



# AIR PACE

## Industrial Smart IoT Edge Computing Gateway

Rediscover Data from The Edge

User Manual

# AiR PACE

## **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:**

AiR PACE 1-XX-CX Series (LTE Version)

AiR PACE 1-XX-CL Series (LoRa Version)

**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 1	10/31/2019	First edition of this document.

## 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 Notice .....	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 .....	17
1.6.1 Insert the SIM Card, MicroSD Card .....	17
1.6.2 Mount the Unit .....	18
1.6.3 Install the External RF Cable and Antenna .....	18
1.6.4 Connecting I/O Devices.....	19
1.6.5 Connecting Serial Devices .....	21
1.6.6 Connecting Power.....	21
1.6.7 Connecting to the Network or a Host .....	22
1.6.8 Setup by Configuring WEB UI .....	22
Chapter 2 Status .....	23
2.1 Dashboard.....	23
2.1.1 Device Dashboard .....	23
2.2 Basic Network .....	25
2.2.1 WAN & Uplink Status .....	25
2.2.2 LAN & VLAN Status .....	29
2.2.3 DDNS Status.....	30
2.3 Security .....	31



2.3.1 VPN Status .....	31
2.3.2 Firewall Status .....	36
2.4 Administration.....	40
2.4.1 Configure & Manage Status .....	40
2.4.2 Log Storage Status .....	42
2.4.3 GNSS Status .....	43
2.5 Statistics & Reports .....	44
2.5.1 Connection Session.....	44
2.5.2 Network Traffic .....	45
2.5.3 Login Statistics .....	46
2.5.4 Cellular Usage.....	47
2.5.4 Cellular Signal .....	47
Chapter 3 Basic Network.....	48
3.1 WAN & Uplink .....	48
3.1.1 Physical Interface .....	49
3.1.2 Connection Setup .....	54
3.1.3 Load Balance .....	74
3.2 LAN & VLAN.....	79
3.2.1 Ethernet LAN .....	79
3.2.2 VLAN.....	81
3.2.3 DHCP Server .....	94
3.3 Port Forwarding.....	102
3.3.1 Configuration.....	103
3.3.2 Virtual Server & Virtual Computer .....	104
3.3.3 Special AP & ALG.....	110
3.3.4 DMZ & Pass Through.....	114
3.4 Routing.....	117
3.4.1 Static Routing.....	118
3.4.2 Dynamic Routing.....	121
3.4.3 Routing Information.....	129

3.5	DNS & DDNS .....	130
3.5.1	DNS & DDNS Configuration .....	130
3.6	QoS .....	134
3.6.1	QoS Configuration .....	134
3.7	Redundancy .....	143
3.7.1	VRRP .....	143
Chapter 4	Object Definition .....	146
4.1	Scheduling .....	146
4.1.1	Scheduling Configuration .....	146
4.2	Grouping .....	148
4.2.1	Host Grouping .....	148
4.3	External Server .....	150
4.4	Certificate .....	153
4.4.1	Configuration .....	153
4.4.2	My Certificate .....	156
4.4.3	Trusted Certificate .....	163
4.4.4	Issue Certificate .....	170
Chapter 5	Field Communication .....	173
5.1	Bus & Protocol .....	173
5.1.1	Port Configuration .....	173
5.1.2	Virtual COM .....	175
5.1.3	Modbus .....	186
5.2	Data Interchange .....	196
5.2.1	MQTT .....	196
5.3	Data Logging .....	207
5.3.1	Data Logging Configuration .....	210
5.3.2	Scheme Setup .....	212
5.3.3	Log File Management .....	214
Chapter 6	Security .....	216
6.1	VPN .....	216
6.1.1	IPSec .....	217

6.1.2 OpenVPN .....	225
6.1.3 L2TP .....	238
6.1.4 PPTP .....	246
6.1.5 GRE .....	253
6.1.6 EoGRE .....	256
6.2 Firewall .....	259
6.2.1 Packet Filter .....	260
6.2.2 URL Blocking .....	265
6.2.3 MAC Control .....	268
6.2.4 IPS .....	271
6.2.5 Options .....	275
Chapter 7 Administration .....	279
7.1 Configure & Manage .....	279
7.1.1 Command Script .....	280
7.1.2 TR-069 .....	284
7.1.3 SNMP .....	289
7.1.4 Telnet & SSH .....	300
7.1.5 LLDP .....	304
7.2 System Operation .....	305
7.2.1 Password & MMI .....	305
7.2.2 System Information .....	308
7.2.3 System Time .....	309
7.2.4 System Log .....	314
7.2.5 Backup & Restore .....	319
7.2.6 Reboot & Reset .....	320
7.3 FTP .....	321
7.3.1 Server Configuration .....	322
7.3.2 User Account .....	324
7.4 Diagnostic .....	325
7.4.1 Diagnostic Tools .....	325

7.4.2 Packet Analyzer.....	326
Chapter 8 Service.....	329
8.1 LoRa .....	329
8.1.1 LoRa Gateway.....	331
8.1.2 LoRa Network Server .....	333
8.2 Cellular Toolkit.....	339
8.2.1 Data Usage .....	340
8.2.2 SMS .....	343
8.2.3 SIM PIN.....	347
8.2.4 USSD.....	351
8.2.5 Network Scan.....	354
8.3 AWS Greengrass .....	356
8.3.1 Configuration Steps.....	358
8.3.2 Installing Greengrass on AiR PACE .....	359
8.4 SMS & Event.....	361
8.4.1 Configuration .....	362
8.4.2 Managing Events.....	366
8.4.3 Notifying Events.....	369
8.5 Azure Run Time .....	371
8.5.1 Setup - Get Connection String from Edge Device.....	371
8.5.2 Start Azure Runtime.....	377
8.5.3 Deploy a module.....	378
8.5.4 Show module status in Azure Runtime UI.....	381
8.6 Location Tracking.....	383
8.6.1 GNSS.....	384
Chapter 9 User Application .....	390
9.1 Edge Computing .....	392
9.1.1 Python .....	392
9.1.2 Node-RED .....	401
Appendix A GPL WRITTEN OFFER .....	410
Contact Information.....	415

## Chapter 1 Introduction

### 1.1 Introduction

Congratulations on your purchase of this outstanding product: AiR PACE, the EtherWAN Industrial Smart IoT Edge Computing Gateway for Internet of Things (IoT), is a configurable and manageable wireless gateway. The Air Pace features various interfaces and supports useful user application tools to meet IoT applications. It provides real-time data analysis and intelligent processing at the fieldbus edge, which is more effective and secure. The Air Pace is both Microsoft Azure IoT edge certified and AWS IoT Greengrass qualified. Quick-to-deploy, the Air Pace smart gateway can be tailored to any IoT application needs.

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

This AiR PACE is loaded with luxuriant security features including VPN, firewall, NAT, port forwarding, DHCP server and many other powerful features for industrial IoT (IIoT) applications.

Main Features:

#### **Highly-reliable network connection**

- » Offers multiple Internet access methods: Gigabit Ethernet, Global 3G/LTE Cat. 4 networks.
- » With support of Dual-SIM, redundant link backup, and VRRP hot standby, the gateway ensures continuous connection by seamless transition to a backup link when main link fails.

#### **Powerful edge computing capabilities**

- » ARM Cortex-A53 processor, 1GHz main frequency, up to 1GB DDR3 RAM and 8GB eMMC FLASH give the gateway powerful edge computing capabilities to perform data optimization, real-time response, agile connection, smart applications, security and privacy protection at the IoT edge

#### **Optional LoRa Gateway with network server for accessing up to 300 of LoRa Edge Nodes nearby**

#### **Compatible with multiple industrial protocols**

- » Modbus RTU, Modbus TCP
- » MQTT for Cloud Connectivity

#### **Comprehensive Data Security VPN Protocols**

- » IPSec, OpenVPN, PPTP, GRE and L2TP VPN

#### **Integrated 12 bit A/D converter for I/O application**

#### **Band management for band lock function**

#### **Instant analytics and precise reaction on edge with Node-RED flow-based programming for IoT applications**

#### **Supports Python development for custom user applications**

#### **Supports major cloud platforms**

- » Microsoft Azure IOT Edge and AWS Greengrass ready for creating user applications, plus Cloud computing enablement on the edge


# AiR PACE

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

## 1.2 Contents List

### 1.2.1 Package Contents

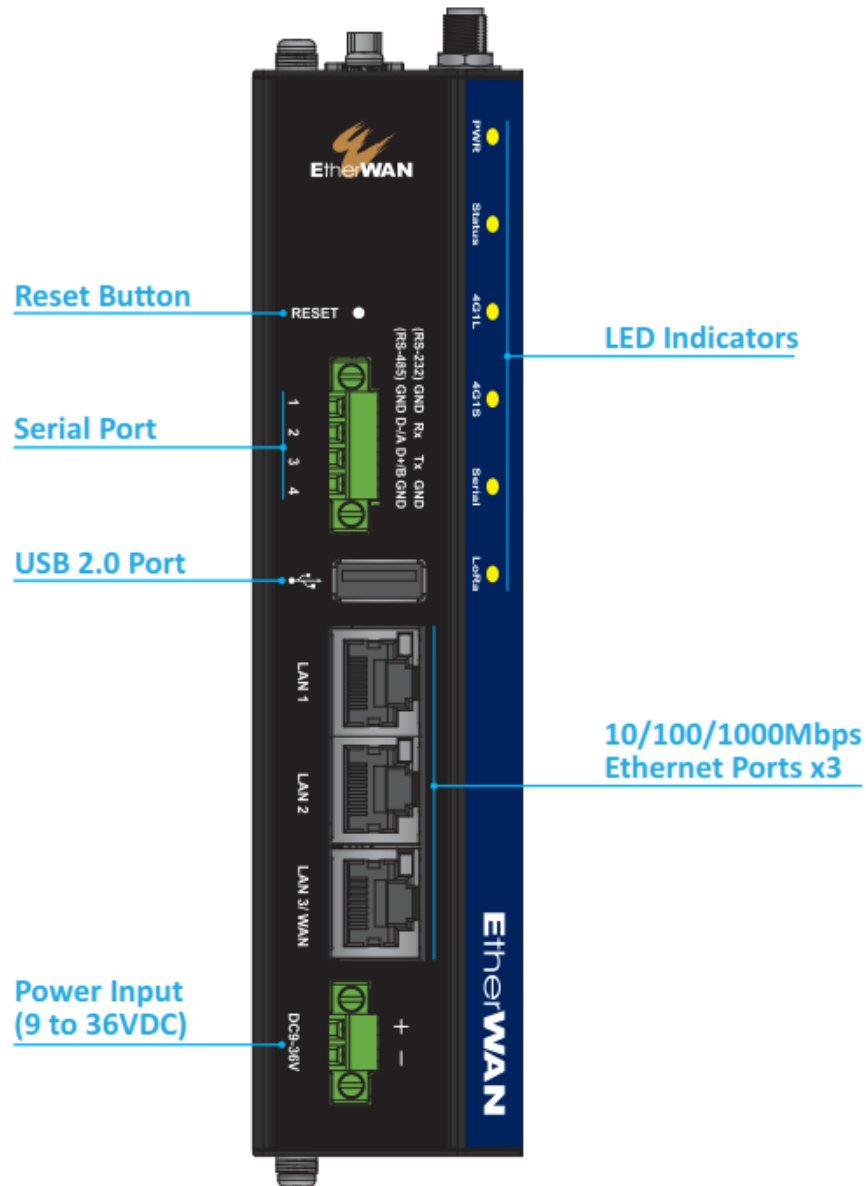
#### #Standard Package

Items	Description	Contents	Quantity
1	AiR PACE Industrial Smart Edge Computing Gateway(*1)		1pcs
2	10 pin Terminal Block		1pcs
3	4 pin Terminal Block		1pcs
4	2 pin Terminal Block		1pcs
5	Antennas		2pcs (3 pcs LoRa Model)
6	DIN-Rail Bracket		1pcs
7	GNSS cable and antenna		1pc
8	SD Card		1pc

1 The maximum power consumption of AiR PACE is 20.0 Watts

## 1.3 Hardware Configuration

### ➤ Front View

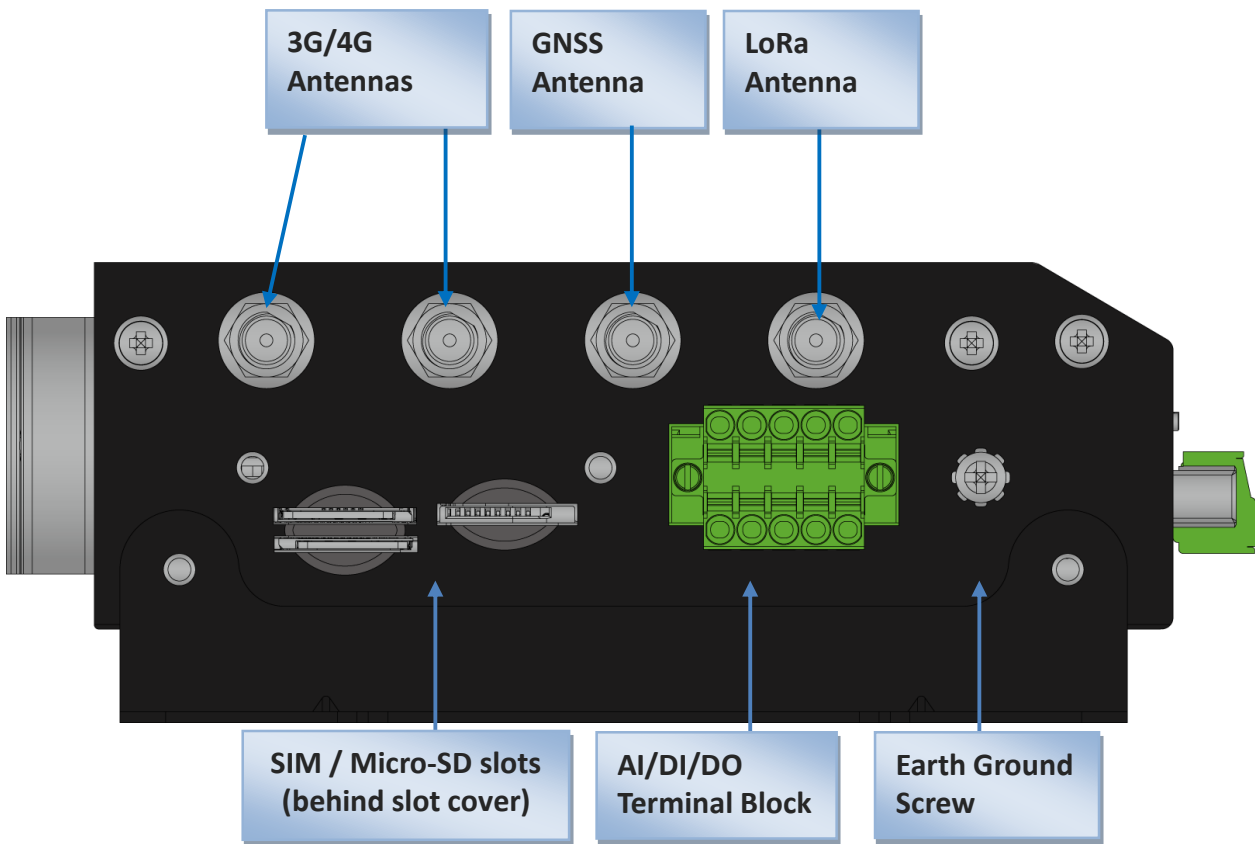


#### ✂ Reset Button

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


# AIR PACE

## ➤ Left View





## 1.4 LED Indicators

LED Icon	Indication	LED Color	Description
<b>PWR</b>	Power Source	Blue	<b>Steady ON:</b> Device is powered ON by power source
<b>Status</b>	Status	Blue	<b>Slow Flash(per Second):</b> Device works normally <b>Very Fast Flash:</b> Device is in Recovery Mode or abnormal
<b>Serial</b>	Serial	Blue	<b>OFF:</b> No Serial data transferred via serial port <b>In Flashing:</b> while data packet transferred via Serial port
<b>4G1L</b>	4G1 Link/Act	Blue	<b>OFF:</b> No data packet transferred via 4G-1 interface <b>Flashing:</b> while data packet transferred via 4G-1 interface
<b>4G1S</b>	4G1 Strength	Blue	<b>Steady On:</b> 4G1 Signal Strength is 61~100% <b>Slow Flash(per Second):</b> 4G1 Signal Strength is 31~60% <b>Fast Flash(per 0.5 second):</b> 4G1 Signal Strength is 0~30%
<b>LoRa</b>	LoRa Signal (AiR PACE-1 XX CL series only)	Blue	<b>OFF:</b> Disabled <b>Steady On:</b> LoRa Gateway enabled <b>Flashing:</b> Data transferred via LoRa interface
	LAN 1 ~ LAN 3/WAN	Green	<b>Steady ON:</b> Ethernet connection of LAN or WAN is established. <b>Flash:</b> Data packets are transferring. <b>OFF:</b> No Ethernet cable attached or Device not linked.

## 1.5 Installation & Maintenance Notice

### 1.5.1 SYSTEM REQUIREMENTS

Network Requirements	<ul style="list-style-type: none"><li>• A gigabit Ethernet RJ-45 cable</li><li>• 3G/4G cellular service subscription</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 operating for a long time, installed at a closed cabinet without air conditioning support, or in a high ambient temperature space.

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

## 1.5.4 Product Information for CE RED Requirements

The following product information is required to be presented in accordance with the latest CE RED requirements.<sup>2</sup>

### (1) Frequency Band & Maximum Power

#### 1.a Frequency Band for Cellular Connection (for EC25-EU version)

Band number	Operating Frequency	Max output power
LTE FDD BAND 1	Uplink: 1920-1980 MHz Downlink: 2110-2170 MHz	23.1 dBm
LTE FDD BAND 3	Uplink: 1710-1785 MHz Downlink: 1805-1880 MHz	23.0 dBm
LTE FDD BAND 7	Uplink: 2500-2570 MHz Downlink: 2620-2690 MHz	22.8 dBm
LTE FDD BAND 8	Uplink: 880-915 MHz Downlink: 925-960 MHz	23.2 dBm
LTE FDD BAND 20	Uplink: 832-862 MHz Downlink: 791-821 MHz	23.5 dBm
LTE FDD BAND 38	Uplink: 2570-2620 MHz Downlink: 2570-2620 MHz	21.7 dBm
LTE FDD BAND 40	Uplink: 2300-2400 MHz Downlink: 2300-2400 MHz	21.5 dBm
WCDMA BAND 1	Uplink: 1920-1980 MHz Downlink: 2110-2170 MHz	23.3 dBm
WCDMA BAND 8	Uplink: 880-915 MHz Downlink: 925-960 MHz	
E-GSM	Uplink: 880-915 MHz Downlink: 925-960 MHz	32.9 dBm
DCS	Uplink: 1710-1785 MHz Downlink: 1805-1880 MHz	29.9 dBm

#### 1.d Frequency Band for LoRa Connection

Band	Operating Frequency	Max. Output Power (EIRP)
868M	863 - 870MHz	100 mW

<sup>2</sup> The information presented in this section is ONLY valid for the EU/EFTA regional version.

## 1.6 Hardware Installation

Hereunder list the available hardware ports of AIR PACE:

- **SIM Slot:** 2 x Micro-SIM (3FF) slot
- **Ethernet:** 3 x 10/100/1000Mbps RJ-45 LAN ports, including one LAN/WAN configurable port
- **LoRa:** 1 x LoRa Gateway (8 channel) (\*For AiR PACE 1-XX-CL Series only)
- **Analog Input:** 2 x AI ports (supports 0~10V)
- **Digital Input:** 2 x DI ports (isolated, "Logic 0": 0~2V, "Logic 1": 5~30V)
- **Digital Output:** 2 x DO ports (isolated, Non-Relayed Output, Maximum 24V/300mA for each port)
- **Field Bus:** 1 x RS-232/485 for legacy serial device, or Modbus RTU/ASCII devices
- **USB Port:** 1 x USB 2.0 Type A port
- **Storage:** 1 x MicroSD slot for SD 3.0 (SDXC) compliant storage expansion
- **Power Source:** 1 x 2-pin Terminal Block for 9~36V DC power

This section describes how to install and configure the hardware.

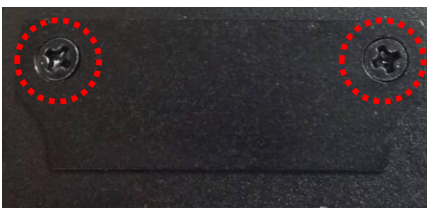
### 1.6.1 Insert the SIM Card, MicroSD Card

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

The SIM card slots are located at the left side of the device housing. You need to unscrew and remove the outer SIM card cover before installing or removing the SIM card and/or MicroSD card. Insert a SIM card as shown in the pictures below.

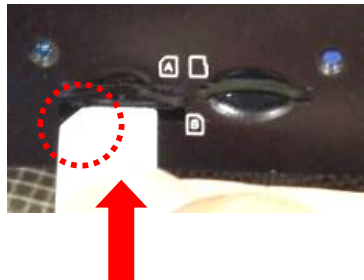
#### Step 1:

Loosen the screws as shown and remove the SIM cover.



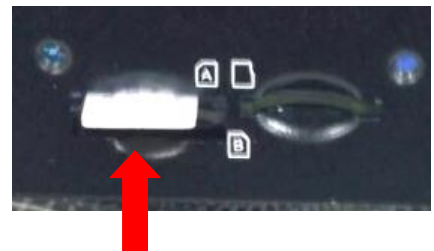
#### Step 2:

Push the SIM card into the slot A (SIM-A) or slot B (SIM-B).



#### Step 3:

Push the inserted SIM card again to eject it from the SIM slot.



## 1.6.2 Mount the Unit

The AIR PACE can be mounted on a wall, horizontal plane, or DIN Rail in a cabinet with the mounting accessories (DIN-rail kit or optional brackets).

## 1.6.3 Install the External RF Cable and Antenna

As illustrated in Section 1.3, there are several SMA antenna Jacks for you to install the required RF cables and antennas for the RF signal transmission and receiving. You must purchase required RF cables and antennas separately for a specific project or installation site to get excellent RF performance.

Since there is limited spacing for allocating all SMA antenna Jacks around the enclosure, the separation among SMA Jacks (or direct-attached antennas) could be not the optimized arrangement. **It is not recommended to attach the SMA antennas directly to the SMA Jacks.** It is very likely to result in degraded RF performance in specific circumstances. It depends heavily on the environment.

However, there are some rules of thumb for solving the antenna separation issue.

- 1: The horizontal distance between antennas should be greater than 1/4 of its wavelength, and there will be best separation at 1/2 of its wavelength.**
- 2. If multiple frequency antennas are near each other, then use spacing distance of the lower frequency antenna, or even better try to satisfy the rule for both frequencies.**

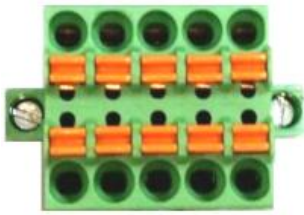
**Wavelength Table for Major RF Category**

RF Category	Frequency	Wavelength	1/2 Wave Length (Best Separation)	1/4 Wave Length (Good Separation)
Cellular LTE	2600MHz	11.5cm	5.8cm	2.9cm
Cellular LTE	2100MHz	14.3cm	7.1cm	3.7cm
Cellular LTE	900MHz	33.3cm	16.6cm	8.3cm
Cellular LTE	700MHz	42.8cm	21.4cm	10.7cm
GPS	1.57GHz	19.0cm	9.5cm	4.7cm

It is recommended to use external RF cables to extend and separate the adjacent antennas and get better antenna separation and RF performance.

## 1.6.4 Connecting I/O Devices

There are multiple AI/DI/DO ports together with a 10-pin terminal block. Please refer to following pin assignment and specification to connect Input and Output devices



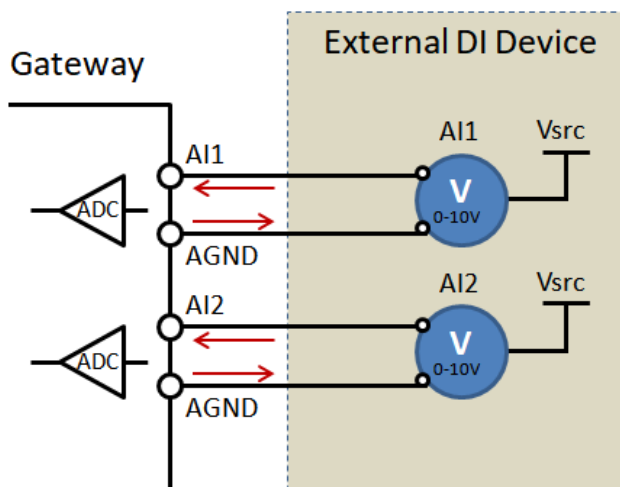
AGND	AGND	DO1	DO_COM	DO2
1	2	3	4	5
6	7	8	9	10
AI1	AI2	DI1	DI_COM	DI2

Mode	Specification	
Analog Input	0-10V analog Voltage	with 12-bit ADC, sample rate upto 125kHz; +/- 2.5mV precision
Digital Input (Isolated)	Trigger Voltage (high)	Logic level 1: 5V~30V
	Normal Voltage (low)	Logic level 0: 0V~2V
Digital Output (Isolated)	Voltage (Non-Relayed Mode)	Depends on external device maximum voltage is 24V/300mA

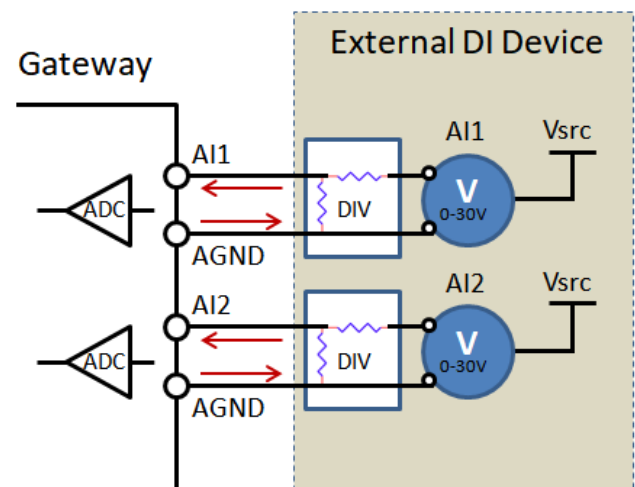
If the AI signal range of your device will run out off the design spec. of AiR PACE (0-10V), you need to add a scaling circuit to prevent overflow readings and possible damage to the AiR PACE.

### Example of AI Connection Diagram

#### (1) AI Connection (for 0~10V signal)

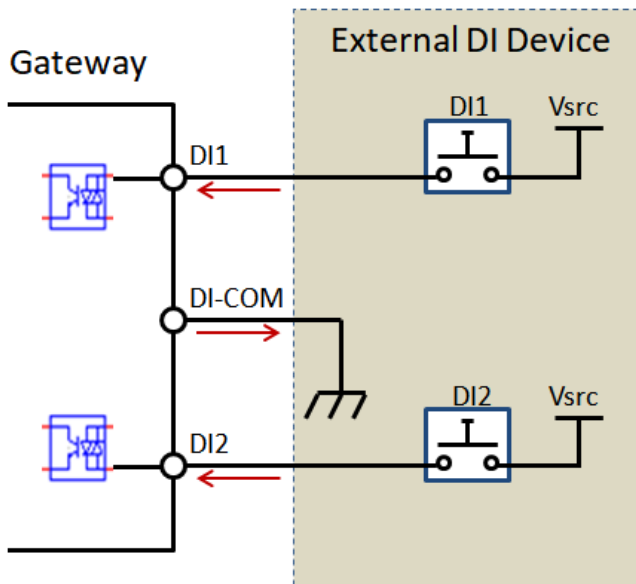


#### (2) AI Connection (for > 10V signal)

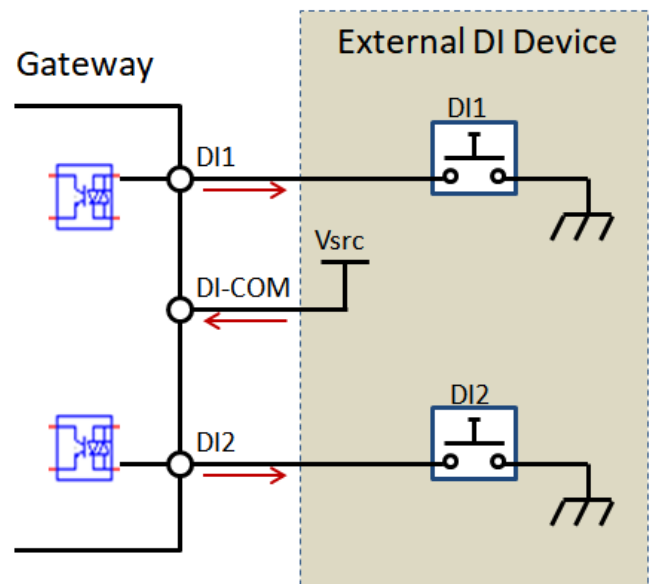


### Example of DI Connection Diagram

## (1) Sink-type DI Connection

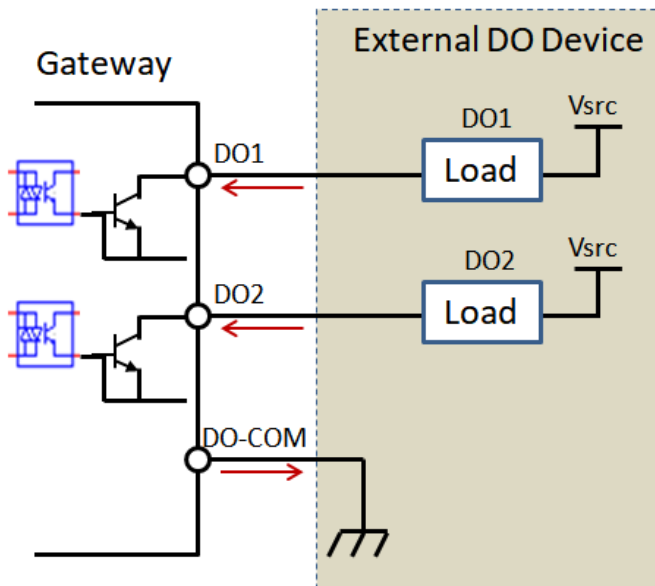


## (2) Source-type DI Connection

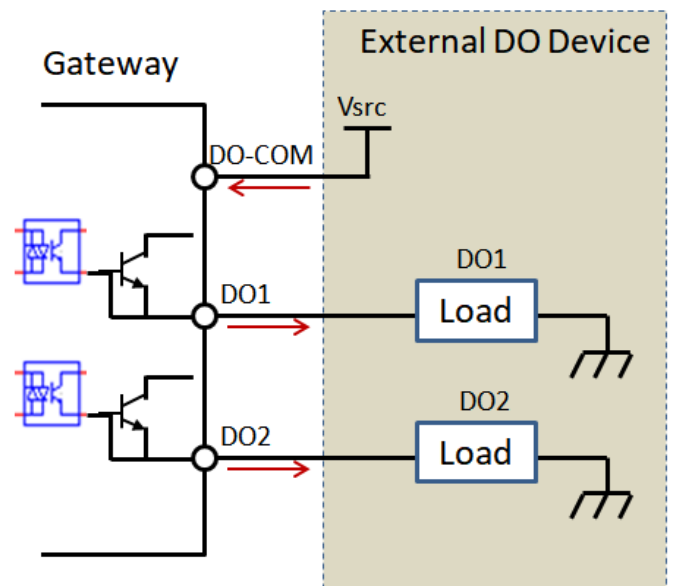


## Example of DO Connection Diagram

### (1) Sink-type DO Connection



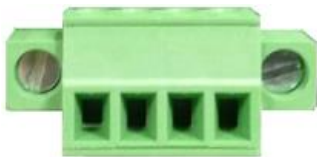
### (2) Source-type DO Connection





1.6.5 Connecting Serial Devices

The AiR PACE provides 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 are shown as below.



	1	2	3	4
RS-232	GND	RxD	TxD	GND
RS-485	GND	D- (A)	D+ (B)	GND

1.6.6 Connecting Power

The AiR PACE can be powered by connecting DC power source to the 2-pin power terminal block. **It supports 9 to 36V DC power input.** The following picture indicates the power terminal block pin assignments. Please check carefully and connect to the right power requirements and polarity.



# AIR PACE

## 1.6.7 Connecting to the Network or a Host

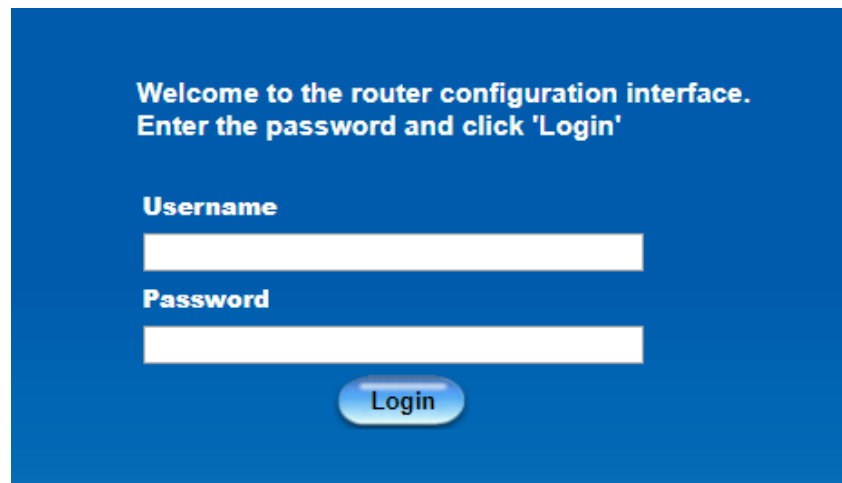
The AiR PACE provides RJ-45 ports to connect 10/100/1000Mbps Ethernet. It can auto detect the transmission speed on the network and configure itself automatically. Connect one Ethernet cable to the RJ-45 port (LAN) of the device and plug another end of the Ethernet cable into your computer's network port. In this way, you can use the RJ-45 Ethernet cable to connect to the host PC's Ethernet port for configuring the device.

## 1.6.8 Setup by Configuring WEB UI

You can browse web UI to configure the device. Type in the IP Address (<http://192.168.123.254>)<sup>3</sup>



When you see the login page, enter the user name and password and then click '**Login**' button. The default setting for both username and password is '**admin**'<sup>4</sup>.

A screenshot of a web interface for a router configuration. The background is blue. At the top, white text reads: "Welcome to the router configuration interface. Enter the password and click 'Login'". Below this, there are two white input fields. The first is labeled "Username" and the second is labeled "Password". At the bottom, there is a blue button with the word "Login" in white text.

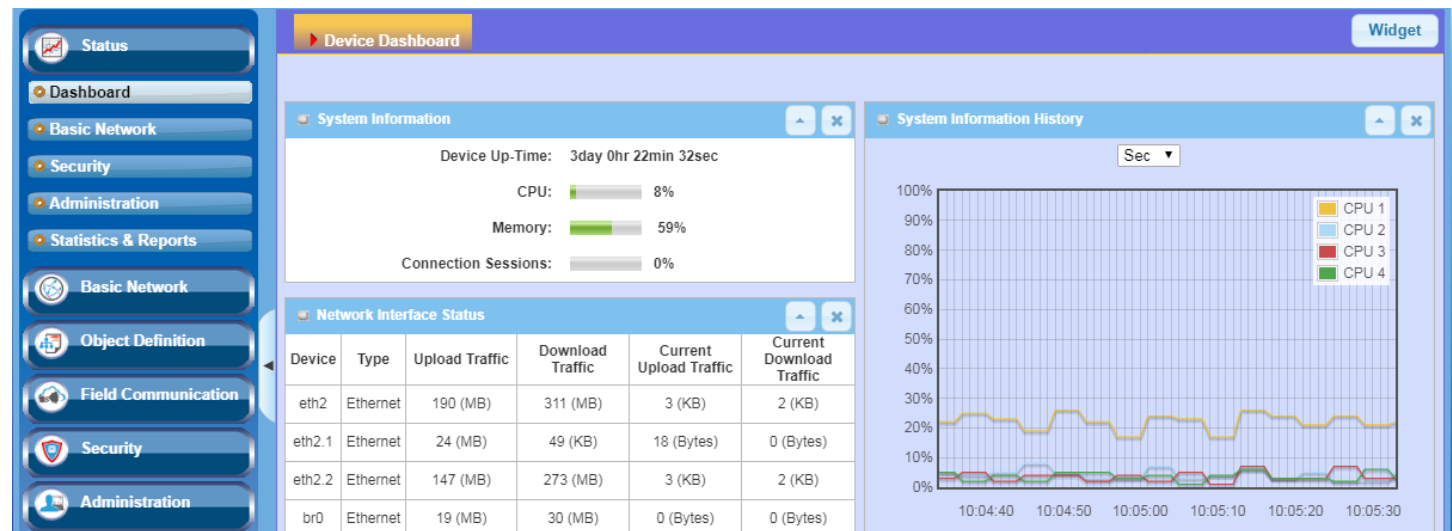
---

<sup>3</sup> The default LAN IP address of this gateway is 192.168.123.254. If you change it, you will need to log in again using the new IP address.

<sup>4</sup> For security considerations, you are strongly recommended to change the login username and password from the default values. Refer to Section 6.1.2 for how to change the settings.

# Chapter 2 Status

## 2.1 Dashboard



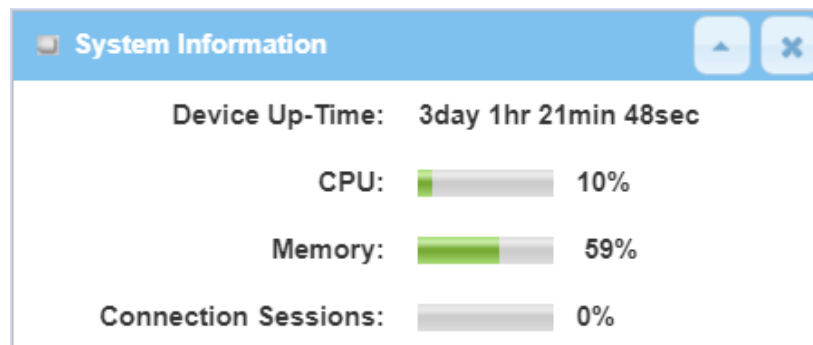
### 2.1.1 Device Dashboard

The **Device Dashboard** window shows the current status in graph or tables for quickly understanding the operation status for 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.

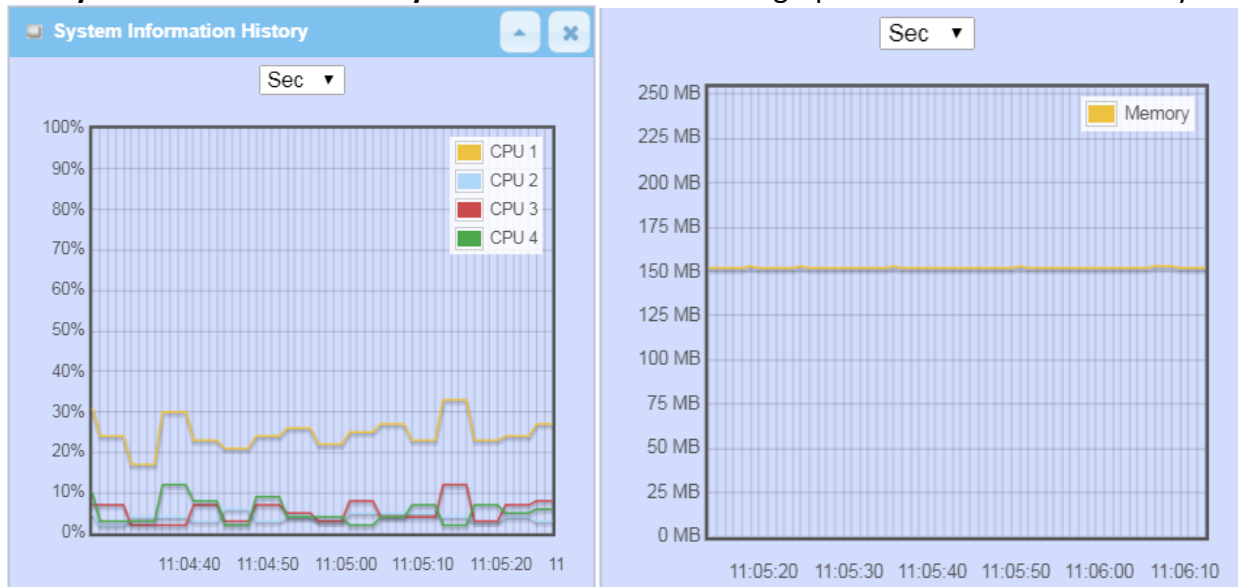
#### System Information Status

The **System Information** screen shows the device Up-time and the resource utilization for the CPU, Memory, and Connection Sessions.



## System Information History

The **System Information History** screen shows the statistic graphs for the CPU and memory.



## Network Interface Status

The **Network Interface Status** screen shows the statistic information for each network interface of the gateway. The statistic information includes the Interface Type, Upload Traffic, Download Traffic, and Current Upload / Download Traffic.

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)

## 2.2 Basic Network

### 2.2.1 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

**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
<b>ID</b>	N/A	It displays corresponding WAN interface WAN IDs.
<b>Interface</b>	N/A	It displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, 3G/4G, etc...
<b>WAN Type</b>	N/A	It displays the method which public IP address is obtained from your ISP. Depending on the model purchased, it can be Static IP, Dynamic IP, PPPoE, PPTP, L2TP, 3G/4G.
<b>Network Type</b>	N/A	It displays the network type for the WAN interface(s). Depending on the model purchased, it can be NAT, Routing, Bridge, or IP Pass-through.
<b>IP Addr.</b>	N/A	It displays the public IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
<b>Subnet Mask</b>	N/A	It displays the Subnet Mask for public IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
<b>Gateway</b>	N/A	It displays the Gateway IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
<b>DNS</b>	N/A	It displays the IP address of DNS server obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left unconfigured.
<b>MAC Address</b>	N/A	It displays the MAC Address for your ISP to allow you for Internet access. Note: Not all ISP may require this field.
<b>Conn. Status</b>	N/A	It displays the connection status of the device to your ISP. Status are Connected or disconnected.

		<p>This area provides functional buttons.</p> <p><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.</p> <p><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.</p> <p><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.</p> <p><b>Disconnect</b> button allows user to manually disconnect the device from the Internet. Note: <b>Connect</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.</p>
Action	N/A	

## LAN Interface Network Status

LAN Interface Network Status screen shows IPv4 information of LAN network.

LAN Interface Network Status			
IPv4 Address	IPv4 Subnet Mask	MAC Address	Action
192.168.123.254	255.255.255.0	00:E0:B3:3F:46:FF	Edit IPv4

LAN Interface Network Status		
Item	Value setting	Description
IPv4 Address	N/A	It displays the current IPv4 IP Address of the gateway This is also the IP Address user use to access Router's Web-based Utility.
IPv4 Subnet Mask	N/A	It displays the current mask of the subnet.
MAC Address	N/A	It displays the LAN MAC Address of the gateway
Action	N/A	This area provides functional buttons. <b>Edit IPv4 Button</b> when pressed, web-based utility will take you to the Ethernet LAN configuration page. ( <b>Basic Network &gt; LAN &amp; VLAN &gt; Ethernet LAN</b> tab).

## 3G/4G Modem Status

3G/4G Modem Status List screen shows status information for 3G/4G WAN network(s).

3G/4G Modem Status List					
Interface	Card Information	Link Status	Signal Strength	Network Name	Action
3G/4G	ZM8620	Connected	70% (-69dBm)	Chunghwa Telecom (LTE)	<button>Detail</button>

3G/4G Modem Status List		
Item	Value setting	Description
<b>Physical Interface</b>	N/A	It displays the type of WAN physical interface. Note: Some device models may support two 3G/4G modules. Their physical interface name will be <b>3G/4G-1</b> and <b>3G/4G-2</b> .
<b>Card Information</b>	N/A	It displays the vendor's 3G/4G modem model name.
<b>Link Status</b>	N/A	It displays the 3G/4G connection status. The status can be Connecting, Connected, Disconnecting, and Disconnected.
<b>Signal Strength</b>	N/A	It displays the 3G/4G wireless signal level.
<b>Network Name</b>	N/A	It displays the name of the service network carrier.
<b>Refresh</b>	N/A	Click the <b>Refresh</b> button to renew the information.
<b>Action</b>	N/A	This area provides functional buttons. <b>Detail Button</b> when pressed, windows of detailed information will appear. They are the Modem Information, SIM Status, and Service Information. Refer to next page for more.

When the **Detail** button is pressed, 3G/4G modem information windows such as Modem Information, SIM Status, Service Information, Signal Strength / Quality, and Error Message 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	<button>Reset</button>
WAN-2		-	-	

Interface Traffic Statistics		
Item	Value setting	Description
<b>ID</b>	N/A	It displays corresponding WAN interface WAN IDs.
<b>Interface</b>	N/A	It displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, 3G/4G, etc...

## AIR PACE

<b>Received Packets (Mb)</b>	N/A	It displays the downstream packets (Mb). It is reset when the device is rebooted.
<b>Transmitted Packets (Mb)</b>	N/A	It displays the upstream packets (Mb). It is reset when the device is rebooted.



## 2.2.2 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.

## 2.2.3 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	It displays the name you entered to identify DDNS service provider
Provider	N/A	It displays the DDNS server of DDNS service provider
Effective IP	N/A	It displays the public IP address of the device updated to the DDNS server
Last Update Status	N/A	It displays whether the last update of the device public IP address to the DDNS server has been successful (Ok) or failed (Fail).
Last Update Time	N/A	It displays time stamp of the last update of public IP address to the DDNS server.
Refresh	N/A	The <b>refresh</b> button allows user to force the display to refresh information.

## 2.3 Security

The screenshot shows the Air Pace VPN Status window. On the left is a navigation menu with options: Status, Dashboard, Basic Network, Security (selected), VPN, Firewall, Administration, and Statistics & Reports. Below these are icons for Basic Network, Object Definition, Field Communication, Security, and Administration. The main content area is titled 'VPN Firewall' and contains several status widgets:

- IPSec Tunnel Status** (Edit button): A table with columns: ID, Tunnel Name, Tunnel Scenario, Local Subnets, Remote IP/FQDN, Remote Subnets, Conn. Time, and Status.
- OpenVPN Server Status** (Edit button): A table with columns: ID, User Name, Remote IP/FQDN, Virtual IP/Mac, Conn. Time, and Status.
- OpenVPN Client Status** (Edit, Detail buttons): A table with columns: ID, OpenVPN Client Name, Interface, Remote IP/FQDN, Remote Subnet, Virtual IP, Conn. Time, and Conn. Status. It shows one client named 'Master\_client' on 'WAN 1' connected to 'm2mcluster.de' with virtual IP '172.17.0.190'.
- L2TP Server Status** (Edit button): A table with columns: ID, User Name, Remote IP, Remote Virtual IP, Remote Call ID, Conn. Time, and Status.
- L2TP Client Status** (Edit button): A table with columns: ID, L2TP Client Name, Interface, Virtual IP, Remote IP/FQDN, Default Gateway/Remote Subnet, Conn. Time, and Status.

### 2.3.1 VPN Status

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

The **VPN Status** window shows the overall VPN tunnel status. The display will be refreshed on 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 <span>Edit</span>							
ID	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	It displays the tunnel name you have entered to identify.
Tunnel Scenario	N/A	It displays the Tunnel Scenario specified.
Local Subnets	N/A	It displays the Local Subnets specified.
Remote IP/FQDN	N/A	It displays the Remote IP/FQDN specified.

<b>Remote Subnets</b>	N/A	It displays the Remote Subnets specified.
<b>Conn. Time</b>	N/A	It displays the connection time for the IPSec tunnel.
<b>Status</b>	N/A	It displays the Status of the VPN connection. The status displays are Connected, Disconnected, Wait for traffic, and Connecting.
<b>Edit Button</b>	N/A	Click on Edit Button to change IPSec setting, 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 <span>Edit</span> <span>▲</span> <span>✕</span>					
ID	User Name	Remote IP/FQDN	Virtual IP/Mac	Conn. Time	Status
OpenVPN Server Status					
Item	Value setting	Description			
<b>User Name</b>	N/A	It displays the Client name you have entered for identification.			
<b>Remote IP/FQDN</b>	N/A	It displays the public IP address (the WAN IP address) of the connected OpenVPN Client			
<b>Virtual IP/MAC</b>	N/A	It displays the virtual IP/MAC address assigned to the connected OpenVPN client.			
<b>Conn. Time</b>	N/A	It displays the connection time for the corresponding OpenVPN tunnel.			
<b>Status</b>	N/A	It displays the connection status of the corresponding OpenVPN tunnel. The status can be Connected, or Disconnected.			

## OpenVPN Client Status

OpenVPN Client Status <span>Edit</span> <span>Detail</span> <span>▲</span> <span>✕</span>							
ID	OpenVPN Client Name	Interface	Remote IP/FQDN	Remote Subnet	Virtual IP	Conn. Time	Conn. Status
OpenVPN Client Status							
Item	Value setting	Description					
<b>OpenVPN Client Name</b>	N/A	It displays the Client name you have entered for identification.					
<b>Interface</b>	N/A	It displays the WAN interface specified for the OpenVPN client connection.					
<b>Remote IP/FQDN</b>	N/A	It displays the peer OpenVPN Server's Public IP address (the WAN IP address) or FQDN.					
<b>Remote Subnet</b>	N/A	It displays the Remote Subnet specified.					
<b>TUN/TAP Read(bytes)</b>	N/A	It displays the TUN/TAP Read Bytes of OpenVPN Client.					
<b>TUN/TAP Write(bytes)</b>	N/A	It displays the TUN/TAP Write Bytes of OpenVPN Client.					
<b>TCP/UDP Read(bytes)</b>	N/A	It displays the TCP/UDP Read Bytes of OpenVPN Client.					
<b>TCP/UDP</b>	N/A	It displays the TCP/UDP Write Bytes of OpenVPN Client.					

# AIR PACE

Write(bytes)		Connection
Conn. Time	N/A	It displays the connection time for the corresponding OpenVPN tunnel.
Conn. Status	N/A	It displays the connection status of the corresponding OpenVPN tunnel. The status can be Connected, or Disconnected.

## L2TP Server/Client Status

**L2TP Server/Client Status** shows the configuration for establishing L2TP tunnel and current connection status.

L2TP Server Status <span>Edit</span>						
ID	User Name	Remote IP	Remote Virtual IP	Remote Call ID	Conn. Time	Status

L2TP Server Status		
Item	Value setting	Description
User Name	N/A	It displays the login name of the user used for the connection.
Remote IP	N/A	It displays the public IP address (the WAN IP address) of the connected L2TP client.
Remote Virtual IP	N/A	It displays the IP address assigned to the connected L2TP client.
Remote Call ID	N/A	It displays the L2TP client Call ID.
Conn. Time	N/A	It displays the connection time for the L2TP tunnel.
Status	N/A	It displays the Status of each of the L2TP client connection. The status displays Connected, Disconnect, Connecting
Edit	N/A	Click on <b>Edit</b> Button to change L2TP server setting, web-based utility will take you to the L2TP server page. ( <b>Security &gt; VPN &gt; L2TP</b> tab)

L2TP Client Status <span>Edit</span>							
ID	L2TP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Conn. Time	Status



  

L2TP Client Status		
Item	Value setting	Description
Client Name	N/A	It displays Name for the L2TP Client specified.
Interface	N/A	It displays the WAN interface with which the gateway will use to request PPTP tunneling connection to the PPTP server.
Virtual IP	N/A	It displays the IP address assigned by Virtual IP server of L2TP server.
Remote IP/FQDN	N/A	It displays the L2TP Server's Public IP address (the WAN IP address) or FQDN.
Default Gateway/Remote Subnet	N/A	It displays the specified IP address of the gateway device used to connect to the internet to connect to the L2TP server –the default gateway. Or other specified subnet if the default gateway is not used to connect to the L2TP server –the remote subnet.
Conn. Time	N/A	It displays the connection time for the L2TP tunnel.
Status	N/A	It displays the Status of the VPN connection. The status displays Connected, Disconnect, and Connecting.
Edit	N/A	Click on <b>Edit</b> Button to change L2TP client setting, web-based utility will take you to the L2TP client page. ( <b>Security &gt; VPN &gt; L2TP</b> tab)

## PPTP Server/Client Status

**PPTP Server/Client Status** shows the configuration for establishing PPTP tunnel and current connection status.

PPTP Server Status						
<div>Edit</div>						
ID	User Name	Remote IP	Remote Virtual IP	Remote Call ID	Conn. Time	Status
PPTP Server Status						
Item	Value setting	Description				
User Name	N/A	It displays the login name of the user used for the connection.				
Remote IP	N/A	It displays the public IP address (the WAN IP address) of the connected PPTP client.				
Remote Virtual IP	N/A	It displays the IP address assigned to the connected PPTP client.				
Remote Call ID	N/A	It displays the PPTP client Call ID.				
Conn. Time	N/A	It displays the connection time for the PPTP tunnel.				
Status	N/A	It displays the Status of each of the PPTP client connection. The status displays Connected, Disconnect, and Connecting.				
Edit Button	N/A	Click on <b>Edit</b> Button to change PPTP server setting, web-based utility will take you to the PPTP server page. ( <b>Security &gt; VPN &gt; PPTP</b> tab)				

PPTP Client Status							Edit	 	
ID	PPTP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Conn. Time	Status		
PPTP Client Status									
Item		Value setting		Description					
Client Name		N/A		It displays Name for the PPTP Client specified.					
Interface		N/A		It displays the WAN interface with which the gateway will use to request PPTP tunneling connection to the PPTP server.					
Virtual IP		N/A		It displays the IP address assigned by Virtual IP server of PPTP server.					
Remote IP/FQDN		N/A		It displays the PPTP Server’s Public IP address (the WAN IP address) or FQDN.					
Default Gateway / Remote Subnet		N/A		It displays the specified IP address of the gateway device used to connect to the internet to connect to the PPTP server –the default gateway. Or other specified subnet if the default gateway is not used to connect to the PPTP server –the remote subnet.					
Conn. Time		N/A		It displays the connection time for the PPTP tunnel.					
Status		N/A		It displays the Status of the VPN connection. The status displays Connected, Disconnect, and Connecting.					
Edit Button		N/A		Click on <b>Edit</b> Button to change PPTP client setting, web-based utility will take you to the PPTP server page. ( <b>Security &gt; VPN &gt; PPTP</b> tab)					

## 2.3.2 Firewall Status

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

The **Firewall Status** provides user a quick view of the firewall status and current firewall settings. It also keeps the log history of the dropped packets by the firewall rule policies, and includes the administrator remote login settings specified in the Firewall Options. The display will be refreshed on every five seconds.

By clicking the icon [+], the status table will be expanded to display log history. Clicking the **Edit** button will switch the screen to the configuration page.

### Packet Filter Status

Packet Filters

Edit

Activated Filter Rule	Detected Contents	IP	Time
-----------------------	-------------------	----	------

Packet Filter Status

Item	Value setting	Description
Activated Filter Rule	N/A	This is the Packet Filter Rule name.
Detected Contents	N/A	This is the logged packet information, including the source IP, destination IP, protocol, and destination port –the TCP or UDP. String format: Source IP to Destination IP: Destination Protocol (TCP or UDP)
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

*Note: Ensure Packet Filter Log Alert is enabled.*

*Refer to **Security > Firewall > Packet Filter** tab. Check Log Alert and save the setting.*

### URL Blocking Status

URL Blocking

Edit

Activated Blocking Rule	Blocked URL	IP	Time
-------------------------	-------------	----	------

URL Blocking Status

Item	Value setting	Description
Activated Blocking Rule	N/A	This is the URL Blocking Rule name.
Blocked URL	N/A	This is the logged packet information.
IP	N/A	The Source IP (IPv4) of the logged packet.



# AIR PACE

<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

Web Content Filters

Edit

⬆

✖

Activated Filter Rule	Detected Contents	IP	Time
Web Content Filter Status			
Item	Value setting	Description	
Activated Filter Rule	N/A	Logged packet of the rule name. String format.	
Detected Contents	N/A	Logged packet of the filter rule. String format.	
IP	N/A	Logged packet of the Source IP. IPv4 format.	
Time	N/A	Logged packet of the Date Time. Date time format ("Month" "Day" "Hours":"Minutes":"Seconds")	

Note: Ensure Web Content Filter Log Alert is enabled.

Refer to **Security > Firewall > Web Content Filter** tab. Check Log Alert and save the setting.

## MAC Control Status

MAC Control		Edit		
Activated Control Rule	Blocked MAC Addresses		IP	Time
MAC Control Status				
Item	Value setting	Description		
Activated Control Rule	N/A	This is the MAC Control Rule name.		
Blocked MAC Addresses	N/A	This is the MAC address of the logged packet.		
IP	N/A	The Source IP (IPv4) of the logged packet.		
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")		

Note: Ensure MAC Control Log Alert is enabled.

Refer to **Security > Firewall > MAC Control** tab. Check Log Alert and save the setting.

## Application Filters Status

Application Filters <span>Edit</span>			
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.*

## IPS Status

IPS

Edit

Detected Intrusion	IP	Time
--------------------	----	------

IPS Firewall Status

Item	Value setting	Description
Detected Intrusion	N/A	This is the intrusion type of the packets being blocked.
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

*Note: Ensure IPS Log Alert is enabled.*

*Refer to **Security > Firewall > IPS** tab. Check Log Alert and save the setting.*

## Firewall Options Status

Options <span>Edit</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.*

## 2.4 Administration

### 2.4.1 Configure & Manage Status

Go to **Status > Administration > Configure & Manage** tab.

The **Configure & Manage Status** window shows the status for managing remote network devices. The type of management available in your device is depended on the device model purchased. The commonly used ones are the SNMP, TR-069, and UPnP. The display will be refreshed on 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	It displays the user name for authentication. This is only available for SNMP version 3.
IP Address	N/A	It displays the IP address of SNMP manager.
Port	N/A	It displays the port number used to maintain connection with the SNMP manager.
Community	N/A	It displays the community for SNMP version 1 or version 2c only.
Auth. Mode	N/A	It displays the authentication method for SNMP version 3 only.
Privacy Mode	N/A	It displays the privacy mode for version 3 only.
SNMP Version	N/A	It displays the SNMP Version employed.

#### SNMP Trap Information

**SNMP Trap Information** screen shows the status of current received SNMP traps.

SNMP Trap Information		
Trap Level	Time	Trap Event

SNMP Trap Information		
Item	Value setting	Description
Trap Level	N/A	It displays the trap level.
Time	N/A	It displays the timestamp of trap event.
Trap Event	N/A	It displays the IP address of the trap sender and event type.

TR-069 Status

TR-069 Status screen shows the current connection status with the TR-069 ACS server.

TR-069 Status	
Link Status	
Off	

TR-069 Status		
Item	Value setting	Description
Link Status	N/A	It displays the current connection status with the TR-068 server. The connection status is either On when the device is connected with the TR-068 server or Off when disconnected.

## 2.4.2 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 Description, Usage, File System, Speed, and status.

Storage Information					
Device Select	Device Description	Usage	File System	Speed	Status

## 2.4.3 GNSS Status

Go to **Status > Administration > GNSS** tab.

The **GNSS Information** screen shows the status for current GNSS positioning information for the gateway.

GNSS Information <span>▲</span> <span>✕</span>						
Condition	No. of Satellites	Satellites ID / Signal Strength (dBm)	Position (Lat, Long)	Altitude (meters)	True Course	Ground Speed (km/h)
Not Fixed	0		,		0	0.00

The available GNSS information includes GNSS Condition, No. of Satellites, Satellites ID / Signal Strength, Position (Lat., Long.), Altitude (meters), True Course, and the equivalent Ground Speed (km/h).

## 2.5 Statistics & Reports

### 2.5.1 Connection Session

Go to **Status > Statistics & Reports > Connection Session** tab.

**Internet Surfing Statistic** shows the connection tracks on this router.

Internet Surfing List (14 entries)					
<a href="#">Previous</a> <a href="#">Next</a> <a href="#">First</a> <a href="#">Last</a> <a href="#">Export (.xml)</a> <a href="#">Export (.csv)</a>					
<a href="#">Refresh</a>					
User Name	Protocol	Internal IP & Port	MAC	External IP & Port	Duration Time
	UDP	192.168.127.58:3847		88.198.95.100:1194	2019/04/01 12:09~
	UDP	192.168.127.58:4486		192.168.123.10:53	2019/04/01 12:09~
	UDP	192.168.127.58:2899		192.168.123.10:53	2019/04/01 12:09~
	UDP	192.168.127.58:1251		192.168.123.10:53	2019/04/01 12:09~
	UDP	192.168.127.58:3145		192.168.123.10:53	2019/04/01 12:09~

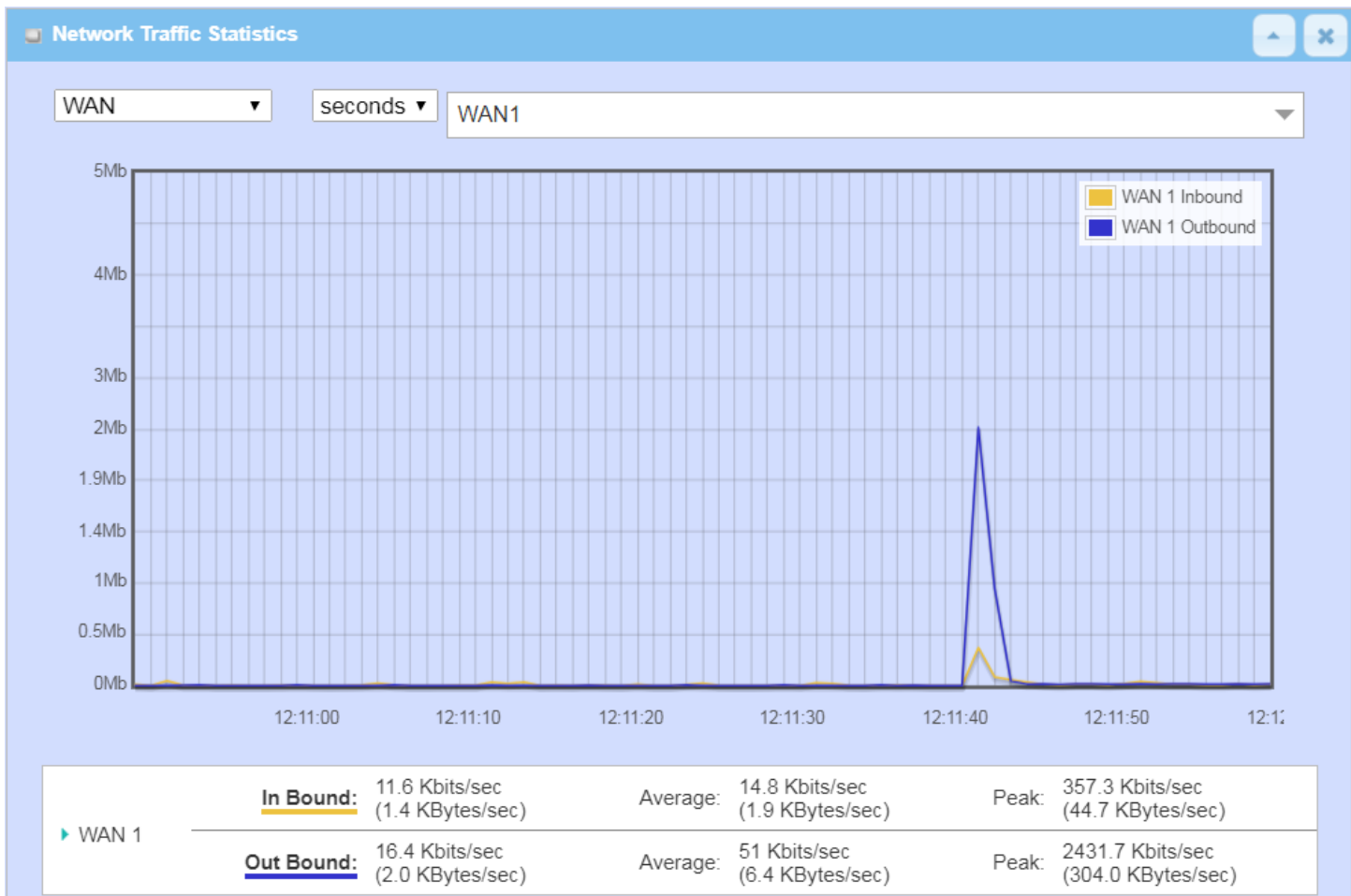
Internet Surfing Statistic		
Item	Value setting	Description
<b>Previous</b>	N/A	Click the <b>Previous</b> button to see the previous page of track list.
<b>Next</b>	N/A	Click the <b>Next</b> button to see the next page of track list.
<b>First</b>	N/A	Click the <b>First</b> button to see the first page of track list.
<b>Last</b>	N/A	Click the <b>Last</b> button to see the last page of track list.
<b>Export (.xml)</b>	N/A	Click the <b>Export (.xml)</b> button to export the list to xml file.
<b>Export (.csv)</b>	N/A	Click the <b>Export (.csv)</b> button to export the list to csv file.
<b>Refresh</b>	N/A	Click the <b>Refresh</b> button to refresh the list.



2.5.2 Network Traffic

Go to **Status > Statistics & Reports > Network Traffic** tab.

**Network Traffic Statistics** screen shows the historical graph for the selected network interface. You can change the interface drop list and select the interface and sampling time interval you want to monitor.



## 2.5.3 Login Statistics

Go to **Status > Statistics & Reports > Login Statistics**

**Login Statistics** shows the login information.

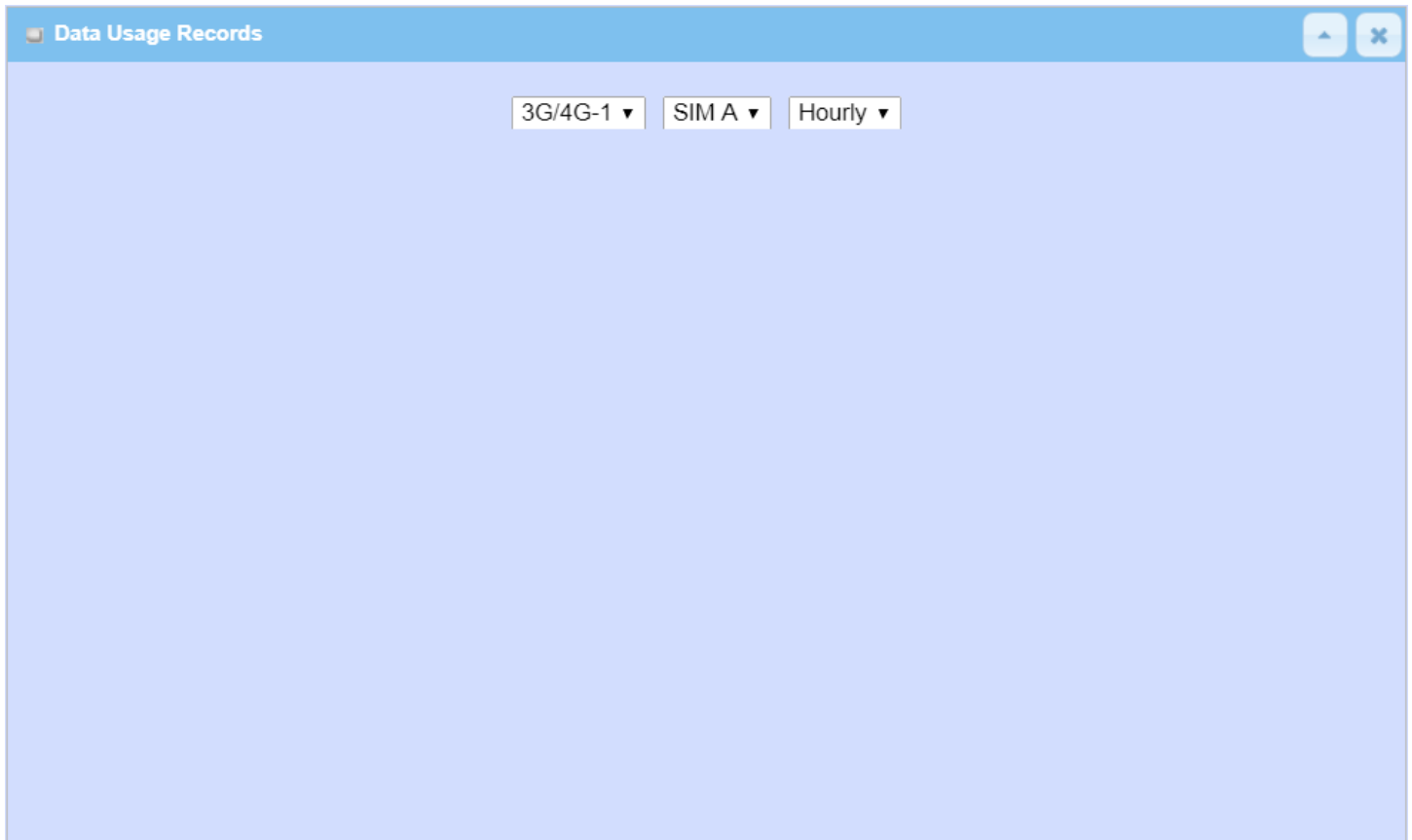
Device Manager Login Statistics				
<a href="#">Previous</a> <a href="#">Next</a> <a href="#">First</a> <a href="#">Last</a> <a href="#">Export (.xml)</a> <a href="#">Export (.csv)</a>				
<a href="#">Refresh</a>				
User Name	Protocol Type	IP Address	Info	Duration Time
admin	HTTP	192.168.123.190	Admin	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
<b>Previous</b>	N/A	Click the <b>Previous</b> button to see the previous page of login statistics.
<b>Next</b>	N/A	Click the <b>Next</b> button to see the next page of login statistics.
<b>First</b>	N/A	Click the <b>First</b> button to see the first page of login statistics.
<b>Last</b>	N/A	Click the <b>Last</b> button to see the last page of login statistics.
<b>Export (.xml)</b>	N/A	Click the <b>Export (.xml)</b> button to export the login statistics to xml file.
<b>Export (.csv)</b>	N/A	Click the <b>Export (.csv)</b> button to export the login statistics to csv file.
<b>Refresh</b>	N/A	Click the <b>Refresh</b> button to refresh the login statistics.

## 2.5.4 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.



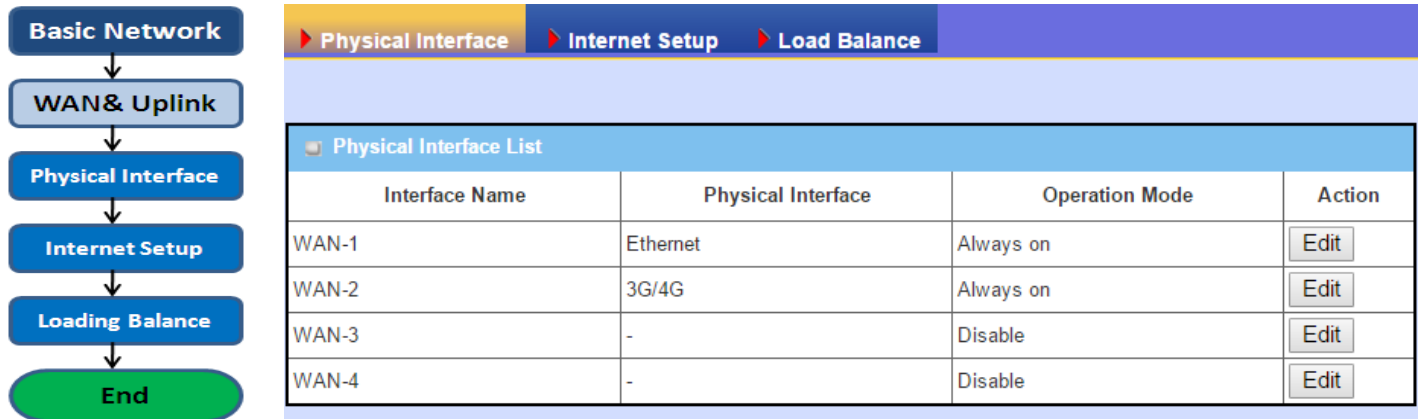
## 2.5.4 Cellular Signal

Go to **Status > Statistics & Reports > Cellular Signal** tab.

This screen shows the cellular signal strength over time.

## Chapter 3 Basic Network

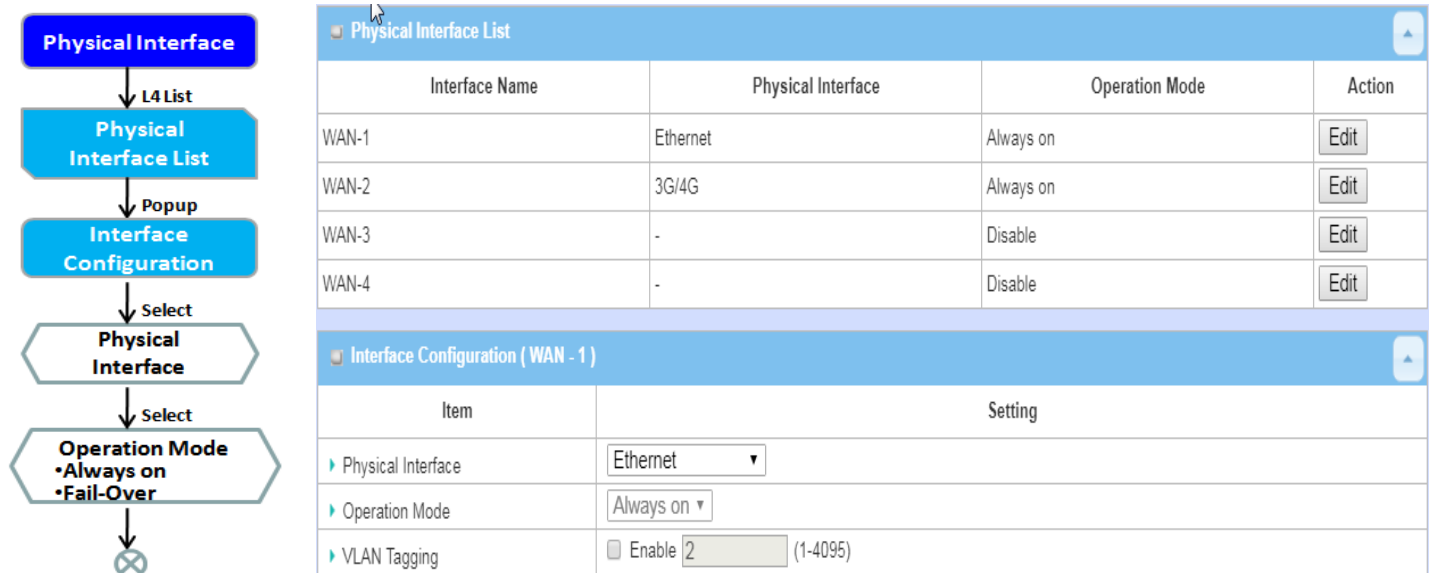
### 3.1 WAN & Uplink



The gateway provides multiple WAN interfaces to let all client hosts in Intranet of the gateway access the Internet via ISP. But ISPs in the world apply various connection protocols to let gateways or user's devices dial in to the ISP and then link to the Internet via different kinds of transmission 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 the ISP. Additionally, since the gateway has multiple WAN interfaces, you can assign a physical interface to participate in the Load Balance function.

## 3.1.1 Physical Interface



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

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". "Physical Interface List" shows all the available physical interfaces. After clicking on the "Edit" button for the interface in "Physical Interface List" window the "Interface Configuration" window will appear to let you configure a WAN interface.

### Physical Interface:

- **Ethernet WAN:** The gateway has one or more RJ-45 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 interface as a WAN connection. For each cellular WAN, 1 or 2 SIM cards can be inserted for special failover function.



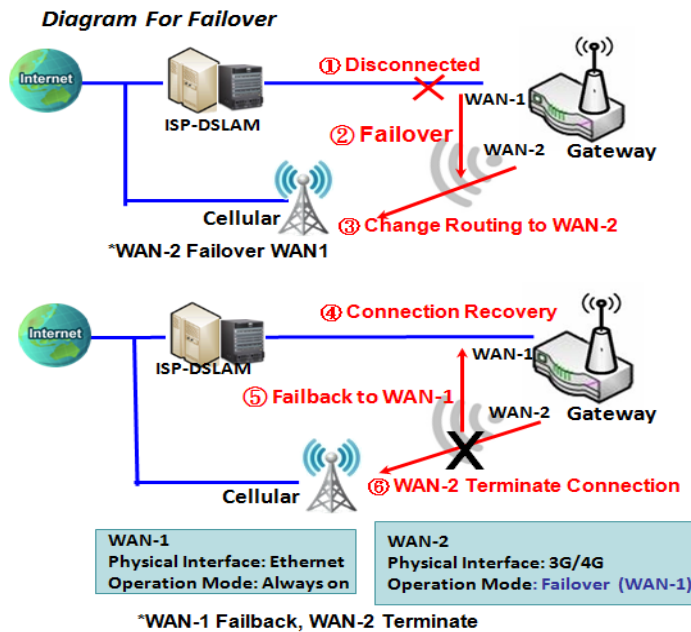
- You **MUST POWER OFF** the gateway before you insert or remove SIM card.
- The SIM card can be damaged if you insert or remove SIM card while the gateway is in operation.

## Operation Mode:

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

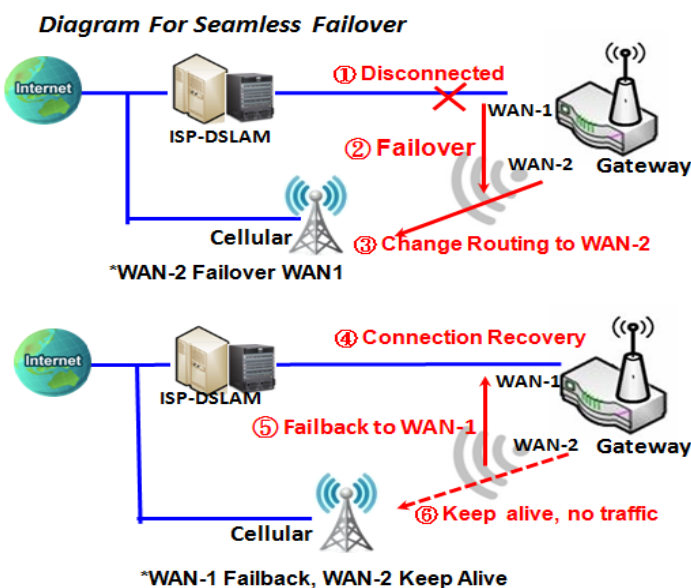
**Always on:** Set this WAN interface to be active all the time. When two or more WAN are established at "Always on" mode, outgoing data will move through these WAN connections based on load balance policies.

## Failover:



A failover interface is a backup connection to the primary. That means only when its primary WAN connection is broken, the backup connection will be started up to substitute for 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.

## Seamless Failover:



In addition, there is a "Seamless" option for Failover operation mode. When seamless option is activated by checking on the "Seamless" box in configuration window, both the primary connection and the failover connection are started up after system rebooting. But only the primary connection executes the data transfer, while the failover one just keeps the connection alive. As soon as the primary connection is broken, the system will switch, meaning failover, the routing path to the failover connection to save the dial up time of the failover connection (since it is already live).

When the "Seamless" enable checkbox is activated, it can allow the Failover interface to be connected continuously from system booting up. Failover WAN interface just keeps connecting without data traffic.

## AIR PACE

The purpose is to shorten the switch time during failover process. So, when primary connection is disconnected, failover interface will take over the data transfer mission instantly by only changing routing path to the failover interface. The dialing-up time of failover connection is saved since it has been connected beforehand.

### **VLAN Tagging**

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

## Physical Interface Setting

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

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

Note: Number of available WAN Interfaces may differ depending on the gateway purchased.

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

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

### Interface Configuration:

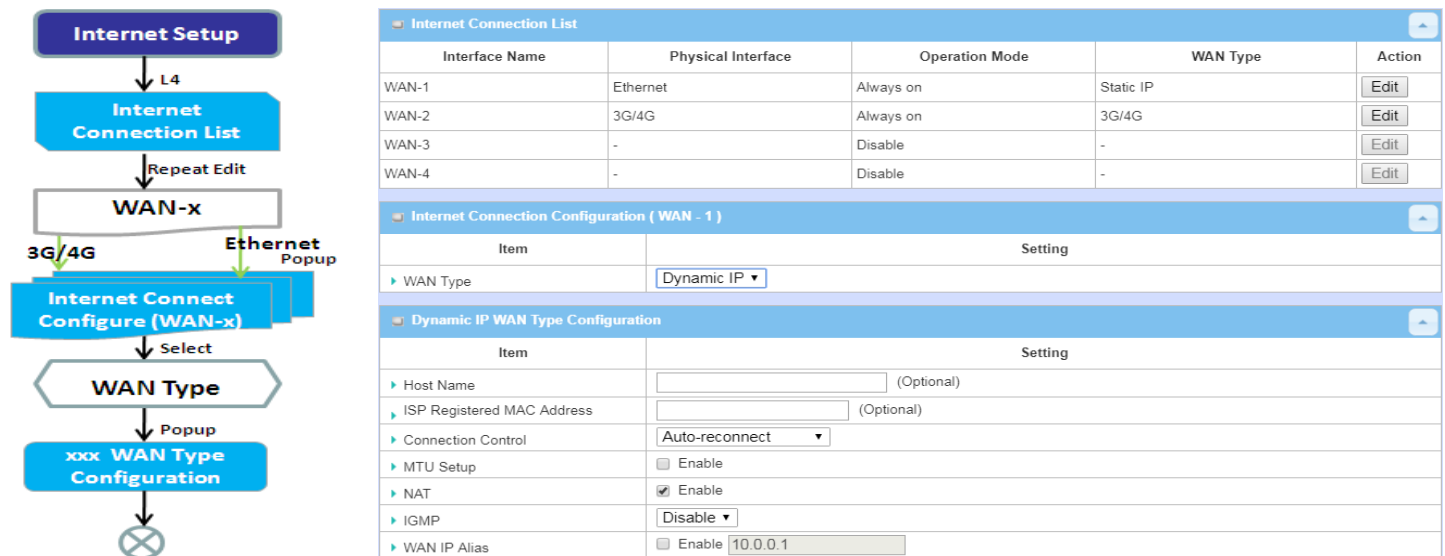
Interface Configuration ( WAN - 1 )	
Item	Setting
Physical Interface	<input type="text" value="Ethernet"/>
Operation Mode	<input type="text" value="Always on"/>
VLAN Tagging	<input type="checkbox"/> Enable <input type="text" value="2"/> (1-4095)

Interface Configuration		
Item	Value setting	Description
<b>Physical Interface</b>	1. Required setting 2. WAN-1 is the primary interface and is factory set to Always on.	Select one expected interface from the available interface dropdown list. It can be <b>3G/4G</b> , or <b>Ethernet</b> . 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 gateway.s
<b>Operation Mode</b>	Required setting	Define the operation mode of the interface. Select <b>Always on</b> to make this WAN always active. Select <b>Disable</b> to disable this WAN interface. 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.



		(Note: for WAN-1, only <b>Always on</b> option is available.)
<b>VLAN Tagging</b>	Optional setting	<p>Check <b>Enable</b> box to enter tag value provided by your ISP. Otherwise uncheck the box.</p> <p><b><u>Value Range: 1 ~ 4095.</u></b></p> <p>Note: This feature is NOT available for 3G/4G WAN connection.</p>

## 3.1.2 Connection Setup

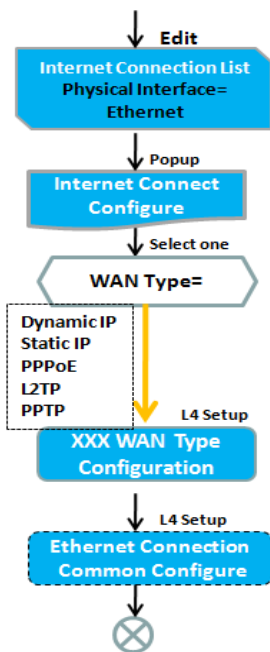


After specifying the physical interface for each WAN connection, administrator must configure their connection profile to meet the dial in process of ISP, so that all client hosts in the Intranet of the gateway can access the Internet.

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

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

## Internet Connection List - Ethernet WAN



Internet Connection Configuration ( WAN - 1 )	
Item	Setting
▶ WAN Type	Dynamic IP ▼
<div>           Dynamic IP WAN Type Conf           <div>             Dynamic IP Static IP PPPoE PPTP L2TP           </div> </div>	
Item	Setting
▶ Host Name	<input type="text"/> (Optional)
▶ ISP Registered MAC Address	<input type="text"/> <input type="button" value="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 <input type="text" value="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	<input type="text" value="5"/> (seconds)
▶ Latency Threshold	<input type="text" value="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 to connect with ISP.

- **Static IP:** Select this option if ISP provides a fixed IP to you when you subscribe the service. Usually is more expensive but very important for cooperative requirements.
- **Dynamic IP:** The assigned IP address for the WAN by a DHCP server is different every time. It 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 **Edit** button is applied, **Internet Connection Configuration** screen will appear. WAN-1 interface is used in this example.

# AIRPACE

## WAN Type = Dynamic IP

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

When you select it, "Dynamic IP WAN Type Configuration" will appear. Items and setting is 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	An optional setting	Enter the host name provided by your Service Provider.
ISP Registered MAC Address	An 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 Internet.

## WAN Type= Static IP

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

When you select it, "Static IP WAN Type Configuration" will appear. Items and setting is 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)

### Static IP WAN Type Configuration

Item	Value setting	Description
<b>WAN IP Address</b>	A Required setting	Enter the WAN IP address given by your Service Provider
<b>WAN Subnet Mask</b>	A Required setting	Enter the WAN subnet mask given by your Service Provider
<b>WAN Gateway</b>	A Required setting	Enter the WAN gateway IP address given by your Service Provider
<b>Primary DNS</b>	A Required setting	Enter the primary WAN DNS IP address given by your Service Provider
<b>Secondary DNS</b>	An 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 you select it, "PPPoE WAN Type Configuration" will appear. Items and setting is explained below

PPPoE WAN Type Configuration

Item	Setting
▶ IP Type	IPv4 ▼
▶ PPPoE Account	<input type="text"/>
▶ PPPoE Password	<input type="password"/>
▶ 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>	A required setting	Enter the PPPoE User Name provided by your Service Provider.
<b>PPPoE Password</b>	A required setting	Enter the PPPoE password provided by your Service Provider.
<b>Primary DNS</b>	An optional setting	Enter the IP address of Primary DNS server.
<b>Secondary DNS</b>	An optional setting	Enter the IP address of Secondary DNS server.
<b>Service Name</b>	An optional setting	Enter the service name if your ISP requires it
<b>Assigned IP Address</b>	An optional setting	Enter the IP address assigned by your Service Provider.

## WAN Type= PPTP

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

When you select it, "PPTP WAN Type Configuration" will appear. Items and setting is 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="password"/>
▶ Connection ID	<input type="text"/> (Optional)
▶ MPPE	<input type="checkbox"/> Enable

PPTP WAN Type Configuration		
Item	Value setting	Description
IP Mode	A 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, WAN Subnet Mask, and WAN Gateway</b>. <ul style="list-style-type: none"> <li><b>WAN IP Address</b> (A Required setting): Enter the WAN IP address given by your Service Provider.</li> <li><b>WAN Subnet Mask</b> (A Required setting): Enter the WAN subnet mask given by your Service Provider.</li> <li><b>WAN Gateway</b> (A 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	A required setting	Enter the PPTP server name or IP Address.
PPTP Account	A required setting	Enter the PPTP username provided by your Service Provider.
PPTP Password	A required setting	Enter the PPTP connection password provided by your Service Provider.
Connection ID	An optional setting	Enter a name to identify the PPTP connection.
MPPE	An optional setting	Select <b>Enable</b> to enable MPPE (Microsoft Point-to-Point Encryption) security for PPTP connection.

## WAN Type= L2TP

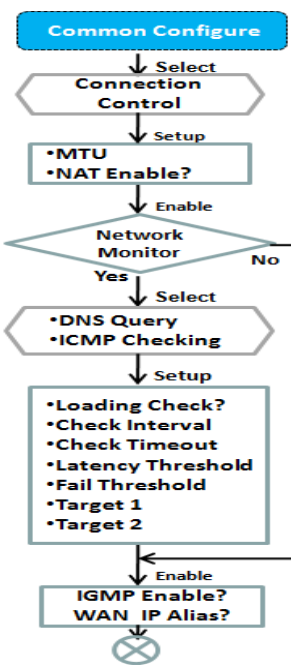
Internet Connection Configuration ( WAN - 1 )	
Item	Setting
▶ WAN Type	L2TP ▼

When you select it, "L2TP WAN Type Configuration" will appear. Items and setting is 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	A 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, WAN Subnet Mask, and WAN Gateway</b>. <ul style="list-style-type: none"> <li><b>WAN IP Address</b> (A Required setting): Enter the WAN IP address given by your Service Provider.</li> <li><b>WAN Subnet Mask</b> (A Required setting): Enter the WAN subnet mask given by your Service Provider.</li> <li><b>WAN Gateway</b> (A 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	A Required setting	Enter the L2TP server name or IP Address.
L2TP Account	A Required setting	Enter the L2TP username provided by your Service Provider.
L2TP Password	A Required setting	Enter the L2TP connection password provided by your Service Provider.
Service Port	A Required setting	<p>Enter the service port that the Internet service.</p> <p>There are three options that can be selected:</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	An optional setting	Select <b>Enable</b> to enable MPPE (Microsoft Point-to-Point Encryption) security for PPTP connection.

## Ethernet Connection Common Configuration



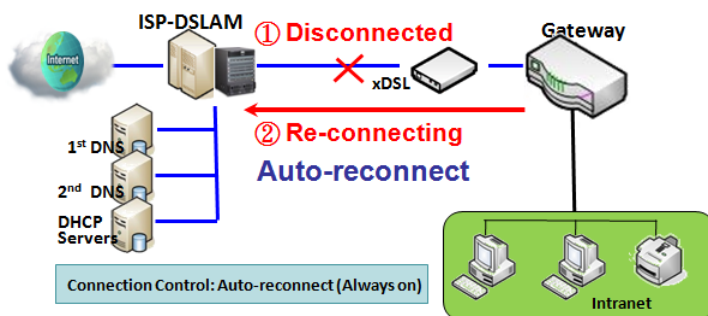
▶ Connection Control	Auto-reconnect ▼
▶ MTU Setup	<input type="checkbox"/> Enable
▶ NAT	<input checked="" type="checkbox"/> Enable
▶ IGMP	Disable ▼
▶ WAN IP Alias	<input type="checkbox"/> Enable 10.0.0.1

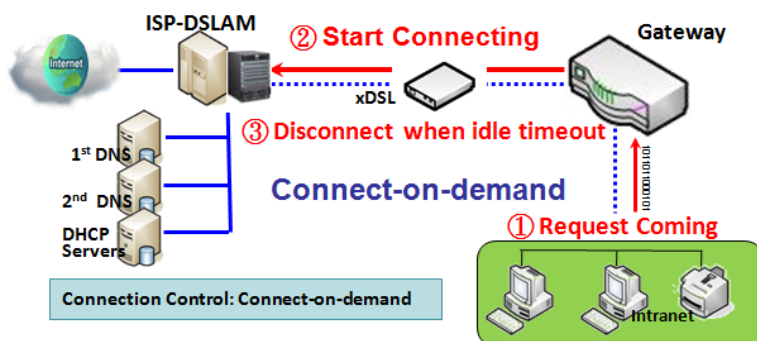
Network Monitoring Configuration	
Item	Setting
▶ Network Monitoring Configuration	<input checked="" type="checkbox"/> Enable
▶ Checking Method	DNS Query ▼
▶ Loading Check	<input checked="" type="checkbox"/> Enable
▶ Query Interval	5 (seconds)
▶ Latency Threshold	3000 (ms)
▶ Fail Threshold	5 (Times)
▶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

There are some important parameters to be set up no matter which Ethernet WAN type is selected. You should follow the rules for configuration.

### Connection Control.

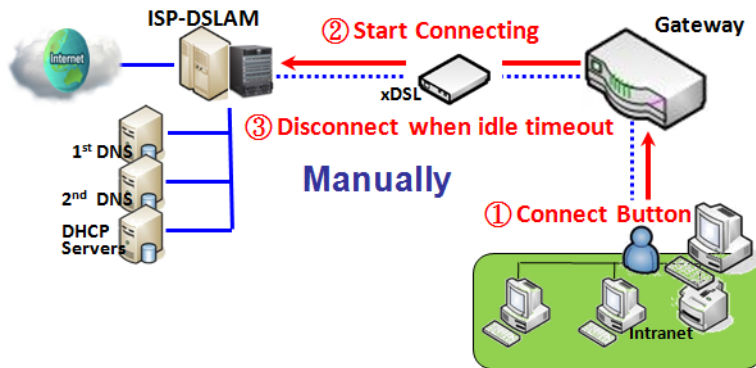


**Auto-reconnect:** This gateway will establish Internet connection automatically once it has been booted up, and try to reconnect once the connection is down. It's recommended to choose this scheme if for mission critical applications to ensure full-time Internet connection.



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

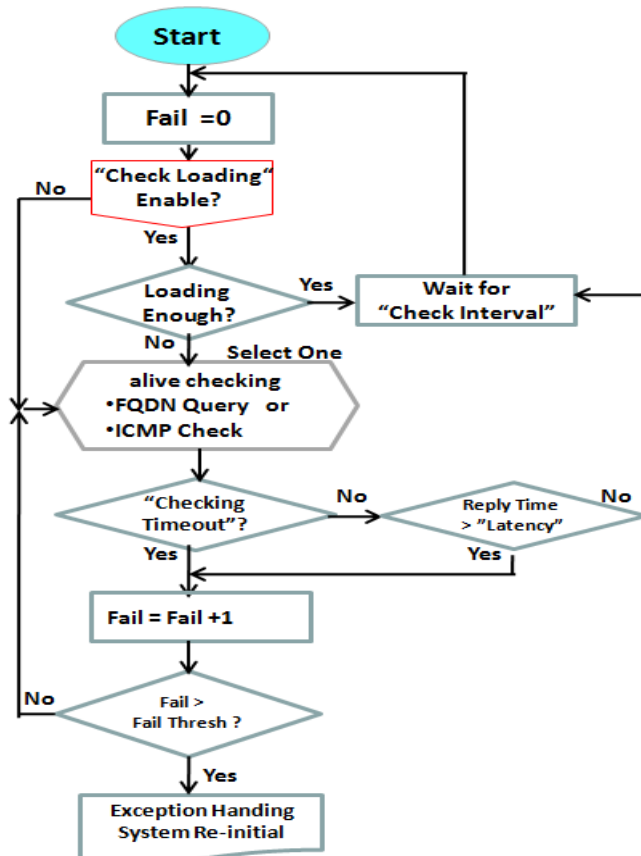




**Manually:** This gateway won't start to establish WAN connection until you press "Connect" button on web UI. After normal data transferring between LAN and WAN sides, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time.

Please 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 to you to configure as the system must set it to "Auto-reconnect (Always on)".

## Network Monitoring



It is necessary to monitor connection status continuously, and "ICMP Check" and "FQDN Query" are used to check. When there is traffic on the connection, checking packets will waste bandwidth. Response time of replied packets may also increase. To avoid "Network Monitoring" from working abnormally, enabling "Checking Loading" option will stop connection check when there is 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 the "Latency", or there is no response within the "Checking Timeout", the "Fail" count will be increased. If it is continuous and "Fail" count is more than "Fail Threshold", gateway will execute exception handling process and re-initialie the connection again . Otherwise, network monitoring process will start again.

## Set up “Ethernet Common Configuration”

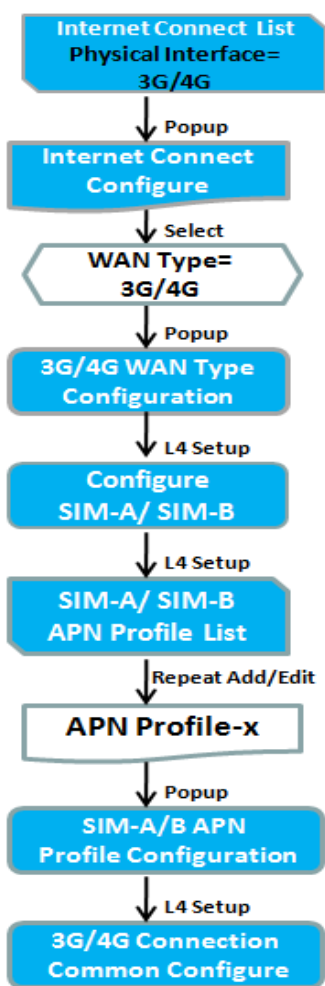
Ethernet WAN Common Configuration		
Item	Value setting	Description
<b>Connection Control</b>	A Required setting	<p>There are three connection modes.</p> <ul style="list-style-type: none"> <li>• <b>Auto-reconnect</b> enables the router to always keep the Internet connection on.</li> <li>• <b>Connect-on-demand</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>
<b>Maximum Idle Time</b>	<ol style="list-style-type: none"> <li>1. An Optional setting</li> <li>2. By default <b>600</b> seconds is filled-in</li> </ol>	<p>Specify the maximum Idle time setting to disconnect the internet connection when the connection idle timed 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>
<b>MTU Setup</b>	<ol style="list-style-type: none"> <li>1. An Optional setting</li> <li>2. <b>Unchecked</b> by default</li> </ol>	<p>Check the Enable box to enable the MTU (Maximum Transmission Unit) limit, and specify the <b>MTU</b> for the 3G/4G connection.</p> <p><b>MTU</b> refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission.</p> <p><b>Value Range:</b> 1200 ~ 1500.</p>
<b>MTU Setup</b>	<ol style="list-style-type: none"> <li>1. A Required setting</li> <li>2. <b>Auto</b> (value zero) is set by default</li> <li>3. Manual set range 1200~1500</li> </ol>	<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>
<b>NAT</b>	<ol style="list-style-type: none"> <li>1. An optional setting</li> <li>2. NAT is enabled by default</li> </ol>	<p>Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.</p>
<b>IGMP</b>	<ol style="list-style-type: none"> <li>1. A Required setting</li> <li>2. Disabled is set by default</li> </ol>	<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 and to avoid flooding the entire network.</p>
<b>WAN IP Alias</b>	<ol style="list-style-type: none"> <li>1. An optional setting</li> <li>2. <b>Unchecked</b> by default</li> </ol>	<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>

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. An 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. An 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.
<b>Loading Check</b>	1. An 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>Query Interval</b>	1. An Optional setting 2. <b>5 seconds</b> is selected by default.	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.
<b>Check Interval</b>	1. An Optional setting 2. <b>5 seconds</b> is selected by default.	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 request packets to the destination specified in Target 1 and Target 2. <b>Value Range:</b> 2 ~ 14400.
<b>Latency Threshold</b>	1. An Optional setting 2. <b>3000 ms</b> 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. An Optional setting 2. <b>5 times</b> 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. An Optional filled 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. An Optional filled 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.

## 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

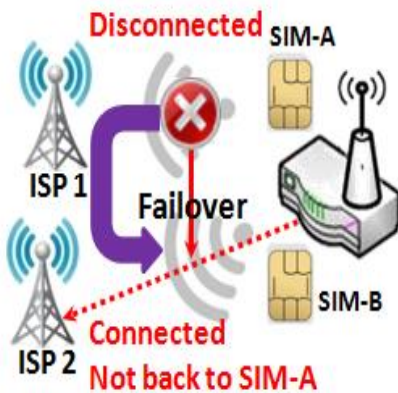
### Preferred SIM Card – Dual SIM Fail Over

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

# AIR PACE

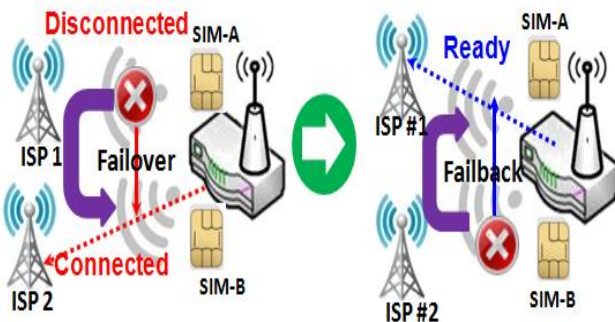
**SIM-A/SIM-B only:** When “SIM-A Only” or “SIM-B Only” is used, the specified SIM slot card is the only one to be used for negotiation parameters between gateway device and cellular ISP.

## 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. And when the connection is broken, the gateway will switch to use the other SIM card as an alternate automatically and **will not switch back** to use the 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 as long as current connection is still alive.

## SIM-A / SIM-B first with Failback enable



With Failback option enabled, “SIM-A First” scenario is used to connect. If the connection is broken, the gateway will switch to SIM-B. When the SIM-A connection is recovered, it will switch back to use the 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.

Internet Connection Configuration ( WAN - 2 )

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

3G/4G Connection Configuration		
Item	Value setting	Description
WAN Type	1. A Required setting 2. <b>3G/4G</b> is set by default.	From the dropdown box, select Internet connection method for 3G/4G WAN Connection. Only <b>3G/4G</b> is available.
Preferred SIM Card	1. A 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. And if the connection fails, it will change 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 the product with 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>
Auto Flight Mode	The box is 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 the cellular tower. It can get data connection instantly, and receive managing SMS all the time as required.</p> <p>If you enabled the <b>Auto Flight Mode</b>, the gateway will pop up a message <i>"Flight mode will cause cellular function to malfunction when the data session is offline."</i>, and it will make the cellular module into flight mode and physically disconnected with the cellular tower. 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</p>

		gateway to enable the Auto Flight Mode.
<b>SIM Switch Policy</b>	NA	Click the <b>Policy Setting</b> button to define the SIM Switch policy or browse the current 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)

## Configure SIM-A / SIM-B Card

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

Connection with SIM-A Card	
Item	Setting
▶ Network Type	<input type="text" value="Auto"/>
▶ Dial-Up Profile	<input type="text" value="Manual-configuration"/>
▶ APN	<input type="text"/>
▶ PIN Code	<input type="text"/> (Optional)
▶ Dial Number	<input type="text"/> (Optional)
▶ Account	<input type="text"/> (Optional)
▶ Password	<input type="text"/> (Optional)
▶ Authentication	<input type="text" value="Auto"/>
▶ IP Mode	<input type="text" value="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 follows the same rule of Configurations of SIM-A Card, here we list SIM-A as the example.

Note\_2: Both **Connection with SIM-A Card** and **Connection with SIM-B Card** will pop up only when the **SIM-A First** or **SIM-B First** is selected, otherwise it only pops out one of them.

### Connection with SIM-A/-B Card



Item	Value setting	Description
<b>Network Type</b>	1. A Required setting 2. By default <b>Auto</b> is selected	<p>Select <b>Auto</b> to register a network automatically, regardless of the network type.</p> <p>Select <b>2G Only</b> to register the 2G network only.</p> <p>Select <b>2G Prefer</b> to register the 2G network first if it is available.</p> <p>Select <b>3G only</b> to register the 3G network only.</p> <p>Select <b>3G Prefer</b> to register the 3G network first if it is available.</p> <p>Select <b>LTE only</b> to register the LTE network only.</p> <p><b>Note:</b> Options may be different due to the specification of the module.</p>
<b>Dial-Up Profile</b>	1. A Required setting 2. By default <b>Manual-configuration</b> is selected	<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.</p> <p>Select <b>APN Profile List</b> to set more than one profile to dial up in turn, until the connection is established. It will pop up a new field, please go to <b>Basic Network &gt; WAN &amp; Uplink &gt; Internet Setup &gt; SIM-A APN Profile List</b> for details.</p> <p>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> You are highly recommended to select the <b>Manual</b> or <b>APN Profile List</b> to specify the network for your subscription. Your ISP always provides such network settings for the subscribers.</p> <p><b>Note_2:</b> If you select <b>Auto-detection</b>, it is likely to connect to an improper network, or failed to find a valid APN for your ISP.</p>
<b>APN</b>	1. A Required setting 2. String format: any text	<p>Enter the <b>APN</b> you want to use to establish the connection.</p> <p>This is a required setting if you selected <b>Manual-configuration</b> as dial-up profile scheme.</p>
<b>IP Type</b>	1. A Required setting 2. By default <b>IPv4</b> is selected	<p>Specify the IP type of the network service provided by your 3G/4G network. It can be <b>IPv4</b>.</p>
<b>PIN code</b>	1. An Optional setting 2. String format: integer	<p>Enter the PIN (Personal Identification Number) code if it is needed to unlock your SIM card.</p>
<b>Dial Number, Account, Password</b>	1. An Optional setting 2. String format: any text	<p>Enter the optional <b>Dial Number</b>, <b>Account</b>, and <b>Password</b> settings if your ISP provided such settings to you.</p> <p>Note: These settings are only displayed when Manual-configuration is selected.</p>
<b>Authentication</b>	1. A Required setting 2. By default <b>Auto</b> is selected	<p>Select <b>PAP</b> (Password Authentication Protocol) and use such protocol to be authenticated with the carrier's server.</p> <p>Select <b>CHAP</b> (Challenge Handshake Authentication Protocol) and use such protocol to be authenticated with the carrier's server.</p> <p>When <b>Auto</b> is selected, it means it will authenticate with the server either <b>PAP</b> or <b>CHAP</b>.</p>
<b>IP Mode</b>	1. A Required setting 2. By default <b>Dynamic IP</b> is selected	<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.</p> <p>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 are required, such as IP address, subnet mask and gateway.</p> <p><b>Note:</b> <b>IP Subnet Mask</b> is a required setting, and make sure you have the</p>

		right configuration. Otherwise, the connection may get issues.
<b>Primary DNS</b>	1. An Optional setting 2. String format: IP address (IPv4 type)	Enter the IP address to change the primary DNS (Domain Name Server) setting. If it is not filled-in, the server address is given by the carrier while dialing-up.
<b>Secondary DNS</b>	1. An Optional setting 2. String format: IP address (IPv4 type)	Enter the IP address to change the secondary DNS (Domain Name Server) setting. If it is not filled-in, the server address is given by the carrier while dialing-up.
<b>Roaming</b>	The box is unchecked by default	Check the box to establish the connection even the registration status is roaming, not in home network.  <b>Note:</b> It may cost additional charges if the connection is under 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	IP Type	Account	Password	Authentication	Priority	Enable	Actions

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

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

SIM-A APN Profile Configuration	
Item	Setting
▶ Profile Name	<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
<b>Profile Name</b>	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.
<b>APN</b>	String format: any text	Enter the <b>APN</b> you want to use to establish the connection.
<b>IP Type</b>	1. A Required setting 2. By default <b>IPv4</b> is	Specify the IP type of the network service provided by your 3G/4G network. It can be <b>IPv4</b> .

	selected	
<b>Account</b>	String format: any text	Enter the <b>Account</b> you want to use for the authentication. <b>Value Range:</b> 0 ~ 53 characters.
<b>Password</b>	String format: any text	Enter the <b>Password</b> you want to use for the authentication.
<b>Authentication</b>	1. A Required setting 2. By default <b>Auto</b> is selected	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> .
<b>Priority</b>	1. A Required setting 2. String format: integer	Enter the value for the dialing-up order. The valid value is from 1 to 16. It will start to dial up with the profile that assigned with the smallest number. <b>Value Range:</b> 1 ~ 16.
<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>X</b> button to restore what you just configured back to the previous setting.

## 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 it will try to keep the Internet connection on all the time 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 detecting data traffic.</p> <p>When <b>Connect Manually</b> is selected, it means you need to click the <b>Connect</b> button 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>

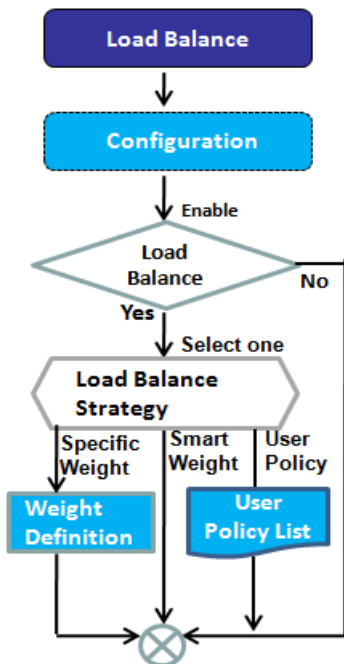
<b>Maximum Idle Time</b>	1. An Optional setting 2. By default <b>600</b> seconds is filled-in	Specify the maximum Idle time setting to disconnect the internet connection when the connection idle times out. <b>Value Range:</b> 300 ~ 86400. <b>Note:</b> This field is available only when <b>Connect-on-demand</b> or <b>Connect Manually</b> is selected as the connection control scheme.
<b>Time Schedule</b>	1. A Required setting 2. By default <b>(0) Always</b> is selected	When <b>(0) Always</b> is selected, it means this WAN is under operation all the time. Once you have set other schedule rules, there will be other options to select. Please go to <b>Object Definition &gt; Scheduling</b> for details.
<b>MTU Setup</b>	1. An Optional setting 2. <b>Unchecked</b> by default	Check the Enable box to enable the MTU (Maximum Transmission Unit) limit, and specify the <b>MTU</b> for the 3G/4G connection. <b>MTU</b> refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. <b>Value Range:</b> 1200 ~ 1500.
<b>IP Pass-through (Cellular Bridge)</b>	1. The box is 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 filled-in 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>	<b>Checked</b> 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. An 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. An Optional setting	Choose either <b>DNS Query</b> or <b>ICMP Checking</b> to detect WAN link.

	2. <b>DNS Query</b> is set by default	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.
<b>Loading Check</b>	1. An 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>Query Interval</b>	1. An Optional setting 2. <b>5 seconds</b> is selected by default.	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.
<b>Check Interval</b>	1. An Optional setting 2. <b>5 seconds</b> is selected by default.	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 request packets to the destination specified in Target 1 and Target 2. <b>Value Range:</b> 2 ~ 14400.
<b>Latency Threshold</b>	1. An Optional setting 2. <b>3000 ms</b> 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. An Optional setting 2. <b>5 times</b> 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. An Optional filled 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. An Optional filled 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.

## 3.1.3 Load Balance

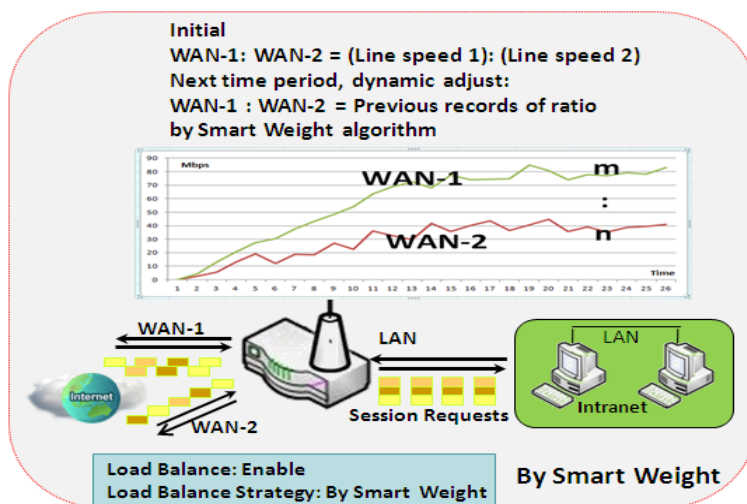


Configuration			
Item	Setting		
Load Balance	<input checked="" type="checkbox"/> Enable		
Load Balance Strategy	By Specific Weight ▼		
	By Smart Weight		
Weight Definition	By Specific Weight		
	By User Policy		
WAN ID	Weight	Action	
WAN - 1	86 %	<input type="button" value="Edit"/>	
WAN - 2	13 %	<input type="button" value="Edit"/>	
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			
User Policy Configuration			
Item	Setting		

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

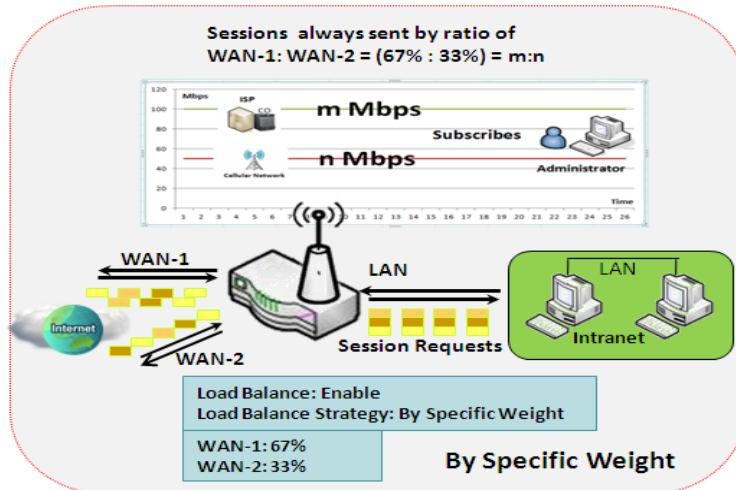
There are three optional strategies for load balance: **“By Smart Weight”**, **“By Specific Weight”**, and **“By User Policy”**. The administrator can select a strategy according to application requirements and environment status. The strategies are explained as below.



### **By Smart Weight**

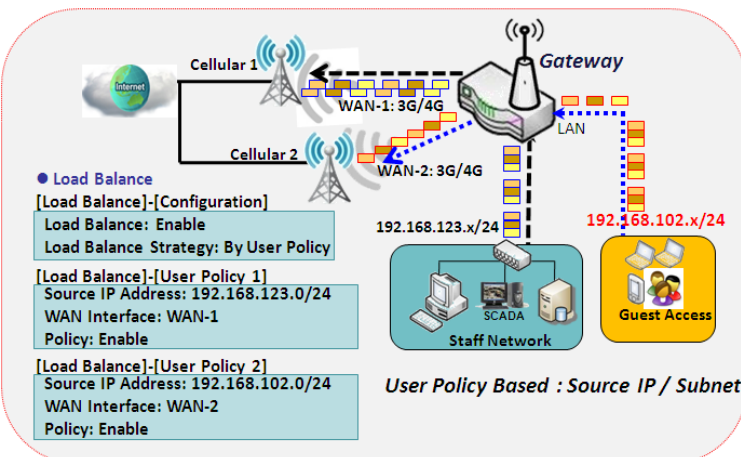
If based on "By Smart Weight" strategy, the gateway will take the line speed settings of all WAN interfaces specified in "Physical Interface" configuration page as default ratio for data transfer. Based on the ratio of packet bytes via these WAN interfaces in past period (maybe 5 minutes), the system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





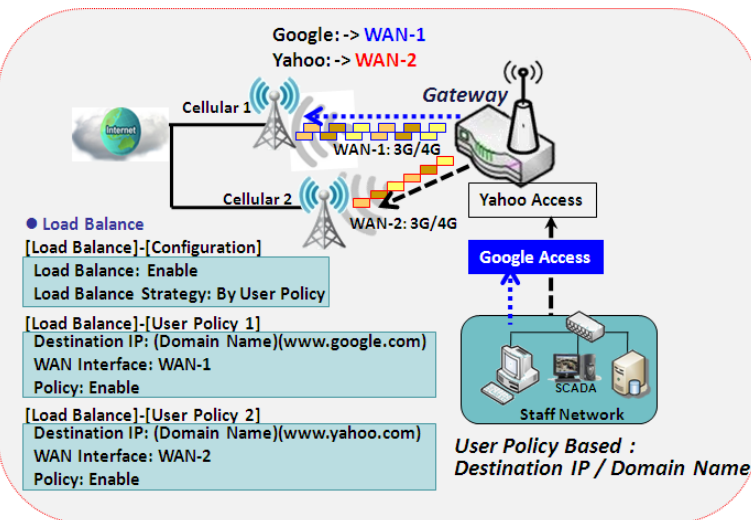
## By Specific Weight

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



## By User Policy

If "By User Policy" load balance strategy is selected, it can allow you to map Source IP, Destination IP, or Destination Port to an assigned WAN interface. This IP address is not only a single IP but 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 set up an IP address and leave others as "any"/ "All". You can also set protocol as TCP, UDP or both.



The diagrams shown on the left are example user policies. 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 name to a certain WAN interface. If packets don't belong to user policy rule, the gateway just routes those packets based on smart weight algorithm.

## 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 you choose "By Smart Weight" strategy, the system will operate load balance function automatically based on the embedded Smart Weight algorithm. However, when you choose "By Specific Weight" strategy, the further "Weight Definition" configuration window will let you define the ratio of transferred sessions between all WAN interfaces for data transfer. At last, when you choose "By User Policy" strategy, the further "User Policy List" shows 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 Specific Weight ▼

Configuration		
Item	Value setting	Description
<b>Load Balance</b>	Unchecked by default	Check the <b>Enable</b> box to activate Load Balance function.
<b>Load Balance Strategy</b>	1. A Required setting 2. <b>By Smart Weight</b> is selected by default.	There are up to three load balance strategies. Select the preferred one. <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. Note: The number of available strategies depends on the model purchased.
<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.

When **By Specific Weight** is selected, the user needs to adjust the percentage of WAN loading. The system will give a value according to the bandwidth ratio of each WAN at first, and keep the value after **Save** button is clicked.



# AIR PACE

Weight Definition		
WAN ID	Weight	Action
WAN - 1	88 %	<button>Edit</button>
WAN - 2	13 %	<button>Edit</button>

Weight Definition		
Item	Value setting	Description
WAN ID	NA	The Identifier for each available WAN interface..
Weight	1. A 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 what you just configured back to the previous setting.

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 user defined rules

## Create User Policy

User Policy List <button>Add</button> <button>Delete</button>						
ID	Source IP Address	Destination IP Address	Destination Port	WAN Interface	Enable	Actions

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

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

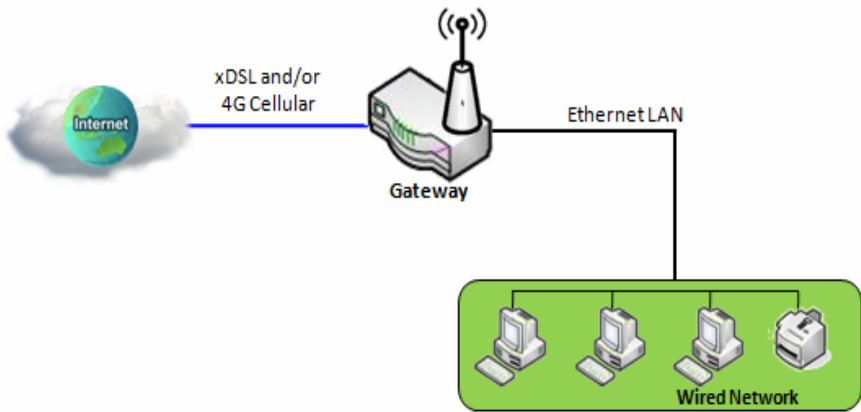
User Policy Configuration		
Item	Value setting	Description
Source IP Address	1. A Required setting 2. <b>Any</b> is selected by default.	There are four options that can be selected: <b>Any:</b> No specific Source IP is provided. The traffic may come from any source <b>Subnet:</b> Specify the Subnet for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

		<p><b>IP Range:</b> Specify the IP Range for the traffic coming from the IPs</p> <p><b>Single IP:</b> Specify a unique IP Address for the traffic coming from the IP. Input format is: xxx.xxx.xxx.xxx e.g. 192.168.123.101.</p>
<b>Destination IP Address</b>	<p>1. A Required setting</p> <p>2. <b>Any</b> is selected by default.</p>	<p>There are five options that can be selected:</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 going to the subnet. 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 going to the IPs</p> <p><b>Single IP:</b> Specify a unique IP Address for the traffic going to the IP. 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 going to the domain</p>
<b>Destination Port</b>	<p>1. A Required setting</p> <p>2. <b>All</b> is selected by default.</p>	<p>There are four options that can be selected:</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 application defined in dropdown list.</p>
<b>Protocol</b>	<p>1. A Required setting</p> <p>2. <b>Both</b> is selected by default.</p>	<p>There are three options that can be selected. They are <b>Both</b>, <b>TCP</b>, and <b>UDP</b>.</p>
<b>WAN Interface</b>	<p>1. A Required setting</p> <p>2. <b>WAN-1</b> is selected by default.</p>	<p>User can select the interface that traffic should go to.</p> <p>Note that the WAN interface dropdown list will only show the available WAN interfaces.</p>
<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.

3.2 LAN & VLAN

This section provides the configuration of LANs and VLANs. VLANs are an optional feature, and their presence depends on the product specification of the purchased gateway.

3.2.1 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 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. A 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> It is also the IP address of web UI. If you change it, you need to type new IP address in the browser to access the web UI.
Subnet Mask	1. A Required setting 2. 255.255.255.0 (/24) is set by default	Select the subnet mask for this gateway from the dropdown list. Subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0 (/24), and it means maximum 254 IP

		addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway, so there are maximum 253 clients allowed in LAN network. <b>Value Range:</b> 255.0.0.0 (/8) ~ 255.255.255.252 (/30).
<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.

## Create / Edit Additional IP

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

Additional IP
 Add Delete
↑ ×

ID	Name	Interface	IP Address	Subnet Mask	Enable	Action
----	------	-----------	------------	-------------	--------	--------

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

Additional IP Configuration
 ↑ ×

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

Save

Configuration		
Item	Value setting	Description
<b>Name</b>	1. An Optional Setting	Enter the name for the alias IP address.
<b>Interface</b>	1. A Required setting 2. <b>lo</b> is set by default	Specify the Interface type. It can be <b>lo</b> or <b>br0</b> .
<b>IP Address</b>	1. An Optional setting 2. <b>192.168.123.254</b> is set by default	Enter the addition IP address for this device.
<b>Subnet Mask</b>	1. A 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. <b>Value Range:</b> 255.0.0.0 (/8) ~ 255.255.255.255 (/32).
<b>Save</b>	NA	Click the <b>Save</b> button to save the configuration

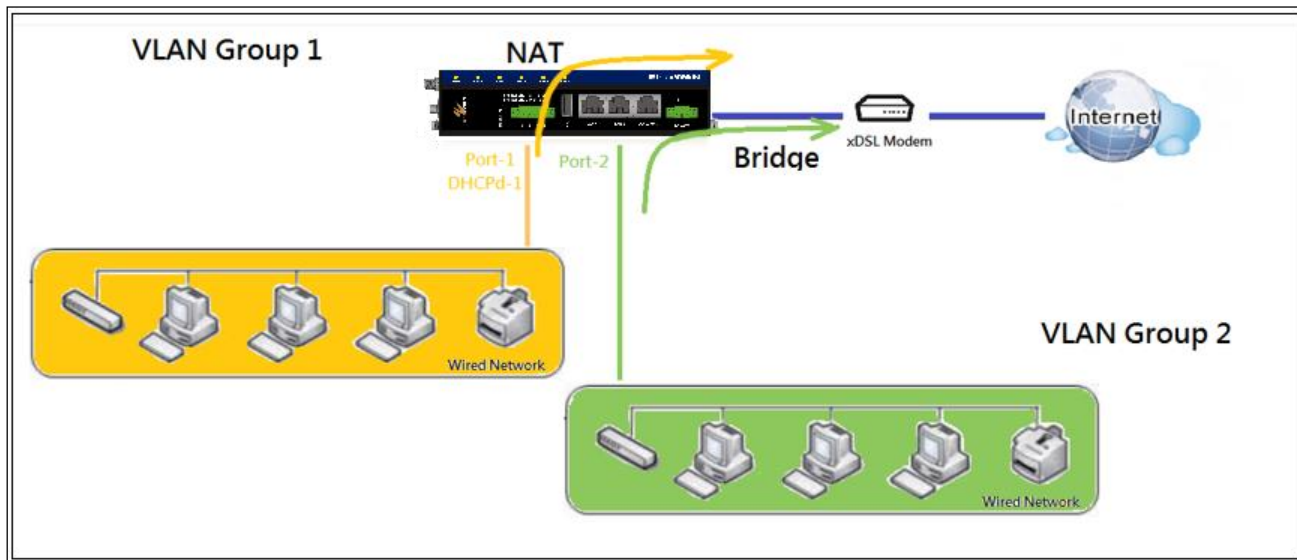
## 3.2.2 VLAN

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 VLANs and Tag-based VLANs. These functions allow you to divide local the network into different “virtual LANs”. It is common requirement for some application scenarios. For example, 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 by your plan. In some cases, ISP may need the router to support “VLAN tags” for certain kinds of services (e.g. IPTV). You can group all devices that require this service as one tag-based VLAN.

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

### ➤ Port-based VLAN

Port-based VLAN function can group Ethernet ports, and Port-1 ~ Port-4 together for differentiated services like Internet surfing, multimedia enjoyment, VoIP talking, and so on. Two operation modes, NAT and Bridge, can be applied to each VLAN group. One DHCP server can be allocated for a NAT VLAN group to let group host member get its IP address. Thus, each host can surf Internet via the NAT mechanism of business access gateway. In bridge mode, Intranet packet flow is delivered out WAN trunk port with VLAN tag to upper link for different services.

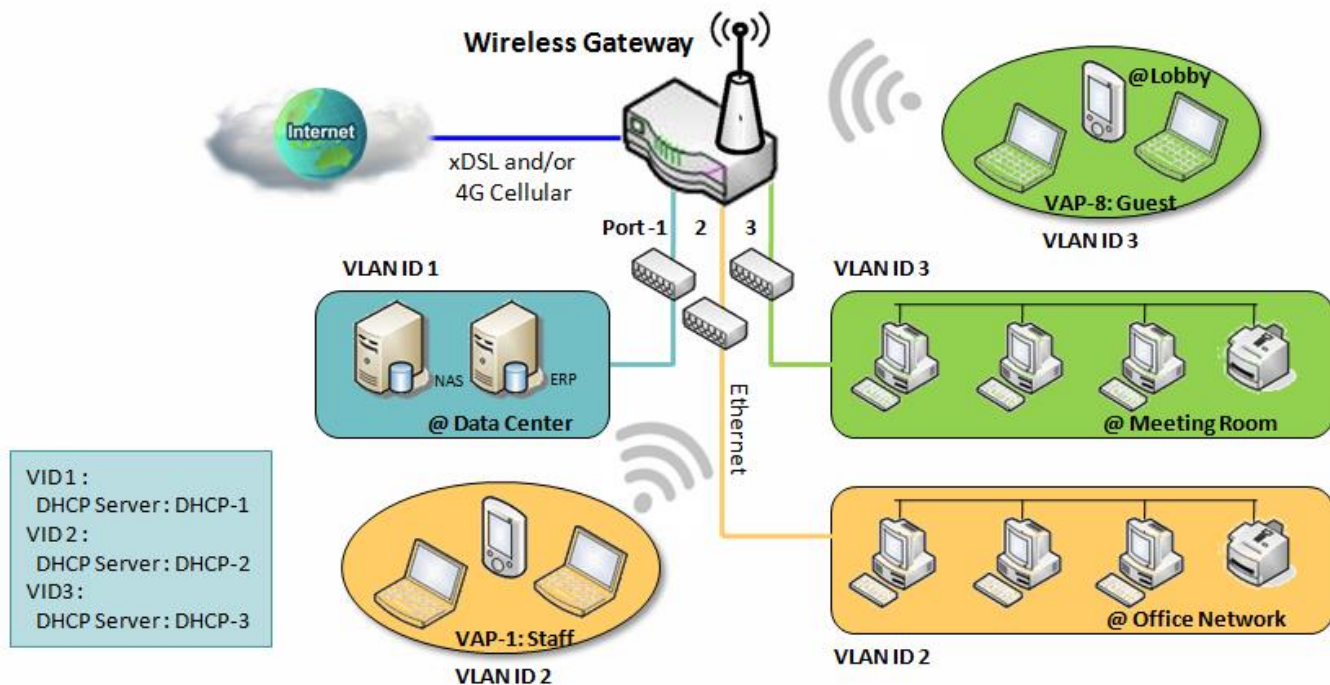


A port-based VLAN is a group of ports on an Ethernet or Virtual APs of Wired or Wireless Gateway that form a logical LAN segment. Following is an example.

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

# AIR PACE

with VLAN ID 1. The VLAN group includes Port-1 with NAT mode to WAN interface as shown in following diagram.



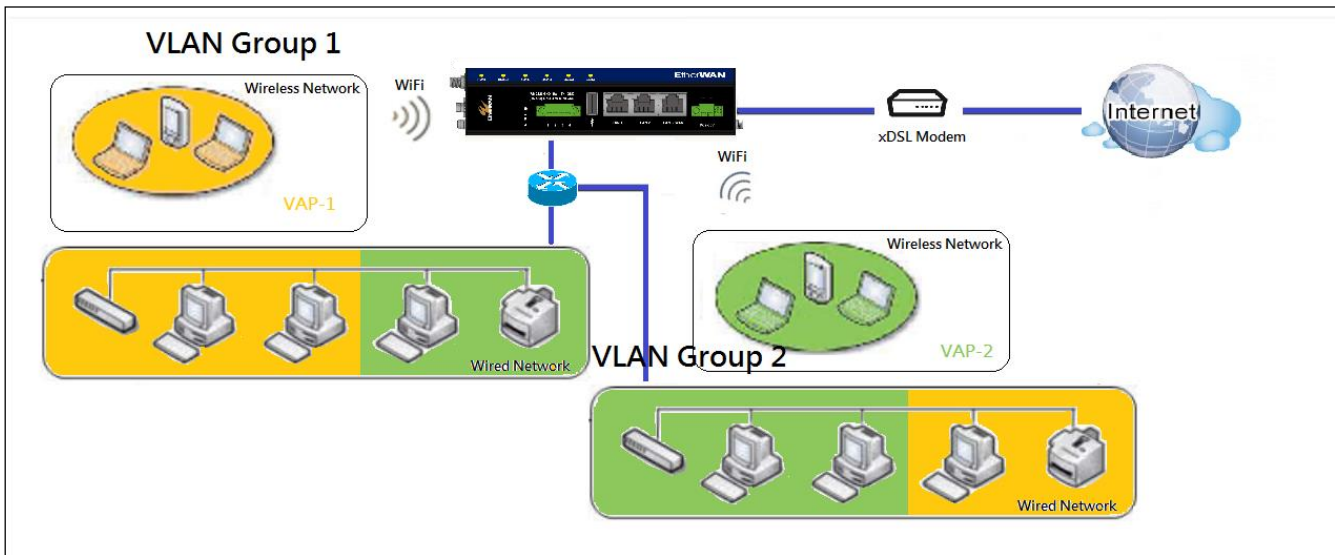
Above is the general case for 3 Ethernet LAN ports in the gateway. But if the device just has one Ethernet LAN port, there will be only one VLAN group for the device. Under such situation, it still supports both the NAT and Bridge mode for the Port-based VLAN configuration.

## ➤ Tag-based VLAN

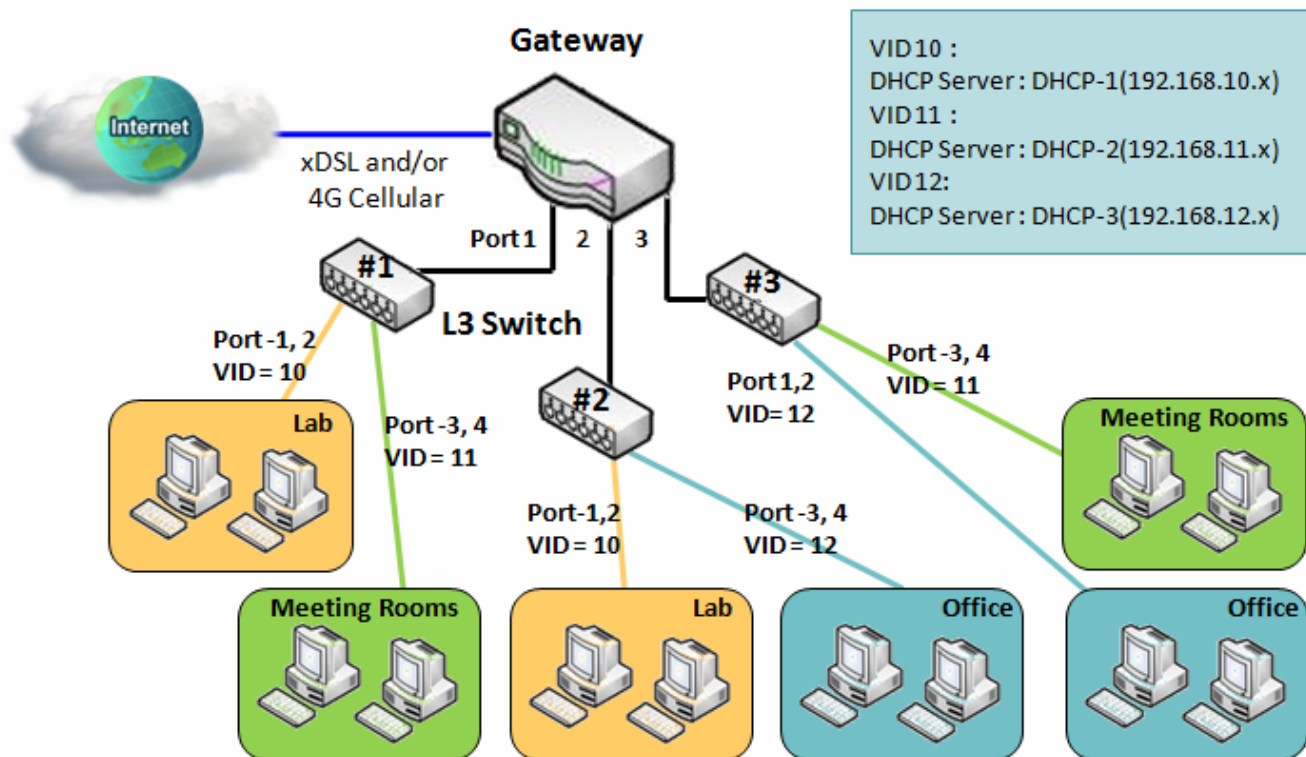
Tag-based VLAN function can group Ethernet ports, Port-1 ~ Port-4 together with different VLAN tags for deploying subnets in Intranet. All packet flows can carry with different VLAN tags even at the same physical Ethernet port for Intranet. These flows can be directed to different destination because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

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

# AIR PACE



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



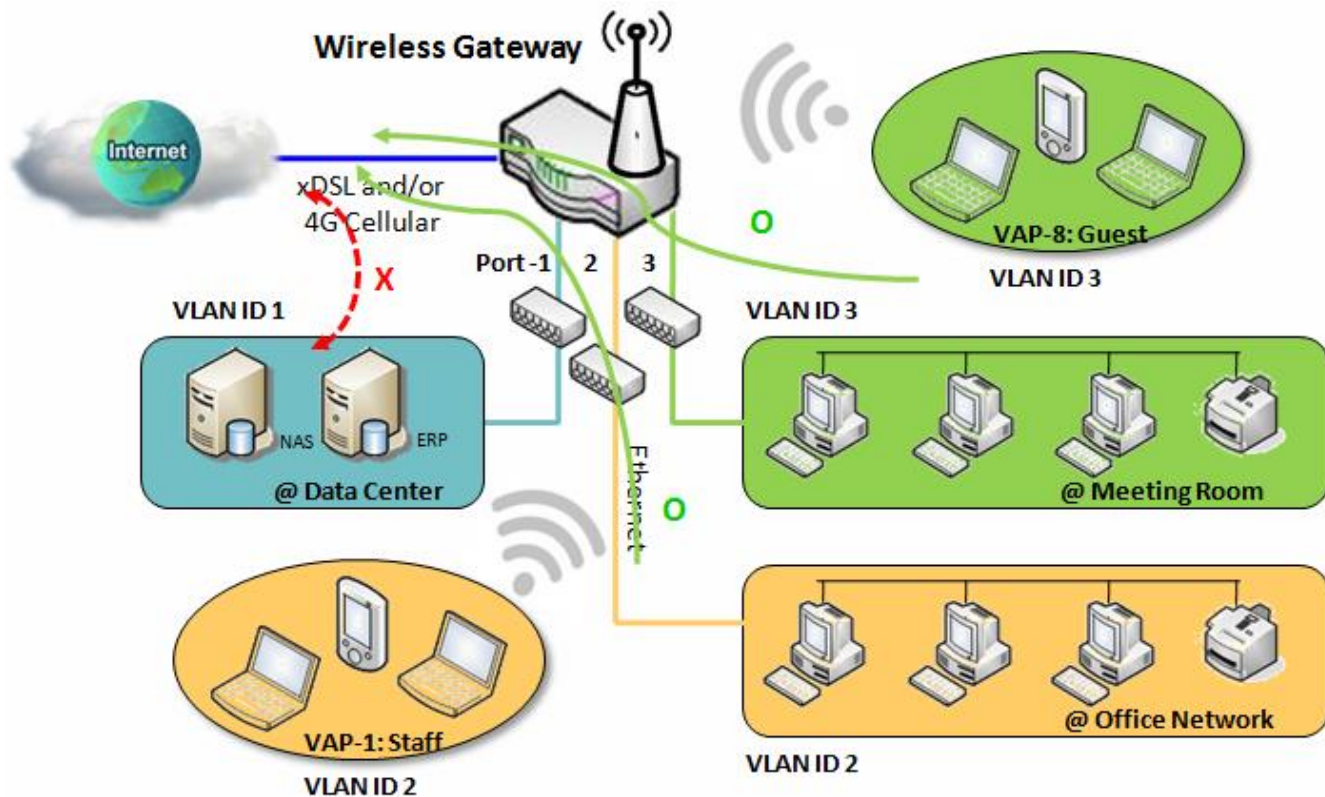


## ➤ VLAN Groups Access Control

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

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

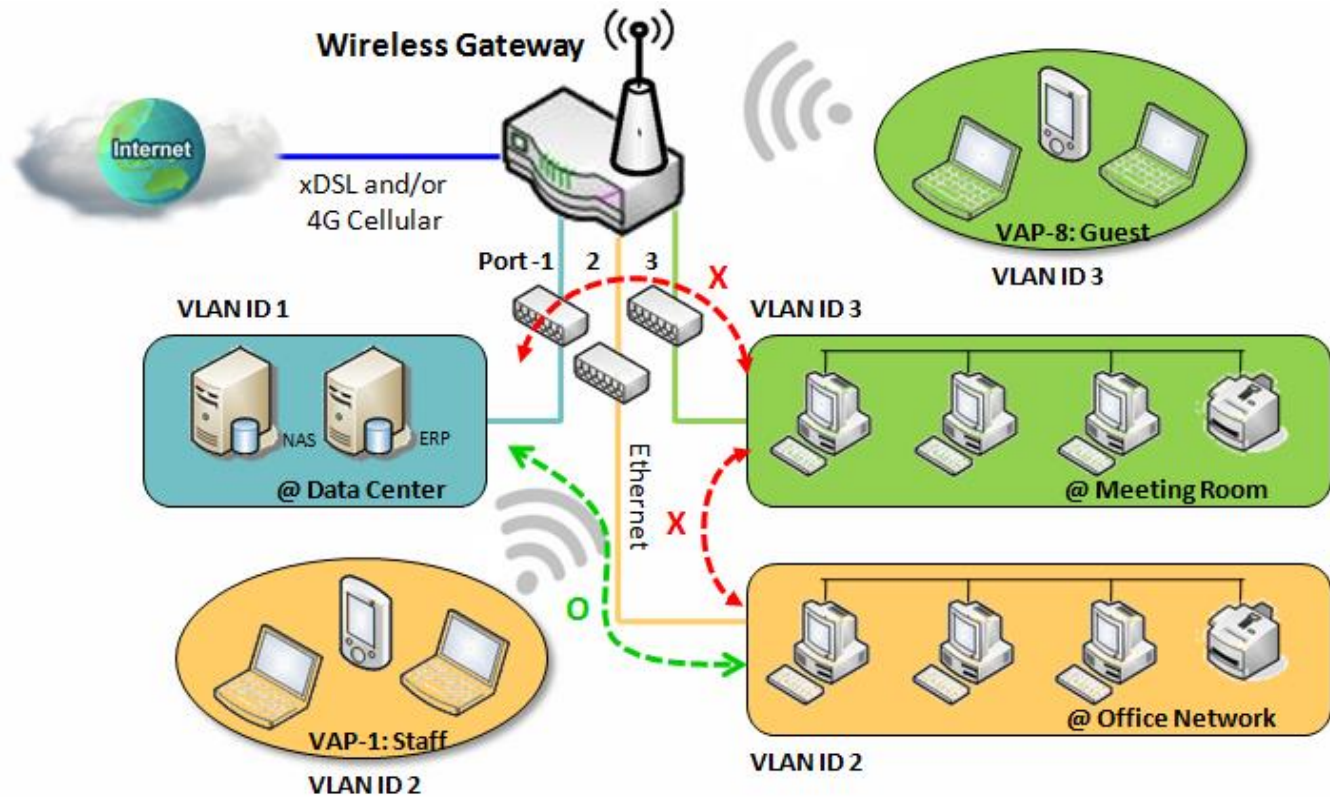




# AIR PACE

## Inter VLAN Group Routing:

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



## VLAN Setting

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

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

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 adopt for organizing you local subnets. <b>Port-based:</b> Port-based VLAN allows you to add rule for each LAN port, and you can do advanced control with its VLAN ID. <b>Tag-based:</b> Tag-based VLAN allows you to add VLAN ID, and select member 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> is 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. Also, if your device has a DMZ port, you will see DMZ configuration, too. The maximum rule numbers is based on LAN port numbers.

Port-based VLAN List <span>Add</span> <span>Delete</span>										
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"/>	<span>Edit</span>
LAN	Native VLAN	X	NAT	<span>Detail</span>	192.168.123.254	255.255.255.0	All WANs	0	<input checked="" type="checkbox"/>	<span>Edit</span>

Apply
Inter VLAN Group Routing

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

## 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-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
▶ LAN to Join	<input type="checkbox"/> Enable <input type="text" value="DHCP 1 ▼"/>

Port-based VLAN Configuration (part-I)		
Item	Value setting	Description
<b>Name</b>	1. A Required setting 2. String format: already have default texts	Define the <b>Name</b> of this rule. It has a default text and cannot be modified.
<b>VLAN ID</b>	A 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>	These boxes are unchecked by default.	Select which LAN port(s) and VAP(s) that you want to add to the rule. Note: The available member list can be different for the purchased product.
<b>LAN to Join</b>	The box is 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.
<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.

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

▶ WAN & WAN VID to Join	All WANs ▼ <input type="button" value="None"/>
▶ LAN IP Address	<input type="text" value="192.168.2.254"/>
▶ Subnet Mask	<input type="text" value="255.255.255.0 (/24)"/> ▼
▶ DHCP Server / Relay	Server ▼
▶ DHCP Server Name	<input type="text"/>
▶ IP Pool	Starting Address: <input type="text" value="192.168.2.100"/> Ending Address: <input type="text" value="192.168.2.200"/>
▶ 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)
▶ Enable	<input type="checkbox"/>

Port-based VLAN Configuration (part-II)		
Item	Value setting	Description
<b>WAN &amp; WAN VID to Join</b>	All WANs are 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>	A 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>	Server is selected by default.	Define the <b>DHCP Server</b> type. There are three types you can select: <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, and 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, and 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>	A 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 Option 82 (for DHCP Relay only)</b>	An Optional setting	If you select <b>Relay</b> type of DHCP Server, you can further enable the DHCP Option 82 setting if the DHCP server support it.
<b>DHCP Server Name</b>	A Required setting	Define name of the DHCP Server for the specified VLAN group.
<b>IP Pool</b>	A 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>	A Required setting	Define a period of time for an IP Address that the DHCP Server leases to a new

# AIR PACE

		device. By default, the <b>lease time</b> is 86400 seconds.
<b>Domain Name</b>	String format, can be 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>	The box is 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 what you just configured back to the previous setting.

# AIR PACE

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

IP Fixed Mapping Rule List <span>Add</span> <span>Delete</span>			
MAC Address	IP Address	Enable	Actions

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

Mapping Rule Configuration		
Item	Value setting	Description
<b>MAC Address</b>	A Required setting	Define the <b>MAC Address</b> target that the DHCP Server wants to match.
<b>IP Address</b>	A 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.
<b>Enable</b>	The box is 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

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

Port-based VLAN List <span>Add</span> <span>Delete</span>										<span>↑</span> <span>×</span>
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	<span>Detail</span>	192.168.66.1	255.255.254.0	All WANs	0	<input checked="" type="checkbox"/>	<span>Edit</span>
<span>Apply</span> <span>Inter VLAN Group Routing</span>										

# AIR PACE

## Port-based VLAN – Inter VLAN Group Routing

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

VLAN Group Internet Access Definition		
VLAN IDs	Members	Internet Access(WAN)
1	Port : 2,3 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 means all <b>VLAN ID</b> members are allow to access WAN interface. If a specific <b>VLAN ID</b> box is unchecked, it means that VLAN ID member can't access the Internet anymore. Note: <b>VLAN ID 1</b> is available always; it is the default VLAN ID of <b>LAN</b> rule. The

		other <b>VLAN IDs</b> are available only when they are enabled.
<b>Inter VLAN Group Routing</b>	The box is unchecked by default.	Click the expected VLAN IDs box to enable the Inter VLAN access function. By default, members in different VLAN IDs can't access each other. The gateway supports up to 4 rules for <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. Also, if your device has a DMZ port, you will see DMZ configuration, too. The router supports up to a maximum of 128 tag-based VLAN rule sets.

Tag-based VLAN List							↑	×
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			<div>Edit</div> <div>Select</div>		

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-I)		
Item	Value setting	Description
<b>VLAN ID</b>	A Required setting	Define the <b>VLAN ID</b> number, that is outside the system reserved range. <b>Value Range:</b> 1 ~ 4095.
<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>	The boxes are 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 wireless gateways have the VAP list.
<b>Bridge Interface</b>	<b>DHCP 1</b> is selected by default.	Select a predefined <b>DHCP Server</b> , a <b>New</b> to defined 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 <b>Save</b> button, always click <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 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

Tag-based VLAN Configuration (part-II)		
Item	Value setting	Description
<b>IP Address</b>	A Required setting	Assign an <b>IP Address</b> for the DHCP Server that the rule uses, this IP address is a gateway IP.
<b>Subnet Mask</b>	<b>255.255.255.0(/24)</b> is selected by default.	Select a <b>Subnet Mask</b> for the DHCP Server.
<b>DHCP Relay</b>	The box is unchecked by default.	Check the box to enable the DHCP Relay function for the VLAN group, and you only need to fill the <b>DHCP Server IP Address</b> field.
<b>WAN Interface</b>	<b>WAN-1</b> is selected by default.	Select which <b>WAN</b> interface that allows accessing Internet.
<b>DHCP Option 82</b>	An Optional setting	If you select <b>Relay</b> type of DHCP Server, you can further enable the DHCP Option 82 setting if the DHCP server support it.
<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.

## Tag-based VLAN Summary

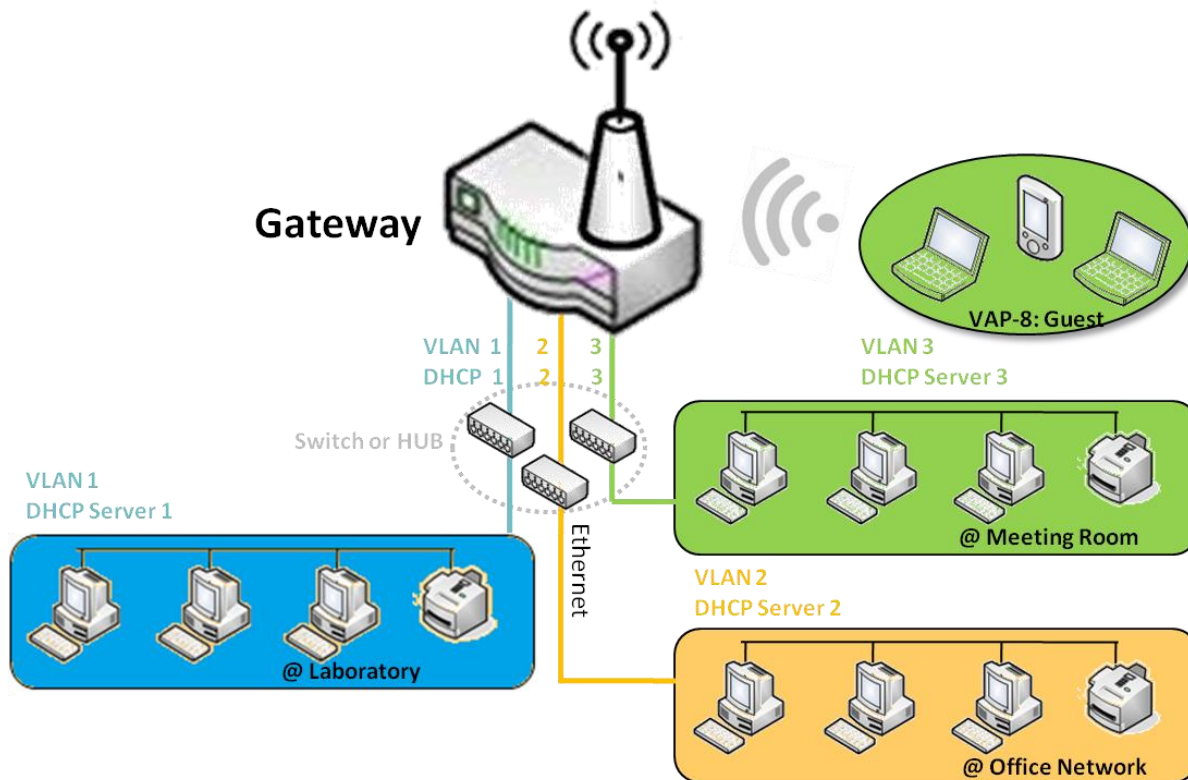
The configured tag-based VLAN group information will be displayed in the following screen.

Tag-based VLAN Summary		▲	✕
Port	VLAN IDs		
Port2	Native VLAN		
Port3	Native VLAN		

## 3.2.3 DHCP Server

### ➤ DHCP Server

The gateway supports up to 4 DHCP servers to fulfill the DHCP requests from different VLAN groups (please refer to VLAN section for more 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 ranges is from “.100” to “.200” as shown at the DHCP Server List page on gateway’s WEB UI.

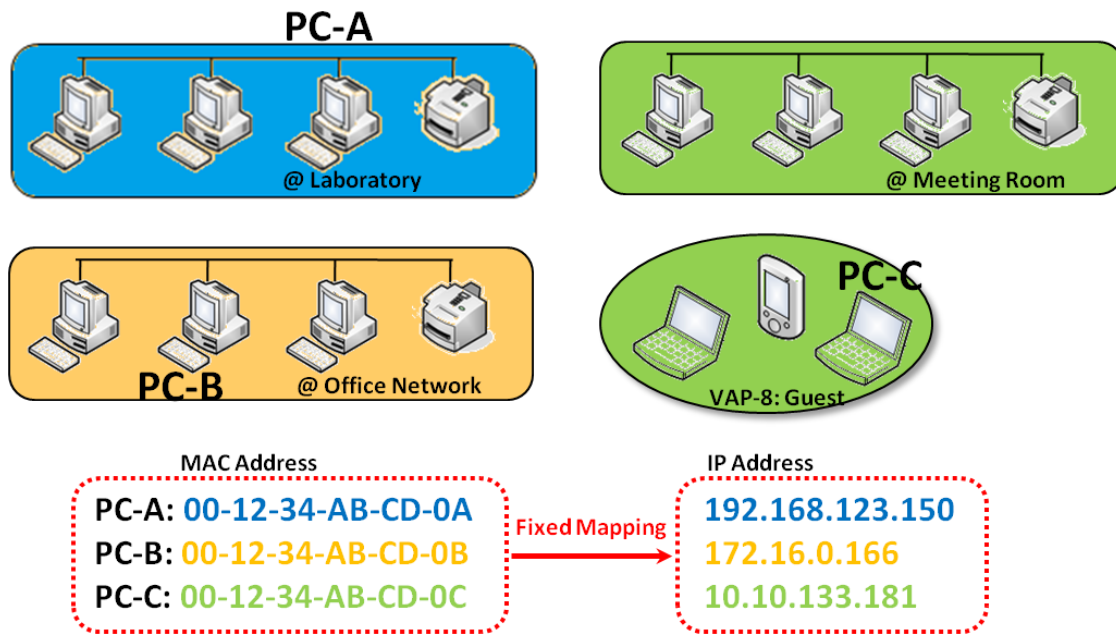


User can add more DHCP server configurations by clicking on the “Add” button behind “DHCP Server List”, or clicking on the “Edit” button at the end of each DHCP Server on list to edit its current settings. Additionally, user can select a DHCP Server and delete it by clicking on the “Select” check-box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

# AIR PACE

## ➤ Fixed Mapping

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



## 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), and it supports up to a maximum of 4 policy sets.

DHCP Server List <span>Add</span> <span>Delete</span> <span>DHCP Client List</span> <span>↑</span> <span>×</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	192.168.66.1	255.255.254.0	192.168.66.100-192.168.66.200	900		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 **Add** button is applied, **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="192.168.2.1"/>
▶ Subnet Mask	<input type="text" value="255.255.255.0 (/24)"/> ▼
▶ 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)

DHCP Server Configuration		
Item	Value setting	Description
<b>DHCP Server Name</b>	1. String format, can be any text 2. A Required setting	Enter a DHCP Server name. Enter a name that is easy to understand.
<b>LAN IP Address</b>	1. IPv4 format. 2. A 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. A Required setting	The IP Pool of this DHCP Server. It composed of Starting Address entered in this field and Ending Address entered in this field.
<b>Lease Time</b>	1. Numeric string format. 2. A Required setting	The Lease Time of this DHCP Server. <b><i>Value Range: 300 ~ 604800 seconds.</i></b>
<b>Domain Name</b>	String format, can be 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>	The box is 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 **Fix Mapping** button is applied, the **Mapping Rule List** screen will appear.

Mapping Rule List <span>Add</span> <span>Delete</span> <span>↑</span> <span>×</span>			
MAC Address	IP Address	Enable	Actions

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

# AIR PACE

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
<b>MAC Address</b>	1. MAC Address string format 2. A Required setting	The MAC Address of this mapping rule.
<b>IP Address</b>	1. IPv4 format. 2. A Required setting	The IP Address of this mapping rule.
<b>Rule</b>	The box is 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
<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 <b>DHCP Server Configuration</b> page.

## View / Copy DHCP Client List

When **DHCP Client List** button is applied, **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

DHCP Client List <span>Copy to Fixed Mapping</span>					
LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time	Actions

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

## Enable / Disable DHCP Server Options

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

Option	Meaning	RFC
66	TFTP server name	<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							
		Add	Delete				
ID	Option Name	DHCP Server Select	Option Select	Type	Value	Enable	Actions

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

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

DHCP Server Option Configuration		
Item	Value setting	Description
<b>Option Name</b>	1. String format, can be any text 2. A Required setting.	Enter a DHCP Server Option name. Enter a name that is easy to understand.
<b>DHCP Server Select</b>	Dropdown list of all available DHCP servers.	Choose the DHCP server this option should apply to.
<b>Option Select</b>	1. A Required setting. 2. <b>Option 66</b> is selected by default.	Choose the specific option from the dropdown list. It can be <b>Option 66</b> , <b>Option 72</b> , <b>Option 144</b> , <b>Option 42</b> , <b>Option 150</b> , or <b>Option 160</b> . <b>Option 42</b> for ntp server; <b>Option 66</b> for tftp;

		Option 72 for www; Option 144 for url;		
Type	Dropdown list of DHCP server option value types	Each different options has different value types.		
		66	Single IP Address	
			Single FQDN	
		72	IP Addresses List, separated by “,”	
		114	Single URL	
		42	IP Addresses List, separated by “,”	
		150	IP Addresses List, separated by “,”	
		160	Single IP Address	
Single FQDN				
Value	1. IPv4 format 2. FQDN format 3. IP list 4. URL format 5. A Required setting	Should conform to Type:		
		66	Type	Value
			Single IP Address	IPv4 format
		72	Single FQDN	FQDN format
			IP Addresses List, separated by “,”	IPv4 format, separated by “,”
114	Single URL	URL format		
Enable	The box is 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	DHCP Relay Option 82	Enable	Actions

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

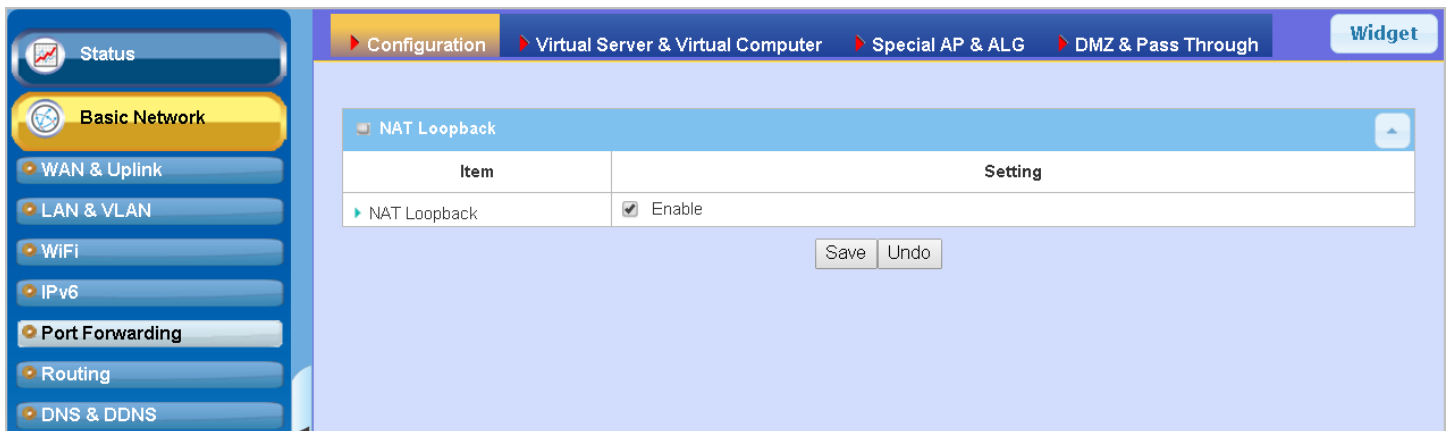
DHCP Relay Configuration	
Item	Setting
▶ Agent Name	<input type="text"/>
▶ LAN interface	LAN ▼
▶ WAN interface	WAN - 1 ▼
▶ Server IP	<input type="text"/>
▶ DHCP OPTION 82	<input type="checkbox"/>
▶ Enable	<input type="checkbox"/>



DHCP Relay Configuration		
Item	Value setting	Description
<b>Agent Name</b>	1. String format, can be any text 2. A Required setting.	Enter a DHCP Relay name. Enter a name that is easy to understand. <b><u>Value Range:</u></b> 1~64 characters.
<b>LAN Interface</b>	1. A 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. A 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. A Required setting. 2. <b>Null</b> is set 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>	The box is 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 requires such information, you have to enable it, otherwise, just leave it as unchecked.
<b>Enable</b>	The box is 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.

## 3.3 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. A 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

### 3.3.1 Configuration

#### NAT Loopback

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

#### Configuration Setting

Go to **Basic Network > Port Forwarding > Configuration** tab.

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

#### Enable NAT Loopback

NAT Loopback	
Item	Setting
▶ NAT Loopback	<input checked="" type="checkbox"/> Enable

Configuration Item	Value setting	Description
NAT Loopback	The box is checked by default	Check the <b>Enable</b> box to activate this NAT 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

## 3.3.2 Virtual Server & Virtual Computer

Configuration

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

Virtual Server List
Add
Delete

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

Virtual Computer List
Add
Delete

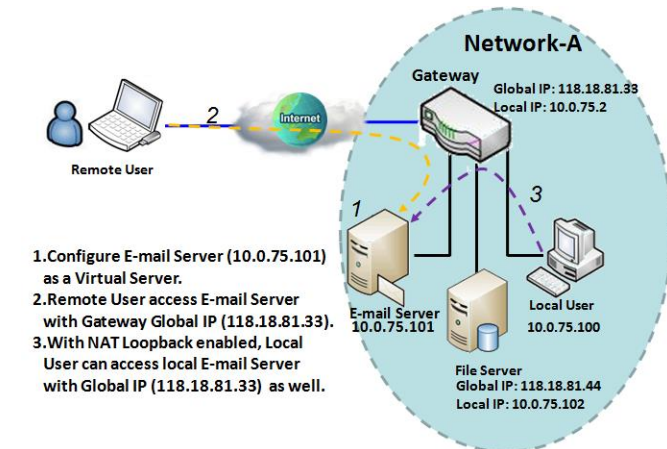
ID	Global IP	Local IP	Enable	Actions
----	-----------	----------	--------	---------

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

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

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

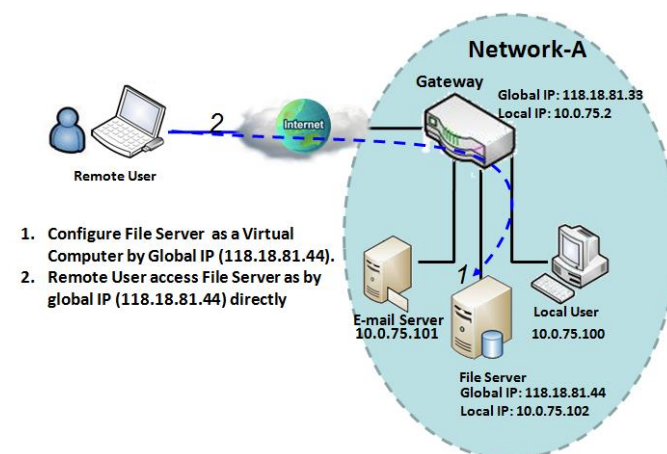
## Virtual Server & NAT Loopback



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 the 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.

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

Configuration Item	Value setting	Description
<b>Virtual Server</b>	The box is unchecked by default	Check the <b>Enable</b> box to activate this port forwarding function
<b>Virtual Computer</b>	The box is checked by default	Check the <b>Enable</b> box to activate this port forwarding 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 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											
										Add	Delete
ID	WAN Interface	Server IP	Source IP	Protocol	Public Port	Private Port	Time Schedule	Enable	Actions		

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

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. A Required setting 2. Default is <b>ALL</b> .	Define the selected interface to be the packet-entering interface of the gateway. 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 gateway from any interface. Select <b>WAN-x</b> box when <b>WAN-x</b> is enabled. <b>Note:</b> The available check boxes ( <b>WAN-1</b> ~ <b>WAN-4</b> ) depend on the number of WAN interfaces for the product.
<b>Server IP</b>	A Required setting	This field is to specify the IP address of the interface selected in the WAN Interface setting above.
<b>Source IP</b>	1. A 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 allow the access coming from any IP addresses. Select <b>Specific IP Address</b> to allow the access coming from an IP address. Select <b>IP Range</b> to allow the access coming from a specified range of IP address.
<b>Protocol</b>	1. A Required setting 2. <b>TCP &amp; UDP</b> is selected by default.	When " <b>ICMPv4</b> " is selected It means the option "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> ) Then check <b>Enable</b> box to enable this rule.  When " <b>TCP</b> " is selected It means the option "Protocol" of packet filter rule is TCP. <b>Public Port</b> selected a predefined port from <b>Well-known Service</b> , and <b>Private Port</b> is the same with <b>Public Port</b> number. <b>Public Port</b> is selected <b>Single Port</b> and specify a port number, and <b>Private Port</b> can be set a <b>Single Port</b> number. <b>Public Port</b> is selected <b>Port Range</b> and specify a port range, and <b>Private Port</b> can be selected <b>Single Port</b> or <b>Port Range</b> . <u>Value Range:</u> 1 ~ 65535 for Public Port, Private Port.

When “**UDP**” is selected

It means the option “Protocol” of packet filter rule is UDP.

**Public Port** selected a predefined port from **Well-known Service**, and **Private Port** is the same with **Public Port** number.

**Public Port** is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number.

**Public Port** is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**.

Value Range: 1 ~ 65535 for Public Port, Private Port.

When “**TCP & UDP**” is selected

It means the option “Protocol” of packet filter rule is TCP and UDP.

**Public Port** selected a predefined port from **Well-known Service**, and **Private Port** is the same with **Public Port** number.

**Public Port** is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number.

**Public Port** is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**.

Value Range: 1 ~ 65535 for Public Port, Private Port.

When “**GRE**” is selected

It means the option “Protocol” of packet filter rule is GRE.

When “**ESP**” is selected

It means the option “Protocol” of packet filter rule is ESP.

When “**SCTP**” is selected

It means the option “Protocol” of packet filter rule is SCTP.

When “**User-defined**” is selected

It means the option “Protocol” of packet filter rule is User-defined.

For **Protocol Number**, enter a port number.

<b>Time Schedule</b>	1. An optional filled 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. An optional filled setting 2. The box is 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>X</b> button to cancel the settings and return to previous page.



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 Add Delete				
ID	Global IP	Local IP	Enable	Actions

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

Virtual Computer Rule Configuration		
Global IP	Local IP	Enable
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

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

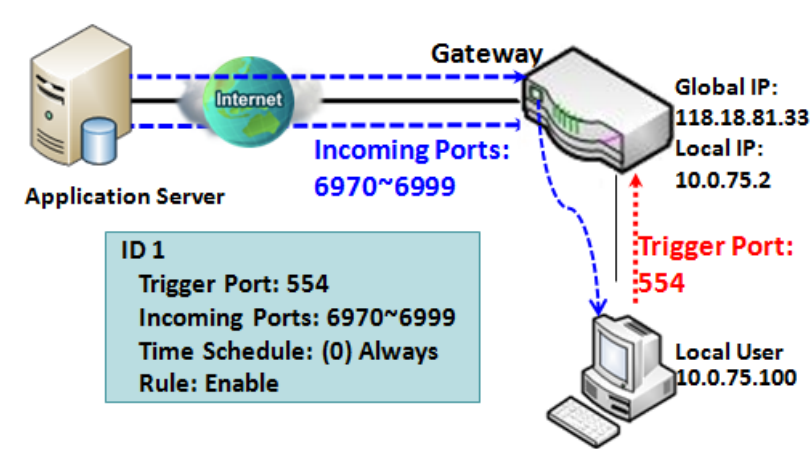
3.3.3 Special AP & ALG

As a NAT gateway, the device doesn't allow active connection requests from the outside world. All of these kinds of requests will be ignored by the NAT gateway. 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.

Additionally, 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

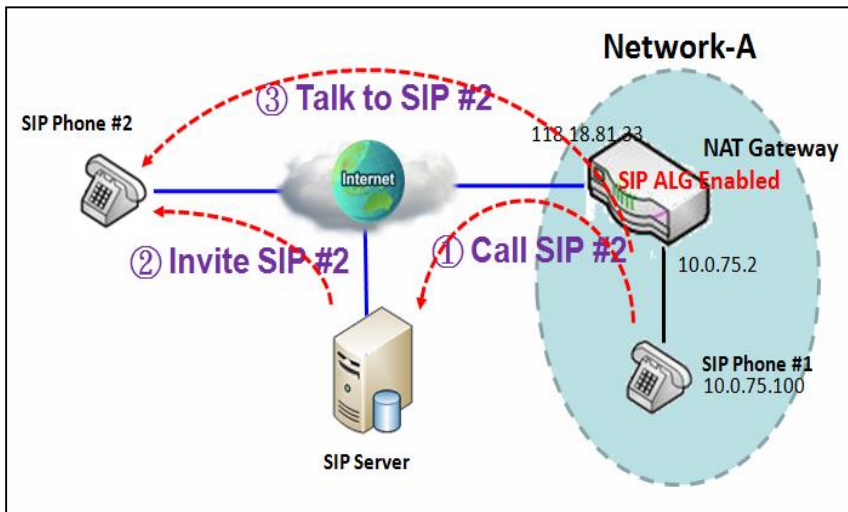


data packet from remote application server will pass through incoming port 6970~6999.

SIP ALG

# AIR PACE

This gateway supports the SIP ALG feature to allow one SIP phone behind the NAT gateway can call another SIP phone in the Internet, even as the gateway executes its NAT mechanism between the Intranet and the Internet. The NAT gateway monitors the control traffic and open 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 recognized the traffic from SIP Phone #2 is part of the connection sessions with SIP Phone #1.

## 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 your Special AP rules. It supports up to a maximum of 8 rule-based Special AP sets.

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

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

Special AP 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 <input type="checkbox"/> WAN-4
▶ 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. A Required setting 2. <b>All</b> is checked by default.	Check the interface box(es) to apply the Special AP rule. By default, <b>All</b> is checked, and the Special AP rule will be applied to all WAN interfaces.
<b>Trigger Port</b>	1. A 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 other popular applications from the dropdown list, the corresponding trigger port(s) and incoming ports will be defined automatically. <u><b>Value Range:</b> 1 ~ 65535.</u>
<b>Incoming Ports</b>	1. A Required setting	Enter the expected Incoming ports if <b>User-defined</b> is selected in the Trigger Port dropdown list. If you select other popular applications from the dropdown list, the corresponding incoming ports will be defined automatically. <u><b>Value Range:</b> 1 ~ 65535; It can be a single port, multiple ports separated by ",", .or port range.</u>
<b>Time Schedule</b>	1. A 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>	The box is 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

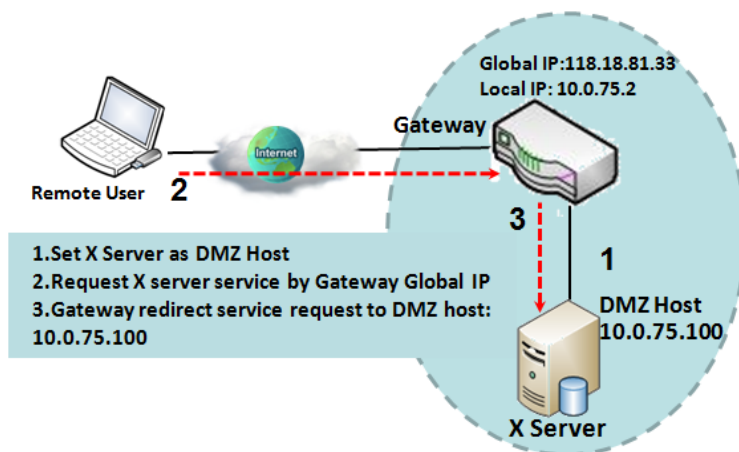
## 3.3.4 DMZ & Pass Through

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

The DMZ function allows you to ask the gateway 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. Certainly, the DMZ host is also protected by the gateway firewall. Activate the feature and specify the DMZ host with a host in the Intranet when needed.

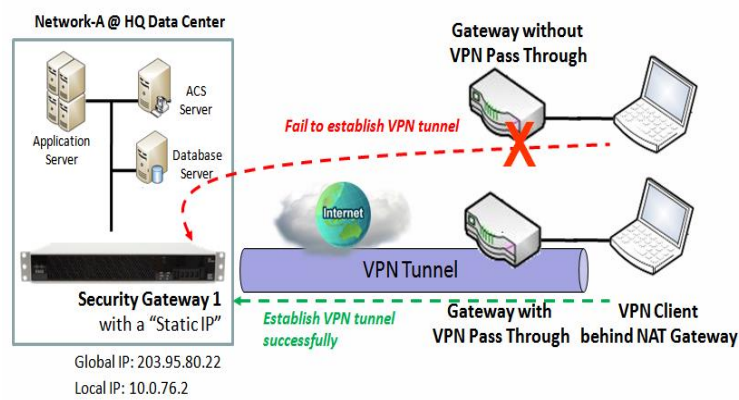
Configuration	
Item	Setting
DMZ	<input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> All <input type="checkbox"/> WAN-1 <input type="checkbox"/> WAN-2 <input type="checkbox"/> WAN-3 <input type="checkbox"/> WAN-4 DMZ Host : <input type="text" value="10.0.75.100"/>
Pass Through 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 some service daemons in a host behind NAT gateway to allow remote users request for services from server actively, you just have to configure this host as DMZ Host. As shown in the diagram, there is an X server installed as DMZ host, whose IP address is 10.0.75.100. Then, remote user can request services from X server just as it is provided by the gateway whose global IP address is 118.18.81.33. The gateway will forward those packets, not belonging to any configured virtual server or applications, directly to the DMZ host.

VPN Pass through Scenario



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

DMZ & Pass Through Setting

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

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

Enable DMZ and Pass Through

Configuration	
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

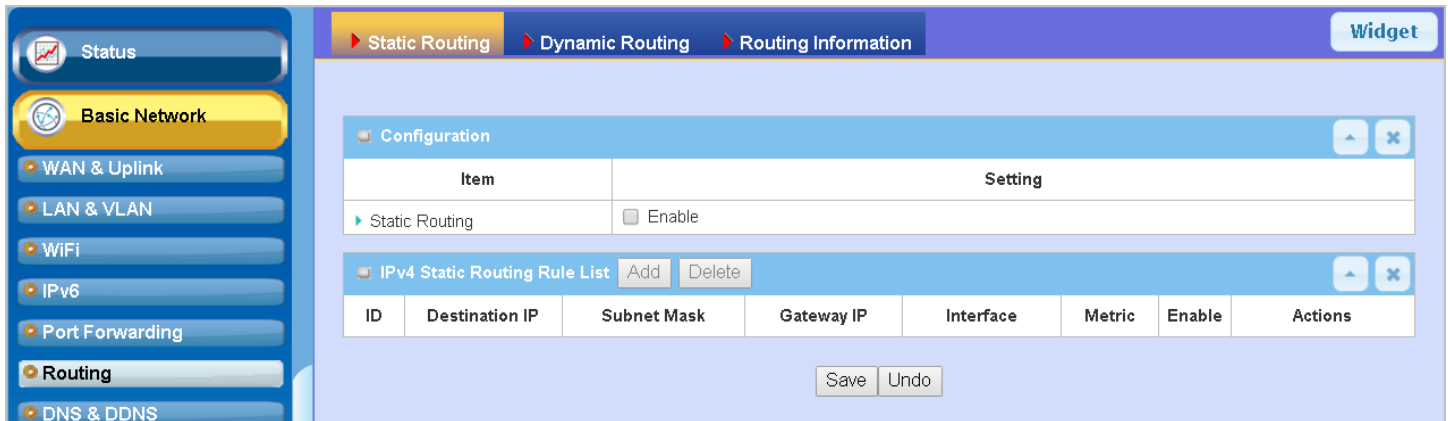
Configuration Item	Value setting	Description
DMZ	<ol style="list-style-type: none"><li>A Required setting</li><li>Default is <b>ALL</b>.</li></ol>	<p>Check the <b>Enable</b> box to activate the DMZ function</p> <p>Define the selected interface to be the packet-entering interface of the gateway, and fill in the IP address of Host LAN IP in <b>DMZ Host</b> field</p> <p>.</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 router from any interfaces.</p> <p>It can be selected <b>WAN-x</b> box when <b>WAN-x</b> enabled.</p> <p><b>Note:</b> The available check boxes (<b>WAN-1 ~ WAN-4</b>) depend on the number</p>

# AIR PACE

		of WAN interfaces for the product.
<b>Pass Through Enable</b>	The boxes are checked by default	Check the box to enable the pass through function for the <b>IPSec</b> , <b>PPTP</b> , and <b>L2TP</b> . With the pass through function enabled, the VPN hosts behind the gateway still can connect to remote VPN servers.
<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



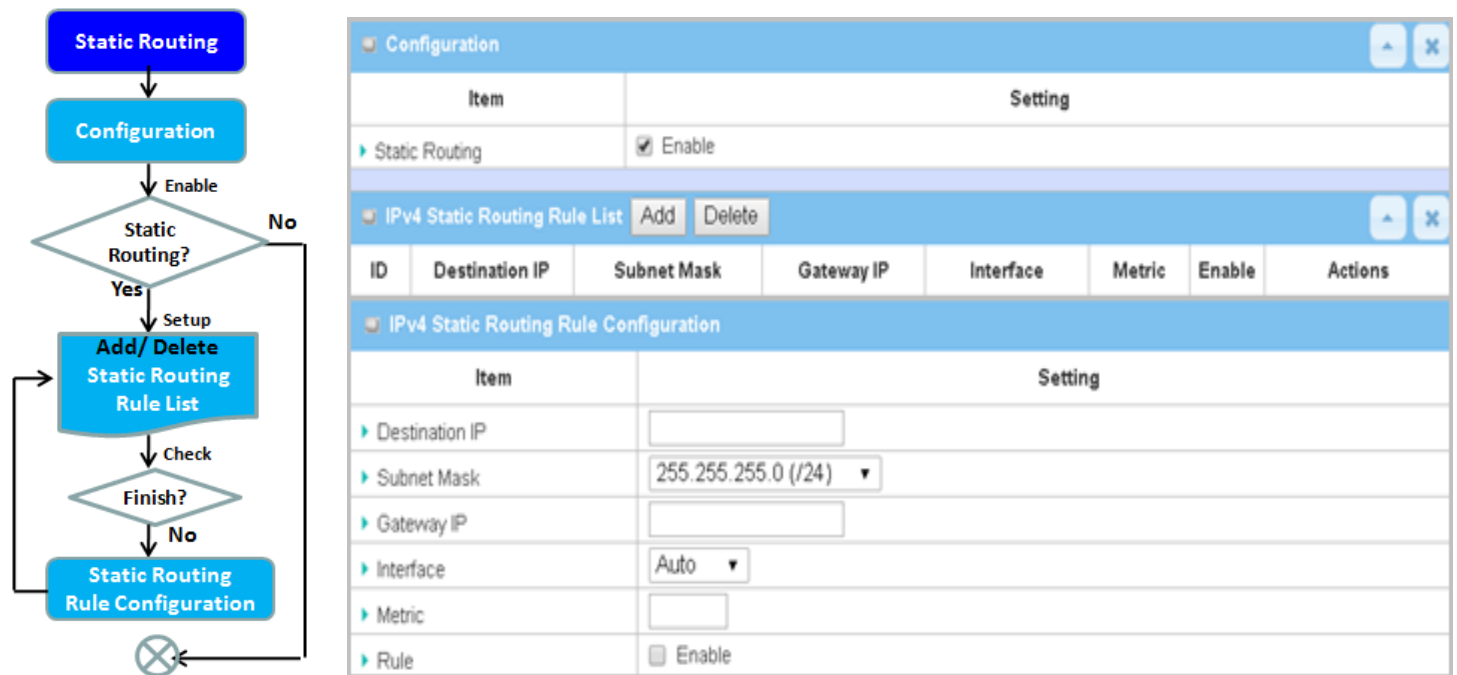
## 3.4 Routing



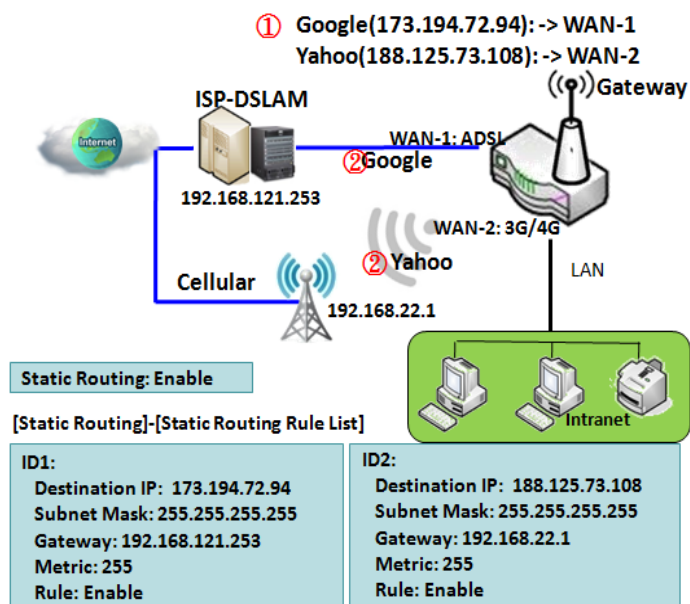
If you have more than one router and subnet, you will need to enable routing function to allow packets to find proper routing path and allow different subnets to communicate with each other. Routing is the process of selecting best paths in a network. It is performed for many kinds of networks, like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

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

## 3.4.1 Static Routing



"Static Routing" function lets you define the routing paths for some dedicated hosts/servers or subnets to store in the routing table of the gateway. The gateway routes incoming packets to different peer gateways based on the routing table. You need to define the static routing information in gateway routing rule list.



When the administrator of the gateway wants to specify what kinds of packets to be transferred via which gateway interface and which peer gateway to their destination. It can be carried out by the "Static Routing" feature. Dedicated packet flows from the Intranet will be routed to their destination via the pre-defined peer gateway and corresponding gateway interface that are defined in the system routing table by manual.

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

## Static Routing Setting

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

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

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

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

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

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

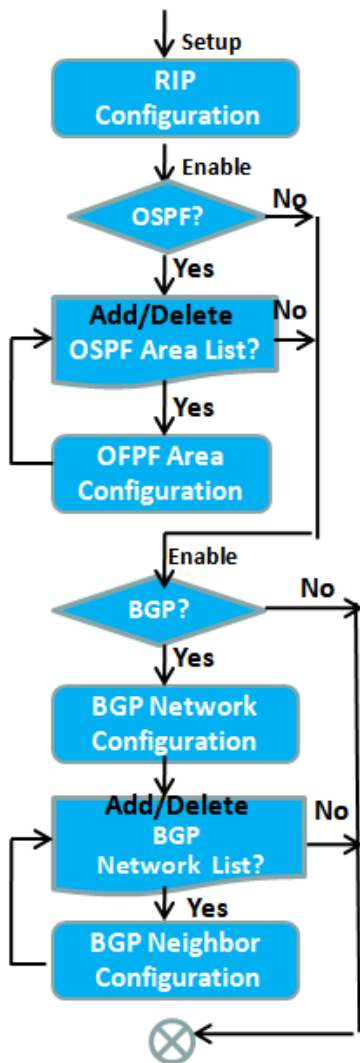
The gateway allows you to customize your static routing rules. It supports up to a maximum of 64 rule sets. When **Add** button is applied, **Static Routing Rule Configuration** screen will appear, while the **Edit** button at the end of each static routing rule lets you modify the rule.

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. A 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. A 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. A Required setting	The Metric of this static routing rule. <i>Value Range: 0 ~ 255.</i>
<b>Rule</b>	The box is 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 what you just configured back to the previous setting.
<b>Back</b>	NA	When the <b>Back</b> button is clicked the screen will return to the Static Routing Configuration page.

## 3.4.2 Dynamic Routing



RIP Configuration				
Item	Setting			
▶ RIP Enable	Disable			

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

OSPF Area List				
ID	Area Subnet	Area ID	Enable	Actions
<div> <div>Add</div> <div>Delete</div> </div>				

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

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

BGP Network List				
ID	Network Subnet	Enable	Actions	
<div> <div>Add</div> <div>Delete</div> </div>				

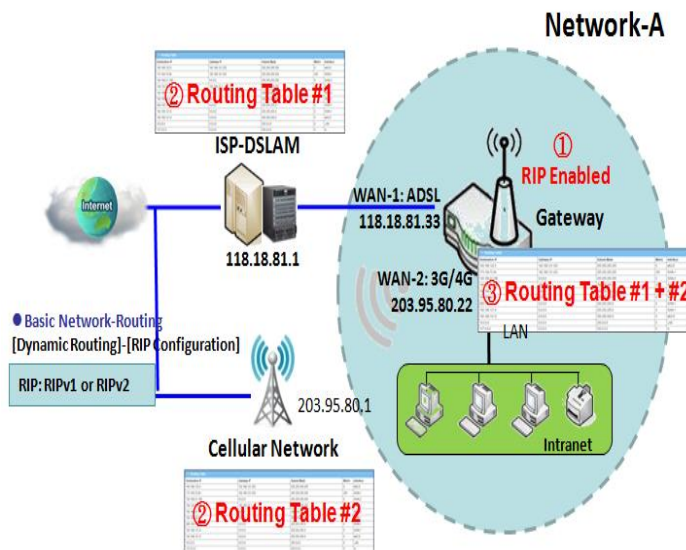
BGP Neighbor List				
ID	Neighbor IP	Remote ASN	Enable	Actions
<div> <div>Add</div> <div>Delete</div> </div>				

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

This gateway supports dynamic routing protocols, including RIPv1/RIPv2 (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol), for you to establish routing table automatically. The feature of dynamic routing will be very useful when there are 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 infrastructures.

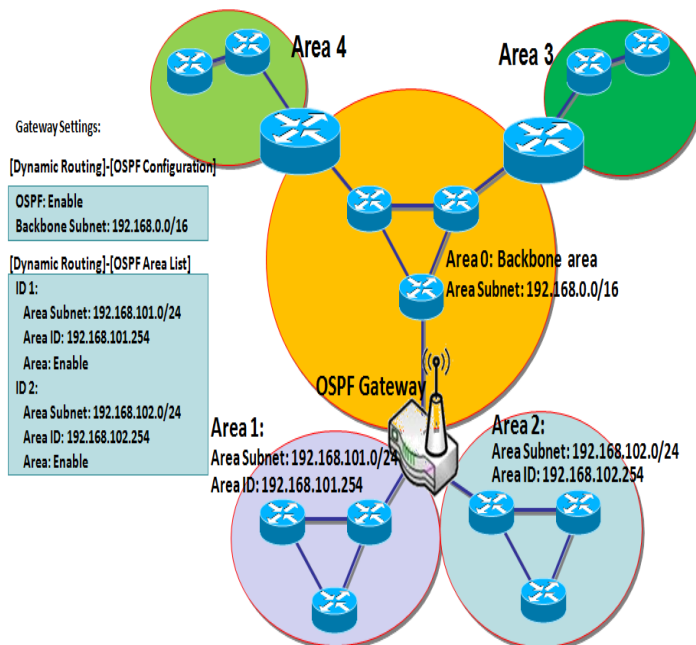
The supported dynamic routing protocols are described as follows.

## RIP Scenario



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

## OSPF Scenario

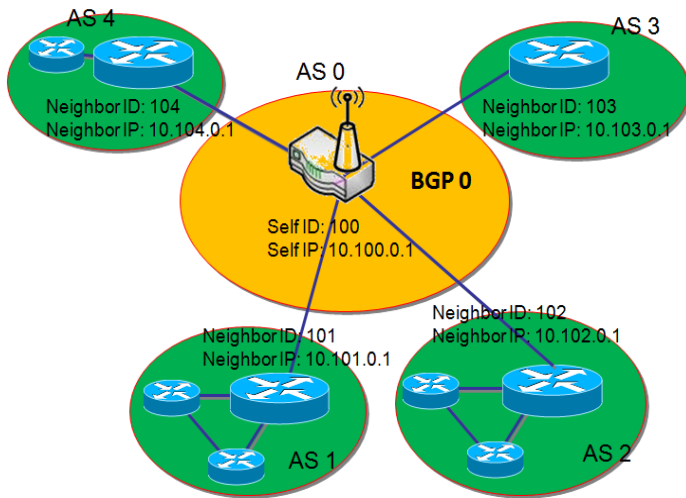


Open Shortest Path First (OSPF) is a routing protocol that uses a link state routing algorithm. It is the most widely used interior gateway protocol (IGP) in large enterprise networks. It gathers link state information from available routers and constructs a topology map of the network. The topology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

Network administrators can deploy an OSPF gateway in large enterprise networks 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, 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.

## BGP Scenario



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

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

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

## Dynamic Routing Setting

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

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

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

The "RIP Configuration" window lets you choose which version of RIP protocol to be activated or disabled. 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. However, the "BGP Configuration" window lets 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

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

RIP Configuration	
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.

### OSPF Configuration

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



OSPF Configuration

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

OSPF Configuration		
Item	Value setting	Description
<b>OSPF</b>	Disable is set by default	Click <b>Enable</b> box to activate the OSPF protocol.
<b>Router ID</b>	1. IPv4 Format 2. A Required setting	The Router ID of this router on OSPF protocol
<b>Authentication</b>	None is set by default	<p>The Authentication method of this router on OSPF protocol.</p> <p>Select <b>None</b> to disable Authentication on OSPF protocol.</p> <p>Select <b>Text</b> to enable Text Authentication with entered Key in this field on OSPF protocol.</p> <p>Select <b>MD5</b> to enable MD5 Authentication with entered ID and Key in these fields on OSPF protocol.</p>
<b>Backbone Subnet</b>	1. Classless Inter Domain Routing (CIDR) Subnet Mask Notation. (Ex: 192.168.1.0/24) 2. A 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



Add

Delete

ID	Area Subnet	Area ID	Enable	Actions
----	-------------	---------	--------	---------

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


**OSPF Area Configuration**

Item	Setting
▶ Area Subnet	<input type="text"/>
▶ Area ID	<input type="text"/>
▶ Area	<input type="checkbox"/> Enable
<div>Save</div>	

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. A Required setting	The Area Subnet of this router on OSPF Area List.
<b>Area ID</b>	1. IPv4 Format 2. A Required setting	The Area ID of this router on OSPF Area List.
<b>Area</b>	The box is 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

# AIR PACE

## BGP Configuration

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

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	The box is unchecked by default	Check the <b>Enable</b> box to activate the BGP protocol.
ASN	1. Numeric String Format 2. A 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. A 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

AddDelete

ID	Network Subnet	Enable	Actions
----	----------------	--------	---------

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

BGP Network Configuration

Item	Setting
▶ Network Subnet	IP : <input type="text"/> 255.255.255.0 (/24) <input type="text"/>
▶ Network	<input type="checkbox"/> Enable

Save

Item	Value setting	Description
Network Subnet	1. IPv4 Format 2. A Required setting	The Network Subnet of this router on BGP Network List. It is composed of the IP address in this field and the selected subnet mask.

<b>Network</b>	The box is 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

## 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 <span>Add</span> <span>Delete</span>				
ID	Neighbor IP	Remote ASN	Enable	Actions

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

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

BGP Neighbor Configuration		
Item	Value setting	Description
<b>Neighbor IP</b>	1. IPv4 Format 2. A Required setting	The Neighbor IP of this router on BGP Neighbor List.
<b>Remote ASN</b>	1. Numeric String Format 2. A Required setting	The Remote ASN of this router on BGP Neighbor List. <b><u>Value Range:</u></b> 1 ~ 4294967295.
<b>Neighbor</b>	The box is 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

## 3.4.3 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	-	-	-	-

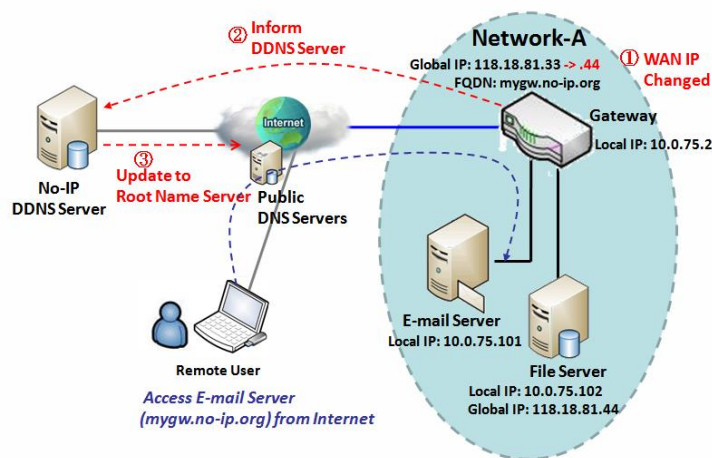
Policy Routing Information		
Item	Value setting	Description
Policy Routing Source	N/A	Policy Routing of Source. String Format.
Source IP	N/A	Policy Routing of Source IP. IPv4 Format.
Destination IP	N/A	Policy Routing of Destination IP. IPv4 Format.
Destination Port	N/A	Policy Routing of Destination Port.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

## 3.5 DNS & DDNS

How does a user access a server if your WAN IP address changes all the time? One way is to register a new domain name, and maintain your own DNS server. Another simpler way is to apply a domain name to a third-party DDNS service provider. The service can be free or charged. If you want to understand the basic concepts of DNS and Dynamic DNS, you can refer to Wikipedia<sup>5,6</sup>.

### 3.5.1 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, a user registered a domain

name to a third-party DDNS service provider (NO-IP) to use DDNS function. Once the IP address of designated WAN interface has changed, the dynamic DNS agent in the gateway will inform the DDNS server with the new IP address. The server automatically re-maps your domain name with the changed IP address. So, other hosts or remote users in the Internet world are able to link to your gateway by using your domain name regardless of the changing global IP address.

5 [http://en.wikipedia.org/wiki/Domain\\_Name\\_System](http://en.wikipedia.org/wiki/Domain_Name_System)

6 [http://en.wikipedia.org/wiki/Dynamic\\_DNS](http://en.wikipedia.org/wiki/Dynamic_DNS)

## DNS & DDNS Setting

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

The DNS & DDNS setting allows user to setup Dynamic DNS feature and DNS redirect rules.

### Setup Dynamic DNS

The gateway allows you to customize your Dynamic DNS settings.

Dynamic DNS	
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>	The box is unchecked by default	Check the <b>Enable</b> 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>	<b>DynDNS.org (Dynamic)</b> is set by default	Select your DDNS provider of Dynamic DNS. It can be <b>DynDNS.org(Dynamic)</b> , <b>DynDNS.org(Custom)</b> , <b>NO-IP.com</b> , etc...
<b>Host Name</b>	1. String format, can be any text 2. A Required setting	Your registered host name of Dynamic DNS. <b><u>Value Range:</u> 0 ~ 63 characters.</b>
<b>User Name / E-Mail</b>	1. String format, can be any text 2. A Required setting	Enter your User name or E-mail addresss of Dynamic DNS.
<b>Password / Key</b>	1. String format, can be any text 2. A Required setting	Enter your Password or Key of Dynamic DNS.
<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

## Setup DNS Redirect

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

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

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

If you enabled 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 corresponding pre-defined IP address.

Redirect Rule					
		Add	Delete		
ID	Mapping Rule	Condition	Description	Enable	Action

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

Redirect Rule

Save

Item	Setting	
Mapping Rule	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
Domain Name	1. String format, can be any text 2. A Required setting	Enter a domain name to be redirected. The traffic to specified domain name will be redirected to the following IP address. <b>Value Range:</b> at least 1 character is required; '*' for any.



<b>IP</b>	1. IPv4 format 2. A Required setting	Enter an IP Address as the target for the DNS redirect.
<b>Condition</b>	1. A 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 when the WAN connection is disconnected, or un-reachable.
<b>Description</b>	1. String format, can be any text 2. A Required setting	Enter a brief description for this rule. <b><u>Value Range:</u></b> 0 ~ 63 characters.
<b>Enable</b>	The box is unchecked by default	Click the <b>Enable</b> 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

## 3.6 QoS

The total amount of data traffic is increasing due to the higher demand of mobile applications, like Games / Chat / VoIP / P2P / Video / Web access. In order to pose new requirements for data transport, e.g. low latency, low data loss, the entire network must ensure them via a connection service guarantee.

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.

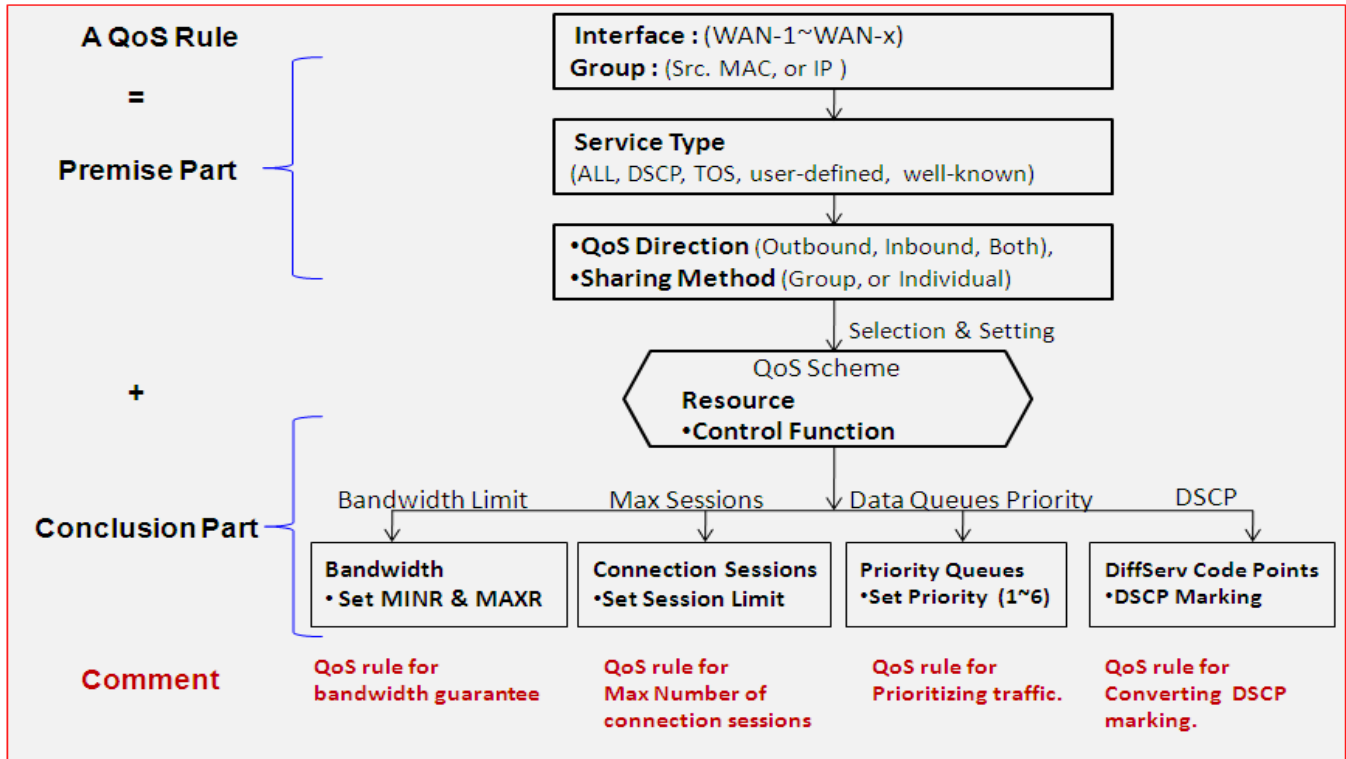
To utilize your network throughput completely, the administrator must define bandwidth control rules carefully to balance the utilization of network bandwidth for all users to access. It is indeed required that an access gateway satisfies the requirements of latency-critical applications, minimum access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

### 3.6.1 QoS Configuration

This gateway provides lots of flexible rules for you to set QoS policies. Basically, you need to know three items 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 will prioritize. Once you have this information, you can continue to learn the functions in this section in more detail.

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

When you want to add a new QoS rule or edit one that already exists, the "QoS Rule Configuration" window shows up for you to configure. 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.



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. However, 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's have 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 functions that act on target objects for specific services of packet flow is based on these resources.

For bandwidth resource, control functions include guaranteeing bandwidth and limiting bandwidth.

# AIR PACE

For priority queue resource, control function is based on 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 specific model.

## Outbound / Inbound Control

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

Two QoS rule examples are listed as 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 administrator wants to limit maximum connection sessions from some client hosts (IP 10.0.75.16~31) to 20000 to avoid resource unbalanced, he can set up this rule as 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 connection sessions totally at any time

## 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 can use the "Rule-based QoS" function to carry out this rule by defining an QoS rule as shown in above configuration. Under such 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.

## QoS Configuration Setting

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

In "QoS Configuration" page, there are some configuration windows for QoS function. They are the "Configuration" window, "System Resource Configuration" window, "QoS Rule List" window, and "QoS Rule Configuration" window.

The "Configuration" window lets 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 FBM algorithm. Second, the "System Configuration" window lets 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. The box is 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	The box is 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 the "Rule-based QoS" function. 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. Certainly, the bandwidth subscription profiles of all current users are considered in system's automatic adjusting algorithm.

## Setup 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. A Required setting. 2. Bandwidth Queue, 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	WAN-1 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. <b>Value Range:</b> For Gigabit Ethernet: 1~1024000Kbps, or 1~1000Mbps; For Fast Ethernet: 1~102400Kbps, or 1~100Mbps; For 3G/4G: 1~153600Kbps, or 1~150Mbps.</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.

## Create / Edit QoS Rules

After enabling the QoS function and configuring the system resources, you have to further specify some QoS rules for provide better service for 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 **Add** button is applied, **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
<b>Interface</b>	<ol style="list-style-type: none"> <li>1. A Required setting.</li> <li>2. <b>All WANs</b> is selected by default.</li> </ol>	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 to or leaving from the interface(s).
<b>Group</b>	<ol style="list-style-type: none"> <li>1. A Required setting.</li> <li>2. <b>Src. MAC Address</b> is selected by default.</li> </ol>	<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 if any group is pre-configured.</p> <p><b>Note:</b> The required host groups must be created in advance and corresponding QoS checkbox in the <b>Multiple Bound Services</b> field must be checked before the <b>Host Group</b> option become available. Refer to <b>Object Definition &gt; Grouping &gt; Host Grouping</b>.</p>



<b>Service</b>	1. A Required setting. 2. <b>All</b> is selected by default.	<p>Specify the service type of traffic to be applied with the QoS rule. 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. You have to 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. You have to define the port range and protocol as well.</p> <p>Select <b>Well-known Service</b> for specific application packets only. You have to select the required service from the dropdown list.</p>
<b>Resource, and Control Function</b>	A 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 you have to 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 you have to 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 you have to 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 you have to select a DSCP marking from the <b>Control Function / DSCP Marking</b> dropdown list.</p>
<b>QoS Direction</b>	1. A Required setting. 2. <b>Outbound</b> is selected by default.	<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 situation, the hosts specified in the Group field is 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 situation, the hosts specified in the Group field is 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>	1. A Required setting. 2. <b>Group Control</b> is selected by default.	<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</p>

		have his own QoS service resource as specified in the rule. <b>Group Control:</b> If <b>Group Control</b> is selected, all the group hosts share the same QoS service resource.
<b>Time Schedule</b>	1. A Required setting. 2. <b>(0) Always</b> is selected by default.	Apply <b>Time Schedule</b> to this rule; otherwise leave it as <b>(0) Always</b> . (refer to <b>Object Definition &gt; Scheduling &gt; Configuration</b> settings)
<b>Rule Enable</b>	The box is 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.

## 3.7 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 IP networking, the access gateway is the critical part of the networking system. Redundant gateways play the backup to the master gateway and will take over the data transmitting job once it finds the master gateway failed.

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

### 3.7.1 VRRP

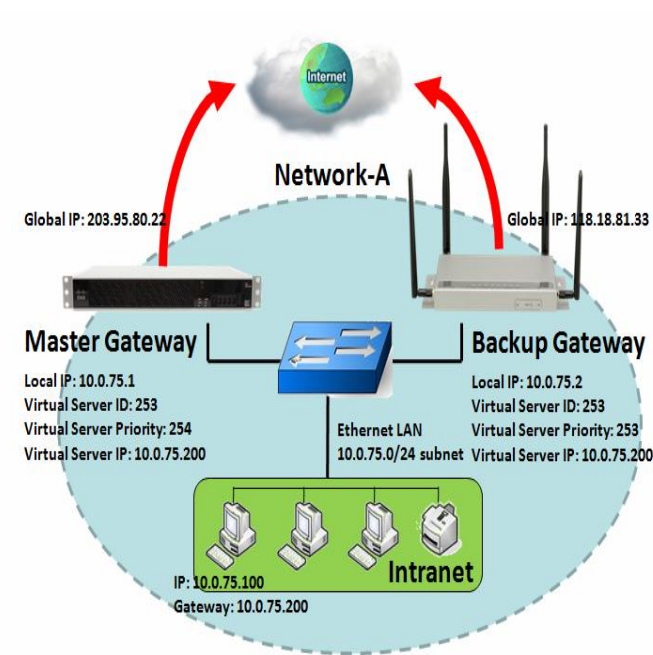
Configuration	
Item	Setting
▶ VRRP	<input type="checkbox"/> Enable
▶ Virtual Server ID	<input type="text"/> (1-255)
▶ Priority of Virtual Server	<input type="text"/> (Lowest 1 ~ 254 Highest)
▶ Virtual Server IP Address	<input type="text"/>

Virtual Router Redundancy Protocol (VRRP) is a computer 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 act as a virtual server with one unique virtual server ID and one unique virtual server IP address. But these VRRP gateways have their own priority values to serve as the sequence for backing up the master gateway.

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



again.

As shown in the diagram, the Master Gateway and Backup Gateway are redundant gateway group of Network-A. The subnet of network-A is 10.0.75.0/24. Master gateway has LAN IP 10.0.75.1 and WAN IP 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

VRRP Setting

The Virtual Router Redundancy Protocol (VRRP) setting allows user to assign available Internet Protocol (IP) routers to participating hosts automatically.

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	The box is unchecked by	Check the <b>Enable</b> box to activate this VRRP function.

	default.	
<b>Virtual Server ID</b>	1. Numeric String Format 2. A Required setting	Specify the Virtual Server ID on VRRP of the gateway. <b><u>Value Range:</u></b> 1 ~ 255.
<b>Priority of Virtual Server</b>	1. Numeric String Format 2. A Required setting	Specify the Priority of Virtual Server on VRRP of the gateway. <b><u>Value Range:</u></b> 1 ~ 254, and 254 is the highest priority.
<b>Virtual Server IP Address</b>	1. IPv4 Format 2. A 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 4 Object Definition

### 4.1 Scheduling

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

#### 4.1.1 Scheduling Configuration

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

Time Schedule List <span>Add</span> <span>Delete</span> <span>▲</span> <span>✕</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 **Add** button is applied, 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 rule name
<b>Rule Policy</b>	Default Inactivate	Inactivate/activate the function been applied to in the time period below

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

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

## 4.2 Grouping

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

### 4.2.1 Host Grouping

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

The Host Grouping function allows user to make host group for some services, such as QoS, Firewall, and Communication Bus. The supported service types may differ depending on specific product.

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

When **Add** button is applied, **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
▶ Group	<input type="checkbox"/> Enable

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



		<p><b>to Join.</b></p> <p>Note: The available Group Type can be different for the purchased 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 add at a time, so you have to add the members to the group one by one.</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	<p>Binding the services that the host group can be applied. If you enable the <b>Firewall</b>, the produced group can be used in firewall service. Same as by enable <b>QoS</b>, or other available service types.</p> <p><b>Note:</b> The supported service type can be different for the purchased product.</p>
<b>Group</b>	The box is unchecked by default	Check the <b>Enable</b> checkbox to activate the host group rule. So that the group can be bound to 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

## 4.3 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 <span>Add</span> <span>Delete</span> <span>▲</span>						
ID	Server Name	Server Type	Server IP/FQDN	Server Port	Server Enable	Actions

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

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

External Server Configuration		
Item	Value setting	Description
<b>Sever Name</b>	1. String format, can be any text	Enter a server name. Enter a name that is easy to understand.
	2. A Required setting	
<b>Server Type</b>	A Required setting	Specify the Server Type of the external server, and enter the required settings for the accessing the server.
		<b>Email Server</b> (A 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> (A 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> (A 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> (A 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> (A 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> (A Required setting):

		<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> (A 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> (A 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><b>Protocol</b> (Select <b>FTP</b> or <b>SFTP</b>)</p> <p><b>Encryprion</b> (Select <b>Plain</b>, <b>Explicit FTPS</b> or <b>Implicit FTPS</b>)</p> <p><b>Transfer mode</b> (Select <b>Passive</b> or <b>Active</b>)</p>
<b>Server IP/FQDN</b>	A Required setting	Specify the IP address or FQDN used for the external server.
<b>Server Port</b>	A 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, 1823 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 3990, 4990 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><b>Value Range:</b> 1 ~ 65535.</p>
<b>Account Port</b>	<p>1. A 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><b>Value Range:</b> 1 ~ 65535.</p>
<b>Server</b>	The box is checked by default	Click <b>Enable to</b> 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.

## 4.4 Certificate

In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are genuine. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner<sup>7</sup>.

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.

### 4.4.1 Configuration

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

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

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

---

<sup>7</sup> [http://en.wikipedia.org/wiki/Public\\_key\\_certificate](http://en.wikipedia.org/wiki/Public_key_certificate).

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"/> E-mail : <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, can be any text 2. A Required setting	Enter a Root CA Certificate name. It will be a certificate file name
<b>Key</b>	A Required setting	This field is to specify the key attribute of certificate. <b>Key Type</b> to set public-key cryptosystems. It only supports RSA now. <b>Key Length</b> to set s the size measured in bits of the key used in a cryptographic algorithm. <b>Digest Algorithm</b> to set identifier in the signature algorithm identifier of certificates
<b>Subject Name</b>	A 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 style.
<b>Validity Period</b>	A Required setting	This field is to specify the validity period of certificate.

## Setup SCEP

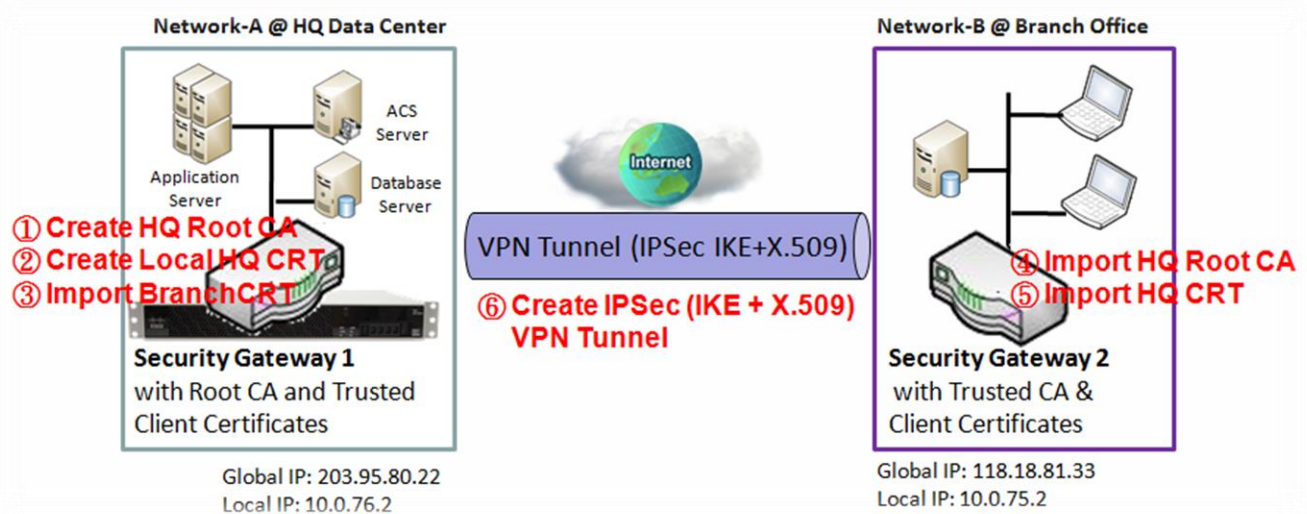
SCEP Configuration	
Item	Setting
▶ SCEP	<input type="checkbox"/> Enable
▶ Automatically re-enroll aging certificates	<input type="checkbox"/> Enable

SCEP Configuration		
Item	Value setting	Description
<b>SCEP</b>	The box is unchecked by default	Check the <b>Enable</b> box to activate SCEP function.
<b>Automatically re-enroll aging certificates</b>	The box is unchecked by default	When <b>SCEP</b> is activated, check the <b>Enable</b> box to activate this function. It will be automatically check which certificate is aging. If certificate is aging, it will activate SCEP function to re-enroll automatically.
<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

## 4.4.2 My Certificate

My Certificate includes a Local Certificate List. The 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 their identity during 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 the Gateway 1 into the Gateway 2 as the trusted ones. (Please also refer to following two sub-sections)

An IPSec VPN tunnel is 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.



# AIR PACE

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

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

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

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

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

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

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

Configuration Path	[IPSec]-[Authentication]
--------------------	--------------------------

# AIR PACE

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

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

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

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

<b>Configuration Path</b>	[My Certificate]-[Local Certificate Configuration]
<b>Name</b>	<b>BranchCRT</b> Self-signed: <input 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>Tainan</b> Organization(O): <b>ETHWERWANBranch</b> Organization Unit(OU): <b>BranchRD</b> Common Name(CN): <b>BranchCRT</b> E-mail: <b>branchcrt@etherwan.com.tw</b>

<b>Configuration Path</b>	[IPSec]-[Configuration]
<b>IPSec</b>	■ <b>Enable</b>

<b>Configuration Path</b>	[IPSec]-[Tunnel Configuration]
<b>Tunnel</b>	■ <b>Enable</b>
<b>Tunnel Name</b>	<b>s2s-102</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>10.0.75.0</b>
<b>Local Netmask</b>	<b>255.255.255.0</b>
<b>Full Tunnel</b>	<b>Disable</b>
<b>Remote Subnet</b>	<b>10.0.76.0</b>
<b>Remote Netmask</b>	<b>255.255.255.0</b>
<b>Remote Gateway</b>	<b>203.95.80.22</b>

# AIR PACE

<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. Gateway 2 Imports the certificates of the root CA and HQCRT into the "Trusted CA Certificate List" and "Trusted Client Certificate List".

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.

## My Certificate Setting

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

The My Certificate setting allows user to create local certificates. On the "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 fill in 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 **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>t-IDG761AM-JH.crt</span> CA Encryption Certificate: <span>--- Option ---</span> (Optional) CA Identifier: <input type="text"/> (Optional)

Local Certificate Configuration		
Item	Value setting	Description
<b>Name</b>	1. String format, can be any text 2. A 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>	A 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>	A 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 setting only.
<b>Extra Attributes</b>	A 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>	A Required setting	This field is to specify the information of SCEP. If user wants to generate a certificate signing request (CSR) and then signed by SCEP server online, user can check the <b>Enable</b> box.  Select a <b>SCEP Server</b> to identify the SCEP server for use. The server detailed information could 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, and the settings are the same as those defined in <b>Section 3.4 External Server</b> .  Select a <b>CA Certificate</b> to identify which certificate could be accepted by SCEP server for authentication. It could be generated in Trusted Certificates.  Select an optional <b>CA Encryption Certificate</b> , if it is required, to identify which certificate could be accepted by SCEP server for encryption data information. It could be generated in Trusted Certificates.  Fill in optional <b>CA Identifier</b> to identify which CA could 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.

# AIR PACE

When **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.

Import

Apply

Cancel

瀏覽...

未選擇檔案。

PEM Encoded

Apply

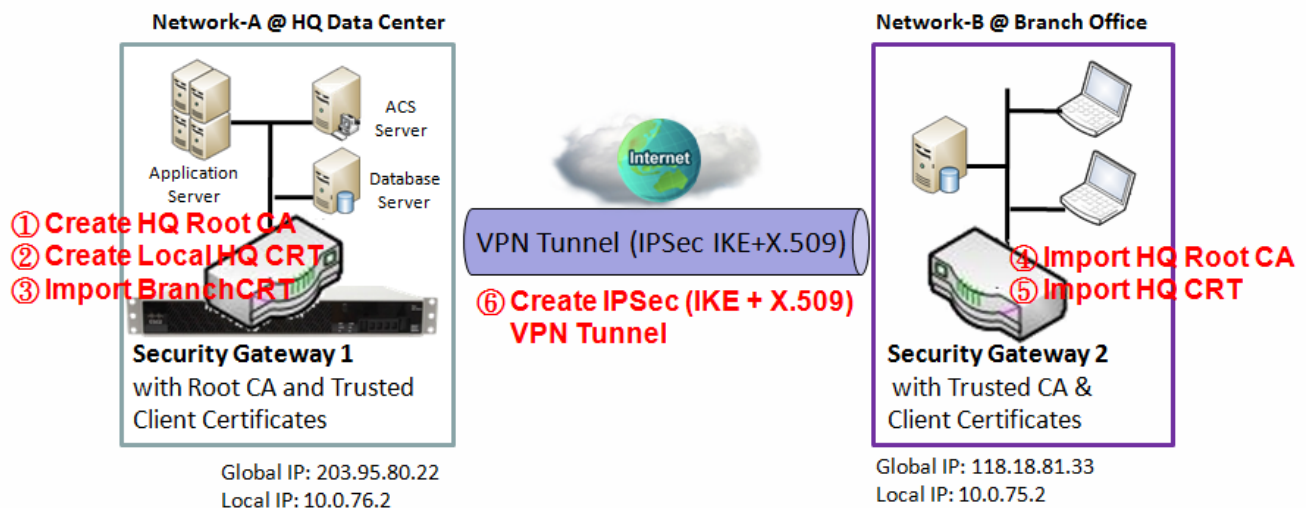
Cancel

Import Item	Value setting	Description
Import	A 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, can be any text 2. A Required setting	This is an alternative approach to importing 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.

## 4.4.3 Trusted Certificate

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

### Self-signed Certificate Usage Scenario



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

When the enterprise gateway owns the root CA and VPN tunneling function, it can generate its own local certificates by being signed by itself. It can also import 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 the one 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 the Gateway 1 sign it to be 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 the Gateway 2 as the trusted ones. (Refer to "My Certificate" and "Issue Certificate" sections).

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

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

# AIR PACE

For Network-A at HQ

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 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

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 above diagram. The configuration example must be combined with the ones in "My Certificate" and "Issued Certificate" sections to complete the setup for the whole user scenario.

<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 the one described in "My Certificate" section)

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

Gateway 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.



## AIR PACE

It imports the obtained BranchCRT certificate (the derived BranchCSR certificate after Gateway 1's root CA signature) into the "Trusted Client Certificate List" of Gateway 1 and the "Local Certificate List" of 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.

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 **Import** button is applied, a **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 Apply Cancel

瀏覽... 未選擇檔案。


Trusted CA Certificate Import from a PEM Apply Cancel

Trusted CA Certificate List		
Item	Value setting	Description
Import from a File	A 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, can be any text 2. A 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.

# AIR PACE

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

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

 **Get CA Configuration**

Item	Setting
▶ SCEP Server	<div>--- Option --- ▼ <span>Add Object</span></div>
▶ CA Identifier	<div><input type="text"/> (Optional)</div>

Get CA Configuration		
Item	Value setting	Description
<b>SCEP Server</b>	A Required setting	Select a <b>SCEP Server</b> to identify the SCEP server for use. The server detailed information could 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.
<b>CA Identifier</b>	1. String format, can be any text	Fill in optional <b>CA Identifier</b> to identify which CA could be used for signing certificates.
<b>Save</b>	N/A	Click <b>Save</b> to save the settings.
<b>Close</b>	N/A	Click the <b>Close</b> button to return to the Trusted Certificates page.

## Import Trusted Client Certificate

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

When **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

ApplyCancel

瀏覽...

未選擇檔案。

Trusted Client Certificate Import from a PEM

ApplyCancel

Trusted Client Certificate List		
Item	Value setting	Description
Import from a File	A 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.
Import from a PEM	1. String format, can be any text 2. A Required setting	This is an alternative approach to importing 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 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.

Import Trusted Client Key

Trusted Client Key List

ImportDelete

ID	Name	Actions
----	------	---------

When **Import** button is applied, a **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

ApplyCancel

瀏覽...

未選擇檔案。

Trusted Client Key Import from a PEM

ApplyCancel

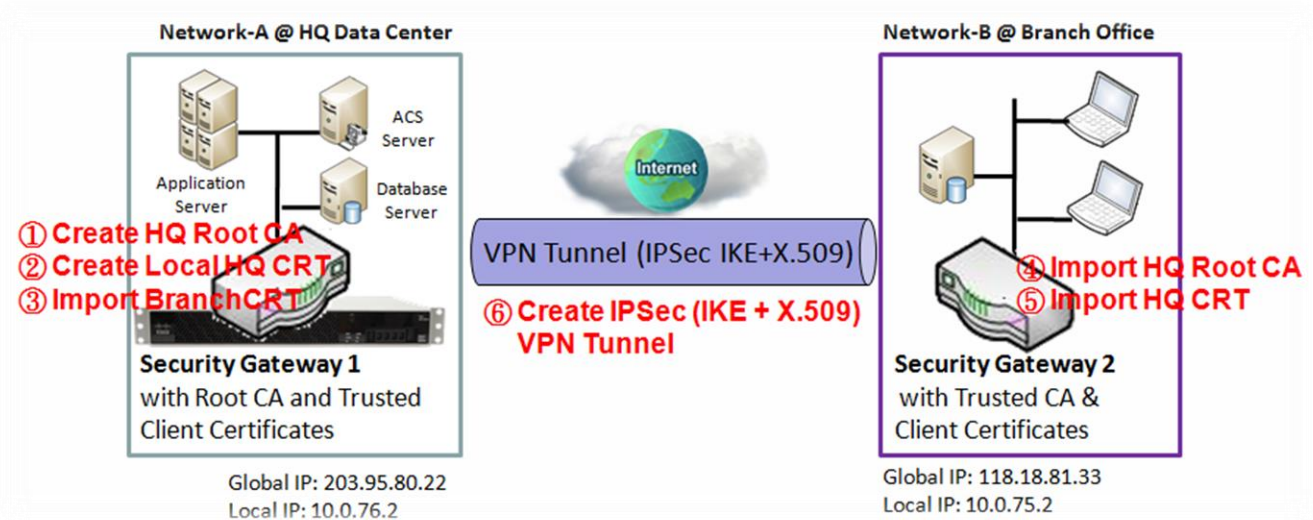
Trusted Client Key List		
Item	Value setting	Description
Import from a File	A Required setting	Select a certificate key file from user's computer, and click the <b>Apply</b> button to import the specified key file to the gateway.
Import from a PEM	1. String format, can be any text 2. A Required setting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

## 4.4.4 Issue Certificate

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

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

### Self-signed Certificate Usage Scenario



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

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

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

Gateway 1 generates the root CA and a local certificate (HQCRT) signed by itself. 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 to be 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 the Gateway 1 into the Gateway 2 as trusted ones. (Refer to "My Certificate" and "Trusted Certificate" sections).

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

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

For Network-A at HQ

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 above diagram. The configuration example must be combined with the ones in "My Certificate" and "Trusted Certificate" sections to complete the setup for whole user scenario.

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

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

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

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

Gateway 1 generates the root CA and a local certificate (HQCRT) that is signed by itself. 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). Take the CSR to be signed by the root CA of the Gateway 1 and obtain the BranchCRT certificate (you need rename it). Import the certificate into the "Trusted Client Certificate List" of the Gateway 1 and the "Local Certificate List" of the Gateway 2.

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

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

## Issue Certificate Setting

# AIR PACE

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

The screenshot displays the 'Issue Certificate' configuration page. It features two tabs for importing a Certificate Signing Request (CSR). The first tab, 'Certificate Signing Request (CSR) Import from a File', is selected and shows a 'Choose File' button and the text 'No file chosen'. The second tab, 'Certificate Signing Request (CSR) Import from a PEM', is currently inactive. Both tabs include a 'Sign' button. The interface is clean with a light blue header and a white main area.

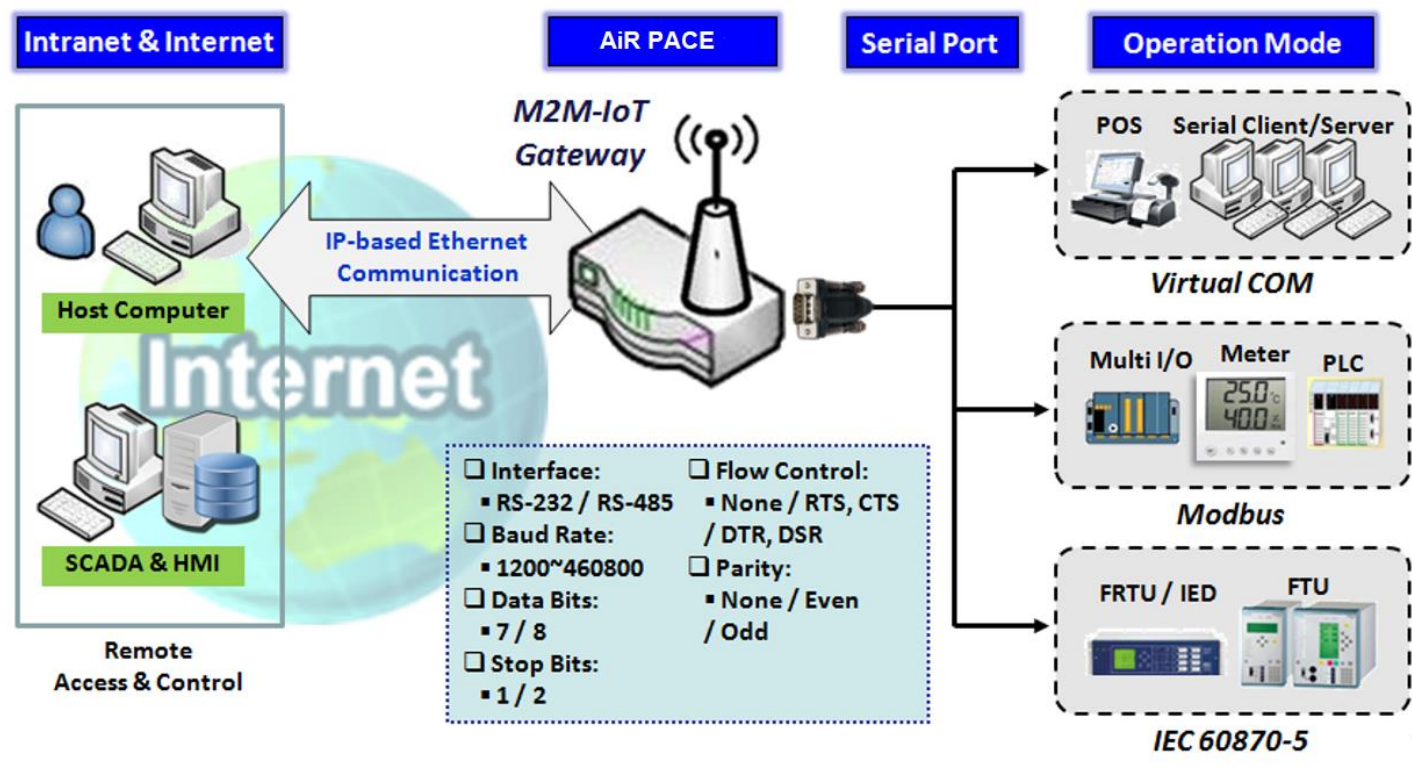
Certificate Signing Request (CSR) Import from a File		
Item	Value setting	Description
Certificate Signing Request (CSR) Import from a File	A Required setting	Select a certificate signing request file you're your computer for importing to the gateway.
Certificate Signing Request (CSR) Import from a PEM	1. String format, can be any text 2. A 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 sign and issue the imported certificate by root CA.



# Chapter 5 Field Communication

## 5.1 Bus & Protocol

The gateway may be equipped with one or more serial port(s) for various serial communication use through connecting the RS-232 or RS-485 serial devices to an IP-based Ethernet LAN. These communication protocols make user access serial devices anywhere over a local LAN or the Internet easily. They can be "Virtual COM" and "Modbus".



### 5.1.1 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 to quickly switch from one communication protocol to another for the serial port. The number of ports and type of the supported protocols may differ depending on the purchased gateway model.

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

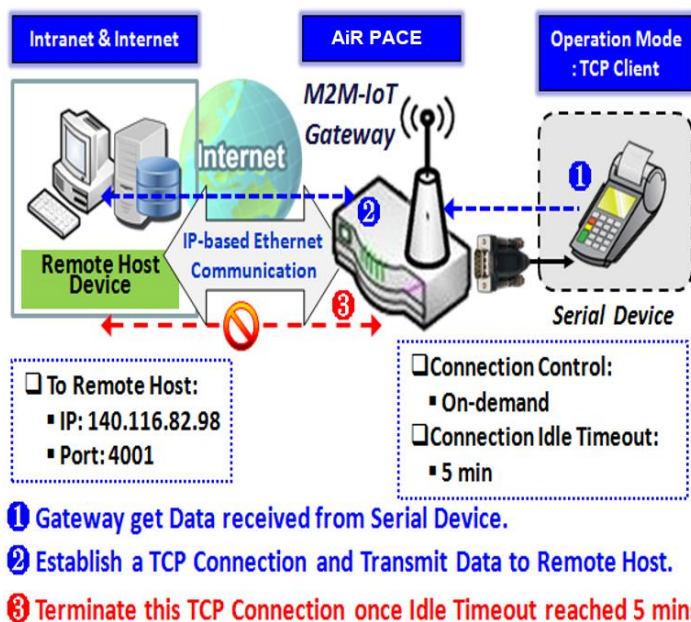
## 5.1.2 Virtual COM

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

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

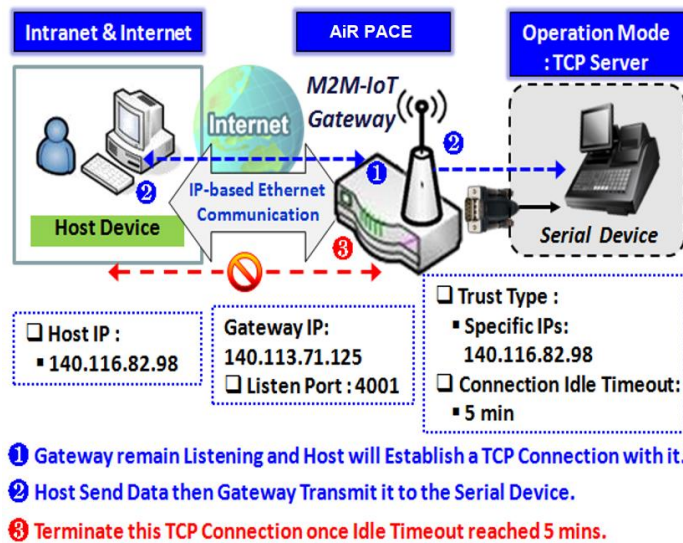
The Virtual COM setting screen enables user to connect a Virtual COM port based device to the Internet. It allows user to access serial data remotely. There are Disable, TCP Client, TCP Server, UDP, and RFC-2217 modes for remote accessing the connected serial device. These operation modes are illustrated as below.

### TCP Client Mode



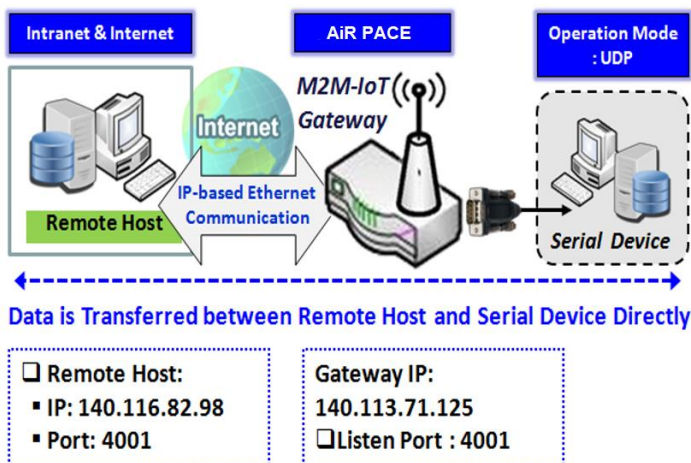
When the administrator expects the gateway to actively establish a TCP connection to a pre-defined host computer when serial data arrives, the operation mode for the "Virtual COM" function is required to be "TCP Client" and when the connection control of virtual COM is "On-demand", once the gateway receives data from the connected serial device, it will establish a TCP connection to transfer the received serial data to the remote host. Additionally, 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.

## TCP Server Mode



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

## UDP Mode



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

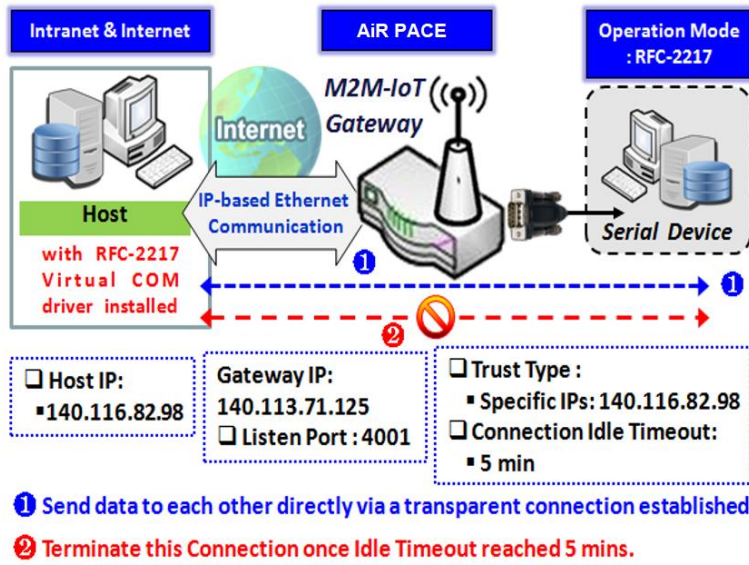
The remote host computer can directly send UDP data to the serial device via the gateway, and also receive UDP data from the serial device via the gateway at the same time. The gateway supports up to 4 legal hosts

to connect simultaneously to the serial device via the gateway.



# AIR PACE

## 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 used to install in the host computer. The driver establishes a transparent connection between host and serial device by mapping the IP:Port of the gateway's serial port to a virtual local COM

port on the host computer.

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

## Virtual COM Setting

The Virtual COM setting screen enables user to connect a Virtual COM port based device to the Internet. It allows user to access serial data remotely. There are Disable, TCP Client, TCP Server, UDP, and RFC-2217 modes for remote accessing the connected serial device. By default, it is configured in Disable mode.

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

After that, go to **Field Communication > Bus & Protocol > Virtual COM** tab for detailed configuration of Virtual COM setting.

### Enable TCP Client Mode

Configure the gateway as the TCP (Transmission Control Protocol) Client. In TCP Client mode, 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. Full time connection with the TCP server can also be enabled.

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
<b>Operation Mode</b>	A Required setting	Select <b>TCP Client</b> .
<b>Connection Control</b>	<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 when idle timeout is reached.
<b>Connection Idle Timeout</b>	1. 0 is set by default 2. Range 0 to 3600 sec.	Enter the idle timeout in minutes. The idle timeout is used to disconnect the TCP connection when idle time elapsed. Idle timeout is only available when <b>On-Demand</b> is selected in the <b>Connection Control</b> field. <b>Value Range:</b> 0 ~ 3600 seconds.
<b>Alive Check Timeout</b>	1. 0 is set by default 2. Range 0 to 3600 sec.	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. <b>Value Range:</b> 0 ~ 3600 seconds.
<b>Enable</b>	The box is 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 the <b>Save</b> button to save the configuration

## 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. An optional filled 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. An optional filled 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. An optional filled 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. An optional filled 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"/>	<button>Edit</button>
2		4001	SPort-0	<input type="checkbox"/>	<button>Edit</button>
3		4001	SPort-0	<input type="checkbox"/>	<button>Edit</button>
4		4001	SPort-0	<input type="checkbox"/>	<button>Edit</button>

Specify TCP Server Window		
Item	Value setting	Description
<b>To Remote Host</b>	A 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. A Required setting 2. Default value is 4001	Enter the TCP port number. This is the listen 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>	The box is 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

## Enable TCP Server Mode

Configure the gateway as the TCP (Transmission Control Protocol) Server. The TCP Server waits for connections to be initiated by a remote TCP client device to receive serial data. The setting allows user to specify specific TCP clients or allow any to send serial data for serial data transmission bandwidth control and access control. The TCP Server supports up to 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	A Required setting	Select <b>TCP Server</b> mode.
Listen Port	4001 is set by default	Indicate the listening port of TCP connection. <b>Value Range:</b> 1 ~ 65535.
Trust Type	Allow All 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. 128 connections 2. 1 is set by default	Set the maximum number of concurrent TCP connections. Up to 128 simultaneous TCP connections can be established. <b>Value Range:</b> 1 ~ 128.
Connection Idle Timeout	1. 0 is set by default 2. Range 0 to 3600 sec.	Enter the idle timeout in minutes. The idle timeout is used to disconnect the TCP connection when idle time elapsed . Idle timeout is only available when <b>On-Demand</b> is selected in the <b>Connection Control</b> field. <b>Value Range:</b> 0 ~ 3600 seconds.
Alive Check Timeout	1. 0 is set by default 2. Range 0 to 3600 sec.	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. <b>Value Range:</b> 0 ~ 3600 seconds.
Enable	The box is 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.



## 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
<b>Host</b>	A Required setting	Enter the IP address range of allowed TCP clients.
<b>Serial Port</b>	The box is unchecked by default	Check the box to specify the rule for selected Serial Port.
<b>Definition Enable</b>	The box is 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

# AIR PACE

## 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)

☐

Edit

Enable UDP Mode Window		
Item	Value setting	Description
Operation Mode	A Required setting	Select <b>UDP</b> mode.
Listen Port	4001 is set by default	Indicate the listening port of UDP connection. <b>Value Range:</b> 1 ~ 65535
Enable	The box is 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

## 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

☐

Edit

2

4001

SPort-0

☐

Edit

3

4001

SPort-0

☐

Edit

4

4001

SPort-0

☐

Edit

Specify Remote UDP hosts Window		
Item	Value setting	Description
Host	A Required setting	Press <b>Edit</b> button to enter IP address range of remote UDP hosts.
Remote Port	4001 is set by default	Indicate the UDP port of peer UDP hosts. <b>Value Range:</b> 1 ~ 65535
Serial Port	SPort-0 is set by default	Apply the UDP hosts for a selected serial port. Up to 4 UDP servers can be configured at the same time for each serial port.
Definition Enable	The box is unchecked by default	Check the <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 RFC-2217 Mode

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

Operation Mode Definition for each Serial Port									
Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	RFC-2217 ▼	4001 (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	A 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	<b>Allow All</b> 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	1. 0 is set by default 2. Range 0 to 3600 sec.	Enter the idle timeout in minutes. The idle timeout is used to disconnect the TCP connection when idle time elapsed . Idle timeout is only available when <b>On-Demand</b> is selected in the <b>Connection Control</b> field. <b>Value Range:</b> 0 ~ 3600 seconds.
Alive Check Timeout	1. 0 is set by default 2. Range 0 to 3600 sec.	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. <b>Value Range:</b> 0 ~ 3600 seconds.
Enable	The box is 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

## 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
<b>Host</b>	A Required setting	Enter the IP address range of allowed clients.
<b>Serial Port</b>	The box is unchecked by default	Check the box to specify the rule for selected Serial Port.
<b>Definition Enable</b>	The box is 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

## 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	Enable
SPort-0	<div>External</div> <div>Download</div> <div>Enable</div>	<div>IP</div> <div>TX Port 0 RX Port 0</div> <div>Enable</div>	<div>--- Option ---</div> <div>Add Object</div> <div>Enable</div>	HEX	3	<input type="checkbox"/>

COM Logging Configuration Window		
Item	Value setting	Description
<b>Storage Device</b>	The box is 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>	The box is 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. <b>Value Range:</b> 1 ~ 65535, and 0 for disabled by default.
<b>Upload Server</b>	The box is unchecked by default.	Check the <b>Enable</b> box and select a pre-defined FTP server from the drop down 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. <b>Value Range:</b> 1 ~ 30 days.
<b>Enable</b>	The box is unchecked by default.	Check the <b>Enable</b> 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

5.1.3 Modbus

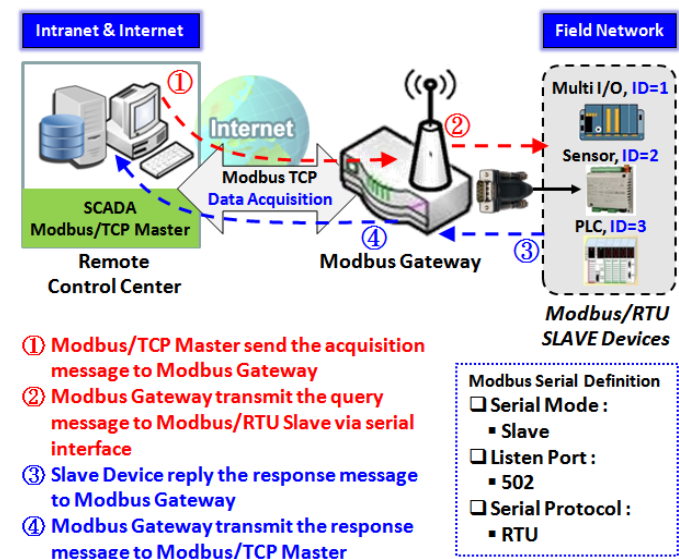
Modbus is one of the most popular automation protocols in the world, supporting traditional RS-232/422/485 devices and recently developed Ethernet devices. Many industrial devices, such as PLCs, DCSs, HMIs, instruments, and smart meters, use Modbus protocol as the communication standard. It is used to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

However, the Ethernet-based Modbus protocol is 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	9600	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

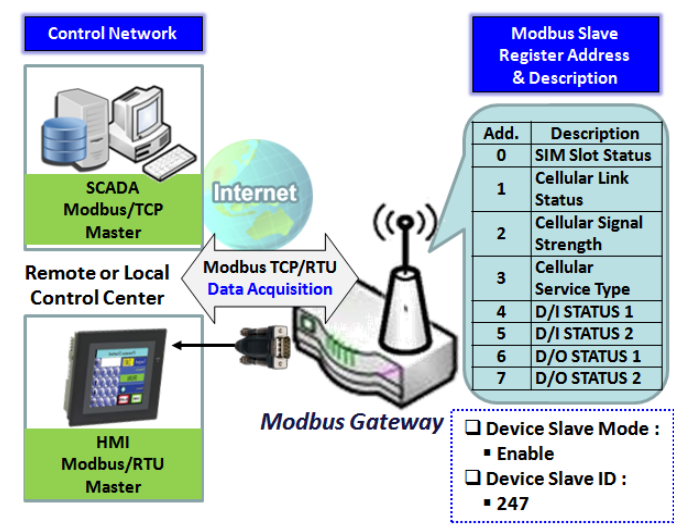


The IoT Gateway serves as a Modbus gateway to communicate with the Modbus TCP Master, the SCADA Server, located at remote control center for Modbus device accessing.

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

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

Modbus Slave Scenario



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

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

## Modbus 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 the Modbus settings in this section are completed, make sure to select Modbus Operation Mode on the Port Configuration screen to enable Modbus communication on the serial port.

### 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 checked="" type="checkbox"/>	Edit

Modbus Gateway Definition		
Item	Value setting	Description
<b>Serial Port</b>	N/A	It displays the name of the serial port used. E.g. SPort-0. The number of serial ports depends on the specific model.
<b>Gateway Mode</b>	<b>Disable</b> is set by default	Specify the Modbus gateway mode for the selected serial port. It can be <b>Disable</b> , <b>Serial as Slave</b> or <b>Serial as Master</b> . A serial port can be attached with one Modbus Master, or daisy-chained a group of Modbus Slave devices.  <b>Disable:</b> Select this to disable the respective Modbus gateway function for the selected serial port. <b>Serial as Slave:</b> Select this when the attached serial device(s) are all Modbus Slave devices. <b>Serial as Master:</b> Select this when the attached serial device is a Modbus Master device.
<b>Device Slave Mode</b>	<b>Disable</b> is set 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. So that, it can function as a Modbus Slave device, and can be accessed with legacy Modbus Function Code from a SCADA management system. Supported Modbus commands are listed in the following Table.  <b>Value Range:</b> 1 ~ 247.
<b>Listen Port</b>	1. <b>502</b> is set by default 2. Range 1 to 65535	Specify the Listen Port number if Slave device(s) is attached to the selected serial port. This setting is not used if a Master device is attached. <b>Value Range:</b> 1 ~ 65535. Note: Use different port number among the serial ports for the product with



		multiple serial ports.
<b>Serial Protocol</b>	<b>RTU</b> 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> .
<b>Enable</b>	N/A	It 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> .

## Specify Gateway Configuration

Gateway Mode Configuration for SPort-0

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

Gateway Mode Configuration for SPort-n		
Item	Value setting	Description
<b>Response Timeout</b>	<b>1000 ms</b> is set by default	This sets the response timeout of the slave after master request sent. If the slave does not response within the specified time, data will be discarded. This applies to the serially attached Master sent request over to the remote Slave or requests send from the remote Master sent to the serially attached Slave. <b>Value Range:</b> 1 ~ 65535.
<b>Timeout Retries</b>	<b>0</b> 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 retries to send the request in a number of specified times. Once the retries are exhausted, the gateway will send a Modbus error message to the Master. However, if the 0Bh exception box is checked (see below), a 0Bh hex code based-error message will be sent instead. <b>Value Range:</b> 0 ~ 5.
<b>0Bh Exception</b>	The box is 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 does not respond within the timeout interval.

<b>Tx Delay</b>	The box is unchecked by default.	Check the <b>Enable</b> box to activate to the minimum amount of time after receiving a response before the next message can be sent out. When Tx Delay is enabled the Gateway 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.
-----------------	----------------------------------	---

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

The following Modbus TCP Configuration items allow user to set up the TCP connection settings so that the remote Modbus Master can access to the Modbus gateway. Additionally, 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 elapsed, the TCP session will be terminated automatically. <b>Value Range:</b> 1 ~ 65535.
<b>Maximum TCP Connections</b>	1. 4 is set by default 2. Range 1 to 4	Enter the allowed maximum simultaneous TCP connections. <b>Value Range:</b> 1 ~ 4.
<b>TCP Keep-alive</b>	The box is 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 has to 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 checked="" type="checkbox"/>	<a href="#">Edit</a>
	2		<input type="checkbox"/>	<a href="#">Edit</a>
	3		<input type="checkbox"/>	<a href="#">Edit</a>
	4		<input type="checkbox"/>	<a href="#">Edit</a>

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

		<p>to access the attached Slave(s).</p> <p>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).</p> <p>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 creation through the Add Rule shortcut button. Settings done through the Add Rule button will also appear in the Host grouping setting screen.</p> <p>Then check <b>Enable</b> box to enable this rule.</p>
<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 in the 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"/>	<b>Edit</b>
	▶ Modbus Priority 2		<input type="checkbox"/>	<b>Edit</b>
	▶ Modbus Priority 3		<input type="checkbox"/>	<b>Edit</b>
	▶ Modbus Priority 4		<input type="checkbox"/>	<b>Edit</b>

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 consequently. So that, the buffered Master requests can further be configured to prioritize request queue to transmit to Slave based on Master's IP address if requests are coming from remote Master, or based on remote Slave ID if requests are coming from serially attached Master, or based on Function Code.
<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	User can specify a Modbus identity with <b>IP Address</b> , <b>Slave ID</b> , or <b>Function Code</b> . The buffered Modbus message that matched the specified identity will be handled with given priority. The Modbus Master requests can be buffered to a certain priority queue according to the Master's IP address if requests are coming from remote Master, or the remote Slave's device ID if requests are coming from serially attached Master, or the specific Function Code that issued by Master.
<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.

## Specify Modbus TCP Slave device(s)

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

Modbus TCP Slave List for SPort-0 <span>Add</span> <span>Delete</span> <span>▲</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). <b><u>Value Range: 1 ~ 65535.</u></b>
<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 specify the Slave IP and Port, for accessing those Remote Modbus RTU Slave(s) located behind another Modbus Gateway, user has to specify the Modus ID range of the Modbus RTU Slave(s). <b><u>Value Range: 1 ~ 247.</u></b>
<b>Enable</b>	It is 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.

## Supported Function Code for Integrated Modbus Slave

This setting can set up the Gateway as a standalone Modbus Slave Device. A 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

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
151	DO_STATUS_1	R/W	0: OFF, 1: ON

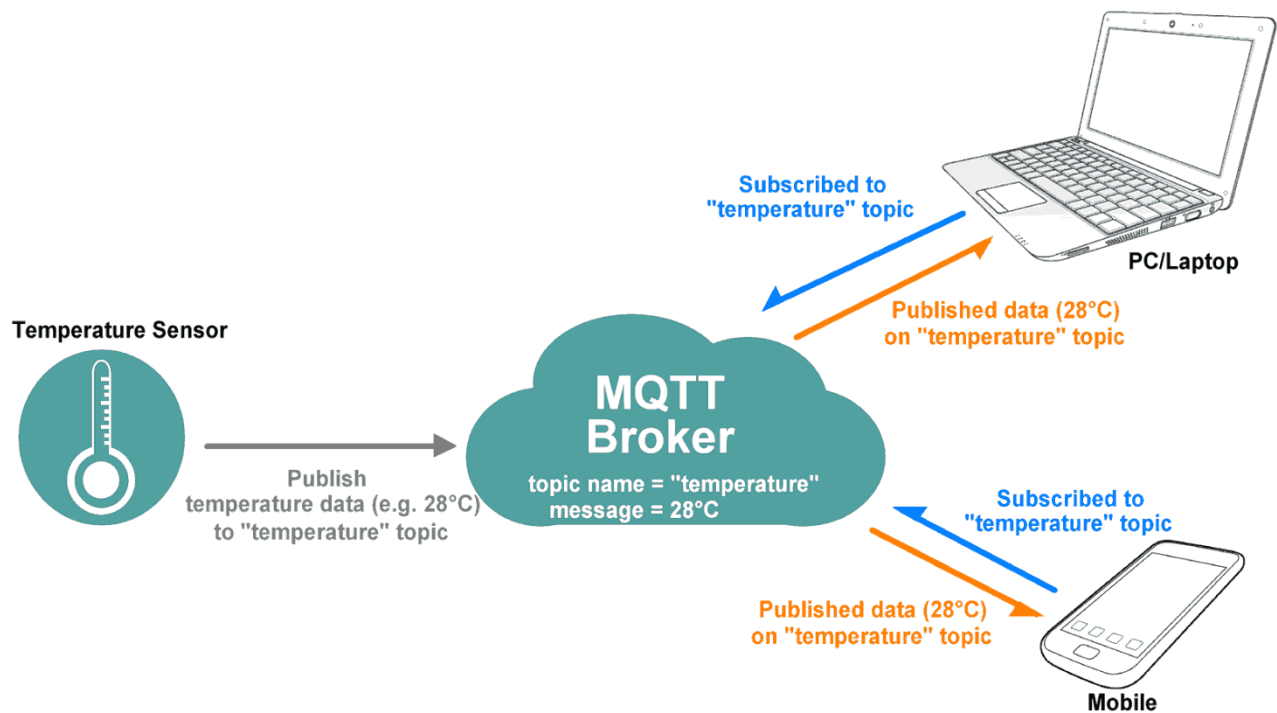
Register Address	Register Name	R / W	Register Range / Description
152	DI_STATUS_2	R	0: OFF, 1: ON
153	DO_STATUS_2	R/W	0: OFF, 1: ON
154	DI_STATUS_3	R	0: OFF, 1: ON
155	DO_STATUS_3	R/W	0: OFF, 1: ON
156	DI_STATUS_4	R	0: OFF, 1: ON
157	DO_STATUS_4	R/W	0: OFF, 1: ON
201	Serial Port-0 Interface	R	1: RS-232, 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
9999	System_Reboot	W	Set 1 for System reboot.

## 5.2 Data Interchange

### 5.2.1 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's 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. <sup>8</sup>

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. <sup>9</sup>



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.

<sup>8</sup> <https://en.wikipedia.org/wiki/MQTT>

<sup>9</sup> <https://randomnerdtutorials.com/what-is-mqtt-and-how-it-works/>



# AIR PACE

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.

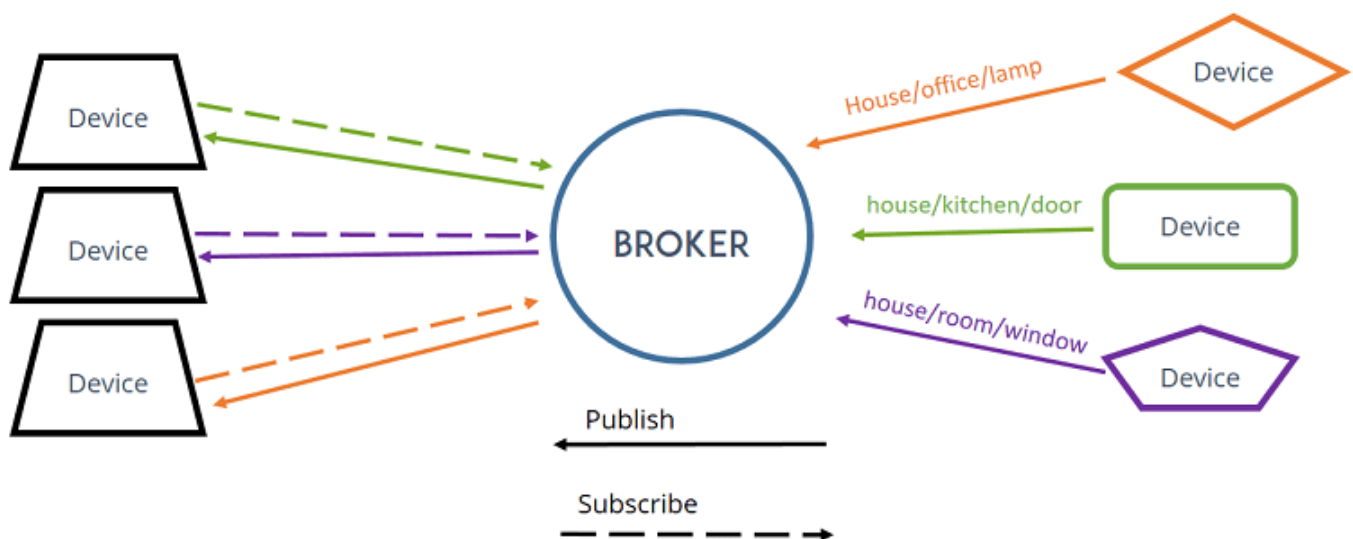
In MQTT there are a few basic concepts that you need to understand:

## 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.



## 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.

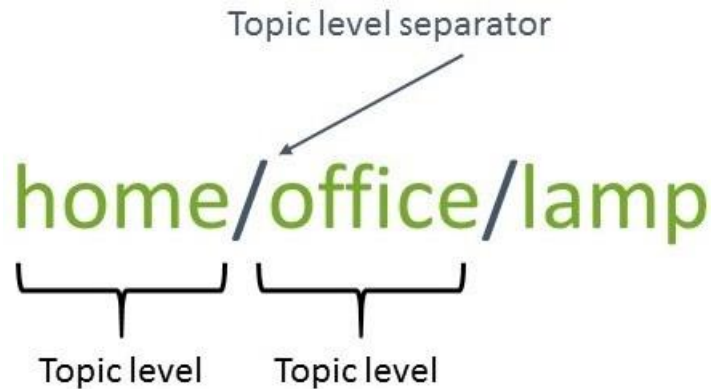
## MQTT – Topics

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.

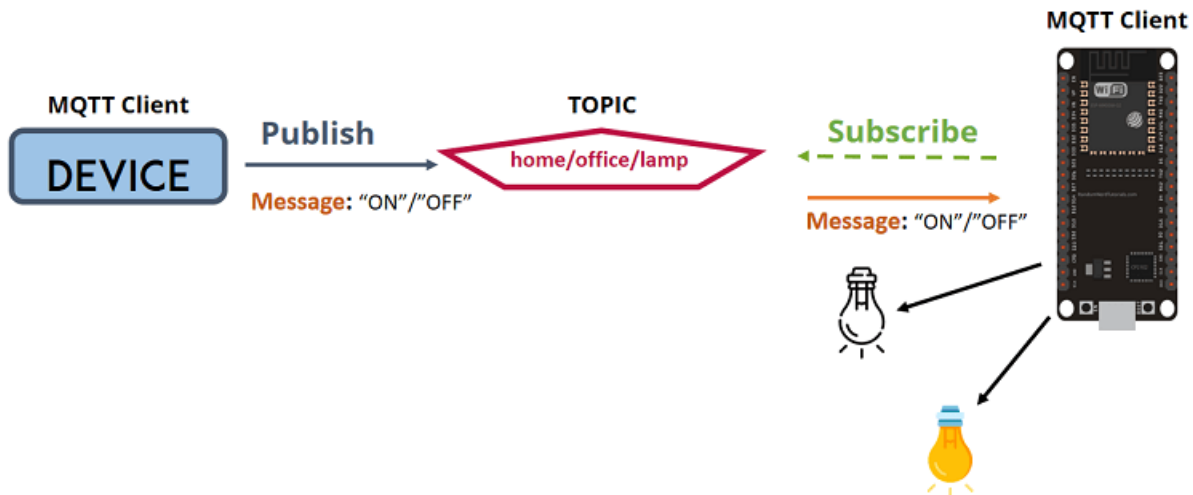
# AIR PACE

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



**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 published "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 similar topics at the same time easily.

`'+'` is single level wildcard; A `'+'` characters 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

# AIR PACE

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 scanrio.

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

## Play as a 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	The box is unchecked by default.	Check the box to activate the MQTT Broker function.
Listening Port	1. An Optional setting. 2. <b>1883</b> 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 is 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.
Security	1. An Optional setting. 2. <b>None</b> 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 listen port will be changed to <b>8883</b> accordingly by default.
Certificate	1. An Optional setting. 2. <b>None</b> is set by default	Select <b>CA File</b> / <b>CERT File</b> / <b>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.
Authentication	1. An Optional setting. 2. The box is unchecked by default.	Check the box if user (account) authentication is required for subscribing to the MQTT messages from the MQTT Broker. With the box checked, you can define up to five user accounts for permitted subscribers.
Save	N/A	Click the <b>Save</b> button to save the settings.

## Create/Edit User List

**User List**
Add
Delete
⬆

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

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

**User List Configuration**
Save
Undo
⬆
✕

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

Scheme Configuration		
Item	Value setting	Description
<b>Username</b>	A Required setting.	Specify a name as the identifier of the MQTT subscriber. <b><u>Value Range:</u></b> 1 ~ 32 characters.
<b>Password</b>	A Required setting.	Specify a password for the user account. <b><u>Value Range:</u></b> 1 ~ 32 characters.
<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.

# AIR PACE

## 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 Broker Configuration		
Item	Value setting	Description
MQTT Client	The box is unchecked by default.	Check the box to activate the MQTT Client function. With the MQTT Client enabled, the gateway acts as a MQTT client and publishes messages to MQTT broker, or subscribes to interested topic(s) from MQTT Broker(s)
Save	N/A	Click the <b>Save</b> 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	Edit
							<input type="checkbox"/> Select	

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 for you 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.

## 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>	The box is 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) <b>Value Range:</b> 1 ~ 64 characters.
<b>Address</b>	1. A 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. An Optional setting. 2. <b>1883</b> is set by default	Specify a port as the port for MQTT connection. <b>Value Range:</b> 1 ~ 65535.
<b>Security</b>	1. An 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. An Optional setting. 2. <b>None</b> is set by default	Select <b>CA File</b> / <b>CERT File</b> / <b>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> could be defined in Trusted Certificate List. <b>CERT File</b> could be defined in Trusted Client Certificate List. <b>KEY File</b> could be defined in Trusted Client Key List.
<b>Client ID</b>	1. A 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. An Optional setting. 2. The box is unchecked by default.	Check the box if user (account) authentication is required for subscribing the MQTT messages. With the box checked, you have to further specify Username and Password for the connection.
<b>Username</b>	A Required setting.	Specify a name as the identifier of the MQTT client. <b>Value Range:</b> 1 ~ 32 characters.
<b>Password</b>	A Required setting.	Specify a password for the user account. <b>Value Range:</b> 1 ~ 32 characters.

<b>Keep Alive</b>	1. An Optional setting. 2. <b>60</b> sec is set by default.	Specify a keep alive interval to keep the connection alive while the connection is idle. <b>Value Range:</b> 5 ~ 86400 sec.
<b>Enable</b>	The box is unchecked by default.	Check the box to activate this MQTT Client configuration
<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.
<b>Back</b>	N/A	Click the <b>Back</b> button to go back to previous configuration screen.

## 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>	The box is 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. A Required setting. 2. Blank by default	Specify the topic for the Last Will message. <b>Value Range:</b> 1 ~ 64 characters, including the topic level separator '/', but excluding the wildcards '+' and '#'.
<b>Message</b>	1. A Required setting. 2. Blank by default	Specify the message content for the Last Will message. <b>Value Range:</b> 1 ~ 256 characters.
<b>QoS</b>	1. An Optional setting. 2. <b>0 (At most once)</b> 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-level handshake to ensure only one copy of the message is received.
<b>Topic prefix (Optional)</b>	1. An Optional-filled setting. 2. Blank by default	Specify the topic prefix for MQTT message. <b><u>Value Range:</u></b> 1 ~ 64 characters.
<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.
<b>Back</b>	N/A	Click the <b>Back</b> 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, **Publish Message Configuration** screen will appear.

Publish Message Configuration	
Item	Setting
▶ Topic	<input type="text"/>
▶ Topics prefix	<input type="checkbox"/> Enable
▶ Message Style	Manual ▼
▶ Message	<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. A Required setting. 2. Blank by default	Specify the topic for the message to be published. <b><u>Value Range:</u></b> 1 ~ 64 characters, including the topic level separator '/', but excluding the wildcards '+' and '#'.
<b>Topic prefix</b>	The box is unchecked by default.	Check the box to add the predefined topic prefix into a MQTT message.
<b>Message Style</b>	1. An Optional-filled setting. 2. <b>Manual</b> is selected	Select a message style from the dropdown list. The supported styles are: <b>Manual:</b> The message is create manually, and you can specify the message content below.



	by default	<b>System Log:</b> The message to be published are the System log of the device. <b>Data Logging:</b> The message to be published are the Data Logging recorded in the designated storage
<b>Message</b>	1. A Required setting. 2. Blank by default	Specify the message content for the Manual publish message. <b>Value Range:</b> 1 ~ 256 characters.
<b>QoS</b>	1. An Optional setting. 2. <b>0 (At most once)</b> 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>	The box is unchecked by default.	Check the box to activate this message retaining function.
<b>Publish Behavior</b>	The box is 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>	The box is unchecked by default.	Check the box to activate this publish message configuration.
<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.
<b>Back</b>	N/A	Click the <b>Back</b> button to go back to previous configuration screen.

## Subscribe Message List

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

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

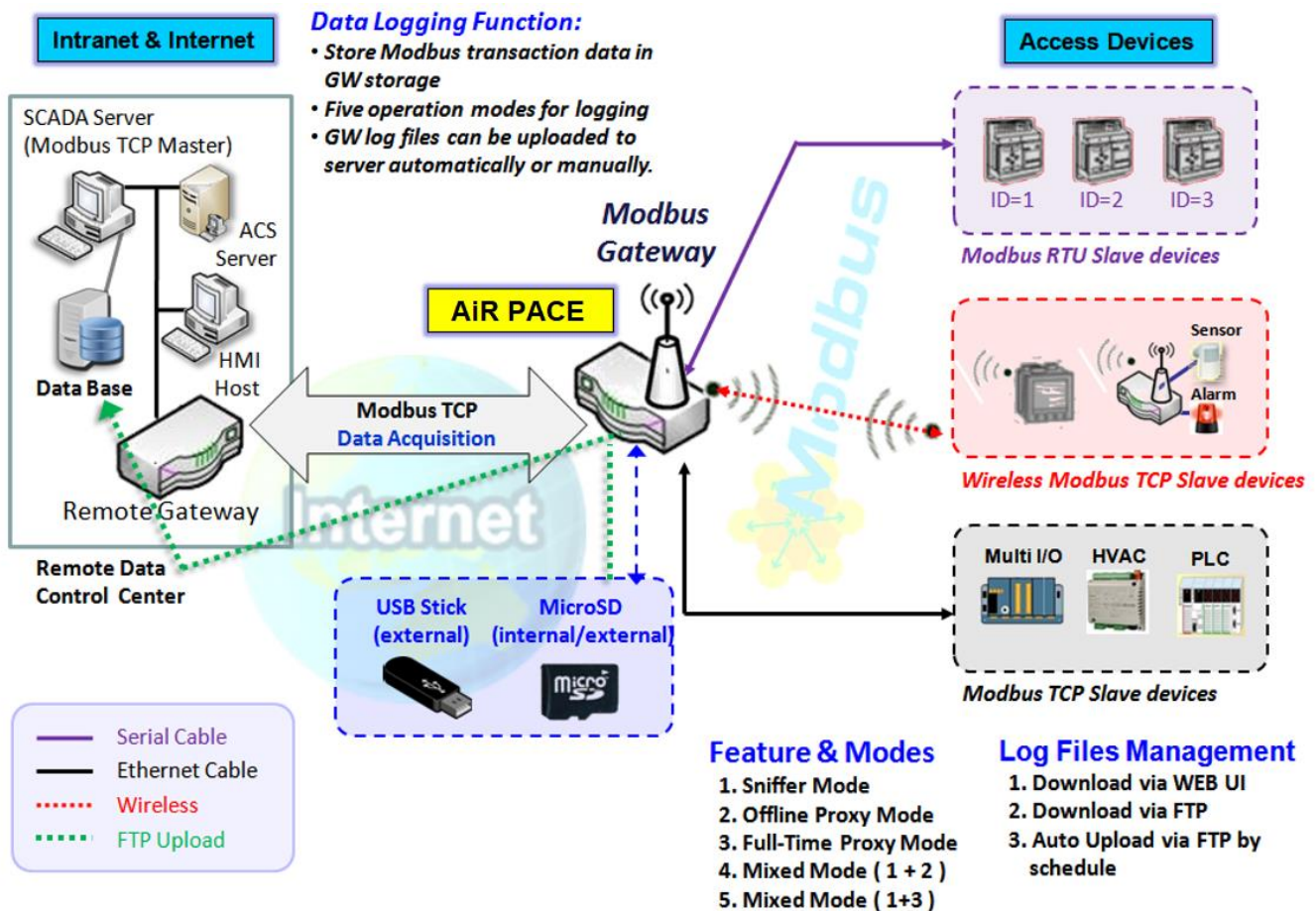
Subscribe Message Configuration <span>Save</span> <span>Undo</span>	
Item	Setting
▶ Topic	<input type="text"/>
▶ Topics prefix	<input type="checkbox"/> Enable
▶ QoS	<input checked="" type="radio"/> 0 (At most once) <input type="radio"/> 1 (At least once) <input type="radio"/> 2 (Exactly once)
▶ Enable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

Subscribe Message Configuration		
Item	Value setting	Description
<b>Topic</b>	1. A Required setting. 2. Blank by default	Specify the topic for the message to be subscribed.  <b><u>Value Range:</u></b> 1 ~ 64 characters, including the topic level separator '/', and wildcards '+', '#'.
<b>Topic prefix</b>	The box is unchecked by default.	Check the box to enable the topic prefix for subscribed message.
<b>QoS</b>	1. An Optional setting. 2. <b>0 (At most once)</b> is set by default	Select the QoS type for subscribing 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>	The box is unchecked by default.	Check the box to activate this subscribe message configuration
<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.
<b>Back</b>	N/A	Click the <b>Back</b> button to go back to previous configuration screen.

## 5.3 Data Logging

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

Even facing the network connection problems with remote NOC/SCADA side, you can also enable the data logging proxy function provided by the purchased gateway and keep doing the data acquisition and storing the collected data in local storage (in .CSV file format). When the network connection recovered, admin/user can download the data log files manually via FTP or web UI for further reference and maintenance.



The Modbus Cellular Gateway provides a complete data logging function for collecting the Modbus transaction data for application requirements. There are some data logging schemes to meet different management requirements. They are the Sniffer Mode, Offline Proxy Mode, Full-Time Proxy Mode, and the mixed modes for sniffer and proxy combinations.

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

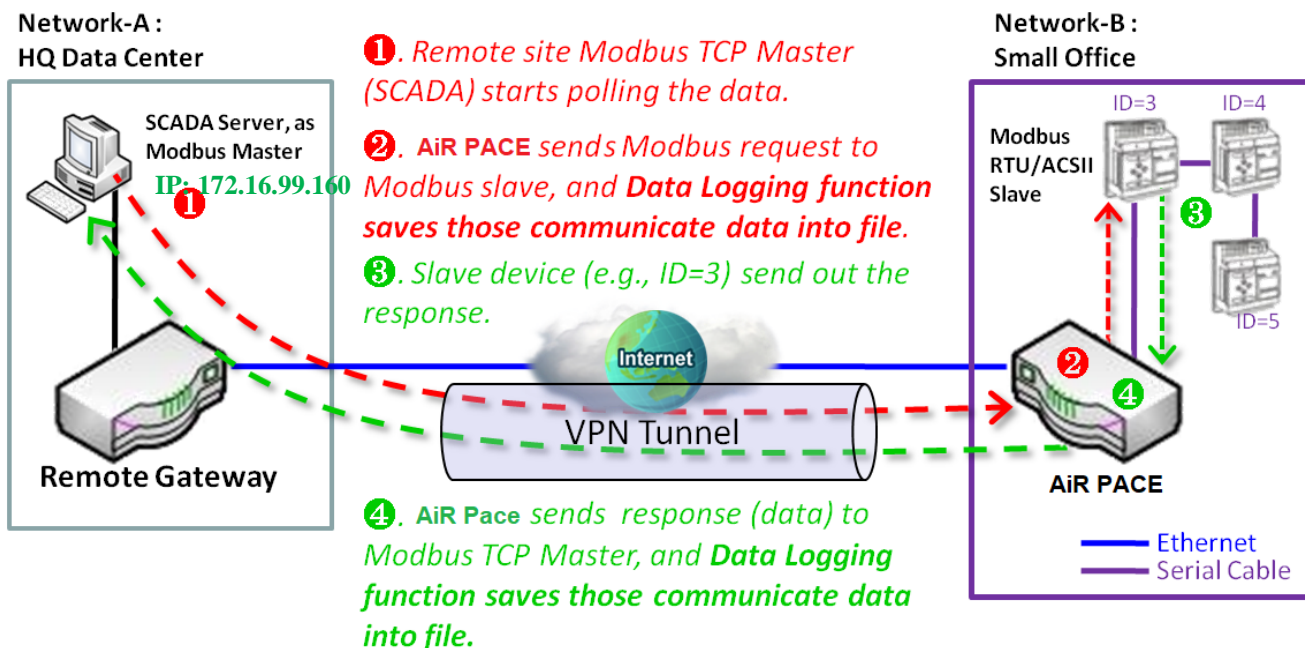
# AiR PACE

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

With the Proxy mode option enabled, when the Modbus gateway 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 may stop the data log proxy function. Remote Modbus server can keep its data acquisition process, and if required, the administrator can also get the stored data log files.

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

## ➤ Scenario for Sniffer Mode Data Logging



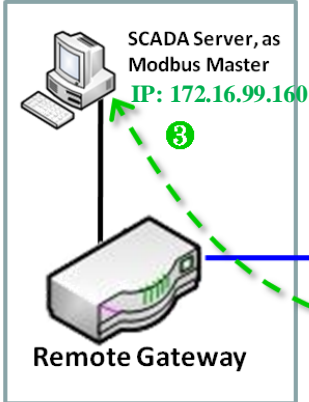
As Illustrated in the diagram, the Modbus gateway will store the following Modbus activities into a log file.

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

## ➤ Scenario for Off-Line Proxy Mode Data Logging

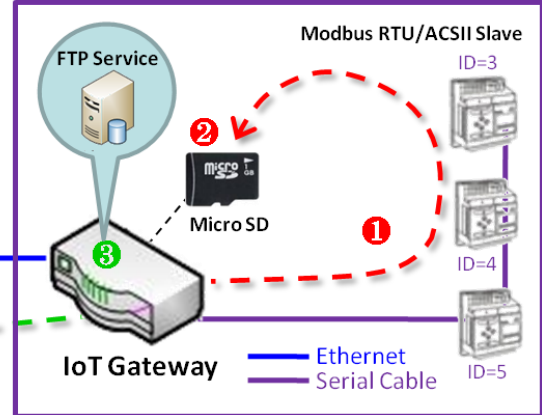
# AIR PACE

Network-A :  
HQ Data Center



- ① To do the Data-Acquisition by IoT Gateway itself automatically.
- ② Save those data as files to internal or external storage unit (e.g., Micro-SD card) .
- ③ Data Logging Files Downloading via FTP or WEB UI.

Network-B :  
Small Office



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

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

The above data acquisition and data logging activities are repeated at 5 second intervals until the connection is recovered.

## 5.3.1 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
<b>Data Logging</b>	The box is unchecked by default.	Check the <b>Enable</b> box to activate to data logging function.
<b>Storage Device</b>	<b>External</b> is set by default	Choose the sotrage device to store the log files. It can be <b>External</b> or <b>Internal</b> , depending on the product specification.
<b>Save</b>	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, and you can't enable it for the data logging. That is, if you selected External Storage, plug-in the storage first, and then enable the function and also make the required configuration.
2. Make sure the Modbus Operation Mode is selected and enabled, or there will be no Modbus transactions to be logged. Please refer to **Field Communication > Bus & Protocol > Port Configuration** and **Modbus** tabs.

### Create/Edit Modbus Proxy Rules

The Gateway allows you to customize your proxy mode rule list. It supports up to a maximum of 20 rules.

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

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

Modbus Proxy Rule List Configuration
Save
Undo

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

Modbus Proxy Rule Configuration		
Item	Value setting	Description
<b>Name</b>	A 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>	IP Address:Port is selected by default.	Specify the Modbus Slave devices to apply with 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. A 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>	Read Coils (0x01) 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. A Required setting. 2. Range 0 to 65535	Specify the Start Address of registers to apply with the specified function code. <b>Value Range:</b> 0 ~ 65535.
<b>Number of Coils/Registers</b>	1. A Required setting. 2. Range 1 to 125	Specify the number of coils/registers to apply with 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. A Required setting. 2. 1000 ms is set by default	Enter the poll time in milliseconds to apply the Proxy Mode Rule. Once the proxy mode is activated, the Modbus Gateway will issue pre-defined Modbus message on each Poll Time interval accordingly. <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.



## 5.3.2 Scheme Setup

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

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

### Create/Edit Data Logging Rules

Scheme List <span>Add</span> <span>Delete</span> <span>⬆</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> <span>✕</span>	
Item	Setting
▶ Name	<input type="text"/>
▶ Mode	Sniffer ▼
▶ Master Type	IP Address ▼ <input type="text"/>
▶ Enable	<input type="checkbox"/>

Scheme Configuration		
Item	Value setting	Description
<b>Name</b>	A Required setting.	Specify a name as the identifier of the data logging rule. <b>Value Range: 1 ~ 16 characters.</b>
<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 the 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 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 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. <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	Specify the Modbus master device to apply with the data logging rule. It can be



	by default.	<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. An Optional setting. 2. <b>60</b> sec is set by default 3. Range 1 to 99999	Specify the timeout value for querying Modbus Master. If no response from the master for the specified timeout setting, selected proxy rule will be triggered and applied with the data logging rule. Note: If Off-Line proxy scheme is selected, the timeout setting will be used to check. Otherwise, this value is not used.
<b>Proxy Rules</b>	An Optional setting.	Select the Proxy rule to be applied with the data logging rule. Note: If any proxy scheme is selected, please create the required Proxy rules in advance, and select from the list.
<b>Enable</b>	The box is 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.

## 5.3.3 Log File Management

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

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

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

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 --- ▼ Add Object
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
<b>Name</b>	N/A	The name of corresponding data log rule will be displayed. The default log file name will be named as ' Name_yyyyMMddHHmmSS.csv '.
<b>File Content Format</b>	<b>Raw Data</b> is selected by default	Select the data format for the log files. It can be <b>Raw Data</b> , or <b>Modbus Type</b> .
<b>Split File by</b>	<b>Size</b> and <b>200 KB</b> are set by default	Specify the split file methodology. It can be by <b>Size</b> , or by <b>Time Interval</b> . User has to specify a certain file size or time interval for splitting the data logs into a series of files. <b>Value Range: 1 ~ 99999.</b>
<b>Auto Upload</b>	1. An Optional filled setting 2. The box is unchecked by default.	Check the <b>Enable</b> box to activate the auto upload function for logged files. Once it has been enabled, user has to specify an external FTP server from the dropdown list for auto uploading the log files to the server. Refer to <b>Object Definition &gt; External Server &gt; External Server</b> tab, or create the FTP server with

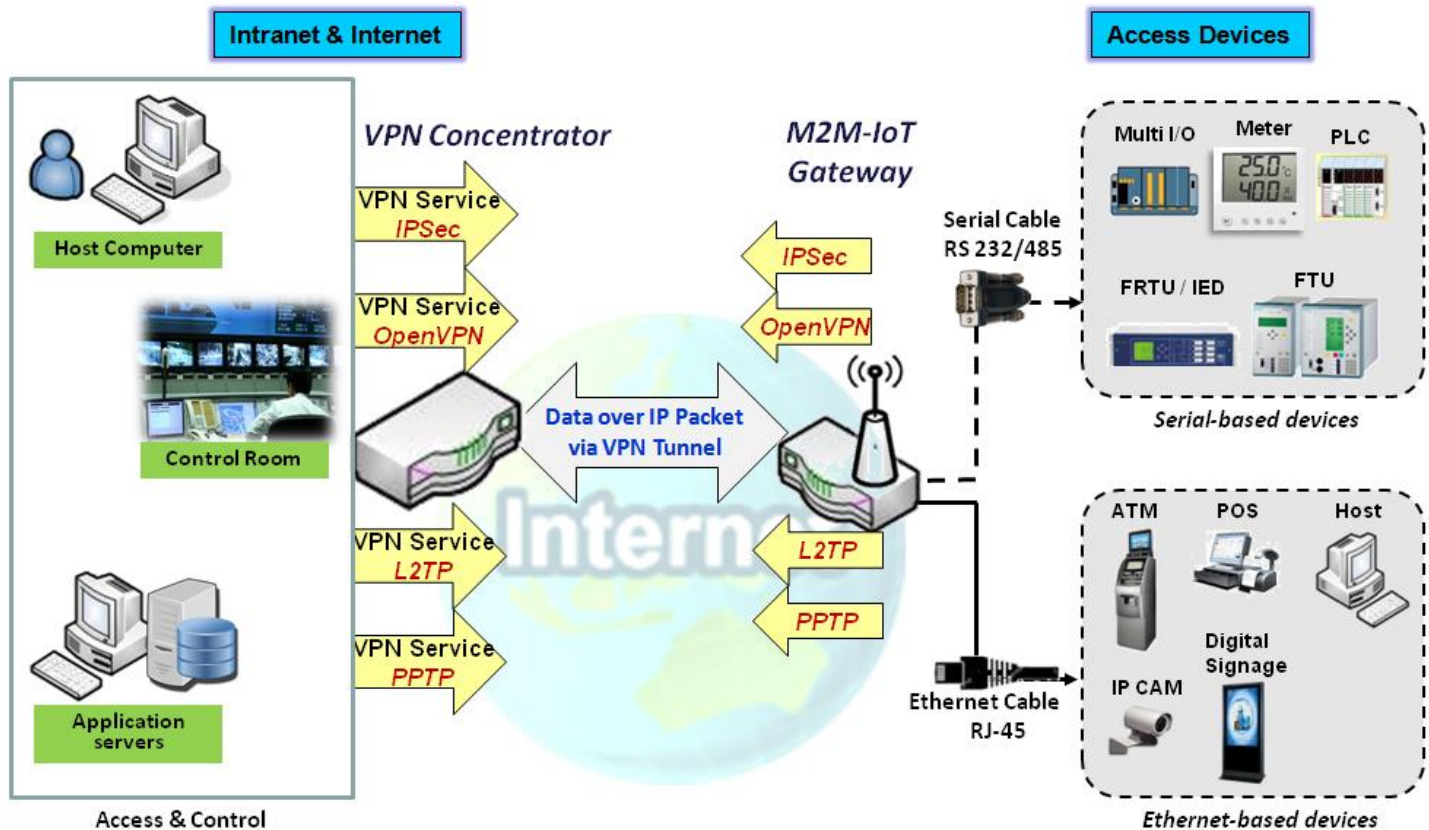
		the <b>Add Object</b> button.
<b>Log File Compression</b>	1. An Optional filled setting 2. The box is unchecked by default	If Auto Upload is activated, user can further specify whether to compress the log file prior it is uploaded or not. Check the <b>Enable</b> button to activate the Log File Compression function...
<b>Delete File After Upload</b>	1. An Optional filled setting 2. The box is unchecked by default	If Auto Upload is activated, user can further specify whether to delete the transferred log from the gateway storage or not. Check the <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 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.

## Chapter 6 Security

### 6.1 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.



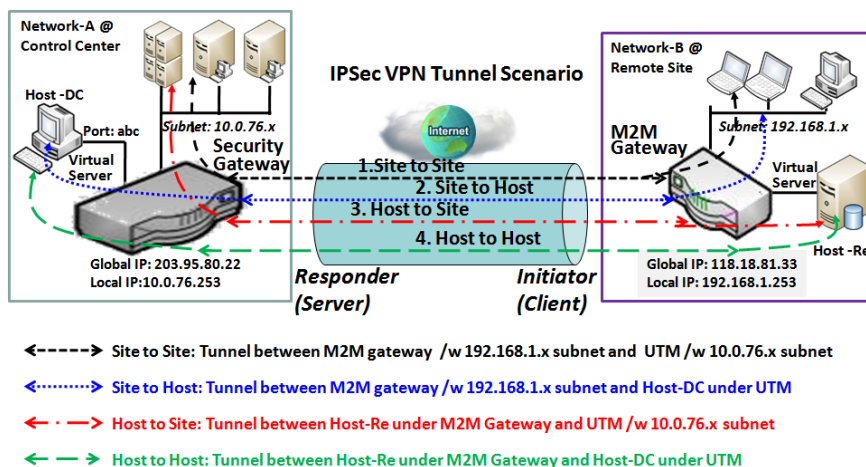
The product series supports different tunneling technologies to establish secure tunnels between multiple sites for data transferring, such as IPSec, OpenVPN, L2TP (over IPSec), PPTP and GRE. Additionally, some advanced functions, like Full Tunnel, Tunnel Failover, Tunnel Load Balance, NetBIOS over IPSec, NAT Traversal and Dynamic VPN, are also supported.

## 6.1.1 IPSec

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

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

### IPSec Tunnel Scenarios



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

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

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

## 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
<b>IPsec</b>	Unchecked by default	Click the <b>Enable</b> box to enable IPSec function.
<b>Max. Concurrent IPSec Tunnels</b>	Depends on Product specification.	The specified value will limit the maximum number of simultaneous IPSec tunnel connection. The default value may differ depending on specific model.
<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 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. You have to 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 ▼

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, can be any text	Enter a tunnel name. Enter a name that is easy for you to identify. <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 the available WAN and LAN interfaces.
<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 among them 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. <b>Value Range:</b> 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 <b>v1</b> or <b>v2</b> .

Local & Remote Configuration				
Item	Setting			
Local Subnet List	ID	Subnet IP Address	Subnet Mask	Actions
	1	192.168.66.0	255.255.255.0(24) ▼	Delete
	Add			
Remote Subnet List	ID	Subnet IP Address	Subnet Mask	Actions
	1		255.255.255.0(24) ▼	Delete
	Add			
Remote Gateway				

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. Click the Add or Delete 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. Note_2: When Host-to-Site or Host-to-Host option in Tunnel Scenario is selected, Local Subnet will not be available. Note_3: When Hub and Spoke option in Hub and Spoke is selected, there will be only one subnet available.</p>
<b>Remote Subnet List</b>	Required setting	<p>Specify the Remote Subnet IP address and Subnet Mask. Click the Add or Delete button to add or delete Remote Subnet setting.</p>
<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.	<p>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.</p>
<b>Local ID</b>	An optional setting	<p>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).</p>
<b>Remote ID</b>	An optional setting	<p>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.</p>



IKE Phase	
Item	Setting
▶ Negotiation Mode	Main Mode ▼
▶ X-Auth	None ▼ X-Auth Account (Optional) User Name : <input type="text"/> Password : <input type="text"/>
▶ 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		
Item	Value setting	Description
<b>Negotiation Mode</b>	Main Mode is set by default default	Specify the Negotiation Mode for this IPSec tunnel. Select <b>Main Mode</b> or <b>Aggressive Mode</b> .
<b>X-Auth</b>	None is selected by default	Specify the X-Auth role for this IPSec tunnel. Select Server, Client, or None. If None then no X-Auth authentication is required. Selected Server this gateway will be an X-Auth server. Click on the X-Auth Account button to create remote X-Auth client account. Selected Client this gateway will be an X-Auth client. Enter User name and Password to be authenticated by the X-Auth server gateway. Note: X-Auth Client will not be available for Dynamic VPN option selected in Tunnel Scenario.
<b>Dead Peer Detection (DPD)</b>	1. Checked by default 2. Default Timeout 180s and Delay 30s	Click <b>Enable</b> box to enable <b>DPD</b> 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-128 ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
2	AES-128 ▼	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-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 <b>Enable</b> box to enable this setting

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

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

IPSec Proposal Definition				
ID	Encryption	Authentication	PFS Group	Definition
1	AES-128 ▼	SHA1 ▼	Group 2 ▼	<input checked="" type="checkbox"/> Enable
2	AES-128 ▼	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
IPSec Proposal Definition	Required setting	<p>Specify the Encryption method. It can be DES / 3DES / AES-128 / AES-192 / AES-256.            Note: None is available when Encapsulation Protocol is set as <b>AH</b>.</p> <p>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.</p> <p>Specify the PFS Group. It can be None / Group1 / Group2 / Group5 / Group14 / Group15 / Group16 / Group17 / Group18.</p> <p>Click <b>Enable</b> to enable this setting</p>
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 previous page.

## Create/Edit Dynamic VPN Server List

Dynamic VPN List
Add
Delete
Refresh

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

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

Tunnel Configuration	
Item	Setting
Tunnel	<input type="checkbox"/> Enable
Tunnel Name	<input type="text" value="Dynamic IPSec1"/>
Interface	<input type="text" value="WAN1"/>
Tunnel Scenario	<input type="text" value="Tunnel Mode"/>
Encapsulation Protocol	<input type="text" value="ESP"/>
IKE Version	<input type="text" value="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, can be any text	Enter a tunnel name. Enter a name that is easy for you to identify. <b><i>Value Range: 1 ~ 19 characters.</i></b>
<b>Interface</b>	1. Required setting 2. <b>WAN 1</b> is selected by default	Select WAN interface on which IPSec tunnel is to be established.
<b>Tunnel Scenario</b>	1. Required setting 2. <b>Tunnel Mode</b> is selected by default	Select the Dynamic IPSec tunneling scenario. It can be <b>Tunnel Mode</b> or <b>Transport Mode</b> .
<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	<input type="text" value="192.168.66.0"/>
Local Netmask	<input type="text" value="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 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>Local ID</b>	An 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>	An 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.

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

## 6.1.2 OpenVPN

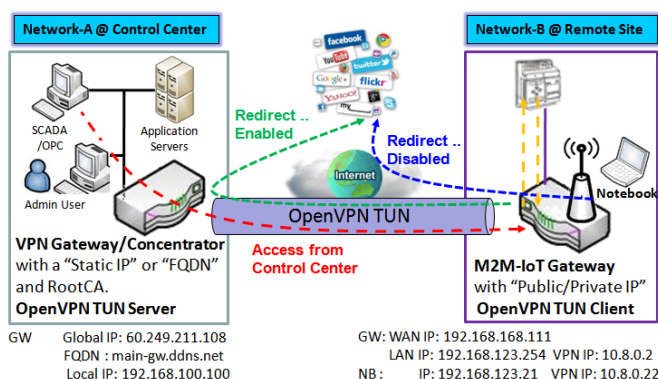
OpenVPN is an application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable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

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

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

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

### OpenVPN TUN Scenario



1. M2M-IoT Gateway (as OpenVPN TUN Client) connects to peer VPN Gateway/Concentrator (as OpenVPN TUN Server).
2. M2M-IoT Gateway will be assigned 10.8.0.2 IP Address after OpenVPN TUN Connection 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.

solution.

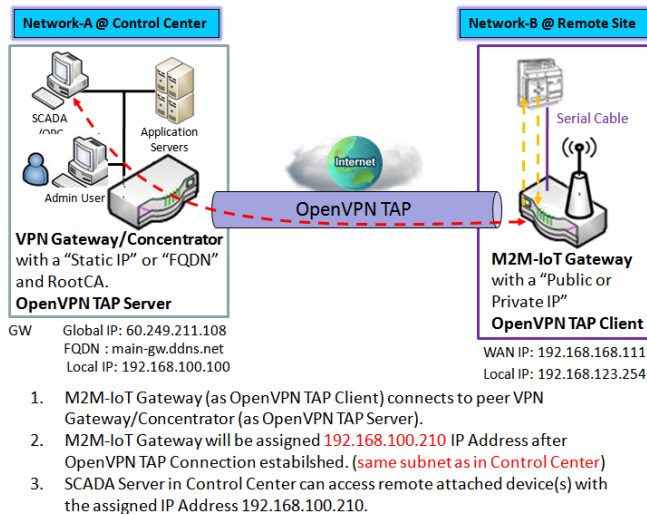
The term "TUN" mode is referred to routing mode and operates with Layer 3 packets. In routing mode, the VPN client is given an IP address on a different subnet than the local LAN under the OpenVPN server. This virtual subnet is created for connecting to any remote VPN computers. In routing mode, the 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

As shown in the diagram, the M2M-IoT Gateway is configured as an OpenVPN TUN Client, and connects to an OpenVPN TUN 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 Center. With such connection, the local networked devices will get a virtual IP 10.8.0.x if its traffic goes through the OpenVPN TUN connection when Redirect Internet Traffic settings is enabled; Additionally, 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" is referred to bridge mode and operates with Layer 2 packets. In bridge mode, the VPN client is given an IP address on the same subnet as the LAN resided under the OpenVPN server. Under such configuration, the OpenVPN client can directly access the resources in the LAN. If you want to offer remote access to the entire remote LAN for VPN client(s), you have to 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 the same subnet as

that of local subnet in Control Center. With such connection, the SCADA Server in Control Center can access remote attached serial device(s) with the virtual IP address (192.168.100.210).

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 ▼

Configuration		
Item	Value setting	Description
OpenVPN	The box is 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 indicates, 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. **OpenVPN Server Configuration** window lets you enable the OpenVPN server function, specify the virtual IP address of OpenVPN server, when remote OpenVPN clients dial in, and the authentication protocol.

Configuration

Item	Setting
OpenVPN	<input checked="" type="checkbox"/> Enable
Server / Client	Server ▼
OpenVPN Configuration file	<input type="checkbox"/> Enable <span>Export</span> client.ovpn

Configuration

Item	Value setting	Description
<b>OpenVPN Configuration File</b>	1. An Optional setting. 2. The box is 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 <b>Export</b> button to get the configuration file.

The OpenVPN Server supports up to 4 TUN / TAP tunnels at the same time.

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	<span>Edit</span>



OpenVPN Server Configuration		
Item	Value setting	Description
<b>OpenVPN Server</b>	The box is unchecked by default.	Click the <b>Enable</b> to activate OpenVPN Server functions.
<b>Protocol</b>	<ol style="list-style-type: none"> <li>1. A Required setting</li> <li>2. By default <b>TCP</b> is selected.</li> </ol>	<p>Define the selected <b>Protocol</b> for connecting to the OpenVPN Server.</p> <ul style="list-style-type: none"> <li>• Select <b>TCP</b> , or <b>UDP</b></li> </ul> <p>-&gt; The TCP protocol will be used to access the OpenVPN Server, and <b>Port</b> will be set as 4430 automatically.</p> <ul style="list-style-type: none"> <li>• Select <b>UDP</b></li> </ul> <p>-&gt; The UDP protocol will be used to access the OpenVPN Server, and <b>Port</b> will be set as 1194 automatically.</p>
<b>Port</b>	<ol style="list-style-type: none"> <li>1. A Required setting</li> <li>2. By default <b>4430</b> is set.</li> </ol>	<p>Specify the <b>Port</b> for connecting to the OpenVPN Server.</p> <p><b>Value Range:</b> 1 ~ 65535.</p>
<b>Tunnel Scenario</b>	<ol style="list-style-type: none"> <li>1. A Required setting</li> <li>2. By default <b>TUN</b> is selected.</li> </ol>	<p>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.</p>
<b>Authorization Mode</b>	<ol style="list-style-type: none"> <li>1. A Required setting</li> <li>2. By default <b>TLS</b> is selected.</li> </ol>	<p>Specify the authorization mode for the OpenVPN Server.</p> <ul style="list-style-type: none"> <li>• <b>TLS</b></li> </ul> <p>-&gt;The 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; 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></li> </ul> <p>-&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.</p>
<b>Local Endpoint IP Address</b>	A Required setting	<p>Specify the virtual <b>Local Endpoint IP Address</b> of this OpenVPN gateway.</p> <p><b>Value Range:</b> The IP format is 10.8.0.x, the range of x is 1~254.</p> <p>Note: Local Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.</p>
<b>Remote Endpoint IP Address</b>	A Required setting	<p>Specify the virtual <b>Remote Endpoint IP Address</b> of the peer OpenVPN gateway.</p> <p><b>Value Range:</b> The IP format is 10.8.0.x, the range of x is 1~254.</p> <p>Note: Remote Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.</p>
<b>Static Key</b>	A Required setting	<p>Specify the <b>Static Key</b>.</p> <p>Note: Static Key will be available only when Static Key is chosen in Authorization Mode.</p>
<b>Server Virtual IP</b>	A Required setting	<p>Specify the <b>Server Virtual IP</b>.</p> <p><b>Value Range:</b> The IP format is 10.y.0.0, the range of y is 1~254.</p> <p>Note: Server Virtual IP will be available only when TLS is chosen in Authorization Mode.</p>
<b>DHCP-Proxy Mode</b>	<ol style="list-style-type: none"> <li>1. A Required setting</li> <li>2. The box is checked by default.</li> </ol>	<p>Check the <b>Enable</b> box to activate the <b>DHCP-Proxy Mode</b>.</p> <p>Note: DHCP-Proxy Mode will be available only when TAP is chosen in Tunnel Device.</p>
<b>IP Pool</b>	A Required setting	<p>Specify the virtual <b>IP pool</b> setting for the OpenVPN server. You have to specify the <b>Starting Address</b> and <b>Ending Address</b> as the IP address pool for the OpenVPN clients.</p> <p>Note: IP Pool will be available only when TAP is chosen in Tunnel Device, and DHCP-Proxy Mode is unchecked (disabled).</p>

<b>Gateway</b>	A 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 supports 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. An Optional setting. 2. The box is unchecked by default.	Check the <b>Enable</b> box to activate the <b>Redirect Default Gateway</b> function.
<b>Encryption Cipher</b>	1. A Required setting. 2. By default <b>Blowfish</b> is selected.	Specify the <b>Encryption Cipher</b> from the dropdown list. It can be <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. It can be <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. It can be <b>Adaptive/YES/NO/Default</b> .
<b>Multicast</b>	1. An Optional setting. 2. The box is checked by default.	Check the <b>Enable</b> box to activate the Multicast function.  <b>Note:</b> Multicast function is only available for TAP tunnel scenario.
<b>Persis Key</b>	1. An 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. An 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>X</b> to cancel the changes and return to last page.

# AIR PACE

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

**OpenVPN Server Advanced Configuration**

Item	Setting
▶ TLS Cipher	None ▼
▶ 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	0
▶ 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. A Required setting. 2. <b>TLS-RSA-WITH-AES128-SHA</b> is selected by default	Specify the <b>TLS Cipher</b> from the dropdown list. It can be <b>None</b> / <b>TLS-RSA-WITH-RC4-MD5</b> / <b>TLS-RSA-WITH-AES128-SHA</b> / <b>TLS-RSA-WITH-AES256-SHA</b> / <b>TLS-DHE-DSS-AES128-SHA</b> / <b>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. An 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. A Required setting 2. The value is <b>1500</b> by default	Specify the <b>Tunnel MTU</b> . <b>Value Range:</b> 0 ~ 1500.
<b>Tunnel UDP Fragment</b>	1. A Required setting 2. The value is <b>1500</b> by default	Specify the <b>Tunnel UDP Fragment</b> . By default, it is equal to <b>Tunnel MTU</b> . <b>Value Range:</b> 0 ~ 1500.

# AIR PACE

	default	Note: Tunnel UDP Fragment will be available only when UDP is chosen in Protocol.
<b>Tunnel UDP MSS-Fix</b>	1. An Optional setting. 2. The box is 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. An 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. An 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. An Optional setting. 2. String format: any text	Specify the <b>Additional Configuration</b> . <b><u>Value Range:</u></b> 0 ~ 256 characters.

# AIRPACE

## 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 <button>Upgrade</button>

OpenVPN Configuration		
Item	Value setting	Description
OpenVPN	The box is 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. An Optional setting. 2. The box is 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 a .ovpn file.  If you enabled this function, you can't add any OpenVPN clients manually.

OpenVPN Client List

AddDelete

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

OpenVPN Client Configuration	
Item	Setting
▶ OpenVPN Client Name	OpenVPN Client #1
▶ Interface	WAN 1 ▼
▶ Protocol	TCP ▼ Port: 443
▶ Tunnel Scenario	TUN ▼
▶ Remote IP/FQDN	
▶ Remote Subnet	<input type="checkbox"/> Enable <input checkbox"="" type="text" value="255.255.255.0/(24) ▼&lt;/td&gt; &lt;/tr&gt; &lt;tr&gt; &lt;td&gt;▶ Redirect Internet Traffic&lt;/td&gt; &lt;td&gt;&lt;input type="/> Enable
▶ NAT	<input checked="" 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	<input type="button" value="Edit"/>
▶ Tunnel	<input type="checkbox"/> Enable

OpenVPN Client Configuration		
Item	Value setting	Description
<b>OpenVPN Client Name</b>	A 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. A 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. A 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;The OpenVPN will use TCP protocol, and <b>Port</b> will be set as 443 automatically.</li> <li>• Select <b>UDP</b> -&gt; The OpenVPN will use UDP protocol, and <b>Port</b> will be set as 1194 automatically.</li> </ul>
<b>Port</b>	1. A 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. A Required setting 2. By default <b>TUN</b> is selected.	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.
<b>Remote IP/FQDN</b>	A Required setting	Specify the <b>Remote IP/FQDN</b> of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the IP address or FQDN.
<b>Remote Subnet</b>	1. An Optional setting. 2. The box is unchecked by default.	Check the <b>Enable</b> box to activate remote subnet function, and 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. An Optional setting. 2. The box is unchecked by default.	Check the <b>Enable</b> box to activate the <b>Redirect Internet Traffic</b> function.
<b>NAT</b>	1. An Optional setting.	Check the <b>Enable</b> box to activate the <b>NAT</b> function.

	2. The box is checked by default.	
<b>Authorization Mode</b>	1. A 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> could be selected in Trusted CA Certificate List. Refer to <b>Object Definition &gt; Certificate &gt; Trusted Certificate</b>. <b>Client Cert.</b> could be selected in Local Certificate List. Refer to <b>Object Definition &gt; Certificate &gt; My Certificate</b>. <b>Client Key</b> could 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;The 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>	A 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>	A 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>	A 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> . It can be <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> . It can be <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. It can be <b>Adaptive/YES/NO/Default</b> .
<b>Persis Key</b>	1. An 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. An 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>Tunnel</b>	The box is 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>X</b> to cancel the changes and return to last page.

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. A Required setting. 2. <b>TLS-RSA-WITH-AES128-SHA</b> is selected by default	Specify the <b>TLS Cipher</b> from the dropdown list. It can be <b>None</b> / <b>TLS-RSA-WITH-RC4-MD5</b> / <b>TLS-RSA-WITH-AES128-SHA</b> / <b>TLS-RSA-WITH-AES256-SHA</b> / <b>TLS-DHE-DSS-AES128-SHA</b> / <b>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. An Optional setting. 2. String format: any text	Specify the <b>TLS Auth. Key</b> for connecting to an OpenVPN server, if the server required it. Note: TLS Auth. Key will be available only when TLS is chosen in Authorization Mode.
<b>User Name</b>	An Optional setting.	Enter the <b>User account</b> for connecting to an OpenVPN server, if the server required it. Note: User Name will be available only when TLS is chosen in Authorization Mode.
<b>Password</b>	An Optional setting.	Enter the <b>Password</b> for connecting to an OpenVPN server, if the server required it. Note: User Name will be available only when TLS is chosen in Authorization Mode.
<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: Bridge TAP to will be available only when TAP is chosen in Tunnel Scenario and NAT is unchecked.
<b>Firewall Protection</b>	The box is 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.
<b>Client IP Address</b>	By default <b>Dynamic IP</b> is	Specify the virtual IP Address for the OpenVPN Client.



	selected	It can be <b>Dynamic IP/Static IP</b> .
<b>Tunnel MTU</b>	1.A Required setting 2.The value is 1500 by default	Specify the value of <b>Tunnel MTU</b> . <b>Value Range:</b> 0 ~ 1500.
<b>Tunnel UDP Fragment</b>	The value is 1500 by default	Specify the value of <b>Tunnel UDP Fragment</b> . <b>Value Range:</b> 0 ~ 1500. Note: Tunnel UDP Fragment will be available only when UDP is chosen in Protocol.
<b>Tunnel UDP MSS-Fix</b>	The box is 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>	The box is 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:</b> -1 ~ 86400.
<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 it is no need to execute connection retry. <b>Value Range:</b> -1 ~ 86400, and -1 means no retry is required.
<b>DNS</b>	By default <b>Automatically</b> is selected	Specify the setting of <b>DNS</b> . It can be <b>Automatically/Manually</b> .
<b>Additional Configuration</b>	An Optional setting.	Enter optional configuration string here. Up to 256 characters is allowable. <b>Value Range:</b> 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.

## 6.1.3 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	<input type="text" value="192.168.10.1"/>
IP Pool Starting Address	<input type="text" value="10"/>
IP Pool Ending Address	<input type="text" value="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 <input type="text" value="40 bits"/> ▼
Service Port	<input type="text" value="1701"/>

L2TP Server Status Refresh

User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

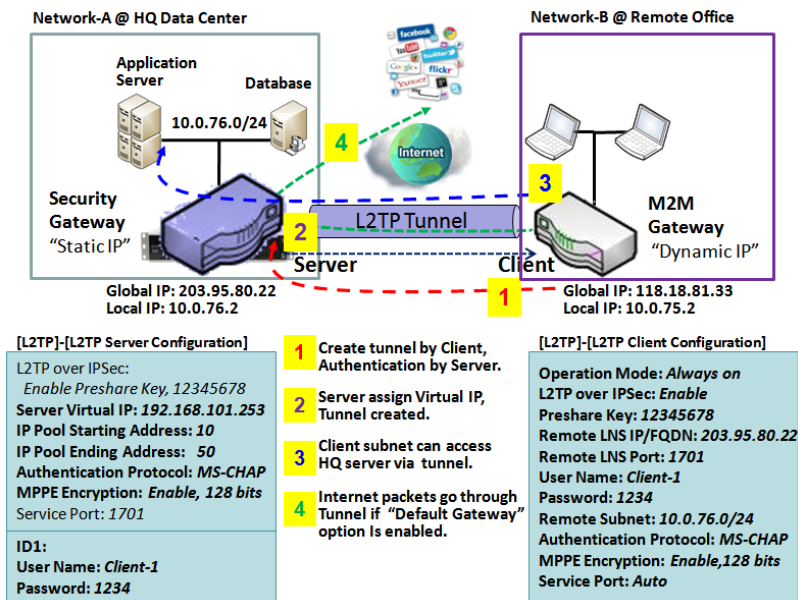
User Account List Add Delete

ID	User Name	Password	Enable	Actions
----	-----------	----------	--------	---------

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

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

**L2TP Client:** It can be mobile users or gateways in remote offices with dynamic IP. To set up a tunnel, “user name”, “password” and server’s global IP are required. In addition, it is required to identify the operation mode for each tunnel as a main connection, a failover for another tunnel, or a load balance tunnel to increase overall bandwidth. “Default Gateway” or “Remote Subnet” for packet flow must be decided. Moreover, you can also define what kind of traffic will pass through the L2TP tunnel in the “Default Gateway / Remote Subnet” parameter.



Additionally, for the L2TP client peer, a Remote Subnet item is required. It is for the Intranet of L2TP server peer. So, 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 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 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. Certainly, those packets come through the L2TP tunnel.

## L2TP Setting

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

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

### Enable L2TP

Configuration	
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>	A Required setting	Specify the role of L2TP. Select <b>Server</b> or <b>Client</b> role your gateway will take. Below are the configuration windows for L2TP Server and for L2TP Client.
<b>Save</b>	N/A	Click <b>Save</b> button to save the settings

### As a L2TP Server

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

L2TP Server Configuration	
Item	Setting
▶ L2TP Server	<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

L2TP Server Configuration		
Item	Value setting	Description
<b>L2TP Server</b>	The box is unchecked by default	Click the <b>Enable</b> box to activate the L2TP server
<b>Interface</b>	1. Required setting 2. <b>All WANs</b> is selected by default	Select the interface on which L2TP tunnel is to be established. It can be on any available WAN interfaces.
<b>L2TP over IPSec</b>	The box is unchecked by default	When the <b>Enable</b> box is clicked, it will enable L2TP over IPSec and the Pre-shared Key ( <b>8~32 characters</b> ) must be filled in.
<b>Server Virtual IP</b>	A Required setting	Specify the L2TP server Virtual IP It will set as this L2TP server local virtual IP
<b>IP Pool Starting Address</b>	1. A Required setting 2. <b>10</b> is set by default.	Specify the L2TP server starting IP of virtual IP pool It will set as the starting IP which assign to L2TP client <b>Value Range:</b> 1 ~ 254.
<b>IP Pool Ending Address</b>	1. A Required setting 2. <b>17</b> is set by default.	Specify the L2TP server ending IP of virtual IP pool It will set as the ending IP which assign to L2TP client <b>Value Range:</b> >= Starting Address, and < (Starting Address + 8) or 254.
<b>Authentication Protocol</b>	A 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>	A 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>	A Required setting	Specify the <b>Service Port</b> which L2TP server 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 recovery 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	It displays the User Name, Remote IP, Remote Virtual IP, and Remote Call ID of the connected L2TP clients. Click the <b>Refresh</b> button to renew the L2TP client information.

User Account List <span>Add</span> <span>Delete</span>				
ID	User Name	Password	Enable	Actions
User Account Configuration <span></span> <span></span>				
User Name		Password	Account	
<input type="text"/>		<input type="text"/>	<input type="checkbox"/> Enable	
<span>Save</span>				

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 user account. Enter 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><u><b>Value Range:</b> 1 ~ 32 characters.</u></p>

# AIRPACE

## As a L2TP Client

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

L2TP Client Configuration	
Item	Setting
L2TP Client	<input type="checkbox"/> Enable

Item Setting	Value setting	Description
L2TP Client	The box is 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.

## Create/Edit L2TP Client

L2TP Client List & Status								
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"/>	<input type="button" value="Edit"/> <input type="checkbox"/> Select

When **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	L2TP #1
Interface	WAN1
L2TP over IPsec	<input type="checkbox"/> Enable Preshared Key (Min. 8 characters)
Remote LNS IP/FQDN	
MTU	1500
Remote LNS Port	1701
User Name	
Password	
Tunneling Password (Optional)	
Remote Subnet	
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	Auto
Interval	30 seconds
Max. Failure Time	6 times
Service Port	Auto
Tunnel	<input type="checkbox"/> Enable

L2TP Client Configuration		
Item Setting	Value setting	Description
<b>Tunnel Name</b>	A Required setting	Enter a tunnel name. Enter a name that is easy for you to identify. <b>Value Range:</b> 1 ~ 32 characters.
<b>Interface</b>	A 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>	The box is 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>	A Required setting	Enter the public IP address or the FQDN of the L2TP server.
<b>MTU</b>	1. A Required setting 2. The value is 1500 by default	Specify the <b>MTU</b> . <b>Value Range:</b> 0 ~ 1500.
<b>Remote LNS Port</b>	1. A Required setting 2. <b>1701</b> is set by default	Enter the Remote LNS Port for this L2TP tunnel. <b>Value Range:</b> 1 ~ 65535.
<b>User Name</b>	A Required setting	Enter the <b>User Name</b> for this L2TP tunnel to be authenticated when connected to L2TP server. <b>Value Range:</b> 1 ~ 32 characters.
<b>Password</b>	A Required setting	Enter the <b>Password</b> for this L2TP tunnel to be authenticated when connected to L2TP server.
<b>Tunneling Password(Optional)</b>	An Optional filled setting	Enter the <b>Tunneling Password</b> for this L2TP tunnel to authenticate.
<b>Remote Subnet</b>	A Required setting	Specify the remote subnet for this L2TP tunnel to reach 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 peer, 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. Certainly, those packets come through the L2TP VPN tunnel.
<b>Authentication Protocol</b>	1. A 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. An optional setting	Specify whether L2TP 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. A Required setting 2. Unchecked by	Specify whether NAT is required or not for this L2TP tunnel.



	default	
<b>LCP Echo Type</b>	1. Auto is set by default	<p>Specify the LCP Echo Type for this L2TP 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>Service Port</b>	A Required setting	<p>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>.</p> <p><b>Auto</b>: The system determines the service port.</p> <p><b>1701 (for Cisco)</b>: The system use port 1701 for connecting with CISCO L2TP Server.</p> <p><b>User-defined</b>: Enter the service port. The default value is 0.</p> <p><b>Value Range</b>: 0 ~ 65535.</p>
<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>X</b> button to cancel the settings and back to last page.

## 6.1.4 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				

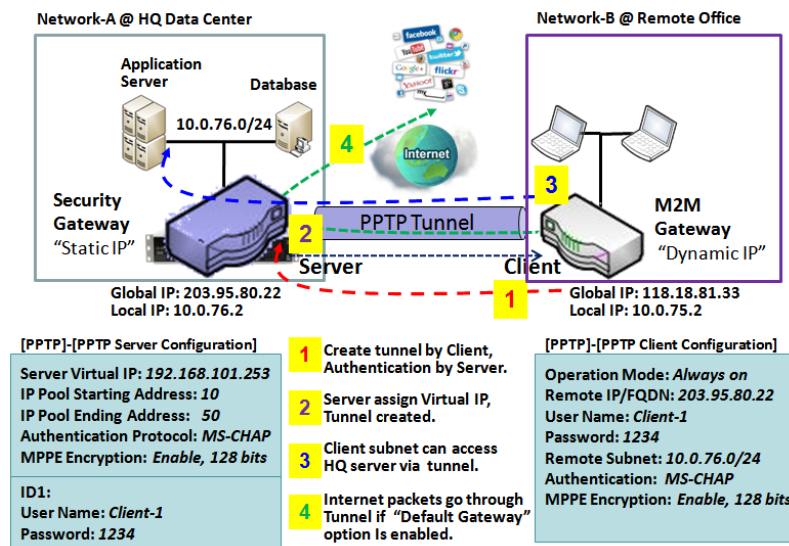
  

User Account List Add Delete				
ID	User Name	Password	Enable	Actions

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, "user name", "password" and server's global IP are required. In addition, it is required to identify the operation mode for each tunnel as a main connection, a failover for another tunnel, or a load balance tunnel to increase overall bandwidth. "Default Gateway" or "Remote Subnet" for packet flow must be selected. Moreover, you can also define what kind of traffic will pass through the PPTP tunnel in the "Default Gateway / Remote Subnet" parameter.



Additionally, for the PPTP client peer, a Remote Subnet item is required. It is for the Intranet of PPTP server peer. So, 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 you enter 0.0.0.0/0 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 peer, 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. Certainly, those packets come through the PPTP tunnel.

## PPTP Setting

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

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

### Enable PPTP

Configuration	
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 your gateway will take. 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 ▼

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</b> is selected by default	Select the interface on which PPTP tunnel is to be established. It can be the available WAN interfaces.
<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. <b>Value Range:</b> 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.

PPTP Server Status <span>Refresh</span>				
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	It 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.

User Account List					Add	Delete		
ID	User Name	Password	Enable	Actions				
User Account Configuration								
User Name	Password		Account					
<input type="text"/>	<input type="text"/>		<input type="checkbox"/> Enable					
					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 a user account. Enter 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 select Client 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.

## Create/Edit PPTP Client

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

When **Add/Edit** button is applied, a series PPTP Client Configuration will appear.

PPTP Client Configuration	
Item	Setting
▶ Tunnel Name	PPTP #1
▶ Interface	WAN1 ▼
▶ Remote IP/FQDN	
▶ MTU	1500
▶ User Name	
▶ Password	
▶ Remote Subnet	
▶ 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	Auto ▼
	Interval 30 seconds Max. Failure Time 6 times
▶ Tunnel	<input type="checkbox"/> Enable

PPTP Client Configuration Window		
Item	Value setting	Description
<b>Tunnel Name</b>	Required setting	Enter a tunnel name. Enter a name that is easy for you to identify. <b>Value Range:</b> 1 ~ 32 characters.
<b>Interface</b>	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> ).
<b>Remote IP/FQDN</b>	1. Required setting. 2. Format can be a ipv4 address or FQDN	Enter the public IP address or the FQDN of the PPTP server.
<b>MTU</b>	1.A Required setting 2.The value is 1500 by default	Specify the <b>MTU</b> . <b>Value Range:</b> 0 ~ 1500.
<b>User Name</b>	Required setting	Enter the <b>User Name</b> for this PPTP tunnel to be authenticated when connected to PPTP server. <b>Value Range:</b> 1 ~ 32 characters.
<b>Password</b>	Required setting	Enter the <b>Password</b> for this PPTP tunnel to be authenticated when connected to PPTP server.
<b>Remote Subnet</b>	Required setting	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. So, at PPTP client peer, the packets whose destination is in the dedicated subnet will be transferred via the PPTP VPN tunnel. Others will be transferred based on current routing policy of the security gateway at PPTP client peer.  If you enter 0.0.0.0/0 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 peer, 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. Certainly, those packets come through the PPTP VPN tunnel.
<b>Authentication Protocol</b>	1. Required setting 2. Unchecked by default	Specify one or multiple <b>Authentication Protocol</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. an 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. A 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	Specify the LCP Echo Type for this PPTP tunnel. It can be <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>Value Range</b> : 1 ~ 99999 for Interval Time, 1~999 for Failure Time.
<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>X</b> button to cancel the settings and back to last page.



## 6.1.5 GRE

Configuration										
Item	Setting									
GRE Tunnel	<input type="checkbox"/> Enable									
Max. Concurrent GRE Tunnels	32									

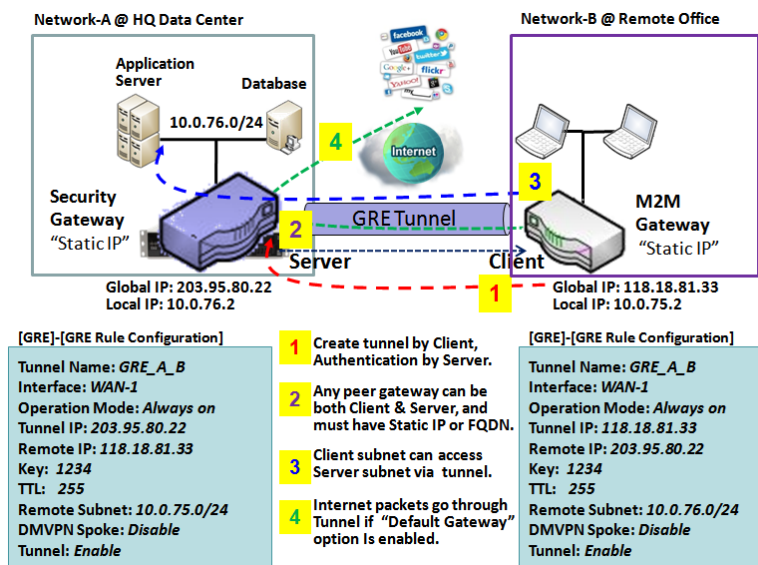
GRE Tunnel List										
			Add		Delete					
ID	Tunnel Name	Interface	Tunnel IP	Remote IP	MTU	Key	TTL	Remote Subnet	Enable	Actions

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

GRE Tunneling is similar to IPSec Tunneling, 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 used as either a client or a server, even using the same set of configuration rule.

### GRE Tunnel Scenario



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

Additionally, each peer must further specify the Remote Subnet item. It is for the Intranet of GRE server peer. So, at GRE client peer, the packets whose destination is in the dedicated subnet will be transferred via the GRE tunnel. Others will be transferred based on current routing policy of the gateway at GRE client peer. But, if you enter 0.0.0.0/0 in the Remote Subnet field, it will be treated as a "Default Gateway" setting for the GRE client peer, all packets, including the Internet accessing of GRE client peer, 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. Certainly, those packets come through the GRE tunnel.

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

## GRE Setting

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

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

### Enable GRE

Configuration	
Item	Setting
GRE Tunnel	<input type="checkbox"/> Enable
Max. Concurrent GRE Tunnels	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 connection. The default value may vary by 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									
ID	Tunnel Name	Interface	Tunnel IP	Remote IP	MTU	Key	TTL	Remote Subnet	Enable
									Actions

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

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. Enter a name that is easy for you to identify. <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>	An 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. A Required setting 2. <b>Auto</b> (value zero or blank) is set by default	<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. <b>Value Range:</b> 0 ~ 1500.
<b>Key</b>	An 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. <b>Value Range:</b> 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. So, at GRE client peer, the packets whose destination is in the dedicated subnet will be transferred via the GRE tunnel. Others will be transferred based on current routing policy of the security gateway at GRE 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 GRE client peer, all packets, including the Internet accessing of GRE client peer, 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. Certainly, those packets come through the GRE tunnel.
<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>X</b> button to cancel the settings and back to last page.

## 6.1.6 EoGRE

Ethernet over GRE (EoGRE) allows for the aggregating of multicast traffic. It enables the bridging of the Ethernet traffic coming from an end host, and encapsulates the traffic in Ethernet packets over an IP GRE tunnel.

### Enable EoGRE

Configuration	
Item	Setting
▶ EoGRE Tunnel	<input type="checkbox"/> Enable
▶ Max. Concurrent EoGRE Tunnels	4

Enable EoGRE Window		
Item	Value setting	Description
<b>EoGRE Tunnel</b>	Unchecked by default	Click the <b>Enable</b> box to enable EoGRE function.
<b>Max. Concurrent EoGRE Tunnels</b>	Depends on Product specification.	The specified value will limit the maximum number of simultaneous EoGRE tunnel connection. The default value can be different for the purchased model.
<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

### Create/Edit EoGRE tunnel

EoGRE Tunnel List									
		Add	Delete						
ID	Tunnel Name	Interface	Tunnel IP	Remote IP	MTU	Key	TTL	Enable	Actions

When **Add/Edit** button is applied, an EoGRE Rule Configuration screen will appear

EoGRE Rule Configuration	
Item	Setting
▶ Tunnel Name	EoGRE #1
▶ Interface	WAN1 ▼
▶ Tunnel IP	IP: <input type="text"/> MASK: -- select one -- ▼ (Optional)
▶ Remote IP	<input type="text"/>
▶ MTU	<input type="text"/> (Optional)
▶ Key	<input type="text"/> (Optional)
▶ TTL	<input type="text"/> (Optional)
▶ Port-based VLAN ID Interface	None ▼
▶ Tunnel	<input type="checkbox"/> Enable

EoGRE Rule Configuration Window		
Item	Value setting	Description
<b>Tunnel Name</b>	A required setting	Enter a tunnel name. Enter a name that is easy for you to identify. <b>Value Range:</b> 1 ~ 8 characters.
<b>Interface</b>	1. A required setting 2. <b>WAN 1</b> is selected by default	Select the interface on which EoGRE tunnel is to be established. It can be the available WAN and LAN interfaces.
<b>Tunnel IP</b>	An Optional setting	Enter the Tunnel IP address and corresponding subnet mask.
<b>Remote IP</b>	A required setting	Enter the Remote IP address of remote EoGRE tunnel gateway. Normally this is the public IP address of the remote EoGRE gateway.
<b>MTU</b>	1. An Optional setting 2. Blank is set by default	<b>MTU</b> refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. When set to blank, the router selects the best MTU for best Internet connection performance. <b>Value Range:</b> 1 ~ 1500.
<b>Key</b>	An Optional setting	Enter the Key for the EoGRE connection. <b>Value Range:</b> 0 ~ 4294967295.
<b>TTL</b>	1. An Optional setting 2. 1 to 255 range	Specify <b>TTL</b> hop-count value for this EoGRE tunnel. <b>Value Range:</b> 1 ~ 255.
<b>Port-based VLAN ID Interface</b>	None is default	System will bridge the EoGRE interface and the Port-based VLAN Interface which user configured in VLAN setting page.
<b>Tunnel</b>	Unchecked by default	Check <b>Enable</b> box to enable this EoGRE tunnel.
<b>Save</b>	N/A	Click <b>Save</b> button to save the settings.

## TAG ID List

When **Add/Edit** button is applied, a TAG ID Rule Configuration screen will appear

TAG ID List
Add
Delete

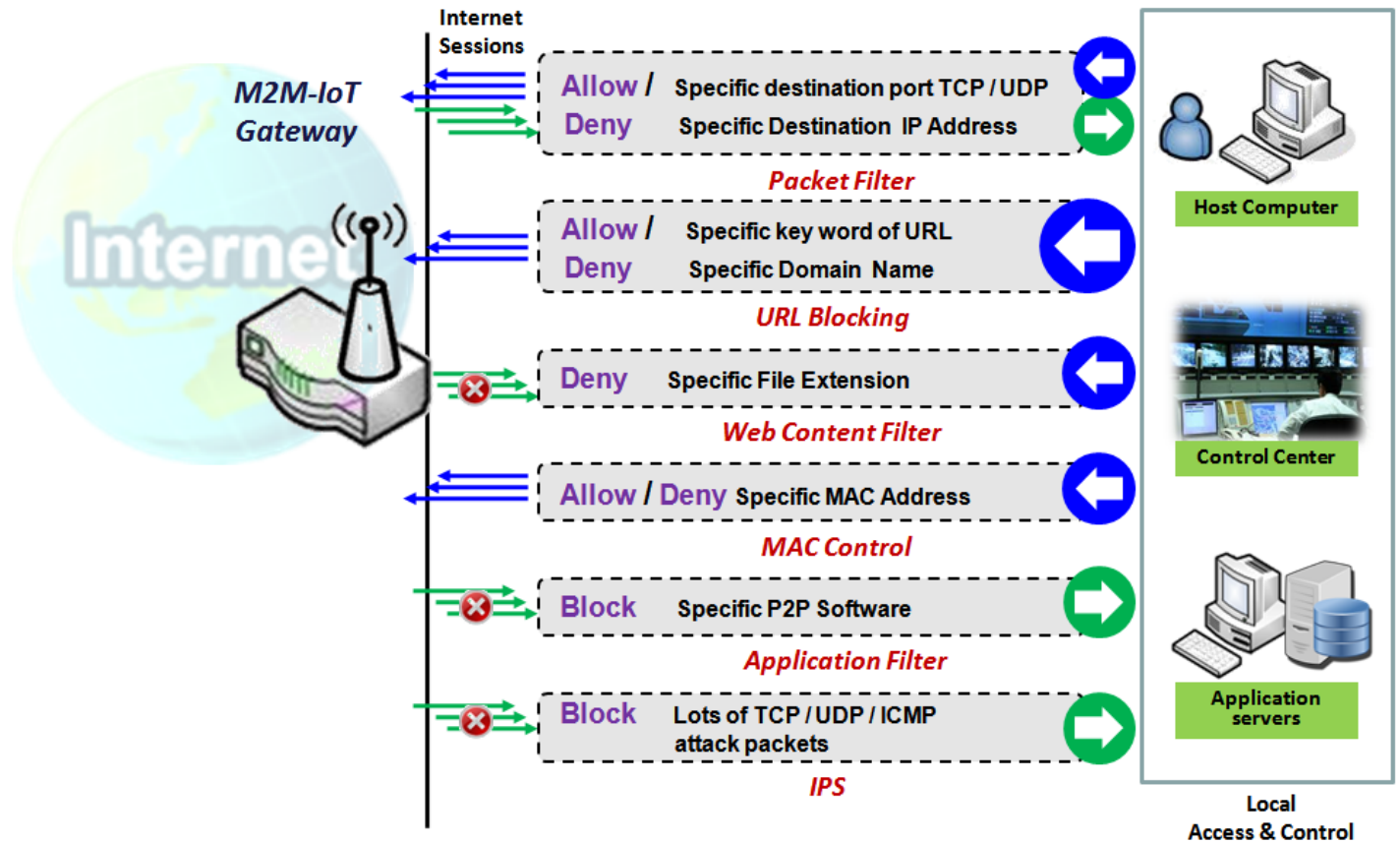
ID	TAG ID	MTU	VLAN ID Interface	Enable	Actions
TAG ID List Save					
Item	Setting				
TAG ID	<input type="text"/>				
MTU	<input type="text"/> (Optional)				
Tag-based VLAN ID Interface	None ▼				
Enable	<input type="checkbox"/>				
Save					

TAG ID List Window		
Item	Value setting	Description
<b>TAG ID</b>	A required setting	Enter the TAG ID. <b>Value Range:</b> 1 ~ 4096.
<b>MTU</b>	1. An Optional setting 2. Blank is set by default	<b>MTU</b> refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. When set to blank, the router selects the best MTU for best Internet connection performance. <b>Value Range:</b> 1 ~ 1500.

## AIR PACE

<b>Tag-based VLAN ID Interface</b>	None is default	System will create a “GTX.Y” interface (X-> index, Y->tagid), and bridge it with the Tag-based VLAN Interface which user configured in VLAN setting page.
<b>Enable</b>	Unchecked by default	Check <b>Enable</b> box to enable this TAG ID rule.
<b>Save</b>	N/A	Click <b>Save</b> button to save the settings

## 6.2 Firewall



The firewall functions include Packet Filter, URL Blocking, Content Filter, MAC Control, Application Filter, IPS and some firewall options. The supported functions may differ depending on specific model.

## 6.2.1 Packet Filter

Configuration

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

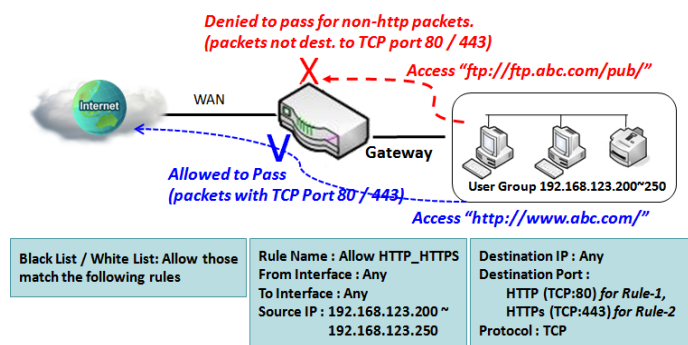
Packet Filter List

AddDelete

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

The "Packet Filter" function lets you define some filtering rules for incoming and outgoing packets. So the gateway can control what packets are allowed or blocked. 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, a time schedule for which the rule will be active should be created.

### Packet Filter with White List Scenario



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

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

### Packet Filter Setting

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

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



## Enable Packet Filter

Configuration	
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
<b>Packet Filter</b>	The box is unchecked by default	Check the <b>Enable</b> box to activate Packet Filter function
<b>Black List / 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 whitelist the packets to pass and the rest will be blocked.
<b>Log Alert</b>	The box is 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.

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

When **Add** button is applied, **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"/> - <input type="text"/>
▶ Destination Port	<input type="text" value="User-defined Service"/> <input type="text"/> - <input type="text"/>
▶ 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, can be any text 2. A Required setting	Enter a packet filter rule name. Enter a name that is easy for you to remember. <b>Value Range: 1 ~ 30 characters.</b>
<b>From Interface</b>	1. A 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. Or <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. A 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. Or <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. A 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 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>Destination IP</b>	1. A Required setting	This field is to specify the <b>Destination IP address</b> .

	<p>2. By default <b>Any</b> is selected</p>	<p>Select <b>Any</b> to filter packets that are entering to any IP addresses.</p> <p>Select <b>Specific IP Address</b> to filter packets entering to an IP address entered in this field.</p> <p>Select <b>IP Range</b> to filter packets entering to a specified range of IP address entered in this field.</p> <p>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.</p>
<b>Source MAC</b>	<p>1. A Required setting</p> <p>2. By default <b>Any</b> is selected</p>	<p>This field is to specify the <b>Source MAC address</b>.</p> <p>Select <b>Any</b> to filter packets coming from any MAC addresses.</p> <p>Select <b>Specific MAC Address</b> to filter packets coming from a MAC address.</p> <p>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.</p>
<b>Protocol</b>	<p>1. A Required setting</p> <p>2. By default <b>Any(0)</b> is selected</p>	<p>For <b>Protocol</b>, select <b>Any</b> to filter any protocol packets</p> <p>Then 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>Then 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: 1 ~ 65535 for Source Port, Destination Port.</b></p>
		<p>For <b>Protocol</b>, select <b>ICMPv4</b> to filter ICMPv4 packets</p>
		<p>For <b>Protocol</b>, select <b>TCP</b> to filter <b>TCP</b> packets</p> <p>Then 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>Then 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: 1 ~ 65535 for Source Port, Destination Port.</b></p>
		<p>For <b>Protocol</b>, select <b>UDP</b> to filter <b>UDP</b> packets</p> <p>Then 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>Then 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: 1 ~ 65535 for Source Port, Destination Port.</b></p>
		<p>For <b>Protocol</b>, select <b>GRE</b> to filter <b>GRE</b> packets</p>
		<p>For <b>Protocol</b>, select <b>ESP</b> to filter <b>ESP</b> packets</p>
		<p>For <b>Protocol</b>, select <b>SCTP</b> to filter <b>SCTP</b> packets</p>
		<p>For <b>Protocol</b>, select <b>User-defined</b> to filter packets with specified port number.</p>

		Then enter a port number in <b>Protocol Number</b> box.
<b>Time Schedule</b>	A Required setting	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>	The box is 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>X</b> to cancel the settings and back to last page.

## 6.2.2 URL Blocking

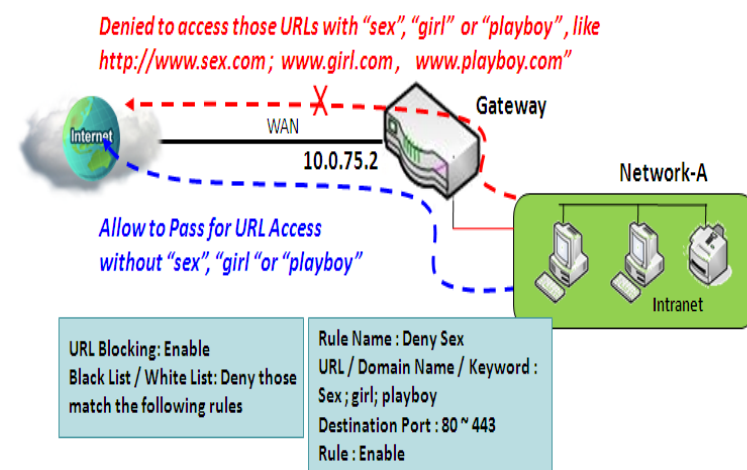
The "URL Blocking" function lets you define blocking or allowing rules for incoming and outgoing Web request packets. With defined rules, the gateway can control the Web requests containing the complete URL, partial domain name, or pre-defined keywords. For example, one can filter out or allow only Web 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. Additionally, a certain 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 the Web requests with some dedicated patterns, he can use the "URL Blocking" function to block specific Web requests by defining the blacklist as shown in above diagram. Certainly, when the administrator wants to allow only the Web requests with some dedicated patterns to go through the gateway, he can also use the "URL Blocking" function by defining the white list to meet the requirement.

As shown in the diagram, enable the URL blocking function and create the first rule to

deny the Web requests with "sex" or "sexygirl" patterns and the other to deny the Web requests with "playboy" pattern to go through the gateway. System will block the Web requests with "sex", "sexygirl" or "playboy" patterns to pass through the gateway.

## URL Blocking Setting

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

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

The "Configuration" window lets you activate the URL blocking function and specify blacklisting or whitelisting the packets defined in the "URL Blocking Rule List" entry. In addition, log alerting can be enabled to record on-going events for any disallowed Web request packets.

The "URL Blocking Rule List" window lists all your defined URL blocking rule entries. And finally, 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>	The box is unchecked by default	Check the <b>Enable</b> box to activate URL Blocking function.
<b>Black List / White List</b>	<b>Deny those match the following rules</b> is set by default	Specify the URL Blocking Policy, either Black List or White List. Black List: 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>	The box is 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

### Create/Edit URL Blocking Rules

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

URL Blocking Rule List								
		Add	Delete					
ID	Rule Name	Source IP	Source MAC	URL / Domain Name / Keyword	Destination Port	Time Schedule	Enable	Actions

# AIR PACE

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

URL Blocking Rule Configuration	
Item	Setting
▶ Rule Name	Rule1
▶ Source IP	Any ▼
▶ Source MAC	Any ▼
▶ URL / Domain Name / Keyword	
▶ Destination Port	Any ▼
▶ Time Schedule Rule	(0) Always ▼
▶ Rule	<input type="checkbox"/> Enable

URL Blocking Rules Configuration		
Item	Value setting	Description
<b>Rule Name</b>	1. String format, can be any text 2. A Required setting	Specify an URL Blocking rule name. Enter a name that is easy to understand.
<b>Source IP</b>	1. A Required setting 2. <b>Any</b> is set by default	<p>This field is to specify the <b>Source IP address</b>.</p> <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 become available. Refer to <b>Object Definition &gt; Grouping &gt; Host grouping</b>.</li> </ul>
<b>Source MAC</b>	1. A Required setting 2. <b>Any</b> is set by default	<p>This field is to specify the <b>Source MAC address</b>.</p> <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 become available. Refer to <b>Object Definition &gt; Grouping &gt; Host grouping</b>.</li> </ul>
<b>URL / Domain Name / Keyword</b>	1. A Required setting 2. Supports a maximum of 10 Keywords in a rule by using the delimiter “;”.	<p>Specify URL, Domain Name, or Keyword list for URL checking.</p> <ul style="list-style-type: none"> <li>In the <b>Black List</b> mode, if a matched rule is found, the packets will be dropped.</li> <li>In the <b>White List</b> mode, if a matched rule is found, the packets will be accepted and the others which don't match any rule will be dropped.</li> </ul>
<b>Destination Port</b>	1. A Required setting 2. <b>Any</b> is set by default	<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>	A 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>X</b> button to cancel the changes and back to last page.

## 6.2.3 MAC Control

Configuration

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	▼ Copy to

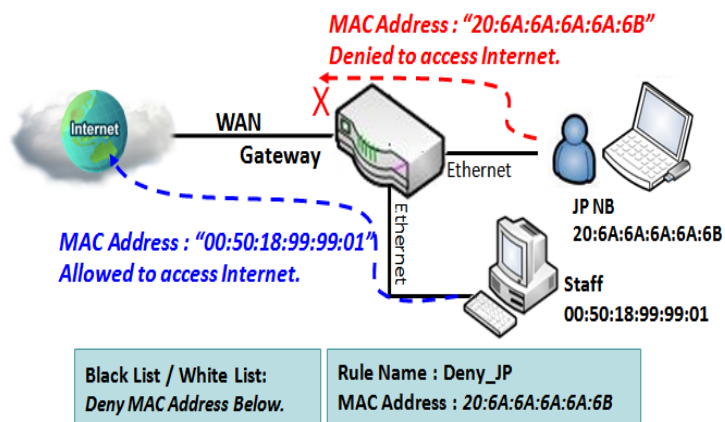
MAC Control Rule List

Add Delete

ID	Rule Name	MAC Address	Time Schedule Rule	Enable	Actions
----	-----------	-------------	--------------------	--------	---------

The "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, he can use the "MAC Control" function to reject with 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" is 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:6B.

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



## 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

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	▼ <input type="button" value="Copy to"/>

Configuration Window		
Item	Value setting	Description
<b>MAC Control</b>	The box is unchecked by default	Check the <b>Enable</b> box to activate the MAC filter function
<b>Black List / White List</b>	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 whitelist the packets to pass and the rest will be blocked.
<b>Log Alert</b>	The box is unchecked by default	Check the <b>Enable</b> box to activate to activate Event Log.
<b>Known MAC from LAN PC List</b>	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.
<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 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
Add
Delete

ID	Rule Name	MAC Address	Time Schedule Rule	Enable	Actions
----	-----------	-------------	--------------------	--------	---------

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

MAC Control Rule Configuration

Rule Name	MAC Address (Use : to Compose)	Time Schedule	Enable
Rule1		(0) Always ▼	<input type="checkbox"/>
Save			

MAC Control Rule Configuration		
Item	Value setting	Description
<b>Rule Name</b>	1. String format, can be any text 2. Required setting	Enter a MAC Control rule name. Enter a name that is easy for you to remember.
<b>MAC Address (Use: to Compose)</b>	1. MAC Address string Format 2. Required setting	Specify the <b>Source MAC Address</b> to filter rule.
<b>Time Schedule</b>	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>
<b>Enable</b>	The box is unchecked by default.	Click <b>Enable</b> box to activate this rule, and 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

## 6.2.4 IPS

Configuration	
Item	Setting
▶ IPS	<input type="checkbox"/> Enable
▶ Log Alert	<input type="checkbox"/> Enable

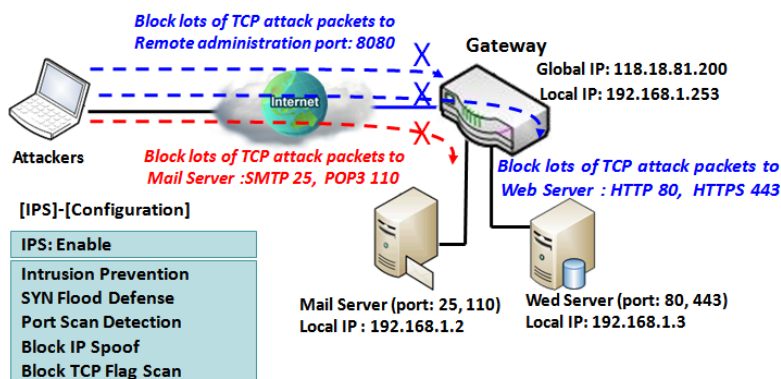
  

Intrusion Prevention	
Item	Setting
▶ SYN Flood Defense	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)
▶ UDP Flood Defense	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)
▶ ICMP Flood Defense	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)
▶ Port Scan Defense	<input type="checkbox"/> Enable <input type="text" value="200"/> Packets/second (10~10000)

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

Intrusion Prevention System (IPS) is 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 system will record Intrusion events when corresponding intrusions are detected.

### IPS Scenario



As shown in the diagram, the gateway serves as an E-mail server, Web Server and also provides TCP port 8080 for remote administration. So, remote users or unknown users can request those services from Internet. With IPS enabled, the gateway can detect incoming attack packets, including the TCP ports (25, 80, 110, 443 and 8080) with services. It will block the attack packets and let the normal packets pass through the 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	
Item	Setting
▶ IPS	<input type="checkbox"/> Enable
▶ Log Alert	<input type="checkbox"/> Enable

Configuration Window		
Item	Value setting	Description
IPS	The box is unchecked by default	Check the <b>Enable</b> box to activate IPS function
Log Alert	The box is 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.

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 Defense	<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 Defense	<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. A 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. The box is 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.	<b>Value Range: 10 ~ 10000.</b>
<b>Port Scan Defection</b>	1. A Required setting	Click <b>Enable</b> box to activate this intrusion prevention rule and enter the traffic threshold in this field.
	2. The box is unchecked by default.	
	3. Traffic threshold is set to 200 by default	
	4. The value range can be from 10 to 10000.	<b>Value Range: 10 ~ 10000.</b>
<b>Block Land Attack</b>		
<b>Block Ping of Death</b>		
<b>Block IP Spoof</b>		
<b>Block TCP Flag Scan</b>		
<b>Block Smurf</b>		
<b>Block Traceroute</b>		
<b>Block Fraggle Attack</b>		
<b>Attack</b>	The box is unchecked by default.	Click <b>Enable</b> box to activate this intrusion prevention rule.

# AIR PACE

ARP Spoofing Defence	1. A Required setting	Click <b>Enable</b> box to activate this intrusion prevention rule and enter the traffic threshold in this field. <b><u>Value Range: 10 ~ 10000.</u></b>
	2. The box is unchecked by default.	
	3. Traffic threshold is set to 300 by default	
	4. The value range can be from 10 to 10000.	
Save	NA	Click <b>Save</b> to save the settings
Undo	NA	Click <b>Undo</b> to cancel the settings

## 6.2.5 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

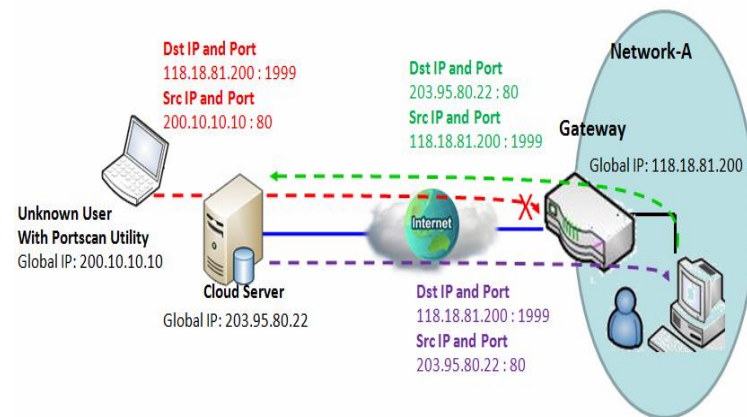
ID	Interface	Protocol	IP	Subnet Mask	Service Port	Enable	Action
1	All WAN	HTTP	Any IP	N/A	80	<input checked="" type="checkbox"/>	Edit
2	All WAN	HTTPS	Any IP	N/A	443	<input checked="" type="checkbox"/>	Edit
3	All WAN	HTTP	Any IP	N/A	80	<input type="checkbox"/>	Edit
4	All WAN	HTTP	Any IP	N/A	80	<input 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 this packet is valid.

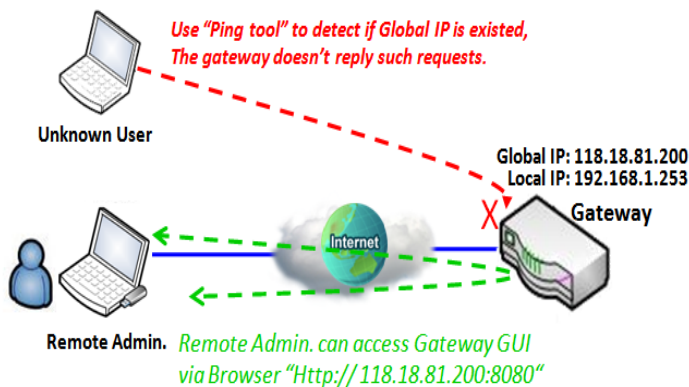
“Discard Ping from WAN” makes any host on the WAN side unable to ping this gateway. And finally, “Remote Administrator Hosts” enables you to perform administration task from a remote host. If this feature is enabled, only specified IP address(es) can perform remote administration.

## 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 access a cloud server through the gateway. Sometimes, unknown users will simulate the packets but use different source IP to masquerade. With the SPI feature 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 reply to any ICMP packets. Enable the Discard Ping from WAN function to prevent security leak when local users surf the internet.

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



Firewall Options Setting

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

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

Enable Firewall Options

Firewall Options	
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
Stealth Mode	The box is unchecked by default	Check the <b>Enable</b> box to activate the Stealth Mode function
SPI	The box is checked by default	Check the <b>Enable</b> box to activate the SPI function
Discard Ping from WAN	The box is unchecked by default	Check the <b>Enable</b> box to activate the Discard Ping from WAN function

Define Remote Administrator Host

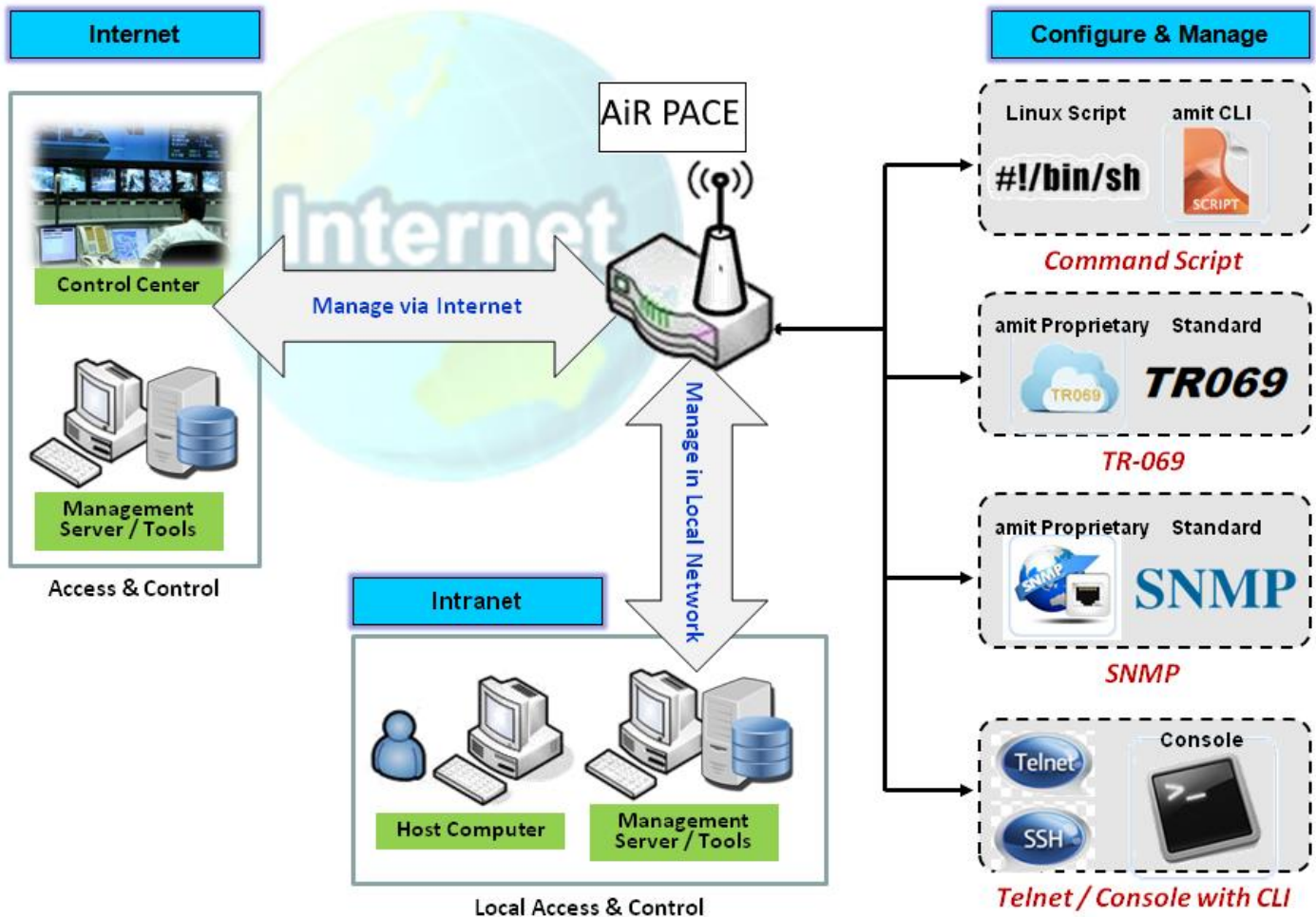
The router allows network administrator to manage router remotely. The network administrator can assign specific IP address and service port to allow accessing the router.

Remote Administrator Host Definition							
ID	Interface	Protocol	IP	Subnet Mask	Service Port	Enable	Action
1	All WAN	HTTP	Any IP	N/A	80	<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

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>	A Required setting	<p>This field is to specify the remote host to assign access right for remote access. Select <b>Any IP</b> to allow any remote hosts</p> <p>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.</p>
<b>Service Port</b>	1. 80 for HTTP by default 2. 443 for HTTPS by default	<p>This field is to specify a Service Port to HTTP or HTTPS connection.</p> <p><b>Value Range:</b> 1 ~ 65535.</p>
<b>Enabling the rule</b>	The box is 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 7 Administration

### 7.1 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 those configurations in the "Configure & Manage" section.

## 7.1.1 Command Script

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

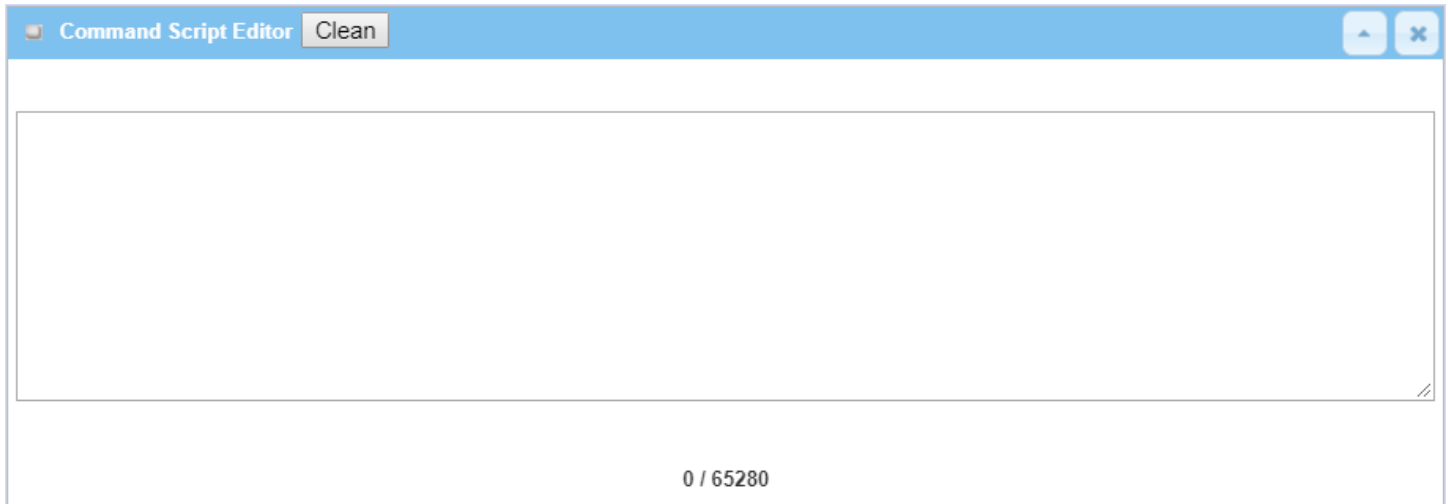
Go to **Administration > Command Script > Configuration** Tab.

### 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
<b>Command Script</b>	The box is unchecked by default	Check the <b>Enable</b> box to activate the Command Script function.
<b>Backup Script</b>	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.
<b>Upload Script</b>	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.
<b>Script Name</b>	1. An Optional setting 2. Any valid file name	Specify a script file name for script backup, or display the selected upload script file name. <b>Value Range:</b> 0 ~ 32 characters.
<b>Version</b>	1. An Optional setting 2. Any string	Specify the version number for the applied Command script. <b>Value Range:</b> 0 ~ 32 characters.
<b>Description</b>	1. An Optional setting 2. Any string	Enter a short description for the applied Command script.
<b>Update time</b>	N/A	This records the upload time for the last commad script upload.

## Edit/Backup Plain Text Command Script



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

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

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

Configuration Content		
Key	Value setting	Description
<b>OPENVPN_ENABLED</b>	1: enable 0: disable	Enable or disable OpenVPN Client function.
<b>OPENVPN_DESCRIPTION</b>	A Required Setting	Specify the tunnel name for the OpenVPN Client connection.
<b>OPENVPN_PROTO</b>	udp tcp	Define the <b>Protocol</b> for the OpenVPN Client. <ul style="list-style-type: none"> <li>Select <b>TCP</b> or <b>TCP /UDP</b> -&gt;The OpenVPN will use TCP protocol, and <b>Port</b> will be set as 443 automatically.</li> <li>Select <b>UDP</b> -&gt; The OpenVPN will use UDP protocol, and <b>Port</b> will be set as 1194 automatically.</li> </ul>
<b>OPENVPN_PORT</b>	A Required Setting	Specify the <b>Port</b> for the OpenVPN Client to use.
<b>OPENVPN_REMOTE_IPADDR</b>	IP or FQDN	Specify the <b>Remote IP/FQDN</b> of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the IP address or FQDN.
<b>OPENVPN_PING_INTVL</b>	seconds	Specify the time interval for OpenVPN keep-alive checking.
<b>OPENVPN_PING_TOUT</b>	seconds	Specify the timeout value for OpenVPN Client keep-alive checking.

<b>OPENVPN_COMP</b>	Adaptive	Specify the <b>LZO Compression</b> algorithm for OpenVPN client.
<b>OPENVPN_AUTH</b>	Static Key/TLS	Specify the authorization mode for the OpenVPN tunnel. <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> need to be specified as well.</li> </ul>
<b>OPENVPN_CA_CERT</b>	A Required Setting	Specify the Trusted CA certificate for the OpenVPN client. It will go through Base64 Conversion.
<b>OPENVPN_LOCAL_CERT</b>	A Required Setting	Specify the local certificate for OpenVPN client. It will go through Base64 Conversion.
<b>OPENVPN_LOCAL_KEY</b>	A Required Setting	Specify the local key for the OpenVPN client. It will go through Base64 Conversion.
<b>OPENVPN_EXTRA_OPTS</b>	Options	Specify the extra options setting for the OpenVPN client.
<b>IP_ADDR1</b>	Ip	Ethernet LAN IP
<b>IP_NETM1</b>	Net mask	Ethernet LAN MASK
<b>PPP_MONITORING</b>	1: enable 0: disable	When the Network Monitoring feature is enabled, the router will use DNS Query or ICMP to periodically check Internet connection – connected or disconnected.
<b>PPP_PING</b>	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.
<b>PPP_PING_IPADDR</b>	IP	Specify an IP address as the target for sending DNS query/ICMP request.
<b>PPP_PING_INTVL</b>	seconds	Specify the time interval for between two DNS Query or ICMP checking packets.
<b>STARTUP</b>	Script file	For the configurations that can be configured with standard Linux commands, you can put them in a script file, and apply the script file with STARTUP command. For example, STARTUP=#!/bin/sh STARTUP=echo “startup done” > /tmp/demo

## Plain Text System Configuration with Telnet

In addition to the web-style plain text configuration as mentioned above, the gateway system also allows the 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
<b>clone</b>	<i>Output file</i>	Duplicate the configuration content from database and store 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.
<b>commit</b>	a existing file	Commit the configuration content to database.

# AIR PACE

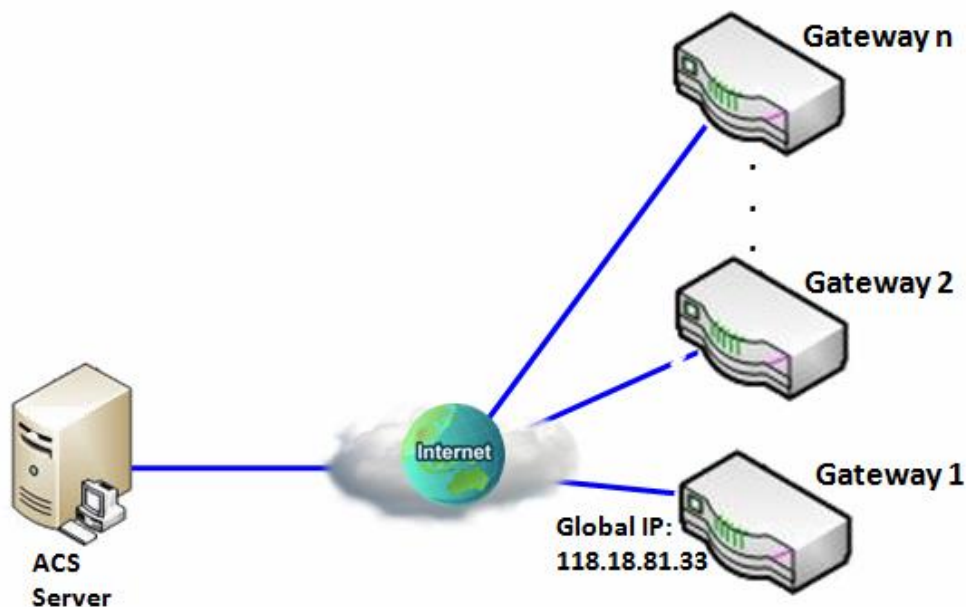
		(ex: <i>txtConfig commit /tmp/config</i> )
<b>enable</b>	NA	Enable plain text system config. (ex: <i>txtConfig enable</i> )
<b>disable</b>	NA	Disable plain text system config. (ex: <i>txtConfig disable</i> )
<b>run_immediately</b>	NA	Apply the configuration content that has been committed in database. (ex: <i>txtConfig run_immediately</i> )
<b>run_immediately</b>	a existing file	Assign a configuration file to apply. (ex: <i>txtConfig run_immediately /tmp/config</i> )

## 7.1.2 TR-069

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

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

Scenario - Managing deployed gateways through an ACS Server



### Scenario Application Timing

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

### Scenario Description

The ACS server can configure, upgrade with latest firmware 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



# AIR PACE

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

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

Configuration Path	[TR-069]-[Configuration]
TR-069	■ <i>Enable</i>
ACS URL	<a href="http://qa.acslite.com/cpe.php">http://qa.acslite.com/cpe.php</a>
ACS User Name	<i>ACSUserName</i>
ACS Password	<i>ACSPassword</i>
ConnectionRequest Port	<i>8099</i>
ConnectionRequest User Name	<i>ConnReqUserName</i>
ConnectionRequest Password	<i>ConnReqPassword</i>
Inform	■ <i>Enable</i> <i>Interval 900</i>

## 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 firmware 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.

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 to 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 for 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 be done 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

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 <input type="text"/>
▶ 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	<div><input checked="" type="radio"/> default</div> <div><input type="radio"/> Select from Certificate List</div> <div>Certificate: <input type="text" value="CA"/> ▾</div>

TR-069		
Item	Value setting	Description
TR-069	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 setting up basic network WAN-1 ~ WAN-n, you can choose WAN-1 ~ WAN-n When you finish setting Security > VPN > IPSec/OpenVPN/PPTP/L2TP/GRE, you can choose IPSec/OpenVPN/PPTP/L2TP/GRE tunnel, the interface is 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 fully complies with TR-069. <b>ACS Cloud Data Model:</b> Select this data model if you intend to use Cloud ACS Server to managing the deployed gateways.
<b>ACS URL</b>	A Required setting	You can ask ACS manager to provide ACS URL and manually set
<b>ACS Username</b>	A Required setting	You can ask ACS manager to provide ACS username and manually set
<b>ACS Password</b>	A Required setting	You can ask ACS manager to provide ACS password and manually set
<b>ConnectionRequest Port</b>	1. A 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>	A Required setting	You can ask ACS manager to provide ACS ConnectionRequest Username and manually set
<b>ConnectionRequest Password</b>	A 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 setting **ACS URL ACS Username ACS Password**, your gateway (CPE, Client Premium Equipment) can send information to ACS Server.

When you finish set **ConnectionRequest Port ConnectionRequest Username ConnectionRequest Password**, ACS Server can ask the gateway (CPE) to send information to ACS Server.

## Enable STUN Server

STUN Settings

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.

## 7.1.3 SNMP

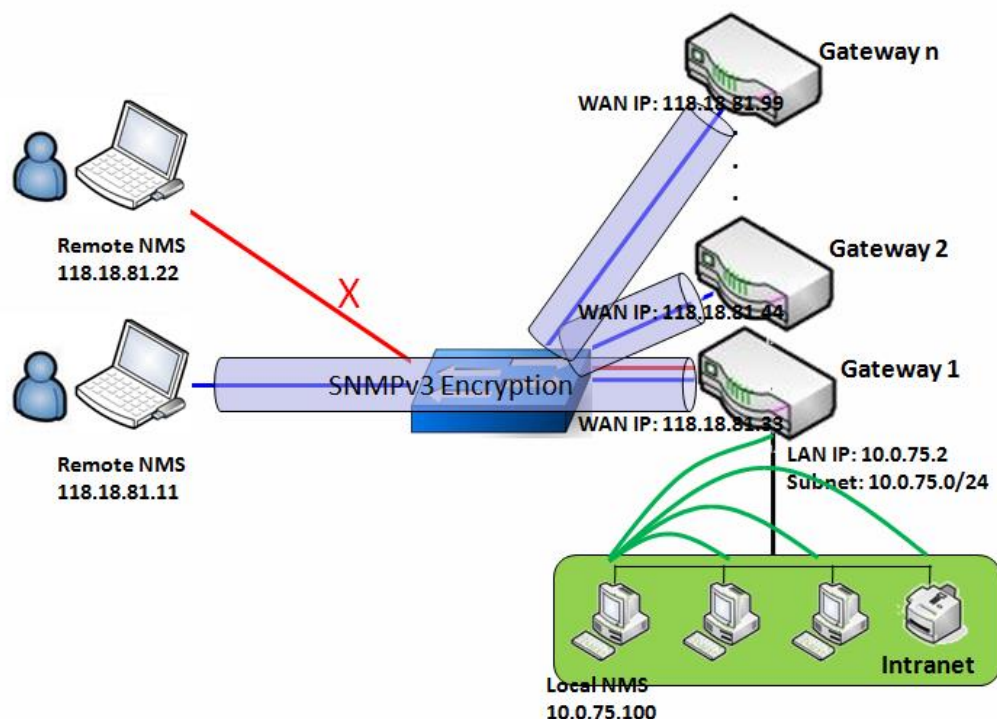
In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

In typical SNMP uses, one or more administrative computers, called managers, have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes, at all times, a software component called an agent which reports information via SNMP to the manager.

SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. These hierarchies, and other metadata (such as type and description of the variable), are described by Management Information Bases (MIBs).

The device supports several public MIBs and one private MIB for the SNMP agent. The supported MIBs are as follow: MIB-II (RFC 1213), IF-MIB, IP-MIB, TCP-MIB, UDP-MIB, SMIv1 and SMIv2, SNMPv2-TM and SNMPv2-MIB, and AMIB (a Proprietary MIB)

### SNMP Management Scenario



### Scenario Application Timing

There are two application scenarios of SNMP Network Management Systems (NMS). The first is where the local NMS is in the Intranet and manages all devices that support SNMP protocol in the Intranet.

Another one is the Remote NMS manages devices whose WAN interfaces are connected together by using a switch or a router with UDP forwarding. If you want to manage some devices and they all support SNMP protocol, use either one application scenario, especially the management of devices in the Intranet. In managing devices in the Internet, the TR-069 is the better solution. Please refer to last sub-section.

## Scenario Description

The NMS server can monitor and configure the managed devices by using SNMP protocol, and those devices are located at where UDP packets can reach from NMS.

The managed devices report urgent trap events to the NMS servers.

Using SNMPv3 version of protocol can protect the transmitting of SNMP commands and responses.

The remote NMS with privileged IP address can manage the devices, but other remote NMS cannot.

## Parameter Setup Example

The following tables list the parameter configuration as an example for the Gateway 1 in above diagram with "SNMP" enabling at LAN and WAN interfaces.

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

Configuration Path	[SNMP]-[Configuration]
SNMP Enable	■ LAN ■ WAN
Supported Versions	■ v1 ■ v2c ■ v3
Get / Set Community	ReadCommunity / WriteCommunity
Trap Event Receiver 1	118.18.81.11
WAN Access IP Address	118.18.81.11

Configuration Path	[SNMP]-[User Privacy Definition]		
ID	1	2	3
User Name	UserName1	UserName2	UserName3
Password	Password1	Password2	Disable
Authentication	MD5	SHA-1	Disable
Encryption	DES	Disable	Disable
Privacy Mode	authPriv	authNoPriv	noAuthNoPriv
Privacy Key	12345678	Disable	Disable
Authority	Read/Write	Read	Read
Enable	■ Enable	■ Enable	■ Enable

## Scenario Operation Procedure

In above diagram, the NMS server can manage multiple devices in the Intranet or a UDP-reachable network. The "Gateway 1" is one of the managed devices, and it has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. It serves as a NAT router.

At the first stage, the NMS manager prepares related information for all managed devices and records

them in the NMS system. Then NMS system gets the status of all managed devices by using SNMP get commands.

When the manager wants to configure the managed devices, the NMS system allows him to do that by using SNMP set commands. The "UserName1" account is used if the manager uses SNMPv3 protocol for configuring the "Gateway 1". Only the "UserName1" account can let the "Gateway 1" accept the configuration from the NMS since the authority of the account is "Read/Write".

Once a managed device has an urgent event to send, the device will issue a trap to the Trap Event Receivers. The NMS itself could be one among them.

If you want to secure the transmitted SNMP commands and responses between the NMS and the managed devices, use SNMPv3 version of protocol.

The remote NMS without privilege IP address can't manage the "Gateway 1", since "Gateway 1" allows only the NMS with privilege IP address can manage it via its WAN interface.

## SNMP Setting

Go to **Administration > Configure & Manage > SNMP** tab.

The SNMP allows user to configure SNMP relevant setting which includes 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></td> <td>-</td> <td></td> <td><input type="checkbox"/> Enable</td> </tr> <tr> <td></td> <td>-</td> <td></td> <td><input type="checkbox"/> Enable</td> </tr> <tr> <td></td> <td>-</td> <td></td> <td><input type="checkbox"/> Enable</td> </tr> <tr> <td></td> <td>-</td> <td></td> <td><input type="checkbox"/> Enable</td> </tr> <tr> <td></td> <td>-</td> <td></td> <td><input type="checkbox"/> Enable</td> </tr> </tbody> </table>		-		<input type="checkbox"/> Enable		-		<input type="checkbox"/> Enable		-		<input type="checkbox"/> Enable		-		<input type="checkbox"/> Enable		-		<input type="checkbox"/> Enable
	-		<input type="checkbox"/> Enable																		
	-		<input type="checkbox"/> Enable																		
	-		<input type="checkbox"/> Enable																		
	-		<input type="checkbox"/> Enable																		
	-		<input type="checkbox"/> Enable																		

SNMP Item	Value setting	Description
<b>SNMP Enable</b>	1. The boxes are unchecked by default	<p>Select the interface for the SNMP and enable SNMP functions.</p> <p>When Checking the <b>LAN</b> box, it will activate SNMP functions and you can access SNMP from LAN side;</p> <p>When Check the <b>WAN</b> box, it will activate SNMP functions and you can access SNMP from WAN side.</p>
<b>WAN Interface</b>	1. A Required setting 2. <b>ALL WANs is selected by default</b>	<p>Specify the WAN interface that a remote SNMP host can access to the device.</p> <p>By default, <b>All WANs</b> is selected, and there is no limitation for the WAN interface.</p>
<b>Supported Versions</b>	1. A Required setting 2. The boxes are unchecked by default	<p>Select the version for the SNMP</p> <p>When Check the <b>v1</b> box.</p> <p>It means you can access SNMP by version 1.</p> <p>When Check the <b>v2c</b> box.</p> <p>It means you can access SNMP by version 2c.</p> <p>When Check the <b>v3</b> box.</p> <p>It means you can access SNMP by version 3.</p>
<b>SNMP Port</b>	1. String format: any port number	<p>Specify the <b>SNMP Port</b>.</p> <p>You can fill in any port number. But you must ensure the port number is not to</p>



	2. The default SNMP port is <b>161</b> . 3. A Required setting	be used. <u>Value Range:</u> 1 ~ 65535.
<b>Limited Remote Access IP</b>	1. String format: any IPv4 address 2. It is an 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 certain 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 left it as 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 user. The router supports up to a maximum of 10 community sets.

Multiple Community List <span>Add</span> <span>Delete</span> <span>↶</span> <span>✕</span>			
ID	Community	Enable	Actions

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

Multiple Community Rule Configuration	
Item	Setting
▶ Community	<span>Read Only ▾</span> <input type="text"/>
▶ Enable	<input checked="" type="checkbox"/> Enable

Multiple Community Rule Configuration		
Item	Value setting	Description
<b>Community</b>	1. <b>Read Only</b> is selected by default 2. A Required setting 3. String format: any text	Specify this version 1 or version v2c user's community that will be allowed <b>Read Only</b> (GET and GETNEXT) or <b>Read-Write</b> (GET, GETNEXT and SET) access respectively. The maximum length of the community is 32.
<b>Enable</b>	1. The 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 button to apply your changes" to remind user to click 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 user. The router supports up to a maximum of 128 User Privacy sets.

User Privacy List <span>Add</span> <span>Delete</span> <span>↑</span> <span>×</span>										
ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	OID Filter Prefix	Enable	Actions

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

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. A Required setting 2. String format: any text	Specify the <b>User Name</b> for this version 3 user. <b>Value Range:</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> , you must specify the <b>Password</b> for this version 3 user. <b>Value Range:</b> 8 ~ 64 characters.
<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> , you must 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> , you must 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. Selected the <b>noAuthNoPriv</b> .

		<p>You do not use any authentication types and encryption protocols.          Selected the <b>authNoPriv</b>.          You must specify the <b>Authentication</b> and <b>Password</b>.          Selected the <b>authPriv</b>.          You must specify the Authentication, Password, Encryption and Privacy Key.</p>
<b>Privacy Key</b>	1. String format: any text	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 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. The default value is 1 2. A 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. <u><b>Value Range:</b> 1 ~2080768.</u>
<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" remind the user to click 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>X</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												Add	Delete		
ID	Server IP	Server Port	SNMP Version	Community Name	User Name	Password	Privacy Mode	Authentication	Encryption	Privacy Key	Enable	Actions			

When **Add** button is applied, **Trap Event Receiver Rule Configuration** screen will appear. The default SNMP Version is v1. The configuration screen will provide the version 1 required items.

Trap Event Receiver Rule Configuration	
Item	Setting
▶ Server IP	<input type="text"/> (IP Address/FQDN)
▶ Server Port	<input type="text" value="162"/>
▶ SNMP Version	<input type="text" value="v1"/>
▶ Community Name	<input type="text"/>
▶ Enable	<input checked="" type="checkbox"/> Enable

When you select v2c, the configuration screen is exactly the same as that of v1, except the version.

When you select v3, 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	<input type="text" value="v3"/>
▶ Community Name	<input type="text"/>
▶ User Name	<input type="text"/>
▶ Password	<input type="text"/>
▶ Privacy Mode	<input type="text" value="noAuthNoPriv"/>
▶ Authentication	<input type="text" value="None"/>
▶ Encryption	<input type="text" value="None"/>
▶ Privacy Key	<input type="text"/>
▶ Enable	<input checked="" type="checkbox"/> Enable




Trap Event Receiver Rule Configuration		
Item	Value setting	Description
<b>Server IP</b>	1. A Required setting 2. String format: any IPv4 address or FQDN	Specify the trap <b>Server IP</b> or <b>FQDN</b> . The DUT will send trap to the server IP/FQDN.
<b>Server Port</b>	1. String format: any port number 2. The default SNMP trap port is 162 3. A Required setting	Specify the trap <b>Server Port</b> . You can fill in any port number. But you must ensure the port number is not to be used. <i>Value Range: 1 ~ 65535.</i>
<b>SNMP Version</b>	1. <b>v1</b> is selected by default	Select the version for the trap Selected the <b>v1</b> .

		<p>The configuration screen will provide the version 1 required items. Selected the <b>v2c</b>.</p> <p>The configuration screen will provide the version 2c required items. Selected the <b>v3</b>.</p> <p>The configuration screen will provide the version 3 required items.</p>
<b>Community Name</b>	<p>1. A <b>v1</b> and <b>v2c</b> Required setting</p> <p>2. String format: any text</p>	<p>Specify the <b>Community Name</b> for this version 1 or version v2c trap.</p> <p><b>Value Range:</b> 1 ~ 32 characters.</p>
<b>User Name</b>	<p>1. A <b>v3</b> Required setting</p> <p>2. String format: any text</p>	<p>Specify the <b>User Name</b> for this version 3 trap.</p> <p><b>Value Range:</b> 1 ~ 32 characters.</p>
<b>Password</b>	<p>1. A <b>v3</b> Required setting</p> <p>2. String format: any text</p>	<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>Value Range:</b> 8 ~ 64 characters.</p>
<b>Privacy Mode</b>	<p>1. A <b>v3</b> Required setting</p> <p>2. <b>noAuthNoPriv</b> is selected by default</p>	<p>Specify the <b>Privacy Mode</b> for this version 3 trap.</p> <p>Selected the <b>noAuthNoPriv</b>.</p> <p>You do not use any authentication types and encryption protocols.</p> <p>Selected the <b>authNoPriv</b>.</p> <p>You must specify the <b>Authentication</b> and <b>Password</b>.</p> <p>Selected the <b>authPriv</b>.</p> <p>You must specify the Authentication, Password, Encryption and Privacy Key.</p>
<b>Authentication</b>	<p>1. A <b>v3</b> Required setting</p> <p>2. <b>None</b> is selected by default</p>	<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>	<p>1. A <b>v3</b> Required setting</p> <p>2. <b>None</b> is selected by default</p>	<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>	<p>1. A <b>v3</b> Required setting</p> <p>2. String format: any text</p>	<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>	<p>1. The box is checked by default</p>	<p>Click <b>Enable</b> to enable this trap receiver.</p>
<b>Save</b>	N/A	<p>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" remind user to click main page <b>Save</b> button.</p>
<b>Undo</b>	N/A	<p>Click the <b>Undo</b> button to cancel the settings.</p>
<b>Back</b>	N/A	<p>Click the <b>X</b> button to return to last page.</p>

## Specify SNMP MIB-2 System

# AIR PACE

If required, you can also specify the required information the the MIB-2 System.




 **SNMP MIB-2 System**  

Item	Setting
▶ sysContact	<input type="text"/>
▶ sysLocation	<input type="text"/>

Item	Value setting	Description
<b>sysContact</b>	1. An Optional filled setting 2. String format: any text	Specify the contact information forMIB-2 system. <b><u>Value Range:</u></b> 0 ~ 64 characters.
<b>sysLocation</b>	1. An Optional filled setting 2. String format: any text	Specify the location information forMIB-2 system. <b><u>Value Range:</u></b> 0 ~ 64 characters.

## Edit SNMP Options

If you use some particular private MIB, you must fill the enterprise name, number and OID.

 **Options**  

Item	Setting
▶ Enterprise Name	<input type="text" value="Default"/>
▶ Enterprise Number	<input type="text" value="12823"/>
▶ Enterprise OID	1.3.6.1.4.1. <input type="text" value="12823.4.4.9"/>

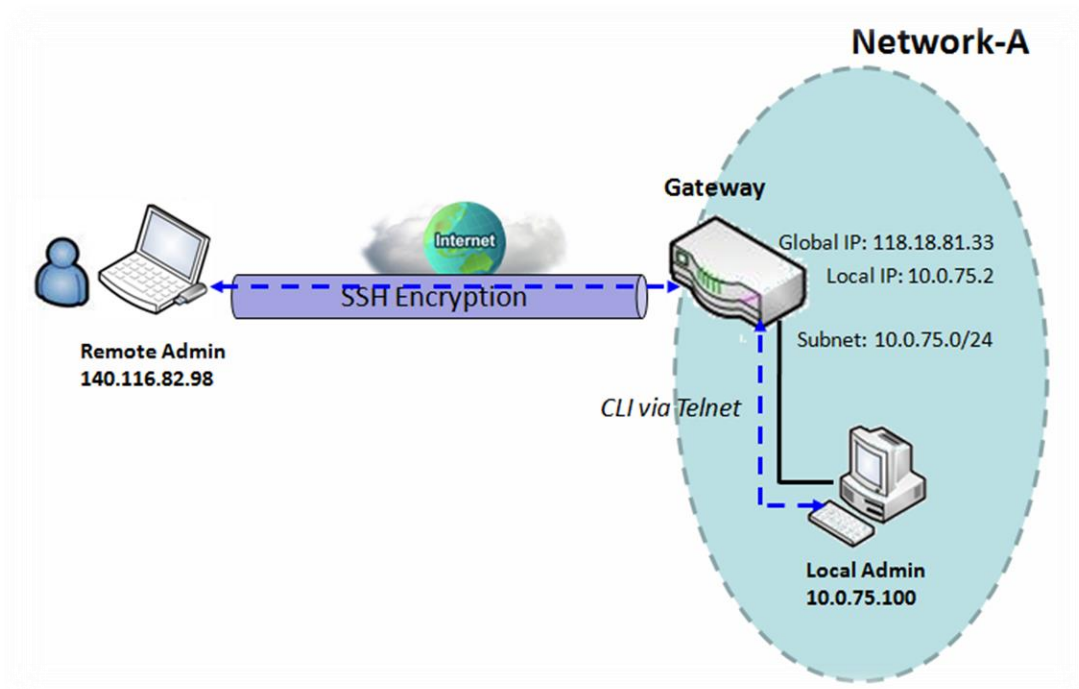
Item	Value setting	Description
<b>Enterprise Name</b>	1. The default value is <b>Default</b> 2. A Required setting 3. String format: any text	Specify the <b>Enterprise Name</b> for the particular private MIB. <b><u>Value Range:</u></b> 1 ~ 10 characters, and only string with A~Z, a~z, 0~9, '-', '_'.
<b>Enterprise Number</b>	The default value is <b>12823</b> (Default Enterprise Number) 2. A Required setting 3. String format: any	Specify the <b>Enterprise Number</b> for the particular private MIB. <b><u>Value Range:</u></b> 1 ~2080768.

	number	
<b>Enterprise OID</b>	<p>1. The default value is 1.3.6.1.4.1.<b>12823.4.4.9</b> (Default Enterprise OID)</p> <p>2. A Required setting</p> <p>3. String format: any legal OID</p>	<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.

## 7.1.4 Telnet & SSH

A command-line interface (CLI), also known as command-line user interface, and console user interface are means of interacting with a computer program where the user (or client) issues commands to the program in the form of successive lines of text (command lines). The interface is usually implemented with a command line shell, which is a program that accepts commands as text input and converts commands to appropriate operating system functions. Programs with command-line interfaces are generally easier to automate via scripting. The device supports both Telnet and SSH (Secure Shell) CLI with default service port 23 and 22, respectively.

### Telnet & SSH Scenario



#### Scenario Application Timing

When the administrator of the gateway wants to manage it from remote site in the Intranet or Internet, he may use "Telnet with CLI" function to do that by using "Telnet" or "SSH" utility.

#### Scenario Description

The Local Admin or the Remote Admin can manage the Gateway by using "Telnet" or "SSH" utility with privileged user name and password.

The data packets between the Local Admin and the Gateway or between the Remote Admin and the Gateway can be plain text or encrypted text. It is suggested that plain text is used in the Intranet for Local Admin to use "Telnet" utility, and encrypted text in the Internet for Remote Admin to use "SSH" utility.



## Parameter Setup Example

The following table lists the parameter configuration as an example for the Gateway in above diagram with "Telnet with CLI" enabling at LAN and WAN interfaces.

Use default values for those parameters that are not mentioned in the table.

Configuration Path	[Telnet & SSH]-[Configuration]
<b>Telnet</b>	LAN: <input checked="" type="checkbox"/> <b>Enable</b> WAN: <input type="checkbox"/> <b>Enable</b> Service Port: <b>23</b>
<b>SSH</b>	LAN: <input checked="" type="checkbox"/> <b>Enable</b> WAN: <input checked="" type="checkbox"/> <b>Enable</b> Service Port: <b>22</b>

## Scenario Operation Procedure

In above diagram, "Local Admin" or "Remote Admin" can manage the "Gateway" in the Intranet or Internet. The "Gateway" is the gateway of Network-A, and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. It serves as a NAT gateway.

The "Local Admin" in the Intranet uses "Telnet" utility with privileged account to log in to the Gateway.

Or the "Remote Admin" in the Internet uses "SSH" utility with privileged account to log in to the Gateway.

The administrator of the gateway can control the device as if she is physically present.

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 (log in) to the device, please configure the related settings and password with care. The password management part allows you to set root password for logging Telnet and SSH.

Configuration

Save

Undo

Item	Setting
Telnet	<div>LAN <input checked="" type="checkbox"/> Enable</div> <div>WAN <input type="checkbox"/> Enable ( WAN-1 <input checked="" type="checkbox"/> WAN-4 <input type="checkbox"/> )</div> <div></div> <div>Service Port 23</div>
SSH	<div>LAN <input checked="" type="checkbox"/> Enable</div> <div>WAN <input type="checkbox"/> Enable ( WAN-1 <input checked="" type="checkbox"/> WAN-4 <input type="checkbox"/> )</div> <div></div> <div>Service Port 22</div>

Configuration		
Item	Value setting	Description
Telnet	<div>1. The LAN Enable box is checked by default.</div> <div>2. By default <b>Service Port</b> is 23.</div>	<div>Check the <b>Enable</b> box to activate the 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><b>Value Range:</b> 1 ~65535.</div>
SSH	<div>3. The LAN Enable box is checked by default.</div> <div>4. By 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><b>Value Range:</b> 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

# AIR PACE

Password Management

Save

Undo

Item	Setting
▶ root	<div>Old Password : <input type="text"/></div> <div>New Password : <input type="text"/></div> <div>New Password Confirmation : <input type="text"/></div>

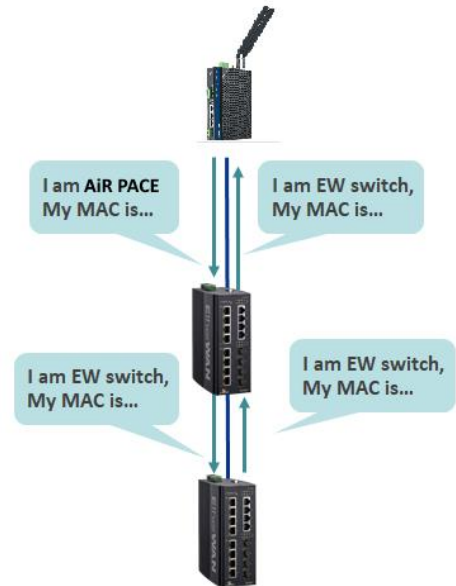
Configuration		
Item	Value setting	Description
root	1. String: any text but no blank character 2. The default password for Telnet is 'wirelessm2m'.	Type old password and specify new password to change root password. <b>Note_1: You are highly recommended to change the default Telnet password with yours before the device is deployed.</b> <b>Note_2: If you have trouble for the default password for 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

## 7.1.5 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

## 7.2 System Operation

System Operation allows the network administrator to manage system, settings such as web-based utility access password change, system information, system time, system log, firmware/configuration backup & restore, and reset & reboot.

### 7.2.1 Password & MMI

Go to **Administration > System Operation > Password & MMI** tab.

#### Setup Host Name

The Host Name screen allows network administrator to set up / 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"/>

Username Configuration		
Item	Value setting	Description
Host Name	1. An Optional setting 2. It is 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 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 <span>Modify</span>
▶ New Username	<input type="text"/>
▶ Password	<input type="text"/>

Username Configuration		
Item	Value setting	Description
<b>Username</b>	1. The default Username for web-based MMI is 'admin'.	Display the current MMI login account (Username).
<b>New Username</b>	String: any text	Enter new Username to replace the current setting.
<b>Password</b>	String: any text	Enter current password to verify if 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 network administrator to change the web-based MMI login password to access gateway.

Password

Item

Setting

▶ Old Password	<input type="password"/>
▶ New Password	<input type="password"/>
▶ New Password Confirmation	<input type="password"/>

Password Configuration		
Item	Value setting	Description
<b>Old Password</b>	1. String: any text 2. The default password for web-based MMI is 'admin'.	Enter the current password to enable you unlock to change password.
<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 Accessing

This is the gateway's web-based MMI access which allows administrator to access the gateway for management. The gateway's web-based MMI will automatically logout when the idle time has elapsed. The setting allows administrator to enable automatic logout and set the logout idle time. When the login timeout is disabled, the system won't logout the administrator automatically.

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"/>

MMI Configuration		
Item	Value setting	Description
Login	3 times is set by default	Enter the login trial counting value. <b><u>Value Range:</u></b> 3 ~ 10. If someone tries to log in to the web GUI with incorrect password for more than the counting value, an warning message “ <b><i>Already reaching maximum Password-Guessing times, please wait a few seconds!</i></b> ” will be displayed and following login trials will be ignored.
Login Timeout	The Enable box is checked, and 300 is set by default.	Check the Enable box to activate the auto logout function, and specify the maximum idle time as well. <b><u>Value Range:</u></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 <b>default</b> 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 a expected certificate and key from the drop down list. Refer to <b>Object Definition &gt; Certificate</b> Section for the Certificate configuration.
HTTP Compression	The box is unchecked by default.	Check the box ( <b>gzip</b> , or <b>deflate</b> ) if any comprerssion method is preferred.
HTTP Binding	1. An Optional setting 2. DHCP-1 is checked by default	Select the DHCP Server to bind with http access.
System Boot Mode	<b>Normal Mode</b> 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

## 7.2.2 System Information

The system Information screen gives network administrator a quick look up on the device information for the purchased 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	It displays the model name of this product.
<b>Device Serial Number</b>	N/A	It displays the serial number of this product.
<b>Kernel Version</b>	N/A	It displays the Linux kernel version of the product
<b>FW Version</b>	N/A	It displays the firmware version of the product
<b>Memory Usage</b>	N/A	It displays the percentage of device memory utilization.
<b>System Time</b>	N/A	It displays the current system time that you browsed this web page.
<b>Device Up-Time</b>	N/A	It 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 immediately.



## 7.2.3 System Time

The gateway provides manual setup and auto-synchronized approaches for the administrator to set up the system time for the gateway. The time supported synchronization methods can be Time Server, Manual, PC, Cellular Module, or GPS Signal. Select the method first, and then configure the rest of the settings.

Instead of manually configuring the system time for the gateway, there are two simple and quick solutions for you to set the correct time information and set it as the system time for the gateway.

The first one is “Sync with Timer Server”. Based on your selection of time zone and time server in above time information configuration window, system will communicate with time server by NTP Protocol to get system date and time after you click on the **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

System Time Configuration

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. A Required item. 2. <b>Time Server is selected by default.</b>	Select the <b>Time Server</b> as the synchronization method for the system time.
<b>Time Zone</b>	1. A Required item. 2. <b>GMT+00:00</b> is selected by default.	Select a time zone where this device is located.
<b>Auto-synchronization</b>	1. A Required item. 2. Auto is selected by default.	Enter the IP or FQDN for the NTP time server you expected, or leave it as auto mode so that the available server will be used for time synchronization one by one.

<b>Daylight Saving Time</b>	1. It is an optional item. 2. Un-checked by default	Check the <b>Enable</b> button to activate the daylight saving function. When you enable this function, you have to specify the start date and end date for the daylight saving time duration.
<b>NTP Service</b>	1. It is an optional item. 2. Un-checked by default	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 Manually Setting

**System Time Configuration**

Item	Setting
▶ Synchronization method	Manual ▼
▶ Time Zone	(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼
▶ Daylight Saving Time	<input type="checkbox"/> Enable
▶ Set Date & Time Manually	2019 ▼ / April ▼ / 18 ▼ (Year/Month/Day) 16 ▼ : 24 ▼ : 27 ▼ (Hour:Minute:Second)
▶ NTP Service	<input type="checkbox"/> Enable

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>Manual</b> as the synchronization method for the system time. It means administrator has to set the Date & Time manually.
<b>Time Zone</b>	1. A Required item. 2. <b>GMT+00:00</b> is selected by default.	Select a time zone where this device is located.
<b>Daylight Saving Time</b>	1. It is an optional item. 2. Un-checked by default	Check the <b>Enable</b> button to activate the daylight saving function. When you enable this function, you have to specify the start date and end date for the daylight saving time duration.
<b>Set Date &amp; Time Manually</b>	1. It is an optional item.	Manually set the date (Year/Month/Day) and time (Hour:Minute:Second) as the system time.
<b>NTP Service</b>	1. It is an optional item. 2. Un-checked by default	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.

Save	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	Active

System Time Information		
Item	Value Setting	Description
Synchronization method	1. A Required item. 2. Time Server is selected by default.	Select <b>PC</b> as the synchronization method for the system time to let system synchronize its date and time to the time of the administration PC.
NTP Service	1. It is an optional item. 2. Un-checked by default	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.
Synchronize immediately	N/A	Click the <b>Active</b> button to synchronize the system time with specified time server immediately.
Save	N/A	Click the <b>Save</b> button to save the settings.
Refresh	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	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>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.
<b>Time Zone</b>	1. A Required item. 2. <b>GMT+00:00</b> is selected by default.	Select a time zone where this device is located.
<b>NTP Service</b>	1. It is an optional item. 2. Un-checked by default	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.

## Synchronize with GPS Time Service

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	Active

System Time Information		
Item	Value Setting	Description
<b>Synchronization method</b>	1. A Required item. 2. <b>Time Server</b> is selected by default.	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 the product with GNSS interface.
<b>Time Zone</b>	1. A Required item. 2. <b>GMT+00:00</b> is selected by default.	Select a time zone where this device is located.
<b>NTP Service</b>	1. It is an optional item. 2. Un-checked by default	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.

7.2.4 System Log

The System Log screen contains various event log tools facilitating network administrator to perform local event logging and remote reporting.

Go to **Administration > System Operation > System Log** tab.

System Log

View

Email Now

Item	Setting
▶ Web Log Type Category	<div><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</div>
▶ Email Alert	<div><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></div>
▶ Syslogd	<div><div><input type="checkbox"/> Enable</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><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></div>

View & Email Log History

The **View** button is provided for network administrator to view log history on the gateway. **Email Now** button enables administrator to send instant Email for analysis.

View & Email Log History		
Item	Value setting	Description
View button	N/A	Click the <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.

Web Log List <span>Previous</span> <span>Next</span> <span>First</span> <span>Last</span> <span>Download</span> <span>Clear</span>	
Time	Log
Apr 1 06:01:36	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb
Apr 1 06:08:31	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb
Apr 1 06:15:30	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb
Apr 1 06:22:06	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb
Apr 1 06:28:42	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb
Apr 1 06:35:42	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb
Apr 1 06:42:20	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb

Web Log List Window		
Item	Value Setting	Description
Time column	N/A	It displays event time stamps
Log column	N/A	It displays Log messages

Web Log List Button Description		
Item	Value setting	Description
Previous	N/A	Click the <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 logs.
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.

▶ 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
System	Checked by default	Check to log system events and to display in the Web Log List window.
Attacks	Checked by default	Check to log attack events and to display in the Web Log List window.
Drop	Checked by default	Check to log packet drop events and to display in the Web Log List window.
Login message	Checked by default	Check to log system login events and to display in the Web Log List window.
Debug	Un-checked by default	Check to log debug events and to display in the Web Log List window.

Email Alert

Email Alert screen allows network administrator to select the type of event to log and be sent to the destined Email account.

Email Alert

☐ Enable

Server: 

--- Option ---

Add Object

E-mail Addresses:

Subject:

Log type Category: ☐ System ☐ Attacks ☐ Drop ☐ Login message ☐ Debug

Email Alert Setting Window		
Item	Value Setting	Description
Enable	Un-checked by default	Check <b>Enable</b> box to enable sending event log messages to destined Email account defined in the E-mail Addresses blank space.
Server	N/A	Select one email server from the Server dropdown box to send Email. If none 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.
E-mail address	String: email format	Enter the recipient’s Email address. Separate Email addresses with comma ‘,’ or semicolon ‘;’ Enter the Email address in the format of ‘myemail@domain.com’
Subject	String: any text	Enter an Email subject that is easy for you to identify on the Email client.
Log type category	Default unchecked	Select the type of events to log and be sent to the designated Email account. Available events are System, Attacks, Drop, Login message, and Debug.



## Syslogd

The Syslogd screen allows network administrator to select the type of event to log and be sent to the designated Syslog server.

► Syslogd

☐ Enable
 Server: --- Option --- ▼
Add Object

Log type Category:
 ☐ System
 ☐ Attacks
 ☐ Drop
 ☐ Login message
 ☐ Debug

Syslogd Setting Window		
Item	Value Setting	Description
<b>Enable</b>	Un-checked by default	Check Enable box to activate the Syslogd function, and send event logs to a syslog server
<b>Server</b>	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.
<b>Log type category</b>	Un-checked by default	Select the type of event to log and be sent to the destined syslog server. Available events are System, Attacks, Drop, Login message, and Debug.

## Log to Storage

The Log to Storage screen allows network administrator to select the type of events to log and be stored at an internal or an external storage.

► Log to Storage

☒ Enable
 Select Device: Internal ▼

Log file name: syslog

Split file: ☐ Enable
 Size: 200 KB ▼

Interval: ☐ Enable 1440 ( 1 ~ 10080 Minutes)

Max Records: 3000 (5~10000)

Download log file clear logs

Log type Category:
 ☒ System
 ☒ Attacks
 ☒ Drop
 ☒ Login message
 ☒ Debug

Log to Storage Setting Window		
Item	Value Setting	Description
<b>Enable</b>	Un-checked by default	Check to enable sending log to storage.
<b>Select Device</b>	Internal is selected by default	Select internal or external storage.
<b>Log file name</b>	Un-checked by default	Enter log file name to save logs in designated storage.
<b>Split file Enable</b>	Un-checked by default	Check <b>enable</b> box to split file whenever log file reaching the specified limit.
<b>Split file Size</b>	200 KB is set by default	Enter the file size limit for each split log file. <b>Value Range:</b> 10 ~ 1000.
<b>Interval Enable</b>	Un-checked by default	Check <b>enable</b> box to enable the log interval setting.
<b>Log Interval</b>	1440 is set by default	Enter the log interval setting. <b>Value Range:</b> 1 ~ 10080 Minute.
<b>Max Records</b>	3000 is set by default	Enter the maximum number of records to be stored in the log storage. <b>Value Range:</b> 5 ~ 10000.
<b>Log type category</b>	Un-checked by default	Check which type of logs to send: System, Attacks, Drop, Login message, Debug

Log to Storage Button Description		
Item	Value setting	Description
<b>Download log file</b>	N/A	Click the <b>Download log file</b> button to download log files to a log.tar file.
<b>Clear Logs</b>	N/A	Click the <b>Clear logs</b> button to delete the log files from the storage.

## 7.2.5 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

Firmware Backup & Restore		
Item	Value Setting	Description
<b>FW Upgrade</b>	<b>Via Web UI</b> is selected by default	<p>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>.</p> <p>After clicking on the “FW Upgrade” command button, you need to specify the file name of new firmware by using “Browse” button, and then click “Upgrade” button to start the firmware upgrading process on this device. If you want to upgrade a firmware which is from GPL policy, please check “Accept unofficial firmware”</p>
<b>Backup Configuration Settings</b>	<b>Download</b> is selected by default	<p>You can back up or restore the device configuration settings by clicking the <b>Via Web UI</b> button.</p> <p><b>Download</b>: to backup the device configuration to a config.bin file.</p> <p><b>Upload</b>: to restore a designated configuration file to the device.</p> <p><b>Via Web UI</b>: to retrieve the configuration file via Web GUI.</p>
<b>Auto Restore Configuration</b>	The <b>Enable</b> box is unchecked by default	<p>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.</p>

## 7.2.6 Reboot & Reset

For some special reason or situation, you may need to reboot the gateway or reset the device configuration to its default value. In addition to perform these operations through the Power ON/OFF, or pressing the reset button on the device panel, you can do it through the web GUI too.

Go to **Administration > System Operation > Reboot & Reset** tab.

In the Reboot & Reset window, you can reboot this device by clicking the “Reboot” button, and reset this device to default settings by clicking the “Reset” button.

System Operation
⬆ ⬇

Item	Setting
▶ Reboot	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;">Now ▼</div> <div style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;">Reboot</div> </div>
▶ Reset to Default	<div style="border: 1px solid #ccc; padding: 2px 10px;">Reset</div>

System Operation Window		
Item	Value Setting	Description
<b>Reboot</b>	<b>Now</b> is selected by default	<p>Click the <b>Reboot</b> button to reboot the gateway immediately or on a pre-defined time schedule.</p> <p><b>Now:</b> Reboot immediately</p> <p><b>Time Schedule:</b> Select a pre-defined auto-reboot time schedule rule to reboot the auto device on a designated tim. To define a time schedule rule, go to <b>Object Definition &gt; Scheduling &gt; Configuration</b> tab.</p>
<b>Reset to Default</b>	N/A	Click the <b>Reset</b> button to reset the device configuration to its default value.

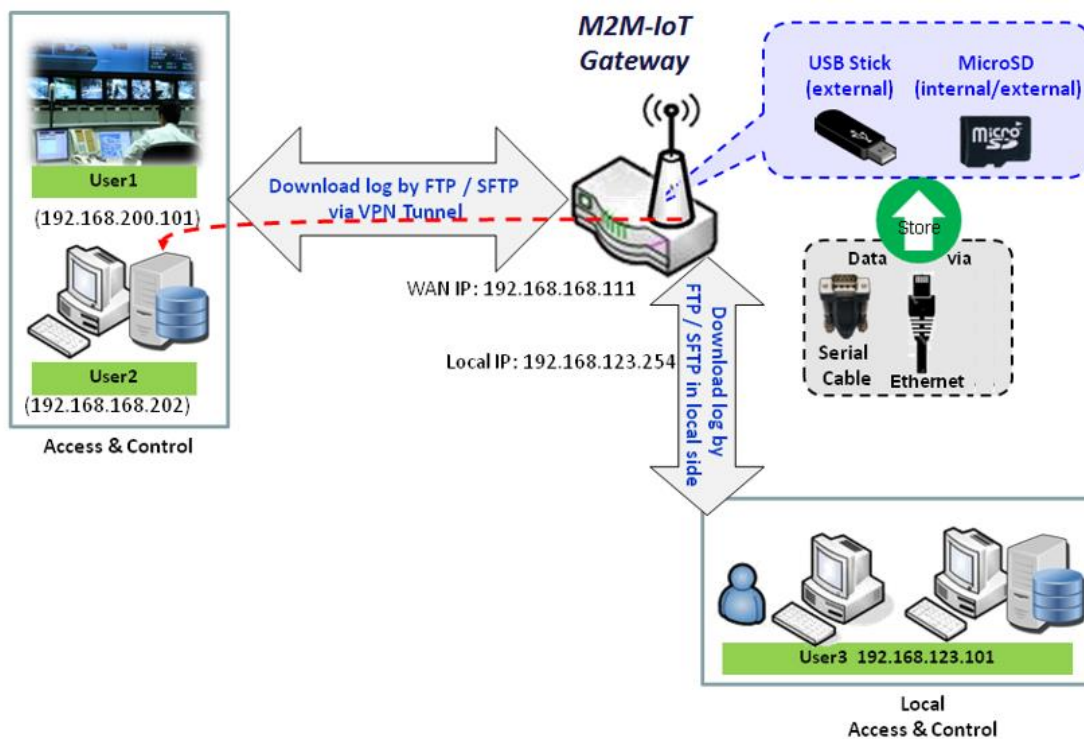
## 7.3 FTP

The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files between a client and server on a computer network. FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it.

For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). Additionally, 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 the log files to his computer or database. In the following two sections, you can configure the FTP server and create the user accounts that can log in to the server. After logging in to the FTP server, you can browse the log directory and have the permission to download the stored log files and delete the files you have downloaded to make more storage space for further data logs.

The available log files can be system logs (refer to Administration > System Operation > System Log), Network Packets (refer to Administrator > Diagnostic > Packet Analyzer), Data Log (refer to Field Communication > Data Logging > Log File Management), and GNSS Log (refer to Service > Location Tracking > GNSS). With proper configuration for the various log functions that supported on your purchased product, you can download the log via FTP / SFTP connections.



## 7.3.1 Server Configuration

This section allows user to setup the embedded FTP and SFTP server for retrieving log files.

Go to **Administration > FTP > Server Configuration** tab.

### Enable FTP Server

FTP Server Configuration

Save

Item	Setting
▶ FTP	<input checked="" 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
<b>FTP</b>	The box is 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 for user file upload to the storage.
<b>FTP Port</b>	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:</b> 1 ~ 65535.
<b>Timeout</b>	<b>300</b> seconds is set by default.	Specify the maximum timeout interval for the FTP connection. Supported range is 60 to 7200 seconds.
<b>Max. Connections per IP</b>	<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.
<b>Max. FTP Clients</b>	<b>5</b> Clients are set by default.	Specify the maximum number of clients for the FTP connection. Up to 32 clients is supported.
<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:</u></b> 1024 ~ 65535.
<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

☐ Enable  
via ☒ LAN  
via ☒ WAN ( WAN-1 ☒ WAN-4 ☐ )

▶ SFTP Port

22

Configuration		
Item	Value setting	Description
<b>SFTP</b>	The box is 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. <ul style="list-style-type: none"> <li>With the SFTP Server enabled, you can retrieve or delete the stored log files via secure SFTP connection.</li> </ul>
<b>SFTP Port</b>	Default 22	Specify a port number for SFTP connection. The gateway will listen for incoming SFTP connections on the specified port. <b><u>Value Range:</u></b> 1 ~ 65535.

## 7.3.2 User Account

This section allows user to setup 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 <span>Add</span> <span>Delete</span>						
ID	User Name	Password	Directory	Permission	Enable	Actions

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

User Account Configuration <span>Save</span>	
Item	Setting
▶ User Name	<input type="text" value="admin"/>
▶ Password	<input type="password" value="....."/>
▶ Directory	<input type="button" value="Browse"/>
▶ Permission	<input type="text" value="Read/Write"/> ▼
▶ Enable	<input checked="" type="checkbox"/>

Configuration		
Item	Value setting	Description
<b>User Name</b>	String: non-blank string	Enter the user account for login to the FTP server. <b><u>Value Range: 1 ~ 15 characters.</u></b>
<b>Password</b>	String: no blank	Enter the user password for login to the FTP server.
<b>Directory</b>	N/A	Select a root directory after user login.
<b>Permission</b>	<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 for user file upload to the storage, even if <b>Read/Write</b> option is selected.
<b>Enable</b>	The box is checked by default.	Check the box to activate the FTP user account.



## 7.4 Diagnostic

This gateway supports simple network diagnosis tools for the administrator to troubleshoot and find the root cause of the abnormal behavior or traffic passing through the gateway. There can be a Packet Analyzer to help record the packets for a designated interface or specific source/destination host, and another Ping and Tracert tools for testing network connectivity issues.

### 7.4.1 Diagnostic Tools

The Diagnostic Tools provide some frequently used network connectivity diagnostic tools (approaches) for the network administrator to check the device connectivity.

Go to **Administration > Diagnostic > Diagnostic Tools** tab.

Diagnostic Tools

Item	Setting
▶ Ping Test	Host IP: <input type="text"/> Outer Interface: <input type="text" value="Auto"/> LAN Source: <input type="text" 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, the Outer interface (auto, WAN, LAN, or VLAN), and LAN source (default, LAN, or VLAN) as well, so 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 for more than twice, then the connection is lost and the route cannot be evaluated. First, you need to specify an IP / FQDN, the test interface (LAN, WAN, or Auto) and the protocol (UDP or ICMP), and by default, it is <b>UDP</b> . Then, 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 allows you to do a quick speed test for verifying the connectivity on 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.

## 7.4.2 Packet Analyzer

The Packet Analyzer can capture packets depend on user settings. User can specify interfaces to capture packets and filter by setting rule. Ensure the log storage is available (either embedded SD-Card or external USB Storage), otherwise **Packet Analyzer** cannot be enabled.

Go to **Administration > Diagnostic > Packet Analyzer** tab.

Configuration

Item	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	<div> <input type="checkbox"/> WAN-1               <input type="checkbox"/> WAN-2               <input type="checkbox"/> WAN-3               <input type="checkbox"/> WAN-4             </div> <div> <input type="checkbox"/> ASY <span>Binary Mode ▼</span> </div> <div>           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         </div> <div>           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         </div>

Configuration		
Item	Value setting	Description
<b>Packet Analyzer</b>	The box is unchecked by default.	Check <b>Enable</b> box to activate the Packet Analyzer function. If you cannot enable the checkbox, please check if the storage is available. Plug in the USB storage and then enable the Package Analyzer function.
<b>File Name</b>	1. An optional setting 2. Blank is set by default, and the default file name is <b>&lt;Interface&gt;_&lt;Date&gt;_&lt;index&gt;</b> .	Enter the 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 extension file name is <b>.pcap</b> .
<b>Split Files</b>	1. An optional setting 2. The 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
<b>Packet Interfaces</b>	An 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. The supported interfaces can be: <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> </ul>

		Select <b>Binary mode</b> or <b>String mode</b> for the serial interface.
		● <b>VAP</b> : This means the virtual AP.
<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.

Once you enabled the Packet Analyzer function on specific Interface(s), you can further specify some filter rules to capture the packets which matched the rules.

Capture Filters

Item	Setting
Filter	<input type="checkbox"/> Enable
Source MACs	
Source IPs	
Source Ports	
Destination MACs	
Destination IPs	
Destination Ports	

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> , which means the source MAC address of packets. Packets which match the rule will be captured. Up to 10 MACs are supported, but they must be separated with “;”, e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when match any one MAC in the rule.
<b>Source IPs</b>	Optional setting	Define the filter rule with <b>Source IPs</b> , which means the source IP address of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with “;”, e.g. 192.168.1.1; 192.168.1.2 The packets will be captured when match any one IP in the rule.

<b>Source Ports</b>	Optional setting	<p>Define the filter rule with <b>Source Ports</b>, which means the source port of packets. The packets will be captured when match any port in the rule.</p> <p>Up to 10 ports are supported, but they must be separated with “;”, e.g. 80; 53</p> <p><b><u>Value Range:</u></b> 1 ~ 65535.</p>
<b>Destination MACs</b>	Optional setting	<p>Define the filter rule with <b>Destination MACs</b>, which means the destination MAC address of packets.</p> <p>Packets which match the rule will be captured.</p> <p>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</p> <p>The packets will be captured when match any one MAC in the rule.</p>
<b>Destination IPs</b>	Optional setting	<p>Define the filter rule with <b>Destination IPs</b>, which means the destination IP address of packets.</p> <p>Packets which match the rule will be captured.</p> <p>Up to 10 IPs are supported, but they must be separated with “;”, e.g. 192.168.1.1; 192.168.1.2</p> <p>The packets will be captured when match any one IP in the rule.</p>
<b>Destination Ports</b>	Optional setting	<p>Define the filter rule with <b>Destination Ports</b>, which means the destination port of packets.</p> <p>The packets will be captured when match any port in the rule.</p> <p>Up to 10 ports are supported, but they must be separated with “;”, e.g. 80; 53</p> <p><b><u>Value Range:</u></b> 1 ~ 65535.</p>

## Chapter 8 Service

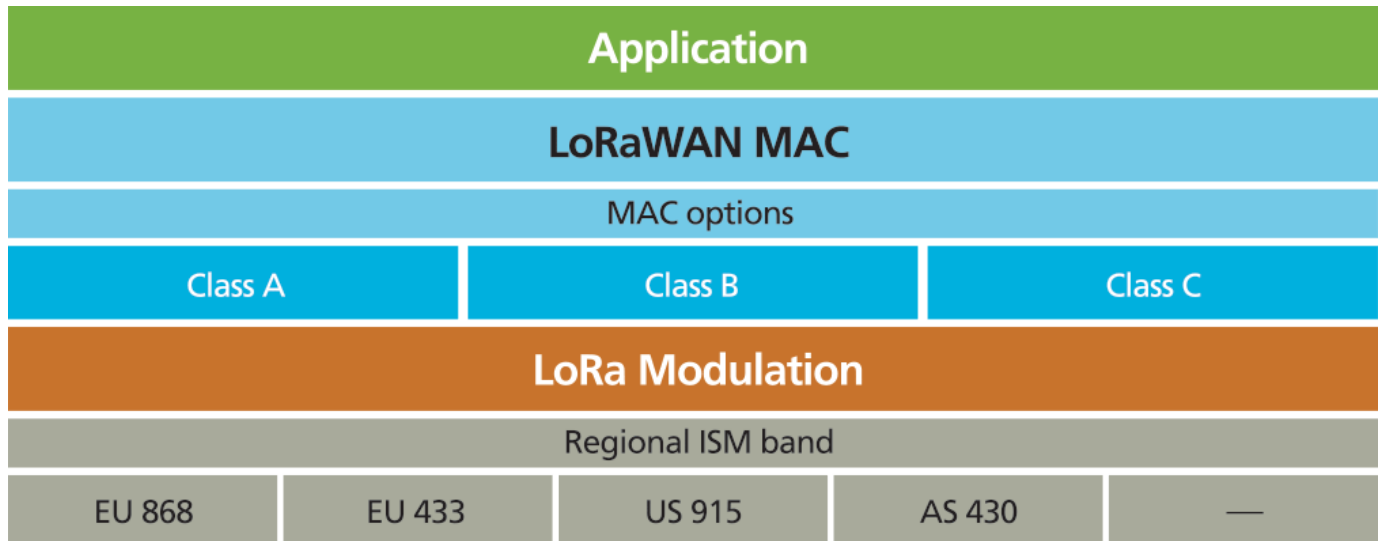
### 8.1 LoRa

**\* (For AiR PACE 1-XX-CL Series only)LoRa Technology**

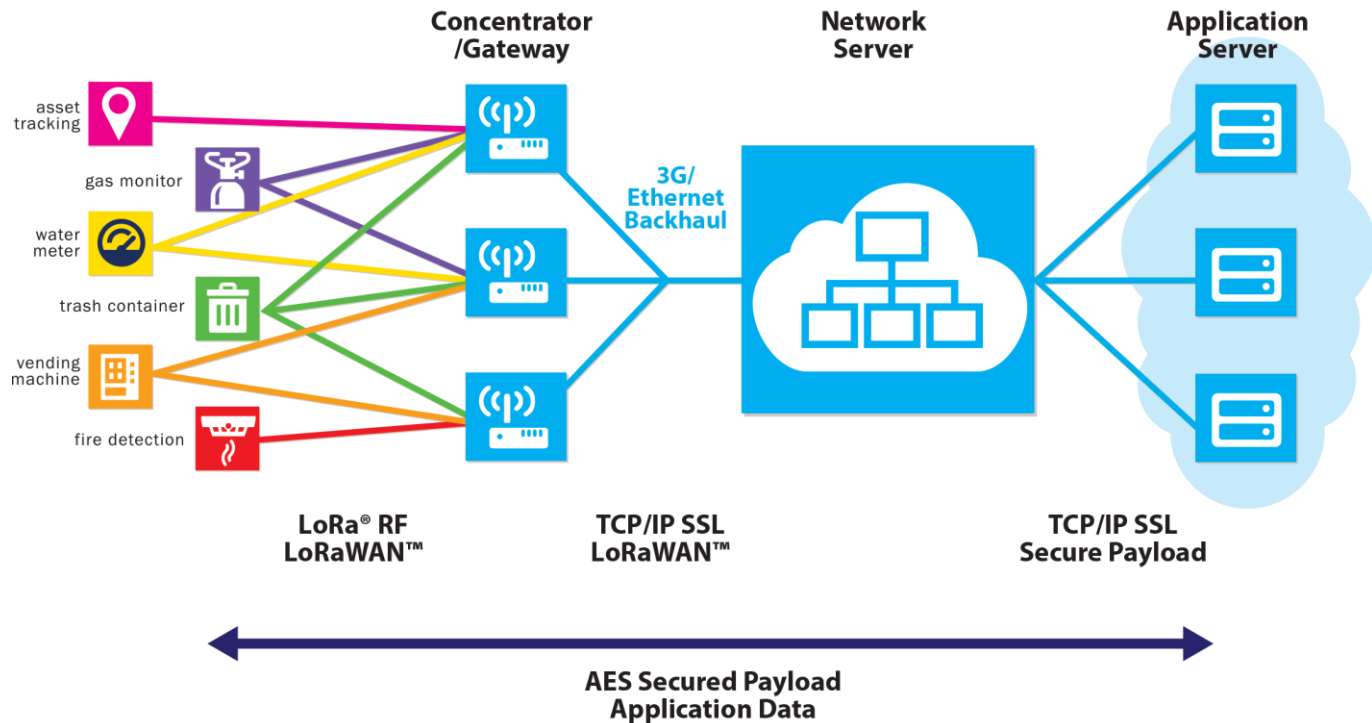
#### LoRa Technology

LoRa is a long range wireless data communication technology developed by Semtech. LoRa uses license-free sub-gigahertz radio frequency bands like 433 MHz, 868 MHz (Europe) and 915 MHz (North America). LoRa enables very-long-range transmissions (more than 10 km in rural areas) with low power consumption. The technology is presented in two parts — LoRa, the physical layer and LoRaWAN, the upper layers.<sup>10</sup>

Semtech builds LoRa Technology into its chipsets. These chipsets are then built into the commercial products, LoRa Gateway and LoRa Nodes, and integrated into LPWANs service by worldwide ISPs.



<sup>10</sup> <https://www.semtech.com/technology/lora/what-is-lora>



## LoRaWAN Protocol

LoRaWAN is a protocol specification built on top of the LoRa technology developed by the LoRa Alliance. It uses unlicensed radio spectrum in the Industrial, Scientific and Medical (ISM) bands to enable low power, wide area communication between remote sensors and gateways connected to the network. This standard-based approach to building a LPWA network allows for quick setup of public or private IoT networks anywhere using hardware and software that is bi-directionally secure, interoperable and mobile, provides accurate localization, and works the way you expect.

LoRaWAN defines the communication protocol and system architecture for the network, while the LoRa physical layer enables the long-range communication link. LoRaWAN is also responsible managing the communication frequencies, data rate, and power for all devices. Devices in the network are asynchronous and transmit when they have data available to send. Data transmitted by an end-node device is received by multiple gateways, which forward the data packets to a centralized network server. The network server filters duplicate packets, performs security checks, and manages the network. Data is then forwarded to application servers.

As depicted in the LoRaWAN network diagram, all the application data between the end nodes and application server are AES-encrypted. The LoRa gateway and network server are merely responsible for data forwarding and security checks, they know nothing about the encrypted data transferred.

## 8.1.1 LoRa Gateway

This product is integrated with an 8-channel LoRa Gateway module. With some basic configuration and specified an accompanied network server, the LoRa Gateway can connect with surrounding LoRa Nodes and forward the received data to Network Server for further processing.

### LoRa Gateway Setting

Go to **Service > LoRa > LoRa Gateway** Tab.

The LoRa Gateway setting page enables user to configure the embedded LoRa gateway, and allow packet forwarding from LoRa nodes to Network Server, or from Network Server to LoRa Nodes.

### LoRa Configuration

LoRa Configuration

Item	Setting
▶ LoRa Gateway	<input type="checkbox"/> Enable
▶ MultiSF Channel	Radio0: Sub-Band(923.2Mhz-923.8Mhz) ▼ Radio1: Sub-Band(924.2Mhz-924.8Mhz) ▼
▶ Gateway ID	005018000FFE0000
▶ Keep Alive Interval	5 (seconds)

LoRa Configuration		
Item	Value setting	Description
<b>LoRa Gateway</b>	The box is unchecked by default	Check <b>Enable</b> box to activate the LoRa Gateway function.
<b>MultiSF Channel</b>	Some channels are selected by default	<p>Select the RF channels to be activated.</p> <p>The LoRa gateway supports up to 8 LoRa channels, defined in <b>Radio0</b> and <b>Radio1</b>, for connecting with LoRa Nodes.</p> <p>For each Radio, you can select one sub band (four channels covered) to operate.</p> <p><b>EU868 Frequency Plan:</b> 8 Sub-Bands for 863.3~863.9 / 864.1~864.7 / 864.9~865.5 / 865.7~866.3 / 866.5~867.1 / 867.3~876.9 / 868.1~868.7 / 868.9~869.5 MHz; and <b>Radio 0</b> is fixed at Sub-Band(868.1~868.7)</p> <p><b>US915 Frequency Plan:</b> 8 Sub-Bands for 902.3~903.7 / 903.9~905.3 / 905.5~906.9 / 907.1~908.5 / 908.7~910.1 / 910.3~911.7 / 911.9~913.3 / 913.5~914.9 MHz</p> <p><b>AS923 Frequency Plan:</b> 5 Sub-Bands for 920.2~921.0 / 921.2~922.0 / 922.2~923.0 / 923.2~924.0 / 924.0~924.8 MHz</p>

		<p><b>Note 1:</b> The supported operation band list is hardware dependent. It depends on the hardware version and regional regulations.</p> <p><b>Note 2:</b> The bandwidth is fixed at 125KHz.</p>
<b>Gateway ID</b>	String format: EUI-64 MAC-like string, with eight 2-digit hex. numbers	<p>Enter an unique ID for the LoRa Gateway. It will be used for communicating with Network Server.</p> <p>Please enter the WAN MAC for the device, and followed with two extra numbers.</p> <p>For example, WAN MAC is 00:50:18:00:08:FE, then input “00:50:18:00:08:FE:11:22” as the Gateway ID.</p>
<b>Keep Alive Interval</b>	<ol style="list-style-type: none"> <li>1. A Must filled setting.</li> <li>2. <b>10</b> is selected by default.</li> </ol>	<p>Specify the time <b>interval</b> (seconds) to keep the connection alive between network server and LoRa gateway even there is no LoRa traffic.</p> <p><b><u>Value Range:</u></b> 10 ~ 999 seconds</p>
<b>Save</b>	NA	Click the <b>Save</b> button to save the configuration



## 8.1.2 LoRa Network Server

For the small scale or private applications, you don't want to use third party's public LoRaWAN network service (bind to a certain LoRa Network Server, Application Server) that is provided by local Telco or ISP. In such case, you will need a private network server for collecting all the data from your deployed LoRa nodes.

This product is integrated with a private LoRa Network Server, and also a simplified Application Server. It supports up to 300 LoRa Nodes. If you intend to use the embedded network server for your private application, you have to proceed with following LoRa Network Server settings.

After that, the collected data from your LoRa nodes is collected and stored in an embedded SQL database. You can access to it with the LAN IP and port 9999.

Note: To customize your application with the product for two-way communication with the Class C LoRa nodes, you may need to get further SDK from the gateway vendor to link with your own application or managing platform.

### LoRa Network Server

Go to **Service > LoRa > LoRa Network Server** Tab.

The LoRa Network Server setting page enables user to configure the LoRa network server, and optionally register the LoRa nodes to the internal LoRa Network Server, when available, to get permissible access.

### LoRa Network Server Configuration

Item	Setting
▶ LoRa Network Server	<input type="checkbox"/> Enable
▶ Server Port	<input type="text" value="1700"/>
▶ Lora Message Database	<input checked="" type="checkbox"/> Enable
▶ Internal / External	<div> <div>External ▼</div> <div>Server: --- Option --- ▼</div> <div>Add Object</div> </div>

LoRa Configuration		
Item	Value setting	Description
<b>LoRa Network Server</b>	The box is unchecked by default	Check <b>Enable</b> box to activate the embedded LoRa Network Server.
<b>Server Port</b>	A required setting Port <b>1700</b> set by default	Specify a <b>Port Number</b> as destination port for sending packets. <b><u>Value Range:</u></b> 1 ~ 65535.
<b>LoRa Message Database</b>	The box is checked by default	Check <b>Enable</b> box to activate the embedded LoRa Message Database. The database can keep up to 600,000 records from connected LoRa nodes.

		Once the records exceed the limit, half of the records will be deleted for recording further messages.
<b>Internal / External</b>	Default value depends on product spec.	<p>Specify the type of LoRa network server to be connected.</p> <p><b>External:</b> Select a LoRa network server, provided by the LoRa Networking Service Provider, to process the packets to/from the LoRa gateway. When the External server is selected, you have to further select a pre-defined server profile from the dropdown list, or click the <b>Add Object</b> button to define the server information to the external LoRa Network Server. Refer to <b>Section 3.4 External Server</b> for the details.</p> <p><b>Internal:</b> Select the internal LoRa network server, embedded with the LoRa Gateway device to process the packets to/from the LoRa gateway.</p> <p><b>Note:</b> Depending on the purchase model, the supported interface type could be <b>Internal</b> or <b>External</b>. Some model just supports <b>External</b> network server.</p>

## Register LoRa Nodes

If you enabled the internal LoRa Network Server, you have to further register all the LoRa Nodes that you are going to deploy in your application sites. Up to 300 LoRa Nodes are supported. Data packets coming from un-registered LoRa nodes will be ignored accordingly.

If you are not familiar with the following terms or items required for registering your LoRa node, you can refer to a helpful article that can be found on the NEWIE VENTURES web page<sup>11</sup>.

You can maintain and see all the registered LoRa nodes in the LoRa Node list.

LoRa Node List <span>Add</span> <span>Delete</span>						
ID	Device Name	Device Class	Device Description	Activation method	Enable	Actions

When **Add** or **Edit** button is applied, the **LoRa Node Configuration** screen will appear.

<sup>11</sup> <https://www.newieventures.com.au/blogtext/2018/2/26/lorawan-otaa-or-abp>

# AIR PACE

LoRa Node Configuration
Save
Undo

Item	Setting
▶ Device Name	<input type="text"/>
▶ Device Class	A ▼
▶ Device Description	<input type="text"/>
▶ Activation method	OTAA ▼
▶ Device EUI	<input type="text"/>
▶ Application EUI	<input type="text"/>
▶ App Key	<input type="text"/>
▶ Device Address	<input type="text"/>
▶ Network Session Key	<input type="text"/>
▶ APP Session Key	<input type="text"/>
▶ Enable	<input type="checkbox"/>

▶ Activation method	ABP ▼
▶ Device EUI	<input type="text"/>
▶ Application EUI	<input type="text"/>
▶ App Key	<input type="text"/>
▶ Device Address	<input type="text"/>
▶ Network Session Key	<input type="text"/>
▶ APP Session Key	<input type="text"/>
▶ Enable	<input type="checkbox"/>

LoRa Node Configuration		
Item	Value setting	Description
<b>Device Name</b>	A required setting Blank by default	Enter an unique name / identifier of the LoRa node being registered. Please enter the WAN MAC for the device, and followed with two extra numbers. <b>Value Range:</b> 1~16 alphanumeric characters; '-' and '_' are valid characters.
<b>Device Class</b>	A Must filled setting Class <b>A</b> is selected by default	Specify the device type of the LoRa node being registered. Currently, Class <b>A</b> and Class <b>C</b> devices are supported.
<b>Device Description</b>	An Optional filled setting Blanked by default	Enter a brief description for the LoRa node be registered.
<b>Activation Method</b>	A Must filled setting <b>OTAA</b> is selected by	Specify the activation method of the LoRa node being registered. <b>OTAA</b> (Over-the-Air Activation) and <b>ABP</b> (Activation by Personalization) are

	default	<p>supported.</p> <p><b>OTAA:</b> OTAA is the preferred and most secure way to connect with network server. Devices perform a join-procedure with the network server, during which a dynamic Device Address is assigned and security keys (Network Session Key, APP Session Key) are negotiated with the device.</p> <p><b>ABP:</b> ABP is a simpler activation method with fixed device address and security keys. For some device, it is manufactured with a hardcode Device Address as well as the security keys in the device. This means it can't work with OTAA method. This strategy might seem simpler, because you skip the join procedure.</p>
<b>Device EUI</b>	A required setting Blanked by default	<p>Enter a unique Device EUI for the LoRa node being registered. The EUI is provided by the device manufacture.</p> <p><b><u>Value Range:</u></b> 16 hexadecimal characters (0~9, A~F)</p>
<b>Application EUI</b>	A required setting Blanked by default	<p>Enter an identifier as the Application EUI for the application you are deploying with the LoRa nodes. For using the private LoRa Network Server, you can define your own Application EUI.</p> <p><b><u>Value Range:</u></b> 16 hexadecimal characters (0~9, A~F)</p>
<b>App Key</b>	A required setting for OTAA scheme	<p>Enter an Application Key, if OTAA activation is selected, to generate required session keys while the LoRa node joins or re-joins to the network. For using the private LoRa Network Server, you can define your own Application Key.</p> <p><b><u>Value Range:</u></b> 32 hexadecimal characters (0~9, A~F)</p>
<b>Device Address</b>	A required setting for ABP scheme	<p>Enter a unique device address for the LoRa node being entered. It is required for ABP activation scheme.</p> <p><b><u>Value Range:</u></b> 8 hexadecimal characters (0~9, A~F)</p>
<b>Network Session Key</b>	A required setting for ABP scheme	<p>Enter a network session key for the LoRa node being registered. The Network Server will use this key to decrypt the meta data that is transmitted from the registered LoRa nodes. It is required for ABP activation scheme.</p> <p><b><u>Value Range:</u></b> 32 hexadecimal characters (0~9, A~F)</p>
<b>APP Session Key</b>	A required setting for ABP scheme	<p>Enter an application session key for the LoRa node being registered. The Application Server will use this key to decrypt the packet payload that is transmitted from the registered LoRa nodes. It is required for ABP activation scheme.</p> <p><b><u>Value Range:</u></b> 32 hexadecimal characters (0~9, A~F)</p>
<b>Enable</b>	Unchecked by default	Check the Enable box to activate the parameters of the LoRa node being registered.
<b>Save</b>	NA	Click the <b>Save</b> button to save the configuration

## Register LoRa Group Nodes

To deploy hundreds of LoRa nodes, you can register the LoRa nodes as a group of LoRa nodes instead of registering one by one.

You can maintain and see all the registered LoRa group nodes in the LoRa Group Node list.

# AIR PACE

LoRa Group Node List <span>Add</span> <span>Delete</span>									
ID	Device Name	Device Class	Activation method	Device Address start	Device Address end	Device EUI start	Device EUI end	Enable	Actions

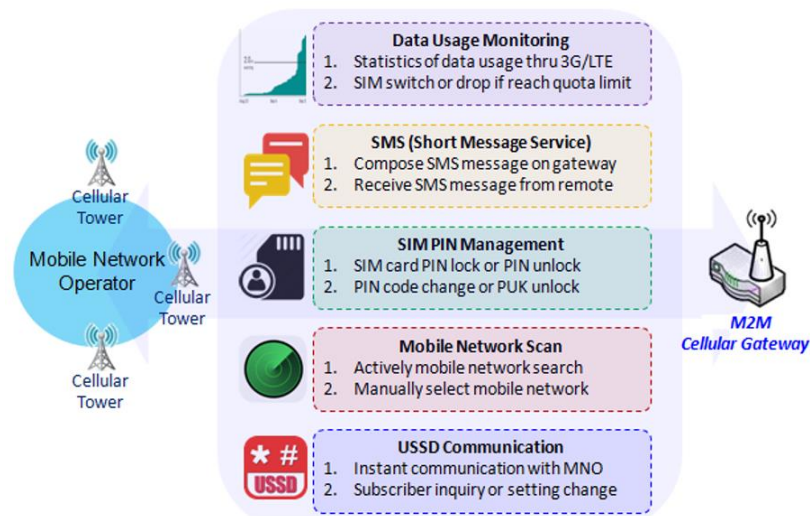
When **Add** or **Edit** button is applied, the **LoRa Group Node Configuration** screen will appear.

LoRa Group Node List <span>Save</span> <span>Undo</span>	
Item	Setting
▶ Device Name	<input type="text"/>
▶ Device Class	A ▼
▶ Device Description	<input type="text"/>
▶ Activation method	OTAA ▼
▶ Device Address start	<input type="text"/>
▶ Device Address end	<input type="text"/>
▶ Device EUI start	<input type="text"/>
▶ Device EUI end	<input type="text"/>
▶ Application EUI	<input type="text"/>
▶ Network Session Key	<input type="text"/>
▶ APP Session Key	<input type="text"/>
▶ Enable	<input type="checkbox"/>

LoRa Group Node Configuration		
Item	Value setting	Description
<b>Device Name</b>	A required setting Blanked by default	Enter an unique name / identifier of the LoRa group node being registered. <b>Value Range:</b> 1~16 alphanumeric characters.
<b>Device Class</b>	A required setting Class <b>A</b> is selected by default	Specify the device type of the LoRa node being registered. Currently, Class <b>A</b> and Class <b>C</b> devices are supported.
<b>Device Description</b>	An Optional setting Blank by default	Enter a brief description for the LoRa group node be registered.
<b>Activation Method</b>	A required setting <b>OTAA</b> is selected by default	Specify the activation method of the LoRa node being registered. <b>OTAA</b> (Over-the-Air Activation) and <b>ABP</b> (Activation by Personalization) are supported. <b>OTAA:</b> OTAA is the preferred and most secure way to connect with network server. Devices perform a join-procedure with the network server, during which a dynamic Device Address is assigned and security keys (Network Session Key, APP Session Key) are negotiated with the device. <b>ABP:</b> ABP is a simpler activation method with fixed device address and security keys. For some device, it is manufactured with a hardcode Device Address as

		well as the security keys in the device. This means it can't work with OTAA method. This strategy might seem simpler, because you skip the join procedure.
<b>Device Address start / Device Address end</b>	A required setting Blank by default	<p>Specify a range of Device address, by entering the start and end address, for the LoRa group nodes. For example, 12340000 as the start address, and 1234FFFF as the end address. Any LoRa Node with Device address in this range will be regarded as a registered node.</p> <p>The address is provided by the device manufacture. It is required for ABP activation scheme.</p> <p><b><u>Value Range:</u></b> 8 hexadecimal characters (0~9, A~F)</p>
<b>Device EUI start / Device EUI end</b>	A required setting Blanked by default	<p>Specify a range of Device EUI, by entering the start and end EUI, for the LoRa group nodes. For example, 1000123AB0100000 as the start EUI, and 1000123AB01FFFFFF as the end EUI. Any LoRa Node with Device EUI in this range will be regarded as a registered node.</p> <p>The EUI is provided by the device manufacture.</p> <p><b><u>Value Range:</u></b> 16 hexadecimal characters (0~9, A~F)</p>
<b>Application EUI</b>	A required setting Blanked by default	<p>Enter an identifier as the Application EUI for the application you are deploying with the LoRa nodes.</p> <p>For using the private LoRa Network Server, you can define your own Application EUI.</p> <p><b><u>Value Range:</u></b> 16 hexadecimal characters (0~9, A~F)</p>
<b>Network Session Key</b>	A required setting for ABP scheme	<p>Enter a network session key for the LoRa node being registered. The Network Server will use this key to decrypt the meta data that is transmitted from the registered LoRa nodes.</p> <p>It is required for ABP activation scheme.</p> <p><b><u>Value Range:</u></b> 32 hexadecimal characters (0~9, A~F)</p>
<b>APP Key Session</b>	A required setting for ABP scheme	<p>Enter an application session key for the LoRa node being registered. The Application Server will use this key to decrypt the packet payload that is transmitted from the registered LoRa nodes.</p> <p>It is required for ABP activation scheme.</p> <p><b><u>Value Range:</u></b> 32 hexadecimal characters (0~9, A~F)</p>
<b>Enable</b>	Unchecked by default	Check the Enable box to activate the parameters of the LoRa node being registered.
<b>Save</b>	NA	Click the <b>Save</b> button to save the configuration

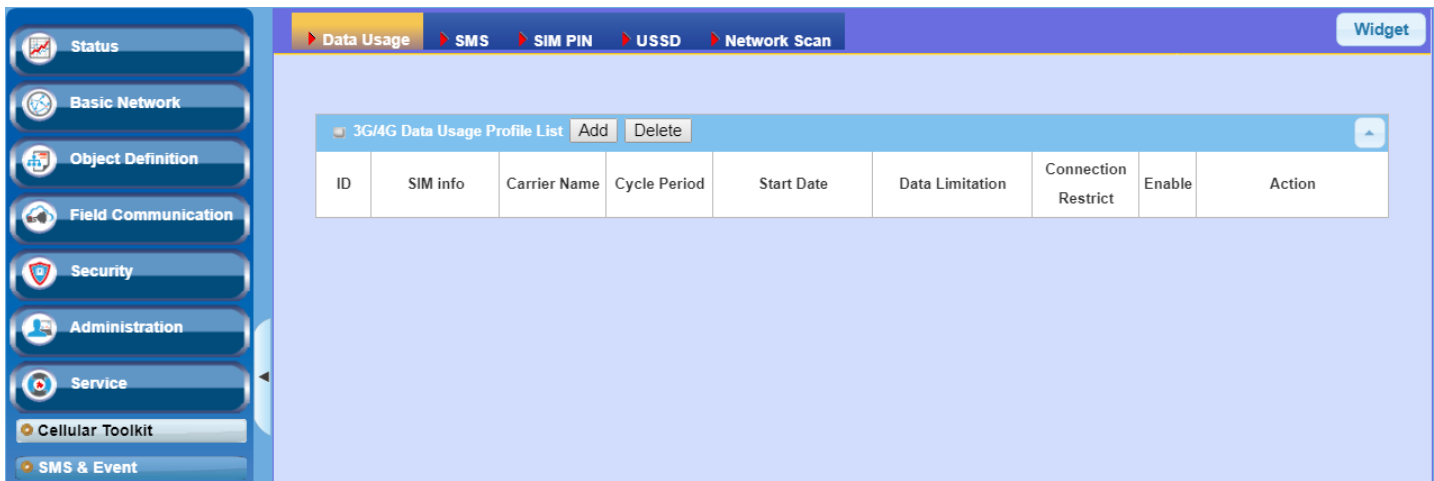
## 8.2 Cellular Toolkit



Besides cellular data connection, you may also like to monitor data usage of cellular WAN, sending text messages through SMS, changing PIN code of SIM card, communicating with carrier/ISP by USSD command, or doing a cellular network scan for diagnostic purpose.

In Cellular Toolkit section, it includes several useful features that are related to cellular configuration or application. You can configure settings of Data Usage, SMS, SIM PIN, USSD, and Network Scan here. Please note at least a valid SIM card is required to be

inserted to device before you continue settings in this section.



## 8.2.1 Data Usage

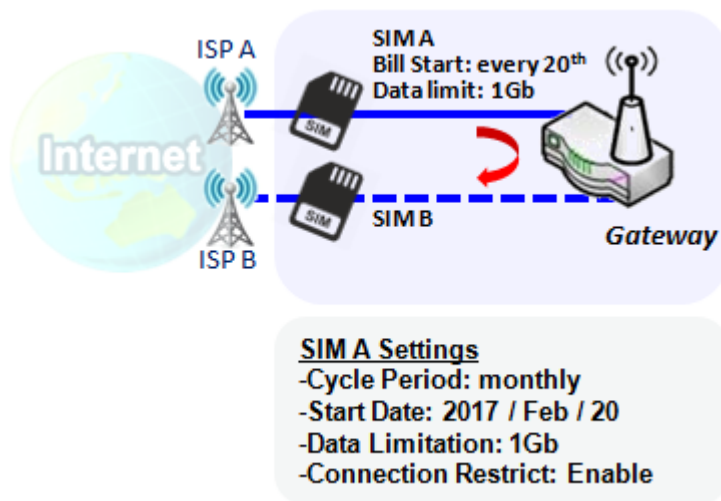
Most data plans for cellular connection have a limited amount of data usage. If the data usage exceeds the quota, either you will get much lower data throughput that may affect your daily operation, or you will get a 'bill shock' in the next month because carrier/ISP charges a lot for the over-quota data usage.

With help from Data Usage feature, the device will monitor cellular data usage continuously and take actions. If data usage reaches limited quota, device can be set to drop the cellular data connection right away. Otherwise, if secondary SIM card is inserted, device can switch to secondary SIM and establish another cellular data connection with secondary SIM automatically.

If Data Usage feature is enabled, all history of cellular data usage can be viewed at **Status > Statistics & Reports > Cellular Usage** tab.

3G/4G Data Usage 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 enables the gateway device to continuously monitor cellular data usage and take actions. In the diagram, quota limit of SIM A is **1Gb** per month and bill start date is **20<sup>th</sup>** of every month. The device knows to start a new calculation of data usage on every 20<sup>th</sup> of month. Enabling Connection Restrict will force gateway device to drop cellular connection of SIM A when data usage reaches quota limit (1Gb in this case). If SIM failover feature is configured in **Internet Setup**, then gateway will switch to SIM B and establish a new cellular data connection automatically.



## Data Usage Setting

Go to **Service > Cellular Toolkit > Data Usage** tab.

Before finishing settings for Data Usage, you need to know bill start date, bill period, and quota limit of data usage according to your data plan. You can ask this information from your carrier or ISP.

### Create / Edit 3G/4G Data Usage Profile

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 **Add** button is applied, 3G/4G Data Usage Profile Configuration screen will appear. You can create up to four data usage profiles, one profile for each SIM card used in the Gateway.

3G/4G Data Usage Profile Configuration	
Item	Setting
▶ SIM Select	3G/4G ▼ SIM A ▼
▶ Carrier Name	<input type="text"/>
▶ Cycle Period	Days ▼ <input type="text"/>
▶ Start Date	2019 ▼ / April ▼ / 1 ▼
▶ 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	Value 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 the product with dual cellular module.
<b>Carrier Name</b>	It is an optional item.	Fill in the Carrier Name for the selected SIM card for identification.
<b>Cycle Period</b>	<b>Days</b> by default	The first box has three types for cycle period. They are <b>Days</b> , <b>Weekly</b> and <b>Monthly</b> . <b>Days:</b> For per Days cycle periods, you have to 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 measure network traffic. Please don't select the day before now, otherwise, the traffic statistics will be incorrect.
<b>Data Limitation</b>	N/A	Specify the allowable data limitation for the defined cycle period.
<b>Connection</b>	Un-Checked by default.	Check the <b>Enable</b> box to activate the connection restriction function.

# AIR PACE

<b>Restrict</b>		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.

## 8.2.2 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

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 <input type="text" value=""/> (1-10)

Configuration Item	Value setting	Description
<b>Physical Interface</b>	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 following SMS function configuration. <b>Note:</b> <b>3G/4G-2</b> is only available for for the product with dual cellular module.
<b>SMS</b>	The box is checked by default	This is the SMS switch. If the box is checked then the SMS function is enabled. If the box is unchecked then the SMS function is disabled.
<b>SIM Status</b>	N/A	Depends on currently SIM status. The possible value will be <b>SIM_A</b> or <b>SIM_B</b> .
<b>SMS Storage</b>	The box is <b>SIM Card Only</b> by default	This is the SMS storage location. Currently the option only <b>SIM Card Only</b> .
<b>SMS Space</b>	The box is unchecked by default	Check the <b>Enable</b> box and specify a number (1-10) for message count to reserve some available storage space and prevent it from running out of storage. The oldest message(s) will be deleted when the SMS storage is full.
<b>Save</b>	N/A	Click the <b>Save</b> button to save the settings

## SMS Summary

Show **Unread SMS**, **Received SMS**, **Sent SMS**, **Remaining SMS**, and edit SMS context to send, read SMS from SIM card.

SMS Summary		New SMS	SMS Inbox	SMS Sent Folder		
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 into the router for the first time, unread SMS value is zero. When a new SMS is received but not read, this value increases by one.
<b>Received SMS</b>	N/A	This value records the existing SMS numbers from SIM card. When a new SMS is received, this value increases by one.
<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. When a new SMS is received, this value decreases by one.
<b>New SMS</b>	N/A	Click <b>New SMS</b> button, a <b>New SMS</b> screen appears. User can set the SMS setting from this screen. 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 to SMS or forward SMS from this screen. Refer to SMS Inbox List in the next page.
<b>Refresh</b>	N/A	Click the <b>Refresh</b> button to update the SMS summary immediately.

## New SMS

You can configure the SMS settings from this screen.

New SMS

Send

Item	Setting
Receivers	<input type="text"/> (Use '+' for International Format and ';' to Compose Multiple Receivers)
Text Message	<div></div> Length of Current Input : 0
Result	

New SMS		
Item	Value setting	Description
Receivers	N/A	Write the receivers that will receive the SMS. Add a semicolon for multiple receivers.
Text Message	N/A	Write the SMS content. The router supports up to a maximum of 1023 character for SMS length.
Send	N/A	Click the <b>Send</b> button, the above text message will be 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

Refresh

Delete

Close

Previous

1 ▾

Next


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	Sender List (Phone Number) for the received SMS
Timestamp	N/A	What time the SMS is received
SMS Text Preview	N/A	Preview the SMS text. Click the <b>Detail</b> button to read a certain message.
Action	The box is unchecked by	Click the <b>Detail</b> button to read the SMS detail; Click the <b>Reply / Forward</b> button

	default	to reply/forward SMS. Additionally, you can check the box(es), and then click the <b>Delete</b> button to delete the checked SMS(s).
<b>Refresh</b>	N/A	Refresh the SMS Inbox List.
<b>Delete</b>	N/A	Delete the SMS for all checked box from Action.
<b>Close</b>	N/A	Close the Detail SMS Message screen.

## SMS Sent Folder

You can read or delete SMS from this screen.

 SMS Sent Folder <button>Delete</button> <button>Close</button> <input type="text" value="0"/> <input type="button" value="Previous"/> <input type="button" value="Next"/>				
ID	Receivers	Timestamp	SMS Text Preview	Actions

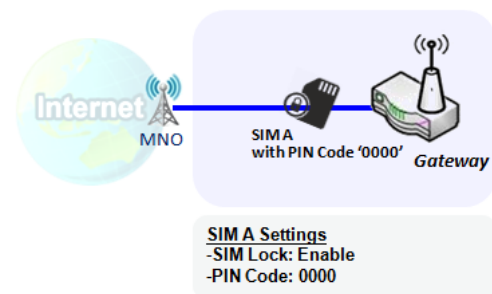
SMS Sent Folder		
Item	Value setting	Description
<b>ID</b>	N/A	The number of SMS.
<b>Receivers</b>	N/A	Receiver list for the sent SMS.
<b>Timestamp</b>	N/A	What time the SMS was sent
<b>SMS Text Preview</b>	N/A	Preview the SMS text. Click the <b>Detail</b> button to read a certain message.
<b>Action</b>	The box is unchecked by default	Click the <b>Detail</b> button to read the SMS detail Additionally, you can check the box(es), and then click the <b>Delete</b> button to delete the checked record(s).
<b>Refresh</b>	N/A	Refresh the SMS Sent Folder.
<b>Delete</b>	N/A	Delete the SMS for all checked box from Action.
<b>Close</b>	N/A	Close the Detail SMS Message screen.

## 8.2.3 SIM PIN

With most cases, users need to insert a SIM card (a.k.a. UICC) into end devices to get on a cellular network for voice service or data surfing. The SIM card is usually released by mobile operators or service providers. Each SIM card has a unique number (so-called ICCID) for network owners or service providers to identify each subscriber. As SIM card plays an important role between service providers and subscribers, some security mechanisms are required on SIM card to prevent any unauthorized access.

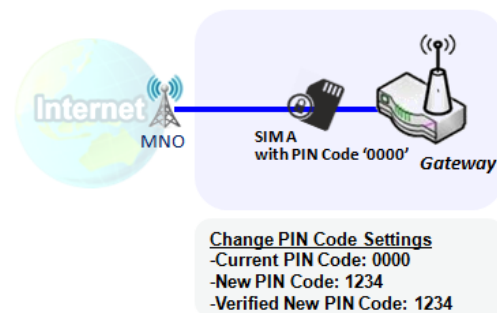
Enabling a PIN code in SIM card is an easy and effective way of protecting cellular devices from unauthorized access. This gateway device allows you to activate and manage PIN code on a SIM card through its web GUI.

### Activate PIN code on SIM Card



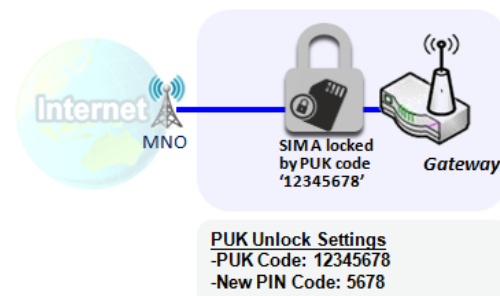
This gateway device allows you to activate PIN code on SIM card. This example shows how to activate PIN code on SIM-A for 3G/4G-1 with default PIN code “0000”.

### Change PIN code on SIM Card



This gateway device allows you to change PIN code on SIM card. Following the example above, you need to type original PIN code “0000”, and then type new PIN code with ‘1234’ if you like to set new PIN code as ‘1234’. To confirm the new PIN code you type is what you want, you need to type new PIN code ‘1234’ in Verified New PIN Code again.

### Unlock SIM card by PUK Code



If you enter an incorrect PIN code at configuration page for 3G/4G-1 WAN over three times, and then it will cause SIM card to be locked by PUK code. Then you have to call service number to get a PUK code to unlock SIM card. In the diagram, the PUK code is “12345678” and new PIN code is “5678”.

## SIM PIN Setting

Go to **Service** > **Cellular Toolkit** > **SIM PIN** Tab

With the SIM PIN Function window, it allows you to enable or disable SIM lock (which means protected by PIN code), or change PIN code. You can also see the information of remaining times of failure trials as we mentioned earlier. If you run out of these failure trials, you need to get a PUK code to unlock SIM card.

### Select a SIM Card

Configuration

Item	Setting
Physical Interface	3G/4G-1 ▼
SIM Status	SIM-A Ready
SIM Selection	SIM-A ▼ <button>Switch</button>

Configuration Window		
Item	Value setting	Description
<b>Physical Interface</b>	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 for the product with dual cellular module.
<b>SIM Status</b>	N/A	Indication for the selected SIM card and the SIM card status. The status could be <b>Ready</b> , <b>Not Insert</b> , or <b>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. That SIM card is still at locked status.
<b>SIM Selection</b>	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 another one. After that, you can configure the SIM card.



## Enable / Change PIN Code

Enable or Disable PIN code (password) function, and even change PIN code function.

SIM function
Save
Change PIN Code

Item	Setting
▶ PIN Lock	<input checked="" type="checkbox"/> Enable PIN Code: <input type="text"/> (4~8 digits)
▶ Remaining times	N/A

SIM function Window		
Item Setting	Value setting	Description
<b>SIM lock</b>	Depend 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, you have to fill in the PIN code as well, and then click <b>Save</b> button to apply the setting.
<b>Remaining times</b>	Depend 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. In the case, if you still want to change the PIN code, you have to enable the SIM Lock function first, fill in the PIN code, and then click the <b>Save</b> button to enable. After that, You can click the <b>Change PIN code</b> button to change the PIN code.

When **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)

Apply
Cancel

Item	Value Setting	Description
<b>Current PIN Code</b>	A Required setting	Fill in the current (old) PIN code of the SIM card.
<b>New PIN Code</b>	A Required setting	Fill in the new PIN Code you want to change.
<b>Verified New PIN Code</b>	A 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 changed the PIN code for a certain SIM card, you must also change the corresponding PIN code specified in the **Basic Network > WAN & Uplink > Internet Setup > Connection with SIM Card** page. Otherwise, it may result in wrong SIM PIN trials with invalid (old) PIN code.

## Unlock with a PUK Code

The PUK Function window is only available for configuration if that SIM card is locked by PUK code. It means that SIM card is locked and needs additional PUK code to unlock. Usually it happens after too many trials of incorrect PIN code, and the remaining times in SIM Function table turns to 0. In this situation, you need to contact your service provider and request a PUK code for your SIM card, and try to unlock the locked SIM card with the provided PUK code. After unlocking a SIM card by PUK code successfully, the SIM lock function will be activated automatically.

PUK function

Save

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
<b>PUK status</b>	<b>PUK Unlock / PUK Lock</b>	Indication for the PUK status. The status could be <b>PUK Lock</b> or <b>PUK Unlock</b> . As mentioned earlier, the SIM card will be locked by PUK code after too many trials of failure PIN code. In this case, the PUK Status will turns to <b>PUK Lock</b> . In a normal situation, it will display <b>PUK Unlock</b> .
<b>Remaining times</b>	Depend on SIM card	Represent the remaining trial times for the PUK unlocking. Note: <b>DO NOT make the remaining times down to 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.
<b>PUK Code</b>	A Required setting	Fill in the PUK code (8 digits) that can unlock the SIM card in PUK unlock status.
<b>New PIN Code</b>	A Required setting	Fill in the New PIN Code (4~8 digits) for the SIM card. You have to determine your new PIN code to replace the old, forgotten one. Keep the PIN code (password) in mind with care.
<b>Save</b>	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 invalid (old) PIN code.

8.2.4 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 <span>▼</span> SIM Status: SIM_A

USSD Profile List

AddDelete

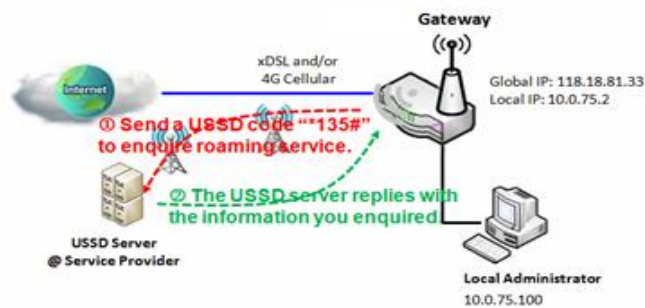
ID	Profile Name	USSD Command	Comments	Actions
----	--------------	--------------	----------	---------

USSD Request

SendClearCancel

Item	Setting
USSD Profile	--- Option --- <span>▼</span>
USSD Command	

USSD Scenario



USSD allows you to have an instant bi-directional communication with carrier/ISP. In the diagram, the USSD command **'\*135#'** is referred to data roaming services. After sending that USSD command to carrier, you can get a response at window USSD Response. Please note the USSD command varies for different carriers/ISP.

## USSD Setting

Go to **Service > Cellular Toolkit > USSD** tab.

In "USSD" page, there are four windows for the USSD function. The "Configuration" window lets you specify which 3G/4G module (physical interface) is used for the USSD function, and system will show which SIM card in the module is the current used one. The second window is the "USSD Profile List" and it shows all your defined USSD profiles that store pre-commands for activating an USSD session. An "Add" button in the window lets you add one new USSD profile and define the commands for the profile in the third window, the "USSD Profile Configuration". When you want to start the activation of an USSD connection session to the USSD server, select the USSD profile or type in the correct pre-command, and then click on the "Send" button for the session. The responses from the USSD server will be displayed beneath the "USSD Command" line. When commands typed in the "USSD Command" field are sent, received responses will be displayed in the "USSD Response" blank space. User can communicate with the USSD server by sending USSD commands and getting USSD responses via the gateway.

### USSD Configuration

Configuration		
Item	Setting	
Physical Interface	3G/4G-1 ▼	SIM Status: SIM_A

Configuration		
Item	Value setting	Description
Physical Interface	The box is <b>3G/4G-1</b> by 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 for the product with dual cellular module.
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					
	Add	Delete			
ID	Profile Name	USSD Command	Comments	Actions	

# AIR PACE

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

USSD Request

Send

Clear

Cancel

▲

✕

Item	Setting
▶ USSD Profile	--- Option --- ▼
▶ USSD Command	

USSD Profile Configuration		
Item	Value setting	Description
Profile Name	N/A	Enter a name for the USSD profile.
USSD Command	N/A	Enter the USSD command defined for the profile. Normally, it is a command string composed with numeric keypad “0~9”, “*”, and “#”. The USSD commands are highly related to the cellular service, please check with your service provider for the details.
Comments	N/A	Enter a brief comment for the profile.

## Send USSD Request

When **send** the USSD command, the USSD Response screen will appear.

When click the **Clear** button, the USSD Response will disappear.

USSD Request

Send

Clear

Cancel

▲

✕

Item	Setting
▶ USSD Profile	--- Option --- ▼
▶ USSD Command	

USSD Request		
Item	Value setting	Description
USSD Profile	N/A	Select a USSD profile name from the dropdown list.
USSD Command	N/A	The USSD Command string of the selected profile will be shown here.
USSD Response	N/A	Click the <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.

## 8.2.5 Network Scan

"Network Scan" function lets the administrator specify how the device connects to the mobile system for data communication in 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 can define their connection sequence for the gateway device to connect to the mobile system automatically. Administrator also can scan the mobile systems in the air manually, select the target operator system and apply it. The manual scanning approach is used for problem diagnosis.

### Network Scan Setting

Go to **Service > Cellular Toolkit > Network Scan** tab.

In "Network Scan" page, there are two windows for the Network Scan function. The "Configuration" window lets you select which 3G/4G module (physical interface) is used to perform Network Scan, and system will show the current used SIM card in the module. You can configure each 3G/4G WAN interface by executing the network scanning one after another. You can also specify the connection sequence of the targeted generation of mobile system, 2G/3G/LTE.


### Network Scan Configuration

Configuration	
Item	Setting
Physical Interface	3G/4G-1 ▼ SIM Status: SIM_A
Network Type	Auto ▼
LTE Band	Auto ▼
Scan Approach	Auto ▼

Configuration		
Item	Value setting	Description
<b>Physical Interface</b>	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 for the product with dual cellular module.
<b>SIM Status</b>	N/A	Show the connected cellular service (identified with <b>SIM_A</b> or <b>SIM_B</b> ).
<b>LTE Band</b>	<b>Auto</b> is selected by default.	Specify the expected LTE Band for connecting to available mobile network. It can be Auto, or available Bands for the embedded cellular module. If a specific band is selected, the device will band lock to that band and not use any other available band. <b>Note:</b> Unless your ISP requires a specific band for providing network service, keep this field at Auto.
<b>Network Type</b>	<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 register automatically;

		If the <b>prefer</b> option is selected, network will be register for your option first; If the <b>only</b> option is selected, network will be register for your option only.
Scan Approach	<b>Auto</b> is selected by default.	When <b>Auto</b> selected, cellular module registers automatically. 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.
Save	N/A	Click <b>Save</b> to save the settings

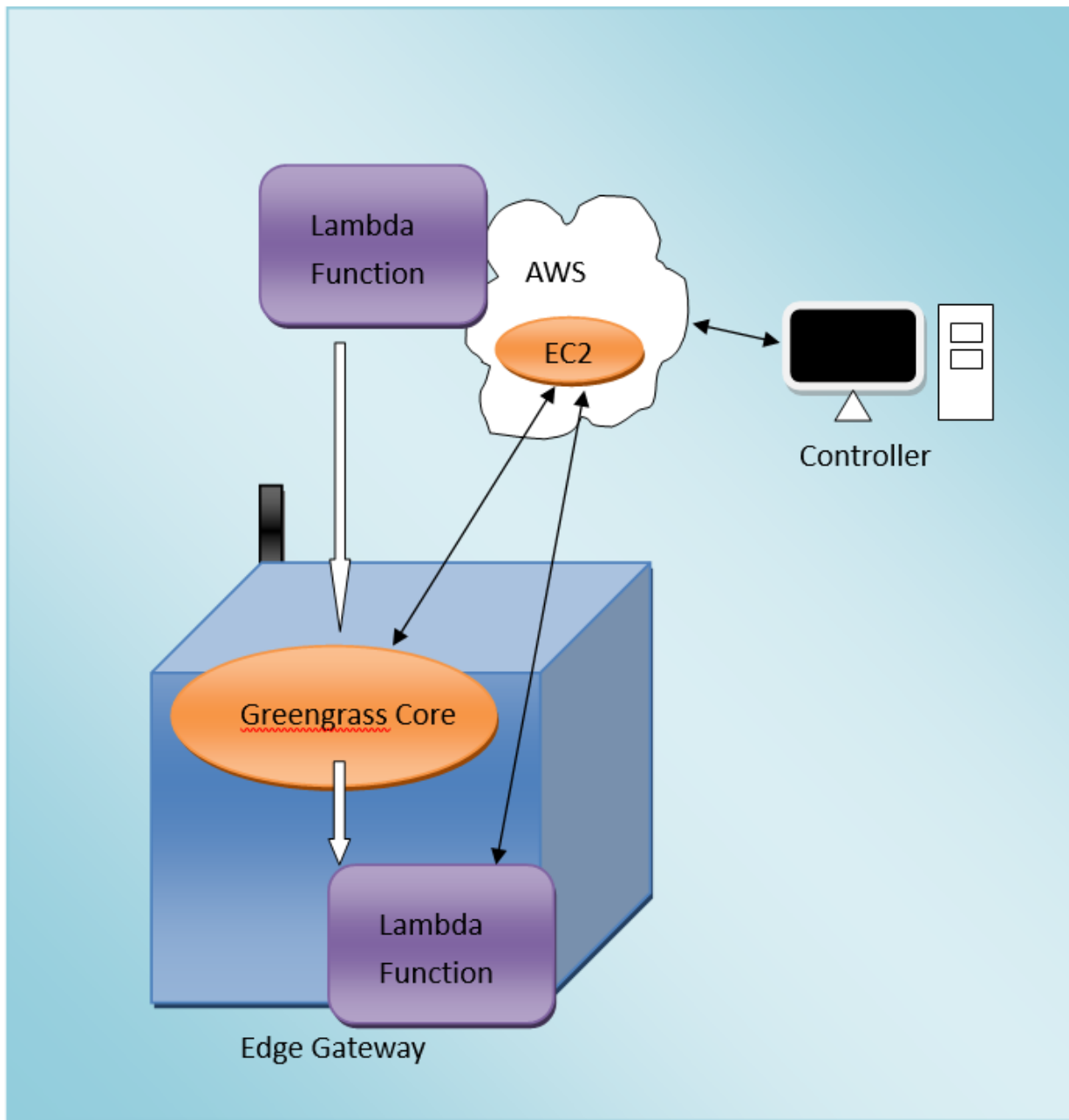
The second window is the "Network Provider List" window and it appears when the **Manually** Scan Approach is selected in the Configuration window. By clicking on the "Scan" button and waiting for 1 to 3 minutes, the found mobile operator systems will be displayed for you to choose. Click again on the "Apply" button to connect to that mobile service provider system for the dedicated 3G/4G interface.

 Network Provider List <span>Scan</span> <span>Apply</span> <span>Close</span>			
Provider Name	Mobile System	Network Status	Action

## 8.3 AWS Greengrass

AWS IoT Greengrass allows Amazon Web Services to work with edge devices, allowing them to act on locally generated data while at the same time using the Cloud for management, analytics, and storage. Devices connected with AWS IoT Greengrass can execute code without the need for a server.

Greengrass Conceptual Figure





Greengrass can be considered as a kind of zombie network.

The controller uses AWS IoT console to ask the Greengrass core running on Edge Gateway to download the Lambda function from cloud, and then execute the Lambda function in the Edge Gateway environment.

As long as the Lambda function executes successfully, it will continuously do the job that controller wants, such like collecting and processing original data before sending back to cloud.

In this way, the controller can reduce the transfer effort between Edge Gateway and Cloud, and also make the computing power of Edge Gateway more useful.

In the picture above, you can see the key points on to make AWS Greengrass work:

- An EC2 server, for deploying Lambda function, communicates with Greengrass cores, and does further processing in the Cloud.
- The Greengrass core is a daemon running at Edge Gateway, which is compiled by AWS team for each platform. You can only get binary format from AWS.
- Lambda function, which will be executed on Edge Gateway. There are several languages supported by Greengrass: C/Python 2.7/Python 3/Node.js/Java. In the first test case, we used Python 2.7. You must download related SDK from AWS to write the Lambda function.

What you can NOT see in this picture is the certification files for EC2 and Greengrass core to communicate with each other. These are called “resource files”, which you can download when you create a new Greengrass group, and that is the only chance to do so.

## 8.3.1 Configuration Steps

These are the necessary steps to set up Greengrass:

- Create an EC2 server. (Check this [URL](#))
- Create a Greengrass group, and download the resource files. (Check this [URL](#))
- Download Greengrass Core binary and install it into Edge Gateway.
- Download Greengrass SDK to write a Lambda function. (Check this [URL](#))
- Upload Lambda function to AWS IoT console page (Check this [URL](#)), and then deploy it to Edge Gateway. (Check this [URL](#))
- Check test result. (Check this [URL](#))

All steps can be found in the Greengrass guide “[Getting Started with AWS IoT Greengrass](#)” (AWS account required), except for “Download Greengrass Core binary and install it into Edge Gateway”. We will show you how to do this with AiR PACE Edge Computing Gateway GUI in next section.

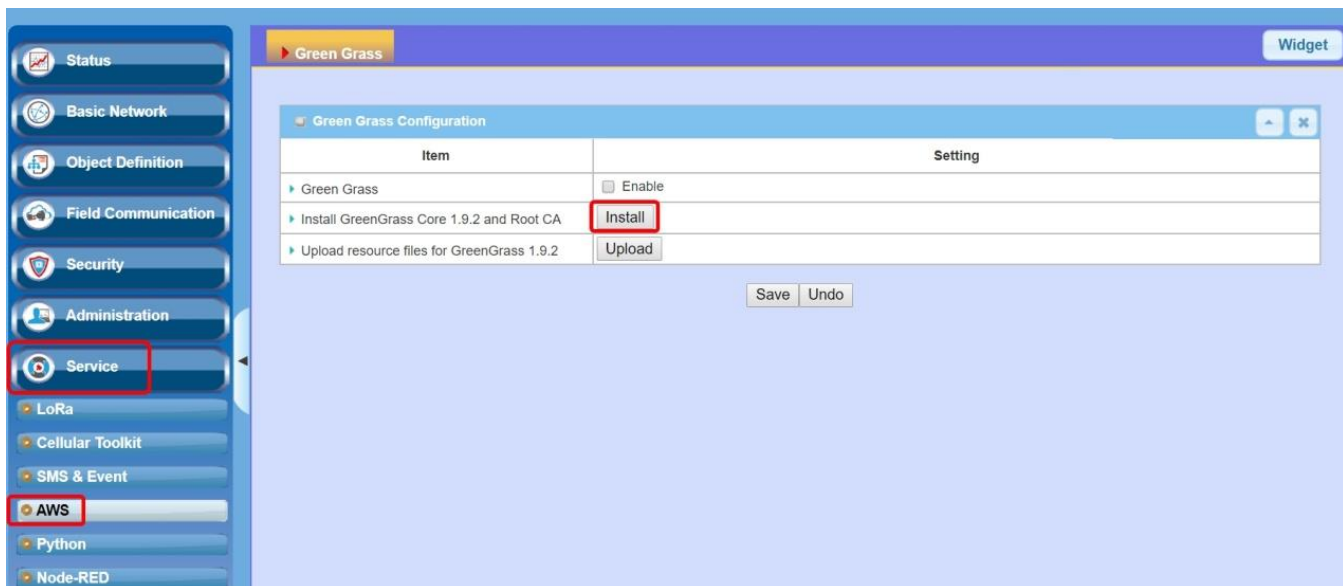
## 8.3.2 Installing Greengrass on AIR PACE

First, you must install the Greengrass Core.



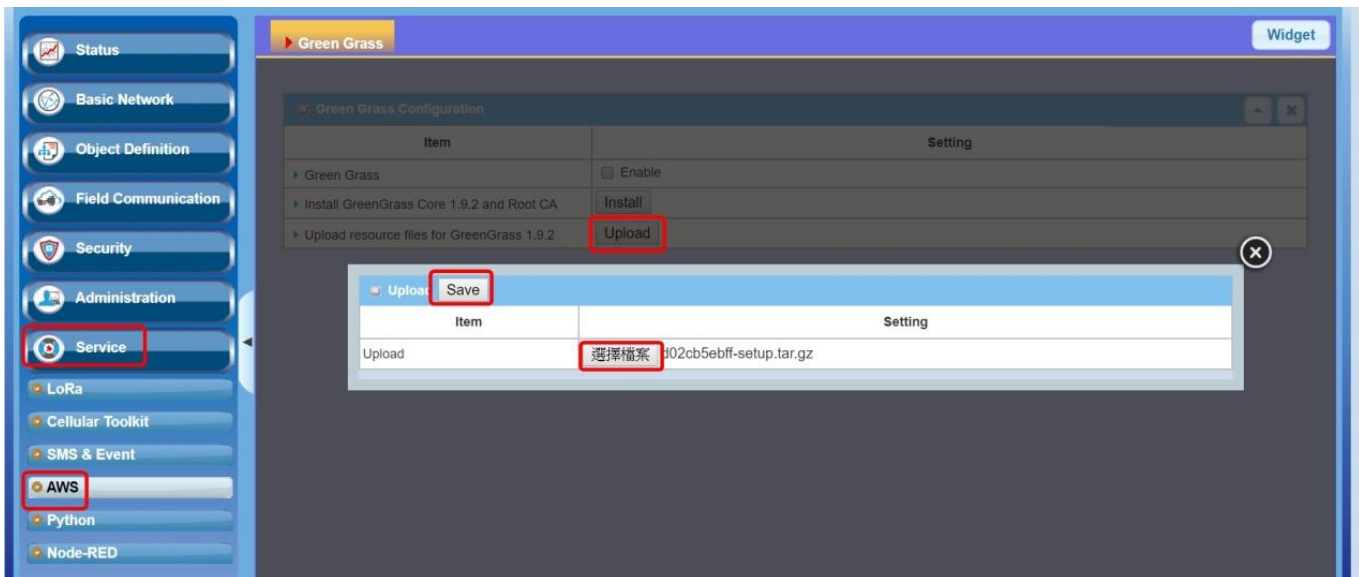
**NOTE:** This installation requires an SD card with EXT4 filesystem inserted into the Edge Gateway. Only the EXT4 file system will work for this installation.

To install Greengrass Core binary, open your browser to the Gateway GUI.  
In Service->AWS, you can see the following page:



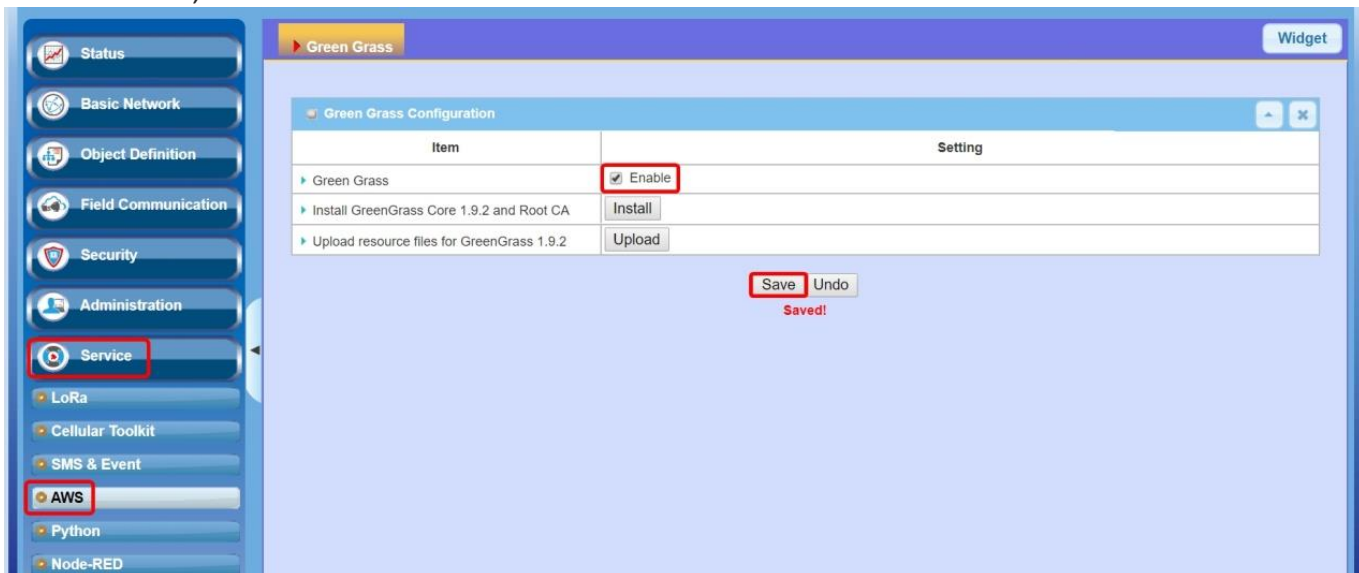
Click the “Install” button, and it will extract built-in Greengrass Core 1.9.2 tarball into SDK. The destination directory should be “/var/usb/C/greengrass”, and then symbolic link to root directory: “/greengrass”.  
You can Telnet/SSH into the Gateway to check the result.

Next, upload the “resource files” that you downloaded from AWS IoT console when you created a Greengrass Core. The file should look like this: “a0b1c2d4e5-setup.tar.gz”, all resource files were compressed together.



Click the button “Upload” and then select the tarball.  
Click the button “Save”, and the Gateway will extract the files into “/greengrass/certs”.  
You can Telnet/SSH into Gateway to check the result.

When all done, check the “Enable” box and then click the “Save” button.



The system will then start the Greengrass Core daemon.

## 8.4 SMS & Event

SMS & Event handling is the application that allows administrator to setup the pre-defined events, handlers, or response behavior with individual profiles. With properly configuring the event handling function, administrator can easily and remotely obtain the status and information via the purchased gateway.

The supported events are categorized into two groups: the **managing events** and **notifying events**.

The **managing events** are the events that are used to manage the gateway or change the settings / status of the specific functionality of the gateway. On receiving the managing event, the gateway will take action to change the functionality, and collect the required status for administration simultaneously.

The **notifying events** are the events that some related objects have been triggered and take corresponding actions on the occurrence of the events. It could be an event for alerting the administrator something happened with SMS message, Email, and SNMP Trap, etc...

For ease of configuration, administrator can create and edit the common pre-defined managing / notifying event profiles for taking instant action on a certain event or managing the devices for some advanced useful purposes. For example, sending/receiving remote managing SMS for the gateway's routine maintenance, and so on. All of such management and notification functions can be realized effectively via the Event Handling feature.

The following is the summary lists for the provided profiles, and events:

- Profiles (Rules):
  - SMS Configuration and Accounts
  - Email Accounts
  - Remote Host profiles
- Managing Events:
  - Trigger Type: SMS, SNMP Trap
  - Actions: Get the Network Status; or Configure the LAN/VLAN behavior, NAT behavior, Firewall behavior, VPN behavior, System Management, Administration, and Remote Host.
- Notifying Events:
  - Trigger Type: Connection Change (WAN, LAN & VLAN, DDNS), Administration, Data Usage.
  - Actions: Notify the administrator with SMS, Syslog, SNMP Trap or Email Alert; Sending collected information to Remote Host.

To use the event handling function, first you have to enable the event management setting and configure the event details with the provided profile settings. You can create or edit pre-defined profiles for individual managing / notifying events. The profile settings are separated into several items; they are the SMS Account Definition, Email Service Definition, and Remote Host Configuration. Then, you have to configure each managing / notifying event with identifying the event's trigger condition, and the corresponding actions (reaction for the event) for the event. For each event, more than one action can be activated simultaneously.

## 8.4.1 Configuration

Go to **Service > SMS & Event > Configuration** Tab.

Event handling is the service that allows administrator to setup the pre-defined events, handlers, or response behavior with individual profiles.

### Enable Event Management

Configuration		
Item	Setting	
▶ Event Management	<input type="checkbox"/> Enable	

Configuration		
Item	Value setting	Description
<b>Event Management</b>	The box is unchecked by default	Check the <b>Enable</b> box to activate the Event Management function.

### Enable SMS Management

To use the SMS management function, you have to configure some important settings first.

SMS Configuration		
Item	Setting	
▶ Message Prefix	<input type="checkbox"/> Enable <input type="text"/>	
▶ Physical Interface	3G/4G-1 ▼ SIM Status: SIM_A	
▶ Delete Managed SMS after Processing	<input type="checkbox"/> Enable	

SMS Configuration		
Item	Value setting	Description
<b>Message Prefix</b>	The box is unchecked by default	Click the <b>Enable</b> box to enable the SMS prefix for validating the received SMS. Once the function is enabled, you have to enter the prefix behind the checkbox. The received managing events SMS must have the designated prefix as an initial identifier, then corresponding handlers will become effective for further processing.
<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> ) to configure the SMS management setting. <b>Note:</b> <b>3G/4G-2</b> is only available for for the product with dual cellular module.

<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>	The box is 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

Setup the SMS Account for managing the gateway through the SMS. It supports up to a maximum of 5 accounts.

SMS Account List <span>Add</span> <span>Delete</span> <span>⬆</span> <span>✕</span>						
ID	Phone Number	Phone Description	Application	Send confirmed SMS	Enable	Actions

You can click the **Add / Edit** button to configure the SMS account.

SMS Account Configuration <span>✕</span>	
Item	Setting
▶ Phone Number	Specific Number ▼ <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
<span>Save</span>	

SMS Account Configuration		
Item	Value setting	Description
<b>Phone Number</b>	1. Mobile phone number format 2. A Required setting	Select the Phone number policy from the drop 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, you have to specify the phone number as the SMS account identifier. <b>Value Range:</b> -1 ~ 32 digits.
<b>Phone Description</b>	1. Any text 2. An Optional setting	Specify a brief description for the SMS account.
<b>Application</b>	A 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 Noftify Handle will be unavailable.
<b>Send confirmed SMS</b>	1. An Optional setting 2. The box is unchecked by default.	Click <b>Enable</b> box to active the SMS response function. The gateway will send a confirmed message back to the sender whenever it received a SMS managing event. The confirmed message is similar to following format: "Device received a SMS with command xxxxx."
<b>Enable</b>	The box is 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

Setup the Email Service Account for event notification. It supports up to a maximum of 5 accounts.

Email Service List <span>Add</span> <span>Delete</span> <span>▲</span> <span>✕</span>				
ID	Email Server	Email Addresses	Enable	Actions

You can click the **Add / Edit** button to configure the Email account.

Email Service Configuration <span>✕</span>	
Item	Setting
▶ Email Server	--- Option --- ▼
▶ Email Addresses	<input type="text"/>
▶ Enable	<input checked="" type="checkbox"/> Enable
<span>Save</span>	

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. A Required setting	Specify the Destination Email Addresses.
<b>Enable</b>	The box is 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 Remote Host Profile

Setup 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

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"/>

Save

Remote Host Configuration		
Item	Value setting	Description
<b>Host Name</b>	1. String format 2. A Required setting	Specify the Remote Host profile name. <b><u>Value Range:</u></b> -1 ~ 64 characters.
<b>Host IP</b>	1. A Required setting 2. IP Address format.	Specify the IP address for the Remote Host. IPv4 Format.
<b>Protocol Type</b>	1. A Required setting 2. TCP is selected by default	Specify the protocol to access the Remote Host. It could be <b>TCP or UDP</b> .
<b>Port Number</b>	1. A Required setting	Specify the Port number for accessing the Remote Host. <b><u>Value Range:</u></b> 1 ~ 65535.
<b>Prefix Message</b>	1. String format 2. An Optional filled setting	Specify the Prefix Message string as pre-defined identification for accessing the remote host, if required. <b><u>Value Range:</u></b> -1 ~ 64 characters.
<b>Suffix Message</b>	1. String format 2. An Optional filled setting	Specify the Suffix Message string as pre-defined identification for accessing the remote host, if required. <b><u>Value Range:</u></b> -1 ~ 64 characters.
<b>Enable</b>	The box is 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 what you just configured back to the previous setting.

8.4.2 Managing Events

Managing Events allow administrator to define the relationship (rule) among event trigger, handlers and response.

Go to **Service > SMS & Event > Managing Events** Tab.

Enable Managing Events

Configuration

Item	Setting
Managing Events	<input type="checkbox"/> Enable

Configuration

Item	Value setting	Description
Managing Events	The box is unchecked by default	Check the <b>Enable</b> box to activate the Managing Events function.

Create / Edit Managing Event Rules

Setup the Managing Event rules. It supports up to a maximum of 128 rules.

Managing Event List

AddDelete

ID	Event Name	Event	Trigger Type	Description	Enable	Actions
----	------------	-------	--------------	-------------	--------	---------

When **Add** or **Edit** button is applied, the **Managing Event Configuration** screen will appear.

**Managing Event Configuration**

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"/> Network Status <input type="checkbox"/> WAN <input type="checkbox"/> LAN&VLAN <input type="checkbox"/> WiFi <input type="checkbox"/> NAT <input type="checkbox"/> Firewall <input type="checkbox"/> VPN <input type="checkbox"/> GRE <input type="checkbox"/> System Manage <input type="checkbox"/> Administration <input type="checkbox"/> Digital Output <input type="checkbox"/> Remote Host
▶ Managing Event	<input checked="" type="checkbox"/> Enable

Managing Event Configuration		
Item	Value setting	Description
<b>Event</b>	<b>None</b> by default	<p>Specify the Event type (<b>SMS</b>, or <b>SNMP Trap</b>) and an event identifier / profile. Up to 3 event conditions can be specified for defining an event, and the event will be triggered when all the conditions hold simultaneously (AND relation).</p> <p>The supported Event types could be:  <b>SMS</b>: Select <b>SMS</b> and fill the message in the textbox to as the trigger condition for the event;  <b>SNMP</b>: Select <b>SNMP Trap</b> and fill the message in the textbox to specify SNMP Trap Event;</p> <p><i>Note: The available Event Type could be different for the purchased product.</i></p>
<b>Trigger Type</b>	<b>Period</b> is selected by default	<p>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.</p>
<b>Interval</b>	<b>0</b> is set by default	<p>Specify the repeatedly event trigger time interval.</p> <p><b>Value Range</b>: 0 ~86400 seconds.</p>
<b>Description</b>	String format: any text.	Enter a brief description for the Managing Event.
<b>Action</b>	All boxes unchecked by	Specify <b>Network Status</b> , or at least one rest action to take when the expected

	default.	<p>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), 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, TR-069 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>Remote Host:</b> Select <b>Remote Host</b> checkbox and a Remote Host profile you defined as the action for the event;</p> <p><i>Note: The available Event Type may differ by product model.</i></p>
<b>Managing Event</b>	The box is 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 what you just configured back to the previous setting.

## 8.4.3 Notifying Events

Go to **Service > SMS & Event > 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
<b>Notifying Events</b>	The box is unchecked by default	Check the <b>Enable</b> box to activate the Notifying Events function.

### Create / Edit Notifying Event Rules

Setup your Notifying Event rules. It supports up to a maximum of 128 rules.

Notifying Event List										
		Add	Delete							
ID	Event Name	Event	Trigger Type	Description	Action	Time Schedule	Enable	Actions		

When **Add** or **Edit** button is applied, the **Notifying Event Configuration** screen will appear.

Notifying Event Configuration		
Item	Setting	
▶ Event Name	<input type="text"/>	
▶ Event	None ▼	
	None ▼	
	None ▼	
▶ Trigger Type	Period ▼	
▶ Interval	<input type="text"/> (0~86400 seconds)	
▶ Description	<input type="text"/>	

▶ Action	<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"/> Remote Host
▶ Time Schedule	(0) Always ▼
▶ Notifying Events	<input checked="" type="checkbox"/> Enable

Notifying Event Configuration		
Item	Value setting	Description
<b>Event</b>	<b>None</b> by default	<p>Specify the Event type and corresponding event configuration. Up to 3 event conditions can be specified for defining an event, and the event will be triggered when all the conditions hold simultaneously (AND relation).</p> <p>The supported Event Type could be:  <b>Power Change:</b> Select <b>Power Change</b> and a trigger condition to specify the event on a certain 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&amp;VLAN 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>Data Usage:</b> Select <b>Data Usage</b>, the SIM Card (Cellular Service) and a trigger condition to specify a certain Data Usage Event;</p> <p><i>Note: The available Event Type could be different for the purchased product.</i></p>
<b>Description</b>	String format: any text.	Enter a brief description for the Notifying Event.
<b>Action</b>	All box is unchecked by default.	<p>Specify at least one action to take when the expected event is triggered.  <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;  <b>Syslog:</b> Select <b>Syslog</b> and select/unselect the Enable Checkbox to as the action for the event;  <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;  <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;  <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><i>Note: The available Event Type may differ by 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>	The box is 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 what you just configured back to the previous setting.

## 8.5 Azure Run Time

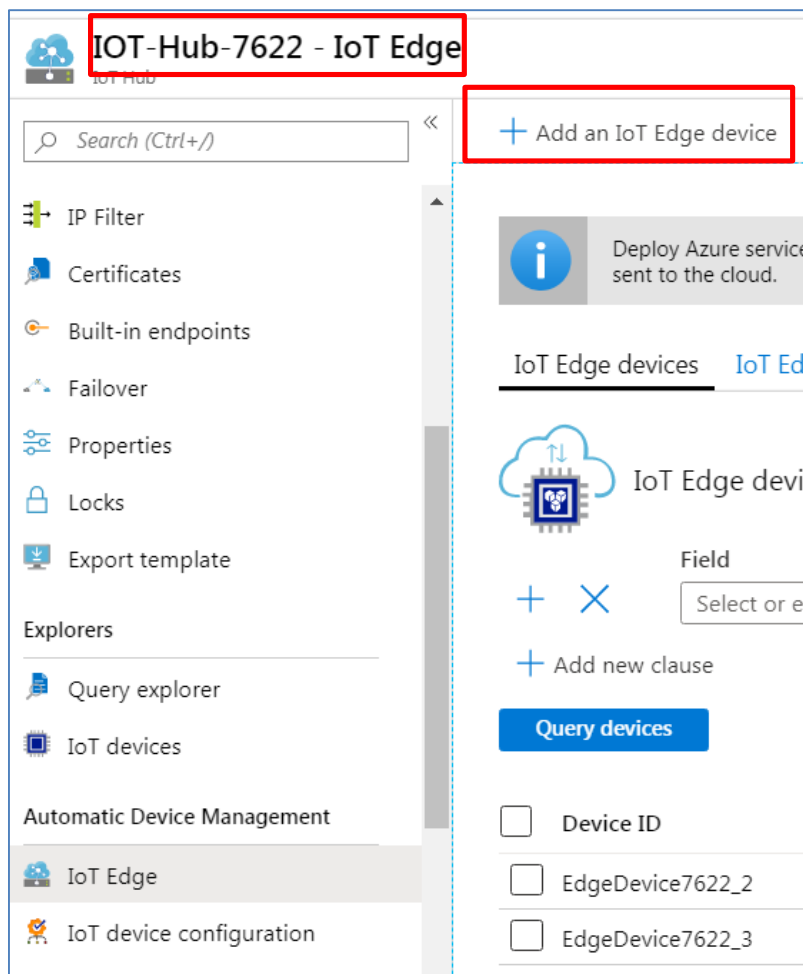
Microsoft Azure is a comprehensive set of cloud services to help your organization meet your business challenges. It delivers the ability to build, manage, and deploy applications on a large scale network using the most popular tools and frameworks. Azure is a highly secure and easy-to-use solution that extends IT infrastructure and enables edge device connectivity in industrial applications.

### 8.5.1 Setup - Get Connection String from Edge Device

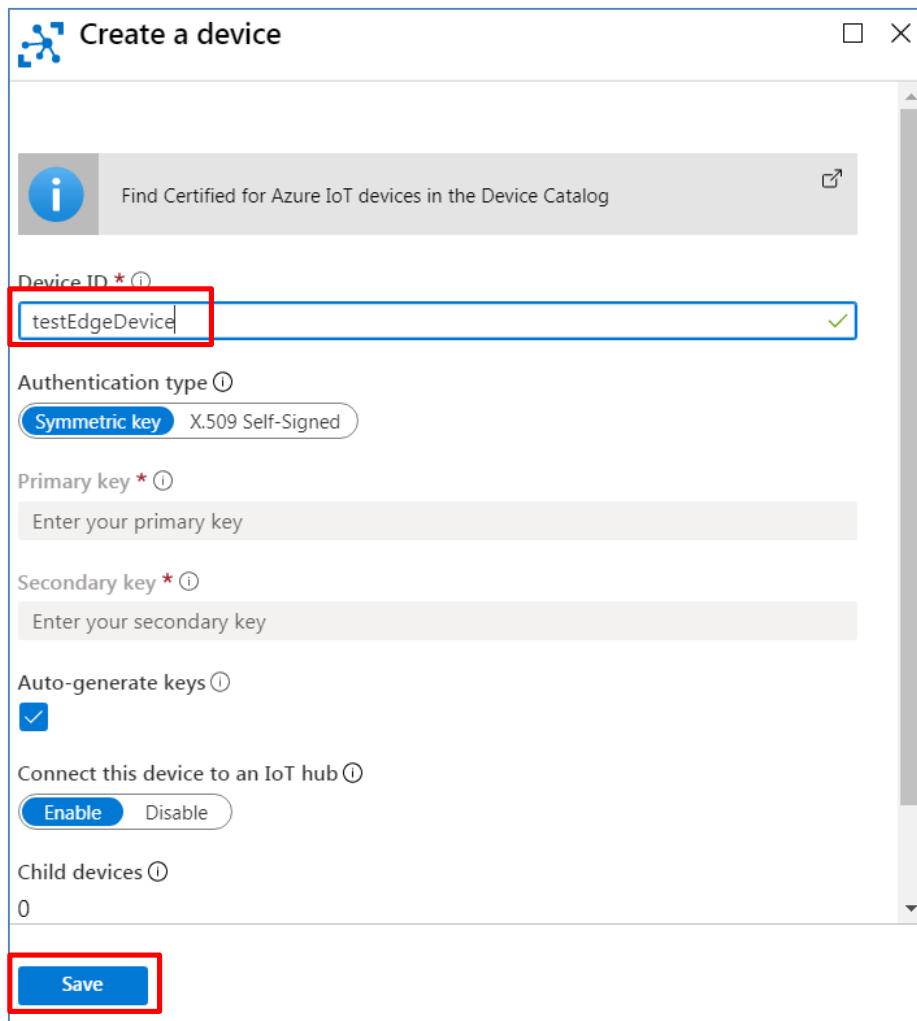


**NOTE:** This installation requires an SD card with EXT4 filesystem inserted into the Edge Gateway. Only the EXT4 file system will work for this installation.

Set up devices to be managed by Azure Run Time by first logging into the Azure IoT Hub at <https://azure.microsoft.com/en-us/services/iot-hub/>. Then navigate to IoT Hub → IoT Edge → Create a device → Device ID field.



Fill in “Device ID” and Click “Save” to create IoT Edge device



**Create a device**

Find Certified for Azure IoT devices in the Device Catalog

Device ID \* ⓘ  
testEdgeDevice ✓

Authentication type ⓘ  
Symmetric key X.509 Self-Signed

Primary key \* ⓘ  
Enter your primary key

Secondary key \* ⓘ  
Enter your secondary key

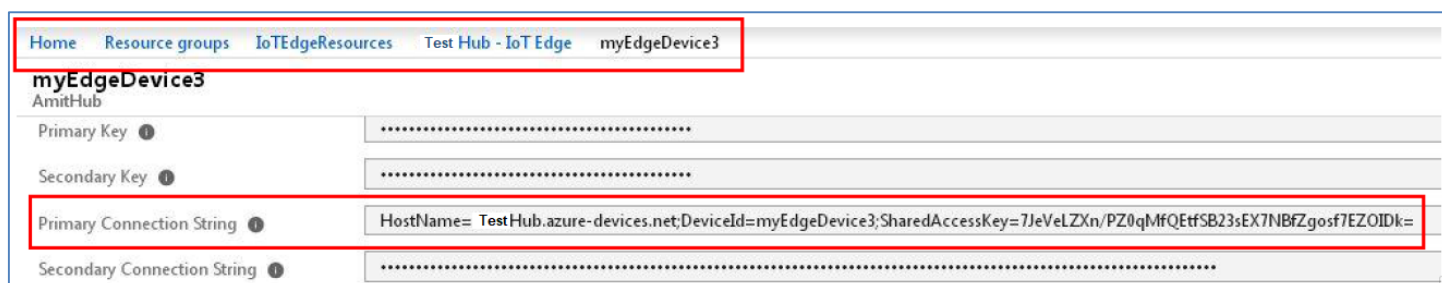
Auto-generate keys ⓘ  
☒

Connect this device to an IoT hub ⓘ  
Enable Disable

Child devices ⓘ  
0

Save

Copy “Primary Connection String” and then click “Set Modules”.



Home Resource groups IoTEdgeResources Test Hub - IoT Edge myEdgeDevice3

**myEdgeDevice3**  
AmitHub

Primary Key ⓘ  
.....


Secondary Key ⓘ  
.....

Primary Connection String ⓘ  
HostName= TestHub.azure-devices.net;DeviceId=myEdgeDevice3;SharedAccessKey=7JeVeLZXn/PZ0qMfQEtfSB23sEX7NBfZgosf7EZOIDk=

Secondary Connection String ⓘ  
.....



Click “Configure advanced Edge Runtime settings”


 **Set modules**  
Set modules

1 Add Modules (optional)

2 Specify Routes (optional)


3 Review Deployment

Name	Address
<input type="text"/>	<input type="text"/>

 An IoT Edge module is a Docker container you can deploy to IoT Edge devices. Setting modules on each device will be counted towards the quota and

Deployment Modules

+ Add

 Delete

<input type="checkbox"/>	Name	Desired Status
No Modules Found		

Configure advanced Edge Runtime settings

Because port 443 is being used, change the “HostPort” from 443 to 4443.

## Runtime Settings

^ Edge Hub

Image \* ⓘ

mcr.microsoft.com/azureiotedge-hub:1.0

Store and forward configuration – time to live (seconds) ⓘ

7200

Create Options ⓘ


```

{
  "HostConfig": {
    "PortBindings": {
      "443/tcp": [
        {
          "HostPort": "443"
        }
      ],
      "5671/tcp": [
        {
          "HostPort": "5671"
        }
      ],
      "8883/tcp": [
        {
          "HostPort": "8883"
        }
      ]
    }
  }
}

```

Save

Click “Next”


**Set modules**  
Set modules


1 Add Modules (optional)

2 Specify Routes (optional)

3 Review Deployment

Name


Address



An IoT Edge module is a Docker container you can deploy to IoT Edge devices. It communicates with module. Setting modules on each device will be counted towards the quota and throttled based on t

Deployment Modules

+ Add

 Delete

☐

Name

Desired Status


No Modules Found

Configure advanced Edge Runtime settings

Previous

Next


Click “Next” again.


**Set modules**  
Set modules

1 Add Modules (optional)

2 Specify Routes (optional)

3 Review Deployment



You can set routes between modules, which gives you the flexibility to send messages where they need to go witho


```

1 {
2   "routes": {
3     "route": "FROM /messages/* INTO $upstream"
4   }
5 }
```

Previous

Next


Then click “Submit”.


**Set modules**  
Set modules

Add Modules  
(optional)

2 Specify Routes  
(optional)

3 **Review Deployment**


Below is a summary of the current deployment.

```

1 {
2   "modulesContent": {
3     "$edgeAgent": {
4       "properties.desired": {
5         "modules": {},
6         "runtime": {
7           "settings": {
8             "minBockerVersion": "v1.25"
9           },
10          "type": "docker"
11        },
12        "schemaVersion": "1.0",
13        "systemModules": {
14          "edgeAgent": {
15            "settings": {
16              "image": "mcr.microsoft.com/azureiotedge-agent:1.0",
17              "createOptions": ""
18            },

```

Previous
Next

Submit

## 8.5.2 Start Azure Runtime

Check the “Enable” box, and paste the copied Connection String into the field so named. Then click “Save”.

Item	Setting
Azure RunTime	<input checked="" type="checkbox"/> Enable
Connection String	HostName=IoT-Hub-7622.azure-devices.net;DeviceId=testEdgeDevice;SharedAccessKey=A+75U0RA9bY2wLe3nfzBywQLd07UC5x9nBBFue3iDdw=

Save Undo

Saved!

Click “Refresh” to show the module status.

Azure Run Time Configuration						
Item	Setting					
Azure RunTime	<input checked="" type="checkbox"/> Enable					
Connection String	HostName=IoT-Hub-7622.azure-devices.net;DeviceId=testEdgeDevice;SharedAccessKey=A+75U0RA9bY2wLe3nfzBywQLd07UC5x9nBBFue3iDdw=					

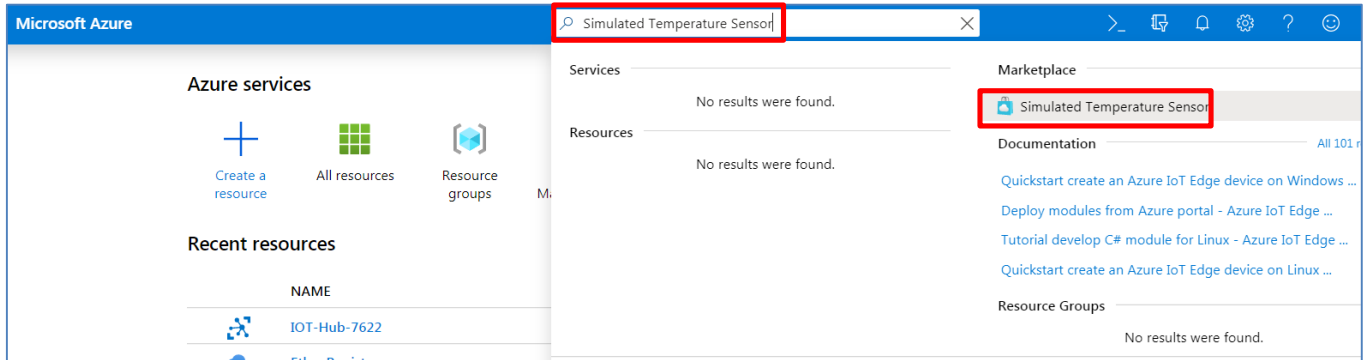
  

Module List						
Refresh						
Name	Status	Description	Config	Show log		
edgeHub	running	Up 30 seconds	mcr.microsoft.com/azureiotedge-hub:1.0	Show		
edgeAgent	running	Up a minute	mcr.microsoft.com/azureiotedge-agent:1.0	Show		

## 8.5.3 Deploy a module

For this example, a simulated temperature sensor will be deployed.

In the Azure portal, enter Simulated Temperature Sensor into the search field and open the Marketplace result.



Select the desired “IoT Hub” from the dropdown menu, then enter the IoT Edge Device Name”. Then click “Create”

### Target Devices for IoT Edge Module

Microsoft

Subscription \* ⓘ

CSP-AZURE

IoT Hub \* ⓘ

IOT-Hub-7622

Deploy to a device Deploy at Scale

IoT Edge Device Name \* ⓘ

testEdgeDevice

Find Device

By deploying this module, I agree to the provider's [terms of use](#) and [privacy policy](#) and understand that the rights to use this product do not come from Microsoft, unless Microsoft is the provider. Use of Azure Marketplace is governed by separate terms.

Create

Click “Next”.

**Set modules**  
Set modules

1 Add Modules (optional)
2 Specify Routes (optional)
3 Review Deployment

Name	Address	U
<input type="text"/>	<input type="text"/>	<input type="text"/>

An IoT Edge module is a Docker container you can deploy to IoT Edge devices. It communicates with other modules and sends module. Setting modules on each device will be counted towards the quota and throttled based on the IoT Hub tier and units.

Deployment Modules

+ Add
Delete

<input type="checkbox"/> Name	Desired Status	
<input type="checkbox"/> SimulatedTemperatureSensor	running	<a href="#">Configure</a>

Configure advanced Edge Runtime settings

Previous

Next

Click “Next” again on the following screen.

**Set modules**  
Set modules

1 Add Modules (optional)
2 Specify Routes (optional)
3 Review Deployment

You can set routes between modules, which gives you the flexibility to send messages where they need to go without the need


```

1 {
2   "routes": {
3     "route": "FROM /messages/* INTO $upstream",
4     "upstream": "FROM /messages/* INTO $upstream"
5   }
6 }
```

Previous

Next


Click “Submit”.


**Set modules**  
Set modules

1 Add Modules  
(optional)

2 Specify Routes  
(optional)

3 Review Deployment


Below is a summary of the current deployment.

```

1 {
2   "modulesContent": {
3     "$edgeAgent": {
4       "properties.desired": {
5         "modules": {
6           "simulatedTemperatureSensor": {
7             "settings": {
8               "image": "mcr.microsoft.com/azureiotedge-simulated-temperature-sensor:1.0",
9               "createOptions": ""
10            },
11            "type": "docker",
12            "status": "running",
13            "restartPolicy": "always",
14            "version": "1.0"
15          }
16        }
17      },
18      "runtime": {
19        "settings": {

```

Previous
Next

Submit



## 8.5.4 Show module status in Azure Runtime UI

Click “Refresh” in the UI as shown below, and the module information will display.

The screenshot shows the Azure Runtime UI interface. At the top, there's a header with "Azure RunTime" and a "Widget" button. Below this is the "Azure RunTime Configuration" section, which includes a table with "Item" and "Setting" columns. The "Item" column lists "Azure RunTime" and "Connection String". The "Setting" column shows "Enable" checked and a connection string: "HostName=IoT-Hub-7622.azure-devices.net;DeviceId=testEdgeDevice;SharedAccessKey=A+75U0RA9bY2wLe3nfzByWQLd07UC5x9nBBfUe3iDdw=". Below the configuration section is the "Module List" section, which has a "Refresh" button highlighted with a red box. The "Module List" section contains a table with columns: "Name", "Status", "Description", "Config", and "Show log". The table lists three modules: "edgeAgent" (running), "edgeHub" (running), and "SimulatedTemperatureSensor" (running). Each module has a "Show" button next to its "Show log" column. At the bottom of the interface, there are "Save" and "Undo" buttons, and a "Saved!" message.

Click “show” to open the file of logs for the module.

The screenshot shows the Azure Runtime UI interface with the log file for the "edgeAgent" module open. The log file is titled "txt\_data - Google Chrome" and shows the following content:

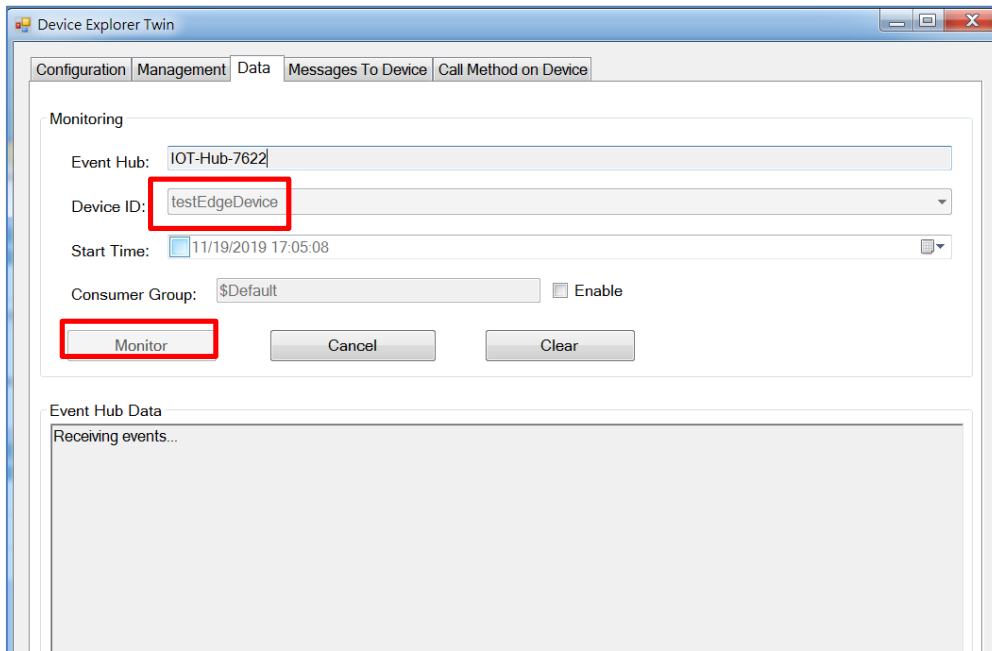
```

2019-11-21 07:53:59 +00:00 Starting Edge Agent
2019-11-21 07:54:00.349 +00:00 Edge Agent Main()
<6> 2019-11-21 07:54:01.909 +00:00 [INF] - Initializing Edge Agent.
<6> 2019-11-
21 07:54:03.038 +00:00 [INF] - Version - 1.0.8.4.26769994 (7f452949464b45ed67f1cdcc5755654d211674ab)
<6> 2019-11-21 07:54:03.041 +00:00 [INF] -

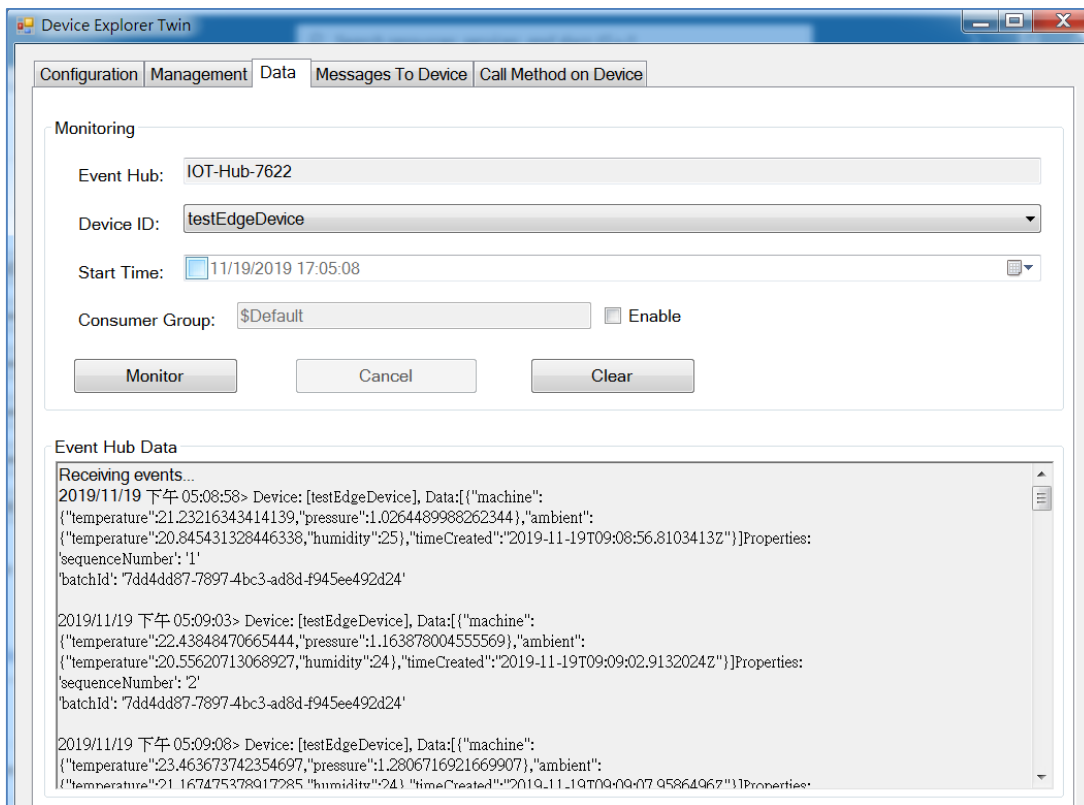
```

The log file also displays a large, stylized "AIR PACE" logo. Below the log file, the "Module List" section is visible, showing the "edgeAgent" module with a "Show" button next to its "Show log" column. The "Show" button is highlighted with a red box. At the bottom of the interface, there are "Save" and "Undo" buttons, and a "Saved!" message.

The messages from devices to IoT Hub can be viewed in Device Explorer. Select a device and click “Monitor”.



The messages from device to IoT Hub will display.



## 8.6 Location Tracking

Location tracking applications are usually referred to applications that take benefits from Global Navigation Satellite System (GNSS). GNSS is the infrastructure that allows devices to determine its position, velocity, and time by processing satellites signals from outer space. GNSS includes varieties of satellite systems and Satellite-Based Augmentation Systems (SBAS). SBAS is usually used for improving positioning accuracy. The tables below show 4 major GNSS system in the world, and SBAS system in different areas.

**Major GNSS System in the world**

GNSS System	Owner
GPS	USA
GLONASS	Russia
Galileo	European Union
BeiDou (COMPASS)	China

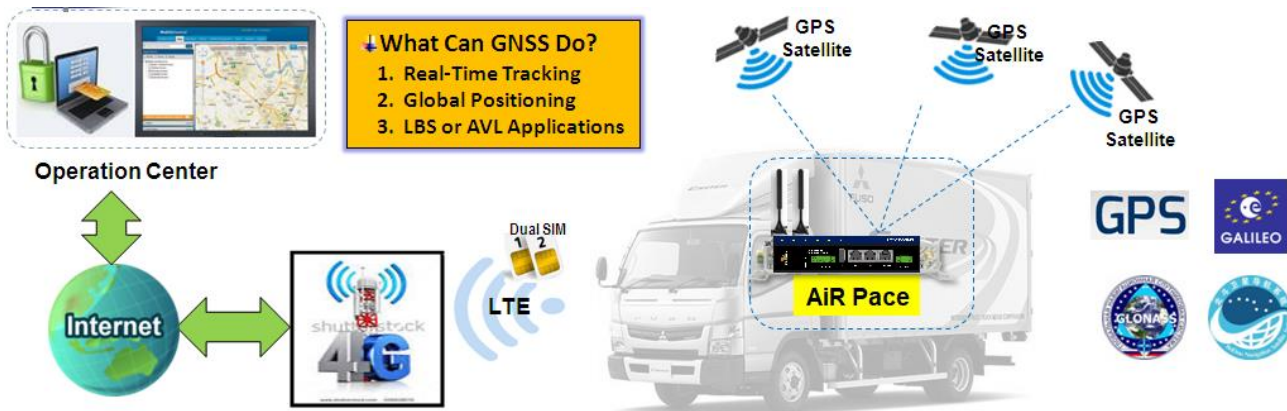
**Satellite-Based Augmentation System (SBAS)**

SBAS	Area Coverage
EGNOS	Europe
WAAS	North America
GAGAN	India
MSAS	Japan

Position applications are widely-used by varieties of industrial applications, including Location-Based Services (LBS), Automatic Vehicle Location (AVL), Fleet Management, or assets tracking. However, in most case, GNSS is a one-way communication. That means GNSS-compatible device can only locate its location by receiving GNSS signal, but it can't forward its location data to any other identity through GNSS system. According to this limitation by GNSS system, devices usually need other technology to transmit their location data to a back-end server for tracking or further analysis. Furthermore, as the position applications are more applied on moving objects, a kind of wireless technology would be more suitable to be adopted to transmit location data. Nowadays, thanks to popularity and wide coverage of cellular technology (GSM, 3G, 4G/LTE), transmitting location data to remote center in real time is no longer a hurdle. In addition, the data format of location data is NMEA 0183 compatible, so the back-end server will be easy to interpret the collected location data.

Hereunder are the main features of GNSS function in cellulargateway, if optional GNSS function is supported.

# AiR PACE



- Retrieve GNSS data from satellites and send to remote operation center periodically or save in local storage.
- Global positioning with multiple GNSS systems, including GPS, and optional for GLONASS, Galileo, or BeiDou.
- Mandatory for varieties of LBS (Location-Based Service) applications, such as advertisement, emergent call.
- Easy integration with AVL (Automatic Vehicle Location) applications, for managing fleet of service vehicles.
- Other value-added applications, such as asset tracking, electronic toll collection, intelligent transport system.

## 8.6.1 GNSS

With GNSS configuration page, you can configure those functions that are mentioned above. Please note the available GNSS features on different models may be different. Please check product datasheet for details.

The configuration steps include following items.

- Activate GNSS feature in gateway and finish settings of cellular WAN.
- Support NMEA 0183 (compatible to 3.0) protocol, and allow customized prefix and suffix.
- Configure GPS data logging on local microSD card storage for route record tracking.
- Indicate remote host, time interval, TCP/UDP, and type of GPS data that would be sent.

### ● GPS Message Type

This item shows all supported types of NMEA 0183 data format. NMEA 0183 data format was defined and maintained by National Marine Electronics Association (NMEA). Select one or more types that you want to use for transmitting GPS data. In most case, this configuration depends on which data format that your central server can recognize. Only select the type you need, otherwise it will consume unnecessary network bandwidth. The table below shows more information for different types of NMEA 0183 message.

Type	Description	Example
GGA	Fix Information	\$GPGGA,123519,4807.038,N,01131.000,E,1,08,0.9,545.4,M,46.9,M,,,*47
GLL	Lat/Lon Data	\$GPGLL,4916.45,N,12311.12,W,225444,A,*1D
GSA	Overall Satellite Data	\$GPGSA,A,3,04,05,,09,12,,,24,,,,,2.5,1.3,2.1*39

# AIR PACE

GSV	Detailed Satellite Data	\$GPGSV,2,1,08,01,40,083,46,02,17,308,41,12,07,344,39,14,22,228,45*75
RMC	Recommended Minimum Data	\$GPRMC,123519,A,4807.038,N,01131.000,E,022.4,084.4,230394,003.1,W*6A
VTG	Vector Track and Speed Over the Ground	\$GPVTG,054.7,T,034.4,M,005.5,N,010.2,K*48

Please note this option is hardware dependent. The available options of GPS message type show on this page is according to product specification. You may not see all options if your product doesn't support all of them.

## ● SBAS

SBAS is Satellite-Based Augmentation Systems that is used to improve accuracy of location data. There are several SBAS systems for different areas in the world.

SBAS	Area Coverage
EGNOS	Europe
WAAS	North America
GAGAN	India
MSAS	Japan

Please note this option is hardware dependent. You may not see this option if your product doesn't support it.

## ● Assisted GPS

Assisted GPS (as known as A-GPS) is used for speeding up location fix, especially when satellite signal is weak. If activating this option, gateway will download almanac data from A-GPS server through IP network instead of from satellite. You can also choose different validity periods of almanac data. The shorter almanac data will get higher accuracy. However, the almanac data with shorter validity period needs to be updated more frequently. It will consume more network bandwidth. Please note this option is hardware dependent. You may not see this option if your product doesn't support it.

## ● Data to Storage

Besides transmitting location data to remote server, you can also store location data into internal storage (e.g. microSD card) or external storage (e.g. USB drive) if any. Regarding to data format, it can either be NMEA 0183 raw data format or GPX file format. The location data will be saved to a new file if the original file size is bigger than the pre-defined file size. The "Download log file" button allows you to browse all saved log files and download to your personal devices.

## ➤ Scenario of location tracking for fleet management

A fleet owner would like to see the locations of his trucks in real time. He also likes to know where his trucks have passed through with time information. In his operations office, there is a server (IP: 100.100.100.1) which can interpret NMEA RMC data format and shows a truck's location and track on map. This server is listening on TCP port 888 to receive NMEA RMC packet from trucks. IMEI number will be added before NMEA RMC data for identification of each truck. Hereunder is the configuration on each truck.

### Basic Settings:

Configuration Path	[GNSS]-[Configuration]
GNSS	<i>Enable</i>
GNSS Type	<i>GPS</i>
GPS Message Types	<i>RMC</i>
SBAS	<i>Enable</i>
Assisted GPS	<i>Enable, 1</i>
Data to Storage	<i>Disable</i>

### Settings for Remote Host:

Configuration Path	[GNSS]-[Remote Host Configuration]
Host Name	<i>Truck-1</i>
Host IP	<i>100.100.100.1</i>
Protocol Type	<i>TCP</i>
Port Number	<i>888</i>
Interval(s)	<i>15</i>
Prefix Message	<i>123456789012345</i>
Suffix Message	<i>[blank]</i>
Enable Checkbox	<i>[Checked]</i>

## GNSS Setting

Go to **Service>Location Tracking> GNSS** Tab.

The GNSS allows user to set the configuration of GNSS, log NMEA data to storage, and send data to remote host. Ensure GNSS is enabled and saved

### Setup GNSS Configuration

Configuration

Item	Setting
▶ GNSS	<input checked="" type="checkbox"/> Enable
▶ GNSS Type	GPS ▼
▶ GNSS Message Types	<input checked="" type="checkbox"/> RMC
▶ Assisted GPS	<input checked="" type="checkbox"/> Enable
▶ Data to Storage	<div> <input type="checkbox"/> Enable           Select Device: Internal ▼         </div> <div>Interval: 5 (s)</div> <div>Data format: RAW ▼</div> <div>Data file name: </div> <div>Split file: <input type="checkbox"/> Enable Size: 200 KB ▼</div> <div>           ▼ Download log file Delete log file         </div>

GNSS Configuration		
Item	Value setting	Description
<b>GNSS Enable</b>	The box is unchecked by default	Check <b>Enable</b> box to activate GNSS functions.
<b>GNSS Type</b>	<b>GPS</b> is selected by default	Select a <b>GNSS Type</b> (GNSS System) that you want to use. Please note this option is hardware dependent. The available options of GNSS type show on this page is according to product specification. You may not see all of these four options if your product doesn't support all of them.
<b>GNSS Message Types</b>	Boxes are unchecked by default.	<p>Select one or more <b>GNSS Message Types</b> that you want to use for transmitting or recording GPS data.</p> <p>There are many sentences in the NMEA standard for selecting, <b>GGA</b>, <b>GLL</b>, <b>GSA</b>, <b>GSV</b>, <b>RMC</b> and <b>VTG</b>. <b>ALL Other</b> includes DTM, GNS, GRS, GST, ZDA, and GBS sentences.</p> <p>Only select the type you need, otherwise it will consume unnecessary network bandwidth.</p> <p>Note: The supported message type is hardware dependent.</p>
<b>SBAS</b>	The box is unchecked by default	Check <b>Enable</b> box to activate satellite-based augmentation system ( <b>SBAS</b> ). Note: Some devices do not support this function.
<b>Assisted GPS</b>	The box is checked by default	Check <b>Enable</b> box to activate Assisted GPS (A-GPS). Select the duration for downloading the <b>Differential Almanac Corrections</b> data

		from A-GPS server through IP network. Note: Some devices may not support this function.
<b>Data to Storage</b>	The box is unchecked by default	<ul style="list-style-type: none"> <li>● <b>Enable</b> (The box is unchecked by default) Check <b>Enable</b> box to activate data to storage function.</li> <li>● <b>Select Device</b> (A Required setting) Select <b>Internal</b> or <b>External</b> device to store log data.</li> <li>● <b>Interval</b> (A Required setting) Specify the time interval between two continuous data logs. By default, 5 seconds is set. <b>Value Range:</b> 5 ~ 60 seconds.</li> <li>● <b>Data Format</b> (A Required setting) Select data format (<b>RAW</b>, or <b>GPX</b>) to store.</li> <li>● <b>Data file name</b> (A Required setting) Define file name to store.</li> <li>● <b>Split Enable</b> Check <b>Enable</b> box to activate file splitting function.</li> <li>● <b>Split Size &amp; Unit</b> Define file size and unit for log file. By default, 200 KB is defined. <b>Value Range:</b> &gt;= 10KB (Minimum file size is 10 KB).</li> <li>● <b>Download log file</b> Select a log file and Click <b>Download log file</b> to download through Web GUI. If the log format which is specified to download is GPX, it will be converted to standard GPX format.</li> </ul>
<b>Save</b>	NA	Click the <b>Save</b> button to save the configuration

## Create / Edit Remote Host

The Remote Host allows you to customize your rules for sending NMEA data to specific IP address and Port. The router supports up to a maximum of 10 rule sets.

Remote Host List										
ID	Host Name	Host IP	Protocol Type	Port Number	Interval(s)	MAC Address Message	Prefix Message	Suffix Message	Enable	Actions

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

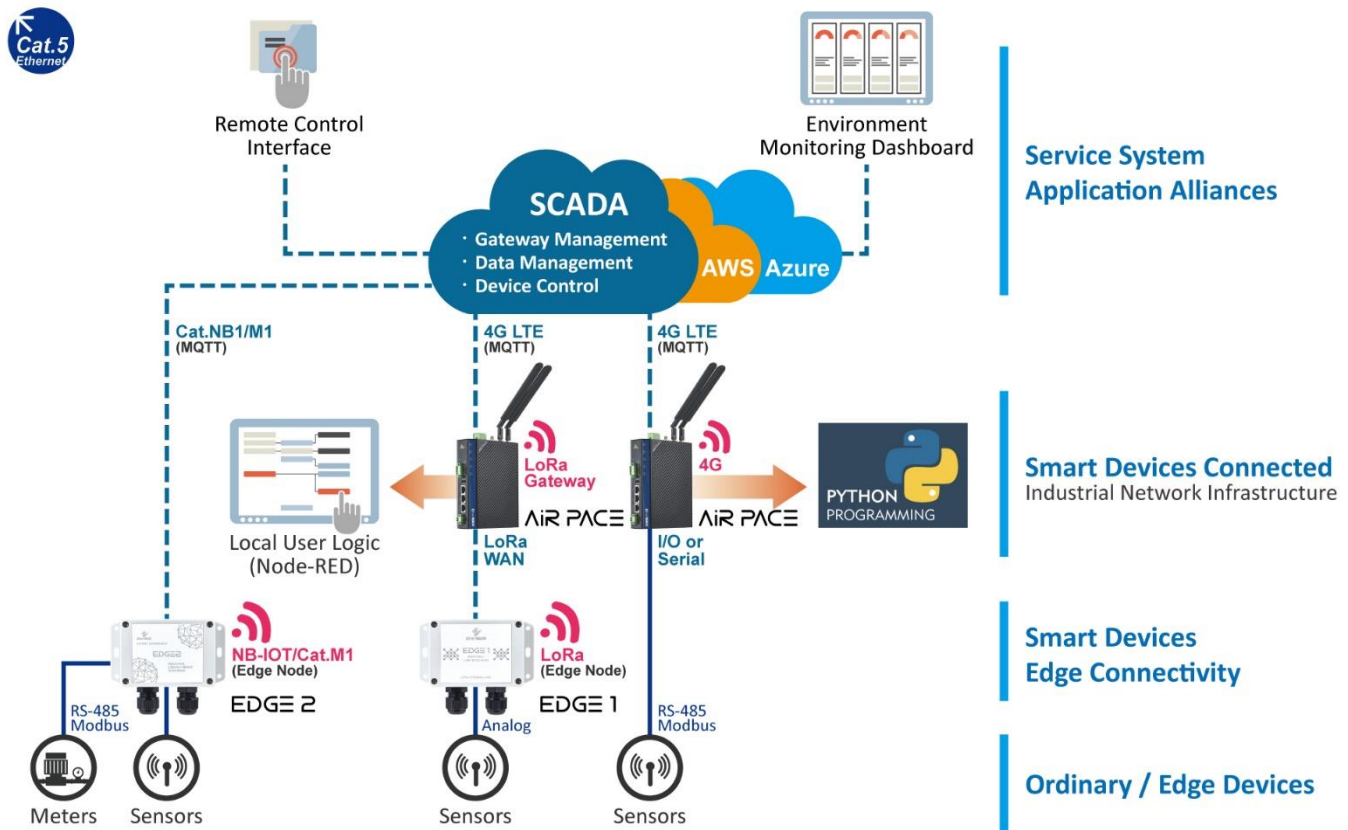


Remote Host Configuration	
Item	Setting
▶ Host Name	<input type="text"/>
▶ Host IP	<input type="text"/>
▶ Protocol Type	TCP ▼
▶ Port Number	<input type="text"/>
▶ Interval(s)	1 <input type="text"/>
▶ MAC Address Message	<input type="checkbox"/>
▶ Prefix Message	<input type="text"/>
▶ Suffix Message	<input type="text"/>
▶ Enable	<input type="checkbox"/>

Remote Host Configuration		
Item	Value setting	Description
Host Name	String format: any text	Enter the host name for the designated remote host. <b>Value Range:</b> -1 ~ 64 characters.
Host IP	A Required setting	Specify the <b>IP Address</b> of remote host. It will be used as destination IP for sending NMEA packets.
Protocol Type	TCP is selected by default	Specify the <b>Protocol (TCP or UDP)</b> to use for sending NMEA packets.
Port Number	A Required setting	Specify a <b>Port Number</b> as destination port for sending NMEA packets. <b>Value Range:</b> 1 ~ 65535.
Interval(s)	A Required setting	Specify the time <b>interval</b> (seconds) between two NMEA packets. <b>Value Range:</b> 1 ~255 seconds.
MAC Address Message	The box is unchecked by default	Check <b>Enable</b> box to send the device MAC address with the NMEA packets, and then your backend server can recognize this GPS data is sent from this device.
Prefix Message	String format: any text	Specify optional prefix string with specific information if your backend server can recognize. For example, you can input the IMEI code of this device here, and then your backend server can recognize this GPS data is sent from this device. You can also leave this field blank.
Suffix Message	String format: any text	Specify optional suffix string with specific information if your backend server can recognize.
Enable	The box is unchecked by default	Check <b>Enable</b> box to activate this remote host rule.
Save	NA	Click the <b>Save</b> button to save the configuration

## Chapter 9 User Application

In the IIoT era, with the advent of cost effective 4G / LPWA connectivity choices, there are more and more field devices (nodes) connected to the internet and cloud storage and computing service for remote data acquisition and analysis. The system integrators and solution providers prepare all kinds of application platforms and networking devices to construct a total solution for each project.



## **AiR PACE-Industrial Smart IoT Edge Computing Gateway Features:**

- Integrate edge computing capability and device connectivity with AiR PACE .
- SI / Solution Provider can develop own edge computing applications with the edge gateway.
- Raw data processing / analysis - take timely actions if rule matched, and save communication costs
- Upload processed results and data to cloud directly for further processing and data storage.

This edge RTU / gateway product supports some public programming tools, like Python, Node-RED, for you to developing your own applications and executing locally, and Edge Computing enablement such as Azure runtime, AWS Greengrass, for connecting to public cloud service and seamless cooperation between cloud computing and edge computing.

## 9.1 Edge Computing

To ease the development task and speed up the deployment of your IIoT data acquisition and analysis requirement in the field, this IoT edge gateway integrates some popular and open programming tools. You can design your application directly with the edge gateway. Once development and verification tasks are completed, you can easily duplicate the application code to different sites.

In the following sections, you can learn how to use the integrated programming tools and select the ones you prefer.

To optimize the memory usage for the edge gateway, just enable the one you would like to use.

### 9.1.1 Python

Python Module

Widget

Python Module

Import

Delete

↑

×

ID	Module Name	Description	Action
----	-------------	-------------	--------

Python IDE

Start IDE

↑

×

Item	Setting
Python IDE Enable	<input checked="" type="checkbox"/> Enable
Login Password	<input type="checkbox"/> Enable <input type="text"/>
Login Port	<input type="text" value="8888"/> (1025-65535)

IDE Application List

↑

×

APP Name	Status	Auto_Start	Action
Untitled.ipynb	Ready	<input type="checkbox"/>	<div>Start</div> <div>Stop</div> <div>Delete</div> <div>Auto</div>

Imported Application List

Import

↑

×

ID	APP Name	Description	Status	Auto_Start	Action
----	----------	-------------	--------	------------	--------

Python is an interpreted, high-level, general-purpose programming language. Created by Guido van Rossum and first released in 1991. Python's design philosophy emphasizes code readability with its notable use of significant whitespace. Its language constructs and object-oriented approach aim to help programmers write clear, logical code for small and large-scale projects.<sup>12</sup>

<sup>12</sup> [https://en.wikipedia.org/wiki/Python\\_\(programming\\_language\)](https://en.wikipedia.org/wiki/Python_(programming_language))

# AIR PACE

Python has become famous because of its apparent and easily understandable syntax, portability, and ease of learning. It is a programming language that includes features of C and Java. It provides the style of writing an elegant code like C, and for object-oriented programming, it offers classes and objects like Java.<sup>13</sup>

Python is a great language for beginner-level programmers and supports the development of a wide range of applications, from simple text processing to WWW internet, social apps, games, and IIoT

The edge gateway supports System Integrator and Solution Provider to develop and integrate his Python programs with this gateway. Besides, a web-based Python IDE, called Jupyter Notebook, is also embedded to simplify the Python development process.

---

<sup>13</sup> <https://www.w3schools.in/python-tutorial/overview/>

## Python Setting

The Python function module is pre-installed in the gateway. You can enable it and deploy the required Python codes for your IoT application.

Go to **Service > Python > Python Module** Tab.

### Import / Edit Python Modules

The edge gateway supports Python 2.7. You can use all the standard libraries that comes with Python. If you are new to Python programming language, you can refer to the following on-line document URL for the detail list and description about the supported libraries.

The Python Standard Library: <https://docs.python.org/2.7/library/index.html>

Python's standard library is very extensive, offering a wide range of facilities as indicated by the long table of contents listed below. The library contains built-in modules (written in C) that provide access to system functionality such as file I/O that would otherwise be inaccessible to Python programmers, as well as modules written in Python that provide standardized solutions for many problems that occur in everyday programming. Some of these modules are explicitly designed to encourage and enhance the portability of Python programs by abstracting away platform-specifics into platform-neutral APIs.

In addition to the standard library, there is a growing collection of several thousand components (from individual programs and modules to packages and entire application development frameworks), available from the Python Package Index ( <https://pypi.org> ). You can get the interested Python modules (\*.tar.gz) and import to the edge gateway to assist and speedup your development.

Python Module <span>Import</span> <span>Delete</span>			
ID	Module Name	Description	Action

The edge gateway supports up to a maximum of 128 imported modules. When **Import** or **Edit** button is applied, the **Import Module Configuration** screen will appear.

Import Module <span>Apply</span>	
Item	Setting
Description	<input type="text"/>
Import Module (.tar / .tar.gz)	<input type="text"/> <span>瀏覽...</span>

Import Module Configuration		
Item	Value setting	Description

# AIR PACE

Description	A Must filled setting.	Enter a brief description for the module.
Import Module (.tar / .tar.gz)	A Must filled setting	Select a Python module file from the file browser, and click the <b>Apply</b> button to save the configuration, and import the specified module file to the gateway.

When you import a Python module, you can find it from the Python Module List.

To use the imported python module, you have to add the path of `/usr/lib/python_modules/[module_name]` in your Python code to append the imported module to the Python system path and then use the APIs for your code development.

```
import sys
sys.path.append('/usr/lib/python_modules/ModuleName-1')
...
sys.path.append('/usr/lib/python_modules/ModuleName-n')
```

The following shapshot illustrates an example for importing *EasyModbus-1.2.6*, *pyserial-3.4*, and *paho-mqtt-1.5.0* modules.

Python Module <span>Import</span> <span>Delete</span> <span>⬆</span> <span>✖</span>			
ID	Module Name	Description	Action
1	EasyModbus-1.2.6	Standard Lib for Modbus RTU Modbus TCP	<span>Edit</span> <input type="checkbox"/> Select
2	pyserial-3.4	Python Serial Port Extension	<span>Edit</span> <input type="checkbox"/> Select
3	paho-mqtt-1.5.0	MQTT Client	<span>Edit</span> <input type="checkbox"/> Select

In this example, you have to add the following lines in the beginning of your Python code:

```
In [1]: import sys
        sys.path.append('/usr/lib/python_modules/EasyModbus-1.2.6')
        sys.path.append('/usr/lib/python_modules/pyserial-3.4')
        sys.path.append('/usr/lib/python_modules/paho-mqtt-1.5.0')
```

Then, you can implement the required functions for using Modbus RTU, Modbus TCP, and also MQTT clients with these imported Python modules.

## Enable Python IDE

Python IDE
Start IDE

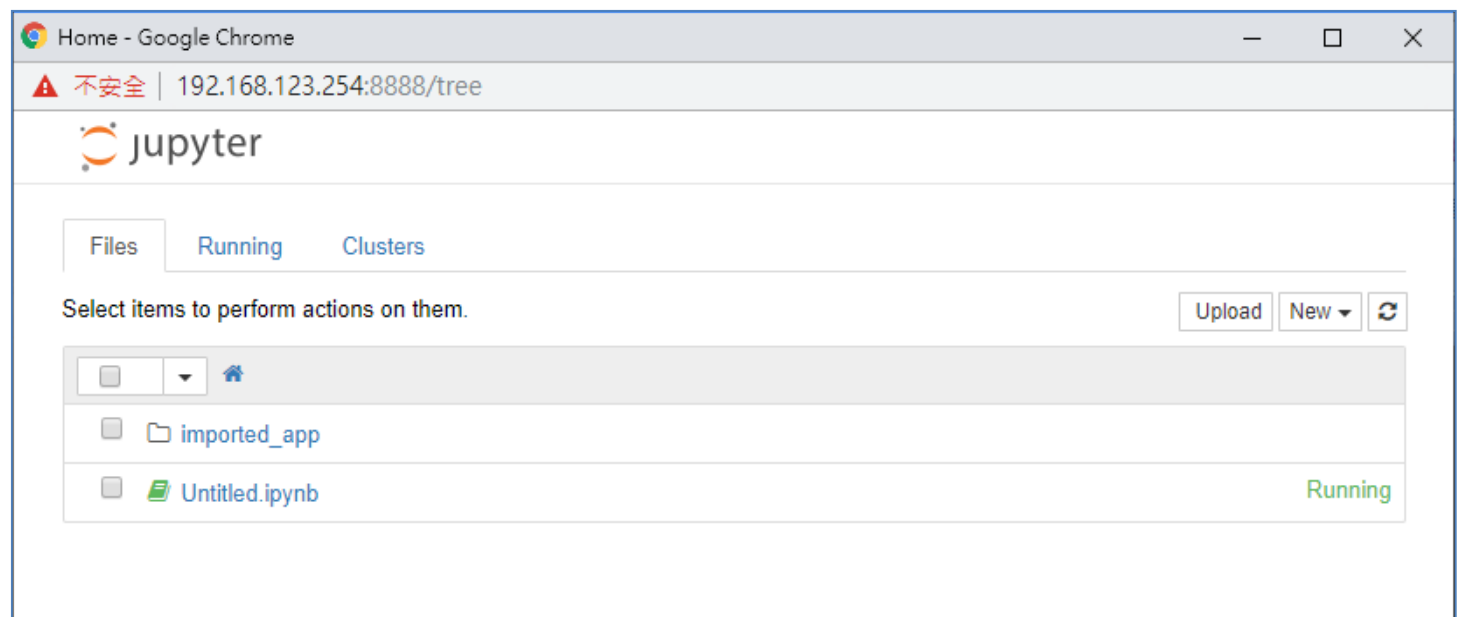
Item	Setting
Python IDE Enable	<input type="checkbox"/> Enable
Login Password	<input type="checkbox"/> Enable <input type="text"/>
Login Port	<input type="text" value="8888"/> (1025-65535)

Python IDE Configuration

Item	Value setting	Description
Python IDE Enable	The box is unchecked by default	Check the <b>Enable</b> box to activate the Python IDE and Python function.
Login Password	The box is unchecked by default	Check the <b>Enable</b> box to activate the Python IDE login check, and enter the required login password for checking.
Login Port	8888 is set by default	Specify the port number for accessing to the Python IDE. 8888 is set by default. <b>Value Range:</b> 1025 ~ 65535 seconds.
Start IDE		Click the <b>Start IDE</b> button to activate the Node-RED web-based IDE. The button will be grey out when Node-RED function is disabled. So, if you just enabled the Node-RED function, you have to save the configuration first to get it be activated.
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.

## Start Python IDE

When you click the Start IDE button, a browser window accessing to `https://LAN IP address : login port` will be displayed. As shown below, the Python IDE with <https://192.168.123.254:8888> is displayed.





# AIR PACE

If login password check is activated, you will be asked to provide the login password first to get access to the Python IDE.

Password or token:

Log in

Token authentication is enabled. You need to open the notebook server with its first-time login token in the URL, or enable a password in order to gain access.  
The command:

```
jupyter notebook list
```

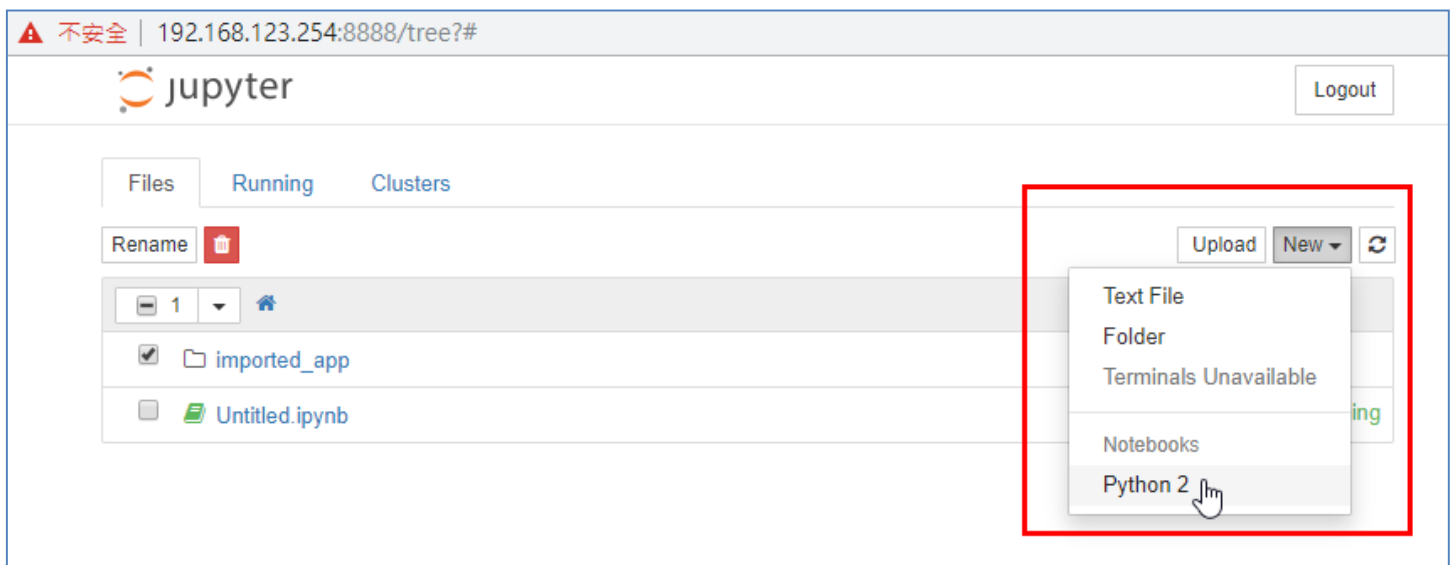
will show you the URLs of running servers with their tokens, which you can copy and paste into your browser. For example:

```
Currently running servers:  
http://localhost:8888/?token=c8de56fa... :: /Users/you/notebook  
s
```

Or you can paste just the token value into the password field on this page.  
Cookies are required for authenticated access to notebooks.

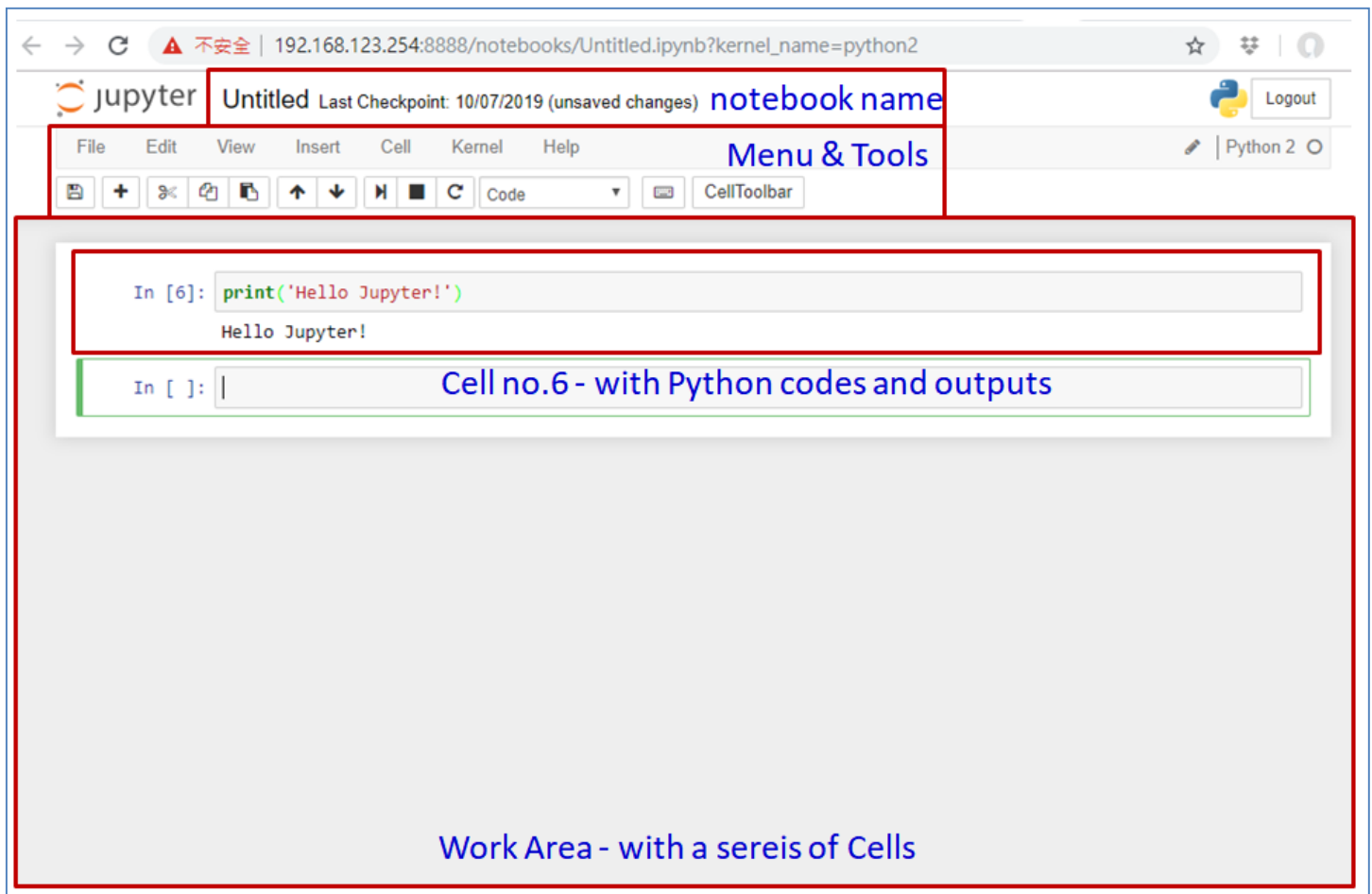
The bundled Python IDE is the Jupyter Notebook. The Jupyter Notebook is an open source web application that you can use to create and share documents that contain live code, equations, visualizations, and text. The Jupyter Notebook support lots of kernels for different programming languages. In this bundle, only Python 2 (2.7) is installed.

To start with the Python programming, you have to create a notebook (Python project) and then write the Python program in the IDE. Click the default **Untitled.ipynb** notebook to edit it, or click **New** to create a new Python notebook file.



# AIR PACE

Hereunder is the Jupyter Notebook IDE. You can see the areas for notebook name, Menu & Tools, Work Area, and also a specific cell with its Python code and execution output beneath the cell.



You can refer to the Jupyter Notebook introduction URL below

<https://realpython.com/jupyter-notebook-introduction/>

You will learn how to create a notebook, how to write python code, and how to run cells (piece of codes).

## IDE Application List

With the Python IDE, Jupyter Notebook, you can create multiple applications (notebook projects) and maintain the code and operation manually via the IDE provided functionality.

All the applications in the IDE will also be displayed in the following IDE Application List. It provides a shortcut for you to control the execution individually.

IDE Application List			
APP Name	Status	Auto_Start	Action
Untitled.ipynb	Ready	<input type="checkbox"/>	<div>Start</div> <div>Stop</div> <div>Delete</div> <div>Auto</div>

IDE Application List Configuration		
Item	Value setting	Description
APP Name	N/A	Indicate the application (notebook project) name, e.g., Untitled.ipynb.
Status	N/A	Indicate the execution status for each Python application in IDE. It can be <b>Ready</b> , <b>Running</b> , or <b>Finish</b> . <b>Ready</b> : Python application is created, and ready to run. <b>Running</b> : Python application is started and running. <b>Finish</b> : Python application has started and finished the execution.
Auto_Start	N/A	Indicate the setting of Auto Start. Checked means the application will be auto started once the gateway is boot up.
Action	N/A	Four command buttons to operate the application. <b>Start</b> : Start to execute the application. <b>Stop</b> : Stop the execution of application. <b>Delete</b> : Delete the corresponding application from the IDE. <b>Auto / Manual</b> : Click <b>Auto</b> to activate the Python application automatically. Once the gateway is boot up with Python enabled, the applications with Auto_Start checked will be started automatically. Click <b>Manual</b> to deactivate the Auto Start function, and the application can be executed by clicking the <b>Start</b> button manually.

The Python IDE is suitable for the applications that are still under developing or validation. You can freely modify the code and execute to check if the result is OK or not.

Deploy Python Application

Once you finished and validated a Python application design with the provided IDE, you can export the the Python code to a .py file and duplicate it on the other gateways for deploying the same application in different sites.

Imported Application List <span>Import</span>					
ID	APP Name	Description	Status	Auto_Start	Action

When **Import** or **Edit** button is applied, the **Import Application Configuration** screen will appear.

Imported Application <span>Save</span>	
Item	Setting
Description	<input type="text"/>
Auto_Start	<input type="checkbox"/> Enable
Import Application (.py)	<input type="text"/> <span>瀏覽...</span>

Import Application Configuration		
Item	Value setting	Description
Description	A required setting.	Enter a brief description for the Python Application.
Auto_Start	The box is unchecked by default	Check the <b>Enable</b> box to activate the imported Python application automatically. Once the gateway is boot up with Python enabled, the Applications with Auto_Start options will be started automatically.
Import Application (.py)	A required setting	Select a Python module file from the file browser, and click the <b>Apply</b> button to save the configuration, and import the specified module file to the gateway.

9.1.2 Node-RED

Node-RED Configuration

Widget

Node-RED Module

Import

Delete

ID	Module Name	Description	Action
----	-------------	-------------	--------

User Privacy List

Add

Delete

ID	User Name	Password	Permissions	Enable	Action
----	-----------	----------	-------------	--------	--------

Node-RED

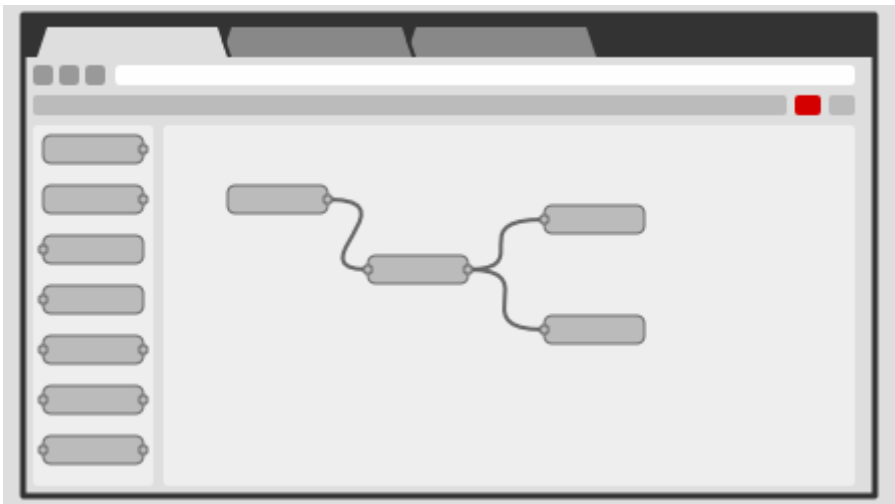
Start IDE

Item	Setting
Node-RED Enable	<input checked="" type="checkbox"/> Enable <input checked="" type="radio"/> http <input type="radio"/> https
Login Port	<input type="text" value="1880"/> (1025-65535)

Save

Undo

Node-RED is a programming tool for wiring together hardware devices, API and online services in new and interesting ways. It provides a browser-based editor that makes it easy to wire together flows using the wide range of nodes in the palette. Flows can be then deployed t othe runtime in a single click. Additionally, JavaScript functions can be created within the editor. A built-in library allows you to save useful functions. templates, or flows for re-use.<sup>14</sup>



The Node-RED function module is built on Node.js, taking full advantage of its event-driven, non-blocking model. This makes it ideal to run at the edge of the network on this IIoT edge gateway product.

The flows created in Node-RED are stored using JSON format which can be easily imported or exported for

<sup>14</sup> <https://nodered.org/>

# AIR PACE

sharing with others or quickly deploy the same flow on a group of gateways.

Node-RED provide an elegant solution to merge different IoT devices and services, and stay within a local area network. It is based on a graphical interface and rely on three main concepts.<sup>15</sup>

**Flow:** A project is called a flow, and consists of data and functions inked together.

**Message:** The messages carry data from one node to another.

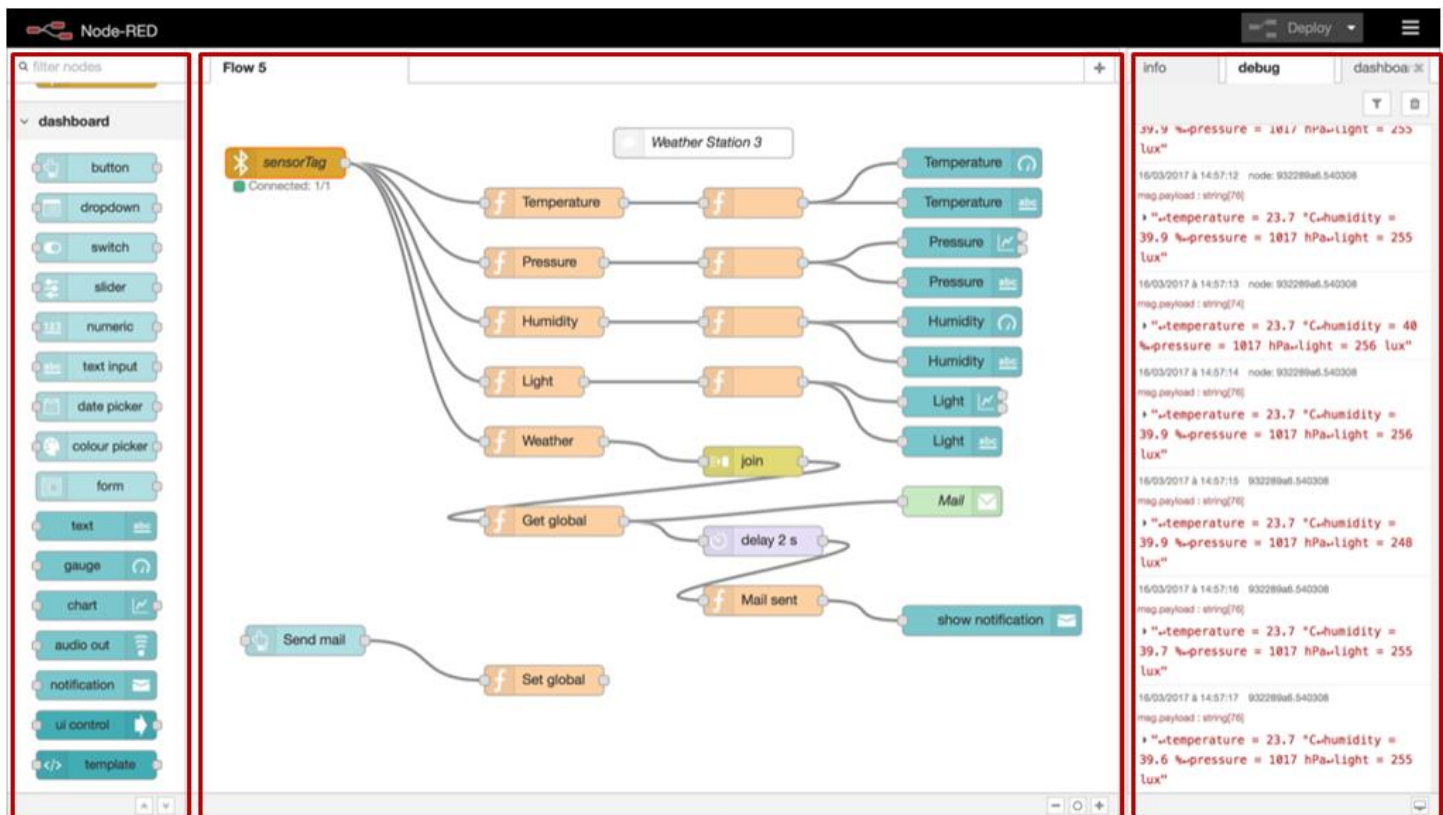
**Node:** The nodes are functions that generate, transform, or use messages.

The Node-RED GUI consists of three parts, from left to right:

**Node Palette** – the left pane lists all the available nodes, grouped by categories.

**Working Area** – the center pane corresponds to the working area, where the flow is going to be designed.

**Information Area** – the right pane provides useful tools as flow information, node information, debug messages, and dashboard.



Node Palette

Working Area

Information Area

<sup>15</sup> <https://embeddedcomputing.weebly.com/iot-with-node-red.html>

If you are new to the Node-RED programming tool, you can easily get many useful resources from the Internet.

You can get the user guide, tutorials from <https://www.nodered.org/docs>

Also, you can also get Chinese version tutorials from 3<sup>rd</sup> party at the following URL:

<https://tutorials.webduino.io/zh-tw/docs/socket/useful/node-red.html>.

Node-RED Setting

The Node-RED function module is pre-installed in the gateway. You can enable it and deploy the required flow for your IoT application.

Go to **Service > Node-RED > Node-RED Configuration** Tab.

Create/Edit User Privacy List

User Privacy List Add Delete					
ID	User Name	Password	Permissions	Enable	Action

When **Add** or **Edit** button is applied, the **User Privacy Rule Configuration** screen will appear. You can create or edit required user accounts and permission for each account to reach the Node-RED GUI. Up to 3 user accounts are supported.

User Privacy Rule Configuration Save	
Item	Setting
User Name	<input type="text"/> (Minimum 4 characters)
Password	<input type="password"/>
Permissions	Full access
Enable	<input type="checkbox"/>

User Privacy List Configuration		
Item	Value setting	Description
User Name	A required setting.	Specify a name as the identifier of the Node-RED user. <b>Value Range:</b> 4 ~ 32 characters.
Password	A required setting.	Specify a password for the user account. <b>Value Range:</b> 1 ~ 32 characters.
Permissions	1. A required setting. 2. <b>Full access</b> is selected by default.	Specify the access permission for the user account. <b>Full access:</b> with both Read and Write permission. <b>Read-only access:</b> Read permission only. There is no write permission for the user account.
Enable	The box is unchecked by default	Check the <b>Enable</b> box to activate the user account.
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.



## Enable Node-RED

Node-RED
Start IDE

Item	Setting
▶ Node-RED Enable	<input checked="" type="checkbox"/> Enable <input checked="" type="radio"/> http <input type="radio"/> https
▶ Login Port	<input type="text" value="1880"/> (1025-65535)

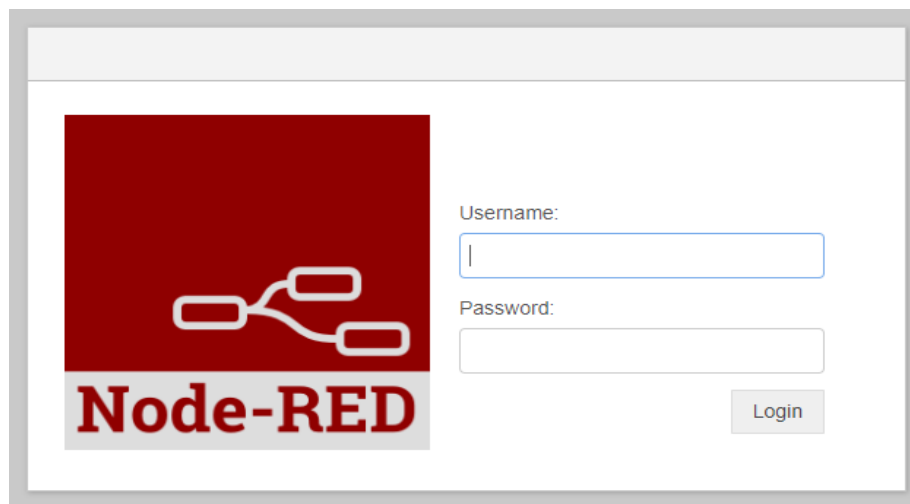
Node-RED Configuration

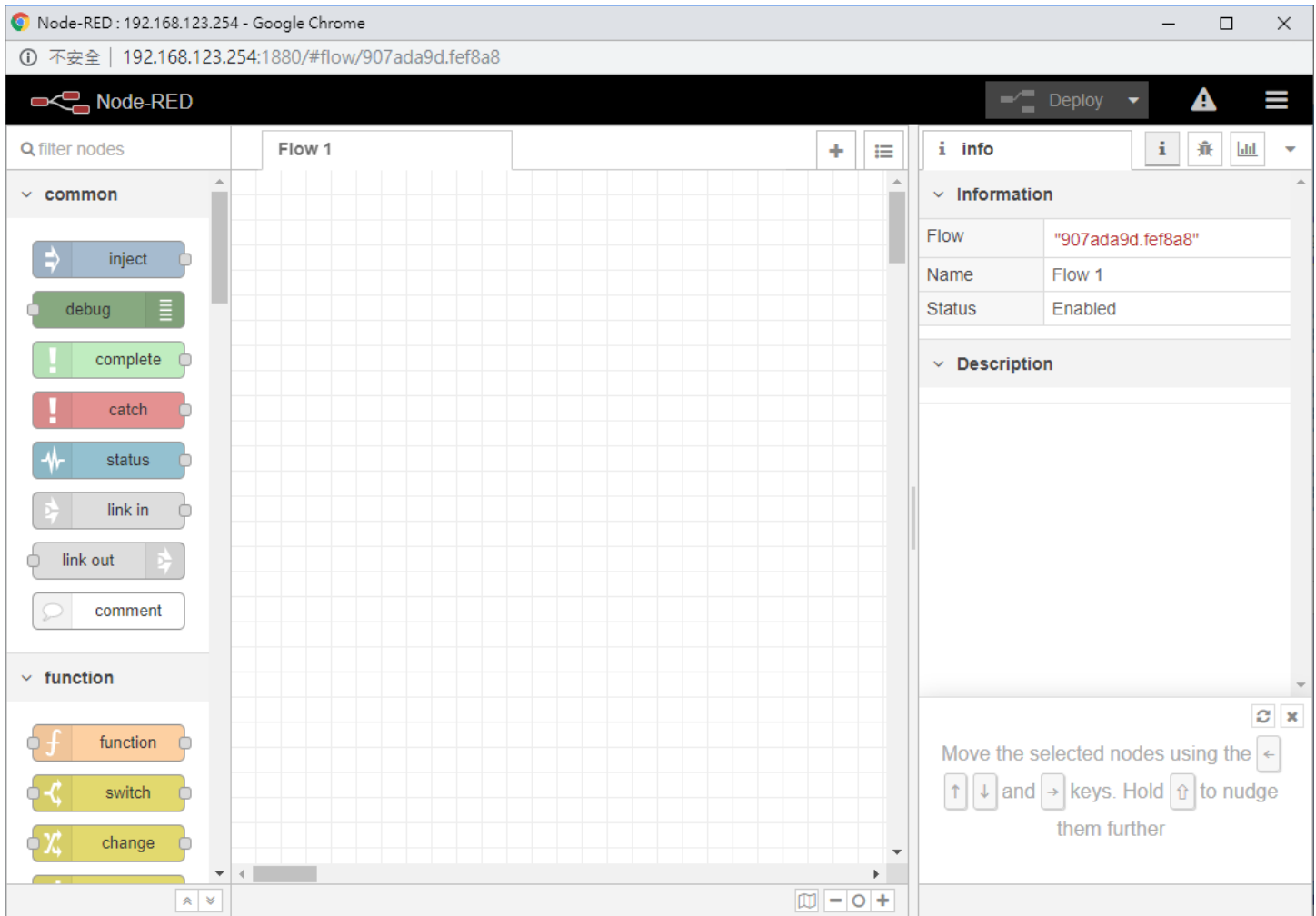
Item	Value setting	Description
<b>Node-RED Enable</b>	The box is unchecked by default	Check the <b>Enable</b> box to activate the Node-RED function. Choose either <b>http</b> or <b>https</b> protocol for accessing the Node-RED IDE.  <b>Note:</b> If you checked the Enable box, the gateway will auto activate the deployed flow(s) after the gateway is boot up. No manually deployment is required.
<b>Login Port</b>	<b>1880</b> is set by default	Specify the port number for accessing to the Node-RED IDE. 1880 is set by default. <b>Value Range:</b> 1025 ~ 65535 seconds.
<b>Start IDE</b>		Click the <b>Start IDE</b> button to activate the Node-RED web-based IDE. The button will be grey out when Node-RED function is disabled. So, if you just enabled the Node-RED function, you have to save the configuration first to get it be activated.
<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.

## Start Node-RED IDE

When you click the Start IDE button, a browser window accessing to *http(s)://LAN IP address : login port* will be displayed. As shown below, the Node-RED GUI with <http://192.168.123.254:1880> is displayed.

If there is any pre-activated user account, you will be asked to provide the user name and password first to get access to the Node-RED GUI.

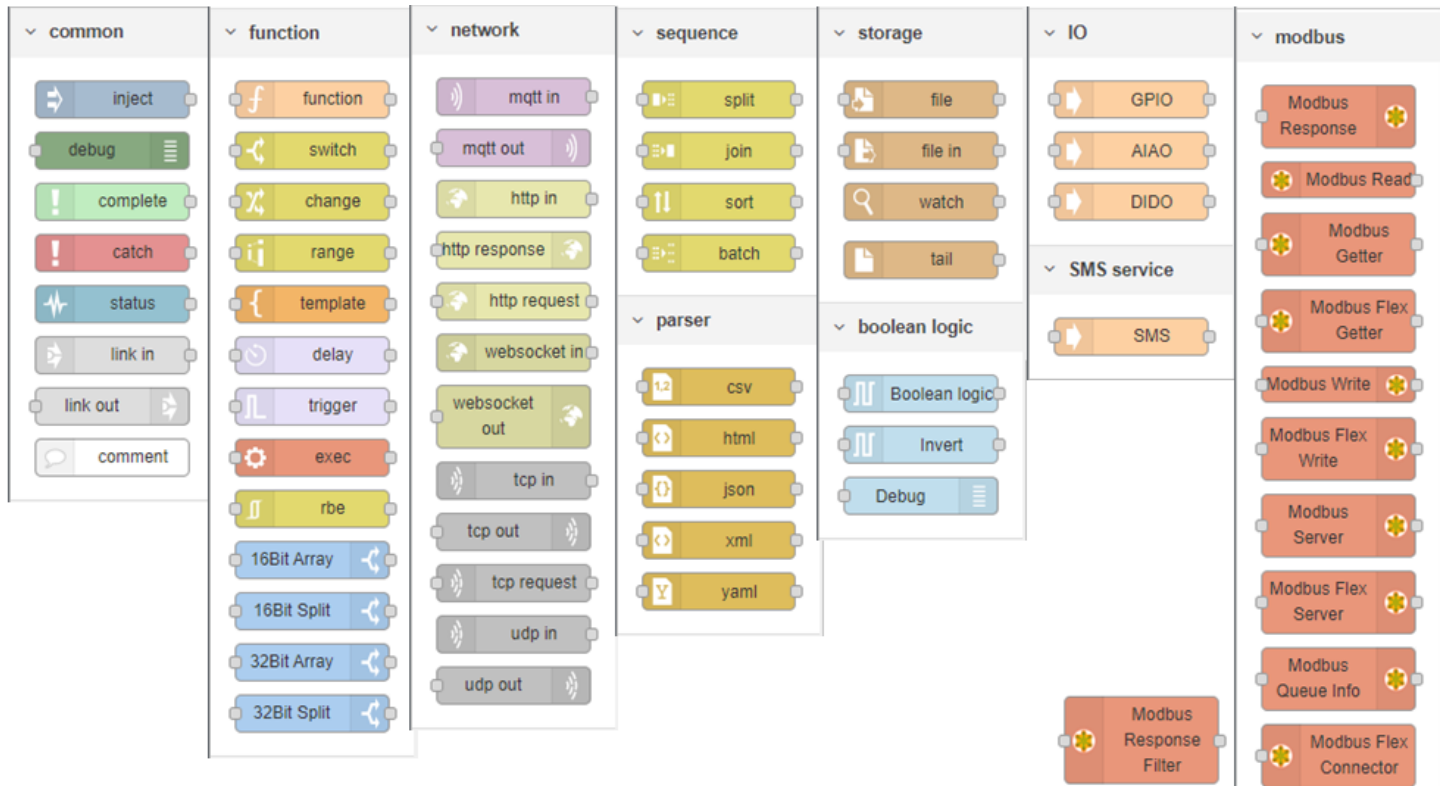




The available nodes in the node palette are categorized into several groups. They are **common**, **function**, **network**, **sequence**, **parser**, **storage**, **boolean logic**, **IO**, **SMS service**, and **modbus**.

Most nodes are generic and accompanied with the standard Node-RED function module, and some nodes are hardware-dependent and provided by the gateway manufacture, like IO, Modbus, and SMS Service.

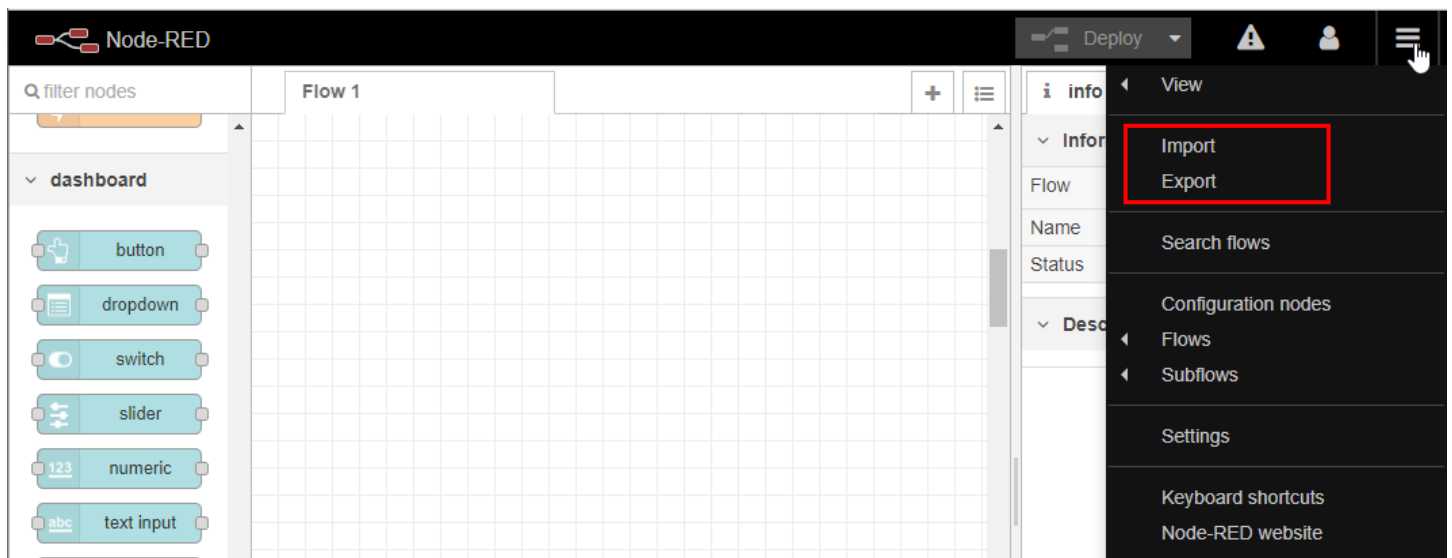
# AIR PACE



## Deploy Node-RED Flow

While you are designing a flow, you can click the **Deploy** button on the Upper-Right corner of Node-RED GUI to activate the flow. And check the outputs from the debug area or dashboard window.

Once you finished and verified a flow design, you can export the flow to a .json file and import it to other gateway for deploying the same application in different sites. You just have to click on the **Menu** button and then select the function item **Import** or **Export**.



Import / Edit Node-RED Modules

By default, there are many available nodes, listed in the node palette, for you to design your flow once you activate the Node-RED function.

Most of the case, if you can't find a certain suitable node for a specific requirement, you have to implement it by yourself with the generic *function* node and write a piece of JavaScript codes for it. However, you can also check with the gateway manufacture for the availability of any related open nodes.

Once you got the required Node-RED module (.tar file), you can import the external Node-RED Module (Node) that is provided by the gateway manufacture. It supports up to a maximum of 32 imported modules.

Node-RED Module Import Delete			
ID	Module Name	Description	Action

When **Import** or **Edit** button is applied, the **Import Module Configuration** screen will appear.

Import Module Apply	
Item	Setting
Module Name	<input type="text"/>
Description	<input type="text"/>
Import Module (.tar)	<input type="text"/> 浏览...

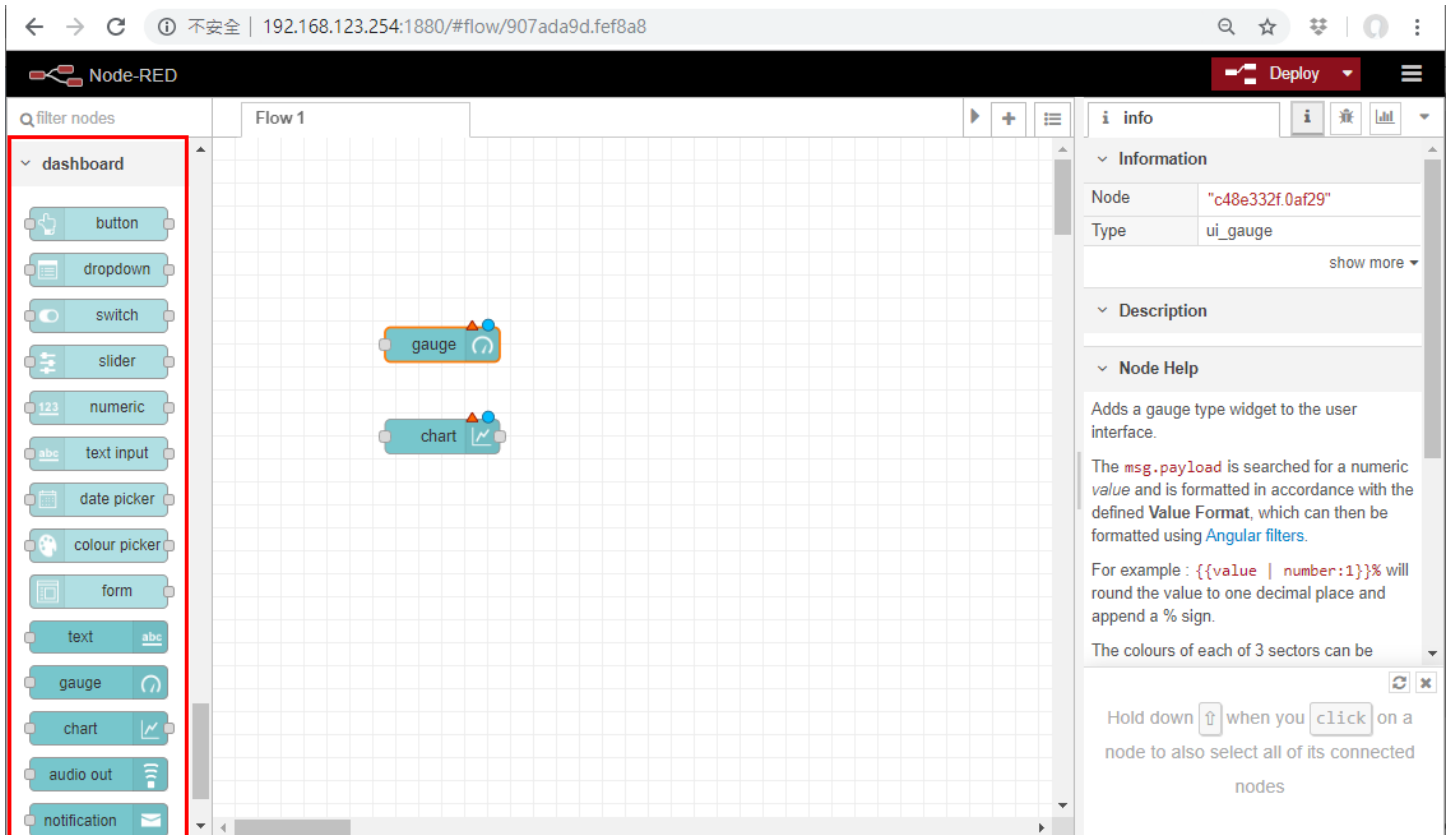
Import Module Configuration		
Item	Value setting	Description
Module Name	A required setting.	Specify the module name for the module to be imported.
Description	A required setting.	Enter a brief description for the module.
Import Module (.tar)	A required setting	Select a Node-RED module file from the file browser, and click the <b>Apply</b> button to save the configuration, and import the specified module file to the gateway.
Undo	NA	Click the <b>Undo</b> button to restore what you just configured back to the previous setting.

When you imported a Node-RED module, you can find it from the Node-RED Module List, and the Node Palette. Then, you can use the imported nodes for flow development.

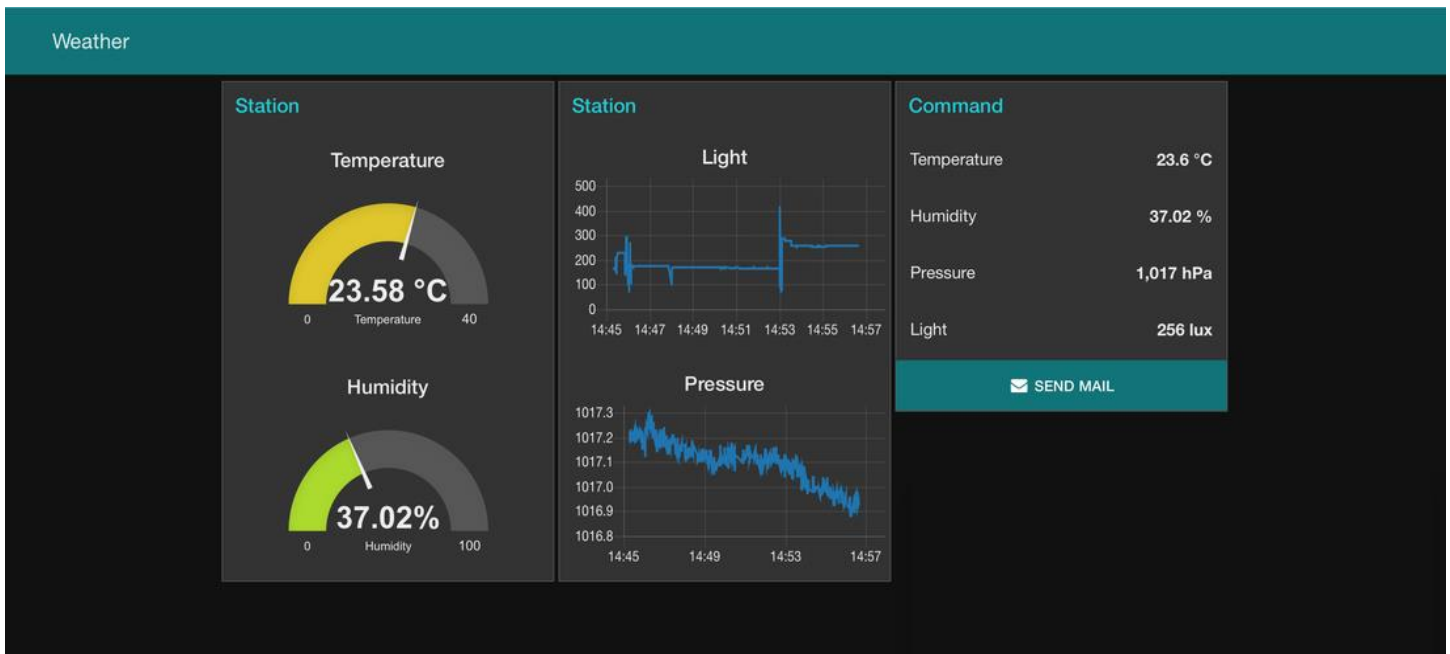
The following snapshots illustrate an example for importing *node-red-dashboard* module.

Node-RED Module Import Delete			
ID	Module Name	Description	Action
1	node-red-dashboard	Node-RED Dashboard	Edit <input type="checkbox"/> Select

# AIR PACE



With the dashboard nodes, you can easily design your own local SCADA dashboard for visually check the status of field devices. If required, the dashboard can be viewed in a browser with the URL `http://local ip:port/ui`.



## Appendix A GPL WRITTEN OFFER

This product incorporates open source software components covered by the terms of third party copyright notices and license agreements contained below.

GPSTBabel

Version 1.4.4

Copyright (C) 2002-2005 Robert Lipe<[robertlipe@usa.net](mailto:robertlipe@usa.net)>

GPL License: <https://www.gpsbabel.org/>

Curl

Version 7.19.6

Copyright (c) 1996-2009, Daniel Stenberg, <[daniel@haxx.se](mailto:daniel@haxx.se)>.

MIT/X derivate License: <https://curl.haxx.se/>

OpenSSL

Version 1.0.2m

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

GPL License: <https://www.openssl.org/>

brctl - ethernet bridge administration

Stephen Hemminger <[shemminger@osdl.org](mailto:shemminger@osdl.org)>

Lennert Buytenhek <[buytenh@gnu.org](mailto:buytenh@gnu.org)>

version 1.1

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

tc - show / manipulate traffic control settings

Stephen Hemminger<[shemminger@osdl.org](mailto:shemminger@osdl.org)>

Alexey Kuznetsov<[kuznet@ms2.inr.ac.ru](mailto:kuznet@ms2.inr.ac.ru)>

version iproute2-ss050330

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

dhcp-fwd — starts the DHCP forwarding agent

Enrico Scholz <[enrico.scholz@informatik.tu-chemnitz.de](mailto:enrico.scholz@informatik.tu-chemnitz.de)>

version 0.7

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

lftp - Sophisticated file transfer program

Alexander V. Lukyanov <[lav@yars.free.net](mailto:lav@yars.free.net)>

version:4.5.x

Copyright (c) 1996-2014 by Alexander V. Lukyanov ([lav@yars.free.net](mailto:lav@yars.free.net))

dnsmasq - A lightweight DHCP and caching DNS server.

Simon Kelley <[simon@thekelleys.org.uk](mailto:simon@thekelleys.org.uk)>

# AIR PACE

version:2.72

dnsmasq is Copyright (c) 2000-2014 Simon Kelley

socat - Multipurpose relay

Version: 2.0.0-b8

GPLv2

<http://www.dest-unreach.org/socat/>

LibModbus

Version: 3.0.3

LGPL v2

<http://libmodbus.org/news/>

LibIEC60870

GPLv2

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

<https://sourceforge.net/projects/mrts/>

Openswan

Version: v2.6.38 GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

<https://www.openswan.org/>

Opennhp

Version: v0.14.1

OpenNHRP is an NHRP implementation for Linux. It has most of the RFC2332 and Cisco IOS extensions.

Project homepage: <http://sourceforge.net/projects/opennhp>

Git repository: <git://opennhp.git.sourceforge.net/gitroot/opennhp>

LICENSE

OpenNHRP is licensed under the MIT License. See MIT-LICENSE.txt for additional details.

OpenNHRP embeds libev. libev is dual licensed with 2-clause BSD and GPLv2+ licenses. See libev/LICENSE for additional details.

OpenNHRP links to c-ares. c-ares is licensed under the MIT License.

<https://sourceforge.net/projects/opennhp/>

IPSec-tools

Version: v0.8

No GPL be written

<http://ipsec-tools.sourceforge.net/>

# AIR PACE

## PPTP

Version: pptp-1.7.1

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA

Everyone is permitted to copy and distribute verbatim copies  
of this license document, but changing it is not allowed.

<http://pptpclient.sourceforge.net/>

## PPTPServ

Version: 1.3.4

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA

Everyone is permitted to copy and distribute verbatim copies

of this license document, but changing it is not allowed. <http://poptop.sourceforge.net/>

## L2TP

Version: 0.4

Copying All software included in this package is Copyright 2002 Roaring  
Penguin Software Inc. You may distribute it under the terms of the  
GNU General Public License (the "GPL"), Version 2, or (at your option)  
any later version.

<http://www.roaringpenguin.com/>

## L2TPServ

Version: v 1.3.1 GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies  
of this license document, but changing it is not allowed.

<http://www.xelerance.com/software/xl2tpd/>

Mpstat: from sysstat, system performance tools for Linux

Version: 10.1.6

Copyright: (C) 1999-2013 by Sebastien Godard (sysstat <at> orange.fr)

SSHD: dropbear, a SSH2 server

Version: 0.53.1

Copyright: (c) 2002-2008 Matt Johnston

Libncurses: The ncurses (new curses) library is a free software emulation of curses in System V Release 4.0 (SVr4), and more.

Version: 5.9

Copyright: (c) 1998,2000,2004,2005,2006,2008,2011,2015 Free Software Foundation, Inc., 51 Franklin Street, Boston, MA 02110-1301, USA



# AIR PACE

MiniUPnP: The miniUPnP daemon is an UPnP IGD (internet gateway device) which provide NAT traversal services to any UPnP enabled client on the network.

Version: 1.7

Copyright: (c) 2006-2011, Thomas BERNARD

CoovaChilli is an open-source software access controller for captive portal (UAM) and 802.1X access provisioning.

Version: 1.3.0

Copyright: (C) 2007-2012 David Bird (Coova Technologies) <support@coova.com>

Krb5: Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.

Version: 1.11.3

Copyright: (C) 1985-2013 by the Massachusetts Institute of Technology and its contributors

OpenLDAP: a suite of the Lightweight Directory Access Protocol (v3) servers, clients, utilities, and development tools.

Version: 2.4

Copyright: 1998-2014 The OpenLDAP Foundation

Samba3311: the free SMB and CIFS client and server for UNIX and other operating systems

Version: 3.3.11

Copyright: (C) 2007 Free Software Foundation, Inc. <<http://fsf.org/>>

NTPClient: an NTP (RFC-1305, RFC-4330) client for unix-alike computers

Version: 2007\_365

Copyright: 1997, 1999, 2000, 2003, 2006, 2007 Larry Doolittle

exFAT: FUSE-based exFAT implementation

Version: 0.9.8

Copyright: (C) 2010-2012 Andrew Nayenko

NTFS\_3G: The NTFS-3G driver is an open source, freely available read/write NTFS driver for Linux, FreeBSD, Mac OS X, NetBSD, Solaris and Haiku.

Version: 2009.4.4

Copyright: (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

mysql-5\_1\_72: a release of MySQL, a dual-license SQL database server

Version: 5.1.72

Copyright: (c) 2000, 2013, Oracle and/or its affiliates

FreeRadius: a high performance and highly configurable RADIUS server

Version: 2.1.12

Copyright: (C) 1999-2011 The FreeRADIUS server project and contributors

# Air PACE

## Python version 2.7.12

This Python distribution contains no GNU General Public Licensed (GPLed) code so it may be used in proprietary projects just like prior Python distributions. There are interfaces to some GNU code but these are entirely optional

## OpenPAM Radula

This software was developed for the FreeBSD Project by ThinkSec AS and Network Associates Laboratories, the Security Research Division of Network Associates, Inc. under DARPA/SPAWAR contract N66001-01-C-8035 ("CBOSS"), as part of the DARPA CHATS research program.

## ISC DHCP Version 4.3.5

Copyright (c) 2004-2016 by Internet Systems Consortium, Inc. ("ISC")

## 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 2019. All Rights Reserved.

All trademarks and registered trademarks are the property of their respective owners

December 19, 2019