among multiple devices.



# EW200 Industrial Cellular Gateway



If a broker receives a topic for which there are no current subscribers, it will discard the topic unless the publisher indicates that the topic is to be retained. This allows new subscribers to a topic to receive the most current value rather than waiting for the next update from a publisher.

When a publishing client first connects to the broker, it can set up a default message to be sent to subscribers if the broker detects that the publishing client has unexpectedly disconnected from the broker.

Clients only interact with a broker, but a system may contain several broker servers that exchange data based on their current subscribers' topics.

In MQTT there are a few basic concepts that need to be understood:

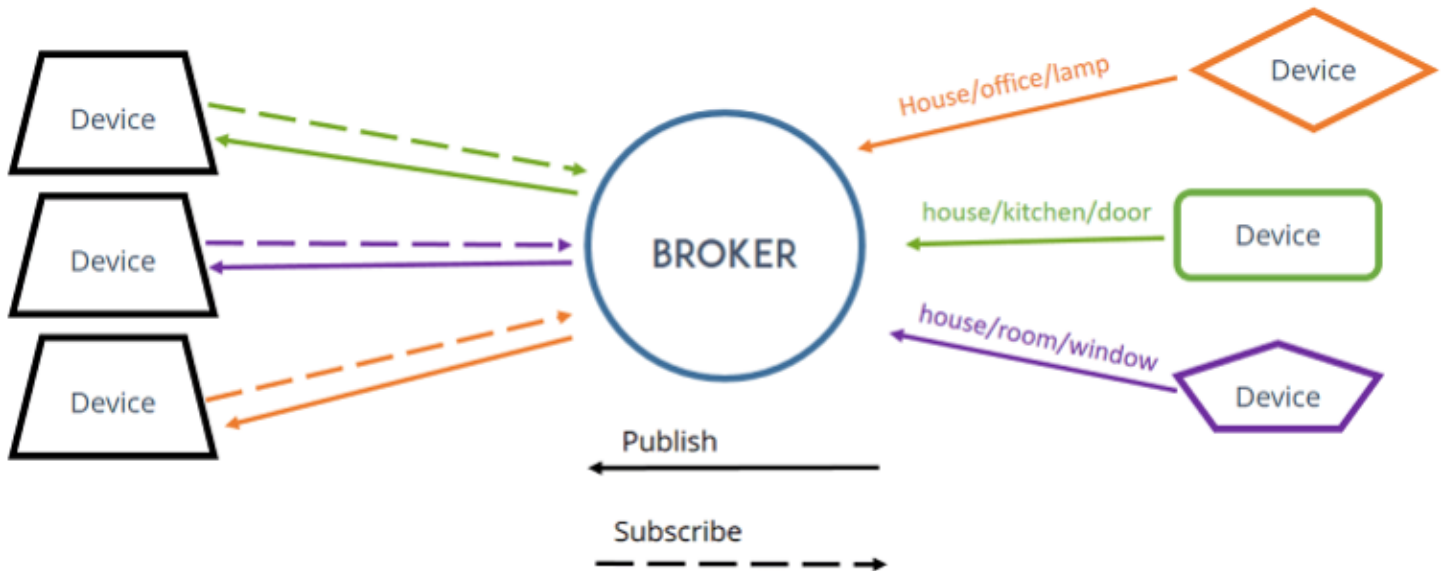
## **MQTT - Publish and Subscribe**

The first concept is the Publish and Subscribe system. In a MQTT publish and subscribe based system, a client device can publish a message on a topic, or it can be subscribed to a particular topic to receive messages.

## **MQTT - Broker**

The broker is primarily responsible for receiving all messages, filtering the messages, decide who is interested in them, and then publishing the message to all subscribed clients.

# EW200 Industrial Cellular Gateway



## MQTT - Messages

Messages are the information that you want to exchange among your devices. Whether it is a command or data.

A minimal MQTT control message can be as little as two bytes of data. There are fourteen defined message types used to connect and disconnect a client from a broker, to publish data, to acknowledge receipt of data, and to supervise the connection between client and server.

## MQTT - Topics

Topics are the way you register interest for incoming messages or how you specify where you want to publish the message.

Topics are represented with strings separated by a forward slash '/'. Each forward slash indicates a topic level.

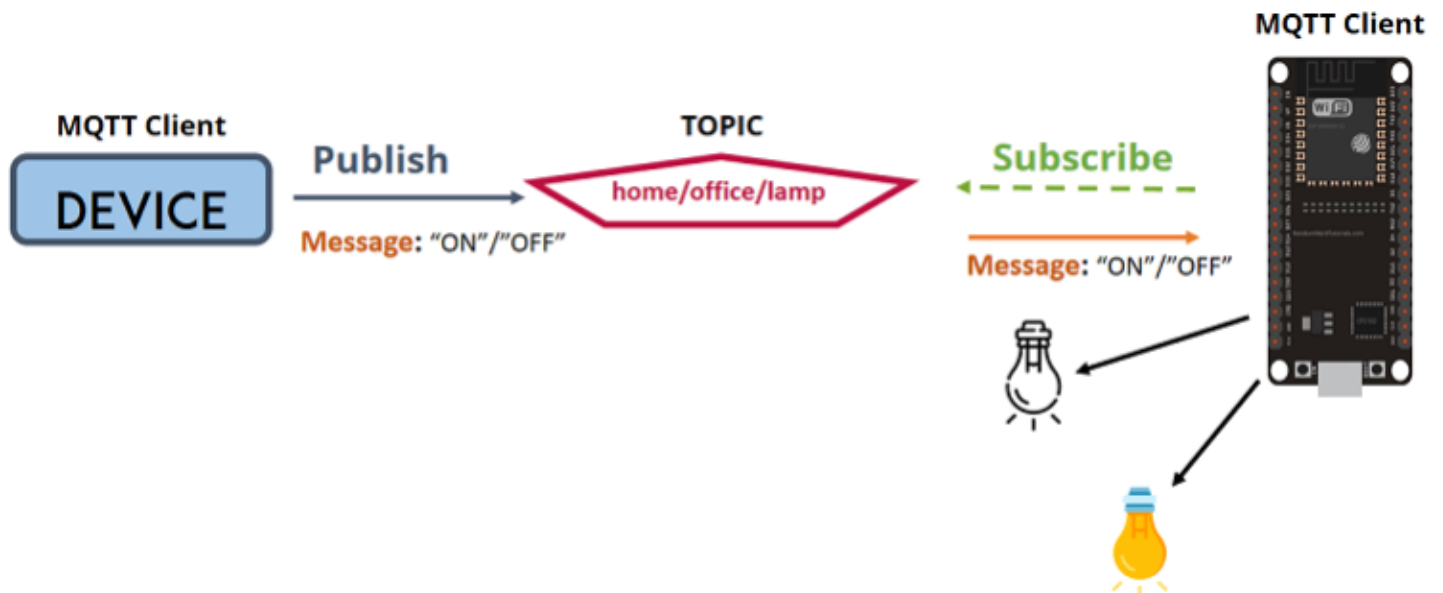
Here is an example on how you would create a topic for a lamp in your home office:



# EW200 Industrial Cellular Gateway

**Note:** topics are case-sensitive!

If you would like to turn on a lamp in your home office using MQTT, you can imagine the following scenario:



1. You have a device that publishes “on” and “off” message on the home/office/lamp topic.
2. You have a device that controls a lamp. And the device is subscribed to that topic: home/office/lamp.
3. So, when a new message is published on that topic, the subscriber received the “on” or “off” message and turns the lamp on or off.

Additionally, there are two wildcard characters ‘+’, and ‘#’. You can use the wildcard characters to subscribe to similar topics at the same time easily.

‘+’ is single level wildcard; A ‘+’ character represents a single level of hierarchy, and is used between delimiters.

For example, you can subscribe the topic “home/+/lamp” for all the lamps in a home.




‘#’ is the multi-level wildcard; A ‘#’ character represents a complete sub-tree of the hierarchy and must be the last character in a subscription topic string. For example, you can subscribe the topic “home/#” for all the related message in a home.

This product is provided with MQTT functionality, both MQTT broker and MQTT client functions are supported. You can configure it for your IoT application scenario

Go to **Field Communication > Data Interchange > MQTT** tab.

# EW200 Industrial Cellular Gateway


## Act as an MQTT Broker

 MQTT Broker Configuration  

Item	Setting
▶ Broker	<input type="checkbox"/> Enable
▶ Listening Port	<input type="text" value="1883"/> (1~65535)
▶ Authentication	<input type="checkbox"/> Enable
▶ Security	<input type="text" value="None"/>




MQTT Broker Configuration		
Item	Value setting	Description
Broker	Unchecked by default	Check the box to activate the MQTT Broker function.
Listening Port	1. Optional setting 2. 1883 is set by default	Specify a port as the listening port for MQTT broker. The MQTT broker will monitor the activity on that port and collect those valid packets from MQTT clients. If there are any MQTT client(s) subscribed to the received topic, the MQTT broker will forward the packet to the corresponding subscriber(s). <b>Value Range:</b> 1 ~ 65535.
Authentication	1. Optional setting. 2. Unchecked by default.	Check the box if user (account) authentication is required for subscribing the MQTT messages from the MQTT Broker. With the box checked, you can define up to five user accounts for permitted subscribers.
Security	1. An Optional setting. 2. None is set by default	Select the security scheme for the MQTT packets. <b>None:</b> no encryption is involved for the MQTT packets. <b>SSL/TLS:</b> SSL/TLS encryption is applied for security. You have to further specify required certificate files. Note: If <b>SSL/TLS</b> is selected, the listening port will be changed to <b>8883</b> accordingly by default.
Save	N/A	Click the Save button to save the settings.

## Create/Edit User List

 User List   

ID	Username	Password	Action
----	----------	----------	--------

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

 User List Configuration    

Item	Setting
▶ Username	<input type="text"/>
▶ Password	<input type="text"/>

# EW200 Industrial Cellular Gateway

User list Configuration		
Item	Value setting	Description
Username	Required Setting	Specify a name as the identifier of the MQTT subscriber. Value Range: 1 ~ 32 characters.
Password	Required Setting	Specify a password for the user account. Value Range: 1 ~ 32 characters.
Save	N/A	Click the Save button to save the settings.

## Act as an MQTT Client

In addition to acting as an MQTT Broker, the gateway also supports MQTT Client function. It can act as an MQTT client and publish messages to MQTT broker, or subscribe to interested topic(s) from MQTT Broker(s).

MQTT Client Function	
Item	Setting
MQTT Client	<input type="checkbox"/> Enable

MQTT Client Configuration		
Item	Value setting	Description
MQTT Client	Unchecked by default	Check the box to activate the MQTT Client function. With the MQTT Client enabled, the gateway acts as an MQTT client and publishes messages to the MQTT broker, or subscribes to interested topic(s) from MQTT Broker(s)
Save	N/A	Click the Save button to save the settings.

## Create/Edit MQTT Client List

MQTT Client List							
		Add	Delete				
ID	Connection Name	Address	Authentication	Security	Port	Enable	Action
1	Broker01	1.2.3.4	<input type="checkbox"/>	None	1883	<input checked="" type="checkbox"/>	Subscriptions Received List <input type="checkbox"/> Select
							Edit

When the **Add** button is applied, a sequence of configuration screens will appear. They are **MQTT Client Configuration**, **MQTT Message Configuration**, **Publish Message List**, and **Subscribe Message List**. Additionally, there is a “**Subscriptions Received List**” button to access the subscribed & received message list. When the “**Subscriptions Received List**” button is applied, a message list will appear, and you can browse it page by page, download the messages to a file, or delete the messages.

# EW200 Industrial Cellular Gateway

## Define MQTT Client Configuration

MQTT Client Configuration	
Item	Setting
▶ Connection Name	<input type="text"/>
▶ Address	<input type="text"/>
▶ Port	<input type="text" value="1883"/> (1~65535)
▶ Authentication	<input type="checkbox"/>
▶ Security	<input type="text" value="None"/>
▶ Client ID	<input type="text" value="00501869E631"/>
▶ Keep Alive	<input type="text" value="60"/> (5~86400 sec)
▶ Enable	<input type="checkbox"/>

MQTT Client Configuration		
Item	Value setting	Description
<b>Connection Name</b>	Unchecked by default	Specify a name as the identifier of the MQTT Client. It can be identified with the Broker Name, or interested message (topic) Value Range: 1 ~ 64 characters.
<b>Address</b>	1. Required setting 2. Blank by default	Specify the host name or IP address of the MQTT broker that the client is going to publish message to it, or subscribe to messages from it.
<b>Port</b>	1. Optional setting 2. <b>1883</b> is set by default	Specify a port as the port for MQTT connection.  Value Range: 1 ~ 65535.
<b>Security</b>	1. Optional setting 2. <b>None</b> is set by default	Select the security scheme for the MQTT connection. <b>None</b> : no encryption is involved for the MQTT connection. <b>SSL/TLS</b> : SSL/TLS encryption is applied for security. You have to further specify required certificate files. Note: If <b>SSL/TLS</b> is selected, the listen port will be changed to <b>8883</b> accordingly by default.
<b>Certificate</b>	1. Optional setting 2. <b>None</b> is set by default	Select <b>CA File / CERT File / Key File</b> from the dropdown lists. If you don't have available items in the dropdown list, you have to define or create it first. Please refer to <b>Object Definition &gt; Certificate &gt; Trusted Certificate</b> . <b>CA File</b> can be defined in Trusted Certificate List. <b>CERT File</b> can be defined in Trusted Client Certificate List. <b>KEY File</b> can be defined in Trusted Client Key List.
<b>Client ID</b>	1. Required setting 2. ID with device MAC is set by default	Specify an unique ID for the MQTT client. By default the MAC address is used as the ID string.
<b>Authentication</b>	1. Optional setting 2. Unchecked by default	Check the box if user (account) authentication is required for subscribing to the MQTT messages. With the box checked, you have to further specify Username and Password for the connection.
<b>Username</b>	Required setting	Specify a name as the identifier of the MQTT client.

# EW200 Industrial Cellular Gateway

		Value Range: 1 ~ 32 characters.
<b>Password</b>	Required setting	Specify a password for the user account. Value Range: 1 ~ 32 characters.
<b>Keep Alive</b>	1. Optional setting 2. <b>60 sec</b> is set by default	Specify a keep alive interval to keep the connection alive while the connection is idle. Value Range: 5 ~ 86400 sec.
<b>Enable</b>	Unchecked by default	Check the box to activate this MQTT Client configuration
<b>Save</b>	N/A	Click the Save button to save the settings.

## Define MQTT Message

You can define the Last Will Message, and optional Topic Prefix for publishing / subscribing MQTT messages.

MQTT Message Configuration	
Item	Setting
▶ Last Will	<input checked="" type="checkbox"/> Enable
▶ Topic	<input type="text"/>
▶ Message	<input type="text"/>
▶ QoS	<input checked="" type="radio"/> 0 (At most once) <input type="radio"/> 1 (At least once) <input type="radio"/> 2 (Exactly once)
▶ Topic prefix (Optional)	<input type="text"/>

MQTT Message Configuration		
Item	Value setting	Description
<b>Enable</b>	Unchecked by default.	Check the box to activate this Last Will message configuration If the box is checked, you have to further specify Topic, Message, and QoS settings. When the MQTT broker detects that the MQTT client is disconnected, it will send the Last Will message to the interested MQTT subscribers.
<b>Topic</b>	1. Required setting 2. Blank by default	Specify the topic for the Last Will message. Value Range: 1 ~ 64 characters, including the topic level separator '/', but excluding the wildcards '+' and '#'. .
<b>Message</b>	1. Required setting 2. Blank by default	Specify the message content for the Last Will message. Value Range: 1 ~ 256 characters.
<b>QoS</b>	1. Optional setting 2. 0 (At most once) is set by default	Select the QoS type for the Last Will message. <b>0 (At most once):</b> the message will be published only once, and the broker and subscribed client(s) take no additional steps to acknowledge the delivery, no matter it is received or not. <b>1 (At least once):</b> the message will be published at least once until acknowledgement is received from the broker or subscribed client(s). <b>2 (Exactly once):</b> the message will be published to subscriber(s) once in a two-

# EW200 Industrial Cellular Gateway

		level handshake to ensure only one copy of the message is received.
<b>Topic Prefix (Optional)</b>	1. Optional setting 2. Blank by default	Specify the topic prefix for MQTT message. Value Range: 1 ~ 64 characters.
<b>Save</b>	N/A	Click the Save button to save the settings.
<b>Undo</b>	N/A	Click the Undo button to cancel the changes.
<b>Back</b>	N/A	Click the Back button to go back to previous configuration screen.

## Publish Message List

Publish Message List <button>Add</button> <span>Delete</span>				
ID	Topic	QoS	Enable	

Up to 64 published messages will be shown in the message list. When the **Add** button is applied, the **Publish Message Configuration** screen will appear.

Publish Message Configuration	
<div> <span>Save</span> <span>Undo</span> </div>	
Item	Setting
▶ Topic	<input type="text"/>
▶ Topics prefix	<input type="checkbox"/> Enable
▶ Message Style	Manual ▼
▶ Message	<div><div></div></div>
▶ QoS	<input checked="" type="radio"/> 0 (At most once) <input type="radio"/> 1 (At least once) <input type="radio"/> 2 (Exactly once)
▶ Retained	<input type="checkbox"/> Enable
▶ Publish Behavior	<input type="checkbox"/> Auto Publish
▶ Enable	<input type="checkbox"/>

Publish Message Configuration		
Item	Value setting	Description
<b>Topic</b>	1. Required setting 2. Blank by default	Specify the topic for the Last Will message. Value Range: 1 ~ 64 characters, including the topic level separator '/', but excluding the wildcards '+' and '#'. .
<b>Topic Prefix</b>	Unchecked by default	Check the box to add the predefined topic prefix into a MQTT message.
<b>Message Style</b>	1. Optional setting 2. <b>Manual</b> is selected by default	Select a message style from the dropdown list. The supported styles are: <b>Manual:</b> The message is created manually, and you can specify the message content below. <b>System Log:</b> The message to be published is the System log of the device. <b>Data Logging:</b> The message to be published is the Data Logging recorded in the designated storage



# EW200 Industrial Cellular Gateway

<b>Message</b>	1. Required setting 2. Blank by default	Specify the message content for the Last Will message. Value Range: 1 ~ 256 characters.
<b>QoS</b>	1. Optional setting 2. 0 (At most once) is set by default	Select the QoS type for publishing a message. <b>0 (At most once):</b> the message will be published only once, and the broker and subscribed client(s) take no additional steps to acknowledge the delivery, no matter it is received or not. <b>1 (At least once):</b> the message will be published at least once until acknowledgement is received from the broker or subscribed client(s). <b>2 (Exactly once):</b> the message will be published to subscriber(s) once in a two-level handshake to ensure only one copy of the message is received.
<b>Retained</b>	Unchecked by default	Check the box to activate this message retaining function.
<b>Publish Behavior</b>	Unchecked by default	Check the box(es) for the expected publish behavior: <b>Auto Publish:</b> auto publish a message with specified time interval (1~65535 sec).  <b>When the Message or Data variation more than <input type="checkbox"/> lines.:</b> publish a new message that varies from previous one for specified changes. Note: if Message style is set to Manual, only Auto Publish is available.
<b>Enable</b>	Unchecked by default	Check the box to activate this publish message configuration.
<b>Save</b>	N/A	Click the Save button to save the settings.
<b>Undo</b>	N/A	Click the Undo button to cancel the changes.
<b>Back</b>	N/A	Click the Back button to go back to previous configuration screen.

## Subscribe Message List

Subscribe Message List <input type="button" value="Add"/> <input type="button" value="Delete"/>			
ID	Topic	QoS	Enable

Up to 64 subscribed messages will be shown in the message list. When the **Add** button is applied, the **Subscribe Message Configuration** screen will appear.

Subscribe Message Configuration <input type="button" value="Save"/> <input type="button" value="Undo"/>	
Item	Setting
▶ Topic	<input type="text"/>
▶ Topics prefix	<input type="checkbox"/> Enable
▶ QoS	<input checked="" type="radio"/> 0 (At most once) <input type="radio"/> 1 (At least once) <input type="radio"/> 2 (Exactly once)
▶ Enable	<input type="checkbox"/>

Subscribe Message Configuration		
Item	Value setting	Description
<b>Topic</b>	1. Required setting 2. Blank by default	Specify the topic for the message to be subscribed. Value Range: 1 ~ 64 characters, including the topic level separator '/', but excluding the wildcards '+' and '#'. .
<b>Topic Prefix</b>	Unchecked by default	Check the box to enable the topic prefix for subscribed message.

## EW200 Industrial Cellular Gateway

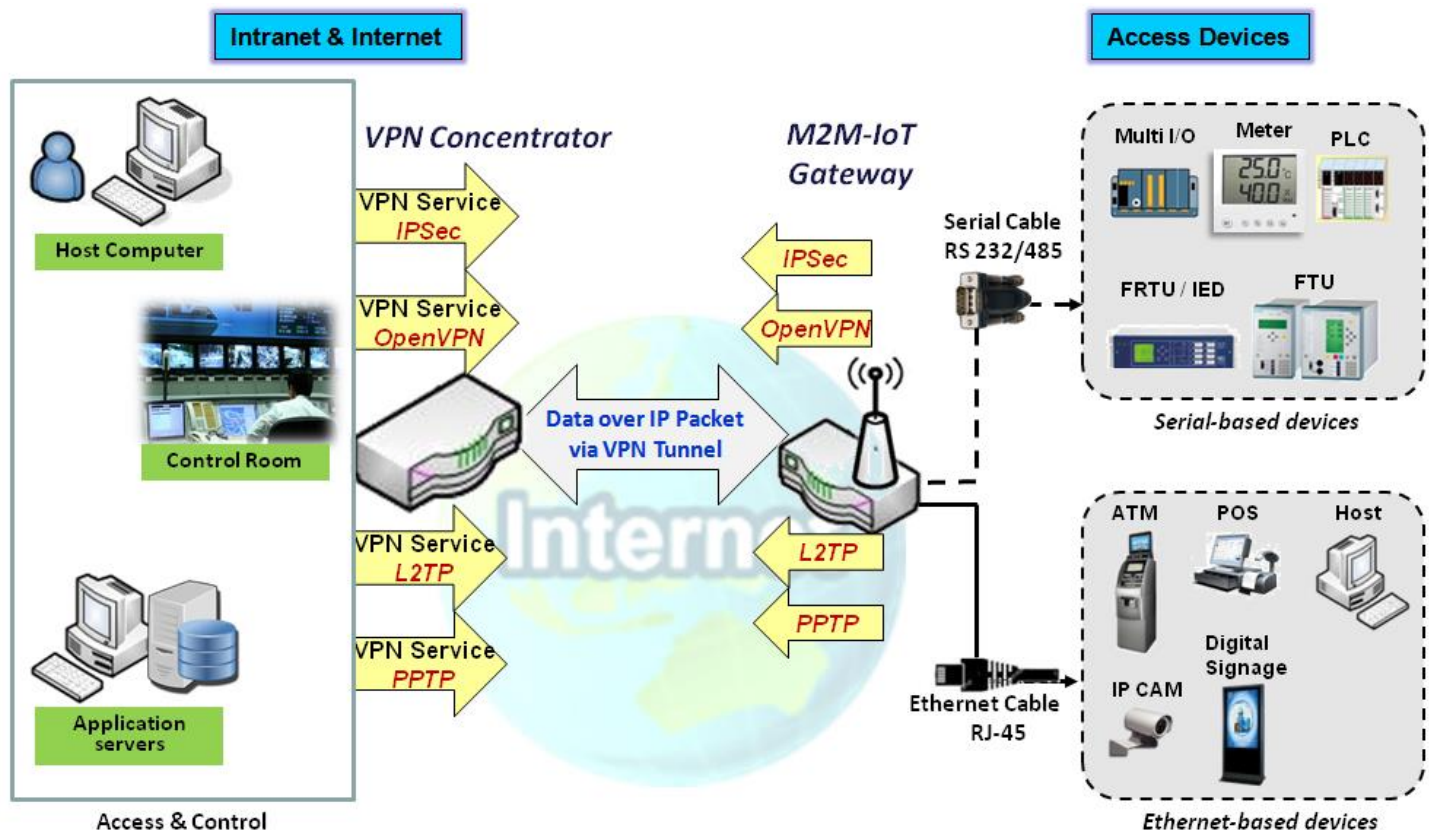
---

<b>QoS</b>	1. Optional setting 2. 0 (At most once) is set by default	Select the QoS type for subscribing to a message. <b>0 (At most once):</b> the message will be published only once, and the broker and subscribed client(s) take no additional steps to acknowledge the delivery, no matter it is received or not. <b>1 (At least once):</b> the message will be published at least once until acknowledgement is received from the broker or subscribed client(s). <b>2 (Exactly once):</b> the message will be published to subscriber(s) once in a two-level handshake to ensure only one copy of the message is received.
<b>Enable</b>	Unchecked by default	Check the box to activate this subscribe message configuration.
<b>Save</b>	N/A	Click the Save button to save the settings.
<b>Undo</b>	N/A	Click the Undo button to cancel the changes.
<b>Back</b>	N/A	Click the Back button to go back to previous configuration screen.

## 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. Additionally, some advanced functions, like Full Tunnel, Tunnel Failover, Tunnel Load Balance, NetBIOS over IPsec, NAT Traversal and Dynamic VPN, are also supported.

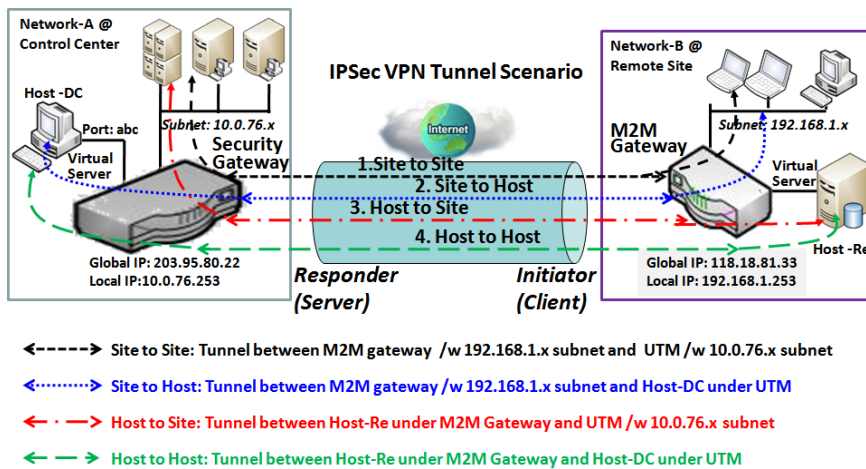
# EW200 Industrial Cellular Gateway

## 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 the initiator and the IPsec VPN server the responder. This gateway can be configured as different roles and establish a number of tunnels with various remote devices. Before going to set up the VPN connections, you may need to decide on the scenario type for the tunneling.

### IPsec Tunnel Scenarios



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

**Site to Site:** You need to set up remote gateway IP and subnet of both gateways. After the IPsec tunnel is established, hosts behind both gateways can communicate with each other through the tunnel.

**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:** For a single host (or mobile user) 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.

# EW200 Industrial Cellular Gateway

## IPsec Setting

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

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

### Enable IPsec

Configuration	
Item	Setting
▶ IPsec	<input type="checkbox"/> Enable
▶ Max. Concurrent IPsec Tunnels	16

Configuration Window		
Item	Value setting	Description
IPsec	Unchecked by default	Click the <b>Enable</b> box to enable IPsec function.
Max. Concurrent IPsec Tunnels	16 is set by default	The specified value will limit the maximum number of simultaneous IPsec tunnel connection.
Save	N/A	Click <b>Save</b> to save the settings
Undo	N/A	Click <b>Undo</b> 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.

IPsec Tunnel List							
		Add	Delete	Refresh			
ID	Tunnel Name	Interface	Remote Gateway	Remote Subnet	Status	Enable	Actions

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. Configure the tunnel details for both local and remote VPN devices.

Tunnel Configuration	
Item	Setting
▶ Tunnel	<input type="checkbox"/> Enable
▶ Tunnel Name	IPsec #1
▶ Interface	WAN1 ▼
▶ Tunnel Scenario	Site-to-Site(Tunnel mode) ▼
▶ Tunnel TCP MSS	Auto ▼ 0 (64~1500 Bytes)
▶ Encapsulation Protocol	ESP ▼
▶ IKE Version	v1 ▼

# EW200 Industrial Cellular Gateway

Tunnel Configuration Window		
Item	Value setting	Description
<b>Tunnel</b>	Unchecked by default	Check the <b>Enable</b> box to activate the IPsec tunnel
<b>Tunnel Name</b>	1. Required setting 2. String format, text	Enter a tunnel name. <b>Value Range:</b> 1 ~ 19 characters.
<b>Interface</b>	1. Required setting 2. <b>WAN 1</b> is selected by default	Select the interface on which IPsec tunnel is to be established. It can be any available WAN and LAN interface.
<b>Tunnel Scenario</b>	1. Required setting 2. <b>Site to site</b> is selected by default	Select an IPsec tunneling scenario from the dropdown box for your application. Select <b>Site-to-Site</b> , <b>Site-to-Host</b> , <b>Host-to-Site</b> , or <b>Host-to-Host</b> . If LAN interface is selected, only <b>Host-to-Host</b> scenario is available. With <b>Site-to-Site</b> or <b>Site-to-Host</b> or <b>Host-to-Site</b> , IPsec operates in tunnel mode. The difference is the number of subnets. With <b>Host-to-Host</b> , IPsec operates in transport mode.
<b>Tunnel TCP MSS</b>	1. An optional setting 2. <b>Auto</b> is set by default	Select from the dropdown box to define the size of Tunnel TCP MSS. Select <b>Auto</b> , and all devices will adjust this parameter automatically. Select <b>Manual</b> , and specify an expected value for Tunnel TCP MSS. Value Range: 64 ~ 1500 bytes.
<b>Encapsulation Protocol</b>	1. Required setting 2. <b>ESP</b> is selected by default	Select the Encapsulation Protocol from the dropdown box for this IPsec tunnel. Available encapsulations are <b>ESP</b> and <b>AH</b> .
<b>IKE Version</b>	1. Required setting 2. <b>v1</b> is selected by default	Specify the IKE version for this IPsec tunnel. Select v1 or v2.

Local & Remote Configuration				
Item	Setting			
▶ Local Subnet List	ID	Subnet IP Address	Subnet Mask	Actions
	1	<input type="text" value="192.168.66.0"/>	<input type="text" value="255.255.255.0(24)"/>	<input type="button" value="Delete"/>
	<input type="button" value="Add"/>			
▶ Remote Subnet List	ID	Subnet IP Address	Subnet Mask	Actions
	1	<input type="text"/>	<input type="text" value="255.255.255.0(24)"/>	<input type="button" value="Delete"/>
	<input type="button" value="Add"/>			
▶ Remote Gateway	<input type="text" value=""/> (IP Address/FQDN)			

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

# EW200 Industrial Cellular Gateway

<b>Remote Subnet List</b>	Required setting	Specify the Remote Subnet IP address and Subnet Mask. Click the Add or Delete button to add or delete Remote Subnet setting.
<b>Remote Gateway</b>	1. Required setting. 2. Format can be a ipv4 address or FQDN	Specify the Remote Gateway.

Authentication	
Item	Setting
▶ Key Management	IKE+Pre-shared Key ▼ <input type="text"/> (Min. 8 characters)
▶ Local ID	Type: User Name ▼ ID: <input type="text"/> (Optional)
▶ Remote ID	Type: User Name ▼ ID: <input type="text"/>

Authentication Configuration Window		
Item	Value setting	Description
<b>Key Management</b>	1. Required setting 2. Pre-shared Key 8 to 32 characters.	Select Key Management from the dropdown box for this IPsec tunnel. <b>IKE+Pre-shared Key:</b> user needs to set a key (8 ~ 32 characters). <b>IKE+X.509:</b> 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 <b>Object Definition &gt; Certificate</b> in web-based utility.
<b>Local ID</b>	Optional setting	Specify the Local ID for this IPsec tunnel to authenticate. Select <b>User Name</b> for Local ID and enter the username. The username may include but can't be all numbers. Select <b>FQDN</b> for Local ID and enter the FQDN. Select <b>User@FQDN</b> for Local ID and enter the User@FQDN. Select <b>Key ID</b> for Local ID and enter the Key ID (English letter or number).
<b>Remote ID</b>	Optional setting	Specify the Remote ID for this IPsec tunnel to authenticate. Select <b>User Name</b> for Remote ID and enter the username. The username may include but can't be all numbers. Select <b>FQDN</b> for Local ID and enter the FQDN. Select <b>User@FQDN</b> for Remote ID and enter the User@FQDN. Select <b>Key ID</b> for Remote ID and enter the Key ID (English letter or number). Note: Remote ID will be not available when Dynamic VPN option in Tunnel Scenario is selected.

IKE Phase	
Item	Setting
▶ Negotiation Mode	Main Mode ▼
▶ X-Auth	None ▼ X-Auth Account (Optional) User Name : <input type="text"/> Password : <input type="password"/>
▶ Dead Peer Detection (DPD)	<input checked="" type="checkbox"/> Enable Timeout : <input type="text"/> 180 (seconds) Delay : <input type="text"/> 30 (seconds)
▶ Phase1 Key Life Time	<input type="text"/> 3600 (seconds) (Max. 86400)

## IKE Phase Window

# EW200 Industrial Cellular Gateway

Item	Value setting	Description
<b>Negotiation Mode</b>	Main Mode is set by default	Specify the Negotiation Mode for this IPsec tunnel. Select Main Mode or Aggressive Mode.
<b>X-Auth</b>	None is selected by default	Specify the X-Auth role for this IPsec tunnel. Select Server, Client, or None. Selected Server for this gateway will be an X-Auth server. Click on the X-Auth Account button to create a remote X-Auth client account. Selected Client for 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.
<b>Dead Peer Detection (DPD)</b>	1. Checked by default 2. Default Timeout 180s and Delay 30s	Click <b>Enable</b> box to enable DPD function. Specify the <b>Timeout</b> and <b>Delay</b> time in seconds. <b>Value Range:</b> 0 ~ 999 seconds for <b>Timeout</b> and <b>Delay</b> .
<b>Phase1 Key Life Time</b>	1. Required setting 2. Default 3600s 3. Max. 86400s	Specify the Phase1 Key Life Time. <b>Value Range:</b> 30 ~ 86400.

IKE Proposal Definition				
ID	Encryption	Authentication	DH Group	Definition
1	AES-auto ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
2	AES-auto ▼	MD5 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
3	DES ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
4	3DES ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable

IKE Proposal Definition Window		
Item	Value setting	Description
<b>IKE Proposal Definition</b>	Required setting	Specify the Phase 1 Encryption method. It can be DES / 3DES / AES-auto / AES-128 / AES-192 / AES-256. Specify the Authentication method. It can be None / MD5 / SHA1 / SHA2-256. Specify the DH Group. It can be None / Group1 / Group2 / Group5 / Group14 / Group15 / Group16 / Group17 / Group18. Check the <b>Enable</b> box to enable this setting.

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



# EW200 Industrial Cellular Gateway

IPsec Phase Window		
Item	Value setting	Description
<b>Phase2 Key Life Time</b>	1. Required setting 2. 28800s is default 3. Max. 86400s	Specify the Phase2 Key Life Time in seconds. <b><u>Value Range:</u></b> 30 ~ 86400.

IPSec Proposal Definition				
ID	Encryption	Authentication	PFS Group	Definition
1	AES-auto ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
2	AES-auto ▼	MD5 ▼		<input checked="" type="checkbox"/> Enable
3	DES ▼	SHA1 ▼		<input checked="" type="checkbox"/> Enable
4	3DES ▼	SHA1 ▼		<input checked="" type="checkbox"/> Enable

IPsec Proposal Definition Window		
Item	Value setting	Description
<b>IPsec Proposal Definition</b>	Required setting	Specify the Encryption method. It can be None / DES / 3DES / AES-auto / AES-128 / AES-192 / AES-256. Note: None is available only when Encapsulation Protocol is set as <b>AH</b> ; it is not available for <b>ESP</b> Encapsulation. Specify the Authentication method. It can be None / MD5 / SHA1 / SHA2-256. Note: None and SHA2-256 are available only when Encapsulation Protocol is set as <b>ESP</b> ; they are not available for <b>AH</b> Encapsulation. Specify the PFS Group. It can be None / Group1 / Group2 / Group5 / Group14 / Group15 / Group16 / Group17 / Group18. Click <b>Enable</b> to enable this setting.
<b>Save</b>	N/A	Click <b>Save</b> to save the settings
<b>Undo</b>	N/A	Click <b>Undo</b> to cancel the settings
<b>Back</b>	N/A	Click <b>Back</b> to return to the previous page.

## Create/Edit Dynamic VPN Server List

Dynamic VPN List	Add	Delete	Refresh	<input type="button" value="↑"/> <input type="button" value="×"/>
------------------	-----	--------	---------	---

Similar to creating an IPsec VPN Tunnel for site/host to site/host scenario, when the **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. Configure the tunnel details for the gateway as a Dynamic VPN server.

Note: You can configure one Dynamic VPN server for each WAN interface.

# EW200 Industrial Cellular Gateway

Tunnel Configuration	
Item	Setting
▶ Tunnel	<input type="checkbox"/> Enable
▶ Tunnel Name	Dynamic IPsec1
▶ Interface	WAN1 ▼
▶ Tunnel Scenario	Tunnel Mode ▼
▶ Encapsulation Protocol	ESP ▼
▶ IKE Version	v1 ▼

Tunnel Configuration Window		
Item	Value setting	Description
<b>Tunnel</b>	Unchecked by default	Check the <b>Enable</b> box to activate the Dynamic IPsec VPN tunnel.
<b>Tunnel Name</b>	1. Required setting 2. String format, any text	Enter a tunnel name. <b><u>Value Range:</u></b> 1 ~ 19 characters.
<b>Interface</b>	1. Required setting 2. <b>WAN 1</b> is selected by default	Select the WAN interface on which IPsec tunnel is to be established.
<b>Tunnel Scenario</b>	1. Required setting 2. Dynamic VPN is selected by default	The IPsec tunneling scenario is fixed to Dynamic VPN.
<b>Encapsulation Protocol</b>	1. Required setting 2. <b>ESP</b> is selected by default	Select the Encapsulation Protocol from the dropdown box for this IPsec tunnel. Available encapsulations are <b>ESP</b> and <b>AH</b> .
<b>IKE Version</b>	1. Required setting 2. <b>v1</b> is selected by default	Specify the IKE version for this IPsec tunnel.

Local & Remote Configuration	
Item	Setting
▶ Local Subnet	192.168.66.0
▶ Local Netmask	255.255.255.0/(24) ▼

Local & Remote Configuration Window		
Item	Value setting	Description
<b>Local Subnet</b>	Required setting	Specify the Local Subnet IP address.
<b>Local Netmask</b>	Required setting	Specify the Local Subnet Mask.

Authentication	
Item	Setting
▶ Key Management	IKE+Pre-shared Key ▼ <input type="text"/> (Min. 8 characters)
▶ Local ID	Type: User Name ▼ ID: <input type="text"/> (Optional)
▶ Remote ID	Type: User Name ▼ ID: <input type="text"/>

Authentication Configuration Window		
Item	Value setting	Description
<b>Key Management</b>	1. Required setting	Select Key Management from the dropdown box for this IPsec tunnel.

## EW200 Industrial Cellular Gateway

	2. Pre-shared Key 8 to 32 characters.	<b>IKE+Pre-shared Key:</b> Set a key (8 ~ 32 characters).
<b>Local ID</b>	Optional setting	<p>Specify the Local ID for this IPsec tunnel to authenticate.</p> <p>Select <b>User Name</b> for Local ID and enter the username. The username may include but can't be all numbers.</p> <p>Select <b>FQDN</b> for Local ID and enter the FQDN.</p> <p>Select <b>User@FQDN</b> for Local ID and enter the User@FQDN.</p> <p>Select <b>Key ID</b> for Local ID and enter the Key ID (letter or number).</p>
<b>Remote ID</b>	Optional setting	<p>Specify the Remote ID for this IPsec tunnel to authenticate.</p> <p>Select <b>User Name</b> for Remote ID and enter the username. The username may include but can't be all numbers.</p> <p>Select <b>FQDN</b> for Local ID and enter the FQDN.</p> <p>Select <b>User@FQDN</b> for Remote ID and enter the User@FQDN.</p> <p>Select <b>Key ID</b> for Remote ID and enter the Key ID (letter or number).</p> <p>Note: Remote ID will be not available when Dynamic VPN option in Tunnel Scenario is selected.</p>

For the remaining 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 descriptions.

# EW200 Industrial Cellular Gateway

## 5.1.2 OpenVPN

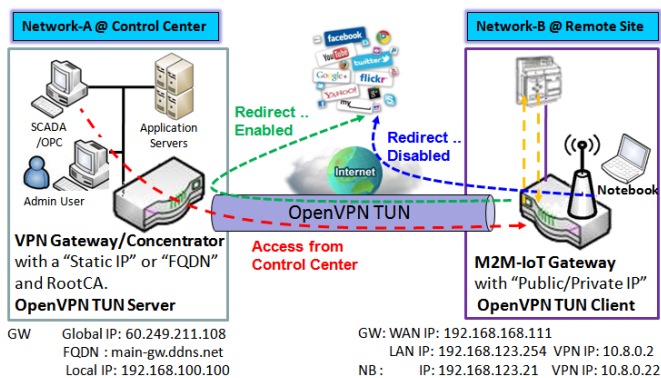
OpenVPN is an application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable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

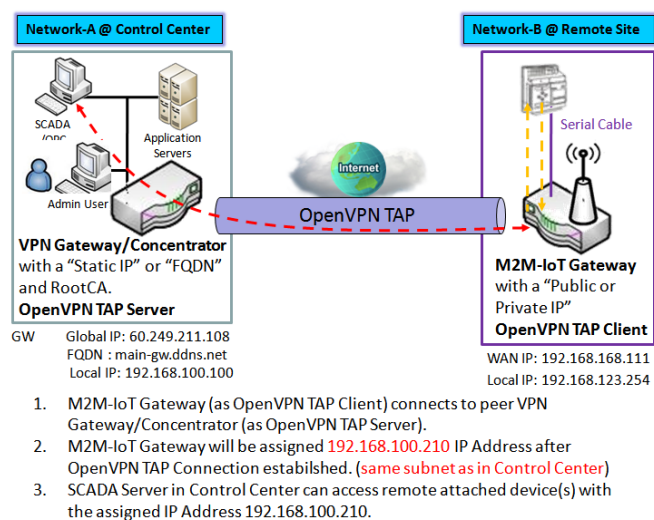
If you want to offer remote access to a VPN server from client(s), and inhibit the access to remote LAN resources under VPN server, OpenVPN TUN mode is the simplest solution.

As shown in the diagram, the M2M-IoT Gateway is configured as an OpenVPN TUN Client, and connects to an 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 belongs to a virtual subnet that is different to the local subnet in Control

# EW200 Industrial Cellular Gateway

Center. With such a 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; 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



The term "TAP" refers 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 resources on the LAN. To offer remote access to the entire remote LAN for VPN client(s), set up 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 on the same subnet as that of local subnet in Control Center. With this

connection, the SCADA Server in Control Center can access remote attached serial device(s) with the virtual IP address (192.168.100.210).

## 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	<input checked="" type="checkbox"/> Enable
Server / Client	Server ▼



# EW200 Industrial Cellular Gateway


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

## As an OpenVPN Server

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

The OpenVPN Server supports up to 4 TUN / TAP tunnels at the same time.

 Configuration 

Item	Setting
▶ OpenVPN	<input checked="" type="checkbox"/> Enable
▶ Server / Client	Server ▼
▶ OpenVPN Configuration file	<input type="checkbox"/> Enable  client.ovpn

OpenVPN Server Configuration		
Item	Value setting	Description
<b>OpenVPN Configuration File</b>	1. Optional setting 2. Unchecked by default	Click the <b>Enable</b> box to activate the export feature of OpenVPN Client configuration to a .ovpn file. You have to further click the Export button to get the configuration file.

The OpenVPN Server supports up to 4 TUN / TAP tunnels at the same time.

# EW200 Industrial Cellular Gateway

OpenVPN Server Configuration

Item	Setting
OpenVPN Server	<input type="checkbox"/> Enable
Protocol	TCP ▼
Port	4430
Tunnel Scenario	TUN ▼
Authorization Mode	TLS ▼ CA Cert.: IDG761AM-JH.crt ▼    Server Cert.: LocalCert1 ▼
Server Virtual IP	10.8.0.0
DHCP-Proxy Mode	<input checked="" type="checkbox"/> Enable
IP Pool	Starting Address: ~ Ending Address:
Gateway	
Netmask	255.255.255.0(/24) ▼
Redirect Default Gateway	<input type="checkbox"/> Enable
Encryption Cipher	Blowfish ▼
Hash Algorithm	SHA-1 ▼
LZO Compression	Adaptive ▼
Persist Key	<input checked="" type="checkbox"/> Enable
Persist Tun	<input checked="" type="checkbox"/> Enable
Advanced Configuration	Edit

OpenVPN Server Configuration		
Item	Value setting	Description
<b>OpenVPN Server</b>	Unchecked by default	Click the <b>Enable</b> to activate OpenVPN Server functions.
<b>Protocol</b>	1. Required setting 2. By default <b>TCP</b> is selected.	Define the selected <b>Protocol</b> for connecting to the OpenVPN Server. <ul style="list-style-type: none"> <li>• Select <b>TCP , or UDP</b> -&gt; TCP will be used to access the OpenVPN Server, and <b>Port</b> will be set to 4430.</li> <li>• Select <b>UDP</b> -&gt; UDP will be used to access the OpenVPN Server, and <b>Port</b> will be set to 1194.</li> </ul>
<b>Port</b>	1. Required setting 2. By default <b>4430</b> is set.	Specify the <b>Port</b> for connecting to the OpenVPN Server. <b>Value Range: 1 ~ 65535.</b>
<b>Tunnel Scenario</b>	1. Required setting 2. By default <b>TUN</b> is selected.	Specify the type of <b>Tunnel Scenario</b> for connecting to the OpenVPN Server. It can be <b>TUN</b> for TUN tunnel scenario, or <b>TAP</b> for TAP tunnel scenario.
<b>Authorization Mode</b>	1. Required setting 2. By default <b>TLS</b> is selected.	Specify the authorization mode for the OpenVPN Server. <ul style="list-style-type: none"> <li>• <b>TLS</b> -&gt; OpenVPN will use TLS authorization mode, and the following items <b>CA Cert.</b>, <b>Server Cert.</b> and <b>DH PEM</b> will be displayed. <b>CA Cert.</b> can be generated in Certificate. Refer to <b>Object Definition &gt;</b></li> </ul>

# EW200 Industrial Cellular Gateway

		<p><b>Certificate &gt; Trusted Certificate.</b>  <b>Server Cert.</b> can be generated in Certificate. Refer to <b>Object Definition &gt; Certificate &gt; My Certificate.</b></p> <ul style="list-style-type: none"> <li>• <b>Static Key</b>  -&gt;The OpenVPN will use static key (pre-shared) authorization mode, and the following items <b>Local Endpoint IP Address</b>, <b>Remote Endpoint IP Address</b> and <b>Static Key</b> will be displayed.  Note: Static Key will be available only when TUN is chosen in Tunnel Scenario.</li> </ul>
<b>Local Endpoint IP Address</b>	Required setting	Specify the virtual <b>Local Endpoint IP Address</b> of this OpenVPN gateway. <b>Value Range:</b> 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.
<b>Remote Endpoint IP Address</b>	Required setting	Specify the virtual <b>Remote Endpoint IP Address</b> of the peer OpenVPN gateway. <b>Value Range:</b> 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.
<b>Static Key</b>	Required setting	Specify the <b>Static Key</b> . Note: Static Key will be available only when Static Key is chosen in Authorization Mode.
<b>Server Virtual IP</b>	Required setting	Specify the <b>Server Virtual IP</b> . <b>Value Range:</b> 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.
<b>DHCP-Proxy Mode</b>	1. Required setting 2. The box is checked by default.	Check the <b>Enable</b> box to activate the <b>DHCP-Proxy Mode</b> . Note: DHCP-Proxy Mode will be available only when TAP is chosen in Tunnel Device.
<b>IP Pool</b>	Required setting	Specify the virtual <b>IP pool</b> setting for the OpenVPN server. Specify the <b>Starting Address</b> and <b>Ending Address</b> 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).
<b>Gateway</b>	Required setting	Specify the <b>Gateway</b> setting for the OpenVPN server. It will be assigned to the connected OpenVPN clients. Note: Gateway will be available only when TAP is chosen in Tunnel Device, and DHCP-Proxy Mode is unchecked (disabled).
<b>Netmask</b>	By default - <b>select one</b> - is selected.	Specify the <b>Netmask</b> setting for the OpenVPN server. It will be assigned to the connected OpenVPN clients. <b>Value Range:</b> 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.
<b>Redirect Default Gateway</b>	1. Optional setting. 2. Unchecked by default	Check the <b>Enable</b> box to activate the <b>Redirect Default Gateway</b> function.
<b>Encryption Cipher</b>	1. Required setting. 2. By default <b>Blowfish</b> is selected.	Specify the <b>Encryption Cipher</b> from the dropdown list. Select from <b>Blowfish/AES-256/AES-192/AES-128/None</b> .
<b>Hash Algorithm</b>	By default <b>SHA-1</b> is selected.	Specify the <b>Hash Algorithm</b> from the dropdown list. Select from <b>SHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable</b> .
<b>LZO Compression</b>	By default <b>Adaptive</b> is selected.	Specify the <b>LZO Compression</b> scheme. Select from <b>Adaptive/YES/NO/Default</b> .
<b>Persis Key</b>	1. Optional setting.	Check the <b>Enable</b> box to activate the <b>Persis Key</b> function.



## EW200 Industrial Cellular Gateway

---

	2. The box is checked by default.	
<b>Persis Tun</b>	1. Optional setting. 2. The box is checked by default.	Check the <b>Enable</b> box to activate the <b>Persis Tun</b> function.
<b>Advanced Configuration</b>	N/A	Click the <b>Edit</b> button to specify the <b>Advanced Configuration</b> setting for the OpenVPN server. If the button is clicked, <b>Advanced Configuration</b> will be displayed below.
<b>Save</b>	N/A	Click <b>Save</b> to save the settings.
<b>Undo</b>	N/A	Click <b>Undo</b> to cancel the changes.

# EW200 Industrial Cellular Gateway

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

OpenVPN Server Advanced Configuration	
Item	Setting
▶ TLS Cipher	TLS-RSA-WITH-AES128-SHA ▼
▶ TLS Auth. Key	<div></div> (Optional)
▶ Client to Client	<input checked="" type="checkbox"/> Enable
▶ Duplicate CN	<input checked="" type="checkbox"/> Enable
▶ Tunnel MTU	1500
▶ Tunnel UDP Fragment	1500
▶ Tunnel UDP MSS-Fix	<input type="checkbox"/> Enable
▶ CCD-Dir Default File	<div></div>
▶ Client Connection Script	<div></div>
▶ Additional Configuration	<div></div>

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

## EW200 Industrial Cellular Gateway

---

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

# EW200 Industrial Cellular Gateway

## As an OpenVPN Client

If **Client** is selected, the configuration screen will be changed as below and an OpenVPN Client List screen appear.

Configuration	
Item	Setting
OpenVPN	<input checked="" type="checkbox"/> Enable
Server / Client	Client ▾
OpenVPN Configuration file	<input type="checkbox"/> Enable <input type="button" value="Upgrade"/>

OpenVPN Client Configuration		
Item	Value setting	Description
OpenVPN	Unchecked by default	Check the <b>Enable</b> box to activate the OpenVPN function.
Server / Client	Server Configuration is selected by default.	When <b>Server</b> is selected, as the name indicated, server configuration will be displayed below for further setup. When <b>Client</b> is selected, you can specify the client settings in another client configuration window.
OpenVPN Configuration file	1. Optional setting 2. Unchecked by default	Click the <b>Enable</b> box to activate the OpenVPN Client configuration via a pre-defined configuration file. You have to further click the <b>Upgrade</b> button to upload the configuration from an .ovpn file. If you enabled this function, you can't add any OpenVPN clients manually.

OpenVPN Client List														
Add Delete														
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

When the **Add** button is applied, the **OpenVPN Client Configuration** screen will appear. OpenVPN Client Configuration window lets 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.

# EW200 Industrial Cellular Gateway

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	<input type="checkbox"/> Enable
▶ NAT	<input type="checkbox"/> 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	<input checked="" type="checkbox"/> Enable
▶ Persist Tun	<input checked="" type="checkbox"/> Enable
▶ Advanced Configuration	Edit
▶ Tunnel	<input type="checkbox"/> Enable

OpenVPN Client Configuration		
Item	Value setting	Description
<b>OpenVPN Client Name</b>	Required setting	The <b>OpenVPN Client Name</b> will be used to identify the client in the tunnel list. <b>Value Range:</b> 1 ~ 32 characters.
<b>Interface</b>	1. Required setting 2. By default <b>WAN-1</b> is selected.	Define the physical interface to be used for this OpenVPN Client tunnel.
<b>Protocol</b>	1. Required setting 2. By default <b>TCP</b> is selected.	Define the <b>Protocol</b> for the OpenVPN Client. <ul style="list-style-type: none"> <li>Select <b>TCP</b> -&gt; OpenVPN will use TCP, and <b>Port</b> will be set to 443.</li> <li>Select <b>UDP</b> -&gt; OpenVPN will use UDP, and <b>Port</b> will be set to 1194.</li> </ul>
<b>Port</b>	1. Required setting 2. By default <b>443</b> is set.	Specify the <b>Port</b> for the OpenVPN Client to use. <b>Value Range:</b> 1 ~ 65535.
<b>Tunnel Scenario</b>	1. Required setting 2. By default <b>TUN</b> is	Specify the type of <b>Tunnel Scenario</b> for the OpenVPN Client to use. It can be <b>TUN</b> for TUN tunnel scenario, or <b>TAP</b> for TAP tunnel scenario.

# EW200 Industrial Cellular Gateway

	selected.	
<b>Remote IP/FQDN</b>	Required setting	Specify the <b>Remote IP/FQDN</b> of the peer OpenVPN Server for this OpenVPN Client tunnel. Enter the IP address or FQDN.
<b>Remote Subnet</b>	Required setting	Specify <b>Remote Subnet</b> of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the remote subnet address and remote subnet mask.
<b>Redirect Internet Traffic</b>	1. Optional setting. 2. Unchecked by default	Check the <b>Enable</b> box to activate the <b>Redirect Internet Traffic</b> function.
<b>NAT</b>	1. Optional setting. 2. Unchecked by default	Check the <b>Enable</b> box to activate the <b>NAT</b> function.
<b>Authorization Mode</b>	1. Required setting 2. By default <b>TLS</b> is selected.	Specify the authorization mode for the OpenVPN Server. <ul style="list-style-type: none"> <li>• <b>TLS</b> -&gt;The OpenVPN will use TLS authorization mode, and the following items <b>CA Cert.</b>, <b>Client Cert.</b> and <b>Client Key</b> will be displayed. <b>CA Cert.</b> can be selected in Trusted CA Certificate List. Refer to <b>Object Definition &gt; Certificate &gt; Trusted Certificate</b>. <b>Client Cert.</b> can be selected in Local Certificate List. Refer to <b>Object Definition &gt; Certificate &gt; My Certificate</b>. <b>Client Key</b> can be selected in Trusted Client key List. Refer to <b>Object Definition &gt; Certificate &gt; Trusted Certificate</b>.</li> <li>• <b>Static Key</b> -&gt; OpenVPN will use static key authorization mode, and the following items <b>Local Endpoint IP Address</b>, <b>Remote Endpoint IP Address</b> and <b>Static Key</b> will be displayed.</li> </ul>
<b>Local Endpoint IP Address</b>	Required setting	Specify the virtual <b>Local Endpoint IP Address</b> of this OpenVPN gateway. <b>Value Range:</b> 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.
<b>Remote Endpoint IP Address</b>	Required setting	Specify the virtual <b>Remote Endpoint IP Address</b> of the peer OpenVPN gateway. <b>Value Range:</b> 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.
<b>Static Key</b>	Required setting	Specify the <b>Static Key</b> . Note: Static Key will be available only when Static Key is chosen in Authorization Mode.
<b>Encryption Cipher</b>	By default <b>Blowfish</b> is selected.	Specify the <b>Encryption Cipher</b> . Select from <b>Blowfish/AES-256/AES-192/AES-128/None</b> .
<b>Hash Algorithm</b>	By default <b>SHA-1</b> is selected.	Specify the <b>Hash Algorithm</b> . Select from <b>SHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable</b> .
<b>LZO Compression</b>	By default <b>Adaptive</b> is selected.	Specify the <b>LZO Compression</b> scheme. Select from <b>Adaptive/YES/NO/Default</b> .
<b>Persis Key</b>	1. Optional setting. 2. The box is checked by default.	Check the <b>Enable</b> box to activate the <b>Persis Key</b> function.
<b>Persis Tun</b>	1. Optional setting. 2. Box is checked by default.	Check the <b>Enable</b> box to activate the <b>Persis Tun</b> function.
<b>Advanced Configuration</b>	N/A	Click the <b>Edit</b> button to specify the <b>Advanced Configuration</b> setting for the OpenVPN server.

## EW200 Industrial Cellular Gateway

---

		If the button is clicked, <b>Advanced Configuration</b> will be displayed below.
<b>Tunnel</b>	Unchecked by default	Check the <b>Enable</b> box to activate this OpenVPN tunnel.
<b>Save</b>	N/A	Click <b>Save</b> to save the settings.
<b>Undo</b>	N/A	Click <b>Undo</b> to cancel the changes.
<b>Back</b>	N/A	Click <b>Back</b> to return to last page.

# EW200 Industrial Cellular Gateway

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

OpenVPN Client Advanced Configuration	
Item	Setting
▶ TLS Cipher	None ▼
▶ TLS Auth. Key(Optional)	<input type="text"/> (Optional)
▶ User Name(Optional)	<input type="text"/> (Optional)
▶ Password(Optional)	<input type="text"/> (Optional)
▶ Bridge TAP to	VLAN 1 ▼
▶ Firewall Protection	<input type="checkbox"/> Enable
▶ Client IP Address	Dynamic IP ▼
▶ Tunnel MTU	1500
▶ Tunnel UDP Fragment	1500
▶ Tunnel UDP MSS-Fix	<input type="checkbox"/> Enable
▶ nsCertType Verification	<input type="checkbox"/> Enable
▶ TLS Renegotiation Time(seconds)	3600 (seconds)
▶ Connection Retry(seconds)	-1 (seconds)
▶ DNS	Automatically ▼
▶ Additional Configuration	<input type="text"/>

OpenVPN Advanced Client Configuration		
Item	Value setting	Description
<b>TLS Cipher</b>	1. Required setting. 2. <b>TLS-RSA-WITH-AES128-SHA</b> is selected by default	Specify the <b>TLS Cipher</b> from the dropdown list. Select from <b>None / TLS-RSA-WITH-RC4-MD5 / TLS-RSA-WITH-AES128-SHA / TLS-RSA-WITH-AES256-SHA / TLS-DHE-DSS-AES128-SHA / TLS-DHE-DSS-AES256-SHA</b> . Note: TLS Cipher will be available only when TLS is chosen in Authorization Mode.
<b>TLS Auth. Key</b>	1. Optional setting. 2. String format: any text	Specify the <b>TLS Auth. Key</b> for connecting to an OpenVPN server, if the server requires it. Note: TLS Auth. Key will be available only when TLS is chosen in Authorization Mode.
<b>User Name</b>	Optional setting.	Enter the <b>User account</b> for connecting to an OpenVPN server, if the server requires it. Note: User Name will be available only when TLS is chosen in Authorization Mode.
<b>Password</b>	Optional setting.	Enter the <b>Password</b> for connecting to an OpenVPN server, if the server requires it. Note: User Name will be available only when TLS is chosen in Authorization Mode.
<b>Bridge TAP to</b>	By default <b>VLAN 1</b> is selected	Specify the setting of “ <b>Bridge TAP to</b> ” to bridge the TAP interface to a certain local network interface or VLAN. Note: <b>Bridge TAP to</b> will be available only when TAP is chosen in Tunnel Scenario and NAT is unchecked.
<b>Firewall Protection</b>	Unchecked by default	Check the box to activate the <b>Firewall Protection</b> function. Note: Firewall Protection will be available only when NAT is enabled.



# EW200 Industrial Cellular Gateway

<b>Client IP Address</b>	By default <b>Dynamic IP</b> is selected	Specify the virtual IP Address for the OpenVPN Client. Select from <b>Dynamic IP/Static IP</b> .
<b>Tunnel MTU</b>	1. Required setting 2. Default is 1500	Specify the value of <b>Tunnel MTU</b> . <b>Value Range: 0 ~ 1500.</b>
<b>Tunnel UDP Fragment</b>	The value is 1500 by default	Specify the value of <b>Tunnel UDP Fragment</b> . <b>Value Range: 0 ~ 1500.</b> Note: Tunnel UDP Fragment will be available only when UDP is chosen in Protocol.
<b>Tunnel UDP MSS-Fix</b>	Unchecked by default	Check the <b>Enable</b> box to activate the <b>Tunnel UDP MSS-Fix</b> function. Note: Tunnel UDP MSS-Fix will be available only when UDP is chosen in Protocol.
<b>nsCerType Verification</b>	Unchecked by default	Check the <b>Enable</b> box to activate the <b>nsCerType Verification</b> function. Note: nsCerType Verification will be available only when TLS is chosen in Authorization Mode.
<b>TLS Renegotiation Time (seconds)</b>	The value is 3600 by default	Specify the time interval of <b>TLS Renegotiation Time</b> . <b>Value Range: -1 ~ 86400.</b>
<b>Connection Retry(seconds)</b>	The value is -1 by default	Specify the time interval of <b>Connection Retry</b> . The default -1 means that there is no need to execute connection retry. <b>Value Range: -1 ~ 86400, and -1 means no retry is required.</b>
<b>DNS</b>	By default <b>Automatically</b> is selected	Specify the setting of <b>DNS</b> . Select from <b>Automatically/Manually</b> .
<b>Additional Configuration</b>	Optional setting	Enter optional configuration string here. Up to 256 characters is allowable. Value Range: 0 ~ 256characters.
<b>Save</b>	N/A	Click <b>Save</b> to save the settings.
<b>Undo</b>	N/A	Click <b>X</b> to cancel the changes and return to last page.

# EW200 Industrial Cellular Gateway

## 5.1.3 L2TP

Configuration

Item	Setting
L2TP	<input type="checkbox"/> Enable
Client/Server	Server ▾

L2TP Server Configuration

Item	Setting
L2TP Server	<input type="checkbox"/> Enable
Interface	All WANs ▾
L2TP over IPsec	<input type="checkbox"/> Enable Preshared Key <input type="text"/> (Min. 8 characters)
Server Virtual IP	192.168.10.1
IP Pool Starting Address	10
IP Pool Ending Address	17
Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
MPPE Encryption	<input type="checkbox"/> Enable 40 bits ▾
Service Port	1701

L2TP Server Status

Refresh

User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

User Account List

AddDelete

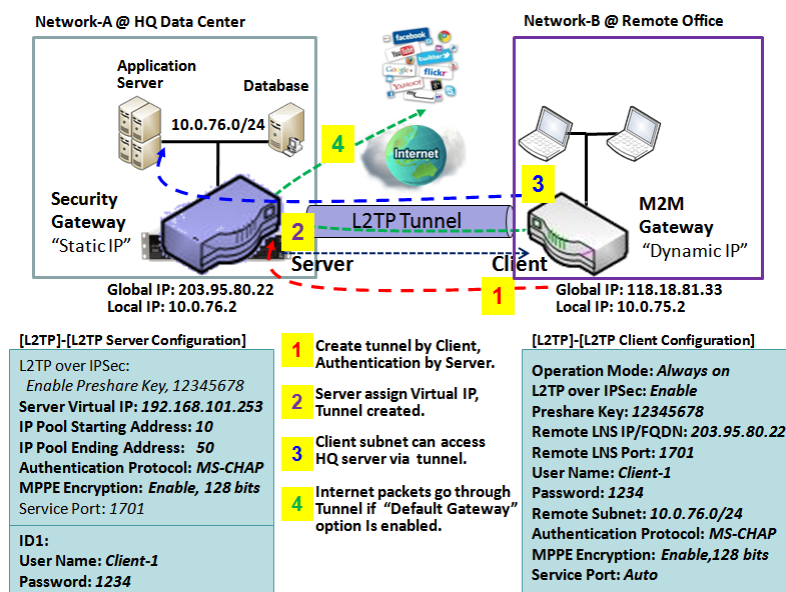
ID	User Name	Password	Enable	Actions
----	-----------	----------	--------	---------

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 an L2TP server and an 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 set up a tunnel, add “user name”, “password” and server’s global IP. In addition, identify the operation mode for each tunnel as main connection, failover for another tunnel, or load balance tunnel to increase overall bandwidth. Select “Default Gateway” or “Remote Subnet” for packet flow. You can also define what kind of traffic will pass through the L2TP tunnel in the “Default Gateway / Remote Subnet” parameter.

# EW200 Industrial Cellular Gateway



For the L2TP client peer, a Remote Subnet item is required for the Intranet of L2TP server peer. At L2TP client peer, the packets whose destination is in the dedicated subnet will be transferred via the L2TP tunnel. Others will be transferred based on current routing policy of the gateway at L2TP client peer. But, if 0.0.0.0/0 is entered in the Remote Subnet field, it will be treated as a "Default Gateway" setting for the L2TP client peer, and all packets, including the Internet accessing of L2TP client peer, will go through the established L2TP tunnel. That means the remote L2TP server peer controls the flow of any packets from the L2TP client peer. Those packets come through the L2TP tunnel.

# EW200 Industrial Cellular Gateway

## L2TP Setting

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

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

### Enable L2TP

Configuration [ Help ]	
Item	Setting
▶ L2TP	<input type="checkbox"/> Enable
▶ Client/Server	Server ▼

#### Enable L2TP Window

Item	Value setting	Description
<b>L2TP</b>	Unchecked by default	Click the <b>Enable</b> box to activate L2TP function.
<b>Client/Server</b>	Required setting	Specify the role of L2TP. Select <b>Server</b> or <b>Client</b> role for the gateway to take. Below are the configuration windows for L2TP Server and for Client.
<b>Save</b>	N/A	Click <b>Save</b> button to save the settings

### As a L2TP Server

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

L2TP Server Configuration	
Item	Setting
▶ L2TP Server	<input type="checkbox"/> Enable
▶ Interface	WAN1 ▼
▶ L2TP over IPsec	<input type="checkbox"/> Enable Preshared Key 1234567890 (Min. 8 characters)
▶ Server Virtual IP	192.168.13.1
▶ IP Pool Starting Address	10
▶ IP Pool Ending Address	17
▶ Authentication Protocol	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
▶ MPPE Encryption	<input type="checkbox"/> Enable 40 bits ▼
▶ Service Port	1701

# EW200 Industrial Cellular Gateway

L2TP Server Configuration		
Item	Value setting	Description
<b>L2TP Server</b>	Unchecked by default	Click the <b>Enable</b> box to activate L2TP server
<b>Interface</b>	1. Required setting 2. <b>All WANs is selected by default</b>	Select the interface on which L2TP tunnel is to be established. It can be any available WAN interface.
<b>L2TP over IPsec</b>	Unchecked by default	Click the <b>Enable</b> box to enable L2TP over IPsec, and fill in the Pre-shared Key (8~32 characters).
<b>Server Virtual IP</b>	Required setting	Specify the L2TP server Virtual IP.
<b>IP Pool Starting Address</b>	1. Required setting 2. <b>10 is set by default.</b>	Specify the L2TP server starting IP of virtual IP pool. Value Range: 1 ~ 254.
<b>IP Pool Ending Address</b>	1. Required setting 2. <b>17 is set by default.</b>	Specify the L2TP server ending IP of virtual IP pool. <b>Value Range:</b> >= Starting Address, and < (Starting Address + 8) or 254.
<b>Authentication Protocol</b>	Required setting	Select single or multiple Authentication Protocols for the L2TP server with which to authenticate L2TP clients. Available authentication protocols are <b>PAP / CHAP / MS-CHAP / MS-CHAP v2.</b>
<b>MPPE Encryption</b>	Required setting	Specify whether to support MPPE Protocol. Click the <b>Enable</b> box to enable MPPE and from dropdown box to select <b>40 bits / 56 bits / 128 bits.</b> Note: when MPPE Encryption is enabled, the Authentication Protocol <b>PAP / CHAP</b> options will not be available.
<b>Service Port</b>	Required setting	Specify the <b>Service Port</b> which L2TP server will use. <b>Value Range:</b> 1 ~ 65535.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the configuration.
<b>Undo</b>	N/A	Click the <b>Undo</b> button to recover the configuration.

L2TP Server Status <span>Refresh</span>				
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

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

# EW200 Industrial Cellular Gateway

User Account List <input type="button" value="Add"/> <input type="button" value="Delete"/>				
ID	User Name	Password	Enable	Actions
User Account Configuration				
User Name	Password		Account	
<input type="text"/>	<input type="text"/>		<input type="checkbox"/> Enable	
<input type="button" value="Save"/>				

User Account List Window		
Item	Value setting	Description
User Account List	Max. of 10 user accounts	<p>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.</p> <p>Click <b>Add</b> button to add a user account. Enter the User name and password. Then check the <b>enable</b> box to enable the user.</p> <p>Click <b>Save</b> button to save the new user account.</p> <p>The selected user account can permanently be deleted by clicking the <b>Delete</b> button.</p> <p><b>Value Range:</b> 1 ~ 32 characters.</p>

## As a L2TP Client

When **Client** is selected in Client/Server, a series of L2TP Client Configuration screens will appear.

L2TP Client Configuration	
Item	Setting
▶ L2TP Client	<input type="checkbox"/> Enable

L2TP Client Configuration		
Item Setting	Value setting	Description
L2TP Client	Unchecked by default	Check the <b>Enable</b> box to enable L2TP client role of the gateway.
Save	N/A	Click <b>Save</b> button to save the settings.
Undo	N/A	Click <b>Undo</b> button to cancel the settings.

# EW200 Industrial Cellular Gateway

## Create/Edit L2TP Client

L2TP Client List & Status <span>Add</span> <span>Delete</span> <span>Refresh</span> <span>↑</span> <span>×</span>								
ID	Tunnel Name	Interface	Virtual IP	Remote IP/FQDN	Remote Subnet	Status	Enable	Actions
1	L2TP #1	WAN 1	0.0.0.0	192.168.127.72			<input type="checkbox"/>	<span>Edit</span> <input type="checkbox"/> Select

When the **Add/Edit** button is applied, a series of configuration screen will appear. You can add up to 8 L2TP Clients.

L2TP Client Configuration	
Item	Setting
▶ Tunnel Name	<input type="text" value="L2TP #1"/>
▶ Interface	<input type="text" value="WAN1"/>
▶ L2TP over IPsec	<input type="checkbox"/> Enable Preshared Key <input type="text" value=""/> (Min. 8 characters)
▶ Remote LNS IP/FQDN	<input type="text"/>
▶ MTU	<input type="text" value="1500"/>
▶ Remote LNS Port	<input type="text" value="1701"/>
▶ User Name	<input type="text"/>
▶ Password	<input type="text"/>
▶ Tunneling Password (Optional)	<input type="text"/>
▶ Remote Subnet	<input type="text"/>
▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
▶ MPPE Encryption	<input type="checkbox"/> Enable
▶ NAT before Tunneling	<input type="checkbox"/> Enable
▶ LCP Echo Type	<input type="text" value="Auto"/> Interval <input type="text" value="30"/> seconds Max. Failure Time <input type="text" value="6"/> times
▶ Service Port	<input type="text" value="Auto"/> <input type="text" value="0"/>
▶ Tunnel	<input type="checkbox"/> Enable

L2TP Client Configuration		
Item	Setting	Description
<b>Tunnel Name</b>	Required setting	Enter a tunnel name. <b>Value Range:</b> 1 ~ 32 characters.
<b>Interface</b>	Required setting	Define the selected interface to be the used for this L2TP tunnel ( <b>WAN-1</b> is available only when WAN-1 interface is enabled) The same applies to other WAN interfaces (e.g. <b>WAN-2</b> ).
<b>L2TP over IPsec</b>	Unchecked by default	Check the <b>Enable</b> box to activate L2TP over IPsec, and further specify a Pre-shared Key (8~32 characters).
<b>Remote LNS IP/FQDN</b>	Required setting	Enter the public IP address or the FQDN of the L2TP server.
<b>MTU</b>	1. Required setting 2. 1500 is set by default	Specify the MTU. Value Range: 0 ~ 1500.

# EW200 Industrial Cellular Gateway

<b>Remote LNS Port</b>	1. Required setting 2. Default is <b>1701</b>	Enter the Remote LNS Port for this L2TP tunnel. <b><u>Value Range:</u></b> 1 ~ 65535.
<b>User Name</b>	Required setting	Enter the <b>User Name</b> for this L2TP tunnel to be authenticated when connect to L2TP server. <b><u>Value Range:</u></b> 1 ~ 32 characters.
<b>Password</b>	Required setting	Enter the <b>Password</b> for this L2TP tunnel to be authenticated when connect to L2TP server.
<b>Tunneling Password(Optional)</b>	Unchecked by default	Enter the <b>Tunneling Password</b> for this L2TP tunnel to authenticate.
<b>Remote Subnet</b>	Required setting	Specify the remote subnet for this L2TP tunnel to reach the L2TP server. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24). 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. If you enter 0.0.0.0/0 in the Remote Subnet field, it will be treated as a default gateway setting for the L2TP client peer, all packets, including the Internet accessing of L2TP Client peers, will go through the established L2TP VPN tunnel. That means the remote L2TP VPN server controls the flow of any packets from the L2TP client peer.
<b>Authentication Protocol</b>	1. Required setting 2. Unchecked by default	Specify one ore multiple <b>Authentication Protocol</b> for this L2TP tunnel. Available authentication methods are <b>PAP / CHAP / MS-CHAP / MS-CHAP v2</b> .
<b>MPPE Encryption</b>	1. Unchecked by default 2. Optional setting	Specify whether L2TP server supports the <b>MPPE Protocol</b> . Click the <b>Enable</b> box to enable MPPE. Note: when MPPE Encryption is enabled, the Authentication Protocol <b>PAP / CHAP</b> options will not be available.
<b>LCP Echo Type</b>	1. Auto is set by default	Specify the LCP Echo Type for this L2TP tunnel. Select from <b>Auto</b> , <b>User-defined</b> , or <b>Disable</b> . <b>Auto:</b> the system sets the Interval and Max. Failure Time. <b>User-defined:</b> enter the Interval and Max. Failure Time. The default value for Interval is 30 seconds, and Maximum Failure Times is 6 Times. <b>Disable:</b> disable the LCP Echo. <b><u>Value Range:</u></b> 1 ~ 99999 for Interval Time, 1~999 for Failure Time.
<b>Service Port</b>	Required setting	Specify the <b>Service Port</b> for this L2TP tunnel to use. It can be <b>Auto</b> , <b>(1701) for Cisco</b> , or <b>User-defined</b> . <b>Auto:</b> The system determines the service port. <b>1701 (for Cisco):</b> The system uses port 1701 for connecting with CISCO L2TP Server. <b>User-defined:</b> Enter the service port. The default value is 0. <b><u>Value Range:</u></b> 0 ~ 65535.
<b>Tunnel</b>	Unchecked by default	Check the <b>Enable</b> box to enable this L2TP tunnel.
<b>Save</b>	N/A	Click <b>Save</b> button to save the settings.
<b>Undo</b>	N/A	Click <b>Undo</b> button to cancel the settings.
<b>Back</b>	N/A	Click <b>Back</b> button to return to the previous page.



# EW200 Industrial Cellular Gateway

## 5.1.4 PPTP

Configuration

Item	Setting
PPTP	<input type="checkbox"/> Enable
Client/Server	Server ▾

PPTP Server Configuration

Item	Setting
PPTP Server	<input type="checkbox"/> Enable
Interface	All WANs ▾
Server Virtual IP	192.168.0.1
IP Pool Starting Address	10
IP Pool Ending Address	17
Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
MPPE Encryption	<input type="checkbox"/> Enable 40 bits ▾

PPTP Server Status Refresh

User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

User Account List Add Delete

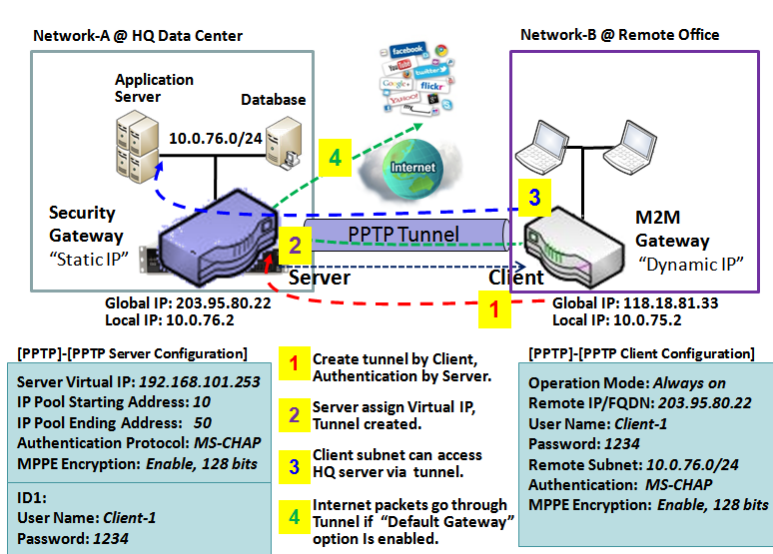
ID	User Name	Password	Enable	Actions
----	-----------	----------	--------	---------

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.

**PPTP Client:** It can be mobile users or gateways in remote offices with dynamic IP. To set up a tunnel, add "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. Select "Default Gateway" or "Remote Subnet" for packet flow. You can also define what kind of traffic will pass through the PPTP tunnel in the "Default Gateway / Remote Subnet" parameter.

# EW200 Industrial Cellular Gateway



For the PPTP client peer, a Remote Subnet item is required. It is for the Intranet of PPTP server peer. At PPTP client peer, the packets whose destination is in the dedicated subnet will be transferred via the PPTP tunnel. Others will be transferred based on current routing policy of the gateway at PPTP client peer. But, if 0.0.0.0/0 is entered in the Remote Subnet field, it will be treated as a "Default Gateway" setting for the PPTP client peer, and all packets, including the Internet accessing of PPTP client peers, will go through the established PPTP tunnel. That means the remote PPTP server peer controls the flow of any packets from the PPTP client peer.

# EW200 Industrial Cellular Gateway

## PPTP Setting

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

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

### Enable PPTP

Configuration [ Help ]	
Item	Setting
▶ PPTP	<input type="checkbox"/> Enable
▶ Client/Server	Server ▼

Enable PPTP Window		
Item	Value setting	Description
PPTP	Unchecked by default	Click the <b>Enable</b> box to activate PPTP function.
Client/Server	Required setting	Specify the role of PPTP. Select <b>Server</b> or <b>Client</b> role. Below are the configuration windows for PPTP Server and for Client.
Save	N/A	Click <b>Save</b> 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.

PPTP Server Configuration	
Item	Setting
▶ PPTP Server	<input type="checkbox"/> Enable
▶ Interface	WAN1 ▼
▶ Server Virtual IP	192.168.12.1
▶ IP Pool Starting Address	10
▶ IP Pool Ending Address	17
▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input checked="" type="checkbox"/> MS-CHAP <input checked="" type="checkbox"/> MS-CHAP v2
▶ MPPE Encryption	<input checked="" type="checkbox"/> Enable 40 bits ▼

# EW200 Industrial Cellular Gateway

PPTP Server Configuration Window		
Item	Value setting	Description
<b>PPTP Server</b>	Unchecked by default	Check the <b>Enable</b> box to enable PPTP server role of the gateway.
<b>Interface</b>	1. Required setting 2. <b>All WANs is selected by default</b>	Select the interface on which PPTP tunnel is to be established. It can be any available WAN interface.
<b>Server Virtual IP</b>	1. Required 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.
<b>IP Pool Starting Address</b>	1. Required setting 2. Default is <b>10</b>	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 ~ 254.
<b>IP Pool Ending Address</b>	1. Required setting 2. Default is <b>17</b>	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. <b>Value Range:</b> >= Starting Address, and < (Starting Address + 8) or 254.
<b>Authentication Protocol</b>	1. Required 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 <b>PAP / CHAP / MS-CHAP / MS-CHAP v2</b> .
<b>MPPE Encryption</b>	1. Required setting 2. Unchecked by default	Specify whether to support MPPE Protocol. Click the <b>Enable</b> box to enable MPPE and from dropdown box to select <b>40 bits / 56 bits / 128 bits</b> . Note: when MPPE Encryption is enabled, the Authentication Protocol <b>PAP / CHAP</b> options will not be available.
<b>Save</b>	N/A	Click <b>Save</b> button to save the settings.
<b>Undo</b>	N/A	Click <b>Undo</b> button to cancel the settings.

<div>  <b>PPTP Server Status</b> <div>Refresh</div> </div>				
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

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

# EW200 Industrial Cellular Gateway

User Account List <input type="button" value="Add"/> <input type="button" value="Delete"/>				
ID	User Name	Password	Enable	Actions
User Account Configuration				
User Name		Password	Account	
<input type="text"/>		<input type="text"/>	<input type="checkbox"/> Enable	
<input type="button" value="Save"/>				

User Account List Window		
Item	Value setting	Description
User Account List	Max. of 10 user accounts	<p>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.</p> <p>Click <b>Add</b> button to add user account. Enter the User name and password. Then check the <b>enable</b> box to enable the user.</p> <p>Click <b>Save</b> button to save new user account.</p> <p>The selected user account can permanently be deleted by clicking the <b>Delete</b> button.</p> <p><b>Value Range:</b> 1 ~ 32 characters.</p>

## As a PPTP Client

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

PPTP Client Configuration	
Item	Setting
▶ PPTP Client	<input type="checkbox"/> Enable

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

# EW200 Industrial Cellular Gateway

## Create/Edit PPTP Client

PPTP Client List & Status <span>Add</span> <span>Delete</span> <span>Refresh</span>								
ID	Tunnel Name	Interface	Virtual IP	Remote IP/FQDN	Remote Subnet	Status	Enable	Actions

When the **Add/Edit** button is applied, a series of PPTP Client Configuration screens will appear.

PPTP Client Configuration	
Item	Setting
▶ Tunnel Name	<input type="text" value="PPTP #1"/>
▶ Interface	<input type="text" value="WAN1"/>
▶ Remote IP/FQDN	<input type="text"/>
▶ MTU	<input type="text" value="1500"/>
▶ User Name	<input type="text"/>
▶ Password	<input type="text"/>
▶ Remote Subnet	<input type="text"/>
▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
▶ MPPE Encryption	<input type="checkbox"/> Enable
▶ NAT before Tunneling	<input type="checkbox"/> Enable
▶ LCP Echo Type	<input type="text" value="Auto"/> Interval <input type="text" value="30"/> seconds Max. Failure Time <input type="text" value="6"/> times
▶ Tunnel	<input type="checkbox"/> Enable

PPTP Client Configuration Window		
Item	Value setting	Description
Tunnel Name	Required setting	Enter a tunnel name. <b>Value Range:</b> 1 ~ 32 characters.
Interface	1. Required setting 2. <b>WAN1</b> is selected by default	Define the selected interface to be the used for this PPTP tunnel ( <b>WAN-1</b> is available only when WAN-1 interface is enabled) The same applies to other WAN interfaces (e.g. <b>WAN-2</b> ).
Operation Mode	1. Required setting 2. <b>Always on</b> is selected by default	Define operation mode for the PPTP Tunnel. It can be <b>Always On</b> , or <b>Failover</b> . If this tunnel is set as a failover tunnel, you need to further select a primary tunnel from which to failover to. Note: <b>Failover</b> mode is not available for gateways with a single WAN.
Remote IP/FQDN	1. Required setting. 2. Format can be a ipv4 address or FQDN	Enter the public IP address or the FQDN of the PPTP server.
MTU	1. Required setting 2. <b>1500 is set by default</b>	Specify the <b>MTU</b> . Value Range: 0 ~ 1500.
User Name	Required setting	Enter the <b>User Name</b> for this PPTP tunnel to be authenticated when connect to PPTP server. <b>Value Range:</b> 1 ~ 32 characters.

# EW200 Industrial Cellular Gateway

<b>Password</b>	Required setting	Enter the <b>Password</b> for this PPTP tunnel to be authenticated when connect to PPTP server.
<b>Remote Subnet</b>	Required setting	<p>Specify the remote subnet for this PPTP tunnel to reach PPTP server. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24). It is for the Intranet of PPTP VPN server. 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.</p> <p>If 0.0.0.0/0 is entered in the Remote Subnet field, it will be treated as a default gateway setting for the PPTP client peer. All packets, including the Internet accessing of PPTP Client peers, will go through the established PPTP VPN tunnel. That means the remote PPTP VPN server controls the flow of any packets from the PPTP client peer.</p>
<b>Authentication Protocol</b>	1. Required setting 2. Unchecked by default	Specify one or multiple <b>Authentication Protocols</b> for this PPTP tunnel. Available authentication methods are <b>PAP / CHAP / MS-CHAP / MS-CHAP v2</b> .
<b>MPPE Encryption</b>	1. Unchecked by default 2. Optional setting	Specify whether PPTP server supports <b>MPPE Protocol</b> . Click the <b>Enable</b> box to enable MPPE. Note: when MPPE Encryption is enabled, the Authentication Protocol <b>PAP / CHAP</b> options will not be available.
<b>NAT before tunneling</b>	1. Required setting 2. Unchecked by default	Specify whether NAT is required or not for this PPTP tunnel.
<b>LCP Echo Type</b>	Auto is set by default	<p>Specify the LCP Echo Type for this PPTP tunnel. It can be <b>Auto</b>, <b>User-defined</b>, or <b>Disable</b>.</p> <p><b>Auto</b>: the system sets the Interval and Max. Failure Time.</p> <p><b>User-defined</b>: enter the Interval and Max. Failure Time. The default value for Interval is 30 seconds, and Maximum Failure Times is 6 Times.</p> <p><b>Disable</b>: disable the LCP Echo.</p> <p><b>Value Range</b>: 1 ~ 99999 for Interval Time, 1~999 for Failure Time.</p>
<b>Tunnel</b>	Unchecked by default	Check the <b>Enable</b> box to enable this PPTP tunnel.
<b>Save</b>	N/A	Click <b>Save</b> button to save the settings.
<b>Undo</b>	N/A	Click <b>Undo</b> button to cancel the settings.
<b>Back</b>	N/A	Click <b>Back</b> button to return to the previous page.

## 5.1.5 GRE

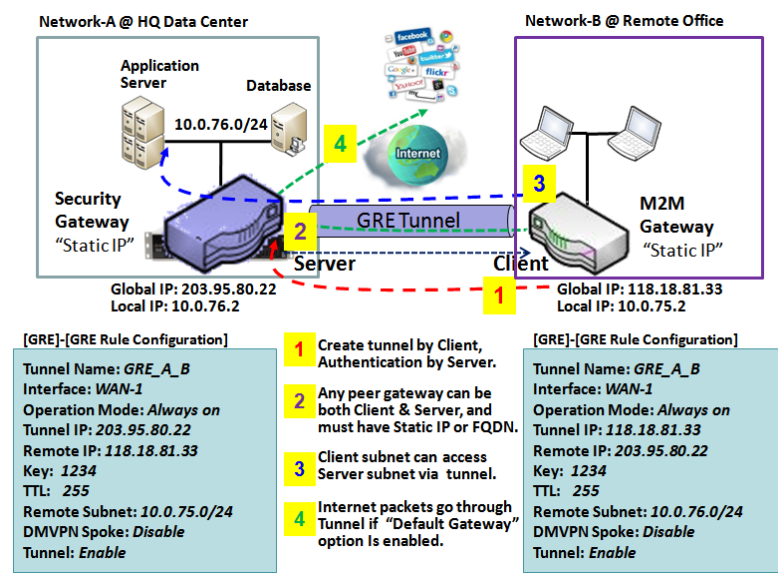
Configuration										
Item		Setting								
GRE Tunnel		<input type="checkbox"/> Enable								
Max. Concurrent GRE Tunnels		32								

GRE Tunnel List										
		Add		Delete						
ID	Tunnel Name	Interface	Tunnel IP	Remote IP	MTU	Key	TTL	Remote Subnet	Enable	Actions

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

GRE Tunneling is similar to IPsec Tunneling, with the 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 rules.

### GRE Tunnel Scenario



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

Each peer must further specify the Remote Subnet item for the Intranet of GRE server peer. 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 0.0.0.0/0 is entered in the Remote Subnet field, it will be treated as a "Default Gateway" setting for the GRE client peer, and all packets, including the Internet accessing of GRE client peers, will go through the established GRE tunnel. That means

the remote GRE server peer controls the flow of any packets from the GRE client peer.

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



# EW200 Industrial Cellular Gateway

## GRE Setting

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

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

### Enable GRE

Configuration [ Help ]	
Item	Setting
GRE Tunnel	<input type="checkbox"/> Enable
Max. Concurrent GRE Tunnels	<input type="text" value="32"/>

Enable GRE Window		
Item	Value setting	Description
GRE Tunnel	Unchecked by default	Click the <b>Enable</b> box to enable GRE function.
Max. Concurrent GRE Tunnels	Depends on Product specification.	The specified value will limit the maximum number of simultaneous GRE tunnel connections. The default value will depend on the device model.
Save	N/A	Click <b>Save</b> button to save the settings
Undo	N/A	Click <b>Undo</b> button to cancel the settings

### Create/Edit GRE tunnel

GRE Tunnel List <input type="button" value="Add"/> <input type="button" value="Delete"/>											
ID	Tunnel Name	Interface	Operation Mode	Tunnel IP	Remote IP	Key	TTL	Keep-alive	Remote Subnet	Enable	Actions

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

# EW200 Industrial Cellular Gateway

GRE Rule Configuration	
Item	Setting
▶ Tunnel Name	GRE #1
▶ Interface	WAN1 ▼
▶ Tunnel IP	IP: <input type="text"/> MASK: -- select one -- ▼ (Optional)
▶ Remote IP	<input type="text"/>
▶ MTU	<input type="text"/>
▶ Key	<input type="text"/> (Optional)
▶ TTL	<input type="text"/>
▶ Remote Subnet	<input type="text"/>
▶ Tunnel	<input type="checkbox"/> Enable

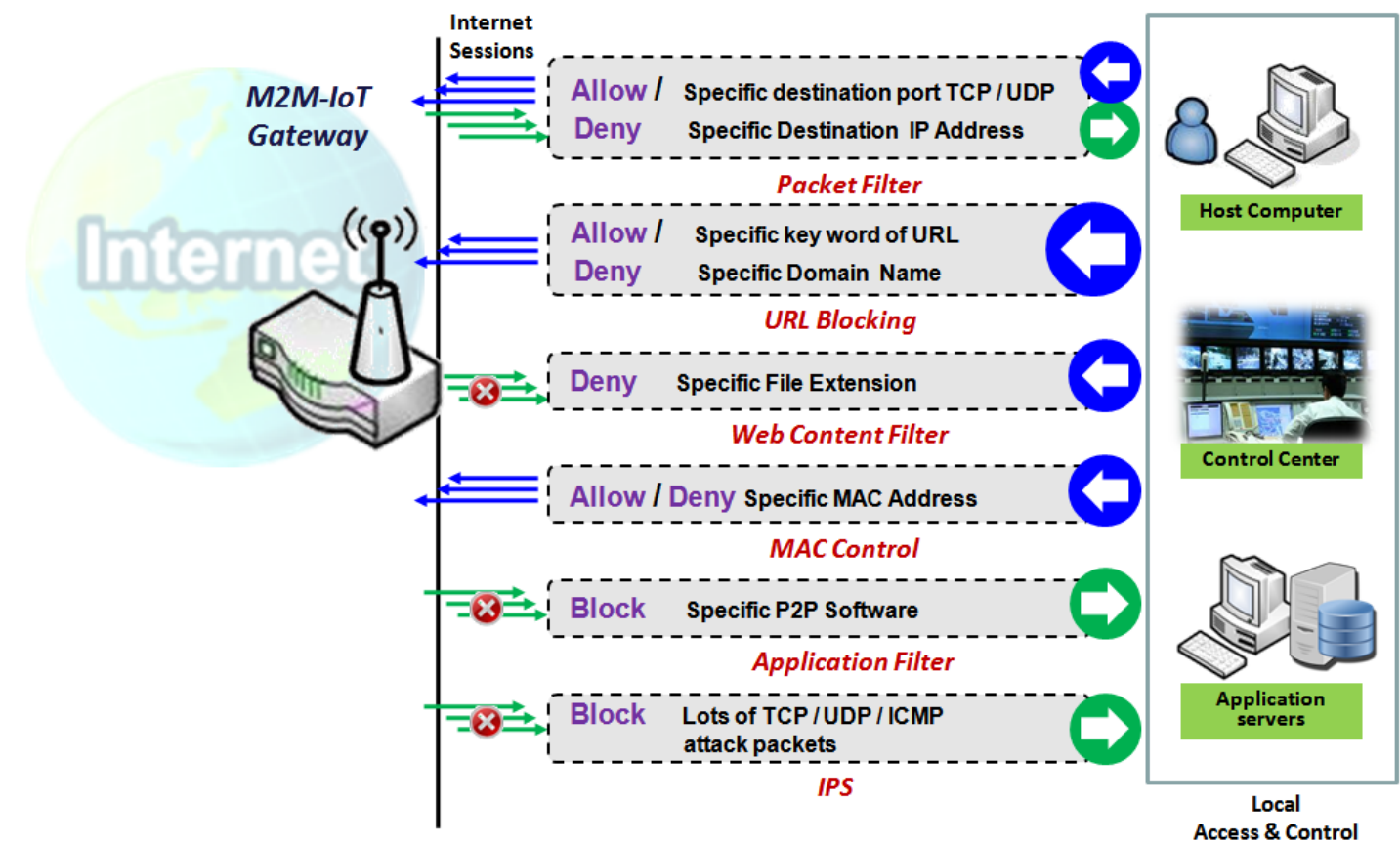
GRE Rule Configuration Window		
Item	Value setting	Description
<b>Tunnel Name</b>	Required setting	Enter a tunnel name. <b>Value Range:</b> 1 ~ 9 characters.
<b>Interface</b>	1. Required setting 2. <b>WAN 1</b> is selected by default	Select the interface on which GRE tunnel is to be established. It can be any available WAN and LAN interface.
<b>Tunnel IP</b>	Optional setting	Enter the Tunnel IP address and corresponding subnet mask.
<b>Remote IP</b>	Required setting	Enter the Remote IP address of remote GRE tunnel gateway. Normally this is the public IP address of the remote GRE gateway.
<b>MTU</b>	1. Required setting 2. <b>Auto (value zero or blank) is set by default</b>	<b>MTU</b> refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. When set to <b>Auto</b> (value '0' or blank), the router selects the best MTU for best Internet connection performance. Value Range: 0 ~ 1500.
<b>Key</b>	Optional setting	Enter the Key for the GRE connection. <b>Value Range:</b> 0 ~ 9999999999.
<b>TTL</b>	1. Required setting 2. 1 to 255 range	Specify <b>TTL</b> hop-count value for this GRE tunnel. Value Range: 1 ~ 255.
<b>Remote Subnet</b>	Required setting	Specify the remote subnet for this GRE tunnel. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24). It is for the Intranet of GRE server peer. 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 security gateway at GRE client peer.  If 0.0.0.0/0 is entered in the Remote Subnet field, it will be treated as a default gateway setting for the GRE client peer, and all packets, including the Internet accessing of GRE client peers, will go through the established GRE tunnel. That

## EW200 Industrial Cellular Gateway

---

		means the remote GRE server peer controls the flow of any packets from the GRE client peer.
<b>Tunnel</b>	Unchecked by default	Check <b>Enable</b> box to enable this GRE tunnel.
<b>Save</b>	N/A	Click <b>Save</b> button to save the settings.
<b>Undo</b>	N/A	Click <b>Undo</b> button to cancel the settings.
<b>Back</b>	N/A	Click <b>Back</b> button to return to the previous page.

5.2 Firewall



The firewall functions include Packet Filter, URL Blocking, Content Filter, MAC Control, Application Filter, IPS and some firewall options. Supported functions vary depending on the gateway model.

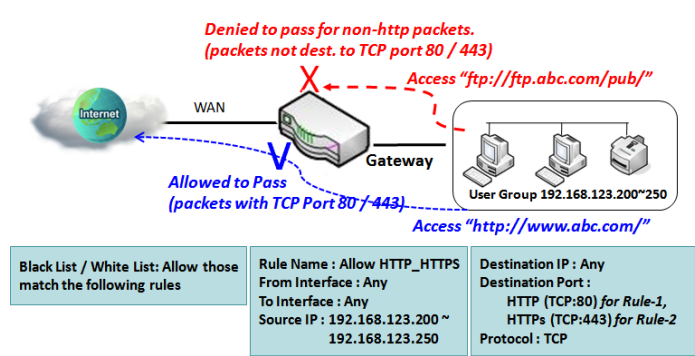
5.2.1 Packet Filter

Configuration [ Help ]												
Item			Setting									
▶ Packet Filters			<input checked="" type="checkbox"/> Enable									
▶ Black List / White List			Deny those match the following rules. ▼									
▶ Log Alert			<input type="checkbox"/> 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

# EW200 Industrial Cellular Gateway

The "Packet Filter" function lets you define filtering rules for incoming and outgoing packets, allowing the gateway to control what packets are allowed or blocked as they 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, there should be a schedule for which the rule will be active.

## Packet Filter with White List Scenario



As shown in the diagram, "Packet Filter Rule List" is specified as a white list (*Allow those matching the following 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 [ Help ]	
Item	Setting
▶ Packet Filters	<input type="checkbox"/> Enable
▶ Black List / White List	Deny those match the following rules. ▼
▶ Log Alert	<input type="checkbox"/> Log Alert

Configuration Window		
Item Name	Value setting	Description
Packet Filter	Unchecked by default	Check the <b>Enable</b> box to activate the Packet Filter function

# EW200 Industrial Cellular Gateway

<b>Blacklist / White List</b>	Deny those match the following rules is set by default	When <b><i>Deny those match the following rules</i></b> is selected, as the name suggests, packets specified in the rules will be blocked –blacklisted. In contrast, with <b><i>Allow those match the following rules</i></b> , you can specifically white list the packets to pass and the rest will be blocked.
<b>Log Alert</b>	Unchecked by default	Check the <b>Enable</b> box to activate Event Log.
<b>Save</b>	N/A	Click <b>Save</b> to save the settings
<b>Undo</b>	N/A	Click <b>Undo</b> 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.

<input type="checkbox"/> Packet Filter List <input type="button" value="Add"/> <input type="button" value="Delete"/>												
ID	Rule Name	From Interface	To Interface	Source IP	Destination IP	Source MAC	Protocol	Source Port	Destination Port	Time Schedule	Enable	Actions

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

Packet Filter Rule Configuration	
Item	Setting
▶ Rule Name	<input type="text" value="Rule1"/>
▶ From Interface	<input type="text" value="Any"/>
▶ To Interface	<input type="text" value="Any"/>
▶ Source IP	<input type="text" value="Any"/>
▶ Destination IP	<input type="text" value="Any"/>
▶ Source MAC	<input type="text" value="Any"/>
▶ Protocol	<input type="text" value="Any(0)"/>
▶ Source Port	<input type="text" value="User-defined Service"/> <input type="text" value=""/> - <input type="text" value=""/>
▶ Destination Port	<input type="text" value="User-defined Service"/> <input type="text" value=""/> - <input type="text" value=""/>
▶ Time Schedule	<input type="text" value="(0) Always"/>
▶ Rule	<input type="checkbox"/> Enable

Packet Filter Rule Configuration		
Item Name	Value setting	Description
<b>Rule Name</b>	1. String format, any text 2. Required setting	Enter a packet filter rule name. <b><u>Value Range:</u></b> 1 ~ 30 characters.

# EW200 Industrial Cellular Gateway

<b>From Interface</b>	1. Required setting 2. By default <b>Any</b> is selected	Define the selected interface to be the packet-entering interface of the router. If the packets to be filtered are coming from <b>LAN to WAN</b> then select LAN for this field. If <b>VLAN-1 to WAN</b> then select <b>VLAN-1</b> for this field. Other examples are VLAN-1 to VLAN-2. VLAN-1 to WAN. Select <b>Any</b> 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.
<b>To Interface</b>	1. Required setting 2. By default <b>Any</b> is selected	Define the selected interface to be the packet-leaving interface of the router. If the packets to be filtered are entering from <b>LAN to WAN</b> then select <b>WAN</b> for this field. If <b>VLAN-1 to WAN</b> then select <b>WAN</b> for this field. Other examples are VLAN-1 to VLAN-2. VLAN-1 to WAN. Select <b>Any</b> 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.
<b>Source IP</b>	1. Required setting 2. By default <b>Any</b> is selected	This field is to specify the <b>Source IP address</b> . Select <b>Any</b> to filter packets coming from any IP addresses. Select <b>Specific IP Address</b> to filter packets coming from an IP address. Select <b>IP Range</b> to filter packets coming from a specified range of IP address. Select <b>IP Address-based Group</b> to filter packets coming from a pre-defined group. Note: group must be pre-defined before this option becomes available. Refer to <b>Object Definition &gt; Grouping &gt; Host grouping</b> . You may also access to create a group by the <b>Add Rule</b> shortcut button.
<b>Destination IP</b>	1. Required setting 2. By default <b>Any</b> is selected	This field is to specify the <b>Destination IP address</b> . Select <b>Any</b> to filter packets that are entering to any IP addresses. Select <b>Specific IP Address</b> to filter packets entering to an IP address entered in this field. Select <b>IP Range</b> to filter packets entering to a specified range of IP address entered in this field. Select <b>IP Address-based Group</b> to filter packets entering to a pre-defined group selected. Note: group must be pre-defined before this selection become available. Refer to <b>Object Definition &gt; Grouping &gt; Host grouping</b> . You may also access to create a group by the <b>Add Rule</b> shortcut button. Setting done through the <b>Add Rule</b> button will also appear in the <b>Host grouping</b> setting screen.
<b>Source MAC</b>	1. Required setting 2. By default <b>Any</b> is selected	This field is to specify the <b>Source MAC address</b> . Select <b>Any</b> to filter packets coming from any MAC addresses. Select <b>Specific MAC Address</b> to filter packets coming from a MAC address. Select <b>MAC Address-based Group</b> to filter packets coming from a pre-defined group selected. Note: group must be pre-defined before this selection become available. Refer to <b>Object Definition &gt; Grouping &gt; Host grouping</b> . You may also access to create a group by the <b>Add Rule</b> shortcut button.
<b>Protocol</b>	1. Required setting 2. By default <b>Any(0)</b> is selected	For <b>Protocol</b> , select <b>Any</b> to filter any protocol packets For <b>Source Port</b> , select a predefined port dropdown box when <b>Well-known Service</b> is selected, otherwise select <b>User-defined Service</b> and specify a port range.

# EW200 Industrial Cellular Gateway

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



## 5.2.2 URL Blocking

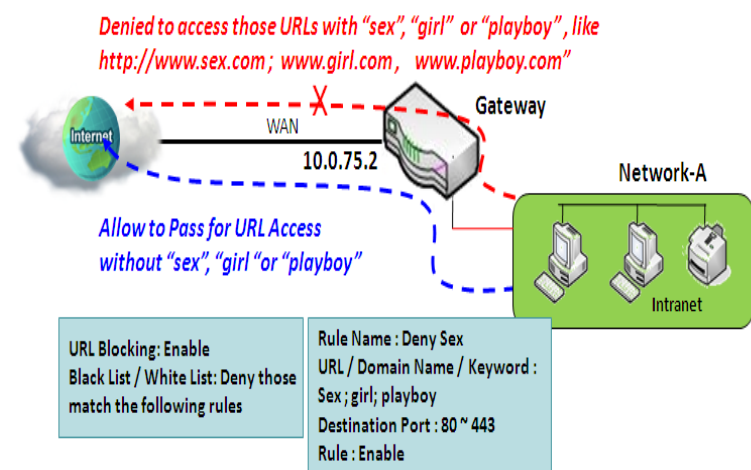
The "URL Blocking" function lets you define blocking or allowing rules for incoming and outgoing web request packets. With defined rules, the gateway can control the Web requests containing the complete URL, partial domain name, or pre-defined keywords. For example, one can filter out or allow only the 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. A time schedule can be applied to activate the URL Blocking rules during pre-defined time interval(s).

The gateway will log and display 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 blacklist. 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 Blacklist



When the administrator of the gateway wants to block web requests with specific patterns, he/she can use the "URL Blocking" function to block specific web requests by defining the blacklist as shown in the diagram. When the administrator wants to allow only web requests with some dedicated patterns to go through the gateway, he/she 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 web requests with "playboy" pattern to go through the gateway. The system will block the web requests with "sex", "sexygirl" or "playboy" patterns to pass through the gateway.

# EW200 Industrial Cellular Gateway

## URL Blocking Setting

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

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

The "Configuration" window lets you activate the URL blocking function and specify blacklisting or whitelisting packets as defined in the "URL Blocking Rule List" entry. 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 logs.

The "URL Blocking Rule List" window lists all your defined URL blocking rule entries. The "URL Blocking Rule Configuration" window lets 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	
Item	Setting
▶ URL Blocking	<input checked="" type="checkbox"/> Enable
▶ Black List / White List	Deny those match the following rules. ▼
▶ Log Alert	<input type="checkbox"/> Enable

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

# EW200 Industrial Cellular Gateway

## Create/Edit URL Blocking Rules

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

URL Blocking Rule List <span>Add</span> <span>Delete</span>								
ID	Rule Name	Source IP	Source MAC	URL / Domain Name / Keyword	Destination Port	Time Schedule	Enable	Actions

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

URL Blocking Rule Configuration	
Item	Setting
▶ Rule Name	<input type="text" value="Rule1"/>
▶ Source IP	<input type="text" value="Any"/>
▶ Source MAC	<input type="text" value="Any"/>
▶ URL / Domain Name / Keyword	<input type="text"/>
▶ Destination Port	<input type="text" value="Any"/>
▶ Time Schedule Rule	<input type="text" value="(0) Always"/>
▶ Rule	<input type="checkbox"/> Enable

URL Blocking Rules Configuration		
Item	Value setting	Description
Rule Name	1. String format, any text 2. Required setting	Specify an URL Blocking rule name.
Source IP	1. Required setting 2. <b>Any</b> is set by default	This field is to specify the <b>Source IP address</b> . <ul style="list-style-type: none"><li>• Select <b>Any</b> to filter packets coming from any IP addresses.</li><li>• Select <b>Specific IP Address</b> to filter packets coming from an IP address entered in this field.</li><li>• Select <b>IP Range</b> to filter packets coming from a specified range of IP address entered in this field.</li><li>• Select <b>IP Address-based Group</b> to filter packets coming from a pre-defined group selected. Note: group must be pre-defined before this option becomes available. Refer to <b>Object Definition &gt; Grouping &gt; Host grouping</b>.</li></ul>
Source MAC	1. Required setting 2. <b>Any</b> is set by default	This field is to specify the <b>Source MAC address</b> . <ul style="list-style-type: none"><li>• Select <b>Any</b> to filter packets coming from any MAC addresses.</li><li>• Select <b>Specific MAC Address</b> to filter packets coming from a MAC address entered in this field.</li><li>• Select <b>MAC Address-based Group</b> to filter packets coming from a pre-defined group selected. Note: group must be pre-defined before this selection becomes available. Refer to <b>Object Definition &gt; Grouping &gt; Host grouping</b>.</li></ul>
URL / Domain Name /	1. Required setting 2. Supports up to a	Specify URL, Domain Name, or Keyword list for URL checking. <ul style="list-style-type: none"><li>• In the <b>Blacklist</b> mode, if a matched rule is found, the packets will be dropped.</li></ul>

## EW200 Industrial Cellular Gateway

<b>Keyword</b>	maximum of 10 Keywords in a rule by using the delimiter “;”.	<ul style="list-style-type: none"> <li>In the <b>White List</b> mode, if a matched rule is found, the packets will be accepted and those which don’t match any rule will be dropped.</li> </ul>
<b>Destination Port</b>	<ol style="list-style-type: none"> <li>Required setting</li> <li><b>Any</b> is set by default</li> </ol>	<p>This field is to specify the <b>Destination Port number</b>.</p> <ul style="list-style-type: none"> <li>Select <b>Any</b> to filter packets going to any Port.</li> <li>Select <b>Specific Service Port</b> to filter packets going to a specific Port entered in this field.</li> <li>Select <b>Port Range</b> to filter packets going to a specific range of Ports entered in this field.</li> </ul>
<b>Time Schedule Rule</b>	Required setting	<p>Apply a specific <b>Time Schedule</b> to this rule; otherwise leave it as <b>(0) Always</b>. If the dropdown list is empty ensure <b>Time Schedule</b> is pre-configured. Refer to <b>Object Definition &gt; Scheduling &gt; Configuration</b> tab.</p>
<b>Rule</b>	Unchecked by default	Click the <b>Enable</b> box to activate this rule.
<b>Save</b>	NA	Click the <b>Save</b> button to save the settings.
<b>Undo</b>	NA	Click the <b>Undo</b> button to cancel the changes.
<b>Back</b>	NA	Click the <b>Back</b> button to return to the URL Blocking Configuration page.

# EW200 Industrial Cellular Gateway

## 5.2.3 MAC Control

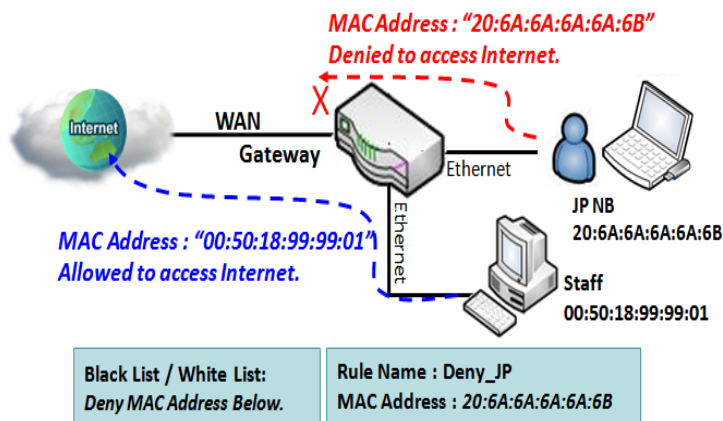
Configuration [ Help ]	
Item	Setting
▶ MAC Control	<input checked="" type="checkbox"/> Enable
▶ Black List / White List	Deny MAC Address Below. ▼
▶ Log Alert	<input type="checkbox"/> Enable
▶ Known MAC from LAN PC List	192.168.1.100(James-P45V) ▼ <input type="button" value="Copy to"/>

MAC Control Rule List <input type="button" value="Add"/> <input type="button" value="Delete"/>					
ID	Rule Name	MAC Address	Time Schedule Rule	Enable	Actions

"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 traffic from some client hosts with specific MAC addresses, the "MAC Control" function can be used to reject according to the blacklist configuration.

### MAC Control with Blacklist Scenario



As shown in the diagram, enable the MAC control function and specify the "MAC Control Rule List" as a blacklist, 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.

The system will block connections from the "JP NB" to the gateway but allow others.

# EW200 Industrial 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	<input type="checkbox"/> Enable
▶ Black List / White List	Deny MAC Address Below. ▼
▶ Log Alert	<input type="checkbox"/> Enable
▶ Known MAC from LAN PC List	192.168.123.100(James-P45V) ▼ <input type="button" value="Copy to"/>

Configuration Window		
Item	Value setting	Description
MAC Control	Unchecked by default	Check the <b>Enable</b> box to activate the MAC filter function
Blacklist / White List	Deny MAC Address Below is set by default	When <b>Deny MAC Address Below</b> is selected, as the name suggest, packets specified in the rules will be blocked – blacklisted. In contrast, with <b>Allow MAC Address Below</b> , you can specifically white list the packets to pass, and the rest will be blocked.
Log Alert	Unchecked by default	Check the <b>Enable</b> 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 <b>Copy to</b> to copy the selected <b>MAC Address</b> to the filter rule.
Save	N/A	Click <b>Save</b> to save the settings
Undo	N/A	Click <b>Undo</b> to cancel the settings

# EW200 Industrial 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 creating control rules.

MAC Control Rule List <input type="button" value="Add"/> <input type="button" value="Delete"/>					
ID	Rule Name	MAC Address	Time Schedule Rule	Enable	Actions

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

MAC Control Rule Configuration			
Rule Name	MAC Address (Use : to Compose)	Time Schedule	Enable
<input type="text" value="Rule1"/>	<input type="text"/>	<input type="text" value="(0) Always"/>	<input type="checkbox"/>
<input type="button" value="Save"/>			

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

# EW200 Industrial Cellular Gateway

## 5.2.4 IPS

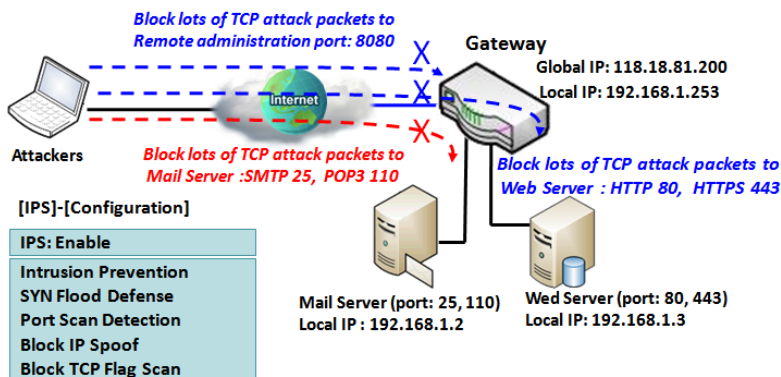
Configuration [ Help ]	
Item	Setting
▶ IPS	<input type="checkbox"/> Enable
▶ Log Alert	<input type="checkbox"/> Enable

Intrusion Prevention	
Item	Setting
▶ SYN Flood Defense	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)
▶ UDP Flood Defense	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)
▶ ICMP Flood Defense	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)
▶ Port Scan Detection	<input type="checkbox"/> Enable <input type="text" value="200"/> Packets/second (10~10000)

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

Intrusion Prevention System (IPS) is a network security appliance that monitors 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 the 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 normal ones pass through the gateway.



# EW200 Industrial 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 <span>[ Help ]</span>	
Item	Setting
▶ IPS	<input type="checkbox"/> Enable
▶ Log Alert	<input type="checkbox"/> Enable

Configuration Window		
Item	Value setting	Description
IPS	Unchecked by default	Check the <b>Enable</b> box to activate IPS function
Log Alert	Unchecked by default	Check the <b>Enable</b> box to activate to activate Event Log.
Save	N/A	Click <b>Save</b> to save the settings
Undo	N/A	Click <b>Undo</b> 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 enabling the defense function.

# EW200 Industrial Cellular Gateway

Intrusion Prevention	
Item	Setting
▶ SYN Flood Defense	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)
▶ UDP Flood Defense	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)
▶ ICMP Flood Defense	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)
▶ Port Scan Detection	<input type="checkbox"/> Enable <input type="text" value="200"/> Packets/second (10~10000)
▶ Block Land Attack	<input type="checkbox"/> Enable
▶ Block Ping of Death	<input type="checkbox"/> Enable
▶ Block IP Spoof	<input type="checkbox"/> Enable
▶ Block TCP Flag Scan	<input type="checkbox"/> Enable
▶ Block Smurf	<input type="checkbox"/> Enable
▶ Block Traceroute	<input type="checkbox"/> Enable
▶ Block Fraggle Attack	<input type="checkbox"/> Enable
▶ ARP Spoofing Defence	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)

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

## EW200 Industrial Cellular Gateway

---

Block Smurf Block Traceroute Block Fraggle Attack		
ARP Spoofing Defence	<ol style="list-style-type: none"><li>1. Required setting</li><li>2. Unchecked by default</li><li>3. Traffic threshold is set to 300 by default</li><li>4. The value range can be from 10 to 10000.</li></ol>	Click <b>Enable</b> box to activate this intrusion prevention rule and enter the traffic threshold in this field. <b><u>Value Range:</u></b> 10 ~ 10000.
Save	NA	Click <b>Save</b> to save the settings
Undo	NA	Click <b>Undo</b> to cancel the settings

# EW200 Industrial Cellular Gateway

## 5.2.5 Options

Firewall Options

Item	Setting
Stealth Mode	<input type="checkbox"/> Enable
SPI	<input type="checkbox"/> Enable
Discard Ping from WAN	<input type="checkbox"/> Enable

Remote Administrator Host Definition

ID	Interface	Protocol	IP	Subnet Mask	Service Port	Enable	Action
1	All WAN	HTTP	Any IP	N/A	80	<input checked="" type="checkbox"/>	Edit
2	All WAN	HTTPS	Any IP	N/A	443	<input checked="" type="checkbox"/>	Edit
3	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit
4	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit
5	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit

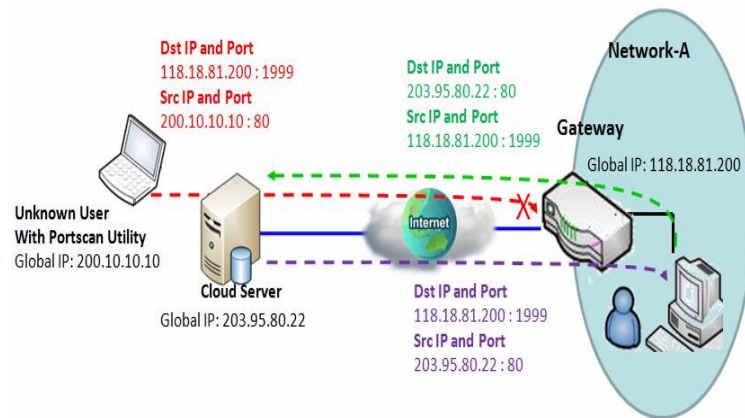
There are some additional useful firewall options in this page.

“Stealth Mode” lets the gateway not respond to port scans from the WAN so that makes it less susceptible to discovery and attacks on the Internet. “SPI” enables the 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 the packet is valid.

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

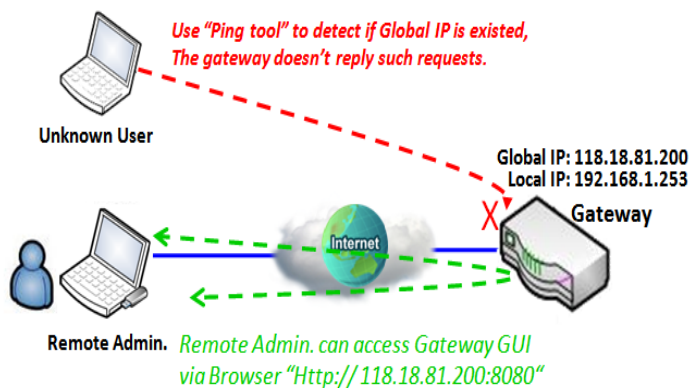
# EW200 Industrial Cellular Gateway

## Enable SPI Scenario



As shown in the diagram, the 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 access to 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 unable to ping this gateway and receive ICMP packet reply. Enable the Discard Ping from WAN function to prevent security leaks when local users use the internet.

If the remote administrator knows the gateway's global IP, he/she can access the Gateway GUI via TCP port 8080.

# EW200 Industrial Cellular Gateway

## 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

Firewall Options [ Help ]	
Item	Setting
▶ Stealth Mode	<input type="checkbox"/> Enable
▶ SPI	<input checked="" type="checkbox"/> Enable
▶ Discard Ping from WAN	<input type="checkbox"/> Enable

Firewall Options		
Item	Value setting	Description
<b>Stealth Mode</b>	Unchecked by default	Check the <b>Enable</b> box to activate the Stealth Mode function
<b>SPI</b>	Checked by default	Check the <b>Enable</b> box to activate the SPI function
<b>Discard Ping from WAN</b>	Unchecked by default	Check the <b>Enable</b> box to activate the Discard Ping from WAN function

### Define Remote Administrator Host

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

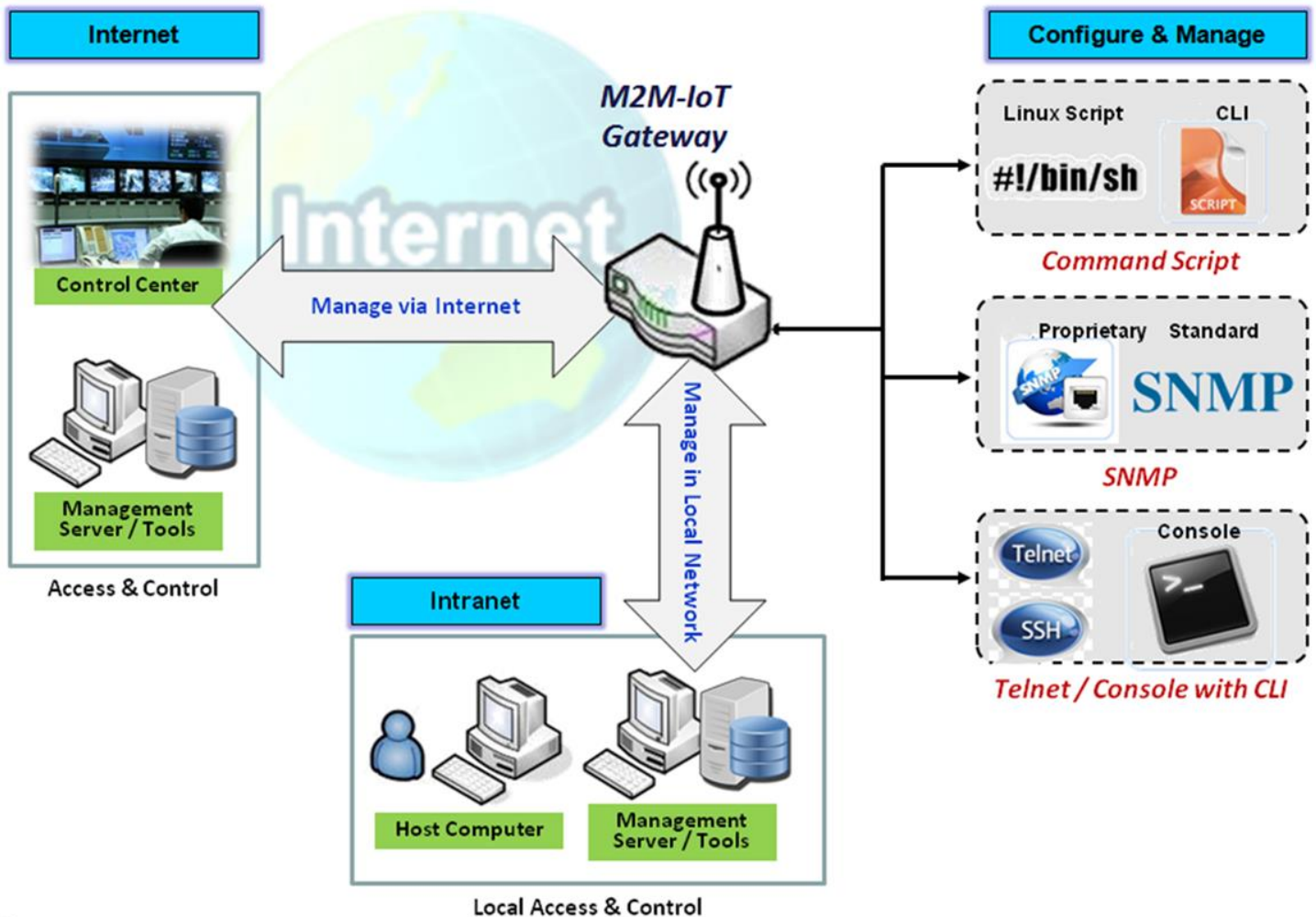
Remote Administrator Host Definition							
ID	Interface	Protocol	IP	Subnet Mask	Service Port	Enable	Action
1	All WAN	HTTP	Any IP	N/A	80	<input checked="" type="checkbox"/>	Edit
2	All WAN	HTTPS	Any IP	N/A	443	<input checked="" type="checkbox"/>	Edit
3	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit
4	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit
5	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit

# EW200 Industrial Cellular Gateway

Remote Administrator Host Definition		
Item	Value setting	Description
<b>Protocol</b>	HTTP is set by default	Select <b>HTTP</b> or <b>HTTPS</b> method for router access.
<b>IP</b>	Required setting	This field is to specify the remote host to assign access rights for remote access. Select <b>Any IP</b> to allow any remote hosts Select <b>Specific IP</b> to allow the remote host coming from a specific subnet. An IP address entered in this field and a selected <b>Subnet Mask</b> to compose the subnet.
<b>Service Port</b>	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. <b><u>Value Range:</u></b> 1 ~ 65535.
<b>Enabling the rule</b>	Unchecked by default	Click <b>Enable</b> box to activate this rule.
<b>Save</b>	N/A	Click <b>Enable</b> box to activate this rule then save the settings.
<b>Undo</b>	N/A	Click <b>Undo</b> 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 set up these configurations in the "Configure & Manage" section.



# EW200 Industrial Cellular Gateway

## 6.1.1 Command Script

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

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

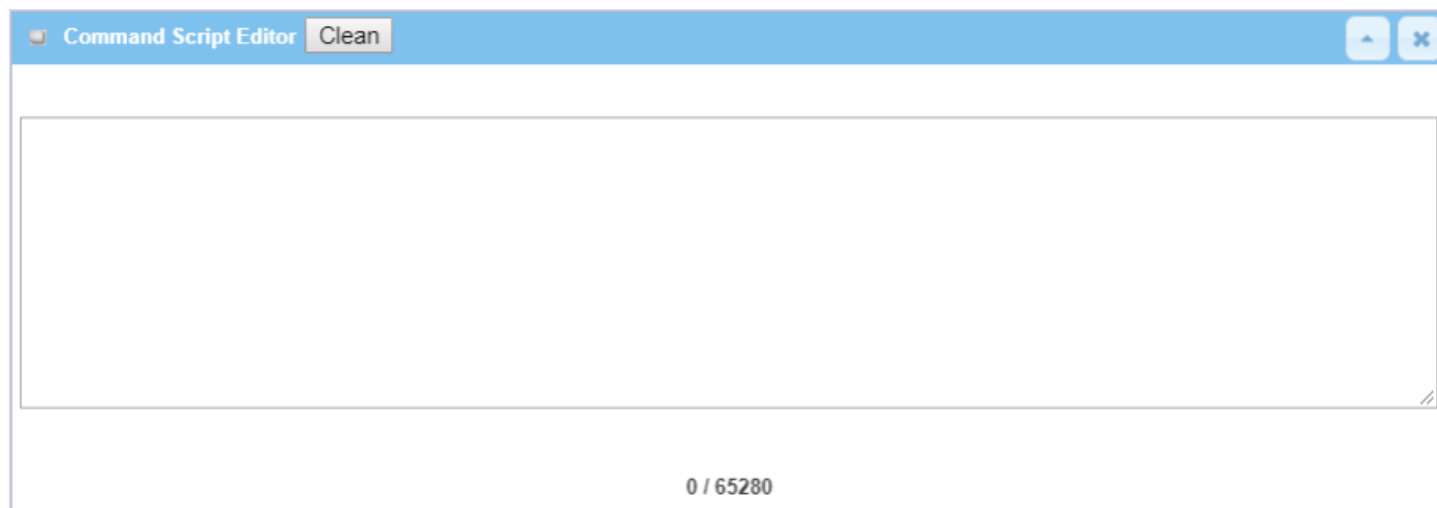
### Enable Command Script Configuration

Configuration	
Item	Setting
▶ Command Script	<input type="checkbox"/> Enable
▶ Backup Script	Via Web UI
▶ Upload Script	Via Web UI
▶ Script Name	<input type="text"/>
▶ Version	<input type="text"/>
▶ Description	<div></div>
▶ Update time	2019-04-08T18:05:31

Configuration		
Item	Value setting	Description
Command Script	Unchecked by default	Check the <b>Enable</b> box to activate the Command Script function.
Backup Script	N/A	Click the <b>Via Web UI</b> or <b>Via Storage</b> button to back up the existing command script in a .txt file. You can specify the script file name in <b>Script Name</b> below.
Upload Script	N/A	Click the <b>Via Web UI</b> or <b>Via Storage</b> button to Upload the existing command script from a specified .txt file.
Script Name	1. Optional setting 2. Any valid file name	Specify a script file name for script backup, or display the selected upload script file name. <b><u>Value Range:</u></b> 0 ~ 32 characters.
Version	1. Optional setting 2. Any string	Specify the version number for the applied Command script. <b><u>Value Range:</u></b> 0 ~ 32 characters.
Description	1. Optional setting 2. Any string	Enter a short description for the applied Command script.
Update time	N/A	It records the upload time for last command script upload.

# EW200 Industrial Cellular Gateway

## Edit/Backup Plain Text Command Script



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

Plain Text Configuration		
Item	Value setting	Description
Clean	NA	Clean text area. (Click <b>Save</b> button to further clean the configuration already saved in the system.)
Backup	NA	Back up 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 configuration with the **STARTUP** command. For configurations without a corresponding Linux command set to configure, you can configure them with a proprietary command set.

Configuration Content		
Key	Value setting	Description
OPENVPN_ENABLED	1: enable 0: disable	Enable or disable OpenVPN Client function.
OPENVPN_DESCRIPTION	Required Setting	Specify the tunnel name for the OpenVPN Client connection.
OPENVPN_PROTO	udp tcp	Define the <b>Protocol</b> for the OpenVPN Client. <ul style="list-style-type: none"><li>• <b>TCP</b> or <b>TCP /UDP</b> -&gt; OpenVPN will use TCP protocol, and <b>Port</b> will be set to 443.</li><li>• <b>UDP</b> -&gt; OpenVPN will use UDP protocol, and <b>Port</b> will be set to 1194.</li></ul>
OPENVPN_PORT	Required Setting	Specify the <b>Port</b> for the OpenVPN Client to use.
OPENVPN_REMOTE_IPADDR	IP or FQDN	Specify the <b>Remote IP/FQDN</b> of the peer OpenVPN Server for this OpenVPN Client tunnel. Enter 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 <b>LZO Compression</b> algorithm for OpenVPN client.

# EW200 Industrial Cellular Gateway

OPENVPN_AUTH	Static Key/TLS	Specify the authorization mode for the OpenVPN tunnel. <ul style="list-style-type: none"><li>• <b>TLS</b> -&gt; OpenVPN will use TLS authorization mode, and the following items <b>CA Cert.</b>, <b>Client Cert.</b> and <b>Client Key</b> need to be specified as well.</li></ul>
OPENVPN_CA_CERT	Required Setting	Specify the Trusted CA certificate for the OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_CERT	Required Setting	Specify the local certificate for OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_KEY	Required 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.
PPP_PING	0: DNS Query 1: ICMP Query	With <b>DNS Query</b> , the system checks the connection by sending DNS Query packets to the destination specified in PPP_PING_IPADDR. With <b>ICMP Query</b> , 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 requests.
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; the STARTUP command. For example, STARTUP=#!/bin/sh STARTUP=echo "startup done" > /tmp/demo

## Plain Text System Configuration with Telnet

In addition to the web-style plain text configuration as mentioned above, the gateway system also allows configuration via Telnet CLI. The 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: <i>txtConfig clone /tmp/config</i> ) 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	an existing file	Commit the configuration content to database. (ex: <i>txtConfig commit /tmp/config</i> )
enable	NA	Enable plain text system config. (ex: <i>txtConfig enable</i> )
disable	NA	Disable plain text system config.

# EW200 Industrial Cellular Gateway

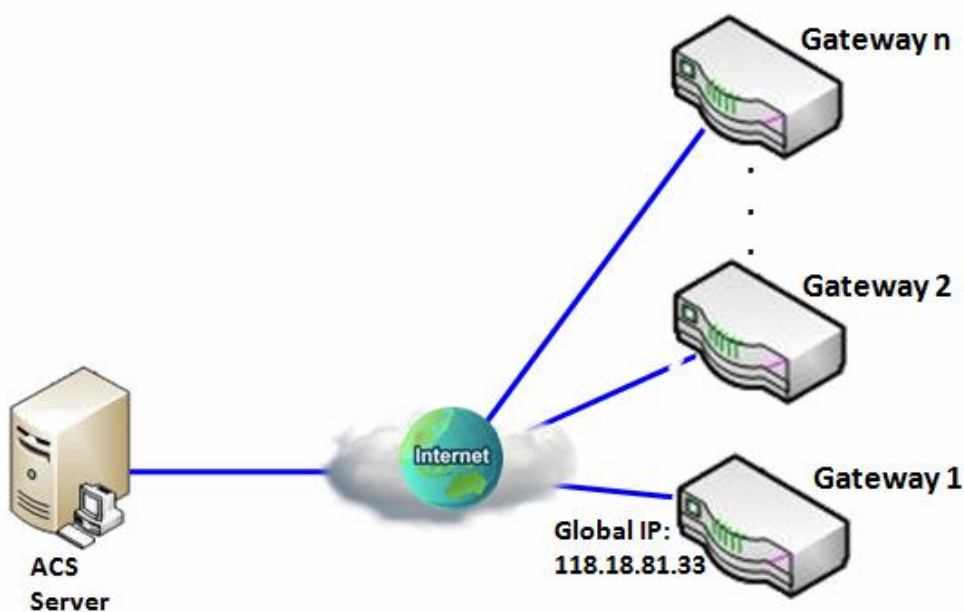
		(ex: <i>txtConfig disable</i> )
<b>run_immediately</b>	NA	Apply the configuration content that has been committed in database. (ex: <i>txtConfig run_immediately</i> )
<b>run_immediately</b>	an existing file	Assign a configuration file to apply. (ex: <i>txtConfig run_immediately /tmp/config</i> )

## 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 recommended 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 lets 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.

# EW200 Industrial Cellular Gateway

---

## 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.

## Parameter Setup Example

The following table lists the parameter configuration as an example for the Gateway 1 in above diagram with "TR-069" enabling.

Configuration Path	[TR-069]-[Configuration]
TR-069	■ Enable
ACS URL	http://qa.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.

# EW200 Industrial 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.

### Enable TR-069

Configuration <span>[ Help ]</span>	
Item	Setting
▶ TR-069	<input type="checkbox"/> Enable
▶ Interface	WAN-1 ▼
▶ Data model	ACS Cloud Data Model ▼
▶ ACS URL	<input type="text"/>
▶ ACS UserName	<input type="text"/>
▶ ACS Password	<input type="password"/>
▶ Connection Request Port	8099
▶ Connection Request UserName	<input type="text"/>
▶ Connection Request Password	<input type="password"/>
▶ Inform	<input checked="" type="checkbox"/> Enable Interval <input type="text" value="300"/>
▶ Certification Setup	<input checked="" type="radio"/> default <input type="radio"/> Select from Certificate List Certificate: <input type="text"/>

# EW200 Industrial Cellular Gateway

TR-069		
Item	Value setting	Description
<b>TR-069</b>	The box is unchecked by default	Check the <b>Enable</b> box to activate TR-069 function.
<b>Interface</b>	<b>WAN-1</b> 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"
<b>Data Model</b>	<b>ACS Cloud Data Model</b> is selected by default.	Select the TR-069 data model for the remote management. <b>Standard</b> : the ACS Server is a standard one, which is fully comply with TR-069. <b>ACS Cloud Data Model</b> : Select this data model if you intend to use a Cloud ACS Server to managing the deployed gateways.
<b>ACS URL</b>	Required setting	You can ask ACS manager to provide ACS URL and manually set
<b>ACS Username</b>	Required setting	You can ask ACS manager to provide ACS username and manually set
<b>ACS Password</b>	Required setting	You can ask ACS manager to provide ACS password and manually set
<b>ConnectionRequest Port</b>	1. Required setting. 2. <b>By default 8099 is set.</b>	You can ask ACS manager to provide ACS ConnectionRequest Port and manually set <u>Value Range</u> : 0 ~ 65535.
<b>ConnectionRequest UserName</b>	Required setting	You can ask ACS manager to provide ACS ConnectionRequest Username and manually set
<b>ConnectionRequest Password</b>	Required setting	You can ask ACS manager to provide ACS ConnectionRequest Password and manually set
<b>Inform</b>	1. The box is checked by default. 2. <b>The Interval value is 300 by default.</b>	When the <b>Enable</b> box is checked, the gateway (CPE) will periodically send inform message to ACS Server according to the <b>Interval</b> setting. <u>Value Range</u> : 0 ~ 86400 for Inform Interval.
<b>Certification Setup</b>	The <b>default</b> box is selected by default	You can leave it as <b>default</b> or select an expected certificate and key from the drop down list. Refer to <b>Object Definition &gt; Certificate</b> Section for the Certificate configuration.
<b>Save</b>	N/A	Click <b>Save</b> to save the settings.
<b>Undo</b>	N/A	Click <b>Undo</b> to cancel the modifications.

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

When you finish set **ConnectionRequest Port ConnectionRequest Username ConnectionRequest Password**, ACS Server can ask the gateway (CPE) to send informs to ACS Server.

# EW200 Industrial Cellular Gateway

## Enable STUN Server

STUN Settings [ Help ]	
Item	Setting
▶ STUN	<input checked="" type="checkbox"/> Enable
▶ Server Address	<input type="text"/>
▶ Server Port	<input type="text" value="3478"/> (1~65535)
▶ Keep Alive Period	<input type="text" value="0"/> (0~65535)second(s)

STUN Settings Configuration		
Item	Value setting	Description
STUN	The box is checked by default	Check the <b>Enable</b> box to activate STUN function.
Server Address	1. String format: any IPv4 address 2. It is an optional item.	Specify the IP address for the expected STUN Server.
Server Port	1. An optional setting 2. <b>3478</b> is set by default	Specify the port number for the expected STUN Server. <u>Value Range:</u> 1 ~ 65535.
Keep Alive Period	1. An optional setting 2. <b>0</b> is set by default	Specify the keep alive time period for the connection with STUN Server. <u>Value Range:</u> 0 ~ 65535.
Save	N/A	Click <b>Save</b> to save the settings.
Undo	N/A	Click <b>Undo</b> to cancel the modifications.



# EW200 Industrial Cellular Gateway

## 6.1.3 SNMP

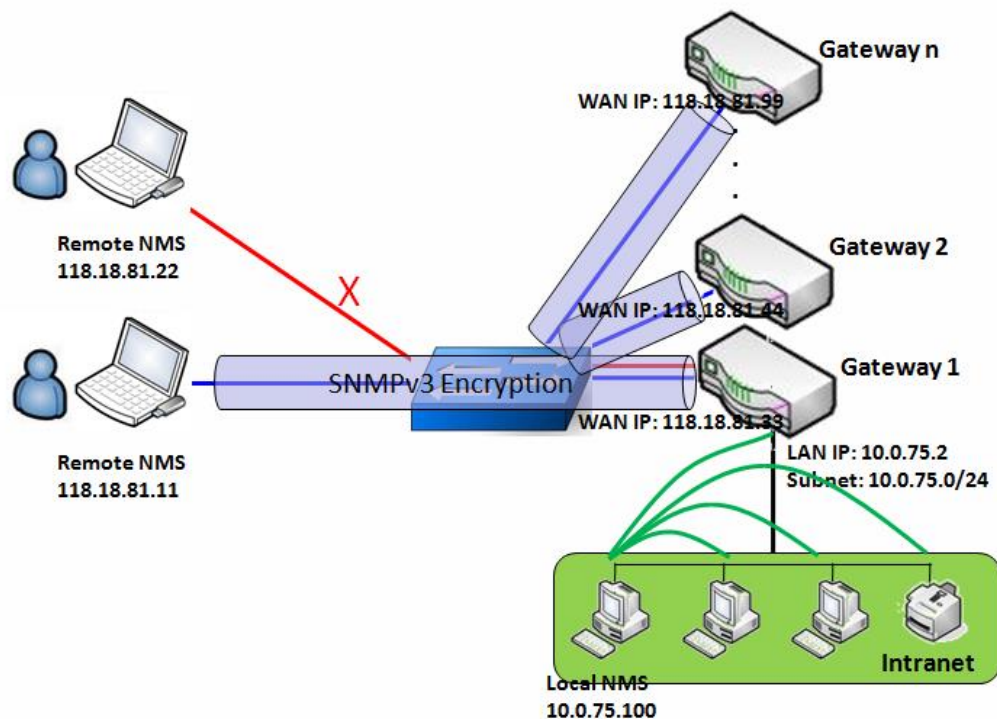
SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

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 deliver management data to 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 (ETHERWAN Private MIB)

### SNMP Management Scenario



### Scenario Application Timing

There are two application scenarios for SNMP Network Management Systems (NMS). Local NMS is in the Intranet and manages all devices that support SNMP. Another is using Remote NMS to manage devices whose WAN interfaces are connected together by a switch or a router with UDP forwarding.

# EW200 Industrial Cellular Gateway

## 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 the other remote NMS can't.

## Parameter Setup Example

Following tables list the parameter configuration as an example for the Gateway 1 in the above diagram with "SNMP" enabling at LAN and WAN interfaces.

Use default value for 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 the above diagram, the NMS server can manage multiple devices in the Intranet or a UDP-reachable network. "Gateway 1" is one of the managed devices, and 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 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 for that with SNMP set commands. The "UserName1" account is used if the manager uses SNMPv3 protocol for configuring "Gateway 1". Only the "UserName1" account can let "Gateway 1" accept the configuration from the NMS since the

## EW200 Industrial Cellular Gateway

---

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.

The remote NMS without privilege IP address can't manage "Gateway 1", since "Gateway 1" allows only the NMS with privilege IP address can manage it via its WAN interface.




# EW200 Industrial Cellular Gateway

## SNMP Setting

Go to **Administration > Configure & Manage > SNMP** tab.

The SNMP tab allows user to configure SNMP relevant settings, including interface, version, access control and trap receiver.

### Enable SNMP

 Configuration  

Item	Setting																				
▶ SNMP Enable	<input checked="" type="checkbox"/> LAN <input type="checkbox"/> WAN																				
▶ WAN Interface	All WANs ▼																				
▶ Supported Versions	<input checked="" type="checkbox"/> v1 <input checked="" type="checkbox"/> v2c <input type="checkbox"/> v3																				
▶ SNMP Port	161																				
▶ Limited Remote Access IP	<div>IP Range ▼</div> <table><tbody><tr><td><input type="text"/></td><td>-</td><td><input type="text"/></td><td><input type="checkbox"/> Enable</td></tr><tr><td><input type="text"/></td><td>-</td><td><input type="text"/></td><td><input type="checkbox"/> Enable</td></tr><tr><td><input type="text"/></td><td>-</td><td><input type="text"/></td><td><input type="checkbox"/> Enable</td></tr><tr><td><input type="text"/></td><td>-</td><td><input type="text"/></td><td><input type="checkbox"/> Enable</td></tr><tr><td><input type="text"/></td><td>-</td><td><input type="text"/></td><td><input type="checkbox"/> Enable</td></tr></tbody></table>	<input type="text"/>	-	<input type="text"/>	<input type="checkbox"/> Enable	<input type="text"/>	-	<input type="text"/>	<input type="checkbox"/> Enable	<input type="text"/>	-	<input type="text"/>	<input type="checkbox"/> Enable	<input type="text"/>	-	<input type="text"/>	<input type="checkbox"/> Enable	<input type="text"/>	-	<input type="text"/>	<input type="checkbox"/> Enable
<input type="text"/>	-	<input type="text"/>	<input type="checkbox"/> Enable																		
<input type="text"/>	-	<input type="text"/>	<input type="checkbox"/> Enable																		
<input type="text"/>	-	<input type="text"/>	<input type="checkbox"/> Enable																		
<input type="text"/>	-	<input type="text"/>	<input type="checkbox"/> Enable																		
<input type="text"/>	-	<input type="text"/>	<input type="checkbox"/> Enable																		

SNMP Item	Value setting	Description
SNMP Enable	1. Boxes are unchecked by default	Select the interface for the SNMP and enable SNMP functions. When <b>LAN</b> box is checked, it will activate SNMP functions and you can access SNMP from LAN side; When <b>WAN</b> box is checked, it will activate SNMP functions and you can access SNMP from WAN side.
WAN Interface	1. Required setting 2. <b>ALL WANs is selected by default</b>	Specify the WAN interface that a remote SNMP host can use to access the device. By default, <b>All WANs</b> is selected, and there is no limitation for the WAN interface.
Supported Versions	1. Required setting 2. The boxes are unchecked by default	Select the version for the SNMP When <b>v1</b> box is checked, you can access SNMP version 1. When <b>v2</b> box is checked, you can access SNMP version 2. When <b>v3</b> box is checked, you can access SNMP version 3.
SNMP Port	1. String format: any port number 2. The default SNMP	Specify the <b>SNMP Port</b> . Enter any port number. But you must ensure the port number is not to be used.

# EW200 Industrial Cellular Gateway

	port is <b>161</b> . 3. Required setting	<u>Value Range</u> : 1 ~ 65535.
<b>Limited Remote Access IP</b>	1. String format: any IPv4 address 2. Optional item	Specify the <b>Remote Access IP</b> for WAN and check the box to enable it as well. Select <b>Specific IP Address</b> , and fill in a specific IP address. It means only this IP address can access SNMP from LAN/WAN side. Select <b>IP Range</b> , and fill in a range of IP addresses. It means the IP address within specified range can access SNMP from LAN/WAN side. If you leave it blank, it means any IP address can access SNMP from WAN side.
<b>Save</b>	N/A	Click <b>Save</b> to save the settings
<b>Undo</b>	N/A	Click <b>Undo</b> to cancel the settings

## Create/Edit Multiple Community

The SNMP allows you to customize your access control for version 1 and version 2 users. The router supports up to a maximum of 10 community sets.

Multiple Community List <input type="button" value="Add"/> <input type="button" value="Delete"/>			
ID	Community	Enable	Actions

When the **Add** button is applied, the **Multiple Community Rule Configuration** screen will appear.

Multiple Community Rule Configuration	
Item	Setting
▶ Community	Read Only ▼ <input type="text"/>
▶ Enable	<input checked="" type="checkbox"/> Enable
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Back"/>	

Multiple Community Rule Configuration		
Item	Value setting	Description
<b>Community</b>	1. <b>Read Only</b> is selected by default 2. Required 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.
<b>Enable</b>	1. Box is checked by default	Click Enable to enable this version 1 or version v2c user.
<b>Save</b>	N/A	Click the <b>Save</b> 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"

# EW200 Industrial Cellular Gateway

		button to apply your changes” to remind the user to click the main page Save button.
<b>Undo</b>	N/A	Click the <b>Undo</b> button to cancel the settings.
<b>Back</b>	N/A	Click the <b>Back</b> button to return to last page.

## Create/Edit User Privacy

The SNMP allows you to customize your access control for version 3 users. The router supports up to a maximum of 128 User Privacy sets.

User Privacy List <input type="button" value="Add"/> <input type="button" value="Delete"/>										
ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	OID Filter Prefix	Enable	Actions

When the **Add** button is applied, **User Privacy Rule Configuration** screen will appear.

User Privacy Rule Configuration	
Item	Setting
▶ User Name	<input type="text"/>
▶ Password	<input type="password"/>
▶ Authentication	<input type="text" value="None"/>
▶ Encryption	<input type="text" value="None"/>
▶ Privacy Mode	<input type="text" value="noAuthNoPriv"/>
▶ Privacy Key	<input type="password"/>
▶ Authority	<input type="text" value="Read"/>
▶ OID Filter Prefix	<input type="text" value="1"/>
▶ Enable	<input checked="" type="checkbox"/> Enable

User Privacy Rule Configuration		
Item	Value setting	Description
<b>User Name</b>	1. Required setting 2. String format: any text	Specify the <b>User Name</b> for this version 3 user. <b><u>Value Range:</u></b> 1 ~ 32 characters.
<b>Password</b>	1. String format: any text	When your <b>Privacy Mode</b> is <b>authNoPriv</b> or <b>authPriv</b> , specify the <b>Password</b> for this version 3 user. <b><u>Value Range:</u></b> 8 ~ 64 characters.

# EW200 Industrial Cellular Gateway

<b>Authentication</b>	1. <b>None</b> is selected by default	When your <b>Privacy Mode</b> is <b>authNoPriv</b> or <b>authPriv</b> , specify the <b>Authentication</b> types for this version 3 user. Selected the authentication types <b>MD5/ SHA-1</b> to use.
<b>Encryption</b>	1. <b>None</b> is selected by default	When your <b>Privacy Mode</b> is <b>authPriv</b> , specify the <b>Encryption</b> protocols for this version 3 user. Selected the encryption protocols <b>DES / AES</b> to use.
<b>Privacy Mode</b>	1. <b>noAuthNoPriv</b> is selected by default	Specify the <b>Privacy Mode</b> for this version 3 user. <b>noAuthNoPriv</b> . No authentication types or encryption protocols are used. <b>authNoPriv</b> . Specify the Authentication and Password. <b>authPriv</b> . Specify the Authentication, Password, Encryption and Privacy Key.
<b>Privacy Key</b>	1. String format: any text	When your <b>Privacy Mode</b> is <b>authPriv</b> , specify the <b>Privacy Key</b> (8 ~ 64 characters) for this version 3 user.
<b>Authority</b>	1. <b>Read</b> is selected by default	Specify this version 3 user's <b>Authority</b> that will be allowed <b>Read Only</b> (GET and GETNEXT) or <b>Read-Write</b> (GET, GETNEXT and SET) access respectively.
<b>OID Filter Prefix</b>	1. Default value is 1 2. Required setting 3. String format: any legal OID	The <b>OID Filter Prefix</b> restricts access for this version 3 user to the sub-tree rooted at the given OID. <b>Value Range:</b> 1 ~2080768.
<b>Enable</b>	1.The box is checked by default	Click <b>Enable</b> to enable this version 3 user.
<b>Save</b>	N/A	Click the <b>Save</b> 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" to remind the user to click the main page <b>Save</b> button.
<b>Undo</b>	N/A	Click the <b>Undo</b> button to cancel the settings
<b>Back</b>	N/A	Click the <b>Back</b> button to return the last page.

## Create/Edit Trap Event Receiver

The SNMP allows you to customize your trap event receiver. The router supports up to a maximum of 4 Trap Event Receiver sets.

Trap Event Receiver List <span>Add</span> <span>Delete</span>												
ID	Server IP	Server Port	SNMP Version	Community Name	User Name	Password	Privacy Mode	Authentication	Encryption	Privacy Key	Enable	Actions

When the **Add** button is applied, the **Trap Event Receiver Rule Configuration** screen will appear. The default SNMP Version is v1. The configuration screen will provide the version 1 required items.

# EW200 Industrial Cellular Gateway

Trap Event Receiver Rule Configuration	
Item	Setting
▶ Server IP	<input type="text"/> (IP Address/FQDN)
▶ Server Port	<input type="text" value="162"/>
▶ SNMP Version	v1 ▼
▶ Community Name	<input type="text"/>
▶ Enable	<input checked="" type="checkbox"/> Enable

When v2c is selected, the configuration screen is exactly the same as that of v1, except the version.

When v3 is selected, the configuration screen will provide more setting items for the version 3 Trap.

Trap Event Receiver Rule Configuration	
Item	Setting
▶ Server IP	<input type="text"/> (IP Address/FQDN)
▶ Server Port	<input type="text" value="162"/>
▶ SNMP Version	v3 ▼
▶ Community Name	<input type="text"/>
▶ User Name	<input type="text"/>
▶ Password	<input type="text"/>
▶ Privacy Mode	noAuthNoPriv ▼
▶ Authentication	None ▼
▶ Encryption	None ▼
▶ Privacy Key	<input type="text"/>
▶ Enable	<input checked="" type="checkbox"/> Enable

Trap Event Receiver Rule Configuration		
Item	Value setting	Description
Server IP	1. Required setting 2. String format: any IPv4 address or FQDN	Specify the trap <b>Server IP</b> or <b>FQDN</b> . Trap will be sent to the server IP/FQDN.
Server Port	1. String format: any port number 2. The default SNMP trap port is 162 3. Required setting	Specify the trap <b>Server Port</b> . Enter any port number. But you must ensure the port number is not to be used. <u>Value Range</u> : 1 ~ 65535.



# EW200 Industrial Cellular Gateway

<b>SNMP Version</b>	1. <b>v1</b> is selected by default	<p>Select the version for the trap</p> <p><b>v1</b> The configuration screen will provide the version 1 required items.</p> <p><b>v2c</b> The configuration screen will provide the version 2c required items.</p> <p><b>v3</b> The configuration screen will provide the version 3 required items.</p>
<b>Community Name</b>	1. <b>v1</b> and <b>v2c</b> Required setting 2. String format: any text	<p>Specify the <b>Community Name</b> for this version 1 or version v2c trap.</p> <p><b><u>Value Range:</u></b> 1 ~ 32 characters.</p>
<b>User Name</b>	1. <b>v3</b> Required setting 2. String format: any text	<p>Specify the <b>User Name</b> for this version 3 trap.</p> <p><b><u>Value Range:</u></b> 1 ~ 32 characters.</p>
<b>Password</b>	1. <b>v3</b> Required setting 2. String format: any text	<p>When your <b>Privacy Mode</b> is <b>authNoPriv</b> or <b>authPriv</b>, you must specify the <b>Password</b> for this version 3 trap.</p> <p><b><u>Value Range:</u></b> 8 ~ 64 characters.</p>
<b>Privacy Mode</b>	1. <b>v3</b> Required setting 2. <b>noAuthNoPriv</b> is selected by default	<p>Specify the <b>Privacy Mode</b> for this version 3 trap.</p> <p>Selected the <b>noAuthNoPriv</b>. You do not use any authentication types and encryption protocols.</p> <p>Selected the <b>authNoPriv</b>. You must specify the <b>Authentication</b> and <b>Password</b>.</p> <p>Selected the <b>authPriv</b>. You must specify the Authentication, Password, Encryption and Privacy Key.</p>
<b>Authentication</b>	1. <b>v3</b> Required setting 2. <b>None</b> is selected by default	<p>When your <b>Privacy Mode</b> is <b>authNoPriv</b> or <b>authPriv</b>, you must specify the <b>Authentication</b> types for this version 3 trap.</p> <p>Selected the authentication types <b>MD5/ SHA-1</b> to use.</p>
<b>Encryption</b>	1. <b>v3</b> Required setting 2. <b>None</b> is selected by default	<p>When your <b>Privacy Mode</b> is <b>authPriv</b>, you must specify the <b>Encryption</b> protocols for this version 3 trap.</p> <p>Selected the encryption protocols <b>DES / AES</b> to use.</p>
<b>Privacy Key</b>	1. <b>v3</b> Required setting 2. String format: any text	<p>When your <b>Privacy Mode</b> is <b>authPriv</b>, you must specify the <b>Privacy Key</b> (8 ~ 64 characters) for this version 3 trap.</p>
<b>Enable</b>	Box is checked by default	Click <b>Enable</b> to enable this trap receiver.
<b>Save</b>	N/A	Click the <b>Save</b> 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" to remind the user to click the main page <b>Save</b> button.
<b>Undo</b>	N/A	Click the <b>Undo</b> button to cancel the settings.
<b>Back</b>	N/A	Click the <b>Back</b> button to return the last page.

# EW200 Industrial Cellular Gateway

## Specify SNMP MIB-2 System

If required, you can also specify the required information for the MIB-2 System.

SNMP MIB-2 System		
Item	Setting	
▶ sysContact	<input type="text"/>	
▶ sysLocation	<input type="text"/>	

SNMP MIB-2 System Configuration		
Item	Value setting	Description
sysContact	1. Optional setting 2. String format: any text	Specify the contact information for MIB-2 system. <b><u>Value Range:</u></b> 0 ~ 64 characters.
sysLocation	1. Optional setting 2. String format: any text	Specify the location information for MIB-2 system. <b><u>Value Range:</u></b> 0 ~ 64 characters.

## Edit SNMP Options

If you use some particular private MIB, you must enter the enterprise name, number and OID.

Options		
Item	Setting	
▶ Enterprise Name	<input type="text" value="EtherWAN"/>	
▶ Enterprise Number	<input type="text" value="2736"/>	
▶ Enterprise OID	1.3.6.1.4.1.	<input type="text" value="2736.4"/>

Options		
Item	Value setting	Description
Enterprise Name	1. The default value is Etherwan 2. Required setting 3. String format: any text	Specify the <b>Enterprise Name</b> for the particular private MIB. <b><u>Value Range:</u></b> 1 ~ 10 characters, and only string with A~Z, a~z, 0~9, '-', '_'.
Enterprise Number	The default value is <b>2736</b> 2. Required setting 3. String format: any number	Specify the <b>Enterprise Number</b> for the particular private MIB. <b><u>Value Range:</u></b> 1 ~ 2080768.

## EW200 Industrial Cellular Gateway

---

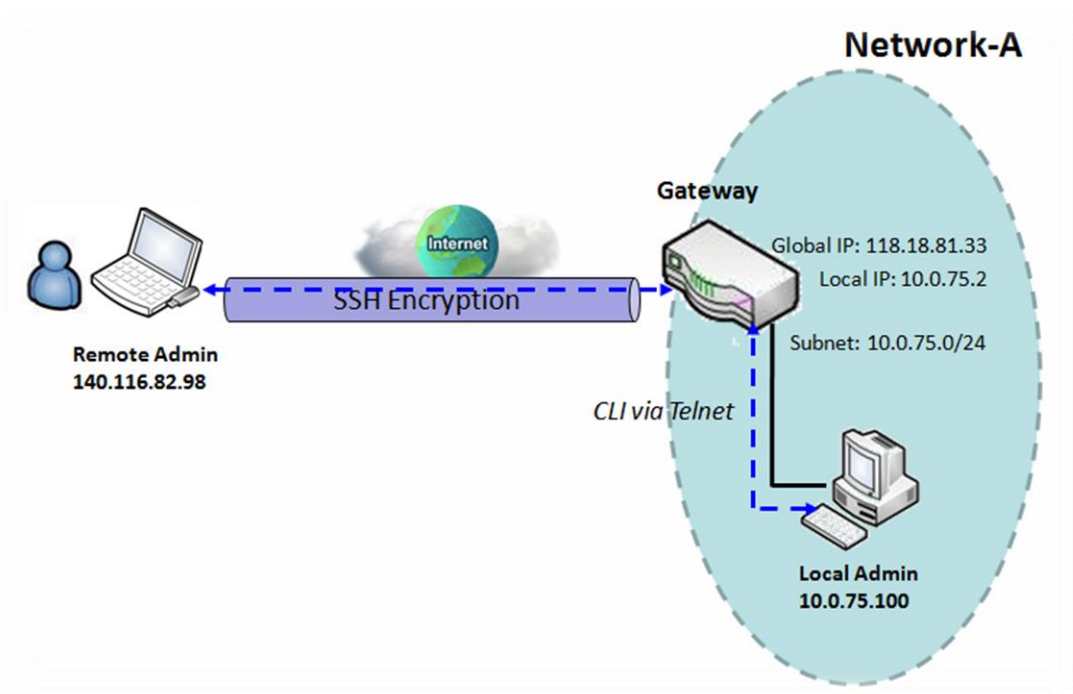
<b>Enterprise OID</b>	<ol style="list-style-type: none"><li>1. The default value is <b>1.3.6.1.4.1.2736.4</b></li><li>2. Required setting</li><li>3. String format: any legal OID</li></ol>	<p>Specify the <b>Enterprise OID</b> for the particular private MIB.</p> <p>The range of the each OID number is 1-2080768.</p> <p>The maximum length of the enterprise OID is 31.</p> <p>The seventh number must be identical with the enterprise number.</p>
<b>Save</b>	N/A	Click the <b>Save</b> button to save the configuration and apply your changes to SNMP functions.
<b>Undo</b>	N/A	Click the <b>Undo</b> button to cancel the settings.

# EW200 Industrial 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/she 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 text or encrypted text. It is suggested to use plain text in the Intranet for Local Admin to use Telnet, and encrypted text in the Internet for Remote Admin to use SSH.

# EW200 Industrial Cellular Gateway

---

## Parameter Setup Example

The following table lists the parameter configuration as an example for the Gateway in the above diagram with "Telnet with CLI" enabled at LAN and WAN interfaces.

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

<b>Configuration Path</b>	[Telnet with CLI]-[Configuration]
<b>Telnet with CLI</b>	LAN: ■ <b>Enable</b> WAN: ■ <b>Enable</b>
<b>Connection Type</b>	Telnet: Service Port <b>23</b> ■ <b>Enable</b> SSH: Service Port <b>22</b> ■ <b>Enable</b>

## Scenario Operation Procedure

In the above diagram, "Local Admin" or "Remote Admin" can manage the "Gateway" from 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 with a privileged account to log in to the Gateway.

The "Remote Admin" in the Internet uses SSH with a privileged account to log in to the Gateway.

# EW200 Industrial Cellular Gateway

## Telnet & SSH Setting

Go to **Administration > Configure & Manage > Telnet & SSH** tab.

The Telnet & SSH setting allows administrator to access this device through the traditional Telnet or SSH Telnet program. Before you can Telnet (login) to the device, configure the related settings and password carefully. The password management part allows you to set a root password for logging in with Telnet and SSH.

Configuration Save Undo

Item	Setting
Telnet	LAN <input checked="" type="checkbox"/> Enable WAN <input type="checkbox"/> Enable ( WAN-1 <input checked="" type="checkbox"/> WAN-4 <input type="checkbox"/> ) <div></div> Service Port <input type="text" value="23"/>
SSH	LAN <input checked="" type="checkbox"/> Enable WAN <input type="checkbox"/> Enable ( WAN-1 <input checked="" type="checkbox"/> WAN-4 <input type="checkbox"/> ) <div></div> Service Port <input type="text" value="22"/>

Configuration		
Item	Value setting	Description
Telnet	<div>1. The LAN Enable box is checked by default.</div> <div>2. The default <b>Service Port</b> is 23</div>	<div>Check the <b>Enable</b> box to activate the Telnet with CLI function for connecting from WAN/LAN interfaces.</div> <div>You can set which number of <b>Service Port</b> you want to provide for the corresponding service.</div> <div>Value Range: 1 ~65535.</div>
SSH	<div>1. The LAN Enable box is checked by default.</div> <div>2. The default <b>Service Port</b> is 22</div>	<div>Check the <b>Enable</b> box to activate the SSH Telnet function for connecting from LAN or WAN interfaces.</div> <div>You can set which number of <b>Service Port</b> you want to provide for the corresponding service.</div> <div>Value Range: 1 ~65535.</div>
Save	N/A	Click <b>Save</b> to save the settings
Undo	N/A	Click <b>Undo</b> to cancel the settings

# EW200 Industrial Cellular Gateway

Password Management		Save	Undo
Item	Setting		
▶ root	Old Password : <input type="text"/>		
	New Password : <input type="text"/>		
	New Password Confirmation : <input type="text"/>		

Configuration		
Item	Value setting	Description
root	1. String: any text but no blank characters 2. The default password for Telnet is 'wirelessm2m'.	Type old password and specify new password to change the root password. <b>Note: It is highly recommended to change the default Telnet password before deploying the device.</b> <b>Note_2: If you have trouble for the default password for a previous firmware version, please check the corresponding user manual to get the correct one.</b>
Save	N/A	Click <b>Save</b> to save the settings
Undo	N/A	Click <b>Undo</b> to cancel the settings

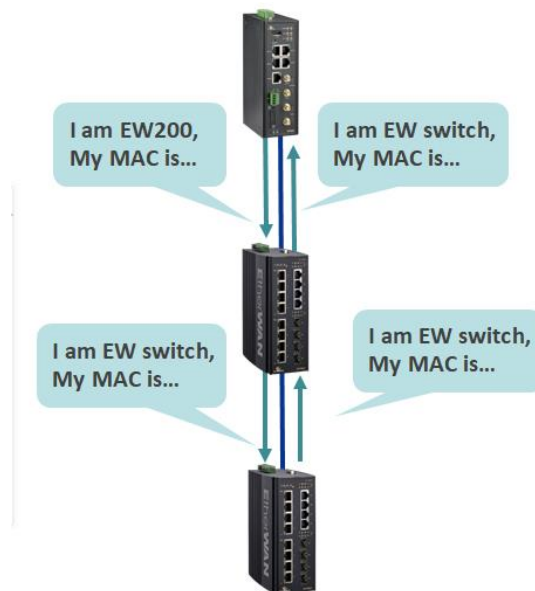
# EW200 Industrial Cellular Gateway

## 6.1.5 LLDP

LLDP is a network discovery protocol that defines a method for network access devices using Ethernet connectivity to advertise information about devices to peer devices on the same physical LAN and store information about the network. It allows a device to learn higher layer management reachability and connection endpoint information from adjacent devices.

Using LLDP, a device is able to advertise its own identification information, its capabilities and media-specific configuration information, as well as learn the same information from the devices connected to it. LLDP advertises this information over Logical Link-Layer Control frames and the information received from other agents in IEEE-defined Management Information Bases (MIB) modules.

LLDP significantly aids in the deployment of any network device that supports the protocol. As a media independent protocol intended to be run on all IEEE 802 devices, LLDP may be used to discover routers, bridges, repeaters, WLAN APs, IP telephones, network camera or any LLDP-enabled device, regardless of manufacturer. Since LLDP runs over the data-link layer only, a switch running one network layer protocol can discover and learn about an access device running a different network layer protocol.



**Note:** If you are using EtherWAN's eVue network management utility, then make sure that LLDP is enabled on this and all other devices that you want to monitor with the software. eVue uses LLDP for its topology visualization.

To enable LLDP, check the box next to **Enable**, and then click **Save**.

Command Script TR-069 SNMP Telnet & SSH **LLDP**

Configuration

Item	Setting
LLDP	<input checked="" type="checkbox"/> Enable

Save Undo



# EW200 Industrial Cellular Gateway

## 6.2 System Operation

System Operation allows the network administrator to manage system and settings such as web-based utility, 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.

#### Setup Host Name

The Host Name screen allows network administrator to setup / change the host name of the gateway. Click the **Modify** button and provide the new username setting.

Host Name

Item	Setting
Host Name	<input type="text"/>

Host Name Configuration		
Item	Value Setting	Description
Host Name	1. Optional setting 2. Blank by default	Enter the host name of the gateway.
Save	N/A	Click <b>Save</b> button to save the settings
Undo	N/A	Click <b>Undo</b> button to cancel the settings

#### Change UserName

The Username screen allows the network administrator to change the web-based MMI login account to access gateway. Click the **Modify** button and provide the new username setting.

Username

Item	Setting
Username	admin <div>Modify</div>
New Username	<input type="text"/>
Password	<input type="text"/>

# EW200 Industrial Cellular Gateway

Username Configuration		
Item	Value Setting	Description
<b>Username</b>	1. The default Username for web-based MMI is <b>admin</b> .	Display the current MMI login account (Username).
<b>New Username</b>	String: any text	Enter a new Username to replace the current setting.
<b>Password</b>	String: any text	Enter the current password to verify that you have the permission to change the username setting.
<b>Save</b>	N/A	Click <b>Save</b> button to save the settings
<b>Undo</b>	N/A	Click <b>Undo</b> button to cancel the settings

## Change Password

The change password screen allows the network administrator to change the web-based MMI (Man-machine interface) login password.

Password [ Help ]	
Item	Setting
▶ Old Password	<input type="text"/>
▶ New Password	<input type="text"/>
▶ New Password Confirmation	<input type="text"/>

Change Password		
Item	Value Setting	Description
<b>Old Password</b>	1. String: any text 2. Default password is <b>'admin'</b> .	Enter the current password.
<b>New Password</b>	String: any text	Enter new password
<b>New Password Confirmation</b>	String: any text	Enter new password again to confirm
<b>Save</b>	N/A	Click <b>Save</b> button to save the settings
<b>Undo</b>	N/A	Click <b>Undo</b> button to cancel the settings

## Change MMI Setting for Access

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 setting allows administrator to enable automatic logout and set the logout idle time.

# EW200 Industrial Cellular Gateway

MMI

Item	Setting
▶ Login	Password-Guessing Attack & MAX: <input type="text" value="3"/> (times)
▶ Login Timeout	<input checked="" type="checkbox"/> Enable <input type="text" value="300"/> (seconds)
▶ GUI Access Protocol	<input type="text" value="http/https"/>
▶ HTTPs Certificate Setup	<input checked="" type="radio"/> default <input type="radio"/> Select from Certificate List Certificate: <input type="text" value="TrustedCert0"/> Key: <input type="text" value="TrustedKey0"/>
▶ HTTP Compression	<input checked="" type="checkbox"/> gzip <input type="checkbox"/> deflate
▶ HTTP Binding	<input checked="" type="checkbox"/> DHCP 1
▶ System Boot Mode	<input type="text" value="Normal Mode"/>

Web UI		
Item	Value Setting	Description
Login	3 times is set by default	Enter the login trial counting value. <b>Value Range:</b> 3 ~ 10. If someone tries to log in to the web GUI with incorrect password for more than this value, a warning message “ <b>Already reaching maximum Password-Guessing times, please wait a few seconds!</b> ” will display and following login attempts ignored.
Login Timeout	Enable box is unchecked by default	Check the Enable box to activate the auto logout function, and specify the maximum idle time as well. <b>Value Range:</b> 30 ~ 65535.
GUI Access Protocol	http/https is selected by default.	Select the protocol that will be used for GUI access. It can be <b>http/https</b> , <b>http only</b> , or <b>https only</b> .
HTTPs Certificate Setup	The default box is selected by default	If the https Access Protocol is selected, the HTTPs Certificate Setup option will be available for further configuration. You can leave it as default or select an expected certificate and key from the drop down list. Refer to Object <b>Definition &gt; Certificate</b> Section for the Certificate configuration.
HTTP Compression	Unchecked by default	Check the box ( <b>gzip</b> , or <b>deflate</b> ) if any comprerssion method is preferred.
HTTP Binding	1. Optional setting 2. DHCP-1 is checked by default	Select the DHCP Server to bind with http access.
System Boot Mode	Normal Mode is selected by default.	Select the system boot mode that will be adopted to boot up the device. <b>Normal Mode:</b> It takes longer boot up time, with complete firmware image check during the device booting.
Save	N/A	Click <b>Save</b> button to save the settings
Undo	N/A	Click <b>Undo</b> button to cancel the settings

# EW200 Industrial Cellular Gateway

## 6.2.2 System Information

The System Information screen gives the network administrator a quick look up on the device information for the gateway.

Go to **Administration > System Operation > System Information** tab.

System Information	
Item	Setting
▶ Model Name	VHG87BAM_0T001
▶ Device Serial Number	
▶ Kernel Version	2.6.36
▶ FW Version	0000Y90.J31_e32.BETA_04021700
▶ System Time	Thu, 18 Apr 2019 16:18:16 +0800
▶ Device Up-Time	15day 22hr 30min 35sec

System Information		
Item	Value Setting	Description
<b>Model Name</b>	N/A	Displays the model name of this product.
<b>Device Serial Number</b>	N/A	Displays the serial number of this product.
<b>Kernel Version</b>	N/A	Displays the Linux kernel version of the product
<b>FW Version</b>	N/A	Displays the firmware version of the product
<b>System Time</b>	N/A	Displays the current system time that you browsed this web page.
<b>Device Up-Time</b>	N/A	Displays the statistics for the device up-time since last boot up.
<b>Refresh</b>	N/A	Click the <b>Refresh</b> button to update the system Information.

# EW200 Industrial Cellular Gateway

## 6.2.3 System Time

The gateway provides manual setup and auto-synchronized approaches for the administrator to set up the system time for the gateway. The supported time synchronization methods are Time Server, Manual, and PC. Select the method first, and then configure the corresponding settings.

Instead of manually configuring the system time for the gateway, there are two simple and quick solutions to set the correct time as the system time for the gateway.

The first one is “Sync with Timer Server”. Based on your selection of time zone and time server in the above time information configuration window, the system will communicate with time server by NTP Protocol to get system date and time after you click on the **Synchronize immediately** button.

The second one is “Sync with my PC”. Select the method and the system will synchronize its date and time to the time of the administration PC.

Go to **Administration > System Operation > System Time** tab.

### Synchronize with Time Server

Item	Setting
▶ Synchronization method	Time Server ▼
▶ Time Zone	(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼
▶ Auto-synchronization	Time Server: <input type="text"/> Available Time Servers (RFC-868): Auto ▼
▶ Daylight Saving Time	<input type="checkbox"/> Enable
▶ NTP Service	<input type="checkbox"/> Enable
▶ Synchronize immediately	Active

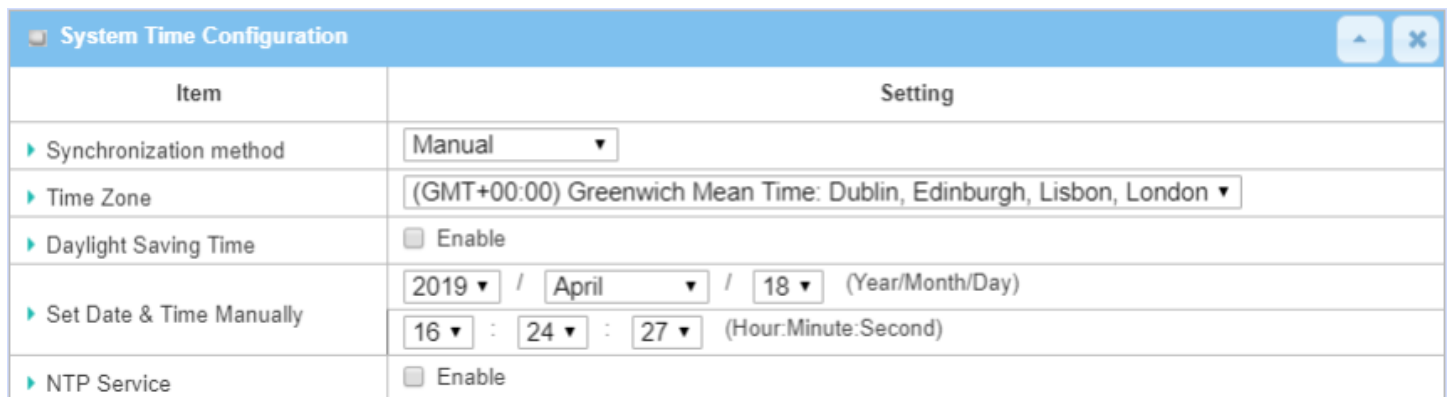
System Time Information		
Item	Value Setting	Description
<b>Synchronization method</b>	1. Required item. 2. <b>Time Server</b> is selected by default.	Select <b>Time Server</b> as the synchronization method for the system time.
<b>Time Zone</b>	1. Required item. 2. <b>GMT+00:00</b> is selected by default.	Select a time zone.
<b>Auto-synchronization</b>	1. Required item. 2. Auto is selected by	Enter the IP or FQDN for the NTP time server, or leave it as auto mode so that available servers will be used for time synchronization.

# EW200 Industrial Cellular Gateway

	default.	
<b>Daylight Saving Time</b>	1. Optional item. 2. Unchecked by default	Check the <b>Enable</b> button to activate the daylight saving function. When this function is enabled, specify the start and end date for the daylight saving time duration.
<b>NTP Service</b>	1. Optional item <b>2. Unchecked by default</b>	Check the <b>Enable</b> button to activate the NTP Service function. When you enable this function, the gateway can provide NTP server service for its local connected devices.
<b>Synchronize immediately</b>	N/A	Click the <b>Active</b> button to synchronize the system time with specified time server immediately.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the settings.
<b>Refresh</b>	N/A	Click the <b>Refresh</b> button to update the system time immediately.

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.

## Synchronize with Manual Setting




A screenshot of the 'System Time Configuration' window. The window has a blue header bar with the title 'System Time Configuration' and two small icons on the right. Below the header is a table with two columns: 'Item' and 'Setting'. The table contains the following rows: 1. 'Synchronization method' with a dropdown menu set to 'Manual'. 2. 'Time Zone' with a dropdown menu showing '(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London'. 3. 'Daylight Saving Time' with a checkbox labeled 'Enable'. 4. 'Set Date & Time Manually' with two rows of input fields: the first row for date (Year: 2019, Month: April, Day: 18) and the second row for time (Hour: 16, Minute: 24, Second: 27). 5. 'NTP Service' with a checkbox labeled 'Enable'.

System Time Information		
Item	Value Setting	Description
<b>Synchronization method</b>	1. Required item. <b>2. Time Server is selected by default.</b>	Select <b>Manual</b> as the synchronization method for the system time.
<b>Time Zone</b>	1. Required item <b>2. Time server is selected by default</b>	Select the time zone where the device is located.
<b>Daylight Saving Time</b>	1. Optional item. 2. Unchecked by default	Check the <b>Enable</b> button to activate the daylight saving function. When this function is enabled, specify the start and end date for the daylight saving time duration.
<b>Set Date &amp; Time Manually</b>	1. Optional item.	Manually set the date (Year/Month/Day) and time (Hour:Minute:Second) as the system time.
<b>NTP Service</b>	1. Optional item	Check the <b>Enable</b> button to activate the NTP Service function.

# EW200 Industrial Cellular Gateway

		When you enable this function, the gateway can provide NTP server service for its local connected devices.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the settings.




## Synchronize with PC

 System Time Configuration  

Item	Setting
▶ Synchronization method	PC ▼
▶ NTP Service	<input type="checkbox"/> Enable
▶ Synchronize immediately	<input type="button" value="Active"/>

System Time Information		
Item	Value Setting	Description
<b>Synchronization method</b>	1. A Required item. 2. <b>Time Server is selected by default.</b>	Select <b>PC</b> as the synchronization method for the system time to let the system synchronize its date and time to the time of the administration PC.
<b>NTP Service</b>	1. Optional item	Check the <b>Enable</b> button to activate the NTP Service function. When you enable this function, the gateway can provide NTP server service for its local connected devices.
<b>Synchronize immediately</b>	N/A	Click the <b>Active</b> button to synchronize the system time with management PC immediately.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the settings.
<b>Refresh</b>	N/A	Click the <b>Refresh</b> button to update the system time immediately.

## Synchronize with Cellular Time Service


 System Time Configuration  

Item	Setting
▶ Synchronization method	Cellular Module ▼
▶ Time Zone	(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼
▶ NTP Service	<input type="checkbox"/> Enable
▶ Synchronize immediately	<input type="button" value="Active"/>

# EW200 Industrial Cellular Gateway

System Time Information		
Item	Value Setting	Description
<b>Synchronization method</b>	1. A Required item. <b>2. Time Server is selected by default.</b>	Select <b>Cellular Module</b> as the synchronization method for the system time to let system synchronize its date and time to the time provided from the connected mobile ISP. Note: this option is only available for products with Cellular WAN interface.
<b>Time Zone</b>	1. Required item <b>2. GMT+00:00 is selected by default</b>	Select the time zone when the device is located.
<b>NTP Service</b>	1. Optional item	Check the <b>Enable</b> button to activate the NTP Service function. When you enable this function, the gateway can provide NTP server service for its local connected devices.
<b>Synchronize immediately</b>	N/A	Click the <b>Active</b> button to synchronize the system time with management PC immediately.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the settings.
<b>Refresh</b>	N/A	Click the <b>Refresh</b> button to update the system time immediately.

## Synchronize with GPS Time Service

System Time Configuration

Item	Setting
▶ Synchronization method	GPS Signal ▼
▶ Time Zone	(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼
▶ NTP Service	<input type="checkbox"/> Enable
▶ Synchronize immediately	<input checked="" type="button" value="Active"/>

System Time Information		
Item	Value Setting	Description
<b>Synchronization method</b>	1. A Required item. <b>2. Time Server is selected by default.</b>	Select <b>GPS Signal</b> as the synchronization method for the system time to let system synchronize its date and time to the time provided from the GNSS service. Note: this option is only available for products with GNSS interface.
<b>Time Zone</b>	1. Required item <b>2. GMT+00:00 is selected by default</b>	Select the time zone when the device is located.
<b>NTP Service</b>	1. Optional item	Check the <b>Enable</b> button to activate the NTP Service function. When you enable this function, the gateway can provide NTP server service for its local connected devices.
<b>Synchronize immediately</b>	N/A	Click the <b>Active</b> button to synchronize the system time with management PC immediately.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the settings.
<b>Refresh</b>	N/A	Click the <b>Refresh</b> button to update the system time immediately.



# EW200 Industrial Cellular Gateway

## 6.2.4 System Log

The system Log screen contains various event log tools to facilitate local event logging and remote reporting.

Go to **Administration > System Operation > System Log** tab.

System Log

View

Email Now

Item	Setting
Web Log Type Category	<input checked="" type="checkbox"/> System <input checked="" type="checkbox"/> Attacks <input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Login message <input type="checkbox"/> Debug
Email Alert	<div><input type="checkbox"/> Enable</div> <div>Server: <div>--- Option ---</div> <div>Add Object</div></div> <div>E-mail Addresses: <div></div></div> <div>Subject: <div></div></div> <div>Log type Category: <input type="checkbox"/> System <input type="checkbox"/> Attacks <input type="checkbox"/> Drop <input type="checkbox"/> Login message <input type="checkbox"/> Debug</div>
Syslogd	<div><input type="checkbox"/> Enable</div> <div>Server: <div>--- Option ---</div> <div>Add Object</div></div> <div>Log type Category: <input type="checkbox"/> System <input type="checkbox"/> Attacks <input type="checkbox"/> Drop <input type="checkbox"/> Login message <input type="checkbox"/> Debug</div>
Log to Storage	<div><input checked="" type="checkbox"/> Enable</div> <div>Select Device: <div>Internal</div></div> <div>Log file name: <div>syslog</div></div> <div>Split file: <input type="checkbox"/> Enable Size: <div>200</div> <div>KB</div></div> <div>Interval: <input type="checkbox"/> Enable <div>1440</div> ( 1 ~ 10080 Minutes)</div> <div>Max Records: <div>3000</div> (5~10000)</div> <div><div>Download log file</div> <div>clear logs</div></div> <div>Log type Category: <input checked="" type="checkbox"/> System <input checked="" type="checkbox"/> Attacks <input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Login message <input checked="" type="checkbox"/> Debug</div>

### View & Email Log History

The **View** button allows for the viewing of log history. The **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 <b>View</b> button to view Log History in Web Log List Window.
Email Now button	N/A	Click the <b>Email Now</b> button to send Log History via Email instantly.

# EW200 Industrial Cellular Gateway

Web Log List		Previous	Next	First	Last	Download	Clear
Time	Log						
Dec 2 18:38:23	kernel: klogd started: BusyBox v1.3.2 (2015-10-29 12:52:33 CST)						
Dec 2 18:38:33	BEID: BEID STATUS : 0 , STATUS OK!						
Dec 2 18:38:40	commander: NETWORK Initialization finished. Result: 0						
Dec 2 18:38:40	commander: Initialize MultiWAN						
Dec 2 18:38:40	commander: index = 14, failover_index = 14						
Dec 2 18:38:40	commander: wantype = 32, wantype index = 99, wan mode = 1, route enable = 1						
Dec 2 18:38:40	commander: fo enable = 14, fo stay enable = 0, fo trigger = 1, fo time = 30, fo sequence = 0						
Dec 2 18:38:40	commander: wantype = 16, wantype index = 0, wan mode = 2, route enable = 1						
Dec 2 18:38:40	commander: fo enable = 14, fo stay enable = 0, fo trigger = 0, fo time = 0, fo sequence = 0						
Dec 2 18:38:40	commander: LOAD BALANCE!						
Dec 2 18:38:40	commander: ROUTING!						
Dec 2 18:38:42	syslog: server_config.pool_check = 1						
Dec 2 18:38:42	syslog: start = 192.168.85.100, end = 192.168.85.200, lan_ip = 192.168.85.2, interface=br0, ifindex=0						
Dec 2 18:38:42	udhcpd[1413]: udhcpd (v0.9.9-pre) started						
Dec 2 18:38:43	syslog: Failure parsing line 13 of /etc/udhcpd_vlan0.conf						
Page: 1/8 (Log Number: 109)							
		Back					

Web Log List Window		
Item	Value Setting	Description
Time column	N/A	Displays event time stamps
Log column	N/A	Displays Log messages

Web Log List Button Description		
Item	Value setting	Description
Previous	N/A	Click the <b>Previous</b> button to move to the previous page.
Next	N/A	Click the <b>Next</b> button to move to the next page.
First	N/A	Click the <b>First</b> button to jump to the first page.
Last	N/A	Click the <b>Last</b> button to jump to the last page.
Download	N/A	Click the <b>Download</b> button to download log to your PC in tar file format.
Clear	N/A	Click the <b>Clear</b> button to clear all log.
Back	N/A	Click the <b>Back</b> button to return to the previous page.

## Web Log Type Category

The 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.

# EW200 Industrial Cellular Gateway

▶ Web Log Type Category	<input checked="" type="checkbox"/> System	<input checked="" type="checkbox"/> Attacks	<input checked="" type="checkbox"/> Drop	<input checked="" type="checkbox"/> Login message	<input type="checkbox"/> Debug
-------------------------	--	---	--	---	--------------------------------

Web Log Type Category Setting Window		
Item	Value Setting	Description
<b>System</b>	Checked by default	Log system events and to display in the Web Log List window.
<b>Attacks</b>	Checked by default	Log attack events and to display in the Web Log List window.
<b>Drop</b>	Checked by default	Log packet drop events and to display in the Web Log List window.
<b>Login message</b>	Checked by default	Log system login events and to display in the Web Log List window.
<b>Debug</b>	Unchecked by default	Log debug events and to display in the Web Log List window.

## Email Alert

The Email Alert screen allows network administrator to select the type of event to log and be sent to the destined Email account.

▶ Email Alert	<input type="checkbox"/> Enable
	Server: <span>--- Option --- ▼</span> <span>Add Object</span>
	E-mail Addresses: <div></div>
	Subject: <input type="text"/>
Log type Category: <input type="checkbox"/> System <input type="checkbox"/> Attacks <input type="checkbox"/> Drop <input type="checkbox"/> Login message <input type="checkbox"/> Debug	

Email Alert Setting Window		
Item	Value Setting	Description
<b>Enable</b>	Unchecked by default	Check <b>Enable</b> box to enable sending event log messages to designated Email account defined in the E-mail Addresses blank space.
<b>Server</b>	N/A	Select one email server from the Server dropdown box to send Email. If none is available, click the <b>Add Object</b> button to create an outgoing Email server. You may also add an outgoing Email server from Object Definition > External Server > External Server tab.
<b>E-mail address</b>	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'
<b>Subject</b>	String: any text	Enter an Email subject that is easy for you to identify on the Email client.
<b>Log type category</b>	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.

# EW200 Industrial Cellular Gateway

## Syslogd

Syslogd screen allows the network administrator to select the type of event to log and be sent to the designated Syslog server.

► Syslogd	<input type="checkbox"/> Enable Server: <span>--- Option --- ▾</span> <span>Add Object</span>
	Log type Category: <input type="checkbox"/> System <input type="checkbox"/> Attacks <input type="checkbox"/> Drop <input type="checkbox"/> Login message <input type="checkbox"/> Debug

Syslogd Setting Window		
Item	Value Setting	Description
Enable	Unchecked by default	Check the <b>Enable</b> 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 send event log to. If none is available, click the <b>Add Object</b> 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	Unchecked 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 the network administrator to select the type of events to log and be stored at an internal or an external storage device.

► Log to Storage	<input checked="" type="checkbox"/> Enable Select Device: <span>Internal ▾</span> Log file name: <input type="text" value="syslog"/> Split file: <input type="checkbox"/> Enable Size: <input type="text" value="200"/> <span>KB ▾</span> Interval: <input type="checkbox"/> Enable <input type="text" value="1440"/> ( 1 ~ 10080 Minutes) Max Records: <input type="text" value="3000"/> (5~10000) <span>Download log file</span> <span>clear logs</span> Log type Category: <input checked="" type="checkbox"/> System <input checked="" type="checkbox"/> Attacks <input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Login message <input checked="" type="checkbox"/> Debug
------------------	--

Log to Storage Setting Window		
Item	Value Setting	Description
Enable	Unchecked by default	Check to enable sending log to storage.
Select Device	Internal is selected by default	Select internal or external storage.
Log file name	Unchecked by default	Enter log file name to save logs in designated storage.
Split file Enable	Unchecked by default	Check <b>enable</b> 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. <b>Value Range:</b> 10 ~1000.
Interval Enable	Unchecked by default	Check <b>enable</b> box to enable the log interval setting.
Log Interval	1440 is set by default	Enter the log interval setting. Value Range: 1 ~ 10080 Minute.
Max Records	3000 is set by default	Enter the maximum number of records to be stored in the log storage. Value Range: 5 ~ 10000.

## EW200 Industrial Cellular Gateway

---

<b>Log type category</b>	Unchecked by default	Check which type of logs to send: System, Attacks, Drop, Login message, Debug
<b>Download log file</b>	N/A	Click the <b>Download log file</b> button to download log files to a log.tar file.

# EW200 Industrial 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	Setting
FW Upgrade	Via Web UI ▼ FW Upgrade
Backup Configuration Settings	Download ▼ Via Web UI
Auto Restore Configuration	<input type="checkbox"/> Enable Save Conf. Clean Conf. Conf. Info.
Self-defined Logo	Download ▼ Via Web UI Reset
Self-defined CSS	Edit : Download ▼ Via Web UI Reset

FW Backup & Restore		
Item	Value Setting	Description
FW Upgrade	Via Web UI is selected by default	If new firmware is available, click the <b>FW Upgrade</b> button to upgrade the device firmware <b>via Web UI</b> , or <b>Via Storage</b> . After clicking on the “FW Upgrade” command button, specify the file name of new firmware by using the “Browse” button, and then click the “Upgrade” button to start the FW upgrading process. If you want to upgrade firmware which is from a GPL policy, please check “Accept unofficial firmware”
Backup Configuration Settings	Download is selected by default	You can back up or restore the device configuration settings by clicking the <b>Via Web UI</b> button. <b>Download</b> : for backing up the device configuration to a config.bin file. <b>Upload</b> : for restoring a designated configuration file to the device. <b>Via Web UI</b> : to retrieve the configuration file via Web GUI.
Auto Restore Configuration	Enable box is unchecked by default	Click the <b>Enable</b> 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 <b>Save Conf.</b> button, or clicking the <b>Clean Conf.</b> button to erase the stored customized configuration.

# EW200 Industrial 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 settings. In addition to performing 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	<div>Now ▼</div> <div>Reboot</div>
▶ Reset to Default	<div>Reset</div>

System Operation Window		
Item	Value Setting	Description
Reboot	Now is selected by default	Click the <b>Reboot</b> button to reboot the gateway immediately or on a pre-defined time schedule. <b>Now:</b> Reboot immediately <b>Time Schedule:</b> Select a pre-defined auto-reboot time schedule rule to reboot the auto device on a designated time To define a time schedule rule, go to <b>Object Definition &gt; Scheduling &gt; Configuration</b> tab.
Reset to Default	N/A	Click the <b>Reset</b> button to reset the device configuration to its default value.

# EW200 Industrial Cellular Gateway

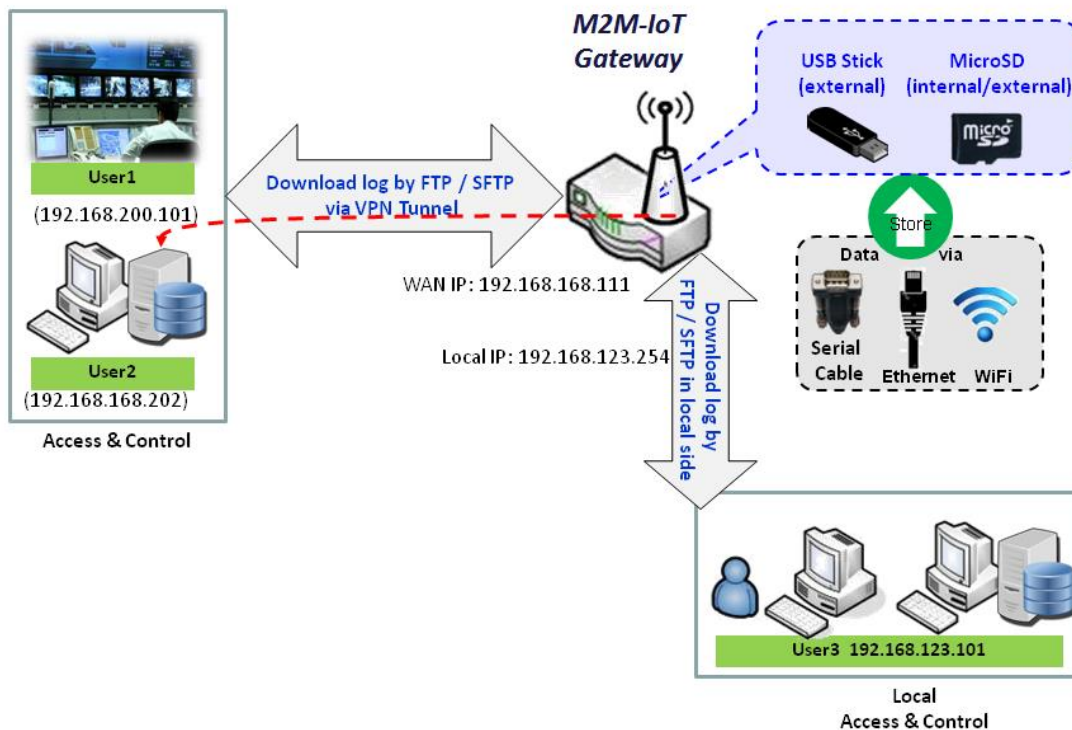
## 6.3 FTP

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 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 also 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). SSH File Transfer Protocol (SFTP) is sometimes also used instead, but is technologically different.

This gateway has an embedded FTP / SFTP server for administrator to download 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 log in to the server. After logging in, you can browse the log directory and have 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.





# EW200 Industrial Cellular Gateway

## 6.3.1 Server Configuration

This section allows user to set up the embedded FTP and SFTP server for retrieving log files.

Go to **Administration > FTP > Server Configuration** tab.

### Enable FTP Server

FTP Server Configuration <span>Save</span>	
Item	Setting
▶ FTP	<input type="checkbox"/> Enable
▶ FTP Port	<input type="text" value="21"/>
▶ Timeout	<input type="text" value="300"/> second(s)(60-7200)
▶ Max. Connections per IP	<input type="text" value="2"/>
▶ Max. FTP Clients	<input type="text" value="5"/>
▶ PASV Mode	<input type="checkbox"/> Enable
▶ Port Range of PASV Mode	<input type="text" value="50000"/> ~ <input type="text" value="50031"/>
▶ Auto Report External IP in PASV Mode	<input type="checkbox"/> Enable
▶ ASCII Transfer Mode	<input type="checkbox"/> Enable
▶ FTPS(FTP over SSL/TLS)	<input type="checkbox"/> Enable

Configuration Item	Value setting	Description
FTP	Unchecked by default	Check <b>Enable</b> 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 write permission is implemented.
FTP Port	Port <b>21</b> is set by default	Specify a port number for FTP connection. The gateway will listen for incoming FTP connections on the specified port. <b>Value Range: 1 ~ 65535.</b>
Timeout	<b>300</b> 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	<b>2</b> 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	<b>5</b> Clients are set by default.	Specify the maximum number of clients for the FTP connection. Up to 32 clients are supported.

# EW200 Industrial Cellular Gateway

<b>PASV Mode</b>	Optional setting	Check the <b>Enable</b> box to activate the support of PASV mode for a FTP connection from FTP clients.
<b>Port Range of PASV Mode</b>	Port <b>50000 ~ 50031</b> is set by default.	Specify the port range to allocate for PASV style data connection. <b><u>Value Range: 1024 ~ 65535.</u></b>
<b>Auto Report External IP in PASV Mode</b>	Optional setting	Check the <b>Enable</b> box to activate the support of overriding the IP address advertising in response to the PASV command.
<b>ASCII Transfer Mode</b>	Optional setting	Check the <b>Enable</b> box to activate the support of ASCII mode data transfers. Binary mode is supported by default.
<b>FTPS (FTP over SSL/TLS)</b>	Optional setting	Check the <b>Enable</b> box to activate the support of secure connections via SSL/TLS.

## Enable SFTP Server

SFTP Server Configuration
Save

Item	Setting
▶ SFTP	<input type="checkbox"/> Enable via <input checked="" type="checkbox"/> LAN via <input checked="" type="checkbox"/> WAN ( WAN-1 <input checked="" type="checkbox"/> WAN-4 <input type="checkbox"/> ) <div></div>
▶ SFTP Port	22

Configuration		
Item	Value setting	Description
<b>SFTP</b>	Unchecked by default	Check <b>Enable</b> box to activate the embedded SFTP Server function. Furthermore, you can check the granted interface(s) for the SFTP connection, via <b>LAN</b> , <b>WAN</b> , or both. With the SFTP Server enabled, you can retrieve or delete the stored log files via secure SFTP connection.
<b>SFTP Port</b>	Default is <b>22</b>	Specify a port number for SFTP connection. The gateway will listen for incoming SFTP connections on the specified port. <b><u>Value Range: 1 ~ 65535.</u></b>

# EW200 Industrial Cellular Gateway

## 6.3.2 User Account

This section allows user to set up user accounts for logging to the embedded FTP and SFTP server to retrieve log files.

Go to **Administration > FTP > User Account** tab.

### Create/Edit FTP User Accounts

User Account List <input type="button" value="Add"/> <input type="button" value="Delete"/>						
ID	User Name	Password	Directory	Permission	Enable	Actions

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

User Account Configuration <input type="button" value="Save"/>	
Item	Setting
▶ User Name	<input type="text"/>
▶ Password	<input type="password"/>
▶ Directory	<input type="button" value="Browse"/>
▶ Permission	<input type="text" value="Read/Write"/>
▶ Enable	<input checked="" type="checkbox"/>

Configuration		
Item	Value setting	Description
User Name	String: non-blank string	Enter the user account name. <b>Value Range:</b> 1 ~ 15 characters.
Password	String: no blank	Enter the user password.
Directory	N/A	Select a root directory after login.
Permission	<b>Read/Write</b> is selected by default.	Select the Read/write permission. Note: The embedded FTP Server is only for log downloading, so no write permission is implemented, even if the <b>Read/Write</b> option is selected.
Enable	The box is checked by default.	Check the box to activate the FTP user account.

# EW200 Industrial Cellular Gateway

## 6.4 Diagnostics

This gateway supports simple network diagnostic tools for the administrator to troubleshoot and analyze abnormal behavior or traffic passing through the gateway.

### 6.4.1 Diagnostic Tools

The Diagnostic Tools provide some frequently used network connectivity tools (approaches) for the network administrator to check device connectivity.

Go to **Administration > Diagnostic > Diagnostic Tools** tab.

Diagnostic Tools

Item	Setting
▶ Ping Test	Host IP: <input type="text"/> Outer Interface: <input type="text" value="Auto"/> LAN Source: <input type="text"/> <input type="button" value="Default"/> <input type="button" value="Ping"/>
▶ Tracert Test	Host IP: <input type="text"/> Interface: <input type="text" value="Auto"/> <input type="text" value="UDP"/> <input type="button" value="Tracert"/>
▶ Speed Test	Interface: <input type="text" value="Auto"/> mode: <input type="text" value="DL+UL"/> <input type="checkbox"/> SSL <input type="button" value="Test"/>
▶ Wake on LAN	<input type="text"/> <input type="button" value="Wake up"/>

Diagnostic Tools		
Item	Value setting	Description
<b>Ping Test</b>	Optional setting	This allows you to specify an IP / FQDN and the test interface (LAN, WAN, or Auto), so the system will try to ping the specified device to test whether it is alive after clicking on the <b>Ping</b> button. A test result window will appear beneath it.
<b>Tracert Test</b>	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 more than twice, then the connection is lost and the route cannot be evaluated. Specify an IP / FQDN, the test interface (LAN, WAN, or Auto) and the protocol (UDP or ICMP). By default, it is <b>UDP</b> . The system will try to trace the specified host to test whether it is alive after clicking on <b>Tracert</b> button. A test result window will appear beneath it.
<b>Speed Test</b>	Optional setting	This allow you to do a quick speed test for verifying the connectivity on a specific interface.
<b>Wake on LAN</b>	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 <b>Wake up</b> command button.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the configuration.

# EW200 Industrial Cellular Gateway

## 6.4.2 Packet Analyzer

The Packet Analyzer can capture packets according to custom settings. User can specify interfaces to capture packets and filter by setting a rule. Ensure that 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	Setting
▶ Packet Analyzer	<input type="checkbox"/> Enable
▶ File Name	<input type="text"/>
▶ Split Files	<input type="checkbox"/> Enable File Size : <input type="text" value="200"/> <span>KB ▼</span>
▶ Packet Interfaces	<input type="checkbox"/> WAN-1 <input type="checkbox"/> WAN-2 <input type="checkbox"/> ASY-1 2.4G : <input type="checkbox"/> VAP-1 <input type="checkbox"/> VAP-2 <input type="checkbox"/> VAP-3 <input type="checkbox"/> VAP-4 <input type="checkbox"/> VAP-5 <input type="checkbox"/> VAP-6 <input type="checkbox"/> VAP-7 <input type="checkbox"/> VAP-8

Configuration		
Item	Value setting	Description
Packet Analyzer	Unchecked by default	Check <b>Enable</b> box to activate the Packet Analyzer function. If you cannot enable the checkbox, check if the storage is available. Plug in the USB storage and then enable the Package Analyzer function.
File Name	1. Optional setting 2. Default is blank, and the default file name is <b>&lt;Interface&gt;_&lt;Date&gt;_&lt;index&gt;</b> .	Enter a file name to save the captured packets in log storage. If <b>Split Files</b> option is also enabled, the file name will be appended with an index code " <b>_&lt;index&gt;</b> ". The file extension is <b>.pcap</b> .
Split Files	1. Optional setting 2. Default value of <b>File Size</b> is 200 KB.	Check <b>enable</b> box to split file whenever log file reaches the specified limit. If the <b>Split Files</b> option is enabled, you can further specify the <b>File Size</b> and <b>Unit</b> for the split files. <b>Value Range: 10 ~ 99999</b> . NOTE: <b>File Size</b> cannot be less than 10 KB
Packet Interfaces	Optional setting	Define the interface(s) that <b>Packet Analyzer</b> should work on. At least one interface is required, but multiple selections are also accepted. Supported interfaces are: <ul style="list-style-type: none"><li>● <b>WAN</b>: When the WAN is enabled at <b>Physical Interface</b>, it can be selected here.</li><li>● <b>ASY</b>: This means the serial communication interface. It is used to capture packets appearing in the <b>Field Communication</b>. Therefore, it can only be selected when specific field communication protocol, like Modbus, is enabled.</li><li>● <b>VAP</b>: This means the virtual AP. When Wi-Fi and VAP are enabled, it can be selected here.</li></ul>
Save	N/A	Click the <b>Save</b> button to save the configuration.
Undo	N/A	Click the <b>Undo</b> button to restore previous settings.

# EW200 Industrial Cellular Gateway

Once you have enabled the Packet Analyzer function on specific Interface(s), you can further specify some filter rules to capture the packets which match the rules.

Capture Filters	
Item	Setting
▶ Filter	<input type="checkbox"/> Enable
▶ Source MACs	<div></div>
▶ Source IPs	<div></div>
▶ Source Ports	<div></div>
▶ Destination MACs	<div></div>
▶ Destination IPs	<div></div>
▶ Destination Ports	<div></div>

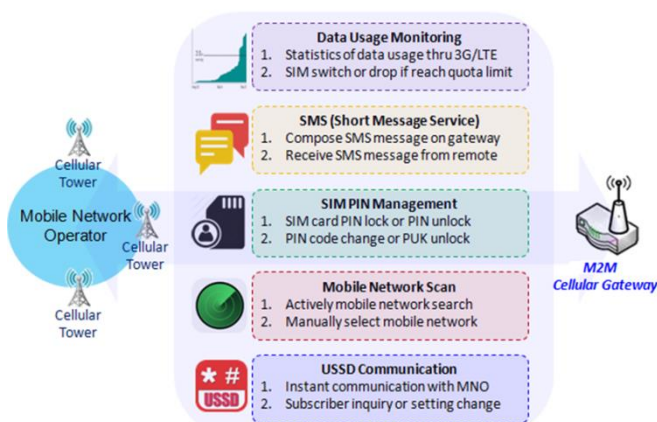
Capture Fitters		
Item	Value setting	Description
<b>Filter</b>	Optional setting	Check <b>Enable</b> box to activate the Capture Filter function.
<b>Source MACs</b>	Optional setting	Define the filter rule with <b>Source MACs</b> , the source MAC address of packets. Packets which match the rule will be 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 matching any one MAC in the rule.
<b>Source IPs</b>	Optional setting	Define the filter rule with <b>Source IPs</b> , 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 any IP is matched.
<b>Source Ports</b>	Optional setting	Define the filter rule with <b>Source Ports</b> , which means the source port of packets. The packets will be captured when any port is matched. Up to 10 ports are supported, but they must be separated with “;”,

# EW200 Industrial Cellular Gateway

		e.g. 80; 53 <b><u>Value Range:</u></b> 1 ~ 65535.
<b>Destination MACs</b>	Optional setting	Define the filter rule with <b>Destination MACs</b> , 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 any MAC address is matched.
<b>Destination IPs</b>	Optional setting	Define the filter rule with <b>Destination IPs</b> , 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 any IP address in the rule is matched.
<b>Destination Ports</b>	Optional setting	Define the filter rule with <b>Destination Ports</b> , the destination port of packets. The packets will be captured when any port in the rule is matched. Up to 10 ports are supported, but they must be separated with “;”, e.g. 80; 53 <b><u>Value Range:</u></b> 1 ~ 65535.

## Chapter 7 Service

### 7.1 Cellular Toolkit



Besides cellular data connection, you may also want to monitor data usage of the cellular WAN, send text messages through SMS, change the PIN code of the SIM card, communicate with carrier/ISP by USSD (Unstructured Supplementary Service Data) command, or perform a cellular network scan for diagnostic purposes.

The Cellular Toolkit section 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 that a valid SIM card is required to be inserted to device before you continue with

the settings in this section.

The screenshot shows the 'Cellular Toolkit' section of the EW200 web interface. The left sidebar contains navigation buttons: Status, Basic Network, Object Definition, Field Communication, Security, Administration, Service, Cellular Toolkit (highlighted), and Event Handling. The main content area has a top navigation bar with tabs: Data Usage (selected), SMS, SIM PIN, USSD, and Network Scan. Below the tabs, there is a section titled '3G/4G Data Usage Profile List' with 'Add' and 'Delete' buttons. A table displays the data usage profiles.

ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable	Action
----	----------	--------------	--------------	------------	-----------------	---------------------	--------	--------



# EW200 Industrial Cellular Gateway

## 7.1.1 Data Usage

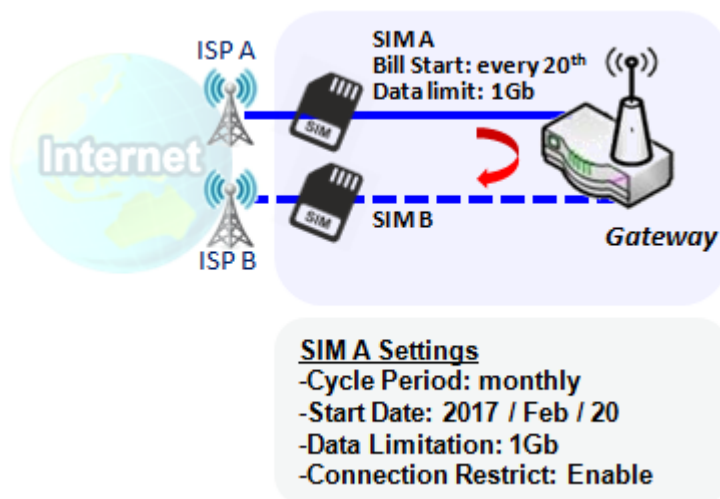
Most data plans for cellular connection have data caps. If data usage is over the set limit, it may result in a much lower data throughput that affects your operations, or an exceptionally high bill with over-quota surcharges.

With the Data Usage feature, the device will monitor cellular data usage continuously and take a preset action. Device can be set to drop the cellular data connection right away or, if a secondary SIM card is inserted, device will switch to the secondary SIM and establish another cellular data connection automatically.

If Data Usage feature is enabled, the entire history of cellular data usage can be viewed at **Status > Statistics & Reports > Cellular Usage** tab.

3G/4G Data Usage Profile List <span>Add</span> <span>Delete</span>								
ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable	Action
1	3G/4G SIM A	ISP A	1 Monthly	Mon Apr 01 2019 00:00:00 GMT+0800	1GB	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<span>Edit</span> <span>Select</span>

### 3G/4G Data Usage



The data Usage feature allows the gateway device to continuously monitor cellular data usage and take action. In the diagram, the limit of SIM A is **1Gb** per month and billing start date is the **20<sup>th</sup>** of every month. The device can start a new calculation of data usage on every 20<sup>th</sup> of the month. **Enable Connection Restrict** will force the gateway to drop cellular connection of SIM A when data usage reaches 1Gb. If SIM failover feature is configured in **Internet Setup**, then the gateway will switch to SIM B and establish a new cellular data connection automatically.

# EW200 Industrial Cellular Gateway

## Data Usage Setting

Go to **Service > Cellular Toolkit > Data Usage** tab.

To configure Data Usage, you need to know the billing start date, bill period, and data limit for your data plan.

### Create / Edit 3G/4G Data Usage Profile

3G/4G Data Usage Profile List <span>Add</span> <span>Delete</span>								
ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable	Action

When the **Add** button is applied, the **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
▶ SIM Select	3G/4G ▼ SIM A ▼
▶ Carrier Name	<input type="text"/>
▶ Cycle Period	Days ▼ 90
▶ Start Date	2016 ▼ / October ▼ / 11 ▼
▶ Data Limitation	<input type="text"/> KB ▼
▶ Connection Restrict	<input type="checkbox"/> Enable
▶ Enable	<input checked="" type="checkbox"/> Enable

3G/4G Data Usage Profile Configuration		
Item	Setting	Description
<b>SIM Select</b>	<b>3G/4G-1</b> and <b>SIM A</b> by default.	Choose a cellular interface ( <b>3G/4G-1</b> or <b>3G/4G-2</b> ), and a SIM card bound to the selected cellular interface to configure its data usage profile. <b>Note:</b> <b>3G/4G-2</b> is only available for products with dual cellular modules.
<b>Carrier Name</b>	Optional item.	Fill in the Carrier Name for the selected SIM card for identification.
<b>Cycle Period</b>	<b>Days</b> by default	The three types of cycle period are <b>Days</b> , <b>Weekly</b> and <b>Monthly</b> . <b>Days:</b> For per Days cycle periods, you must further specify the number of days in the second box. <b>Value Range:</b> 1 ~ 90 days. <b>Weekly, Monthly:</b> The cycle period is one week or one month.
<b>Start Date</b>	N/A	Specify the date to start measuring network traffic. Don't select a day in the past. This will cause traffic statistics to be incorrect.
<b>Data Limitation</b>	N/A	Specify the allowable data limitation for the defined cycle period.
<b>Connection Restrict</b>	Un-Checked by default.	Check the <b>Enable</b> 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.
<b>Enable</b>	Un-Checked by default.	Check the <b>Enable</b> box to activate the data usage profile.

# EW200 Industrial 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	SMS Setup	Managing Events Setup	Notifying Events Setup
Item	Setting		
Physical Interface	3G/4G-1		
SMS	<input type="checkbox"/> Enable SIM Status: SIM_A		
SMS Storage	SIM Card Only		
SMS Space	<input type="checkbox"/> Enable & Keep Available Space (1-10)		

Configuration Item	Value setting	Description
Physical Interface	3G/4G-1 by default	Choose a cellular interface ( <b>3G/4G-1</b> or <b>3G/4G-2</b> ) for the following SMS function configuration. <b>Note: 3G/4G-2</b> is only available for products with dual cellular modules.
SMS	Checked by default	Check to enable SMS function.
SIM Status	N/A	Depends on current SIM status. The possible values are <b>SIM_A</b> or <b>SIM_B</b> .
SMS Storage	The box is <b>SIM Card Only</b> by default	This is the SMS storage location. Currently the only option is <b>SIM Card Only</b> .
SMS Space	Unchecked by default	Check the Enable box and specify a number (1-10) for message count to reserve available storage space and prevent it from running out of storage. The oldest message(s) will be deleted when the SMS storage is nearly full.
Save	N/A	Click the <b>Save</b> button to save the settings

# EW200 Industrial Cellular Gateway

## SMS Summary

Shows **Unread SMS**, **Received SMS**, **Remaining SMS**, and allows editing of SMS context to send, reading of SMS from SIM card.

SMS Summary	
<div>New SMS SMS Inbox SMS Sent Folder</div>	
Item	Setting
▶ Unread SMS	0
▶ Received SMS	10
▶ Sent SMS	0
▶ Remaining SMS	0

SMS Summary		
Item	Value setting	Description
<b>Unread SMS</b>	N/A	If SIM card is inserted for first time, unread SMS value is zero. When new SMS are received but not read, this value increases.
<b>Received SMS</b>	N/A	This value records the number of SMS from SIM card.
<b>Sent SMS</b>	N/A	This value records the number of out going SMS. When an SMS is sent, this value Increases by one.
<b>Remaining SMS</b>	N/A	This value is SMS capacity minus received SMS.
<b>New SMS</b>	N/A	Click <b>New SMS</b> button, a <b>New SMS</b> screen appears. Refer to New SMS in the next page.
<b>SMS Inbox</b>	N/A	Click <b>SMS Inbox</b> button, a <b>SMS Inbox List</b> screen appears. User can read or delete SMS, reply SMS or forward SMS from this screen. Refer to SMS Inbox List on the next page.
<b>Refresh</b>	N/A	Click the <b>Refresh</b> button to update the SMS summary.

## New SMS

Configure SMS settings from this screen.

# EW200 Industrial Cellular Gateway

☐ New SMS

Item	Setting
▶ Receivers	<input type="text"/> (Use '+' for International Format and ';' to Compose Multiple Receivers)
▶ Text Message	<div></div> <div>Length of Current Input : 0</div>
▶ Result	

New SMS		
Item	Value setting	Description
Receivers	N/A	Enter the receivers to which the SMS will be sent. Add a semicolon to separate multiple receivers.
Text Message	N/A	Write the SMS content. A maximum length of 1023 characters is supported.
Send	N/A	Click the <b>Send</b> button have the text message sent as a SMS.
Result	N/A	If SMS has been sent successfully, it will show <b>Send OK</b> , otherwise <b>Send Failed</b> will be displayed.

## SMS Inbox List

You can read or delete SMS, reply SMS or forward SMS from this screen.

☐ SMS Inbox List

ID	From Phone Number	Timestamp	SMS Text Preview	Actions
----	-------------------	-----------	------------------	---------

SMS Inbox List		
Item	Value setting	Description
ID	N/A	The number of SMS.
From Phone Number	N/A	From phone number of SMS
Timestamp	N/A	Time received
SMS Text Preview	N/A	Preview the SMS text. Click the <b>Detail</b> button to read a specific message.
Action	Unchecked by default	Click the <b>Detail</b> button to read the SMS detail; Click the <b>Reply / Forward</b> button to reply/forward SMS. Check the box(es), and then click the <b>Delete</b> button to delete the SMS(s).
Refresh	N/A	Refresh the SMS Inbox list.
Delete	N/A	Delete the SMS for all checked box from Action.

# EW200 Industrial Cellular Gateway

Close	N/A	Close the Detail SMS Message screen.
-------	-----	--------------------------------------

## SMS Sent foler

You can read or delete SMS from this screen.

SMS Sent Folder					Delete	Close	Previous	0 ▼	Next	
ID	Receivers	Timestamp	SMS Text Preview	Actions						

SMS Inbox List		
Item	Value setting	Description
ID	N/A	The number of SMS.
Receivers	N/A	Receiver list for sent SMS
Timestamp	N/A	Time received
SMS Text Preview	N/A	Preview the SMS text. Click the <b>Detail</b> button to read a specific message.
Action	Unchecked by default	Click the <b>Detail</b> button to read the SMS detail; Check the box(es), and then click the <b>Delete</b> button to delete the 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.

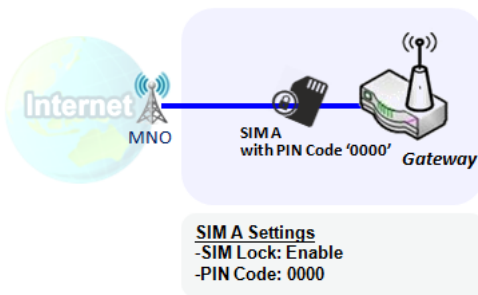
# EW200 Industrial Cellular Gateway

## 7.1.3 SIM PIN

In most cases, users need to insert a SIM card (a.k.a. UICC) into end devices connecting to a cellular network. 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 cards play an important role between service providers and subscribers, some security mechanisms are required on SIM card to prevent any unauthorized access.

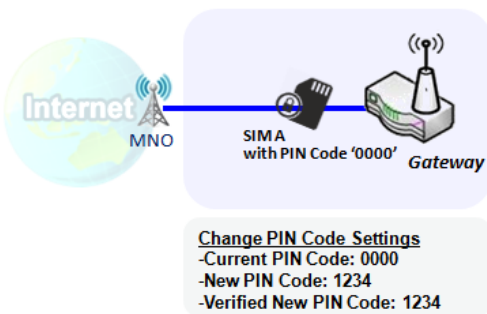
Enabling a PIN code in SIM card is an easy and effective way of protecting cellular devices from unauthorized access. This gateway device allows you to activate and manage PIN code son a SIM card through the web GUI.

### Activate PIN code on SIM Card



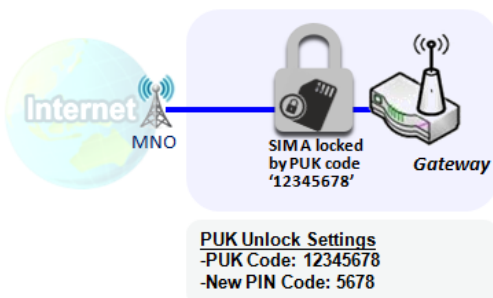
This gateway device allows you to activate a PIN code on SIM card. This example shows how to activate PIN code on SIM-A for 3G/4G-1 with default PIN code “0000”.

### 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: ‘1234’ to set the new PIN code to ‘1234’. To confirm the new PIN code retype the new PIN code in the Verified New PIN Code field again.

### Unlock SIM card by PUK Code



If you entered an incorrect PIN code at configuration page for 3G/4G-1 WAN over three times, then the SIM card will be locked by PUK (personal unlocking key) code. You will have to call a service number to get a PUK code to unlock the SIM card. In the diagram, the PUK code is “12345678” and new PIN code is “5678”.

# EW200 Industrial 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 the PIN code. You can also see the information for remaining times of failure trials as mentioned earlier. If you run out of these failure trials, you will 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 ▼ <input type="button" value="Switch"/>

Configuration Window		
Item	Value setting	Description
Physical Interface	The box is <b>3G/4G-1</b> by default	Choose a cellular interface ( <b>3G/4G-1</b> or <b>3G/4G-2</b> ) to change the SIM PIN setting for the selected SIM Card. <b>Note:</b> <b>3G/4G-2</b> is only available for products with dual cellular modules.
SIM Status	N/A	Indication for the selected SIM card and the SIM card status: <b>Ready, Not Insert, or SIM PIN.</b> <b>Ready</b> -- 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. <b>Not Insert</b> -- No SIM card is inserted in that SIM slot. <b>SIM PIN</b> -- SIM card is protected by PIN code, and it's not unlocked by a correct PIN code yet. SIM card is still in locked status.
SIM Selection	N/A	Select the SIM card for further SIM PIN configuration. Press the <b>Switch</b> button, then the Gateway will switch SIM card to the other one.



# EW200 Industrial Cellular Gateway

## Enable / Change PIN Code

Enable or Disable PIN code (password) function, and even change PIN code function.

SIM function <input type="button" value="Save"/> <input type="button" value="Change PIN Code"/>	
Item	Setting
▶ SIM lock	<input type="checkbox"/> Enable PIN Code: <input type="text"/> (4~8 digits)
▶ Remaining times	3

SIM function Window		
Item Setting	Value setting	Description
<b>SIM lock</b>	Depends on SIM card	Click the <b>Enable</b> button to activate the SIM lock function. For the first time you want to enable the SIM lock function, fill in the PIN code as well, and then click the <b>Save</b> button to apply the setting.
<b>Remaining times</b>	Depends on SIM card	Represents the remaining trial times for the SIM PIN unlocking.
<b>Save</b>	N/A	Click the <b>Save</b> button to apply the setting.
<b>Change PIN Code</b>	N/A	Click the <b>Change PIN code</b> button to change the PIN code (password). If the <b>SIM Lock</b> function is not enabled, the <b>Change PIN code</b> button is disabled. If you still want to change the PIN code, enable the SIM Lock function first, fill in the PIN code, and then click the <b>Save</b> button to enable. After that, you can click the <b>Change PIN code</b> button to change the PIN code.

When the **Change PIN Code** button is clicked, the following screen will appear.

Item	Setting
▶ Current PIN Code	<input type="text"/> (4~8 digits)
▶ New PIN Code	<input type="text"/> (4~8 digits)
▶ Verified New PIN Code	<input type="text"/> (4~8 digits)

Item	Value Setting	Description
<b>Current PIN Code</b>	Required setting	Enter the current (old) PIN code of the SIM card.
<b>New PIN Code</b>	Required setting	Enter the new PIN Code.
<b>Verified New PIN Code</b>	Required setting	Confirm the new PIN Code again.
<b>Apply</b>	N/A	Click the <b>Apply</b> button to change the PIN code with specified new PIN code.
<b>Cancel</b>	N/A	Click the <b>Cancel</b> button to cancel the changes and keep current PIN code.

Note: If you change the PIN code for a certain SIM card, you must also change the corresponding PIN code

# EW200 Industrial Cellular Gateway

specified in the **Basic Network > WAN & Uplink > Internet Setup > Connection with SIM Card** page. Otherwise, it may result in wrong SIM PIN trials with the 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. Usually this happens after too many trials using an incorrect PIN code, and the remaining times in the 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 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.

PUK function <span>Save</span>	
Item	Setting
▶ PUK status	PUK unlock.
▶ Remaining times	N/A
▶ PUK Code	<input type="text"/> (8 digits)
▶ New PIN Code	<input type="text"/> (4~8 digits)

PUK Function Window		
Item	Value setting	Description
PUK status	PUK Unlock / PUK Lock	Indication for the PUK status: <b>PUK Lock</b> or <b>PUK Unlock</b> . As mentioned earlier, the SIM card will be locked by PUK code after too many access attempts with an incorrect PIN code. In this case, the PUK Status will turns to <b>PUK Lock</b> . In a normal situation, it will display <b>PUK Unlock</b> .
Remaining times	Depend on SIM card	The remaining trial times for the PUK unlocking. Note: <b>DO NOT allow the remaining times to reach zero, it will damage the SIM card FOREVER !</b> 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	Required setting	Enter the PUK code (8 digits) that can unlock the SIM card in PUK unlock status.
New PIN Code	Required setting	Enter the New PIN Code (4~8 digits) for the SIM card. You will have to ascertain your new PIN code to replace the old, forgotten one. Keep the PIN code (password) in mind with care.
Save	N/A	Click the <b>Save</b> 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 the invalid (old) PIN code.

# EW200 Industrial 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

AddDelete

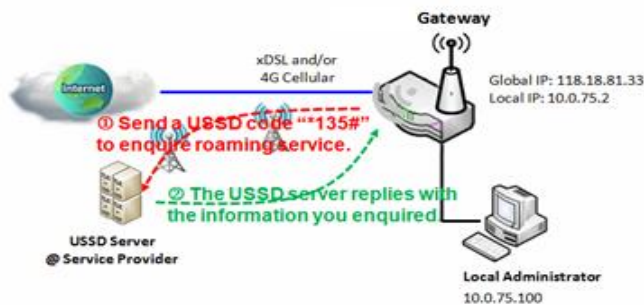
ID	Profile Name	USSD Command	Comments	Actions
----	--------------	--------------	----------	---------

USSD Request

SendClearCancel

Item	Setting
USSD Profile	--- Option ---
USSD Command	

### USSD Scenario



USSD allows you to have an instant bi-directional communication with the carrier/ISP. In the diagram, the USSD command ‘\*135#’ refers 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/ISPs.

### USSD Setting

Go to **Service > Cellular Toolkit > USSD** tab.

In the "USSD" page, there are four windows for the USSD function. The "Configuration" window lets you specify which 3G/4G module (physical interface) is used USSD, and the system will show which SIM card in the module is the current one. The second window is the "USSD Profile List" and it shows all your defined USSD profiles that

# EW200 Industrial Cellular Gateway

store pre-commands for activating a USSD session. An "Add" button in the window lets you add one new USSD profile and define the commands for the profile in the third window, "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 <input type="button" value="v"/> SIM Status: SIM_A

Configuration Item	Value setting	Description
Physical Interface	3G/4G-1 is default.	Choose a cellular interface ( <b>3G/4G-1</b> or <b>3G/4G-2</b> ) to configure the USSD setting for the connected cellular service (identified with <b>SIM_A</b> or <b>SIM_B</b> ). <b>Note:</b> <b>3G/4G-2</b> is only available for products with dual cellular modules.
SIM Status	N/A	Show the connected cellular service (identified with <b>SIM_A</b> or <b>SIM_B</b> ).

## Create / Edit USSD Profile

The cellular gateway allows you to customize your USSD profile. It supports up to a maximum of 35 USSD profiles.

USSD Profile List <input type="button" value="Add"/> <input type="button" value="Delete"/>				
ID	Profile Name	USSD Command	Comments	Actions

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

USSD Request <input type="button" value="Send"/> <input type="button" value="Clear"/> <input type="button" value="Cancel"/>	
Item	Setting
USSD Profile	--- Option --- <input type="button" value="v"/>
USSD Command	<input type="text"/>

# EW200 Industrial Cellular Gateway

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 details.

## Send USSD Request

When you **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	<input type="text"/>		

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 <b>Send</b> button to send the USSD command, and the <b>USSD Response</b> screen will appear. You will see the response message of the corresponding service, receive the service SMS.

# EW200 Industrial Cellular Gateway

## 7.1.5 Network Scan

The "Network Scan" function lets the administrator specify how the device will connect to the mobile system for data communication for each 3G/4G interface. For example, the administrator can specify which generation of mobile system is used for connection, 2G, 3G or LTE. Moreover, he/she can define their connection sequence for connecting to mobile systems. The administrator can also scan the mobile systems available manually, then select the target operator system and apply it.

### Network Scan Setting

Go to **Service > Cellular Toolkit > Network Scan** tab.

In the "Network Scan" page, there are two windows for the Network Scan function. The "Configuration" window lets you select which 3G/4G module (physical interface) is used to perform Network Scan, and the system will show the current used SIM card in the module. You can configure each 3G/4G WAN interface by executing the network scan 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 <b>3G/4G-1</b> by default	Choose a cellular interface ( <b>3G/4G-1</b> or <b>3G/4G-2</b> ) for the network scan function. <b>Note:</b> <b>3G/4G-2</b> is only available for products with dual cellular modules.
SIM Status	N/A	Show the connected cellular service (identified with <b>SIM_A</b> or <b>SIM_B</b> ).
Network Type	<b>Auto</b> 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 LTE Only. When <b>Auto</b> is selected, the network will be registered automatically; If the <b>prefer</b> option is selected, network will be registered for your option first; If the <b>only</b> option is selected, network will be registered for your option only.
Scan Approach	<b>Auto</b> is selected by default.	When <b>Auto</b> selected, the cellular module registers automatically.

# EW200 Industrial Cellular Gateway

		If the <b>Manually</b> option is selected, a <b>Network Provider List</b> screen appears. Press <b>Scan</b> button to scan for the nearest base stations. Select (check the box) the preferred base stations then click <b>Apply</b> button to apply settings.
<b>Save</b>	N/A	Click <b>Save</b> 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 waiting for 1 to 3 minutes, the found mobile operator systems will be displayed for you to choose from. Click again on the "Apply" button to have the system connect to that mobile operator system for the dedicated 3G/4G interface.

 Network Provider List <span>Scan</span> <span>Apply</span> <span>↑</span>			
Provider Name	Mobile System	Network Status	Action

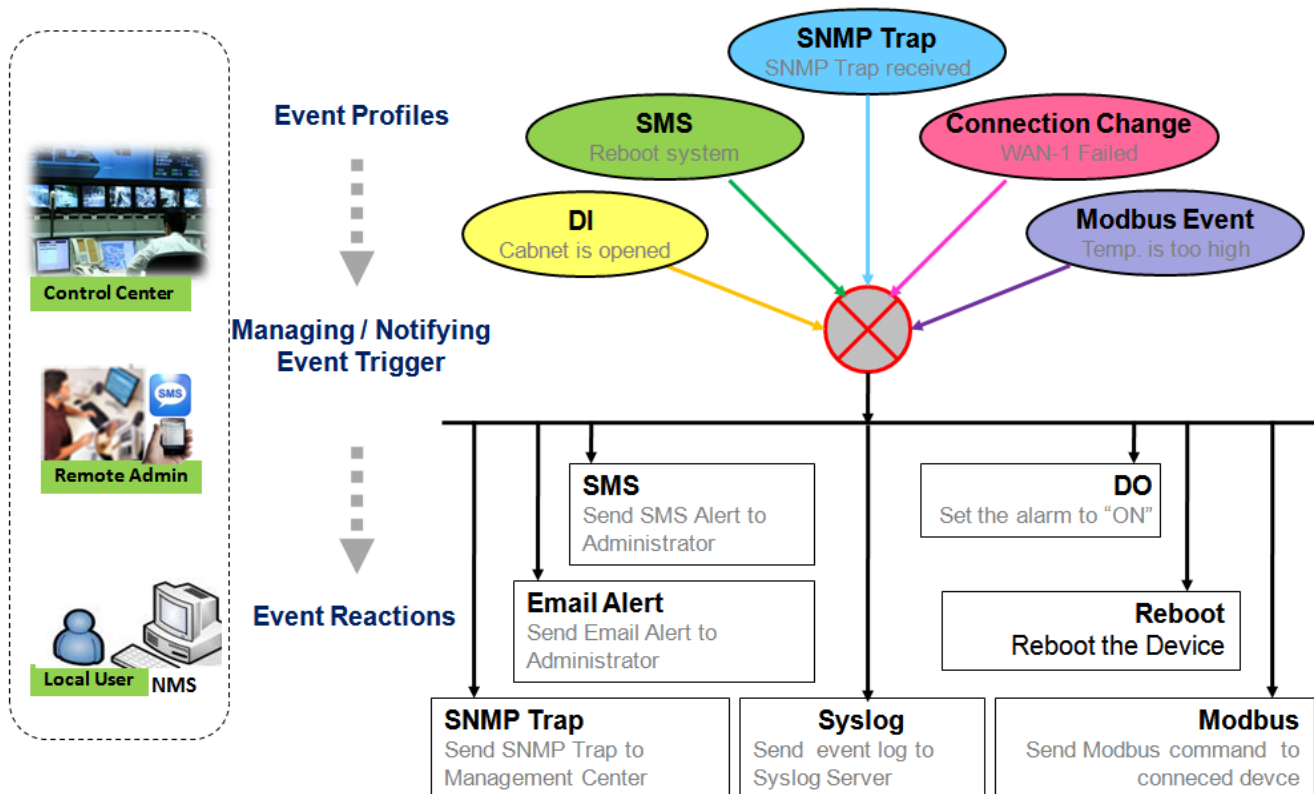
## 7.2 SMS & Event

SMS & Event is the application that allows the administrator to setup pre-defined events, handlers, or response behavior with individual profiles. With proper configuration, the administrator can easily and remotely obtain the status and information via the gateway. Moreover, he/she can also handle and manage some important system related functions, even connected field bus devices and D/O devices.

The supported events are categorized into two groups: **managing events** and **notifying events**.

**Managing events** are events that are used to manage the gateway or change the setting / status of the specific functionality of the gateway. On receiving a managing event, the gateway will take action to change the functionality, collect the required status for administration, and also change the status of a connected field bus device.

**Notifying events** are events in which some related objects have been triggered and corresponding actions are taken. It could be an event generated from the connected sensor, or a certain connected field bus device. Alerts can be sent by SMS message, Email, and SNMP Trap.



For ease of configuration, the administrator can create and edit the common pre-defined managing / notifying event profiles for taking instant action on a certain event or managing the devices for advanced purposes. For example, sending/receiving remote managing SMS for the gateway's routine maintenance, field bus device status monitoring, digital sensor detection controlling, and so on. All such management and notification functions can be realized effectively via the Event Handling feature.



# EW200 Industrial Cellular Gateway

---

The following is the summary list for the provided profiles, and events:

**(Note:** The available profiles and events will vary depending on product model.)

- 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, Wi-Fi 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, Wi-Fi, 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, 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, configure each managing / notifying event by setting the event's trigger condition, and the corresponding actions for the event. For each event, multiple actions can be activated simultaneously.

# EW200 Industrial Cellular Gateway

## 7.2.1 Configuration

Go to **Service > SMS & Event> Configuration** Tab.

Event handling is the service that allows administrator to set up pre-defined events, handlers, or response behavior with individual profiles.

### Enable Event Management

Configuration	
Item	Setting
▶ Event Management	<input type="checkbox"/> Enable

Configuration		
Item	Value setting	Description
Event Management	Unchecked by default	Check the <b>Enable</b> box to activate the Event Management function.

### Enable SMS Management

To use the SMS management function, configure these settings first.

SMS Configuration	
Item	Setting
▶ Message Prefix	<input type="checkbox"/> Enable & <input type="text"/>
▶ Physical Interface	<input type="text" value="3G/4G-1"/> SIM Status: SIM_A
▶ Delete Managed SMS after Processing	<input type="checkbox"/> Enable


SMS Configuration		
Item	Value setting	Description
Message Prefix	Unchecked by default	Click the <b>Enable</b> box to enable the SMS prefix for validating the received SMS. Once the function is enabled, 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.

# EW200 Industrial Cellular Gateway


<b>Physical Interface</b>	The box is 3G/4G-1 by default.	Choose a cellular interface ( <b>3G/4G-1</b> or <b>3G/4G-2</b> ). <b>Note:</b> <b>3G/4G-2</b> is only available for products with dual cellular modules.
<b>SIM Status</b>	N/A	Show the connected cellular service (identified with <b>SIM_A</b> or <b>SIM_B</b> ).
<b>Delete Managed SMS after Processing</b>	Unchecked by default	Check the <b>Enable</b> box to delete the received managing event SMS after it has been processed.

## Create / Edit SMS Account

Set up the SMS Account for managing the gateway through SMS. It supports up to a maximum of 5 accounts.

 <b>SMS Account List</b> <input type="button" value="Add"/> <input type="button" value="Delete"/>						
ID	Phone Number	Phone Description	Application	Send confirmed SMS	Enable	Actions

You can click the **Add / Edit** button to configure the SMS account.

 <b>SMS Account Configuration</b>	
<b>Item</b>	<b>Setting</b>
▶ Phone Number	<span>Specific Number ▼</span> <input type="text"/>
▶ Phone Description	<input type="text"/>
▶ Application	<input type="checkbox"/> Event Trigger <input type="checkbox"/> Notify Handle
▶ Send confirmed SMS	<input type="checkbox"/> Enable
▶ Enable	<input checked="" type="checkbox"/> Enable
<input type="button" value="Save"/>	

SMS Account Configuration		
Item	Value setting	Description
<b>Phone Number</b>	1. Mobile phone number format 2. Required setting	Select the Phone number policy from the dropdown list, and specify a mobile phone number as the SMS account identifier if required. It can be <b>Specific Number</b> , or <b>Allow Any</b> . If <b>Specific Number</b> is selected, specify the phone number as the SMS account identifier. <b>Value Range:</b> -1 ~ 32 digits.
<b>Phone Description</b>	1. Any text 2. Optional setting	Specify a brief description for the SMS account.
<b>Application</b>	Required setting	Specify the application type. It could be <b>Event Trigger</b> , <b>Notify Handle</b> , or <b>both</b> . If the Phone Number policy is <b>Allow Any</b> , the Notify Handle will be unavailable.
<b>Send confirmed SMS</b>	1. Optional setting 2. Unchecked by default	Click the <b>Enable</b> box to activate the SMS response function. The gateway will send a confirmed message back to the sender whenever it receives a SMS managing event. The confirmed message is similar to following

# EW200 Industrial Cellular Gateway

		format: "Device received a SMS with command xxxxx."
<b>Enable</b>	Unchecked by default	Click <b>Enable</b> box to activate this account.
<b>Save</b>	NA	Click the <b>Save</b> button to save the configuration.

## Create / Edit Email Service Account

Set up the Email Service Account for event notification. It supports up to a maximum of 5 accounts.

<div> <div>Email Service List</div> <div>Add</div> <div>Delete</div> </div>				
ID	Email Server	Email Addresses	Enable	Actions

Click the **Add / Edit** button to configure the Email account.

Email Service Configuration	
Item	Setting
▶ Email Server	--- Option --- ▼
▶ Email Addresses	<input type="text"/>
▶ Enable	<input checked="" type="checkbox"/> Enable
<div>Save</div>	

Email Service Configuration		
Item	Value setting	Description
<b>Email Server</b>	--- Option ---	Select an Email Server profile from <b>External Server</b> setting for the email account setting.
<b>Email Addresses</b>	1. Internet E-mail address format 2. Required setting	Specify the Destination Email Addresses.
<b>Enable</b>	Unchecked by default	Click <b>Enable</b> box to activate this account.
<b>Save</b>	NA	Click the <b>Save</b> button to save the configuration

# EW200 Industrial Cellular Gateway

## Create / Edit Digital Input (DI) Profile Rule (DI/DO support required)

Set up the Digital Input (DI) Profile rules. It supports up to a maximum of 10 profiles.

Digital Input (DI) Profile List <span>Add</span> <span>Delete</span>								
ID	DI Profile Name	Description	DI Source	Normal Level	Signal Active Time (s)	Check Interval	Enable	Actions

When the the **Add** button is applied, the **Digital Input (DI) Profile Configuration** screen will appear.

Digital Input (DI) Profile Configuration <span>✕</span>	
Item	Setting
▶ DI Profile Name	<input type="text"/>
▶ Description	<input type="text"/>
▶ DI Source	ID1 ▼
▶ Continues Update Status	<input type="checkbox"/> Enable & Update Interval <input type="text" value="2"/> (2~86400 seconds)
▶ Normal Level	Low ▼
▶ Signal Active Time	<input type="text" value="1"/> (seconds)
▶ Profile	<input checked="" type="checkbox"/> Enable
<span>Save</span>	

Digital Input (DI) Profile Configuration		
Item	Value setting	Description
<b>DI Profile Name</b>	1. String format 2. Required setting	Specify the DI Profile Name. <b>Value Range:</b> -1 ~ 32 characters.
<b>Description</b>	1. Any text 2. Optional setting	Specify a brief description for the profile.
<b>DI Source</b>	ID1 by default	Specify the DI Source. It could be ID1 or ID2. The number of available DI sources will depend on the product model.
<b>Continue Update Status</b>	Uncked by default	Click <b>Enable</b> box to activate this function for the DI event with designated update interval setting. If the event condition keeps active for a long time interval, the gateway will send repeated notify events for each check interval. Value Range: 2 ~ 86400 seconds. Note: To prevent receiving too many notify events for the same situation, you can adjust the check interval to a proper one for your application.
<b>Normal Level</b>	Low by default	Specify the Normal Level: <b>Low</b> or <b>High</b> .
<b>Signal Active Time</b>	1. Numeric String format 2. Required setting	Specify the Signal Active Time. The Signal Active Time setting will be ignored when 'Continue Update Status' function is enabled. <b>Value Range:</b> 1 ~ 10 seconds.
<b>Profile</b>	Unchecked by default	Click <b>Enable</b> box to activate this profile setting.
<b>Save</b>	NA	Click the <b>Save</b> button to save the configuration.

# EW200 Industrial Cellular Gateway

## Create / Edit Digital Output (DO) Profile Rule (DI/DO support required)

Set up the Digital Output (DO) Profile rules. It supports up to a maximum of 10 profiles.

Digital Output (DO) Profile List <span>Add</span> <span>Delete</span>									
ID	DO Profile Name	Description	DO Source	Normal Level	Total Signal Period (ms)	Repeat & Counter	Duty Cycle(%)	Enable	Actions

When the **Add** button is applied, the **Digital Output (DO) Profile Configuration** screen will appear.

Digital Output (DO) Profile Configuration	
Item	Setting
▶ DO Profile Name	<input type="text"/>
▶ Description	<input type="text"/>
▶ DO Source	ID1 ▼
▶ Normal Level	Low ▼
▶ Total Signal Period	<input type="text" value="10"/> (ms)
▶ Repeat & Counter	<input type="checkbox"/> Enable & Counter: <input type="text" value="0"/>
▶ Duty Cycle	<input type="text"/> (%)
▶ Profile	<input checked="" type="checkbox"/> Enable
<span>Save</span>	

Digital Output (DO) Profile Configuration		
Item	Value setting	Description
<b>DO Profile Name</b>	1. String format 2. Required setting	Specify the DO Profile Name. <b>Value Range:</b> -1 ~ 32 characters.
<b>Description</b>	1. Any text 2. Optional setting	Specify a brief description for the profile.
<b>DO Source</b>	ID1 by default	Specify the DO Source.
<b>Normal Level</b>	Low by default	Specify the Normal Level: <b>Low</b> or <b>High</b> .
<b>Total Signal Period</b>	1. Numeric String format 2. Required setting	Specify the Total Signal Period. <b>Value Range:</b> 10 ~ 120000 ms
<b>Repeat &amp; Counter</b>	Unchecked by default	Check the Enable box to activate the repeated Digital Output, and specify the Repeat times. <b>Value Range:</b> 0 ~ 65535
<b>Duty Cycle</b>	1. Numeric String format 2. Required setting	Specify the Duty Cycle for the Digital Output. <b>Value Range:</b> 1 ~100 %
<b>Profile</b>	Unchecked by default	Click <b>Enable</b> box to activate this profile setting.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the configuration.

# EW200 Industrial Cellular Gateway

## Create / Edit Modbus Notifying Events Profile (Modbus support required)

Set up the Modbus Notifying Events Profile. It supports up to a maximum of 10 profiles.

Modbus Notifying Events Profile List <span>Add</span> <span>Delete</span>												
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	<input checked="" type="checkbox"/>	<div>Edit</div> <div>Select</div>

Click the **Add / Edit** button to configure the profile.

Modbus Notifying Events Profile Configuration	
Item	Setting
▶ Modbus Name	<input type="text"/>
▶ Description	<input type="text"/>
▶ Read Function	Read Coils (0x01) ▼
▶ Modbus Mode	Serial ▼
▶ IP	<input type="text"/>
▶ Port	<input type="text"/>
▶ Device ID	<input type="text"/>
▶ Register	<input type="text"/>
▶ Logic Comparator	> ▼
▶ Value	<input type="text" value="0"/>
▶ Enable	<input checked="" type="checkbox"/> Enable
<div>Save</div>	

Modbus Notifying Events Profile		
Item	Value setting	Description
<b>Modbus Name</b>	1. String format 2. Required setting	Specify the Modbus profile name. <b>Value Range:</b> -1 ~ 32 characters.
<b>Description</b>	1. Any text 2. Optional setting	Specify a brief description for the profile.
<b>Read Function</b>	Read Holding Registers by default	Specify the Read Function for <b>Notifying Events</b> .
<b>Modbus</b>	<b>Serial</b> by default	Specify the Modbus Mode: <b>Serial</b> or <b>TCP</b> .

# EW200 Industrial Cellular Gateway

Mode		
IP	1. NA for Serial on Modbus Mode. 2. Required 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. Required setting for TCP on Modbus Mode.	Specify the Port for TCP on Modbus Mode. <b><u>Value Range:</u></b> 1 ~ 65535.
Device ID	1. Numeric String format 2. Required setting	Specify the Device ID of the Modbus device. It can be from 1 to 247.
Register	1. Numeric String format 2. Required setting	Specify the Register number of the Modbus device. <b><u>Value Range:</u></b> 0 ~ 65535.
Logic Comparator	Logic Comparator '>' by default.	Specify the Logic Comparator for <b>Notifying Events</b> . It can be '>', '<', '≐', '>=', or '<='.
Value	1. Numeric String format 2. Required setting	Specify the Value. <b><u>Value Range:</u></b> 0 ~ 65535.
Enable	Unchecked by default	Click <b>Enable</b> box to activate this profile setting.
Save	NA	Click the <b>Save</b> button to save the configuration
Undo	NA	Click the <b>Undo</b> button to restore what you just configured back to the previous setting.



# EW200 Industrial Cellular Gateway

## Create / Edit Modbus Managing Events Profile (Modbus support required)

Set up the Modbus Managing Events Profile. It supports up to a maximum of 10 profiles.

Modbus Managing Events Profile List <span>Add</span> <span>Delete</span>											
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	<input checked="" type="checkbox"/>	<span>Edit</span> <span>Select</span>

You can click the **Add / Edit** button to configure the profile.

Modbus Managing Events Profile Configuration	
Item	Setting
▶ Modbus Name	<input type="text"/>
▶ Description	<input type="text"/>
▶ Write Function	<span>Write Single Coil (0x05)</span> ▼
▶ Modbus Mode	<span>Serial</span> ▼
▶ IP	<input type="text"/>
▶ Port	<input type="text"/>
▶ Device ID	<input type="text"/>
▶ Register	<input type="text"/>
▶ Value	<input type="text" value="0"/>
▶ Enable	<input checked="" type="checkbox"/> Enable
<span>Save</span>	

Modbus Managing Events Profile		
Item	Value setting	Description
Modbus Name	1. String format 2. Required setting	Specify the Modbus profile name. <b><u>Value Range:</u></b> -1 ~ 32 characters.
Description	1. Any text 2. Optional setting	Specify a brief description for the profile.
Write Function	Write Single Registers by default	Specify the Write Function for <b>Managing Events</b> .
Modbus Mode	Serial by default	Specify the Modbus Mode: <b>Serial</b> or <b>TCP</b> .
IP	1. NA for Serial on Modbus	Specify the IP for TCP on Modbus Mode. IPv4 Format.

# EW200 Industrial Cellular Gateway

	Mode. 2. Required setting for TCP on Modbus Mode.	
Port	1. NA for Serial on Modbus Mode. 2. Required setting for TCP on Modbus Mode.	Specify the Port for TCP on Modbus Mode. <b>Value Range:</b> 1 ~ 65535.
Device ID	1. Numeric String format 2. Required setting	Specify the Device ID of the Modbus device. <b>Value Range:</b> 1 ~ 247.
Register	1. Numeric String format 2. Required setting	Specify the Register number of the Modbus device. <b>Value Range:</b> 0 ~ 65535.
Value	1. Numeric String format 2. Required setting	Specify the Value. <b>Value Range:</b> 0 ~ 65535.
Enable	Unchecked by default	Click <b>Enable</b> box to activate this profile setting.
Save	NA	Click the <b>Save</b> button to save the configuration
Undo	NA	Click the <b>Undo</b> button to restore previous settings.

## Create / Edit Remote Host Profile

Set up the Remote Host Profile. It supports up to a maximum of 10 profiles.

Remote Host List <span>Add</span> <span>Delete</span> <span>↑</span> <span>×</span>								
ID	Host Name	Host IP	Protocol Type	Port Number	Prefix Message	Suffix Message	Enable	Actions

You can click the **Add / Edit** button to configure the profile.

Remote Host Configuration <span>×</span>	
Item	Setting
▶ Host Name	<input type="text"/>
▶ Host IP	<input type="text"/>
▶ Protocol Type	TCP ▼
▶ Port Number	<input type="text"/>
▶ Prefix Message	<input type="text"/>
▶ Suffix Message	<input type="text"/>
▶ Enable	<input type="checkbox"/>
<span>Save</span>	

Modbus Managing Events Profile		
Item	Value setting	Description
Host Name	1. String format 2. Required setting	Specify the Remote Host profile name. Value Range: -1 ~ 64 characters.
Host IP	1. Required setting 2. IP address format	Specify the IP address for the Remote Host. IPv4 Format.

# EW200 Industrial Cellular Gateway

<b>Protocol Type</b>	1. Required setting 2. <b>TCP</b> is selected by default	Specify the protocol to access the Remote Host. It can be <b>TCP</b> or <b>UDP</b> .
<b>Port Number</b>	1. Required setting	Specify the Port number for accessing the Remote Host. Value Range: 1 ~ 65535.
<b>Prefix Message</b>	1. String format 2. Optional setting	Specify the Prefix Message string as pre-defined identification for accessing the remote host, if required. Value Range: -1 ~ 64 characters.
<b>Suffix Message</b>	1. String format 2. Optional setting	Specify the Suffix Message string as pre-defined identification for accessing the remote host, if required. Value Range: -1 ~ 64 characters.
<b>Enable</b>	Unchecked by default	Click <b>Enable</b> box to activate this profile setting.
<b>Save</b>	NA	Click the <b>Save</b> button to save the configuration
<b>Undo</b>	NA	Click the <b>Undo</b> button to restore previous settings.

## Create / Edit MQTT Publish Message Profile

Set up the MQTT Publish Message Profile. It supports up to a maximum of 2 profiles.

MQTT Publish Message List <span>Add</span> <span>Delete</span>					
ID	Connection Name	Topic	QoS	Enable	Action
1	Broker01	/Device_01/Event_act01	0	<input checked="" type="checkbox"/>	<span>Publish Now</span> <span>Edit</span> <input type="checkbox"/> Select

You can click the **Add / Edit** button to configure the profile.

When the **Add** button is clicked, the configuration page / **Field Communication / Data Interchange / MQTT** will be displayed. Make sure the MQTT Client is enabled for further adding any MQTT Client Connections for the MQTT Publish Message profile.

Refer to the **MQTT** section for how to configure the details of MQTT Client and Publish Message.

MQTT Client Function

Item

Setting

MQTT Client

☒ Enable

MQTT Client List

Add

Delete

ID	Connection Name	Address	Authentication	Security	Port	Enable	Action
1	Broker01	1.2.3.4	<input type="checkbox"/>	None	1883	<input checked="" type="checkbox"/>	<div>Subscriptions Received List</div> <div>Edit<input type="checkbox"/> Select</div>

For the message to be published via Managing Event or Notifying Event, you have to configure the **Message Style** as “Manual” and further specify the message content as well. Besides, leave the **Publish Behavior** (Auto Publish) unchecked. Refer to the example highlighted in the following image.

# EW200 Industrial Cellular Gateway

Publish Message Configuration	
Item	Setting
▶ Topic	<input type="text" value="/Device_01/Event_act01"/>
▶ Topics prefix	<input type="checkbox"/> Enable
▶ Message Style	<input type="text" value="Manual"/>
▶ Message	<input type="text" value="Event_act01 triggered!"/>
▶ QoS	<input checked="" type="radio"/> 0 (At most once) <input type="radio"/> 1 (At least once) <input type="radio"/> 2 (Exactly once)
▶ Retained	<input type="checkbox"/> Enable
▶ Publish Behavior	<input type="checkbox"/> Auto Publish
▶ Enable	<input checked="" type="checkbox"/>

# EW200 Industrial Cellular Gateway

## 7.2.2 Managing Events

Managing Events allow the administrator to define the relationship (rule) among event triggers, handlers and response.

Go to **Service > Event Handling > Managing Events** Tab.

## Enable Managing Events

Configuration	
Item	Setting
▶ Managing Events	<input type="checkbox"/> Enable

Configuration Item	Value setting	Description
Managing Events	Unchecked by default	Check the <b>Enable</b> box to activate the Managing Events function.

## Create / Edit Managing Event Rules

Set up the Managing Event rules. It supports up to a maximum of 128 rules.

Managing Event List <span>Add</span> <span>Delete</span> <span>↑</span> <span>×</span>						
ID	Event Name	Event	Trigger Type	Description	Enable	Actions

When the **Add** or **Edit** button is applied, the **Managing Event Configuration** screen will appear.

# EW200 Industrial Cellular Gateway

Managing Event Configuration

Item	Setting
▶ Event Name	<input type="text"/>
▶ Event	<div>None ▼</div> <div>None ▼</div> <div>None ▼</div>
▶ Trigger Type	<div>Period ▼</div>
▶ Interval	<div>0</div> (0~86400 seconds)
▶ Description	<div></div>
▶ Action	<div><input type="checkbox"/> Network Status</div> <div><input type="checkbox"/> LAN&amp;VLAN</div> <div><input type="checkbox"/> NAT</div> <div><input type="checkbox"/> Firewall</div> <div><input type="checkbox"/> VPN</div> <div><input type="checkbox"/> GRE</div> <div><input type="checkbox"/> System Manage</div> <div><input type="checkbox"/> Administration</div> <div><input type="checkbox"/> Digital Output</div> <div><input type="checkbox"/> Modbus</div> <div><input type="checkbox"/> Remote Host</div> <div><input type="checkbox"/> MQTT</div>

Save

Managing Event Configuration		
Item	Value setting	Description
Event Name	Blank by default	Specify a name or identifier for this managing event rule. Value Range: 0 ~ 64 characters.
Event	None by default	Specify the Event type ( <b>SMS</b> , <b>SNMP Trap</b> , or <b>Digital Input</b> ) and an event identifier / profile. <b>SMS</b> : Select <b>SMS</b> and enter the message in the textbox as the trigger condition for the event; <b>SNMP</b> : Select <b>SNMP Trap</b> and enter the message in the textbox to specify the SNMP Trap Event; <b>Digital Input</b> : Select <b>Digital Input</b> and a DI profile you defined to specify a certain Digital Input Event;  <i>Note: The available Event Types will depend on product model.</i>
Trigger Type	Period is selected by default	Specify the type of event trigger, either <b>Period</b> or <b>Once</b> . <b>Period</b> : Select <b>Period</b> and specify a time interval, the event will be repeatedly triggered on every time interval when the specified event condition holds. <b>Once</b> : Select <b>Once</b> and the event will be just triggered just one time when the specified event condition holds.
Interval	0 is selected by default	Specify the repeatedly event trigger time interval.

# EW200 Industrial Cellular Gateway

		Value Range: 0 ~86400 seconds.
<b>Description</b>	String format: any text.	Enter a brief description for the Managing Event.
<b>Action</b>	All boxes unchecked by default.	<p>Specify <b>Network Status</b>, or at least one action to take when the expected event is triggered.</p> <p><b>Network Status</b>: Select <b>Network Status</b> Checkbox to get the network status as the action for the event;</p> <p><b>LAN&amp;VLAN</b>: Select <b>LAN&amp;VLAN</b> Checkbox and the relevant sub-items (Port link On/Off), and the gateway will change the settings as the action for the event;</p> <p><b>Wi-Fi</b>: Select <b>Wi-Fi</b> Checkbox and the relevant sub-items (Wi-Fi radio On/Off), the gateway will change the settings as the action for the event;</p> <p><b>NAT</b>: Select <b>NAT</b> Checkbox and the relevant sub-items (Virtual Server Rule On/Off, DMZ On/Off), the gateway will change the settings as the action for the event;</p> <p><b>Firewall</b>: Select <b>Firewall</b> Checkbox and the relevant sub-items (Remote Administrator Host ID On/Off), the gateway will change the settings as the action for the event;</p> <p><b>VPN</b>: Select <b>VPN</b> Checkbox and the relevant 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;</p> <p><b>GRE</b>: Select <b>GRE</b> Checkbox and the relevant sub-items (GRE Tunnel On/Off), the gateway will change the settings as the action for the event;</p> <p><b>System Manage</b>: Select <b>System Manage</b> Checkbox and the relevant sub-items (WAN SSH Service On/Off), the gateway will change the settings as the action for the event;</p> <p><b>Administration</b>: Select <b>Administration</b> Checkbox and the relevant sub-items (Backup Config, Restore Config, Reboot, Save Current Setting as Default), the gateway will change the settings as the action for the event;</p> <p><b>Digital Output</b>: Select <b>Digital Output</b> checkbox and a DO profile you defined as the action for the event;</p> <p><b>Modbus</b>: Select <b>Modbus</b> checkbox and a Modbus Managing Event profile you defined as the action for the event;</p> <p><b>Remote Host</b>: Select <b>Remote Host</b> checkbox and a Remote Host profile you defined as the action for the event;</p> <p><b>MQTT</b>: Select <b>MQTT</b> checkbox and a MQTT Publish Message profile you defined as the action for the event;</p> <p><i>Note: The available Event Types will depend on product model.</i></p>
<b>Managing Event</b>	Unchecked by default	Click <b>Enable</b> box to activate this Managing Event setting.
<b>Save</b>	NA	Click the <b>Save</b> button to save the configuration
<b>Undo</b>	NA	Click the <b>Undo</b> button to restore previous settings.

## 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

Configuration		
Item	Setting	
▶ Notifying Events	<input checked="" type="checkbox"/> Enable	

Configuration		
Item	Value setting	Description
Notifying Events	Unchecked by default	Check the <b>Enable</b> box to activate the Notifying Events function.

### Create / Edit Notifying Event Rules



Set up your Notifying Event rules. Up to 128 rules are supported.

Notifying Event List									
ID	Event Name	Event	Trigger Type	Description	Action	Time Schedule	Enable	Actions	

When the **Add** or **Edit** button is applied, the **Notifying Event Configuration** screen will appear.



# EW200 Industrial Cellular Gateway

Item	Setting
▶ Event Name	<input type="text"/>
▶ Event	<div>None ▼</div> <div>None ▼</div> <div>None ▼</div>
▶ Trigger Type	Period ▼
▶ Interval	0 (0~86400 seconds)
▶ Description	<input type="text"/>
▶ Action	<input type="checkbox"/> Digital Output <input type="checkbox"/> SMS <input type="checkbox"/> Syslog <input type="checkbox"/> SNMP Trap (Only Support v1 and v2c) <input type="checkbox"/> Email Alert <input type="checkbox"/> Modbus <input type="checkbox"/> Remote Host <input type="checkbox"/> MQTT
▶ Time Schedule	(0) Always ▼
▶ Notifying Events	<input checked="" type="checkbox"/> Enable

Save

Notifying Event Configuration		
Item	Value setting	Description
Event Name	Blank by default	Specify a name or identifier for this notifying event rule. Value Range: 0 ~ 64 characters.
Event	Digital Input (or WAN) by default	Specify the Event type and corresponding event configuration. The supported Event Types are: <b>Digital Input:</b> Select <b>Digital Input</b> and a DI profile you defined to specify a certain Digital Input Event; <b>Power Change:</b> Select <b>Power Change</b> and a trigger condition to specify the event on a specific power source. <b>WAN:</b> Select <b>WAN</b> and a trigger condition to specify a certain WAN Event; <b>LAN&amp;VLAN:</b> Select <b>LAN&amp;VLAN</b> and a trigger condition to specify a certain LAN&VLAN Event; <b>Wi-Fi:</b> Select <b>Wi-Fi</b> and a trigger condition to specify a certain Wi-Fi Event; <b>DDNS:</b> Select <b>DDNS</b> and a trigger condition to specify a certain DDNS Event; <b>Administration:</b> Select <b>Administration</b> and a trigger condition to specify a certain Administration Event; <b>Modbus:</b> Select <b>Modbus</b> and a Modbus Notifying Event profile you defined to specify a certain Modbus Event; <b>Data Usage:</b> Select <b>Data Usage</b> , the SIM Card (Cellular Service) and a trigger condition to specify a certain Data Usage Event;  <i>Note: The available Event Types will depend on product model.</i>
Description	String format: any text.	Enter a brief description for the Notifying Event.

## EW200 Industrial Cellular Gateway

<b>Action</b>	All box is unchecked by default.	<p>Specify at least one action to take when the expected event is triggered.</p> <p><b>Digital Output:</b> Select <b>Digital Output</b> checkbox and a DO profile you defined as the action for the event;</p> <p><b>SMS:</b> Select <b>SMS</b>, and the gateway will send out a SMS to all the defined SMS accounts as the action for the event;</p> <p><b>Syslog:</b> Select <b>Syslog</b> and select/unselect the Enable Checkbox to as the action for the event;</p> <p><b>SNMP Trap:</b> Select <b>SNMP Trap</b>, and the gateway will send out SNMP Trap to the defined SNMP Event Receivers as the action for the event;</p> <p><b>Email Alert:</b> Select <b>Email Alert</b>, and the gateway will send out an Email to the defined Email accounts as the action for the event;</p> <p><b>Modbus:</b> Select <b>Modbus</b> and a Modbus Notifying Event profile you defined as the action for the event;</p> <p><b>Remote Host:</b> Select <b>Remote Host</b> checkbox and a Remote Host profile you defined as the action for the event;</p> <p><b>MQTT:</b> Select <b>MQTT</b> checkbox and a MQTT Publish Message profile you defined as the action for the event;</p> <p><i>Note: The available Event Types will depend on product model.</i></p>
<b>Time Schedule</b>	<b>(0) Always</b> is selected by default	Select a time scheduling rule for the Notifying Event.
<b>Notifying Events</b>	Unchecked by default	Click <b>Enable</b> box to activate this Notifying Event setting.
<b>Save</b>	NA	Click the <b>Save</b> button to save the configuration
<b>Undo</b>	NA	Click the <b>Undo</b> button to restore previous settings.

# EW200 Industrial Cellular Gateway

---

## 7.3 Azure Agent

This feature allows for the upload of sensors' data to Azure Server via Azure Agent on EW-200.

Data Flow

Sensor → EW-200 → Azure Server → Azure Remote Monitor

### 7.3.1 Azure Configuration

Go to **Service > Azure Agent > Configuration** Tab.

The configuration steps are as follows:

1. Configure Azure Cloud
  - Register and login Azure Server
  - Install Azure Remote Monitor
  - Build the IoT devices on IoT Hub
2. Configure EW-200
  - Modbus RS-485 setting
  - Data logging
  - Azure Agent
3. Display on Azure Remote Monitor

First, register and log in to the Microsoft Azure site.

<https://portal.azure.com/>

Then, install Azure Remote Monitor

<https://www.azureiotsolutions.com/Accelerators>

After installing and starting the Azure Remote Monitor, you will see the Azure Remote Monitor Page. You can add IoT devices to the Azure Server by clicking on **IoT Hub**, and then click on the **iothub-xmk3h**, which is created by Azure Remote Monitor.

# EW200 Industrial Cellular Gateway

Click on **IoT devices**.


Click **Add** to create a new IoT device.


Enter Device ID.

Select Auto-generate keys.

Save the configuration.

Dashboard > IoT Hub > iothub-xmk3h - IoT devices > Create a device

 **Create a device** □

 Find Certified for Azure IoT devices in the Device Catalog □

\* Device ID ⓘ

ethantest ✓

Authentication type ⓘ

Symmetric key

X.509 Self-Signed

X.509 CA Signed

\* Primary key ⓘ

Enter your primary key

\* Secondary key ⓘ

Enter your secondary key

Auto-generate keys ⓘ

☒

Connect this device to an IoT hub ⓘ

Save

# EW200 Industrial Cellular Gateway

## 7.3.2 EW-200 Azure Configuration

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

Input the parameters and save the configuration.

**Port Configuration** **Virtual COM** **Modbus**

**Serial Port Definition**

Serial Port	Operation Mode	Interface	Baud Rate	Data Bits	Stop Bits	Flow Control	Parity	Action
SPort-0	Modbus ▼	RS-485 ▼	9600 ▼	8 ▼	1 ▼	None ▼	None ▼	<a href="#">Edit</a>

[Save](#) [Undo](#)

Next, navigate to **Field Communication > Bus & Protocol> Modbus** tab.

Input the parameters and save the configuration.

**Port Configuration** **Virtual COM** **Modbus**

**Modbus Gateway Definition**

Serial Port	Gateway Mode	Device Slave Mode	Listen Port	Serial Protocol	Enable	Action
▶ SPort-0	Serial as Slave ▼	Slave Mode: <input checked="" type="checkbox"/> Enable Slave ID: <input type="text" value="101"/> (1~247)	<input type="text" value="502"/> (1~65535)	RTU ▼	<input checked="" type="checkbox"/>	<a href="#">Edit</a>

**Gateway Mode Configuration for SPort-0**

Item	Setting
▶ Response Timeout	<input type="text" value="1000"/> ms (1~65535)
▶ Timeout Retries	<input type="text" value="0"/> times (0~5)
▶ 0Bh Exception	<input type="checkbox"/> Enable
▶ Tx Delay	<input type="checkbox"/> Enable
▶ TCP Connection Idle Time	<input type="text" value="300"/> sec (1~65535)
▶ Maximum TCP Connections	<input type="text" value="1"/> connections (1~4)
▶ TCP Keep-alive	<input type="checkbox"/> Enable
▶ Modbus Master IP Access	Allow All ▼
▶ Message Buffering	<input type="checkbox"/> Enable

[Save](#) [Undo](#)

# EW200 Industrial Cellular Gateway

Next, navigate to **Field Communication > Data Logging> Configuration** tab.

Input the parameters and save the configuration. Repeat the procedure for the **Scheme Setup** and **Log File Management** tabs.

**Configuration** **Scheme Setup** **Log File Management**

**Configuration**

Item	Setting
Data Logging	<input checked="" type="checkbox"/> Enable
Storage Device	Internal ▼

**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
1	azure_test	SPort-0	21 - 21	Read Holding Registers (0x03)	2	1	1000	<b>Edit</b> <input type="checkbox"/> Select

**Modbus Proxy Rule List Configuration** **Save** **Undo**

Item	Setting
Name	azure_test
Modbus Slave Type	Local Serial Port ▼ SPort-0 ▼
Slave ID	21 (1~247) - 21 (1~247)
Function Code	Read Holding Registers (0x03) ▼
Start Address	2 (0~65535)
Number of Coils/Registers	1 (1~125)
Polling Rate (ms)	1000 (500~99999)

Finally, navigate to **Services > Azure Agent**. Click the checkbox to enable Azure agent, and click **Save**. Then use the **Add** button to add Azure rules.

# EW200 Industrial Cellular Gateway

**Configuration**

Item	Setting
Azure Agent	<input checked="" type="checkbox"/> Enable

**Azure Rule List** Add Delete

ID	DeviceId	Sensor Type : Name	ConnectString	Data Period	Enable	Actions
----	----------	--------------------	---------------	-------------	--------	---------

Save Undo

Navigate to the Azure website, and click on the device that you have created.

Dashboard > IoT Hub > iothub-xmk3h - IoT devices

**iothub-xmk3h - IoT devices**

+ Add Refresh Delete

DEVICE ID	STATUS	LAST ACTIVITY	LAST STATUS UPDATE	AUTHENTICATION T...	CLOUD TO DEVICE ...
chiller-01.0	Enabled			Sas	0
chiller-02.0	Enabled			Sas	0
delivery-truck-01.0	Enabled	Tue Feb 26 2019 1...		Sas	0
delivery-truck-02.0	Enabled	Mon Feb 25 2019...		Sas	0
elevator-01.0	Enabled			Sas	0
elevator-02.0	Enabled	Mon Feb 25 2019...		Sas	0
engine-01.0	Enabled			Sas	0
engine-02.0	Enabled			Sas	0
<input checked="" type="checkbox"/> ethantest	Enabled	Tue Feb 26 2019 1...		Sas	0

Click on the button to copy the Connection String.

# EW200 Industrial Cellular Gateway

Dashboard > IoT Hub > iotHub-xmk3h - IoT devices > Device details

## Device details

ethantest

Save Message to device Direct method Device twin Add module identity Regenerate keys Refresh

Device Id: ethantest

Primary key: eJSmJlme3BlzZJR0pa0SLKeVRRSfgMus3gal5OveelU=

Secondary key: 8ChXYLvpYlhY4WgOd4XHtG1nN09+tfWHXtGDghj+mXE=

Connection string (primary key): **HostName=iothub-xmk3h.azure-devices.net;DeviceId=ethantest;SharedAccessKey=eJSmJlme3BlzZJR0pa0SLKeVRRSfgMus3gal5OveelU=**

Connection string (secondary key): HostName=iothub-xmk3h.azure-devices.net;DeviceId=ethantest;SharedAccessKey=8ChXYLvpYlhY4WgOd4XHtG1nN09+tfWHXtGDghj+mXE=

Navigate back to the EW-2000 web console, and paste the Connection String into the corresponding field. Click the checkbox to enable Azure Rule Configuration. Then click **Save**.

### Configuration

Item	Setting
Azure Agent	<input checked="" type="checkbox"/> Enable

### Azure Rule List

Add Delete

ID	DeviceId	Sensor Type : Name	ConnectionString	Enable	Actions
1	ethan1	Modbus Proxy : azure_test	HostName=iothub-e5grf.azure-devices.net;DeviceId=ethan1;SharedAccessKey=e7pie0eh0yRfc1erdbeGcyu2JzBFh4q6zNdda4pe1j8=	<input checked="" type="checkbox"/>	Edit Select

### Azure Rule Configuration

Save Undo






Item	Setting
Sensor Type : Name	Modbus Proxy Select azure_test
ConnectionString	<b>HostName=iothub-xmk3h.azure-devices.net;DeviceId=ethantest;SharedAccessKey=eJSmJlme3BlzZJR0pa0SLKeVRRSfgMus3gal5OveelU=</b>
Enable	<input checked="" type="checkbox"/>


Navigate to the Azure Remote Monitor web console, and click on the newly created device. You will be able to directly monitor the data from the device.



# EW200 Industrial Cellular Gateway

## Devices

■ DEVICE NAME ↕	SIMULATED	DEVICE TYPE	FIRMWARE
■ <a href="#">delivery-truck-02.0</a>	 Yes	Truck	---
■ <a href="#">elevator-01.0</a>	 Yes	Elevator	---
■ <a href="#">elevator-02.0</a>	 Yes	Elevator	---
■ <a href="#">engine-01.0</a>	 Yes	Engine	---
■ <a href="#">engine-02.0</a>	 Yes	Engine	---
■ <a href="#">ethan1</a>	No	---	---



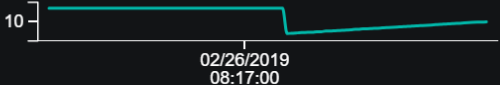
**ethan1**  
Physical  
Connected

### Telemetry

[Explore in Time Series Insights](#) ⓘ

AzureTest [1]    DeviceId [1]

ethan1



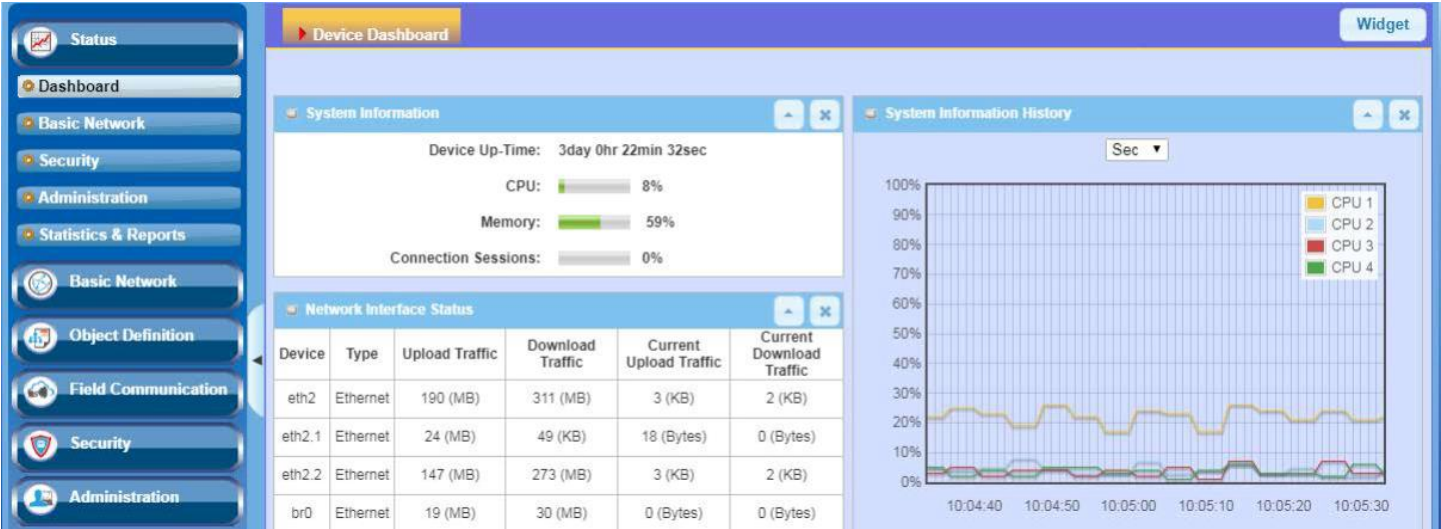
10

02/26/2019 08:17:00

Tags

# Chapter 8 Status

## 8.1 Dashboard

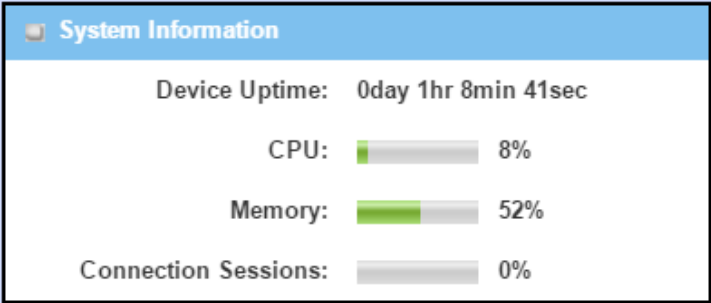


### 8.1.1 Device Dashboard

The **Device Dashboard** window shows the current status in graph or table format for quickly understanding the operation status of the gateway. They are the System Information, System Information History, and Network Interface Status. The display will be refreshed once per second. From the menu on the left, select **Status > Dashboard > Device Dashboard** tab.

#### System Information Status

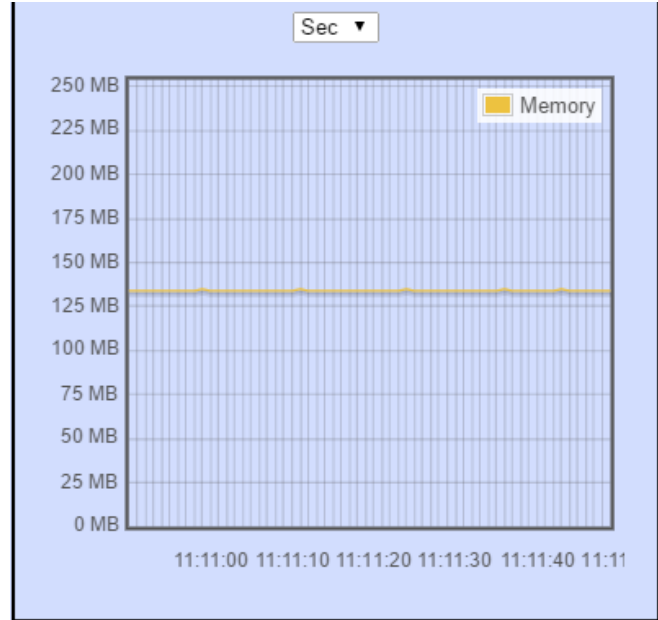
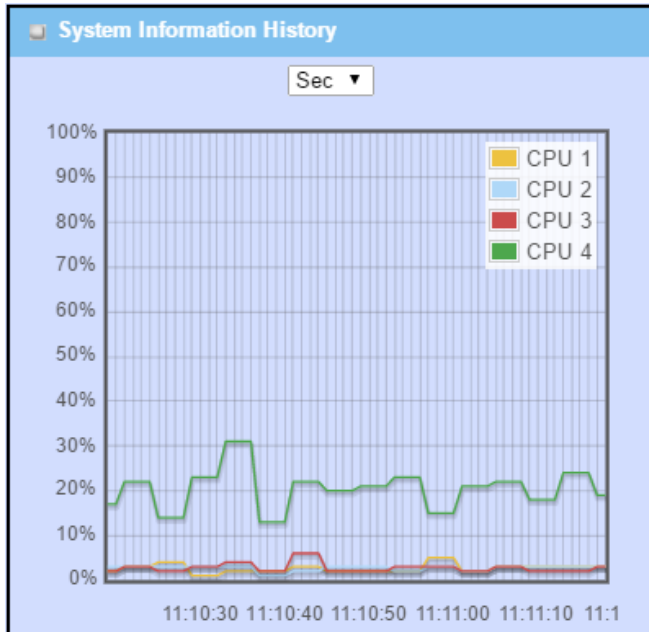
The System Information screen shows the device uptime and the resource utilization for the CPU, Memory, and Connection Sessions.



# EW200 Industrial Cellular Gateway

## System Information History

The **System Information History** screen shows statistical graphs for the CPU and memory.



## Network Interface Status

The **Network Interface Status** screen shows the statistical information for each network interface of the gateway. The statistical information includes the Interface Type, Upload Traffic, Download Traffic, and Current Upload / Download Traffic.

## EW200 Industrial Cellular Gateway

Network Interface Status					
Device	Type	Upload Traffic	Download Traffic	Current Upload Traffic	Current Download Traffic
eth2	Ethernet	211 (MB)	321 (MB)	3 (KB)	3 (KB)
eth2.1	Ethernet	24 (MB)	71 (KB)	64 (Bytes)	0 (Bytes)
eth2.2	Ethernet	168 (MB)	283 (MB)	3 (KB)	3 (KB)
br0	Ethernet	19 (MB)	31 (MB)	42 (Bytes)	0 (Bytes)
ra0	Wireless LAN	1 (MB)	1 (MB)	0 (Bytes)	0 (Bytes)
rai0	Wireless LAN	21 (MB)	42 (MB)	0 (Bytes)	0 (Bytes)
ra1	Wireless LAN	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)
rai1	Wireless LAN	362 (Bytes)	4 (KB)	0 (Bytes)	0 (Bytes)
tun0	Ethernet	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)

## 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 types, including network configuration, connecting information, modem status and traffic statistics. The display will be refreshed every five seconds.

#### WAN interface IPv4 Network Status

The **WAN interface IPv4 Network Status** screen shows status information for IPv4 network.

WAN Interface IPv4 Network Status										
ID	Interface	WAN Type	Network Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Action
WAN-1	3G/4G	3G/4G	NAT	10.59.152.73	255.255.255.252	10.59.152.74	168.95.1.1, 168.95.192.1	N/A	Connected 0 day 0:26:38	Edit
WAN-2		Disable								Edit

#### WAN interface IPv4 Network Status

Item	Value setting	Description
ID	N/A	Displays corresponding WAN interface WAN IDs.
Interface	N/A	Displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, 3G/4G, etc.
WAN Type	N/A	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.
Network Type	N/A	Displays the network type for the WAN interface(s). Depending on the model purchased, it can be NAT, Routing, Bridge, or IP Pass-through.
IP Addr.	N/A	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	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	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	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	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	Displays the connection status of the device to your ISP. Status are Connected or disconnected.

# EW200 Industrial Cellular Gateway

Action	N/A	<b>Renew</b> button allows user to force the device to request an IP address from the DHCP server. Note: <b>Renew</b> button is available when DHCP WAN Type is used and WAN connection is disconnected.
		<b>Release</b> button allows user to force the device to clear its IP address setting to disconnect from DHCP server. Note: <b>Release</b> button is available when DHCP WAN Type is used and WAN connection is connected.
		<b>Connect</b> 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 <b>Edit</b> button in <b>Basic Network &gt; WAN &amp; Uplink &gt; Internet Setup</b> ) and WAN connection status is disconnected.
		<b>Disconnect</b> button allows user to manually disconnect the device from the Internet. Note: <b>Disconnect</b> button is available when Connection Control in WAN Type setting is set to Connect Manually (Refer to <b>Edit</b> button in <b>Basic Network &gt; WAN &amp; Uplink &gt; Internet Setup</b> ) and WAN connection status is connected.

## WAN interface IPv6 Network Status

**WAN interface IPv6 Network Status** screen shows status information for IPv6 networks.

WAN Interface IPv6 Network Status						
ID	Interface	WAN type	Link-local IP Address	Global IP Address	Conn. Status	Action
WAN-1	3G/4G	IPv6		/64	Disconnected	<input type="button" value="Edit"/>

WAN interface IPv6 Network Status		
Item	Value setting	Description
ID	N/A	Displays corresponding WAN interface WAN IDs.
Interface	N/A	Displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, 3G/4G, etc.
WAN Type	N/A	Displays the method which public IP address is obtained from your ISP. WAN type setting can be changed from <b>Basic Network &gt; IPv6 &gt; Configuration</b> .
Link-local IP Address	N/A	Displays the LAN IPv6 Link-Local address.
Global IP Address	N/A	Displays the IPv6 global IP address assigned by your ISP for your Internet connection.
Conn. Status	N/A	Displays the connection status. The status can be connected, disconnected and connecting.
Action	N/A	This area provides functional buttons. <b>Edit Button</b> when pressed, the web-based utility will take you to the IPv6 configuration page. ( <b>Basic Network &gt; IPv6 &gt; Configuration</b> .)

# EW200 Industrial Cellular Gateway

## LAN Interface Network Status

LAN Interface Network Status screen shows IPv4 and IPv6 information of LAN networks.

LAN Interface Network Status					
IPv4 Address	IPv4 Subnet Mask	IPv6 Link-local Address	IPv6 Global Address	MAC Address	Action
192.168.66.1	255.255.254.0	fe80::250:18ff:fe3a:4a5f	/64	00:50:18:3A:4A:5F	<a href="#">Edit IPv4</a> <a href="#">Edit IPv6</a>

LAN Interface Network Status		
Item	Value setting	Description
IPv4 Address	N/A	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	Displays the current mask of the subnet.
IPv6 Link-local Address	N/A	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	Displays the current IPv6 global IP address assigned by your ISP for your Internet connection.
MAC Address	N/A	Displays the LAN MAC address of the gateway.
Action	N/A	This area provides functional buttons. <b>Edit IPv4 Button</b> when press, web-based utility will take you to the Ethernet LAN configuration page. ( <b>Basic Network &gt; LAN &amp; VLAN &gt; Ethernet LAN</b> tab). <b>Edit IPv6 Button</b> when press, web-based utility will take you to the IPv6 configuration page. ( <b>Basic Network &gt; IPv6 &gt; Configuration</b> .)

## 3G/4G Modem Status

3G/4G Modem Status List screen shows status information for 3G/4G WAN network(s).

3G/4G Modem Status List <a href="#">Refresh</a>					
Interface	Card Information	Link Status	Signal Strength	Network Name	Action
3G/4G	ME3620-J	Disconnected	N/A		<a href="#">Detail</a>

3G/4G Modem Status List		
Item	Value setting	Description
Physical Interface	N/A	Displays the type of WAN physical interface. Note: Some device models may support two 3G/4G modules. Their physical interface names will be <b>3G/4G-1</b> and <b>3G/4G-2</b> .
Card Information	N/A	Displays the vendor's 3G/4G modem model name.

# EW200 Industrial Cellular Gateway

Link Status	N/A	Displays the 3G/4G connection status. The status can be Connecting, Connected, Disconnecting, and Disconnected.
Signal Strength	N/A	Displays the 3G/4G wireless signal level.
Network Name	N/A	Displays the name of the service network carrier.
Refresh	N/A	Click the <b>Refresh</b> button to renew the information.
Action	N/A	<b>Detail Button:</b> when pressed, windows with detailed information will appear. They are 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.

Interface Traffic Statistics				
ID	Interface	Received Packets(Mb)	Transmitted Packets(Mb)	Action
WAN-1	3G/4G	217.13	167.09	Reset
WAN-2		-	-	

Interface Traffic Statistics		
Item	Value setting	Description
ID	N/A	Displays corresponding WAN interface WAN IDs.
Interface	N/A	Displays the type of WAN physical interface. Depending on the model, it can be Ethernet, 3G/4G, etc.
Received Packets (Mb)	N/A	Displays the downstream packets (Mb). It is reset when the device is rebooted.
Transmitted Packets (Mb)	N/A	Displays the upstream packets (Mb). It is reset when the device is rebooted.



# EW200 Industrial 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 Client List				
LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time
Ethernet	Dynamic / 192.168.66.100	25613572	00-13-3B-0E-5B-1D	00:15:00

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.

# EW200 Industrial Cellular Gateway

## 8.2.3 Wi-Fi Status

Go to **Status > Basic Network > Wi-Fi** tab.

The **Wi-Fi Status** window shows the overall statistics of Wi-Fi VAP entries.

### Wi-Fi Virtual AP List

The Wi-Fi Virtual AP List shows all of the virtual AP information. The **Edit** button allows for quick configuration changes.

WiFi Module One Virtual AP List									
Op. Band	ID	WiFi Enable	Op. Mode	SSID	Channel	WiFi System	Auth.& Security	MAC Address	Action
2.4G	VAP-1	<input checked="" type="checkbox"/>	WDS Hybrid	Staff_2.4G	Auto	b/g/n Mixed	Auto(None)	00:50:18:14:15:18	<a href="#">Edit</a> <a href="#">QR Code</a>
2.4G	VAP-2	<input type="checkbox"/>	WDS Hybrid	default	Auto	b/g/n Mixed	Auto(None)	02:50:18:10:15:18	<a href="#">Edit</a> <a href="#">QR Code</a>
2.4G	VAP-3	<input type="checkbox"/>	WDS Hybrid	default	Auto	b/g/n Mixed	Auto(None)	02:50:18:11:15:18	<a href="#">Edit</a> <a href="#">QR Code</a>
2.4G	VAP-4	<input type="checkbox"/>	WDS Hybrid	default	Auto	b/g/n Mixed	Auto(None)	02:50:18:12:15:18	<a href="#">Edit</a> <a href="#">QR Code</a>
2.4G	VAP-5	<input type="checkbox"/>	WDS Hybrid	default	Auto	b/g/n Mixed	Auto(None)	02:50:18:13:15:18	<a href="#">Edit</a> <a href="#">QR Code</a>
2.4G	VAP-6	<input type="checkbox"/>	WDS Hybrid	default	Auto	b/g/n Mixed	Auto(None)	02:50:18:14:15:18	<a href="#">Edit</a> <a href="#">QR Code</a>
2.4G	VAP-7	<input type="checkbox"/>	WDS Hybrid	default	Auto	b/g/n Mixed	Auto(None)	02:50:18:15:15:18	<a href="#">Edit</a> <a href="#">QR Code</a>
2.4G	VAP-8	<input checked="" type="checkbox"/>	WDS Hybrid	Guest_2.4G	Auto	b/g/n Mixed	Auto(None)	02:50:18:16:15:18	<a href="#">Edit</a> <a href="#">QR Code</a>

Wi-Fi Virtual AP List		
Item	Value setting	Description
Op. Band	N/A	Displays the Wi-Fi Operation Band (2.4G or 5G) of VAP.
ID	N/A	Displays the ID of VAP.
Wi-Fi Enable	N/A	Displays whether the VAP wireless signal is enabled or disabled.
Op. Mode	N/A	The Wi-Fi Operation Mode of VAP. Depending on device model, modes are AP Router, WDS Only and WDS Hybrid, Universal Repeater and Client.
SSID	N/A	Displays the network ID of VAP.
Channel	N/A	Displays the wireless channel used.
Wi-Fi System	N/A	The Wi-Fi System of VAP.
Auth. & Security	N/A	Displays the authentication and encryption type used.
MAC Address	N/A	Displays MAC Address of VAP.
Action	N/A	Click the <b>Edit</b> button to quickly access the Wi-Fi configuration page. ( <b>Basic Network &gt; Wi-Fi &gt; Configuration</b> tab) The <b>QR Code</b> button allows you to generate QR code for quick connection to the VAP by scanning the QR code.

# EW200 Industrial Cellular Gateway

## Wi-Fi IDS Status

The Wi-Fi Traffic Statistic shows all the received and transmitted packets on Wi-Fi network.

WiFi Module One IDS Status								
Authentication Frame	Association Request Frame	Re-association Request Frame	Probe Request Frame	Disassociation Frame	Deauthentication Frame	EAP Request Frame	Malicious Data Frame	Action
0	0	0	0	0	0	0	0	<input type="button" value="Reset"/>

Wi-Fi IDS Status		
Item	Value setting	Description
Authentication Frame	N/A	Displays the receiving Authentication Frame count.
Association Request Frame	N/A	Displays the receiving Association Request Frame count.
Re-association Request Frame	N/A	Displays the receiving Re-association Request Frame count.
Probe Request Frame	N/A	Displays the receiving Probe Request Frame count.
Disassociation Frame	N/A	Displays the receiving Disassociation Frame count.
Deauthentication Frame	N/A	Displays the receiving Deauthentication Frame count.
EAP Request Frame	N/A	Displays the receiving EAP Request Frame count.
Malicious Data Frame	N/A	Displays the number of receiving unauthorized wireless packets.
Action	N/A	Click the <b>Reset</b> button to clear the entire statistic and reset counter to 0.

---

Ensure WIDS function is enabled

Go to Basic Network > Wi-Fi > Advanced Configuration tab

Note that the WIDS of 2.4G or 5G should be configured separately.

---

# EW200 Industrial Cellular Gateway

## Wi-Fi Traffic Statistics

The Wi-Fi Traffic Statistics shows all the received and transmitted packets on Wi-Fi network.

WiFi Module One Traffic Statistics <span>Refresh</span>				
Op. Band	ID	Received Packets	Transmitted Packets	Action
2.4G	VAP-1	0	0	<span>Reset</span>
2.4G	VAP-2	0	0	<span>Reset</span>
2.4G	VAP-3	0	0	<span>Reset</span>
2.4G	VAP-4	0	0	<span>Reset</span>
2.4G	VAP-5	0	0	<span>Reset</span>
2.4G	VAP-6	0	0	<span>Reset</span>
2.4G	VAP-7	0	0	<span>Reset</span>
2.4G	VAP-8	0	0	<span>Reset</span>

Wi-Fi Traffic Statistic		
Item	Value setting	Description
<b>Op. Band</b>	N/A	Displays the Wi-Fi Operation Band (2.4G or 5G) of VAP.
<b>ID</b>	N/A	Displays the VAP ID.
<b>Received Packets</b>	N/A	Displays the number of received packets.
<b>Transmitted Packet</b>	N/A	Displays the number of transmitted packets.
<b>Action</b>	N/A	Click the <b>Reset</b> button to clear individual VAP statistics.
<b>Refresh Button</b>	N/A	Click the <b>Refresh</b> button to update the entire VAP Traffic Statistic instantly.

## 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

DDNS Status List				
Host Name	Provider	Effective IP	Last Update Status	Last Update Time

DDNS Status		
Item	Value Setting	Description
Host Name	N/A	Displays the name you entered to identify DDNS service provider
Provider	N/A	Displays the DDNS server of DDNS service provider
Effective IP	N/A	Displays the public IP address of the device updated to the DDNS server
Last Update Status	N/A	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	Displays time stamp of the last update of public IP address to the DDNS server.
Refresh	N/A	The <b>refresh</b> button allows user to force the display to refresh information.

8.3 Security



8.3.1 VPN Status

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

The **VPN Status** widow shows the overall VPN tunnel status. The display will be refreshed every five seconds.

IPsec Tunnel Status

**IPsec Tunnel Status** windows show the configuration for establishing IPsec VPN connection and current connection status.


IPSec Tunnel Status						
Edit						
Tunnel Name	Tunnel Scenario	Local Subnets	Remote IP/FQDN	Remote Subnets	Conn. Time	Status
IPsec Tunnel Status						
Item	Value setting	Description				
Tunnel Name	N/A	Displays the tunnel name you have entered.				
Tunnel Scenario	N/A	Displays the Tunnel Scenario specified.				
Local Subnets	N/A	Displays the Local Subnets specified.				
Remote IP/FQDN	N/A	Displays the Remote IP/FQDN specified.				
Remote Subnets	N/A	Displays the Remote Subnets specified.				
Conn. Time	N/A	Displays the connection time for the IPsec tunnel.				

# EW200 Industrial Cellular Gateway

Status	N/A	Displays the Status of the VPN connection: Connected, Disconnected, Wait for traffic, and Connecting.
Edit Button	N/A	Click the Edit Button to change IPsec setting, the web-based utility will take you to the IPsec configuration page. ( <b>Security &gt; VPN &gt; IPsec</b> tab)

## 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		<a href="#">Edit</a>				
User Name		Remote IP/FQDN		Virtual IP/Mac	Conn. Time	Status

OpenVPN Server Status		
Item	Value setting	Description
User Name	N/A	Displays the Client name you have entered for identification.
Remote IP/FQDN	N/A	Displays the public IP address (the WAN IP address) of the connected OpenVPN Client
Virtual IP/MAC	N/A	Displays the virtual IP/MAC address assigned to the connected OpenVPN client.
Conn. Time	N/A	Displays the connection time for the corresponding OpenVPN tunnel.
Status	N/A	Displays the connection status of the corresponding OpenVPN tunnel. The status can be Connected, or Disconnected.

## OpenVPN Client Status

OpenVPN Client Status

Edit

Detail

ID	OpenVPN Client Name	Interface	Remote IP/FQDN	Remote Subnet	Virtual IP	Conn. Time	Conn. Status
OpenVPN Client Status							
Item	Value setting		Description				
OpenVPN Client Name	N/A		Displays the Client name you have entered for identification.				
Interface	N/A		Displays the WAN interface specified for the OpenVPN client connection.				
Remote IP/FQDN	N/A		Displays the peer OpenVPN Server's Public IP address (the WAN IP address) or FQDN.				
Remote Subnet	N/A		Displays the Remote Subnet specified.				
Virtual IP	N/A		Displays the virtual IP address				
Conn. Time	N/A		Displays the connection time for the corresponding OpenVPN tunnel.				
Conn. Status	N/A		Displays the connection status of the corresponding OpenVPN tunnel. The status can be Connected, or Disconnected.				

# EW200 Industrial Cellular Gateway

## L2TP Server/Client Status

**L2TP Server/Client Status** shows the configuration for establishing L2TP 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	Displays the login name of the user used for the connection.
Remote IP	N/A	Displays the public IP address (the WAN IP address) of the connected L2TP client.
Remote Virtual IP	N/A	Displays the IP address assigned to the connected L2TP client.
Remote Call ID	N/A	Displays the L2TP client Call ID.
Conn. Time	N/A	Displays the connection time for the L2TP tunnel.
Status	N/A	Displays the Status of each of the L2TP client connection: Connected, Disconnect, Connecting
Edit	N/A	Click on <b>Edit</b> Button to change L2TP server settings, the web-based utility will take you to the L2TP server page. ( <b>Security &gt; VPN &gt; L2TP</b> 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	Displays Name for the L2TP Client specified.
Interface	N/A	Displays the WAN interface with which the gateway will use to request PPTP tunneling connection to the PPTP server.
Virtual IP	N/A	Displays the IP address assigned by Virtual IP server of L2TP server.
Remote IP/FQDN	N/A	Displays the L2TP Server's Public IP address (the WAN IP address) or FQDN.
Default Gateway/Remote Subnet	N/A	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	Displays the connection time for the L2TP tunnel.
Status	N/A	Displays the Status of the VPN connection: Connected, Disconnect, and Connecting.
Edit	N/A	Click on <b>Edit</b> Button to change L2TP client settings, the web-based utility will take you to the L2TP client page. ( <b>Security &gt; VPN &gt; L2TP</b> tab)



# EW200 Industrial 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	Displays the login name of the user used for the connection.
Remote IP	N/A	Displays the public IP address (the WAN IP address) of the connected PPTP client.
Remote Virtual IP	N/A	Displays the IP address assigned to the connected PPTP client.
Remote Call ID	N/A	Displays the PPTP client Call ID.
Conn. Time	N/A	Displays the connection time for the PPTP tunnel.
Status	N/A	Displays the Status of each of the PPTP client connection: Connected, Disconnect, and Connecting.
Edit Button	N/A	Click on <b>Edit</b> Button to change PPTP server settings, the web-based utility will take you to the PPTP server page. ( <b>Security &gt; VPN &gt; PPTP</b> 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	Displays the Name for the PPTP Client specified.
Interface	N/A	Displays the WAN interface with which the gateway will use to request PPTP tunneling connection to the PPTP server.
Virtual IP	N/A	Displays the IP address assigned by Virtual IP server of PPTP server.
Remote IP/FQDN	N/A	Displays the PPTP Server's Public IP address (the WAN IP address) or FQDN.
Default Gateway / Remote Subnet	N/A	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	Displays the connection time for the PPTP tunnel.
Status	N/A	Displays the Status of the VPN connection: Connected, Disconnect, and Connecting.
Edit Button	N/A	Click on <b>Edit</b> Button to change PPTP client settings, the web-based utility will take you to the PPTP server page. ( <b>Security &gt; VPN &gt; PPTP</b> tab)

# EW200 Industrial 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 packets dropped by the firewall rule policies, and includes the administrator remote login settings specified in the Firewall Options. The display will be refreshed every five seconds.

By clicking the icon [+], the status table will be expanded to display log history. Clicking the Edit button will switch the view to the configuration page.

### Packet Filter Status

Packet Filters <span>Edit</span> <span>[ + ]</span>			
Activated Filter Rule	Detected Contents	IP	Time

Packet Filter Status		
Item	Value setting	Description
Activated Filter Rule	N/A	The Packet Filter Rule name.
Detected Contents	N/A	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 <span>Edit</span> <span>[ + ]</span>			
Activated Blocking Rule	Blocked URL	IP	Time

URL Blocking Status		
Item	Value setting	Description
Activated Blocking Rule	N/A	The URL Blocking Rule name.


# EW200 Industrial Cellular Gateway

<b>Blocked URL</b>	N/A	The logged packet information.
<b>IP</b>	N/A	The Source IP (IPv4) of the logged packet.
<b>Time</b>	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

 <b>Web Content Filters</b> <span>Edit</span> <span>[ + ]</span>			
<b>Activated Filter Rule</b>	<b>Detected Contents</b>		<b>IP</b>
			<b>Time</b>

Web Content Filter Status		
Item	Value setting	Description
<b>Activated Filter Rule</b>	N/A	Logged packet of the rule name. String format.
<b>Detected Contents</b>	N/A	Logged packet of the filter rule. String format.
<b>IP</b>	N/A	Logged packet of the Source IP. IPv4 format.
<b>Time</b>	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.*

# EW200 Industrial Cellular Gateway

## MAC Control Status

MAC Control <div>Edit</div> <div>[ + ]</div>				
Activated Control Rule	Blocked MAC Addresses		IP	Time
MAC Control Status				
Item	Value setting	Description		
Activated Control Rule	N/A	The MAC Control Rule name.		
Blocked MAC Addresses	N/A	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 <div>Edit</div> <div>[ + ]</div>				
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.

# EW200 Industrial Cellular Gateway

## IPS Status

IPS <span>Edit</span> <span>[+]</span>		
Detected Intrusion	IP	Time
IPS Firewall Status		
Item	Value setting	Description
Detected Intrusion	N/A	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 <span>Edit</span> <span>▲</span> <span>✕</span>			
Stealth Mode	SPI	Discard Ping from WAN	Remote Administrator Management
Disable	Disable	Disable	IP: 192.168.121.54, User Name: admin, Time: Apr 1 11:14:54
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.

## 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 and UPnP. The display will be refreshed every five seconds.

#### SNMP Linking Status

**SNMP Link Status** screen shows the status of current active SNMP connections.

SNMP Linking Status						
User Name	IP Address	Port	Community	Auth. Mode	Privacy Mode	SNMP Version

SNMP Link Status		
Item	Value setting	Description
User Name	N/A	Displays the user name for authentication. This is only available for SNMP version 3.
IP Address	N/A	Displays the IP address of SNMP manager.
Port	N/A	Displays the port number used to maintain connection with the SNMP manager.
Community	N/A	Displays the community for SNMP version 1 or version 2c only.
Auth. Mode	N/A	Displays the authentication method for SNMP version 3 only.
Privacy Mode	N/A	Displays the privacy mode for version 3 only.
SNMP Version	N/A	Displays the SNMP Version employed.

#### SNMP Trap Information

**SNMP Trap Information** screen shows the status of current received SNMP traps.

SNMP Trap Information		
Trap Level	Time	Trap Event

SNMP Trap Information		
Item	Value setting	Description
Trap Level	N/A	Displays the trap level.
Time	N/A	Displays the timestamp of trap event.
Trap Event	N/A	Displays the IP address of the trap sender and event type.

# EW200 Industrial Cellular Gateway

## TR-069 Status

The **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 <b>On</b> when the device is connected with the TR-068 server or <b>Off</b> when disconnected.

## 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



## 8.5 Statistics & Reports

### 8.5.1 Connection Session

Go to **Status > Statistics & Reports > Connection Session** tab.

**Internet Surfing Statistic** shows the connected tracks on this router.

Internet Surfing List (33 entries)					
User Name	Protocol	Internal IP & Port	MAC	External IP &Port	Duration Time
	UDP	192.168.123.100:51736		192.168.123.254:53	2017/03/22 03:43~
	UDP	192.168.123.100:55986		192.168.123.254:53	2017/03/22 03:43~
	UDP	192.168.123.100:49548		192.168.123.254:53	2017/03/22 03:43~
	UDP	192.168.123.100:60969		192.168.123.254:53	2017/03/22 03:43~
	UDP	192.168.123.100:56053		192.168.123.254:53	2017/03/22 03:43~

Internet Surfing Statistic		
Item	Value setting	Description
Previous	N/A	Click the <b>Previous</b> button to see the previous page of track list.
Next	N/A	Click the <b>Next</b> button to see the next page of track list.
First	N/A	Click the <b>First</b> button to see the first page of track list.
Last	N/A	Click the <b>Last</b> button to see the last page of track list.
Export (.xml)	N/A	Click the <b>Export (.xml)</b> button to export the list to xml file.
Export (.csv)	N/A	Click the <b>Export (.csv)</b> button to export the list to csv file.
Refresh	N/A	Click the <b>Refresh</b> button to refresh the list.

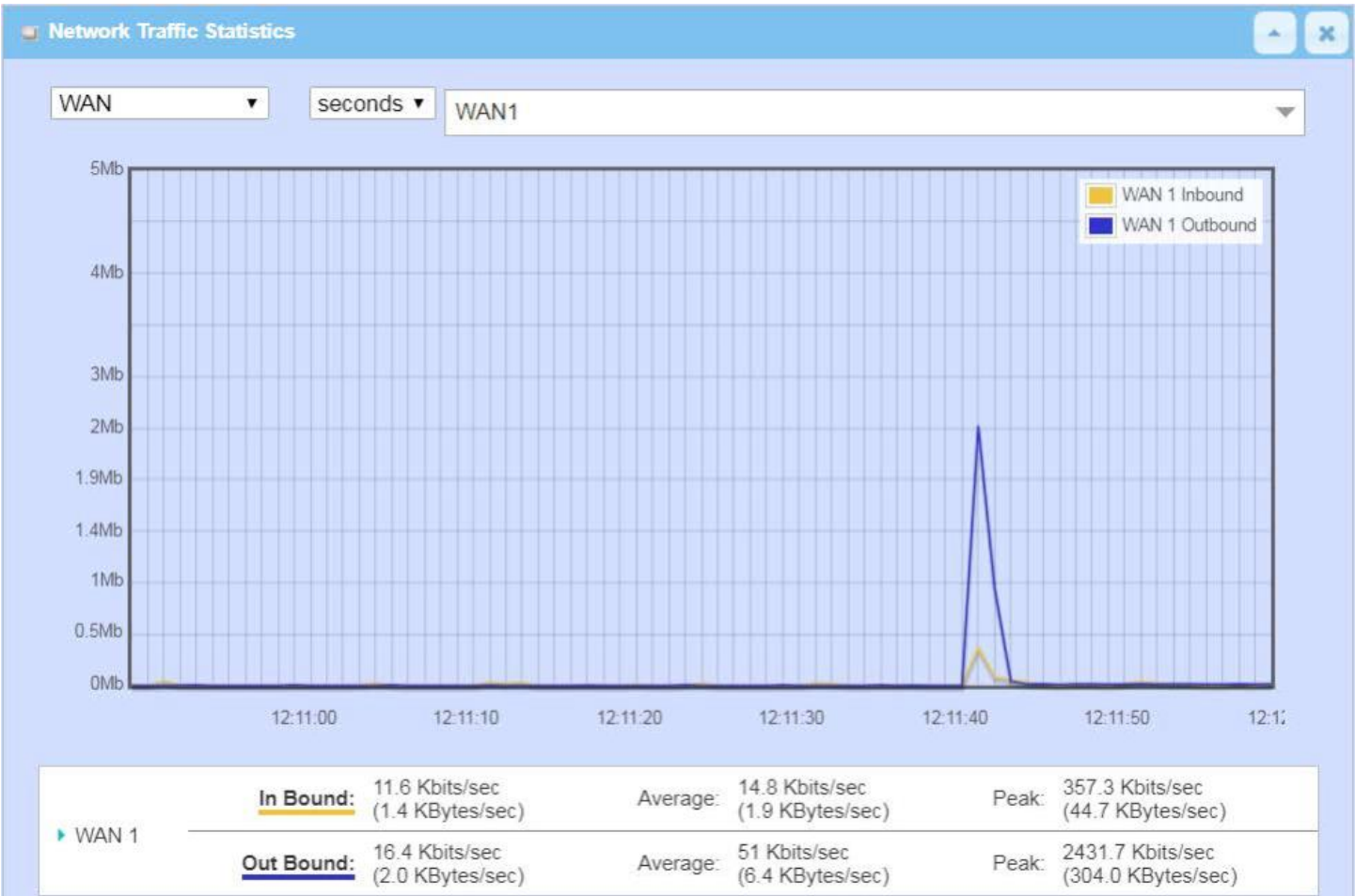
# EW200 Industrial Cellular Gateway

## 8.5.2 Network Traffic

Go to **Status > Statistics & Reports > Network Traffic** tab.

**Network Traffic Statistics** screen shows the historical graph for the selected network interface.

Use the interface dropdown list to select the interface you want to monitor.



# EW200 Industrial Cellular Gateway

## 8.5.3 Device Administration

Go to **Status > Statistics & Reports > Login Statistics** tab.

**Login Statistics** shows the login information.

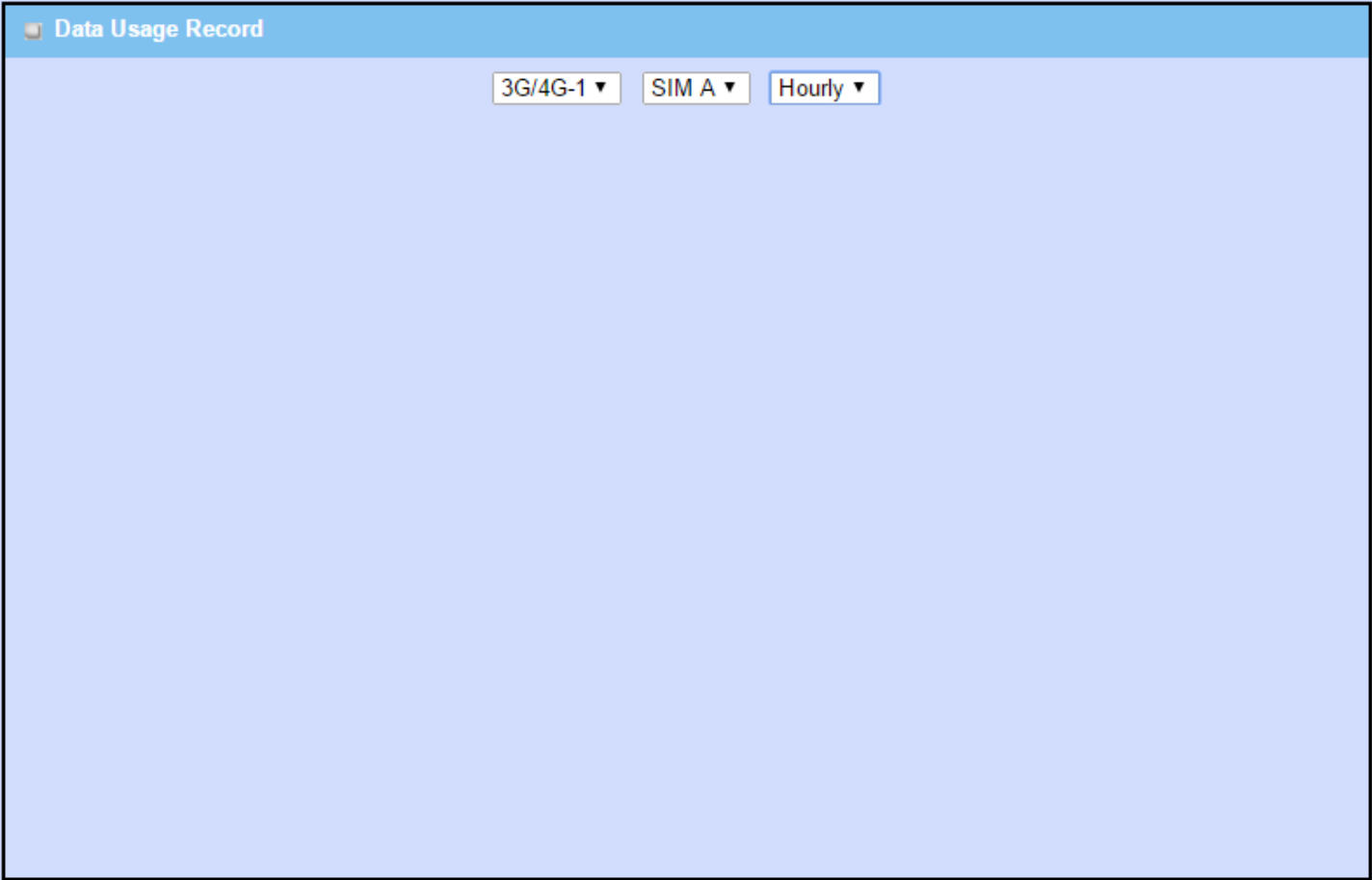
Device Manager Login Statistics				
<div>PreviousNextFirstLastExport (.xml)Export (.csv)</div>				
<div>Refresh</div>				
User Name	Protocol Type	IP Address	Info	Duration Time
admin	HTTP	192.168.123.190	Admin	2018/01/01 00:00~
admin	HTTP	192.168.123.190	Admin	2018/01/01 00:02~
admin	HTTP	192.168.123.190	Login Fail	2019/06/05 16:30~
admin	HTTP	192.168.123.190	Admin	2019/06/05 16:30~

Device Manager Login Statistic		
Item	Value setting	Description
Previous	N/A	Click the <b>Previous</b> button to see the previous page of login statistics.
Next	N/A	Click the <b>Next</b> button to see the next page of login statistics.
First	N/A	Click the <b>First</b> button to see the first page of login statistics.
Last	N/A	Click the <b>Last</b> button to see the last page of login statistics.
Export (.xml)	N/A	Click the <b>Export (.xml)</b> button to export the login statistics to xml file.
Export (.csv)	N/A	Click the <b>Export (.csv)</b> button to export the login statistics to csv file.
Refresh	N/A	Click the <b>Refresh</b> button to refresh the login statistics.

## 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.



# EW200 Industrial Cellular Gateway

## 8.5.4 Cellular Signal

Go to **Status > Statistics & Reports > Cellular Signal** tab.

**Cellular Signal** screen shows signal information for the selected cellular interface.

The screenshot shows the 'Cellular Signal' tab selected in the top navigation bar. The main content area has a light blue background. At the top of this area is a 'Cellular Signal Record' header with a close button. Below the header is a form with two dropdown menus. The first dropdown menu has the text 'Please at least select one option' and a downward arrow. The second dropdown menu is set to 'hours' and also has a downward arrow. Below the form, the text 'Waiting for Data!!!' is displayed in red.

Connection Session Network Traffic Login Statistics Cellular Usage Cellular Signal Widget

Cellular Signal Record

Please at least select one option hours

Waiting for Data!!!

# EW200 Industrial Cellular Gateway

## Specifications

Cellular Interface	
Standards	Cellular Frequency Bands: (Refer to order information for optional bands) 4G LTE: FDD-LTE, TDD-LTE 3G: WCDMA 2G: GSM/EDGE
Antenna connectors	2 x SMA Male
SIM Slots	2

WLAN Interface	
WiFi	802.11 a/b/g/n/ac 2T2R (2.4G/5GHz selectable)
Frequency Band	Europe / CE 2.4 GHz (13 channels) 5GHz (4 channels) America / FCC 2.4GHz (11 channels) 5GHz (9 channels) Taiwan / NCC 2.4GHz(11 channels) 5GHz (9 channels) Singapore / iDA 2.4GHz (13 channels) 5GHz (9 channels)
Encryption Security	WEP 、 WPA 1/2-PAK & WPA 1/2 (8 x VAP / SSID)
Antenna connector	2 x SMA Female

Ethernet	
Standard	IEEE 802.3 10Base-T IEEE802.3u 100BASE-TX/100BASE-FX IEEE802.3ab 1000BASE-T IEEE802.1x, Full duplex flow control
Ports	1 x RJ45 GE (WAN/LAN configurable) + 4*RJ45 GE
Physical Layer	10/100/1000Base-T

## EW200 Industrial Cellular Gateway

---

Serial	
Ports	1 x RS-232/RS-485

I/O	
Digital I/O	1 x DI ("Logic 0": 0~2V, "Logic 1": 5V~30V), 1 x DO (Relay Mode, up to 30V / 1A)

USB	
Standard	USB 2.0
Ports	1 x USB Type A

Functions	
Wi-Fi LAN	AP Router, WDS, WDS Hybrid Modes
VLAN	Port-based, Tag-based VLAN
Port Forwarding	Virtual Server/ Computer, DMZ Host, PPTP/L2TP/IPSec Pass-through
Routing	Static, Dynamic: RIP1/RIP2, OSPF, BGP
QoS	Policy-based Bandwidth Control and Packet Flow Prioritization
Virtual COM	RFC 2217, TCP Client, TCP Server, UDP
Modbus	Modbus Slave; Modbus Gateway for Modbus TCP, Modbus RTU/ASCII Master/Slave Access
VPN	IPSec, OpenVPN, PPTP, L2TP, GRE
Firewall	SPI Firewall with Stealth Mode, IPS
Event Handling	Managing / Notifying Events; DI, DO, Modbus, SMS, Syslog, SNMP Trap, Email Alert, Reboot
Device Management Solution	eVue (Q4, 2018)

Power	
Redundant Input Power	2 x DC 12V ~ 48V (Terminal Block)
Power Consumption	Max. 20W

## EW200 Industrial Cellular Gateway

---

Physical	
Dimensions (W x D x H)	62 x 125 x 160mm (w/o mounting kit) 62 x 135 x 160mm (with DIN Rail kit) 200 x 125 x 65mm (with Bracket kit)
Weight	1.2Kg (2.64lb)
Mounting	DIN-Rail / Wall mount

Environmental	
Operating Temperature	-30 to +70°C (-22 to +158°F)
Storage Temperature	-40 to +85°C (-40 to +185°F)
Relative Humidity	5% to 95% (non-condensing)

Regulatory Approvals	
GSM/UMTS	PTCRB (Q4, 2018)
Emissions / Immunity	CE / FCC / NCC BSMI / iDA
Safety	EN 60950-1 EN 62368-1:2014



## Contact Information

**EtherWAN System, Inc.**

[www.etherwan.com](http://www.etherwan.com)

---

### **USA Office**

2301 E. Winston Road  
Anaheim, CA 9280  
Tel: +1-714-779-3800  
Email: [info@etherwan.com](mailto:info@etherwan.com)

### **Pacific Rim Office**

8F., No.2, Alley 6, Lane 235, Baoqiao Rd.  
Xindian District, New Taipei City 231  
Taiwan  
Tel: +886 -2- 6629-8986  
Email: [info@etherwan.com.tw](mailto:info@etherwan.com.tw)

---

EtherWAN has made a good faith effort to ensure the accuracy of the information in this document and disclaims the implied warranties of merchantability and fitness for a particular purpose, and makes no express warranties, except as may be stated in its written agreement with and for its customers.

EtherWAN shall not be held liable to anyone for any indirect, special or consequential damages due to omissions or errors. The information and specifications in this document are subject to change without notice.

Copyright 2020. All Rights Reserved.

All trademarks and registered trademarks are the property of their respective owners

EW200 Industrial Cellular Gateway

September 24, 2020