Version 1.01 | 06/28/2024



User Manual

5G IIoT Gateway

DOM-550-GSO

Information in this document is subject to change without notice. Reproduction of this document in any manner, without the written permission of the D-Link Corporation, is strictly forbidden.

Trademarks used in this text: D-Link and the D-Link logo are trademarks of the D-Link Corporation; Microsoft and Windows are registered trademarks of the Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either as the entities claiming the marks and the names or their products. D-Link Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

© 2024 D-Link Corporation. All rights reserved.

Chapter 1 Introduction 8
1.1 Introduction 8
1.2 Contents List 9
1.2.1 Package Contents 9
1.3 Hardware Configuration 10
1.4 Indicator LEDs 13
1.5 Installation & Maintenance Notice 14
1.5.1 SYSTEM REQUIREMENTS 14
1.5.2 WARNING 14
1.5.3 HOT SURFACE CAUTION 16
1.5.4 Product Information for CE RED Requirements 17
1.6 Hardware Installation 19
1.6.1 Insert the SIM Card & MicroSD Card 19
1.6.2 Mount the Unit 20
1.6.3 Install the External RF Cable and Antenna 20
1.6.4 Connecting I/O Devices 20
1.6.5 Connecting Serial Devices 23
1.6.6 Connecting Power 23
1.6.7 Connecting to the Network or a Host 24
1.6.8 Connecting the Web UI 24
1.6.9 Configure User Country area 26
Chapter 2 Basic Network 27
2.1 WAN & Uplink 27
2.1.1 Physical Interface 28
2.1.2 Connection Setup 31
2.1.3 Load Balance 52
2.2 LAN & VLAN 57
2.2.1 Ethernet LAN 57
2.2.2 VLAN 59
2.2.3 DHCP Server 72
2.3 Wi-Fi 80
2.3.1 Wi-Fi Configuration 81

2.3.2 Wireless Client List 94
2.3.3 Advanced Configuration 95
2.4 IPv6 98
2.4.1 IPv6 Configuration 98
2.5 Port Forwarding 105
2.5.1 Configuration 106
2.5.2 Virtual Server & Virtual Computer 107
2.5.3 DMZ & Pass Through 112
2.5.5 IP Translation 114
2.6 Routing 117
2.6.1 Static Routing 118
2.6.2 Dynamic Routing 121
2.6.3 Routing Information 128
2.7 DNS & DDNS 129
2.7.1 DNS & DDNS Configuration 129
2.8 QoS 133
2.8.1 QoS Configuration 133
2.9 Redundancy 142
2.9.1 VRRP 142
Chapter 3 Object Definition 145
3.1 Scheduling 145
3.1.1 Scheduling Configuration 145
3.2 Grouping 147
3.2.1 Host Grouping 147
3.3 External Server 149
3.4 Certificate 152
3.4.1 Configuration 152
3.4.2 My Certificate 155
3.4.3 Trusted Certificate 162
3.4.4 Issue Certificate 166
Chapter 4 Field Communication 167
4.1 Bus & Protocol 167

4.1.1 Port Configuration 167
4.1.2 Virtual COM 169
4.1.3 Modbus 180
4.2 Data Logging 190
4.2.1 Data Logging Configuration 192
4.2.2 Scheme Setup 194
4.2.3 Log File Management 196
4.3 Data Interchange 198
4.3.1 MQTT 198
Chapter 5 Security 208
5.1 VPN 208
5.1.1 IPSec 209
5.1.2 OpenVPN 217
5.1.3 L2TP 229
5.1.4 PPTP 237
5.1.5 GRE 244
5.1.6 WireGuard 246
5.2 Firewall 250
5.2.1 Packet Filter 250
5.2.2 URL Blocking 254
5.2.3 MAC Control 257
5.2.6 IPS 260
5.2.7 Options 264
Chapter 6 Administration 267
6.1 Configure & Manage 267
6.1.1 Command Script 268
6.1.2 D-ECS (D-LINK EDGE CLOUD SOLUTION) 272
6.1.3 SNMP 274
6.1.4 Telnet & SSH 283
6.2 System Operation 286
6.2.1 Password & MMI 286
6.2.2 System Information 290

6.2.3 System Time 291
6.2.4 System Log 296
6.2.5 Backup & Restore 301
6.2.6 Reboot & Reset 302
6.3 FTP 303
6.3.1 Server Configuration 304
6.3.2 User Account 306
6.4 Diagnostic 307
6.4.1 Diagnostic Tools 307
6.4.2 Packet Analyzer 308
Chapter 7 Service 310
7.1 Cellular Toolkit 310
7.1.1 Data Usage 310
7.1.2 SMS 314
7.1.3 SIM PIN 318
7.1.5 Network Scans 322
7.2 Event Handling 324
7.2.1 Configuration 324
7.2.2 Notifying Events 326
Chapter 8 Status 328
8.1 Dashboard 328
8.2 Basic Network 330
8.2.1 WAN & Uplink Status 330
8.2.2 LAN & VLAN Status 334
8.2.3 Wi-Fi Status 335
8.2.4 DDNS Status 338
8.3 Security 339
8.3.1 VPN Status 339
8.3.2 Firewall Status 343
8.4 Administration 347
8.4.1 Configure & Manage Status 347
8.4.2 Log Storage Status 348

8.5 Statistics & Report 349
8.5.1 Connection Session 349
8.5.2 Network Traffic 350
8.5.3 Login Statistics 351
8.5.4 Cellular Usage 352
8.5.5 Cellular Signal 353
Regulatory Information 354

Chapter 1 Introduction

1.1 Introduction

The 5G IIoT Gateway is designed specially for Industrial IoT applications with industrial-grade components to support stringent reliability, making it suitable for deployment in harsh environments.
The built-in world-class 5G module allows you to connect to the Internet by just inserting a SIM card from a local mobile carrier. The dual-SIM design allows for uninterrupted WAN connection with a backup connection to provide failover mechanism required for critical applications. The system also features VPN tunneling technology for convenient and secure remote site connection. The AI/DI/DO connectors can trigger real-time responses whenever events are detected by connected sensors.

This DOM-550-GSO series product is also equipped with essential security features such as firewall protection, NAT, and port forwarding.

The following highlights the capabilities of the DOM-550-GSO series product:

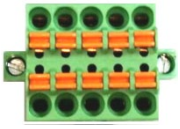
- A high speed 5G NR cellular module for high bandwidth and low latency connectivity.
- Dual-SIM connector for redundant WAN connections.
- Gigabit Ethernet ports to connect with other IP-based devices.
- RS-232/485 serial port to connect with legacy serial devices or Modbus devices.
- 802.11b/g/n/ac with concurrent dual-band Wi-Fi access point.
- Solid and yet flexible metal case design for versatile mount in industrial environments.

Before you install and use this product, please read this manual carefully to understand the functions and operating procedure of this product.

1.2 Contents List

1.2.1 Package Contents

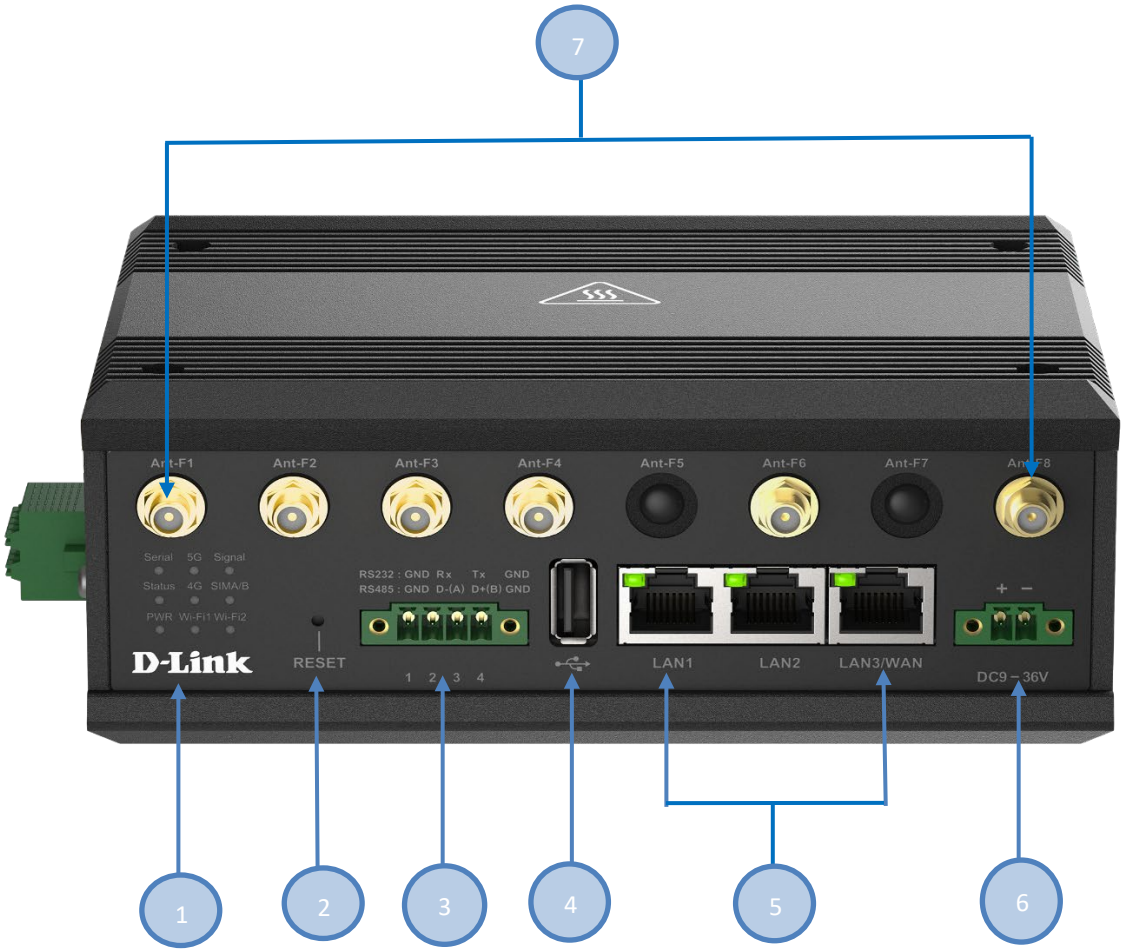
Standard Package

Items	Description	Contents	Quantity
1	**DOM-550-GSO 5G IIoT gateway (*1)**		1pcs
2	**10-pin Terminal Block**		1pcs
3	**4-pin Terminal Block**		1pcs
4	**2-pin Terminal Block**		1pcs
5	**RJ45 Cable**		1pcs
6	**DIN-Rail Bracket**		1pcs
7	**5G NR FR1 Antenna (optional)**		4pcs
8	**Wi-Fi 2.4G/5G Antenna (optional)**		2pcs
9	**DC 12 V Power adapter**		1pcs

1 The maximum power consumption of the DOM-550-GSO series is 30.0 Watt.

1.3 Hardware Configuration

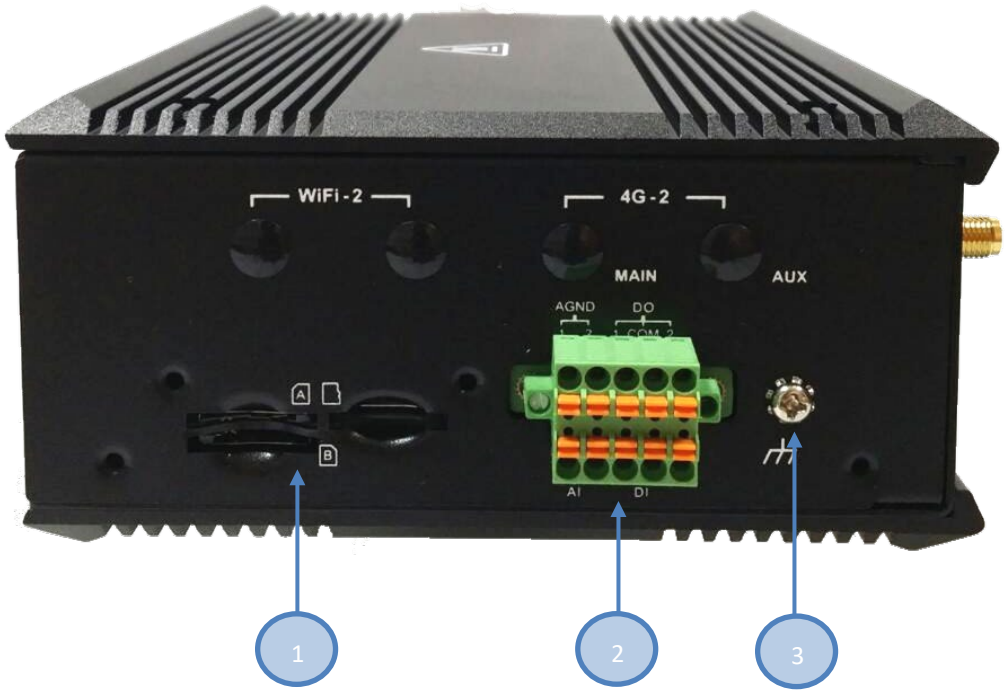
➢ Front View



No	Indicator, button, or connector	Description
1	**Indicator LEDs**	LEDs indicate the operating status of the device. Refer to **1.4 Indicator LEDs** for the LEDs and their meaning.
2	**Reset Button**	The RESET button provides you with a quick and easy way to restore the device to its factory default settings. Press the RESET button and hold it for 6 seconds (when the Status LED startgs blinking rapidly), and then release it. (During the reset, all LEDs will turn on and then off completely.) Note that all configuration changes will be erased.
3	**Serial Port**	A terminal block for serial devices connection. Refer to **1.6.5 Connecting Serial Devices** for pin assignments and voltage requirements.
4	**USB Port**	A USB 2.0 port to connect USB drives for data logging and packet analyzing. Refer to **4.2 Data Logging** and **6.4.2 Packet Analyzer** for more information about these functions.

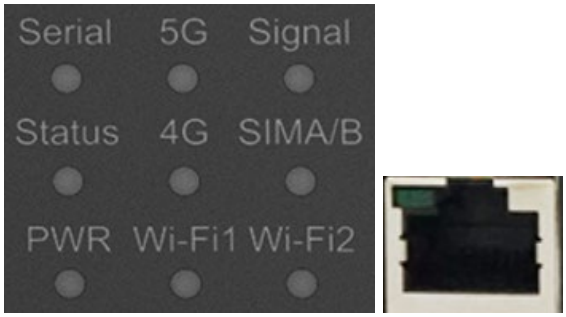
5	**Auto MDI/MDIX Port** **2x GbE LAN,** **1x GbE LAN/WAN**	Connects to Ethernet devices such as computers, switches, storage (NAS) devices at speeds of up to 1000 Mbps. The LAN3 port can also be used as a WAN port to connect to another network or Internet. Refer to **2.1 WAN & Uplink** for WAN interface configuration.
6	**DC Power** **Terminal Block**	A terminal block for connecting with power supply. Refer to **1.6.6 Connecting Power** for power input voltage and pin assignments.
7	**5G NR & Wi-Fi Antenna**	Install antennas for 5G (or 4G) and Wi-Fi networks with the corresponding receptacles: **Ant-F1~F4:** 5G or 4G antenna **Ant-F6/Ant-F8:** Wi-Fi antenna Note that **5G NR and Wi-Fi antennas are optional accessories, and not included in the standard package.** You need to purchase suitable antennas and RF cables for your application. Refer to **1.6.3 Install the External RF Cable and Antenna** for installation instructions.

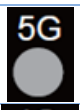
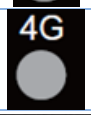
➢ Left View



No	Connector	Description
1	**SIM / MicroSD slots (with a slot cover)**	SIM and MicroSD slots. Refer to **1.6.1 Insert the SIM Card & MicroSD Card** for installation instructions.
2	**AI/DI/DO Terminal Block**	A terminal block for analog input and digital input/output connection. Refer to **1.6.4 Connecting I/O Devices** for pin assignments and voltage requirements.
3	**Earth Ground Screw**	Screws for grounding for protection against shock and damage to the device.

1.4 Indicator LEDs



LED Icon	Indication	LED Color	Description
	Power Source	Blue	**OFF:** Device is powered off. **Steady ON:** Device is powered ON.
	Status	Blue	**Flash (slow):** Device is working properly. **Flash (very fast):** Device is in Recovery Mode or is not working properly.
	Serial	Blue	**OFF:** No data transmission **Flash:** Data is being transmitted via the serial port.
	Wi-Fi-1	Blue	**OFF:** Wi-Fi function is disabled **Steady ON:** Wi-Fi (2.4GHz) is enabled **Flash:** Data packets being transmitted via the Wi-Fi 1 LAN interface.
	Wi-Fi-2	Blue	**OFF:** Wi-Fi function is disabled **Steady ON:** Wi-Fi (5GHz) is enabled **Flash:** Data packets being transmitted via the Wi-Fi 2 LAN interface.
	5G NR	Blue	**OFF:** 5G mobile is not in service **Steady ON:** 5G is attached **Flash (per Second):** Data is being transmitted
	4G LTE	Blue	**OFF**: 3G/4G mobile is not in service **Steady On**: 3G/4G is attached **Flash (per Second)**: Data is being tranmitted
	SIM A/B	Blue	**OFF:** No SIM card is inserted or operational **Steady ON**: **SIM A** slot is in use **Flash (per Second)**: **SIM B** slot is in use
	Signal	Blue	**Steady On:** Signal Strength is 61~100% **Slow Flash (on/off per 2 Seconds):** Signal Strength is 31~60% **Flash (on/off per seconds):** Signal Strength is 0~30% **OFF:** No signal
	LAN 1 ~ LAN 3/WAN	Green	**OFF:** Ethernet not connected to the host yet. **Steady ON:** Ethernet connection of LAN or WAN is established. **Flash:** Data is being transmitted via the Ethernet port.

1.5 Installation & Maintenance Notice

1.5.1 SYSTEM REQUIREMENTS

Network Requirements	• An RJ45 cable • 5G cellular service subscription • IEEE 802.11 b/g/n/a/ac wireless clients • 10/100/1000 Ethernet adapter on PC
Web-based Configuration Utility (Web UI) Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Microsoft Edge™ • Chrome™ 2.0 or higher • Firefox® 3.0 or higher • Safari® 3.0 or higher

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.

Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FOR PORTABLE DEVICE USAGE (<20 cm from body/SAR needed)

Radiation Exposure Statement:

The product comply with the FCC portable RF exposure limit set forth for an uncontrolled environment and are safe for intended operation as described in this manual. The further RF exposure reduction can be achieved if the product can be kept as far as possible from the user body or set the device to lower output power if such function is available.

FOR MOBILE DEVICE USAGE (>20 cm/low power)

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

FOR COUNTRY CODE SELECTION USAGE (WLAN DEVICES)

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all Wi-Fi product marketed in US must be fixed to US operation channels only.

1.5.3 HOT SURFACE CAUTION



CAUTION: The surface temperature of the metallic enclosure can be very high! It is especially hot after operating for a long time or if it is installed at a closed cabinet without air conditioning support or in a high ambient temperature space.
DO NOT touch the hot surface with your fingers while servicing!!

1.5.4 Product Information for CE RED Requirements

The following product information is required to be presented in product User Manual for the latest CE RED requirements. [2]

(1) Frequency Band & Maximum Power

1.a Frequency Band for 5G NR / 4G LTE Connection (for RXL-G1 version) [3]

Band number	Operating Frequency	Max output power
LTE & 5G NR Band 1	Uplink: 1920-1980 MHz Downlink: 2110-2170 MHz	25 dBm (EN-DC 20dBm)
LTE & 5G NR Band 3	Uplink: 1710-1785 MHz Downlink: 1805-1880 MHz	
LTE Band 7	Uplink: 2500-2570 MHz Downlink: 2620-2690 MHz	
LTE Band 8	Uplink: 880-915 MHz Downlink: 925-960 MHz	
LTE & 5G NR Band 20	Uplink: 832-862 MHz Downlink: 791-821 MHz	
LTE & 5G NR Band 28	Uplink: 758-803 MHz Downlink: 704.5-746.5 MHz	
LTE Band 32	Downlink: 1454.5-1493.5 MHz	
LTE Band 38	(TDD) 2572.5-2617.5 MHz	
5G NR Band 78	(TDD) 3400 ~ 3800 MHz	
WCDMA BAND 1	Uplink: 1920-1980 MHz Downlink: 2110-2170 MHz	24 dBm
WCDMA BAND 8	Uplink: 880-915 MHz Downlink: 925-960 MHz	

1.b Frequency Band for Wi-Fi Connection

Band	Operating Frequency	Max. Output Power (EIRP)
2.4G	2.4 – 2.4835 GHz	100 mW
5G	5.15– 5.25 GHz / 5.725– 5.85 GHz	1W Client device(250mw)

(2) 5150 ~ 5350MHz In Door Use Statements

This product equips the IEEE 802.11ac compliance 5GHz wireless radio module. According to the RED requirement, the channels covered in the 5150 ~ 5350 MHz frequency band are for indoor use only.

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

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

3 Different cellular modules can be integrated in the device for EU/EFTA regional version. Refer to the cellular module identifier printed on the device label for the purchased device.

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



AT	**BE**	**BG**	**CH**	**CY**	**CY**	**DK**
DE	**EE**	**EL**	**ES**	**FI**	**FR**	**HR**
HU	**IE**	**IT**	**LT**	**LU**	**LV**	**MT**
NL	**NO**	**PL**	**PT**	**RO**	**SI**	**SK**
SE	**TR**	**UK**				

(4) RF Exposure Statements

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

(5) Unit Mounting Notice

The product is suitable for mounting at heights <= 2m (approx. 6 ft), or in a cabinet.

Ensure the unit is fixed tightly to reduce the likelihood of injury due to exposure to mechanical hazards if dropped.

1.6 Hardware Installation

The available connectors and ports of the DOM-550-GSO:

- **SIM Slot:** 2* Micro SIM (3FF) slot
- **Ethernet:** 3* 10/100/1000Mbps RJ45 LAN port (one can be configured as LAN or WAN)
- **Analog Input:** 2* AI ports (supports 0~10V)
- **Digital Input:** 2* DI ports (isolated, “Logic 0”: 0~2V, “Logic 1”: 5~30V)
- **Digital Output:** 2* DO ports (isolated, Non-Relayed Output, Maximum 24V/300mA for each port)
- **Field Bus:** 1* RS-232/485 for legacy serial device, or Modbus RTU/ASCII devices
- **USB Port:** 1* USB 2.0 Type A port
- **Storage:** 1* MicroSD slot for SD 3.0 (SDXC) compliant storage expansion
- **Power Source:** 1* 2-pin Terminal Block for 9~36V DC power input

This below section describes how to install and configure the hardware.

1.6.1 Insert the SIM Card & MicroSD Card

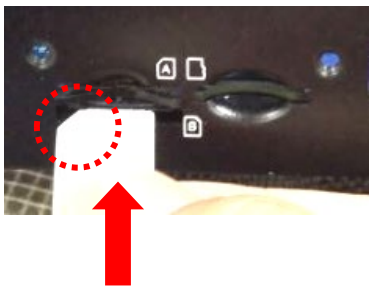
WARNING: Before inserting or changing the SIM card or MicroSD card, make sure that the power of the device is switched off.

The SIM card slots are located at the left side of the device housing. You need to unscrew and remove the SIM card cover before installing or removing the SIM card or MicroSD card. Please follow the instructions below to insert a SIM card. After the SIM card is inserted, push the SIM card to secure it in place.

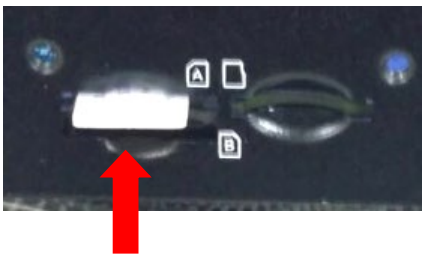
Step 1:
Loosen the screws as shown below and remove the SIM cover.



Step 2:
Align the SIM card and the slot with the right orientation as shown below. Push the SIM card into 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 DOM-550-GSO can be mounted on a wall, horizontal plane, or DIN Rail in a cabinet with the mounting accessories (DIN-rail kit or optional brackets). The mounting accessories are not attached to the device when the product is shipped. Please install the DIN-rail bracket or wall-mount bracket on the device first.

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 have to purchase the required RF cables and antennas separately according to your application requirements or the condition of the installation site for optimal RF performance.

Since there is limited space for allocating all SMA antenna jacks around the enclosure, the separation among SMA jacks (or direct-attached antennas) should be optimized. **It is not recommended to attach the SMA antennas directly to the SMA jacks.** It is very likely to get degraded RF performance depending on the circumstances at the installation site.

However, there are well-known 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 rules for both frequencies.

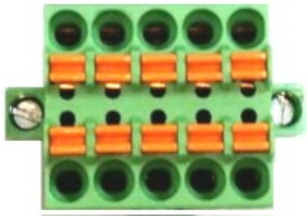
Wavelength Table for Major RF Category

RF Category	Frequency	Wavelength	1/2 Wave Length (Best Separation)	1/4 Wave Length (Good Separation)
Wi-Fi 802.11	5.8GHz	5.2cm	2.6cm	1.3cm
Wi-Fi 802.11	2.4GHz	12.5cm	6.2cm	3.1cm
Celllular 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

For example, if you have a 900MHz LTE antenna and a Wi-Fi 2.4GHz antenna, you should separate them by at least 8.3cm to satisfy good antenna separation. **Therefore, it is recommended to use some external RF cables to extend and separate the adjacent antennas and get better antenna separation and RF performance, if required.**

1.6.4 Connecting I/O Devices

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



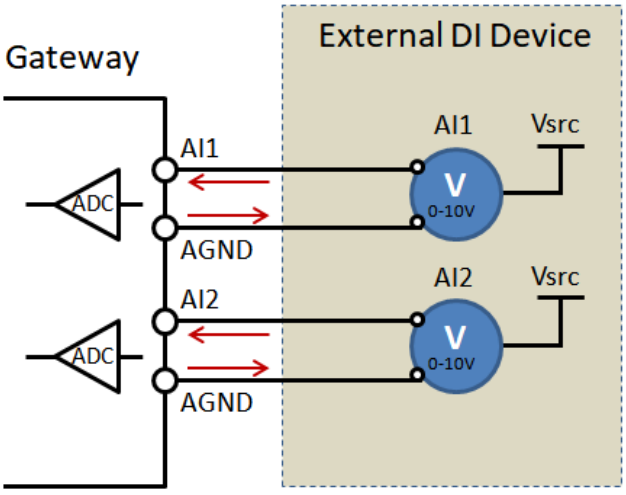
AGND	AGND	DO1	DO_COM	DO2
1	2	3	4	5
6	7	8	9	10
AI1	AI2	DI1	DI_COM	DI2

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

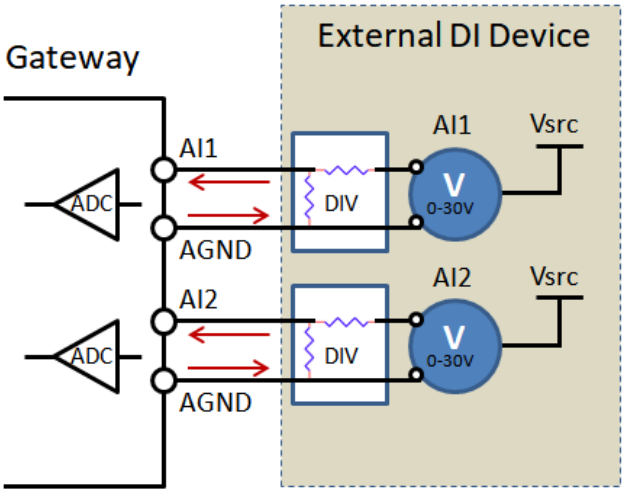
If the AI signal range of your device falls outside the design specification of the required 0~10V for DOM-550-GSO, you have to add a certain scaling circuit to prevent electric overflow that can cause damage to the DOM-550-GSO.

Example of AI Connection Diagram

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

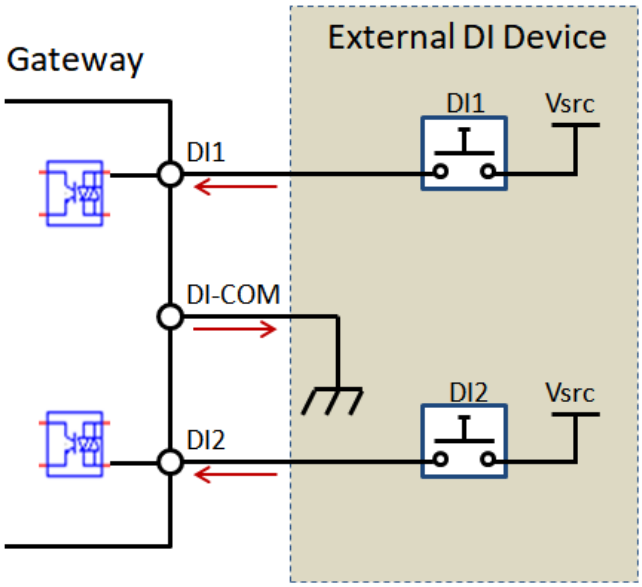


(2) AI Connection (for > 10V signal)

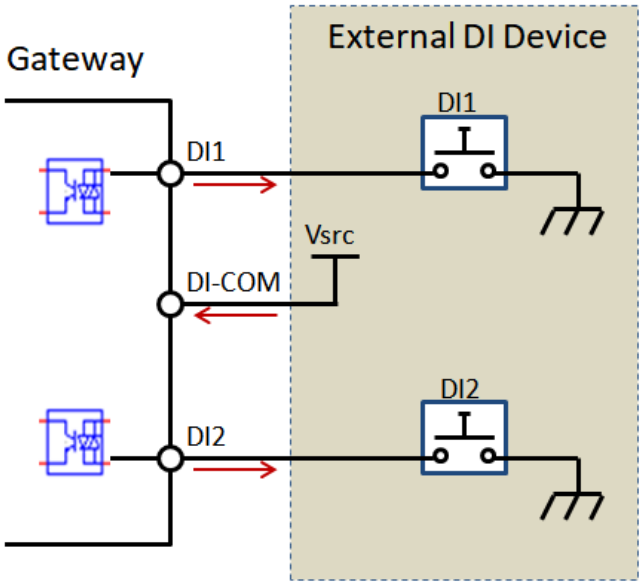


Example of DI Connection Diagram

(1) Sink-type DI Connection

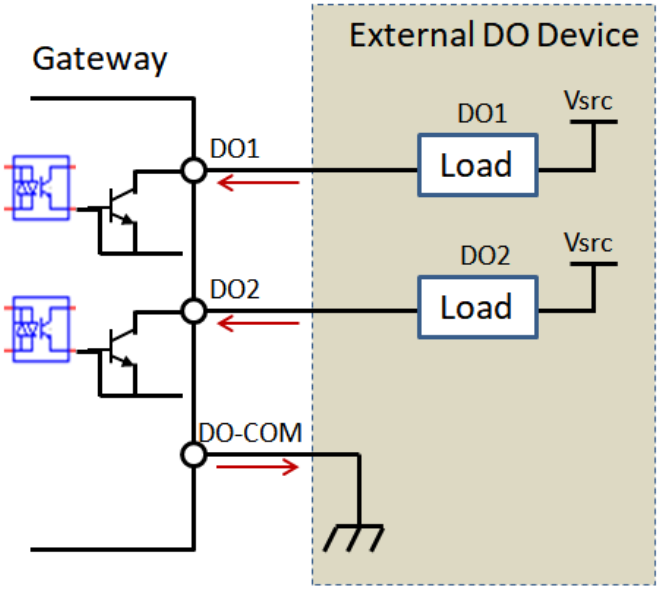


(2) Source-type DI Connection

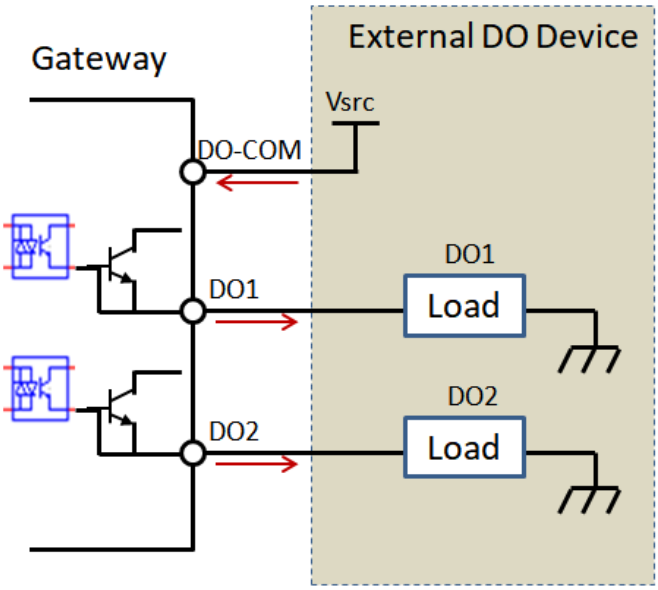


Example of DO Connection Diagram

(1) Sink-type DO Connection

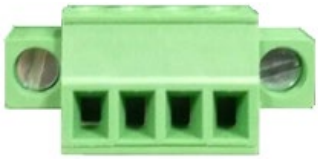


(2) Source-type DO Connection



1.6.5 Connecting Serial Devices

The DOM-550-GSO series provides serial communication via RS232/485 ports on a 4-pin terminal block. Connect your serial devices to the terminal block with the right pin assignments as shown 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 DOM-550-GSO series can be powered by connecting a DC power source to the 2-pin power terminal block. **It supports 9 to 36V DC power input**. Please connect the power supply according to the following pin assignments with correct polarity.



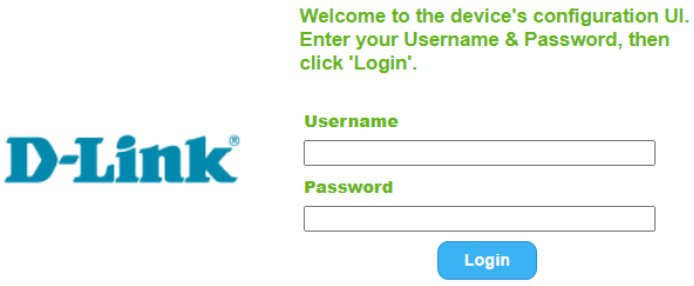
1.6.7 Connecting to the Network or a Host

The DOM-550-GSO series provides RJ45 ports with 10/100/1000Mbps Ethernet connectivity. It can detect the transmission speed of the link and negotiates the transmission speed automatically. Connect one end of the Ethernet cable to the RJ45 port (LAN) of the device and plug another end of the Ethernet cable into your computer's network port for device configuration.

1.6.8 Connecting the Web UI

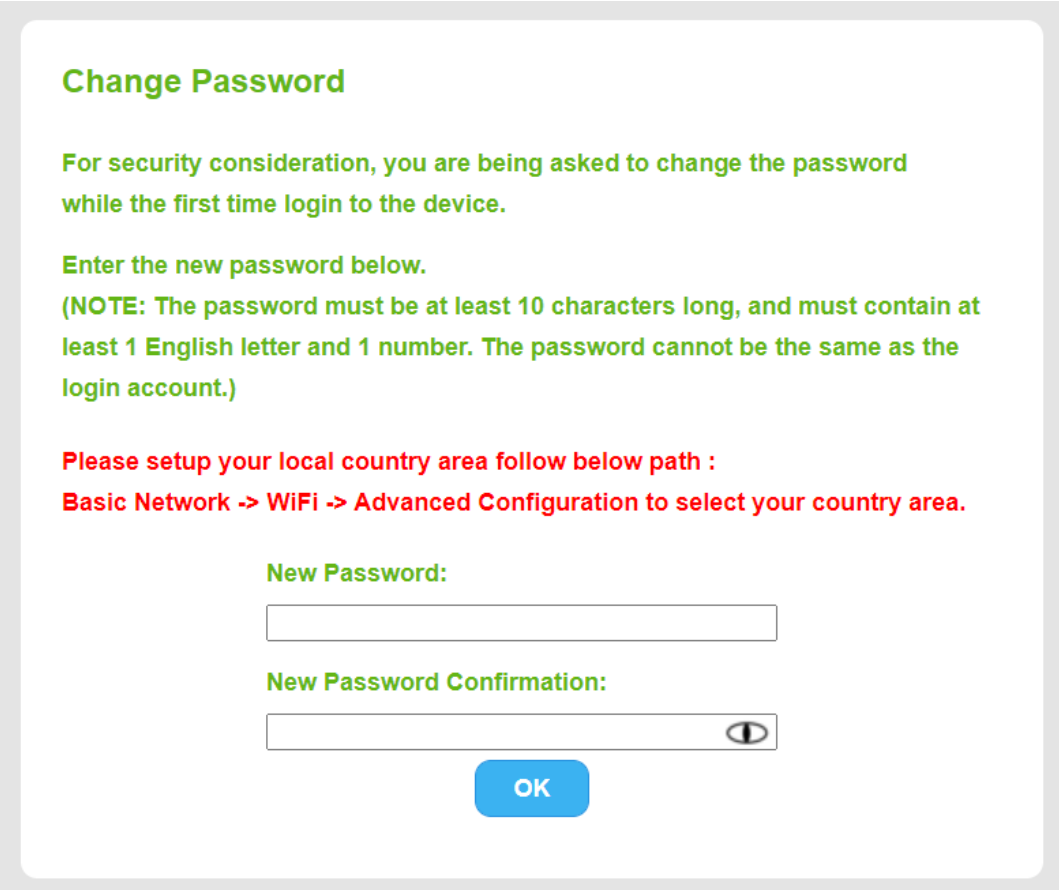
Open the browser to connect to the Web UI of the device by typing the IP Address (**http://192.168.0.1**)[4] in the address field.

When you see the login page, enter the username and password and then click **'Login'**.
The default setting for both username and password is **'admin'**.



For better security, you will be required to change the loging password the first time you log in to the device. Then, log in again with the new password.

4 The default LAN IP address of this gateway is 192.168.0.1. If you change it, you need to log in using the new IP address.



Note:

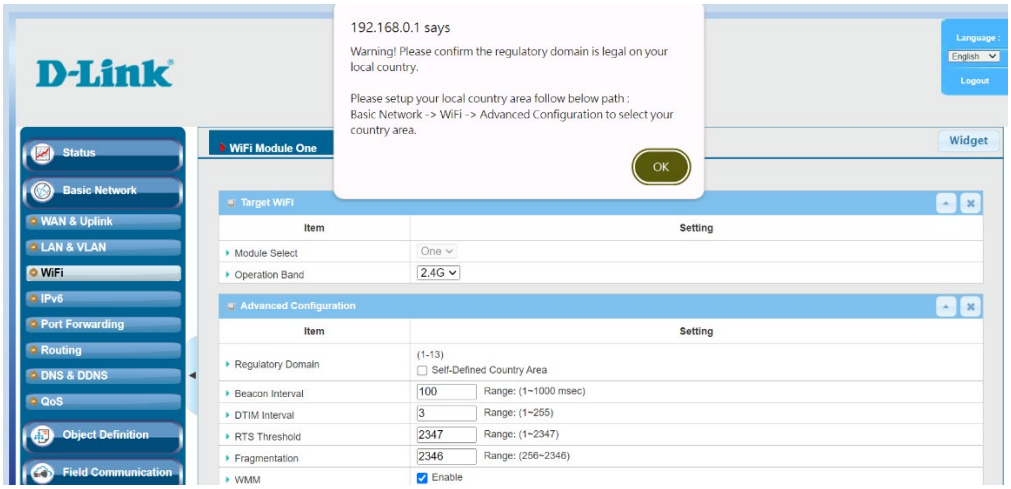
Keep the login password properly for future configuration. If you lose or forget the login password, the ONLY way to recover this is to restore the device to its factory default settings using the Reset button. Resetting the device to its factory defaults will erase your device configuration completely. Therefore, you may also need to back up the device configuration for future recovery. Refer to **6.2.5 Backup & Restore**.

1.6.9 Configure User Country area

Please Set up your country area before you use DOM-550-GSO function.
Please use the following procedure to configure your country area:

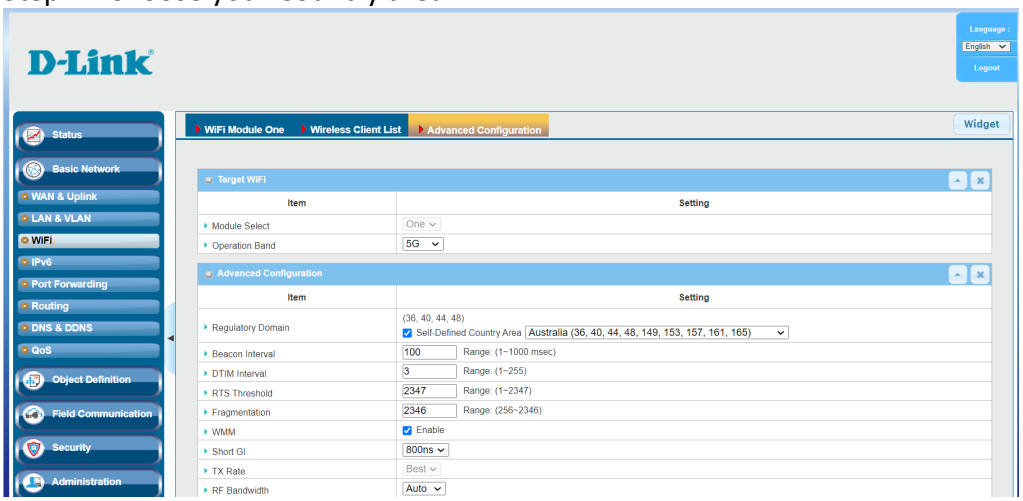
(1) Wi-Fi 2.4GHz

Step 1: Select **Basic Network > WiFi > Advanced Configuration**.
Step 2: Set Operation Band to 2.4G.
Step 3: Enable **Self-Defined Country Area**.
Step 4: Choose your Country area.



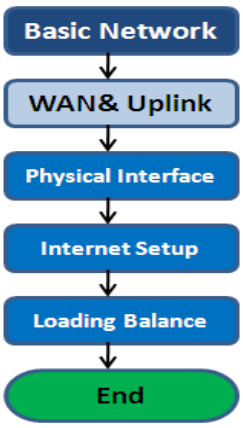
(2) Wi-Fi 5GHz

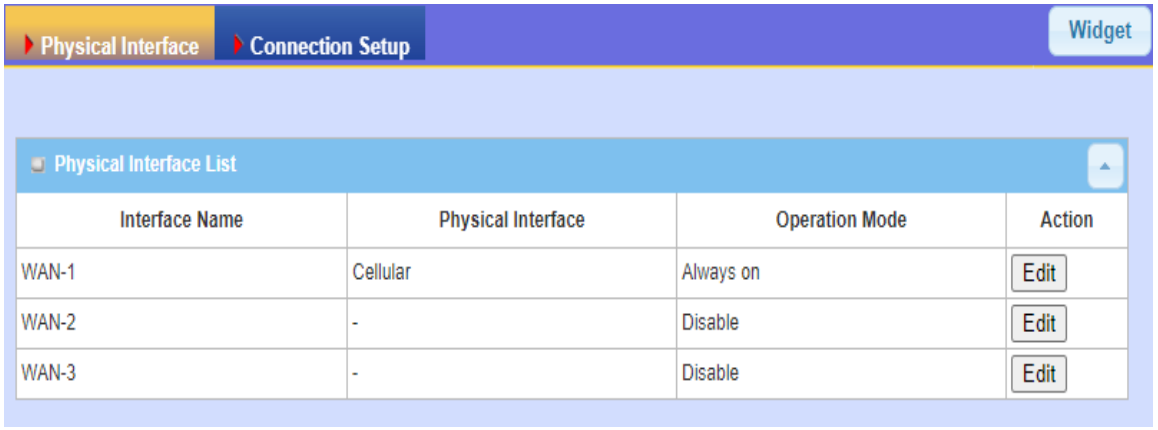
Step 1: Select **Basic Network > WiFi > Advanced Configuration.**
Step 2: Set Operation Band to 5G.
Step 3: Enable **Self-Defined Country Area**.
Step 4: Choose your Country area.



Chapter 2 Basic Network

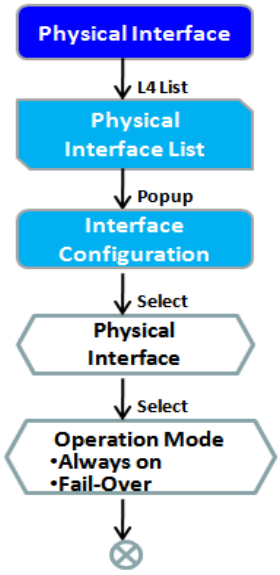
2.1 WAN & Uplink

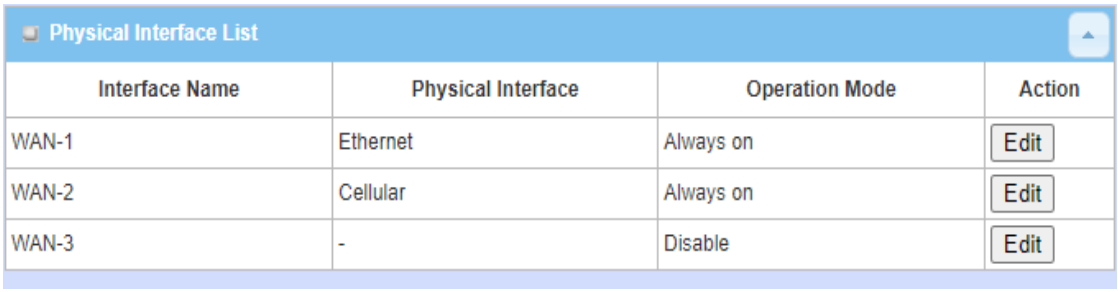


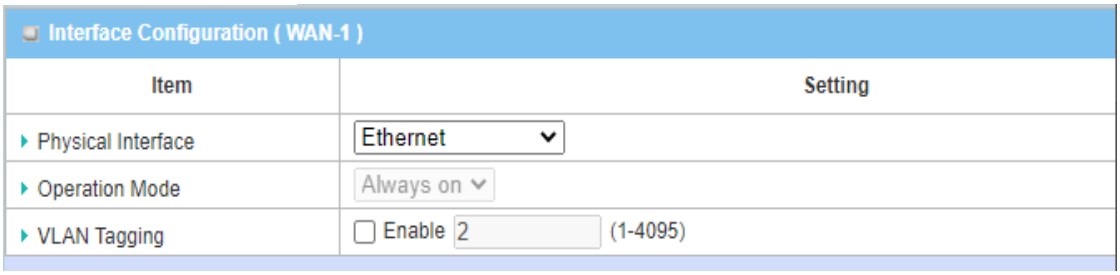


The gateway provides multiple WAN interfaces to achive redundant Internet connections. But ISPs in the world require different connection methods for Internet connectivity via different transmission media. Hence, you need to configure WAN Internet Setup and WAN Load Balance for Internet access with load balance among selected physical interfaces.

2.1.1 Physical Interface







Network gateways are usually equipped with various WAN interfaces to support different WAN connection scenarios. You can configure the WAN interface one by one to set up proper Internet connections. **Refer to the product specification for the available WAN interface types supported in the product.**

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

To configure a WAN interface, go to **Basic Network > WAN & Uplink > Physical Interface.**

In the "Physical Interface" page, the "Physical Interface List" window shows all the available physical interfaces. To configure a WAN interface, click the **Edit** button for a specific interface in the "Physical Interface List" window to display the "Interface Configuration" window.

Physical Interface:

- **Ethernet WAN:** The gateway has one or more RJ45 WAN ports that can be connected to a DSL modem or to an existing a firewall device.
- **Cellular WAN:** The gateway has one built-in 5G NR modem for WAN connection. For each cellular WAN, there are 1 or 2 SIM cards to allow for failover.

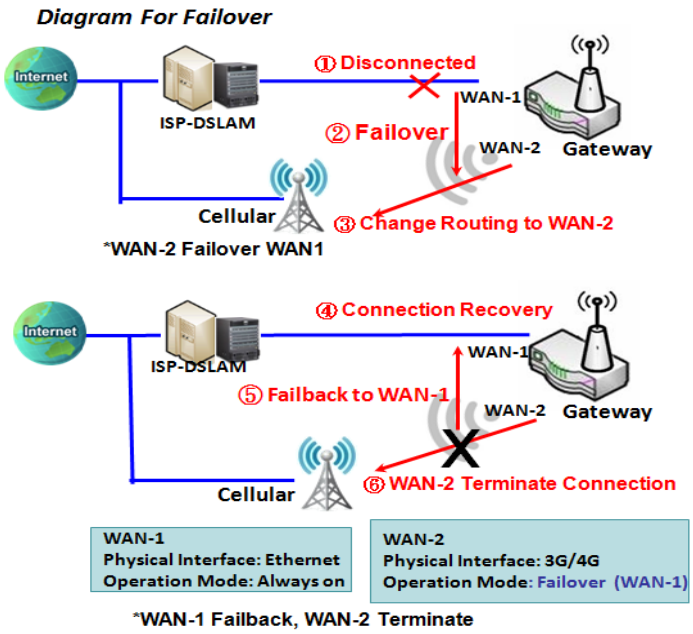


- Please **POWER OFF** the gateway before you insert or remove a SIM card.
- The SIM card can be damaged if you insert or remove it while the gateway is powered on.

Operation Mode:

There are three options for the mode: Always on, Failover, and Disable.

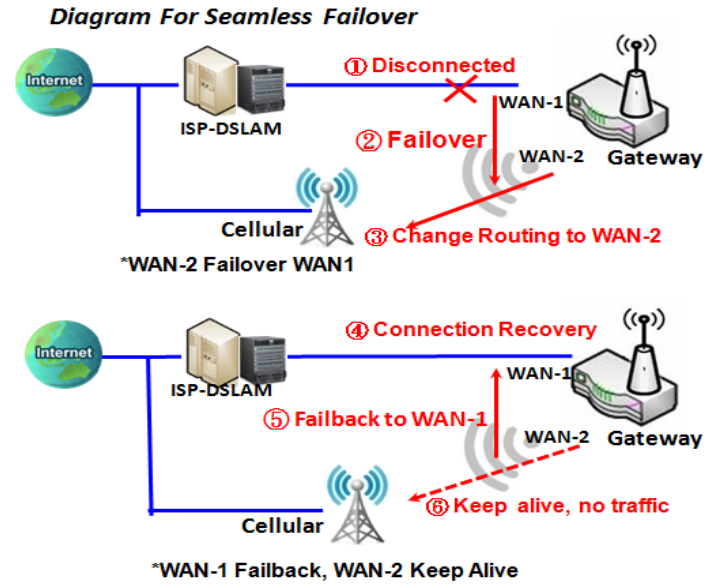
Always on: Set this WAN interface to be constantly active. When two or more WAN interfaces are established in "Always on" mode, traffic for WAN connections will be distributed according to load balance policies.



Failover:

A failover interface is a backup connection to the primary. When its primary WAN connection is broken, the backup connection will substitute for the primary connection.

As shown in the diagram, WAN-2 is the 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 transmission again and WAN-2 connection will be terminated.



Seamless Failover:

In addition, there is a "Seamless" option for Failover operation mode, which activates both primary connection and the failover connection after system restarts; however, only the primary connection is active while the failover connection is in standby mode. As soon as the primary connection is broken, the system will switch to the failover connection without the need to dial up to save time for the failover process because it has been connected continuously since system boot.

VLAN Tagging

Sometimes, your ISP required a VLAN tag to be inserted into the WAN packets from the gateway for specific services. Please enable VLAN tagging and specify tag in the WAN physical interface. Note that only Ethernet and ADSL physical interfaces support this feature.

Physical Interface Setting

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

Note: The number of available WAN Interfaces can be different depending on the device model.

Physical Interface List

Interface Name	Physical Interface	Operation Mode	Action
WAN-1	Ethernet	Always on	Edit
WAN-2	Cellular	Always on	Edit
WAN-3	-	Disable	Edit

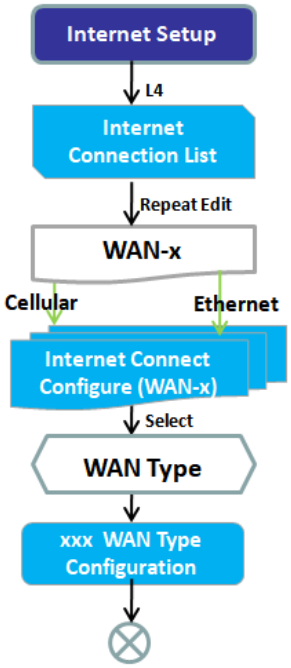
To configure a WAN interface, click **Edit** and the **Interface Configuration** screen appears.

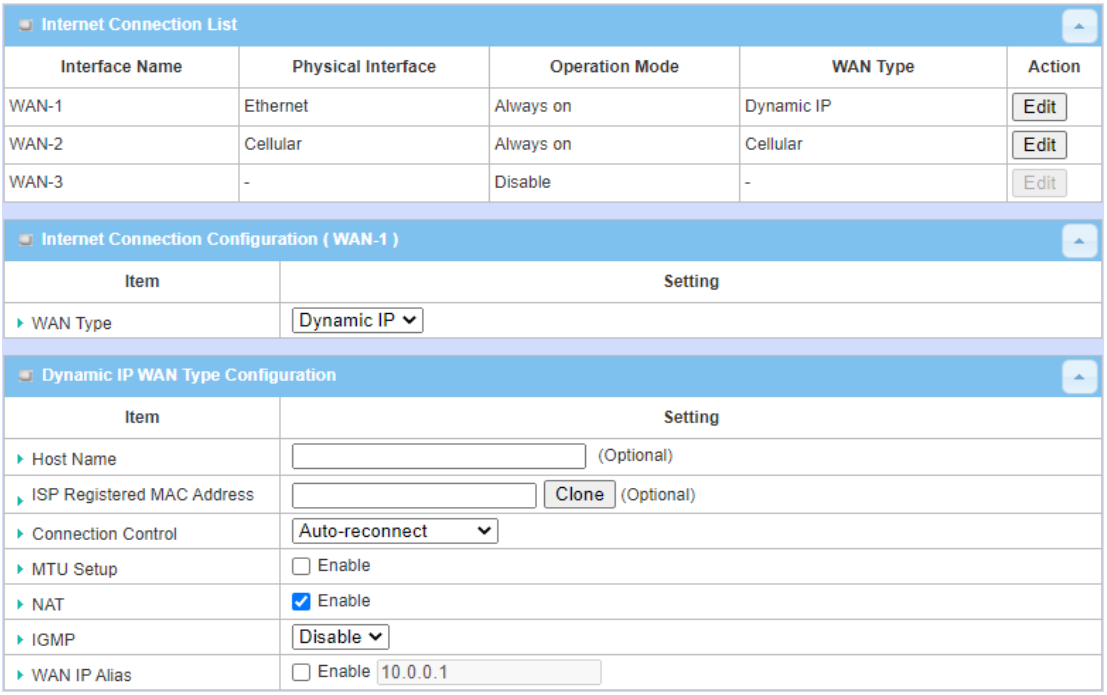
Interface Configuration (WAN-1)

Item	Setting
Physical Interface	Ethernet
Operation Mode	Always on
VLAN Tagging	Enable 2 (1-4095)

Interface Configuration		
Item	**Value setting**	**Description**
Physical Interface	1. A must-filled setting 2. WAN-1 is the primary interface and the default is set to Always on.	Select an interface from the available interface dropdown list. The options are **Cellular** and **Etherent**. The **Disable** and **Failover** options will be available only to models with multiple WAN interfaces.
Operation Mode	A must-filled setting	Define the operation mode of the interface. Select **Always on** to make this WAN always active. Select **Disable** to disable this WAN interface. Select **Failover** to make this WAN a Failover WAN when the primary or the secondary WAN link fails. Then select the primary WAN interface to switch Failover from. **Notes**: 1. For WAN-1, only the **Always on** option is available. 2. For WAN-2, disable this interface if you want to use it as a LAN interface.
VLAN Tagging	Optional setting	Check **Enable** box to enter VLAN tag provided by your ISP. *Value Range*: 1 ~ 4095. Note: This feature is NOT available for cellular WAN connection.

2.1.2 Connection Setup





After specifying the physical interface for each WAN connection, you must configure their connection profile according to the ISP's connection requirement to access the Internet.

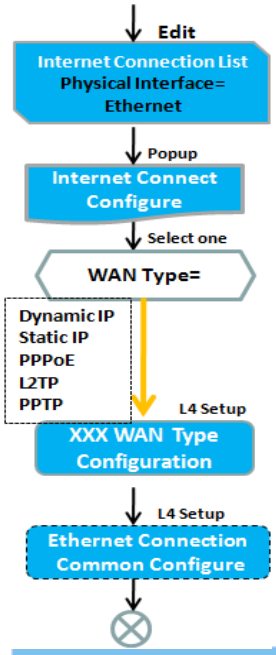
To configure a connection profile:

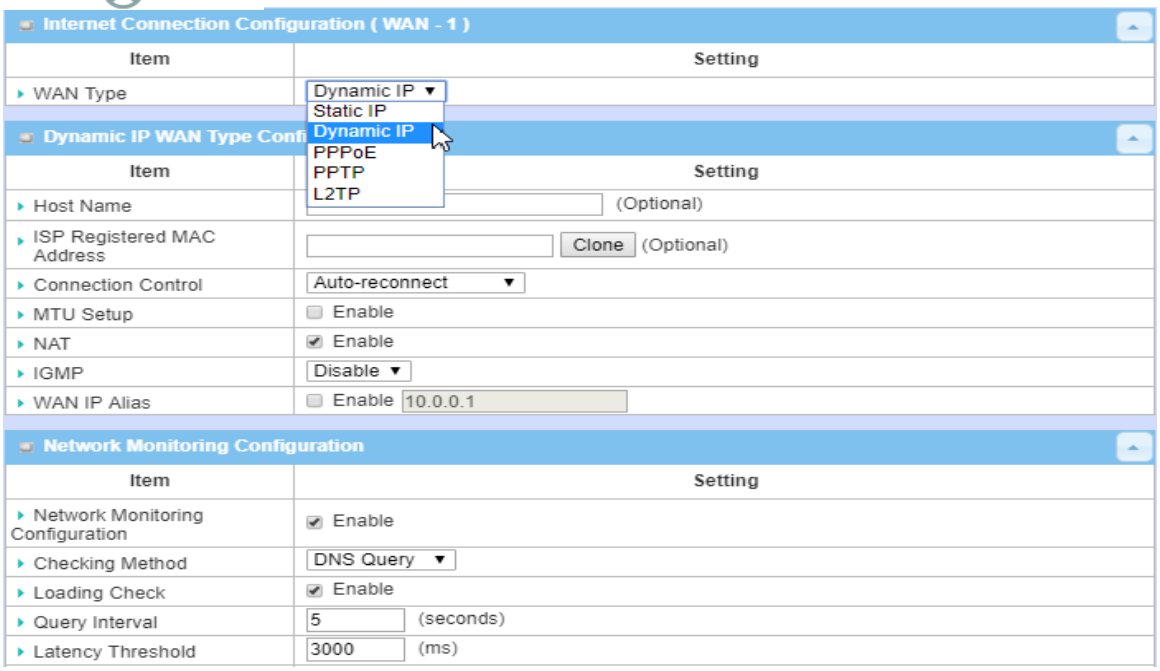
1. Click the "Connection Setup" page to access the configuration windows: "Internet Connection List", "Internet Connection Configuration", and "WAN Type Configuration". For the Internet setup of each WAN interface, you must specify its WAN type first and then proceed to configure its related parameters according to the selected WAN type.

2. Click the **Edit** button of a physical interface in "Internet Connection List" window, the "Internet Connection Configuration" window will appear. You can then specify the WAN type for that physical interface to make an Internet connection.

The following sections describe the configuration parameters for different WAN types.

Internet Connection List - Ethernet WAN





Ethernet is one of the the most common WAN and uplink interfaces for gateways. Usually, it is connected to a xDSL or cable modem. There are various WAN types to connect with an ISP:

- **Static IP:** Select this option if your ISP provides a fixed IP to you when you subsribe the service. Usually it is more expensive but common for corporate networks.
- **Dynamic IP:** The assigned IP address for the WAN by a DHCP server is different every time. It is cheaper and usually for residential use.
- **PPP over Ethernet:** As known as PPPoE. This WAN type is widely used for ADSL connection.
- **PPTP:** Point-to-Point Tunneling Protocol (PPTP) is a tunneling protocol popular in some countries such as Russia.
- **L2TP:** Layer 2 Tunneling Protocol (L2TP) is also a tunneling protocol popular in some countries such as

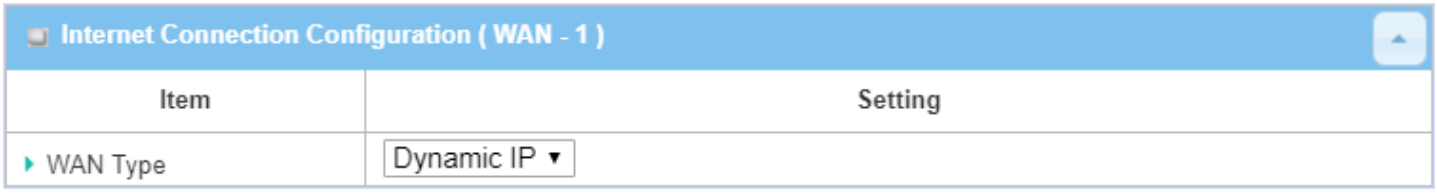
Israel.

Note: The available WAN types depend on product model.

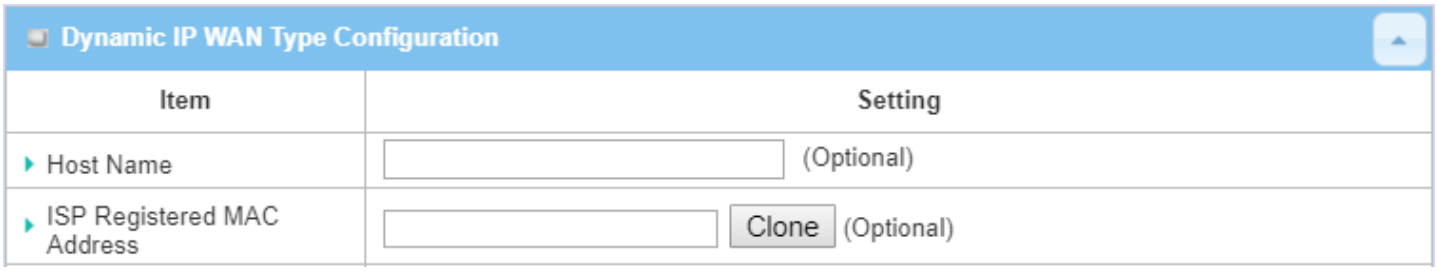
Configure Ethernet WAN Setting

To configure the WAN type for Internet access, click **Edit** to open the **Internet Connection Configuration** screen. WAN-1 interface is used in this example.

WAN Type: Dynamic IP

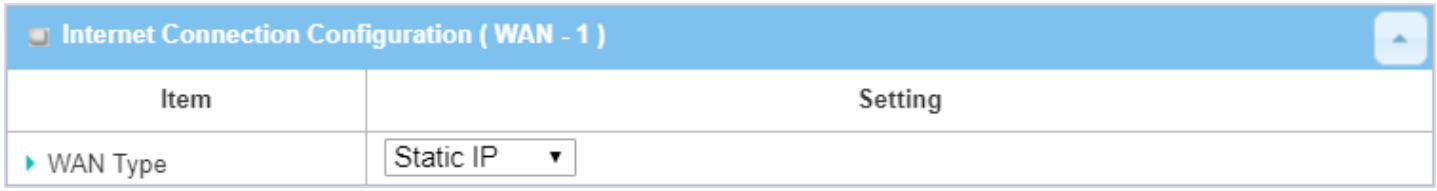


Select **Dynamic IP** to open **Dynamic IP WAN Type Configuration**.

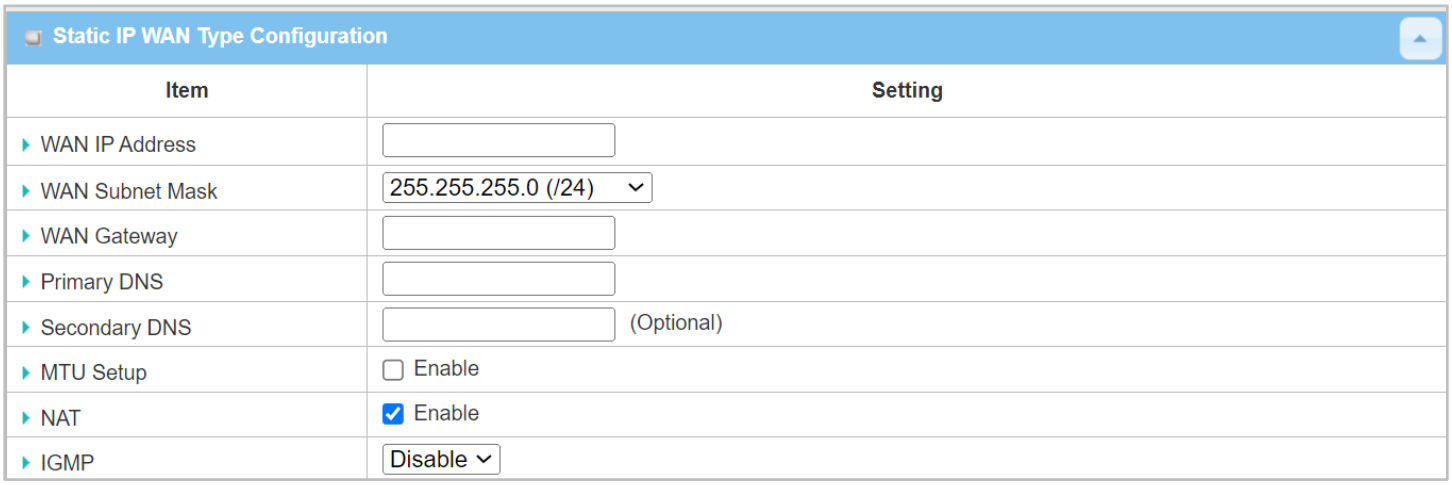


Dynamic IP WAN Type Configuration		
Item	**Value setting**	**Description**
Host Name	An optional setting	Enter the host name provided by your ISP.
ISP Registered MAC Address	An optional setting	Enter the MAC address that you have registered with your ISP. Or Click the **Clone** button to clone your PC's MAC to this field.

WAN Type: Static IP

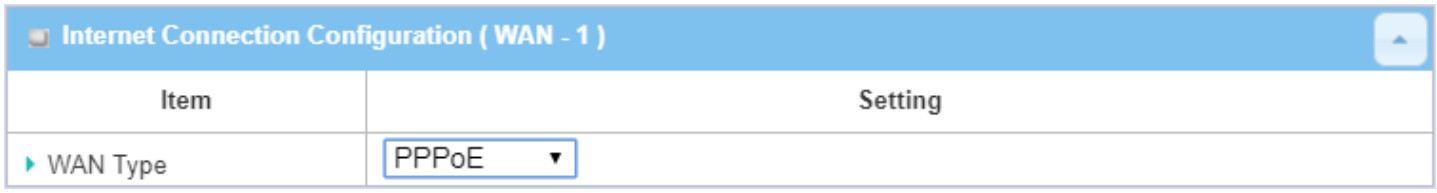


Select **Static IP** to open **Static IP WAN Type Configuration**.

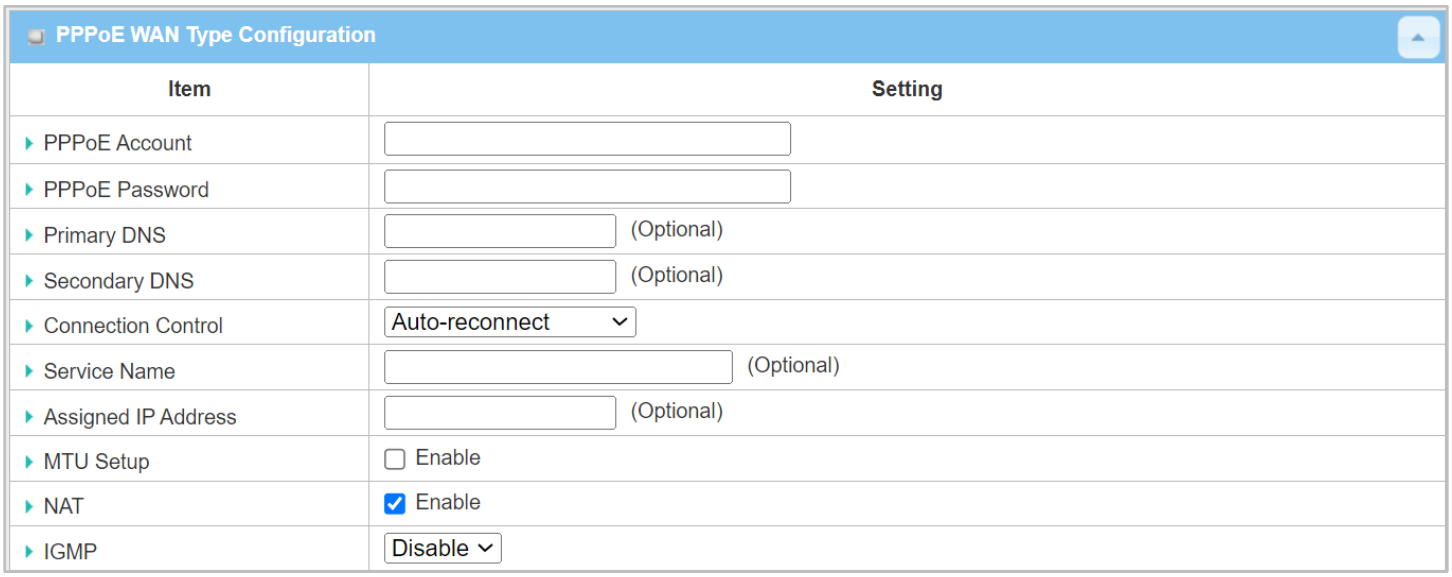


Static IP WAN Type Configuration		
Item	**Value setting**	**Description**
WAN IP Address	A must-filled setting	Enter the WAN IP address given by your ISP.
WAN Subnet Mask	A must-filled setting	Enter the WAN subnet mask given by your ISP.
WAN Gateway	A must-filled setting	Enter the WAN gateway IP address given by your ISP.
Primary DNS	A must-filled setting	Enter the primary WAN DNS IP address given by your ISP.
Secondary DNS	An optional setting	Enter the secondary WAN DNS IP address given by your ISP.
MTU Setup	1. An optional setting 2. **Uncheck** by default	Check the Enable box to enable the MTU (Maximum Transmission Unit) limit and specify the **MTU** (Maximum Transmission Unit). The **MTU** specifies the largest packet size permitted for Internet transmission. When set to **Auto** (value '0'), the gateway selects the best MTU for optimal Internet connection performance. *Value Range*: 1200 ~ 1500.
NAT	1. An optional setting NAT is enabled by default	Enable NAT to apply Network Address Translation (NAT) on the WAN connection.
IGMP	1. A must-filled setting 2. Disable is set by default	Enable Internet Group Management Protocol (IGMP) would enable the gateway to listen to IGMP packets to discover which interfaces are connected to which device. The gateway uses the interface information gathered by IGMP to conserve bandwidth consumption in a multi-access network environment to avoid flooding multicast traffic in the network.

WAN Type: PPPoE



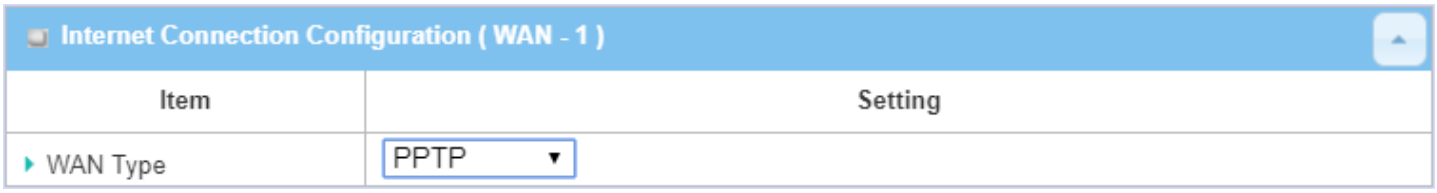
Select **PPPoE** to open **PPPoE WAN Type Configuration**.



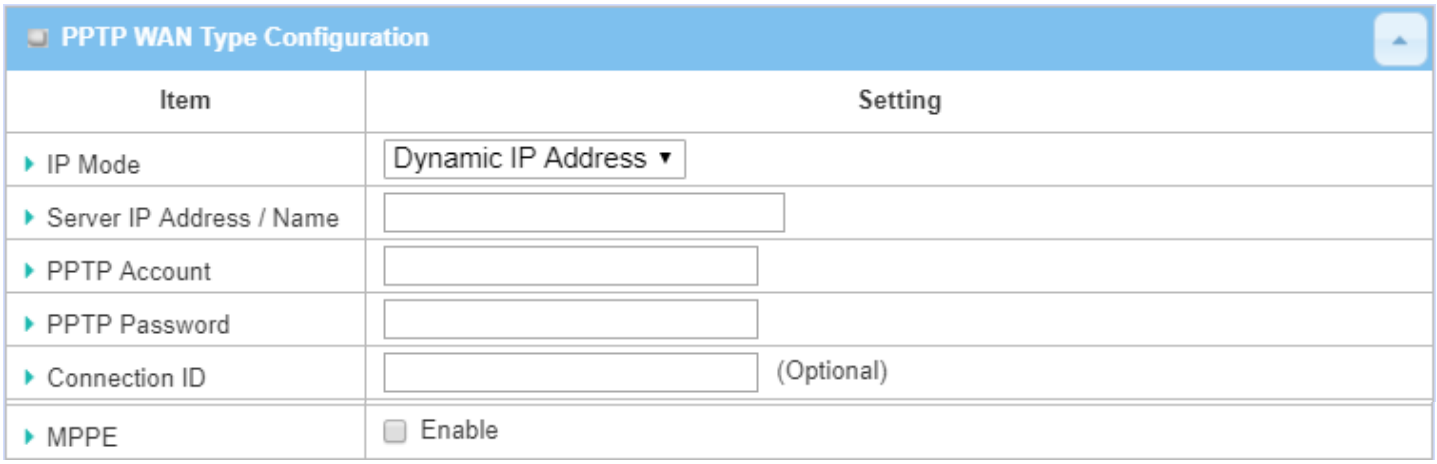
PPPoE WAN Type Configuration		
Item	**Value setting**	**Description**
PPPoE Account	A must-filled setting	Enter the PPPoE username provided by your ISP.
PPPoE Password	A must-filled setting	Enter the PPPoE password provided by your ISP.
Primary DNS	An optional setting	Enter the IP address of Primary DNS server.
Secondary DNS	An optional setting	Enter the IP address of Secondary DNS server.
Service Name	An optional setting	Enter the service name if your ISP requires it.
Assigned IP Address	An optional setting	Enter the IP address assigned by your ISP.
Connection Control	A must-filled setting	There are three connection modes: • **Auto-reconnect** enables the gateway to always keep the Internet connection on. • **Connect-on-demand** enables the gateway to automatically re-establish an Internet connection as soon as you attempt to access the Internet. Internet connection will be disconnected when it has been inactive for the specified idle time. **Connect Manually** allows you to connect to the Internet manually**.** Internet connection will be closed after it has been inactive for the specified idle time.
Maximum Idle Time	1. An optional setting 2. The default is **600** seconds	Specify the maximum Idle time after which the Internet will be disconnected. *Value Range*: 300 ~ 86400. **Note**: This field is available only when **Connect-on-demand** or **Connect Manually** is selected as thautoe connection control scheme.
MTU Setup	1. An optional setting	Check the Enable box to enable the MTU (Maximum Transmission Unit)

	2. **Uncheck** by default	limit and specify the **MTU** (Maximum Transmission Unit). The **MTU** specifies the largest packet size permitted for Internet transmission. When set to **Auto** (value '0'), the gateway selects the best MTU for optimal Internet connection performance. *Value Range*: 1200 ~ 1500.
NAT	2. An optional setting NAT is enabled by default	Enable NAT to apply Network Address Translation (NAT) on the WAN connection.
IGMP	1. A must-filled setting 3. 2. Disable is set by default	Enable Internet Group Management Protocol (IGMP) would enable the gateway to listen to IGMP packets to discover which interfaces are connected to which device. The gateway uses the interface information gathered by IGMP to conserve bandwidth consumption in a multi-access network environment to avoid flooding multicast traffic in the network.

WAN Type: PPTP

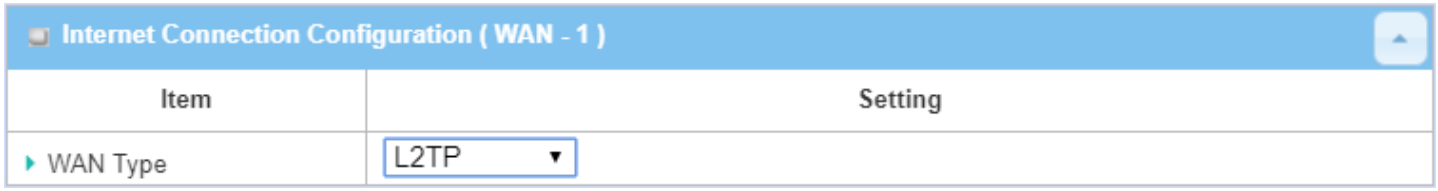


Select **PPTP** to open **PPTP WAN Type Configuration**.

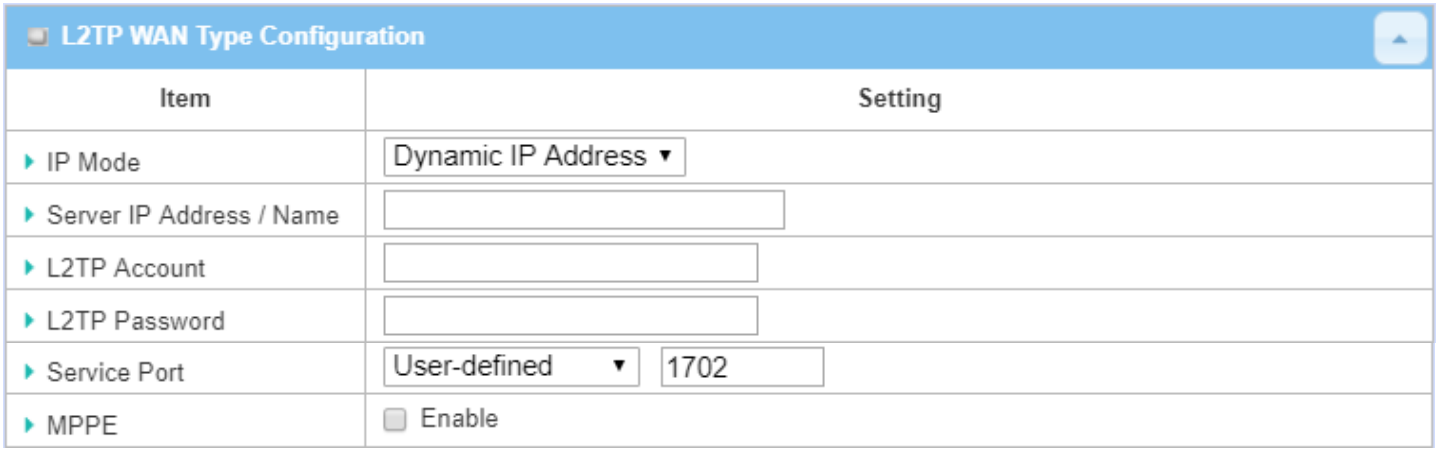


PPTP WAN Type Configuration		
Item	**Value setting**	**Description**
IP Mode	A must-filled setting	Select either Static or Dynamic IP address for PPTP Internet connection. ● When **Static IP Address** is selected, you will need to enter the **WAN IP Address**, **WAN Subnet Mask,** and **WAN gateway**. ■ **WAN IP Address** (A must-filled setting)**:** Enter the WAN IP address given by your ISP. ■ **WAN Subnet Mask** (A must-filled setting)**:** Enter the WAN subnet mask given by your ISP. ■ **WAN gateway** (A must-filled setting)**:** Enter the WAN gateway IP address given by your ISP. ● When **Dynamic IP** is selected, none of the above settings is required.
Server IP Address/Name	A must-filled setting	Enter the PPTP server name or IP Address.
PPTP Account	A must-filled setting	Enter the PPTP username provided by your ISP.
PPTP Password	A must-filled setting	Enter the PPTP connection password provided by your ISP.
Connection ID	An optional setting	Enter a name to identify the PPTP connection.
MPPE	An optional setting	Select **Enable** to enable MPPE **(**Microsoft Point-to-Point Encryption) security for PPTP connection.

WAN Type: L2TP

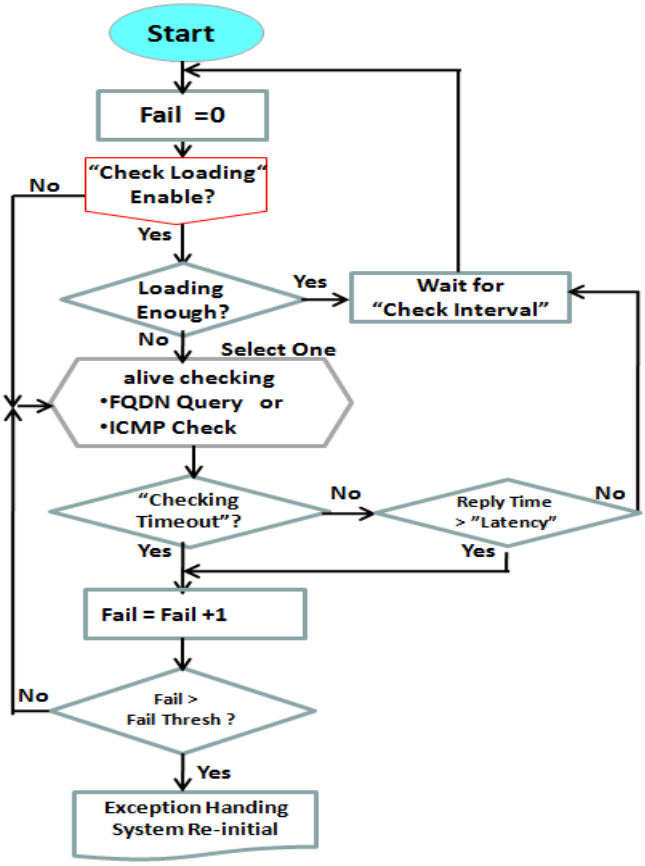


Select **L2TP** to open **L2TP WAN Type Configuration**.

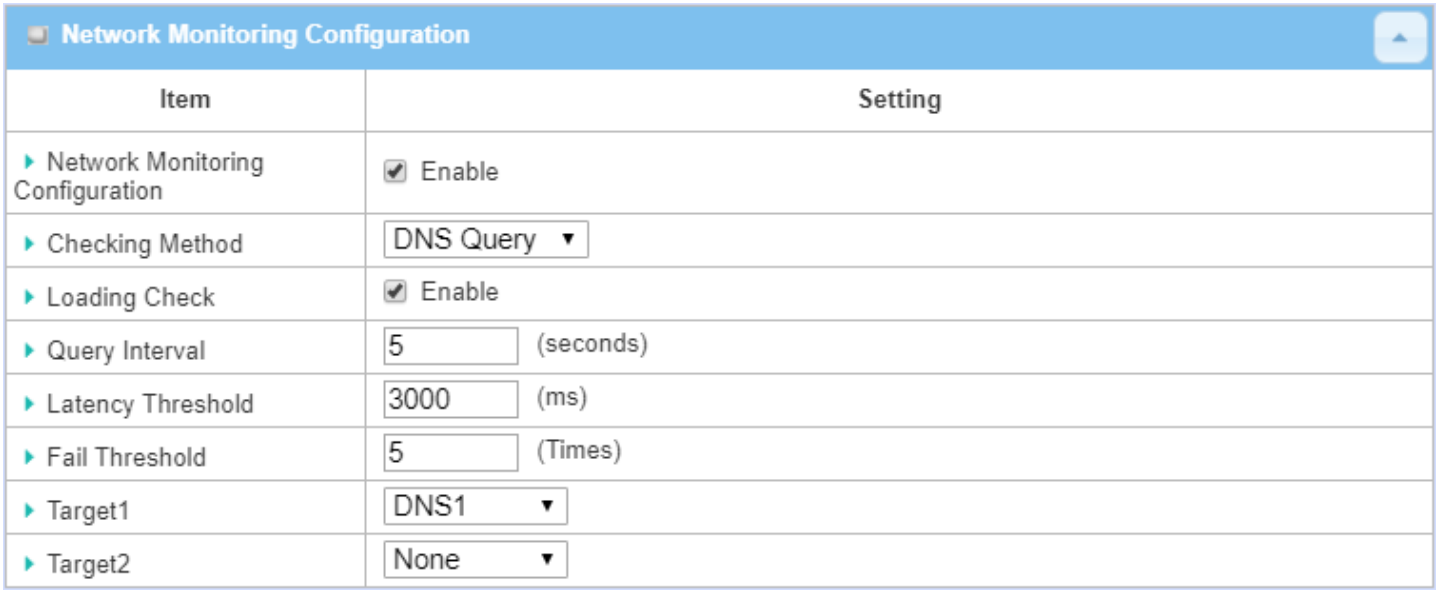


L2TP WAN Type Configuration		
Item	**Value setting**	**Description**
IP Mode	A must-filled setting	Select either Static or Dynamic IP address for L2TP Internet connection. ● When **Static IP Address** is selected, you will need to enter the **WAN IP Address**, **WAN Subnet Mask,** and **WAN gateway**. ■ **WAN IP Address** (A must-filled setting)**:** Enter the WAN IP address given by your ISP. ■ **WAN Subnet Mask** (A must-filled setting)**:** Enter the WAN subnet mask given by your ISP. ■ **WAN gateway** (A must-filled setting)**:** Enter the WAN gateway IP address given by your ISP. ● When **Dynamic IP** is selected, none of the above settings is required.
Server IP Address/Name	A must-filled setting	Enter the L2TP server name or IP Address.
L2TP Account	A must-filled setting	Enter the L2TP username provided by your ISP.
L2TP Password	A must-filled setting	Enter the L2TP connection password provided by your ISP.
Service Port	A must-filled setting	Enter the service port that the Internet service will use: ● **Auto:** Port will be automatically assigned. ● **1701 (For Cisco)**: Set service port to port 1701 to connect to a CISCO server. ● **User-defined**: enter a service port provided by your ISP.
MPPE	An optional setting	Select **Enable** to enable MPPE **(**Microsoft Point-to-Point Encryption) security for PPTP connection.

Network Monitoring



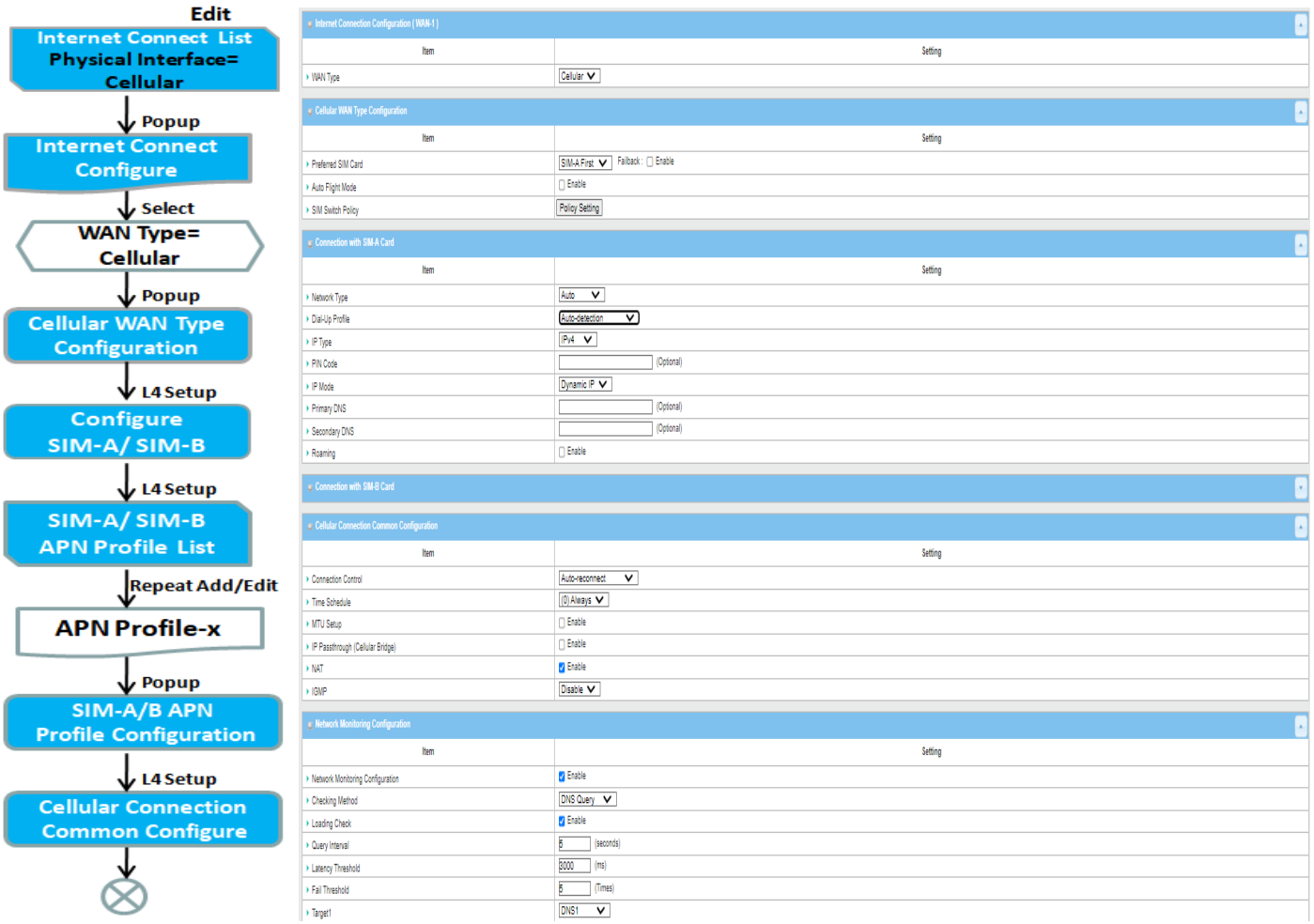
If it is necessary to monitor connection status continuously, "ICMP Check" and "FQDN Query" can be applied. However, this consumes bandwidth and increases response time. To minimize the impact of "Network Monitoring" on network performance, "Check Loading" can be enabled to stop connection monitoring when there is traffic. The diagram at the left illustrates the "Check Loading" mechanism.



Network Monitoring Configuration		
Item	**Value setting**	**Description**
Network Monitoring Configuration	1. An optional setting 2. Box is checked by default	Check the **Enable** box to activate the network monitoring function.
Checking Method	1. An optional setting 2. **DNS Query** is set by default	Choose either **DNS Query** or **ICMP Checking** to check if the WAN link is connected properly. With **DNS Query**, the system checks the connection using DNS query sent to the destination specified in Target 1 and Target 2. With **ICMP Checking**, the system checks connection using ICMP request sent to the destination specified in Target 1 and Target 2.
Loading Check	1. An optional setting 2. Box is checked by default	Check the **Enable** 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.
Query Interval	1. An optional setting 2. **5 seconds** is selected by default.	If you select DNS Query as the Checking Method, specify a time interval for the **DNS Query**. **Query Interval** defines the transmitting interval between two DNS Query or ICMP checking packets. With **DNS Query,** the system checks the connection by sending DNS query packets to the destination specified in Target 1 and Target 2. *Value Range*: 2 ~ 14400.
Check Interval	1. An optional setting 2. **5 seconds** is selected by default.	If you select ICMP Checking as the Checking Method, specify a time interval for the **ICMP Checking**. **Query Interval** defines the transmitting interval between two DNS Query or ICMP checking packets. With **ICMP Checking,** the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2. *Value Range*: 2 ~ 14400.
Latency Threshold	1. An optional setting 2. **3000 ms** is set by default	Enter a number as the threshold time for disconnection detection time. **Latency Threshold** defines the timeout threshold of response time. *Value Range*: 2000 ~ 3000 seconds.
Fail Threshold	1. An optional setting 2. **5 times** is set by default	Enter a number as the threshold for disconnection detection time. **Fail Threshold** specifies the number of detected disconnection times before the gateway recognizes the down status of the WAN link. *Value Range*: 1 ~ 10 times.
Target 1	1. An optional setting 2. **DNS1** is selected by	**Target1** specifies the first target of sending a DNS query/ICMP request. **DNS1**: the primary DNS is set as the target.

	default	**DNS2**: the secondary DNS is set as the target. **Gateway**: set the Current gateway to be the target. **Other Host**: enter an IP address to be the target.
Target 2	1. An optional setting 2. **None** is selected by default	**Target1** specifies the second target of sending a DNS query/ICMP request. **None:** no second target is required. **DNS1**: the primary DNS is set as the target. **DNS2**: the secondary DNS is set as the target. **Gateway**: set the Current gateway to be the target. **Other Host**: enter an IP address to be the target.
Save	*N/A*	Save the settings.
Undo	*N/A*	Discard the settings.

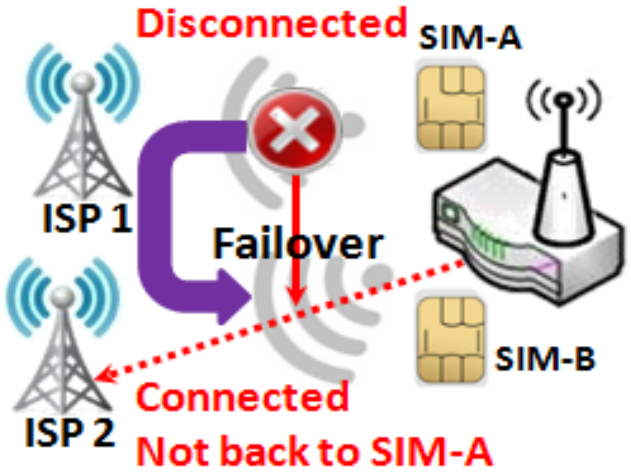
Internet Connection – Cellular WAN



Preferred SIM Card – Dual SIM Failover

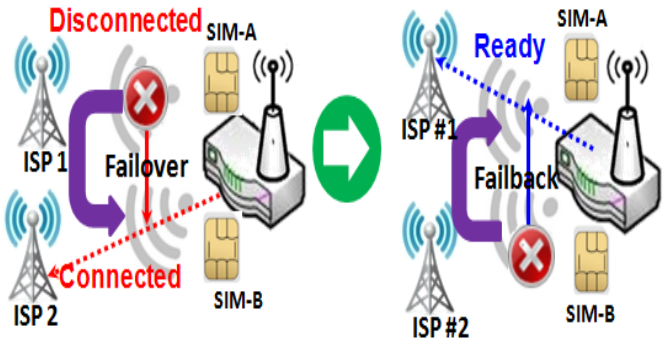
For devices with mobile connectivity, one embedded cellular module can be used for only one WAN interface. This device uses dual SIM cards with advanced failover mechanism. This feature is useful for switching between different mobile network carriers when the location is changed. The “Dual SIM Failover” can be implemented in various usage scenarios, including "SIM-A First" or "SIM-B First“ with or without “Failback” as well as “SIM-A Only and “SIM-B Only”.

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



SIM-A / SIM-B first without Failback

By default, “SIM-A First” scenario is used to connect to cellular ISP for data transfer. In the case of “SIM-A First” or “SIM-B First” scenario, the gateway will try to connect to the Internet by using SIM-A or SIM-B card first. And when the connection is broken, the gateway will switch to use the other SIM card as an alternative automatically and **will not switch back** to use the original SIM card unless the current SIM connection is also broken.

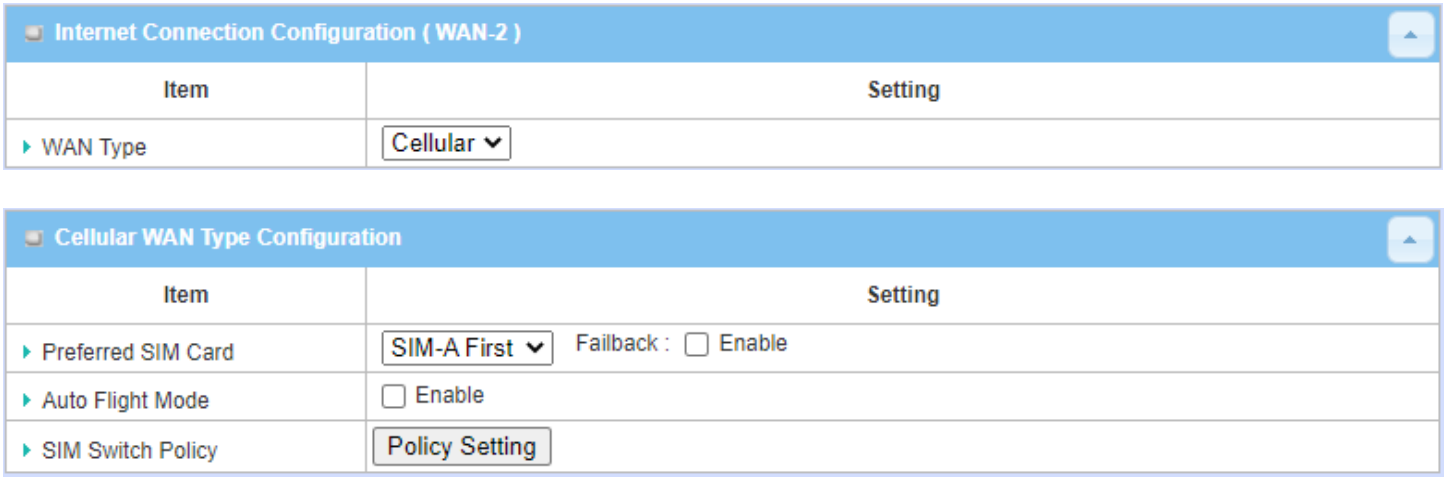


SIM-A / SIM-B first with Failback

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

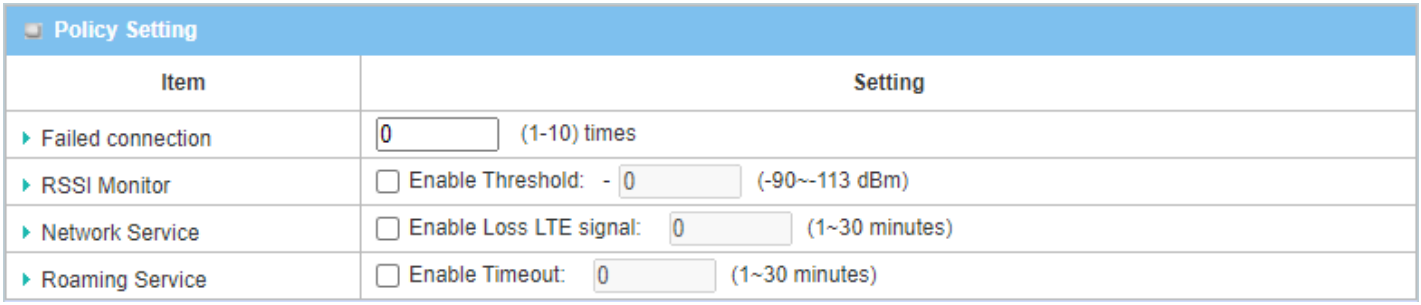
Configure Cellular WAN Type Setting

To configure cellular WAN setting, select the **Cellular** as the WAN Type for the designated WAN interface and click **Edit** to open the **Cellular WAN Type Configuration** screen.



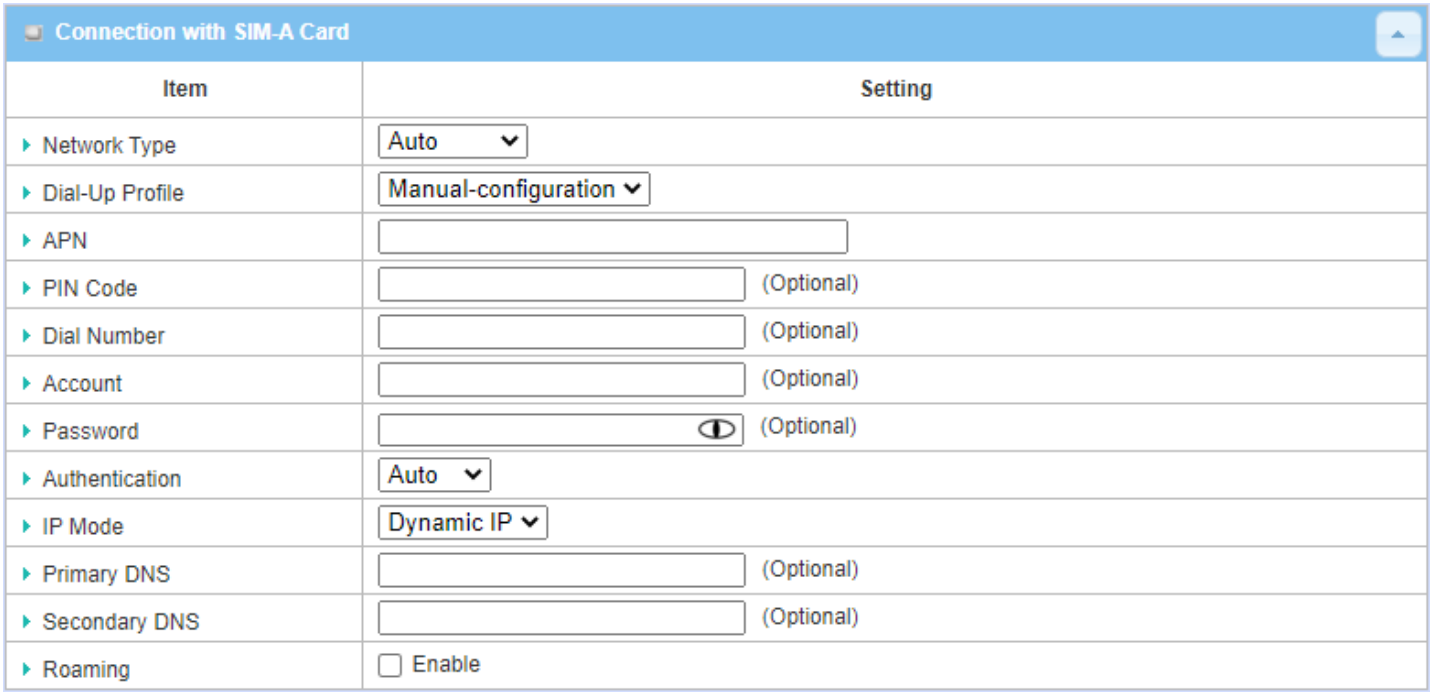
Cellular WAN Type Configuration Item	Value setting	Description
WAN Type	1. A must-filled setting 2. **Cellular** is set by default.	From the dropdown box, **Cellular** is selected as the Internet connection method for cellular WAN connection.
Preferred SIM Card	1. A must-filled setting 2. By default **SIM-A First** is selected 3. **Failback** is unchecked by default	Choose which SIM card you want to use for connection. When **SIM-A First** or **SIM-B First** is selected, it means that the connection is built first by using the specified SIM A/SIM B. And if the connection fails, the gateway will use the other SIM card for connection establishment. When **SIM-A only** or **SIM-B only** is selected, the gateway will try to dial up only using the SIM card you selected. When Failback is checked, the gateway will switch back to the preferred SIM for connection establishment after the failover operation. **Note:** For models with single SIM design, only the **SIM-A Only** option is available. **Note: Failback** is available only when SIM-A First or SIM-B First is selected.
Auto Flight Mode	The box is unchecked by default	Check the Enable box to activate the function. By default, if you disable the Auto Flight Mode, the cellular module will always occupy a physical channel. It can establish data connection instantly and enable SMS all the time as needed. If you enable the **Auto Flight Mode**, the following message will pop up, “Flight mode will cause cellular function to be malfunctioned when the data session is offline.”, and it will disconnect the cellular connection entirely. In, addition, whenever the cellular module is used for failover as the backup for the failed primary connection, the cellular module will take few more seconds to connect with the cellular tower.

		Note: Keep it unchecked unless your mobile carrier requires the Auto Flight Mode being enabled.
SIM Switch Policy	NA	Click the **Policy Setting** button to define the SIM failover condition or select a pre-configured policy.



Policy Setting Item	Value setting	Description
Failed connection	0 is set by default.	Enter the maximum number of failed connections that can be allowed before changing to another cellular connection.
RSSI Monitor	The box is unchecked by default.	Received Signal Strength Indication, which measures the power of a received radio signal. Enter the acceptable RSSI Threshold value to keep the current connection.
Network Service	The box is unchecked by default.	Enter the number of minutes (1-30) that can be tolerated for losing LTE signal.
Roaming Service	The box is unchecked by default.	Enter the maximum timeout value in minutes (1-30) for mobile roaming service.

Configure SIM-A / SIM-B Card



Note: Configurations of SIM-B Card follows the same rule as the Configurations of SIM-A Card; we use SIM-A as an example here.

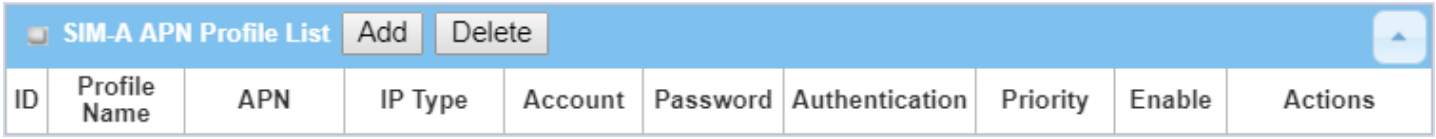
Note: The **Connection with SIM-A Card** and/or **Connection with SIM-B Card** will appear depending on the selection of the **Preferred SIM Card** field.

Connection with SIM-A/-B Card		
Item	**Value setting**	**Description**
Network Type	1. A must-filled setting 2. By default, **Auto** is selected	Select **Auto** to register a network automatically, regardless of the network type. Select **5G SA** to register the 5G network. Select **LTE only** to register the 4G network only. **Note**: Options may be different depending on the specification of the module.
Dial-Up Profile	1. A must-filled setting 2. By default **Manual-configuration** is selected	Specify the type of dial-up profile for your cellular network. It can be **Manual-configuration**, **APN Profile List**, or **Auto-detection**. Select **Manual-configuration** and set APN (Access Point Name), **Dial Number, Account,** and **Password** that your carrier provides. Select **APN Profile List** to set more than one profile for dial-up, which will be used for making connection attempts in turn until a connection is established. Go to Basic **Network > WAN & Uplink > Connection Setup > SIM-A APN Profile List** for details. Select **Auto-detection** to configure the required information automatically for dial-up. **Note:** It is highly recommended to select Manual or APN Profile List to specify the connection settings of your subscription. Your ISP will provide such information. For Auto-detection, check the mobile network the gateway connects to is valid.
APN	1. A must-filled setting 2. String format : any text	Enter the **Access Point Name (APN)** provided by your ISP to connect to the mobile network. This is a must-filled setting if you selected **Manual-configuration** as the dial-up profile scheme.
IP Type	1. A must-filled setting 2. By default **IPv4** is selected	Specify the IP type of the network provided by your ISP. It can be **IPv4**, **IPv6**, or **IPv4/6**.
PIN code	1. An optional setting 2. String format : interger	Enter the Personal Identification Number (PIN) code to unlock your SIM card.
Dial Number, Account, Password	1. An optional setting 2. String format : any text	Enter the optional **Dial Number**, **Account**, and **Password** settings if your carrier provids these settings. **Note:** These settings are only available when Manual-configuration is selected.
Authentication	1. A must-filled setting 2. By default, **Auto** is selected	Select **Password Authentication Protocol (PAP)** to authenticate with the carrier's server. Select **Challenge Handshake Authentication Protocol (CHAP)** to authenticate with the carrier's server. Select **Auto** to authenticate with the carrier's server using either PAP or CHAP.
IP Mode	1. A must-filled setting 2. By default **Dynamic IP** is selected	When **Dynamic IP** is selected, all IP configurations can be obtained from the carrier's server and set to the device directly. Select **Static IP** mode and fill in all the parameters required, such as IP address, subnet mask, and gateway.

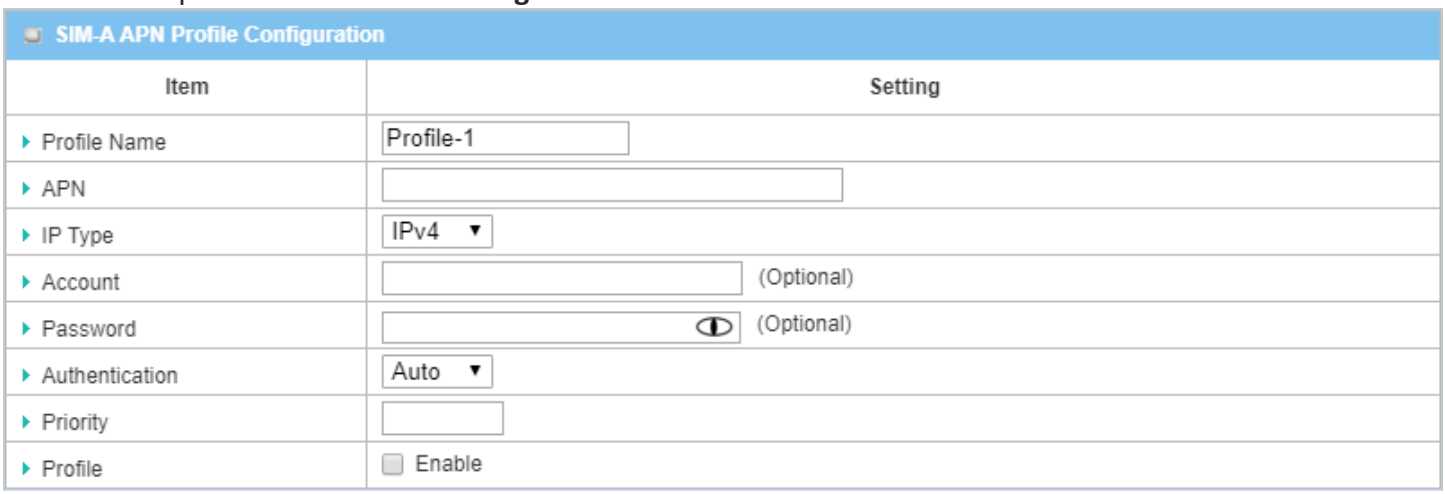
		Note: **IP Subnet Mask** is a must-filled setting. Please make sure to set up the configuration correctly to avoid any issues.
Primary DNS	1. An optional setting 2. String format : IP address (IPv4 type)	Enter the IP address of the primary DNS (Domain Name Server) setting or it will be automatically assigned by your carrier during a dial-up.
Secondary DNS	1. An optional setting 2. String format : IP address (IPv4 type)	Enter the IP address of the secondary DNS (Domain Name Server) setting or it will be automatically assigned by your carrier during a dial-up.
Roaming	The box is unchecked by default	Check the box to establish a connection through roaming. **Note**: Additional charges may incur.

Create SIM-A / SIM-B APN Profile List

You can add a new APN profile for the connection. The list of APN profiles will be displayed only when you select **APN Profile List** as the **Dial-Up Profile**.



Click **Add** to open the **APN Profile Configuration** screen.

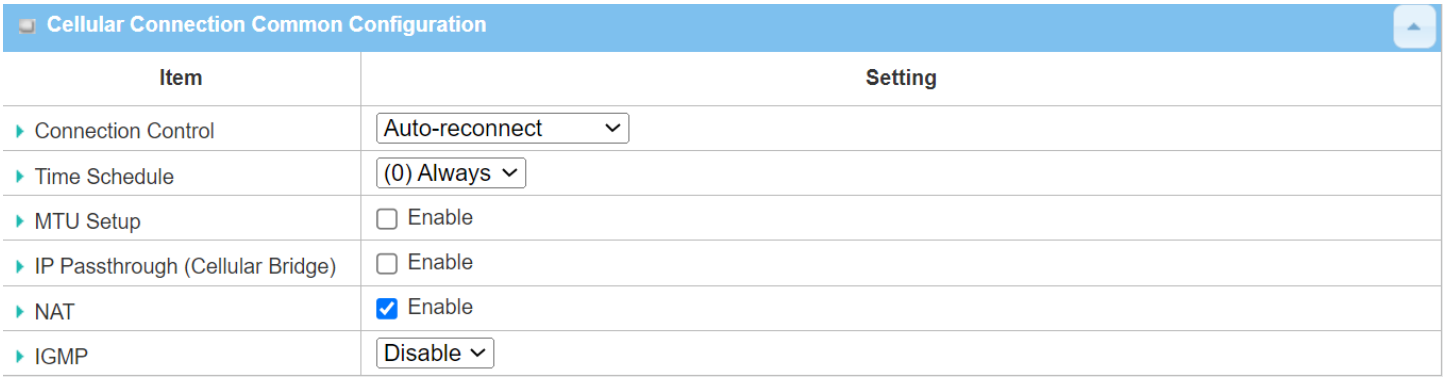


SIM-A/-B APN Profile Configuration **Item**	**Value setting**	**Description**
Profile Name	1. By default **Profile-No.** is listed 2. String format : any text	Enter a profile name.
APN	String format : any text	Enter the **Access Point Name (APN)** provided by your ISP to connect to the mobile network.
IP Type	1. A must-filled setting 2. By default **IPv4** is selected	Specify the IP type of the network service used by your cellular carrier: **IPv4**, **IPv6**, or **IPv4/6**.
Account	String format : any text	Enter the **Account** for authentication. *Value Range*: 0 ~ 53 characters.
Password	String format : any text	Enter the **Password** for authentication.
Authentication	1. A must-filled setting 2. By default, **Auto** is selected	Select the Authentication method: **Auto**, **PAP**, **CHAP**, or **None**.
Priority	1. A must-filled setting	Enter a value (from 1-16) for the dial-up process where a dial-up will start

	2. String format: integer	from a profile of the smallest number. *Value Range*: 1 ~ 16.
Profile	The box is checked by default	Check the box to enable this profile.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **X** button to revert to the previous settings.

Configure Cellular Connection Common Configuration

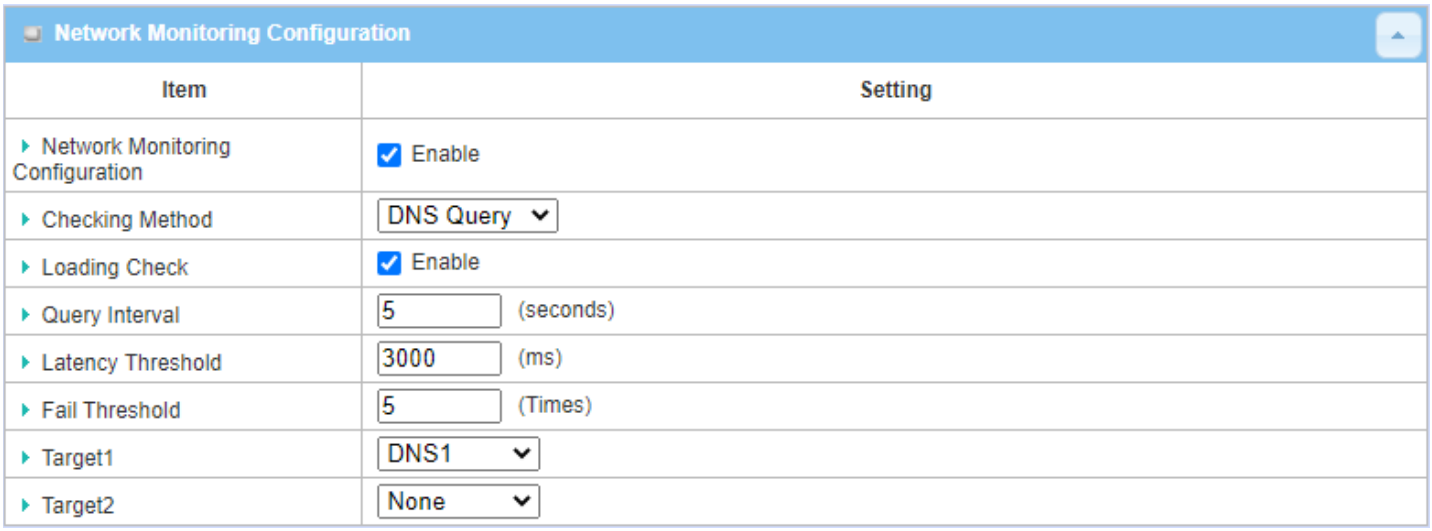
Here you can change common configurations for cellular WAN.



Cellular Connection Common Configuration		
Item	**Value setting**	**Description**
Connection Control	By default **Auto-reconnect** is selected	When **Auto-reconnect** is selected, the gateway will try to keep the Internet connection on all the time whenever the physical link is connected. When **Connect-on-demand** is selected, the Internet connection will be established only when data traffic is present. When **Connect Manually** is selected, you need to click the Connect button to dial up the connection manually. Please go to **Status > Basic Network > WAN & Uplink** tab and perform Connect or Disconnet under the Action column. **Note:** 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".
Maximum Idle Time	1. An optional setting 2. By default **600** seconds is filled-in	Specify the maximum Idle time setting to disconnect the internet connection when the connection has not been used for the specified value. *Value Range*: 300 ~ 86400. **Note:** This field is available only when **Connect-on-demand** or **Connect Manually** is selected as the connection control scheme.
Time Schedule	1. A must-filled setting 2. By default **(0) Always** is selected	Select **(0) Always** is selected to use this WAN configuration all the time. Or select a pre-configured schedule. Please go to **Object Definition > Scheduling** to configure schedules.
MTU Setup	1. An optional setting 2. **Uncheck** by default	Check the Enable box to enable the MTU (Maximum Transmission Unit) limit, and specify the largest packet size permitted for cellular connection. *Value Range:* 1200 ~ 1500.
IP Pass-through (Cellular Bridge)	1. The box is unchecked by default	Enable this function to assign a WAN IP to the first connected local LAN client.

	2. String format for **Fixed MAC**: MAC address, e.g. 00:50:18:aa:bb:cc	Note: When the IP Pass-through is enabled, NAT will be unavailable.
NAT	**Check** by default	Uncheck the box to disable **NAT** (Network Address Translation) function.
IGMP	By default **Disable** is selected	Enable or disable **IGMP Proxy**. The gateway uses the interface information gathered by IGMP to conserve bandwidth consumption in a multi-access network environment to avoid flooding multicast traffic in the network.

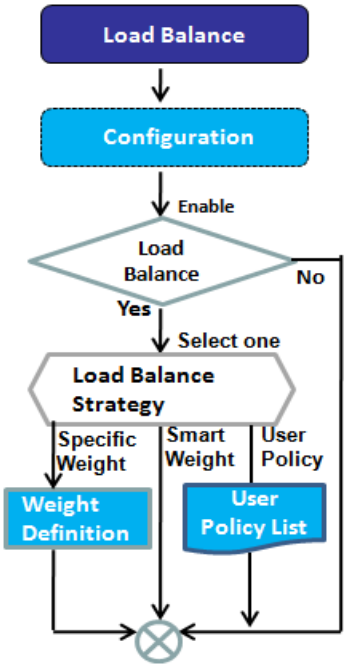
Configure Network Monitoring



Network Monitoring Configuration		
Item	**Value setting**	**Description**
Network Monitoring Configuration	1. An optional setting 2. Box is checked by default	Check the **Enable** box to activate the network monitoring function.
Checking Method	1. An optional setting 2. **DNS Query** is set by default	Choose either **DNS Query** or **ICMP Checking** to check if the WAN link is connected properly. With **DNS Query**, the system checks the connection using DNS query sent to the destination specified in Target 1 and Target 2. With **ICMP Checking**, the system checks connection using ICMP request sent to the destination specified in Target 1 and Target 2.
Loading Check	1. An optional setting 2. Box is checked by default	Check the **Enable** 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.
Query Interval	1. An optional setting 2. **5 seconds** is selected by default.	Specify a time interval for the **DNS Query**. You can specify a **Query Interval** to define the transmitting interval between two DNS Query or ICMP checking packets. With **DNS Query,** the system checks the connection by sending DNS query packets to the destination specified in **Target 1** and **Target 2**. *Value Range*: 2 ~ 14400.
Check Interval	1. An optional setting 2. **5 seconds** is selected by default.	Specify a time interval for the **ICMP Checking**. You can specify an ICMP Checking interval to define the transmitting interval between two DNS Query or ICMP checking packets. With **ICMP Checking,** the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2.

		Value Range: 2 ~ 14400.
Latency Threshold	1. An optional setting 2. **3000 ms** is set by default	Specify a number as the threshold latency for disconnection detection before disconnection is acknowledged. **Latency Threshold** defines the timeout threshold of responding time. *Value Range*: 2000 ~ 3000 seconds.
Fail Threshold	1. An optional setting 2. **5 times** is set by default	Specify a number as the threshold time for disconnection detection before disconnection is acknowledged. Fail Threshold specifies the number of detected disconnection checks before the WAN link down status is acknowledged. *Value Range*: 1 ~ 10 times.
Target 1	1. An optional setting 2. **DNS1** is selected by defaultAn optional setting	**Target1** specifies the first target of sending a DNS query/ICMP request. **DNS1**: the primary DNS is set as the target. **DNS2**: the secondary DNS is set as the target. **Other Host**: enter an IP address to be the target.
Target 2	1. An optional setting 2. **None** is selected by defaultAn optional setting	**Target2** specifies the second target of sending a DNS query/ICMP request. **None:** no second target is required. **DNS1**: the primary DNS is set as the target. **DNS2**: the secondary DNS is set as the target. **Other Host**: enter an IP address to be the target.
Save	*N/A*	Save the settings.
Undo	*N/A*	Discard the settings.

2.1.3 Load Balance

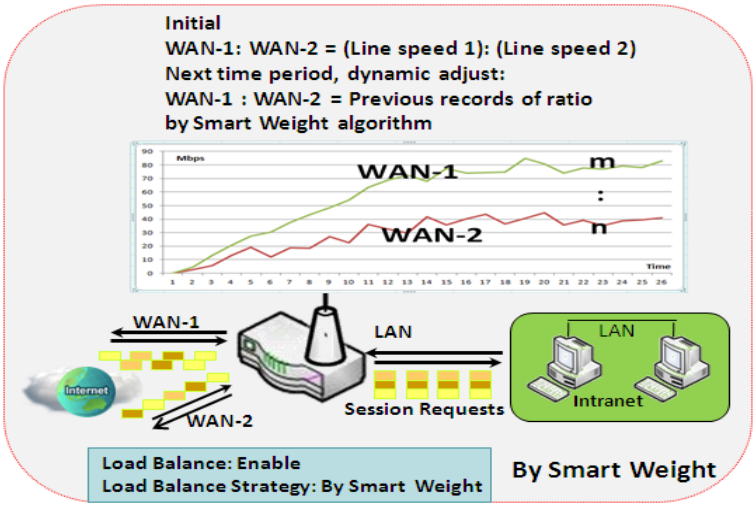




When there are multiple WAN interfaces, the dual-WAN function can be used to increase the total WAN bandwidth and distribute the WAN traffic optimally.

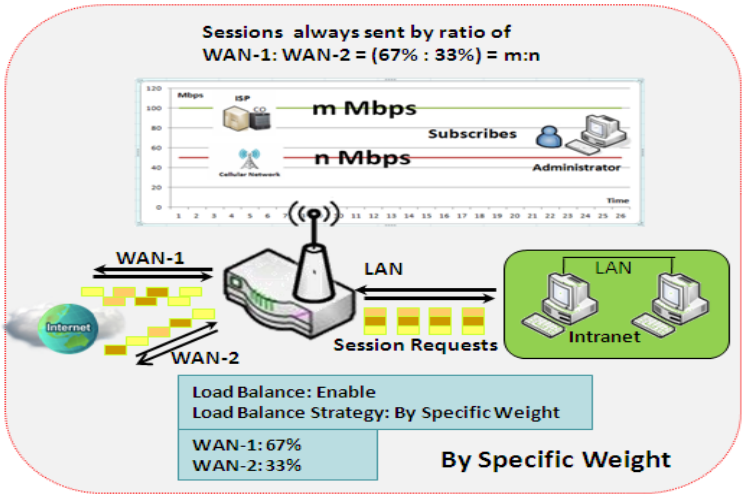
Load Balance Strategy

There are three different strategies for load balance: ***"By Smart Weight"***, "***By Specific Weight"***, and "***By User Policy"***. You can select the bandwidth allocation strategy according to the application requirements and the network environment.



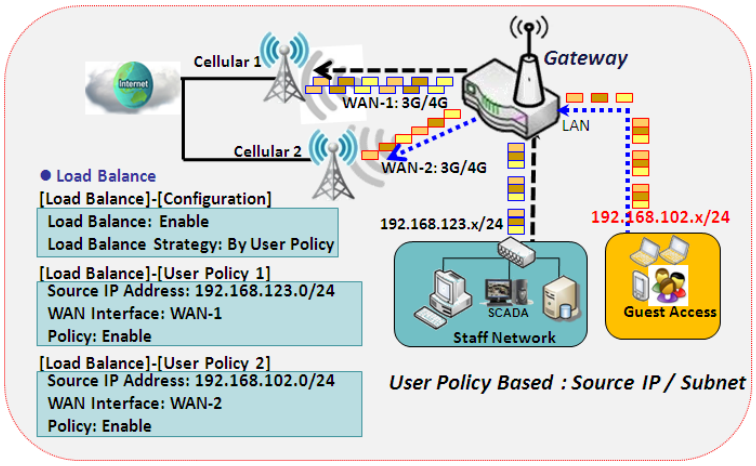
By Smart Weight

In the "By Smart Weight" strategy, the ratio for traffic transmission among these WAN interfaces in the previous time slot (5-minutes period) will be used to allot the transmission ratio for the next time slot dynamically. The default transmission ratio is based on the line speed configured on the WAN interfaces.



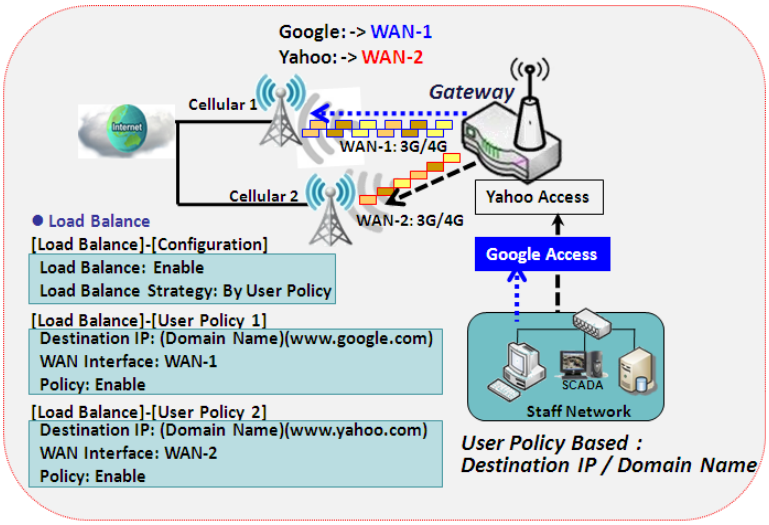
By Specific Weight

When you select "By Specific Weight", you need to set up ratio of WAN-1/WAN-2 to decide the exact ratio for session transmission. Ratio is usually defined based on the WAN speed of the network environment.



By User Policy

The "By User Policy" strategy allows you to route traffic using criteria such as the IP addresses and ports of the source and destination network. The IP address can be a single IP, a subnet or an IP range. The ports can be a single port or a port range.



Diagrams shown on left side are illustrated as examples for setting user policy. The first diagram illustrates the mapping from various source IP subnets to different WAN interfaces. Packets from different subnets will be routed to the assigned WAN interfece. You can manage and balance the traffic load among available WAN interfaces accordingly.

The second diagram illustrates how packets with designated destination IP or domain name are routed to a certain WAN interface.

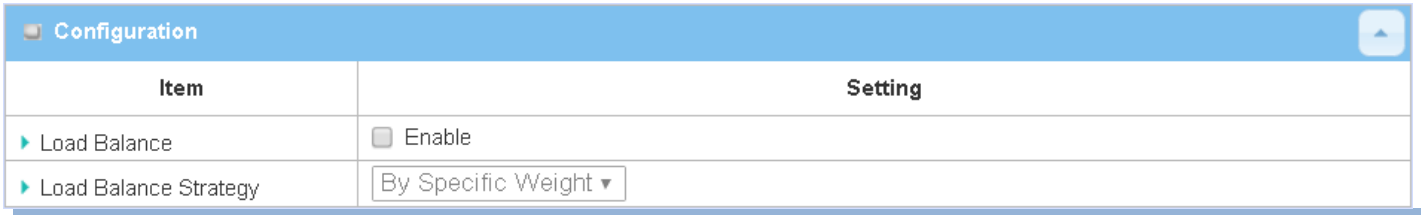
If traffic does not map to any user policy, the gateway will apply the smart weight strategy to route the traffic.

Load Balance Setting

The **Load Balance** function is used to manage bandwidth among multiple WAN connections to achieve the optimized balance of usage. When you choose "By Smart Weight" strategy, the system will operate load balance automatically according to the embedded Smart Weight algorithm. However, when you choose "By Specific Weight" strategy, you will need to define the data transfer ratio for all WAN interfaces. And when you choose "By User Policy" strategy, you can create and define transfer policies for dedicated traffic flows.

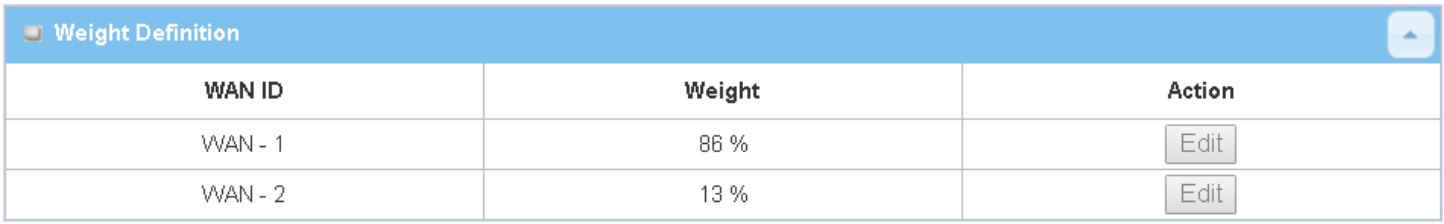
Go to **Basic Network > WAN & Uplink > Load Balance.**

Enable Load Balance



Configuration		
Item	**Value setting**	**Description**
Load Balance	Unchecked by default	Check the **Enable** box to activate Load Balance function.
Load Balance Strategy	1. A must-filled setting 2. **By Smart Weight** is selected by default.	Select the preferred load-balancing strategy: **By Smart Weight**: the gateway will automatically perform load balance according to the embedded Smart Weight algorithm. **By Specific Weight**: the gateway will adjust the bandwidth ratio of transferred sessions among all WAN interfaces according to the specified weights for each interface. **By User Policy**: the gateway will route traffic through available WAN interfaces according to user-defined rules. **Note:** The number of available strategies depends on the model.
Save	NA	Save the configuration
Undo	NA	Restore to the previous settings.

When **By Specific Weight** is selected, you can adjust the loading of the WAN interfaces by assigning weights. A value based on the bandwidth ratio of each WAN will be assigned as the default.



Weight Definition		
Item	**Value setting**	**Description**

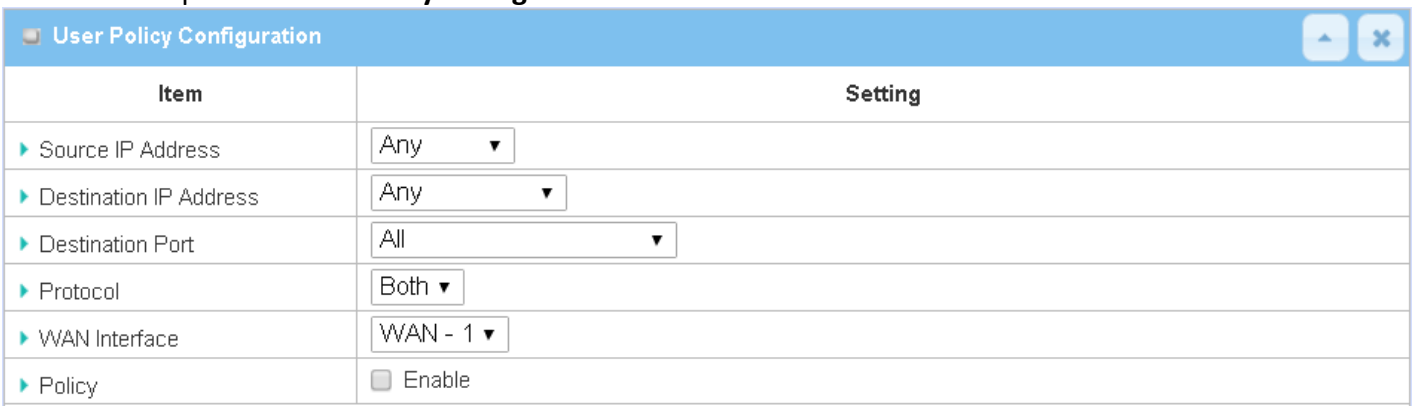
WAN ID	N/A	The Identifier for each available WAN interface.
Weight	1. A must-filled setting 2. A default value is assigned to each WAN.	Enter a weight for each WAN interface by clicking **Edit**. *Value Range*: 1 ~ 99. **Note:** The sum of all weights can't be greater than 100%.
Save	N/A	Save the configuration
Undo	N/A	Restore to the previous settings.

If **By User Policy** is selected for load-balancing strategy, the **User Policy List** screen will appear.

Create User Policy



Click **Add** to open the **User Policy Configuration** screen.



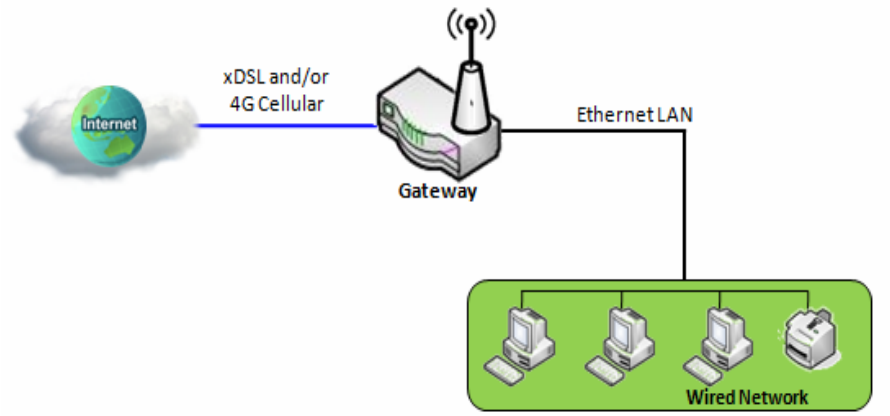
User Policy Configuration **Item**	**Value setting**	**Description**
Source IP Address	1. A must-filled setting 2. **Any** is selected by default.	There are four options for Source IP Address: **Any**: Select this option for traffic that comes from any source. **Subnet**: Specify the subnetwork of the source address. Input format: IP network address/subnet length (e.g. 192.168.123.0/24). **IP Range**: Specify the IP range of the source. **Single IP**: Specify the IP address of the source traffic.
Destination IP Address	1. A must-filled setting 2. **Any** is selected by default.	Select one of the options of Destination IP Address: **Any**: Select this option for traffic that is destined for any address. **Subnet**: Specify the subnetwork of the destination address. Input format: IP network address/subnet length (e.g. 192.168.123.0/24). traffic. **IP Range**: Specify the IP Range of the destination. **Single IP**: Specify the IP address of the destination.traffic **Domain Name**: Specify the domain name of the destination.
Destination Port	1. A must-filled setting 2. **All** is selected by default.	Select one of the options of Destination Port: **All**: Any port number for the destination ports. **Port Range**: Specify a port range of destination ports. **Single Port**: Specify a unique destination port. **Well-known Applications**: Select the service port of a well-known application defined in the dropdown list.
Protocol	1. A must-filled setting	There are three options: **Both**, **TCP**, and **UDP**.

	2. **Both** is selected by default.	
WAN Interface	1. A must-filled setting 2. **WAN-1** is selected by default.	Select an interface for the traffic to pass through. Note that the WAN interface dropdown list will only show the available WAN interfaces.
Policy	Unchecked by default	Check the **Enable** checkbox to activate the policy rule.
Save	NA	Save the configuration.
Undo	NA	Restore to the previous settings.

2.2 LAN & VLAN

This section provides the configuration of LAN and VLAN. VLAN is an optional feature, depending on the model.

2.2.1 Ethernet LAN



The Local Area Network (LAN) can be used to share data or files among computers connected to the LAN. The left diagram illustrates the network that interconnects computers in the LAN.

Configure the IPv4 Ethernet LAN



Configuration Item	Value setting	Description
IP Mode	NA	It shows the LAN IP mode of the gateway. **Static IP**: The LAN IP mode is fixed at Static IP when one WAN interface is enabled. **Dynamic IP**: The LAN IP mode becomes Dynamic IP when all available WAN interfaces are disabled.
LAN IP Address	1. A must-filled setting **2. 192.168.0.1 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. **Note**: Once you have changed the gateway's default IP address, you have to use the new IP address to access the Web UI as well.
Subnet Mask	1. A must-filled setting 2. **255.255.255.0 (/24)** is set by default	Select the subnet mask for this gateway from the dropdown list. A subnet mask defines the number of hosts of the subnetwork. The gateway's default subnet mask is 255.255.255.0 (/24), which indicates the subnet contains up to 254 IP addresses, including 253 IP addresses available for client connection (one is used by the gateway itself). *Value Range*: 255.0.0.0 (/8) ~ 255.255.255.252 (/30).
Save	NA	Save the configuration

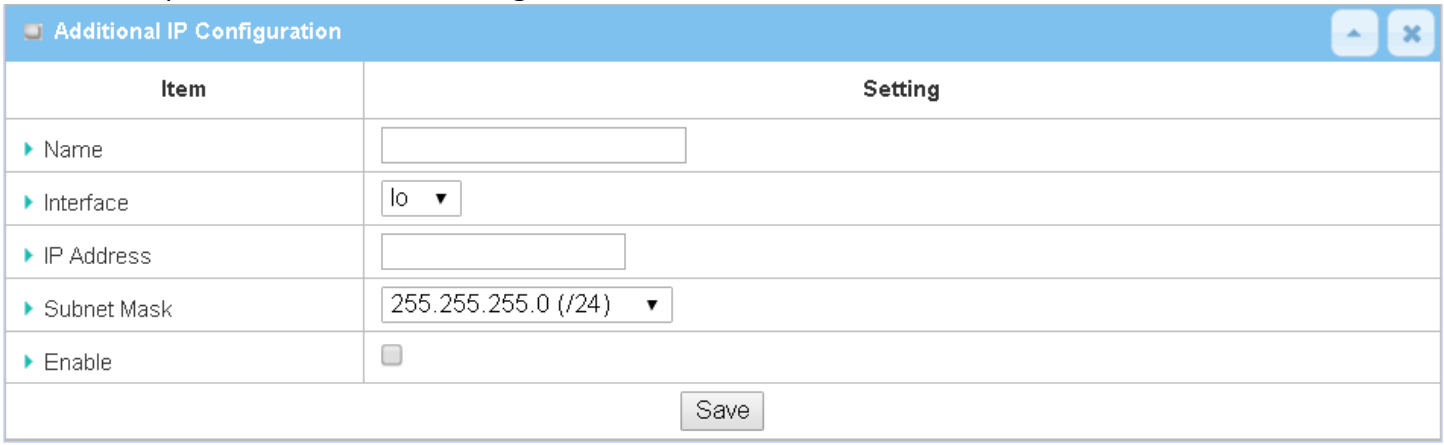
Undo	NA	Restore back to the previous settings.

Create / Edit Additional IP

The LAN IP alias function can be used to add an additional LAN IP to access this gateway.



Clik **Add** to open the **Addtional IP Configuration** screen.



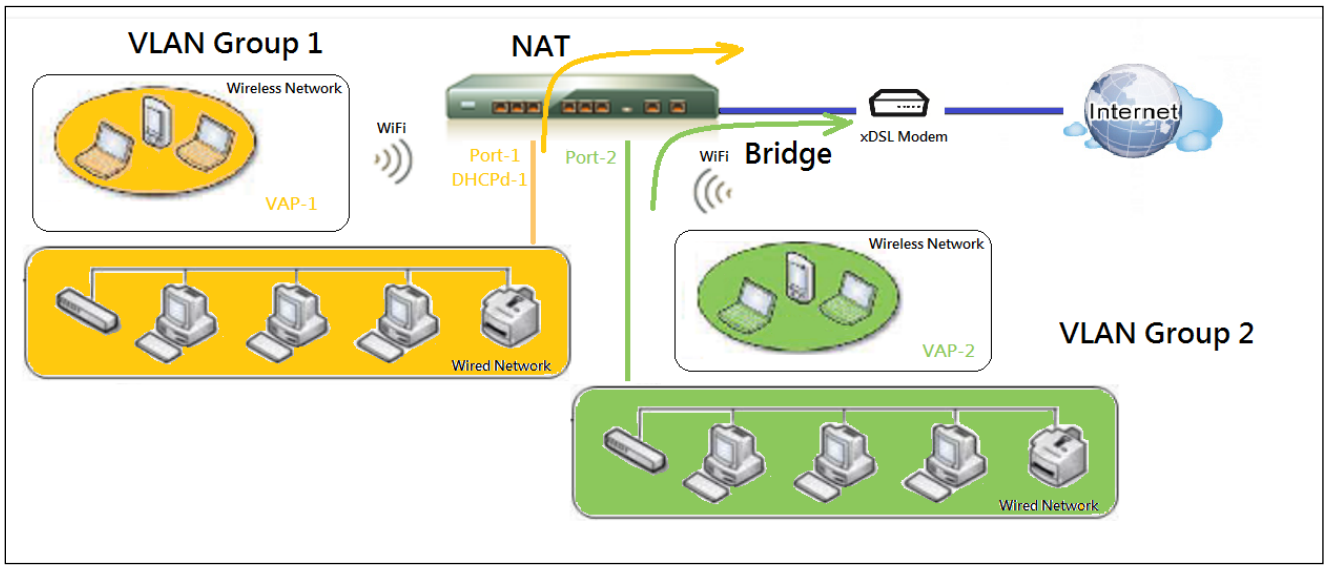
Configuration Item	Value setting	Description
Name	1 An optional setting	Enter a name for the alias IP address.
Interface	1. A must-filled setting 2. **lo** is set by default	Specify the Interface type : **lo** or **br0**.
IP Address	1. An optional setting **2. 192.168.0.1 is the default IP address of this gateway**	Enter an IP address that is different from the above set LAN IP Address for this additional IP configuration.
Subnet Mask	1. A must-filled setting 2. **255.255.255.0 (/24)** is set by default	Select the subnet mask for this gateway from the dropdown list. A subnet mask defines the number of hosts of the subnetwork. The default subnet mask is 255.255.255.0 (/24). *Value Range*: 255.0.0.0 (/8) ~ 255.255.255.252 (/30).
Save	NA	Save the configuration

2.2.2 VLAN

Virtual LAN (VLAN) is a logical network that can be used to group client hosts with a specific VLAN ID. This gateway supports both Port-based VLAN and Tag-based VLAN. These functions allow you to divide a local network into different “virtual LANs”. It is a common feature that makes it easy for you to subdivide a single network with multiple groups that have distinct resource and access requirments. You can divide the local network using either port-based VLAN or tag-based VLAN, and hosts in each VLAN share common access privilege and QoS property. VLAN tagging can also be used for connecting with an ISP for certain kinds of services (e.g. IPTV). You can group all devices requiring this service with one tagged VLAN.

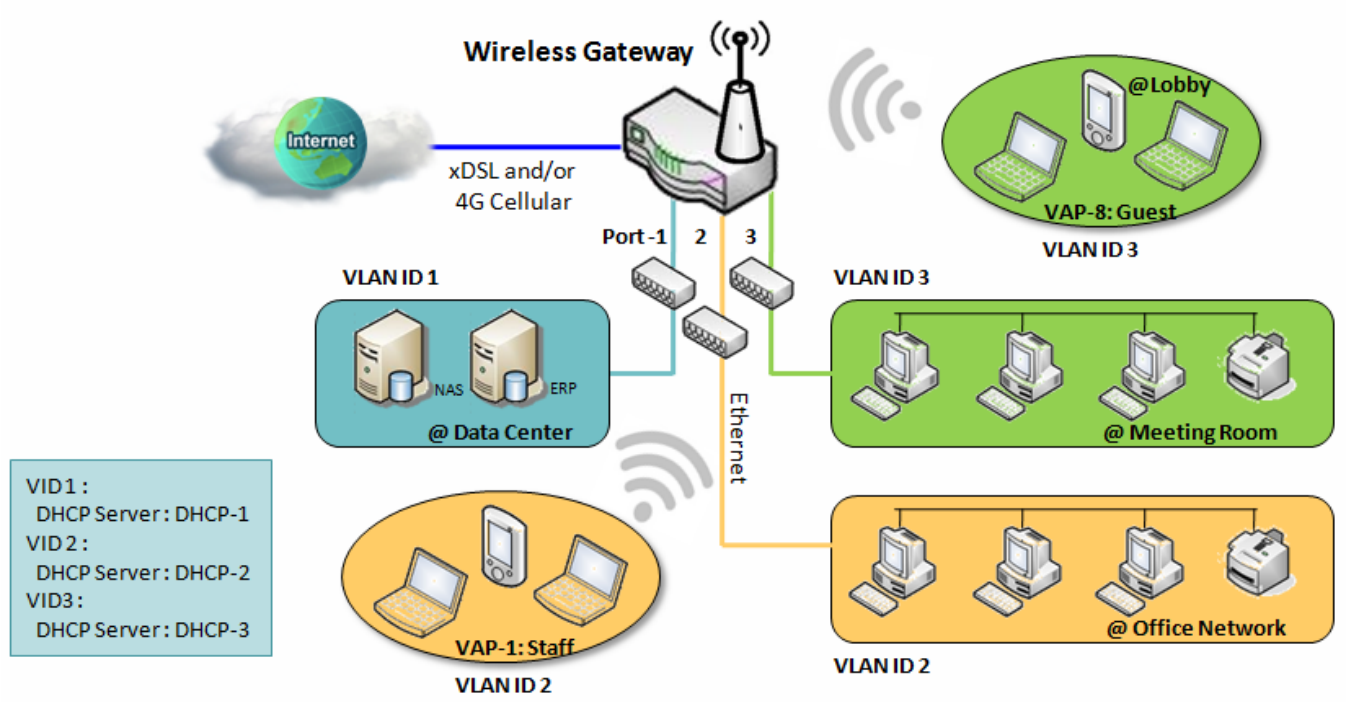
➢ Port-based VLAN

Port-based VLAN function enables grouping of Ethernet ports, such as Port-1 ~ Port-4, and Wi-Fi Virtual Access Points, such as VAP-1 ~ VAP-8, 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. And a DHCP server can be utilized for a NAT VLAN group to administer DHCP assignmentlet to hosts of the group. On the other hand, in bridge mode, LAN traffic is routed through the WAN trunk port with a VLAN tag to another network for different services.



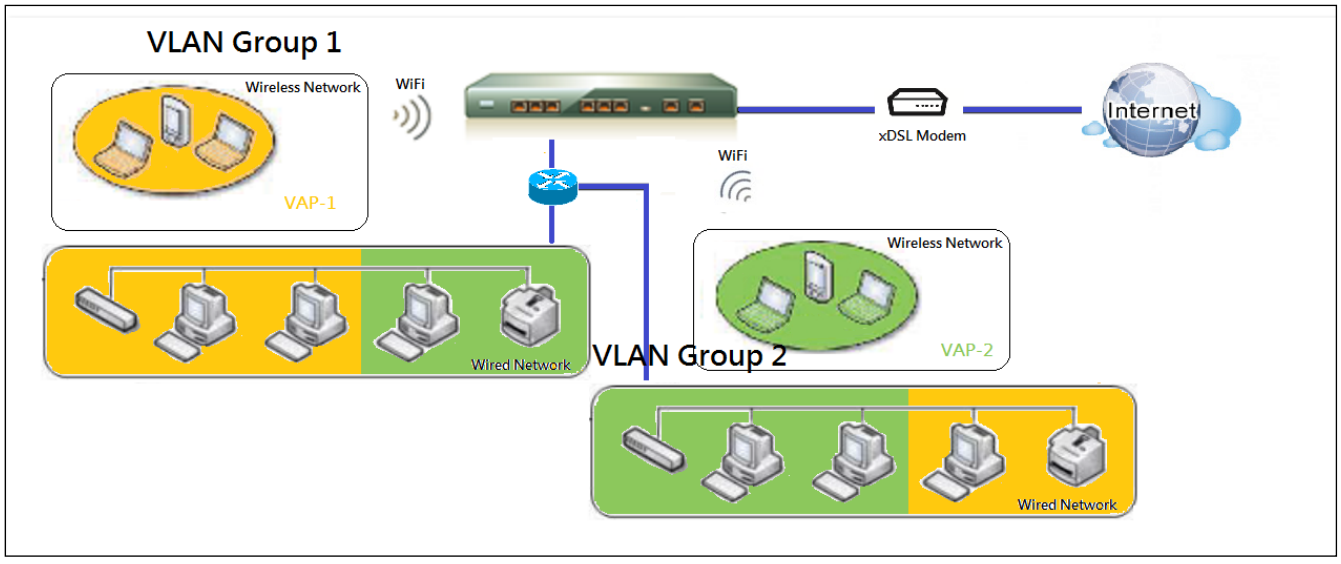
A port-based VLAN is a group of ports on a gateway that forms a logical LAN segment.

The below example illustrates 3 network segments constructed: Lobby/Meeting Room, Office, and Data Center. You can configure Lobby/Meeting Room segment with VLAN ID 3. The VLAN group 3 includes Port-3 and VAP-8 (SSID: Guest) of the gateway in NAT mode. The Office segment can be assigned with VLAN ID 2. The VLAN group 2 includes Port-2 and VAP-1 (SSID: Staff) of the gateway in NAT mode. The Data Center segment can be assigned with VLAN ID 1. The VLAN group 1 includes Port-1 in NAT mode as shown in the following diagram. Each VLAN group also has a dedicated DHCP server.

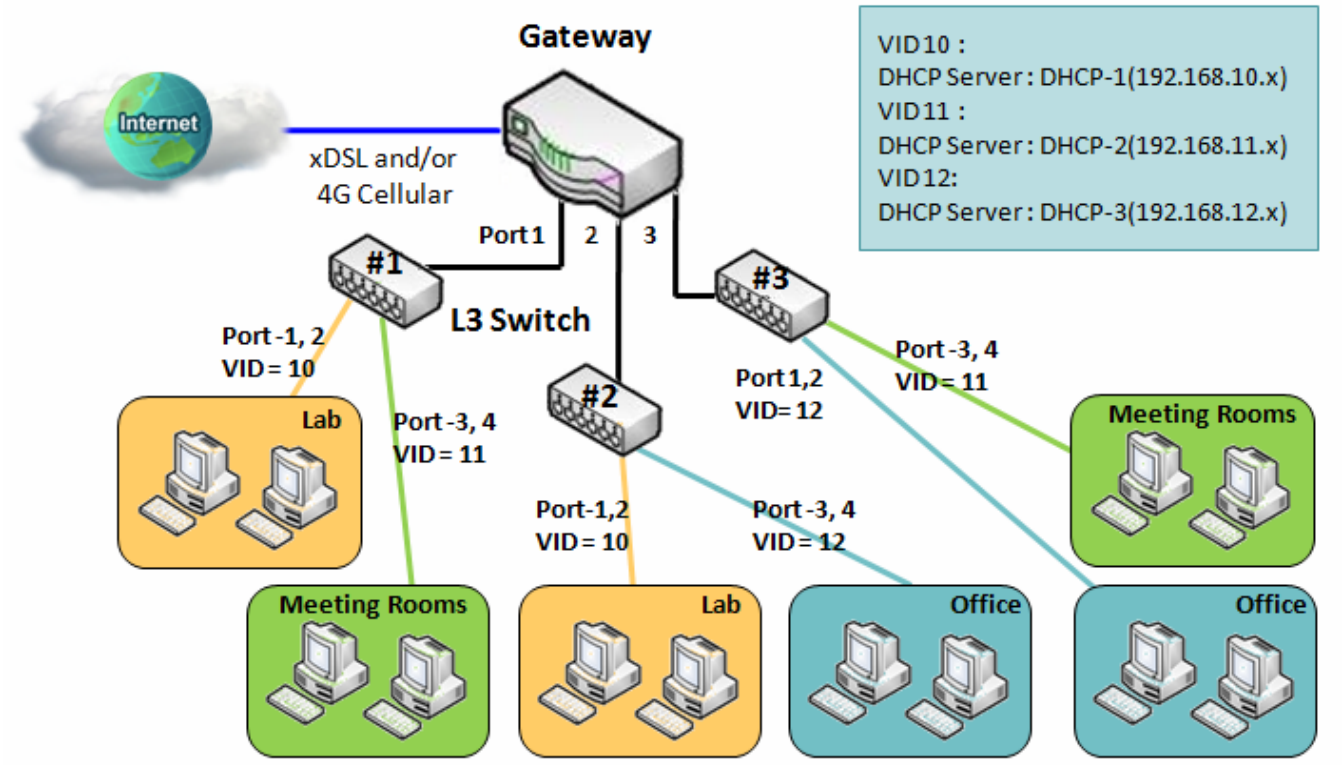


➢ Tagged VLAN

Tagged VLAN function allws you to group hosts from different geopgraphic locations to be on the same network. Traffic will be differentiated with VLAN tags and delivered through a VLAN trunk, which collects all traffic flows with different VLAN IDs from the gateway and delivers them in the LAN.



The above example illustrates 3 network segments: Lab, Meeting Rooms, and Office. In a VPN gateway, you can configure Office segment with VLAN ID 12 (the VLAN group is equipped with DHCP-3 server that assigns IP addresses with the 192.168.12.x subnet). You can also configure Meeting Rooms segment with VLAN ID 11 (the VLAN group is equipped with DHCP-2 that assigns IP addresses with the 192.168.11.x subnet). He can also configure Lab segment with VLAN ID 10 (the VLAN group is equipped with DHCP-1 server that assigns IP addresses with a 192.168.10.x subnet).

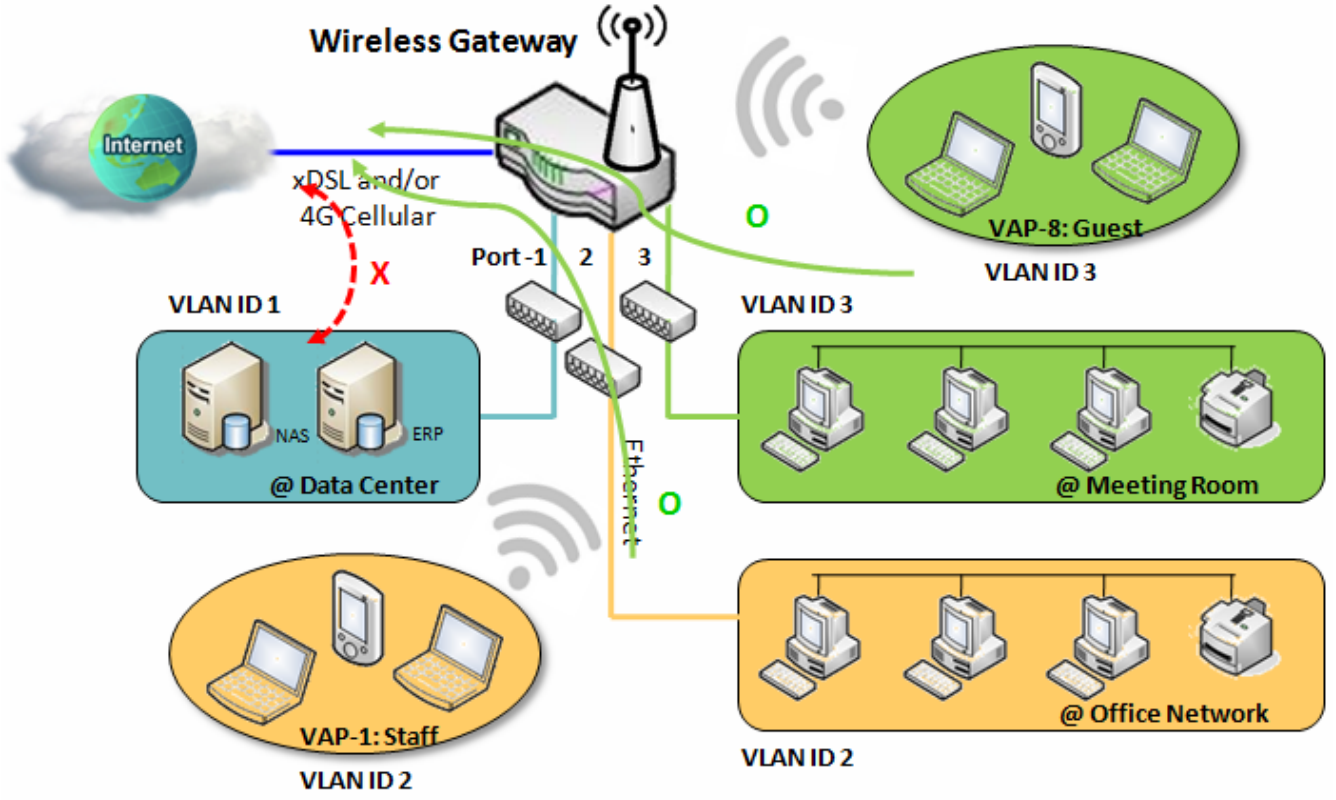

Gateway
Internet
xDSL and/or
4G Cellular
Port 1
2
3
#1
L3 Switch
#2
#3
VID 10 :
DHCP Server : DHCP-1(192.168.10.x)
VID 11 :
DHCP Server : DHCP-2(192.168.11.x)
VID 12:
DHCP Server : DHCP-3(192.168.12.x)
Port -1, 2
VID = 10
Lab
Port -3, 4
VID = 11
Meeting Rooms
Port-1,2
VID = 10
Lab
Port -3, 4
VID = 12
Office
Port 1,2
VID= 12
Port -3, 4
VID = 11
Meeting Rooms
Office

➢ VLAN Groups Access Control

You can specify the Internet access permission for all VLAN groups. You can also configure which VLAN groups are allowed to communicate with one another.

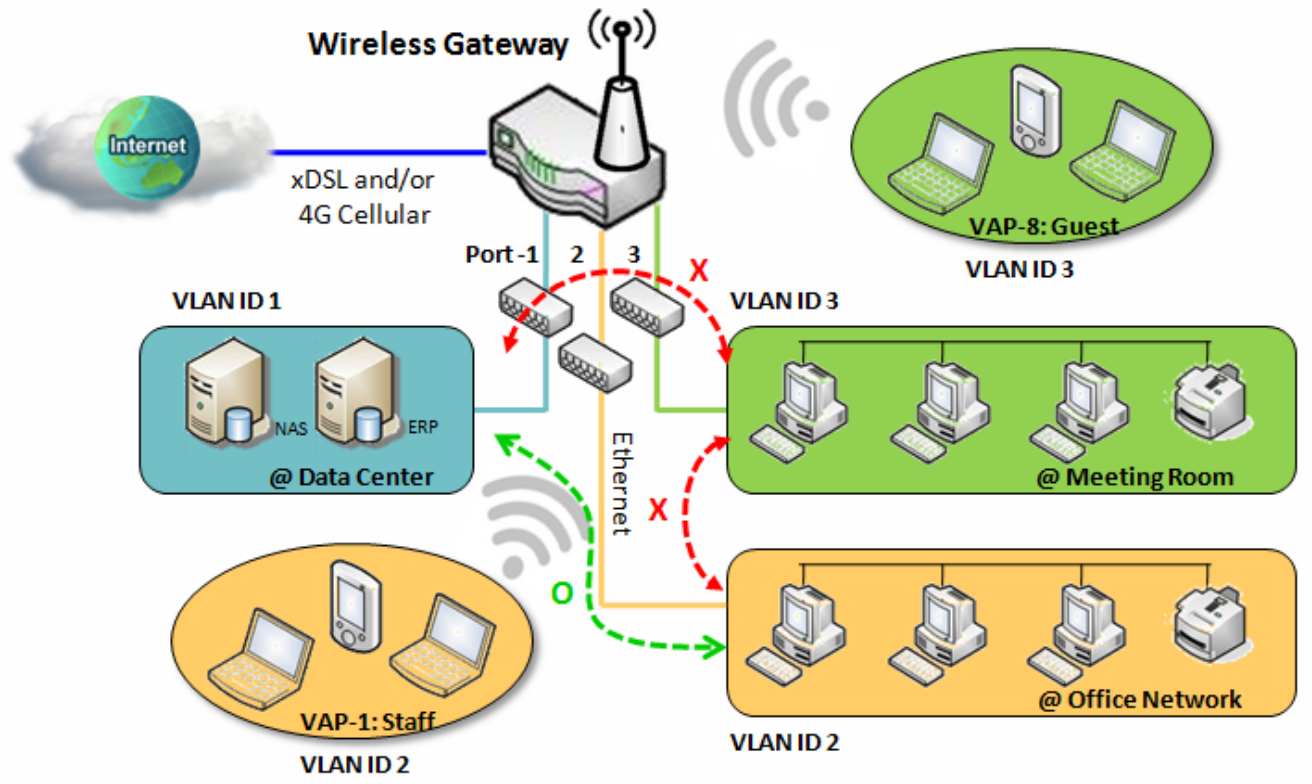
VLAN Group Internet Access

The following is an example that allows VLAN groups of VID 2 and 3 to access the Internet but not VLAN group of VID 1. In addition, servers in the data center can only be accessed by trusted staff via secure tunnels.



Inter-VLAN Group Routing:

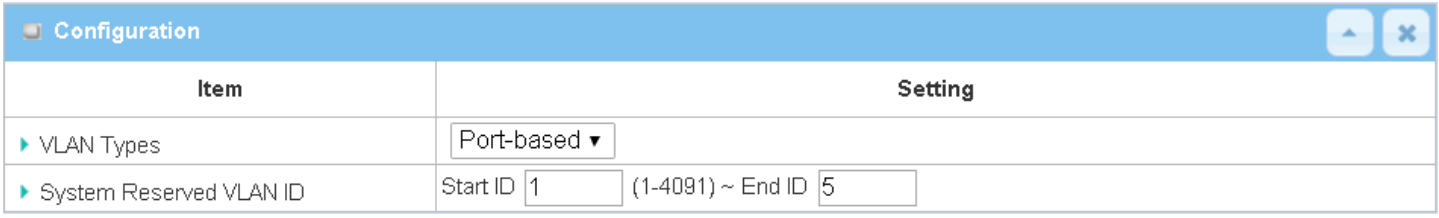
In Port-based VLAN, you can create communication pairs, which specify member hosts of one VLAN group to be able to communicate with members of another VLAN group. One VLAN group can join many communication pairs. But communication pair doesn't have the transitive property as shown in the following diagram: VLAN groups of VID 1 and 2 can communicate with each other but the groups of VID 1 and VID 3 or groups of VID 2 and VID 3 cannot communicate with each other.



VLAN Setting

To configure VLAN settings, go to Basic Network > LAN & VLAN > VLAN.

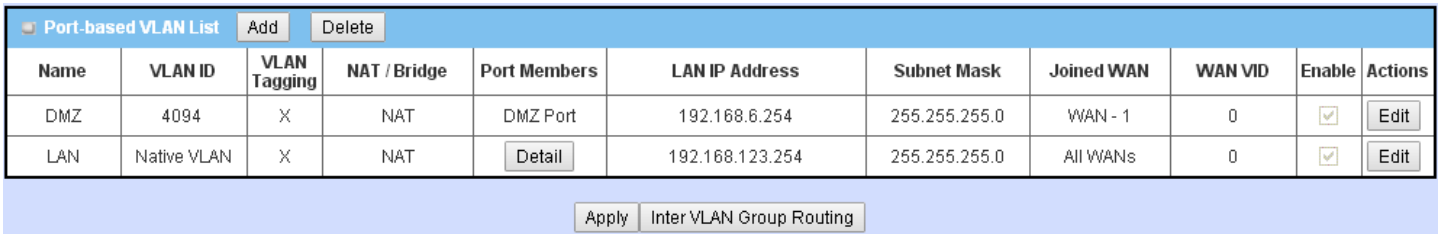
The VLAN function allows you to divide a local network into different virtual LANs. There are Port-based and Tagged VLAN types.



Configuration Item	Value setting	Description
VLAN Type	**Port-based** is selected by default	Select the VLAN type for your local subnets: **Port-based**: Port-based VLAN allows you to add rules for each LAN port. **Tag-based**: Tagged VLAN allows you to add VLAN ID and select member ports and DHCP Server for this VLAN ID.
System Reserved VLAN ID	**1 ~ 5** is reserved by default	Specify a range of VLAN ID to be reserved for system operation. For port-based/tag-based VLAN grouping, only use an ID outside the reserved range. *Value Range*: 1 ~ 4091.
Save	NA	Save the configuration

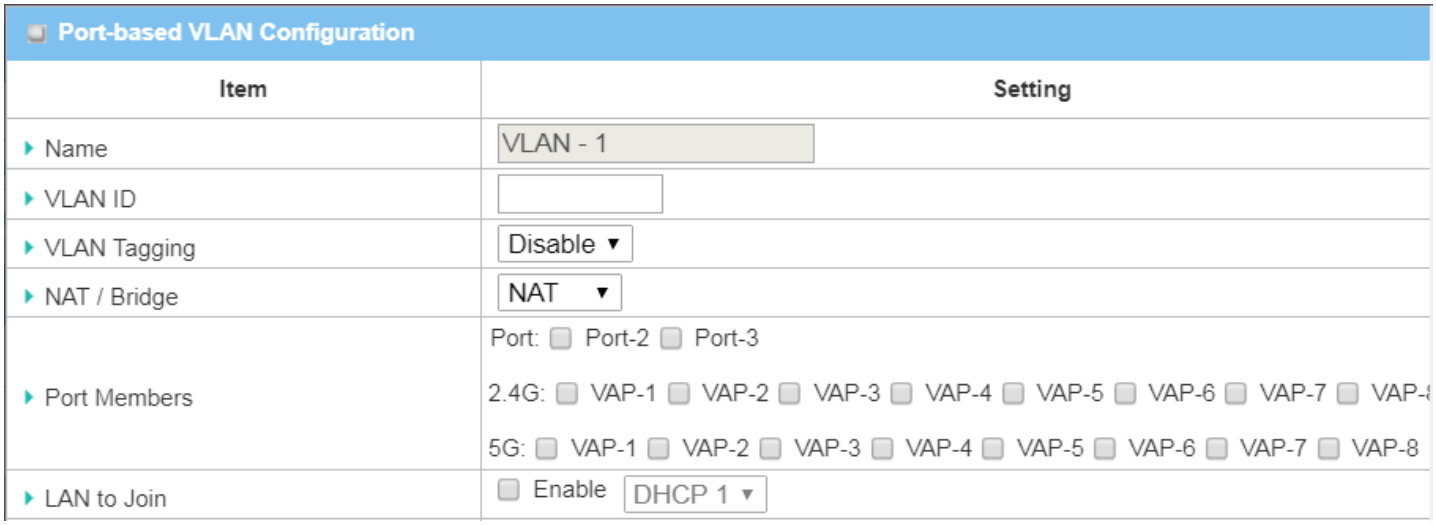
Port-based VLAN – Create/Edit VLAN Rules

The port-based VLAN allows you to customize each LAN port. A default rule shows the configuration of all the LAN ports. And if your device has a DMZ port, you can edit the DMZ configuration. The number of rules you can create depends on the number of LAN ports on your device.



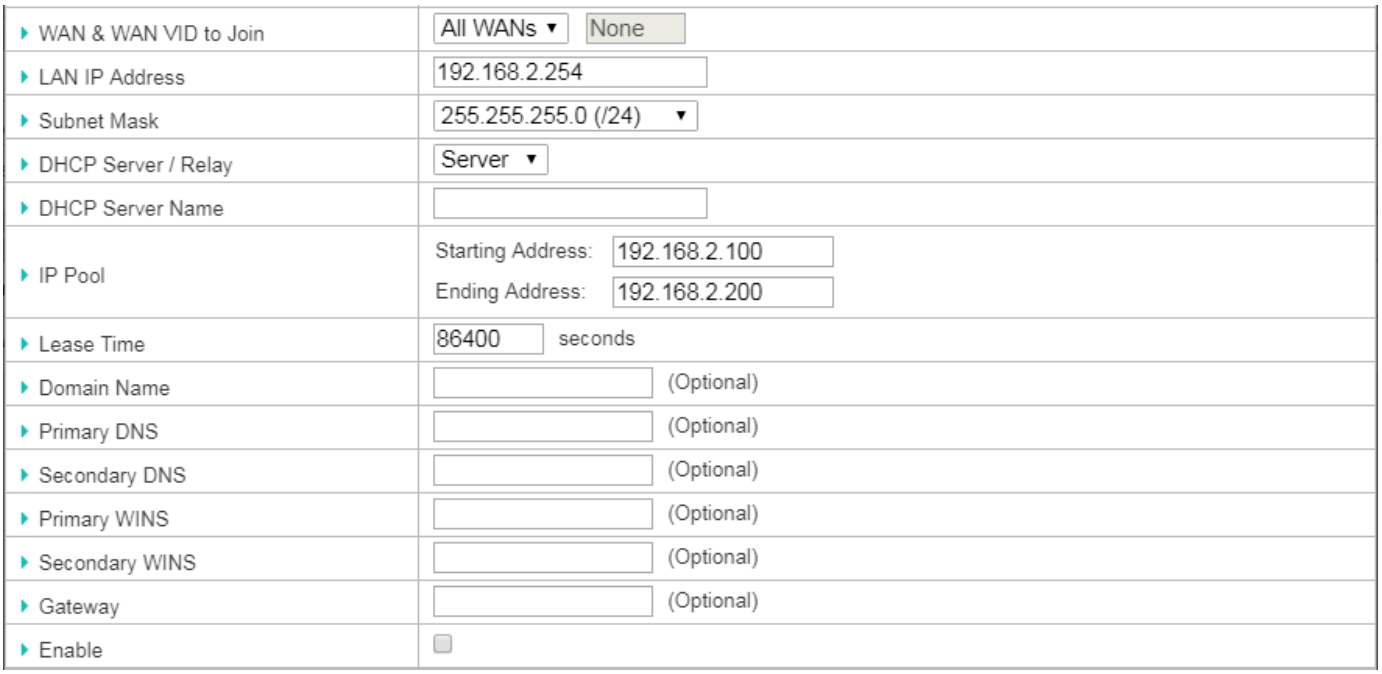
Click **Add** to open the **Port-based VLAN Configuration** screen, which includes 3 sections: Port-based VLAN Configuration, IP Fixed Mapping Rule List, and Inter-VLAN Group Routing.

Port-based VLAN – Configure VLAN Properties



Port-based VLAN Configuration (part-I)		
Item	**Value setting**	**Description**
Name	1. A must-filled setting 2. String format: already have default texts	The **Name** for this rule is displayed.
VLAN ID	A must-filled setting	Define the VLAN ID number, range is 1~4094.
VLAN Tagging	**Disable** is selected by default.	Enable VLAN Tagging for the rule with the configured **VLAN ID** and **Port Members** .
NAT / Bridge	**NAT** is selected by default.	Select **NAT** mode or **Bridge** mode for the rule.
Port Members	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 varies depending on the model.
LAN to Join	The box is unchecked by default.	Enable this and select one of the defined DHCP Servers from the list to add a DHCP server for the VLAN group.
Save	NA	Save the configuration
Undo	NA	Restore to the previous settings.

If a VLAN has not been assigned with a DHCP server, you have to configure the following settings.



Port-based VLAN Configuration (part-II)		
Item	**Value setting**	**Description**
WAN & WAN VID to Join	**All WANs** is selected by default.	Select a **WAN** or **All WANs** for connecting with the Internet. **Note**: If Bridge mode is selected, you need to select a specific WAN interface.
LAN IP Address	A must-filled setting	Assign an **IP Address** for the DHCP Server; the IP address will be the gateway's IP address.
Subnet Mask	**255.255.255.0(/24)** is selected by default.	Select a **Subnet Mask** for the DHCP Server.
DHCP Server /Relay	**Server** is selected by default.	Define the **DHCP Server** type. There are three types available: **Server**, **Relay**, and **Disable**. **Relay**: Select **Relay** to enable DHCP Relay function for the VLAN group and enter the **DHCP Server IP Address**. **Server**: Select **Server** to enable DHCP Server for a VLAN group and specify the DHCP Server settings. **Disable**: Select **Disable** to disable DHCP Server for a VLAN group.
DHCP Server IP Address (for DHCP **Relay** only)	A must-filled setting	If you select **Relay** for the DHCP Server, enter the relay DHCP Server's IP address.
DHCP Option 82 (for DHCP **Relay** only)	An optional setting	Enable the addition of DHCP Option 82 relay agent information if the relay DHCP server supports it.
DHCP Server Name	A must-filled setting	Enter a name for the DHCP Server for this VLAN group.
IP Pool	A must-filled setting	Define the IP Pool range for DHCP assignment by entering the **Starting Address** and **Ending Address**.
Lease Time	A must-filled setting	Define the duration for DHCP lease. By default, the **lease time** is 86400 seconds.
Domain Name	String format can be any text	Enter a Domain Name for this DHCP Server. *Value Range*: 0 ~ 31 characters.
Primary DNS	IPv4 format	Enter a primary DNS for this DHCP server.
Secondary DNS	IPv4 format	Enter a Secondary DNS for this DHCP Server.
Primary WINS	IPv4 format	Enter a primary WINS for this DHCP server

Secondary WINS	IPv4 format	Enter a secondary WINS for this DHCP server
Gateway	IPv4 format	Enter a gateway for this DHCP server.
Enable	The box is unchecked by default.	Activate this rule.
Save	NA	Save the configuration
Undo	NA	Restore to the previous settings.

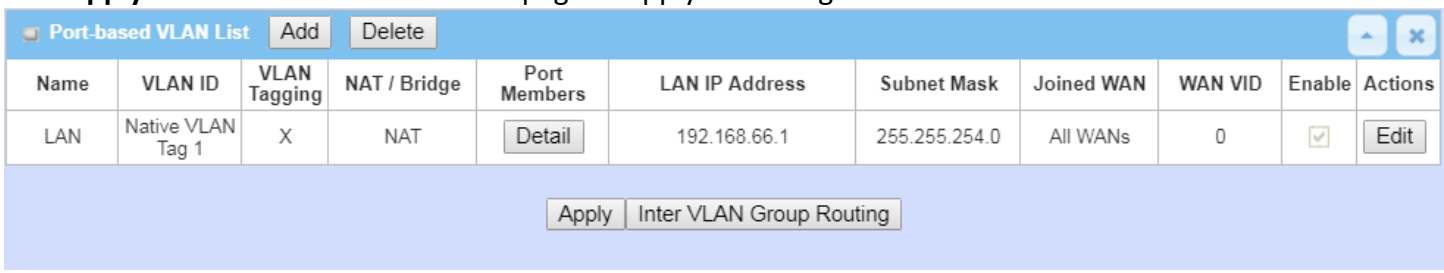
Add IP rules in the **IP Fixed Mapping Rule List** for the DHCP Server of the VLANs.



Click **Add** to open the **Mapping Rule Configuration** screen.

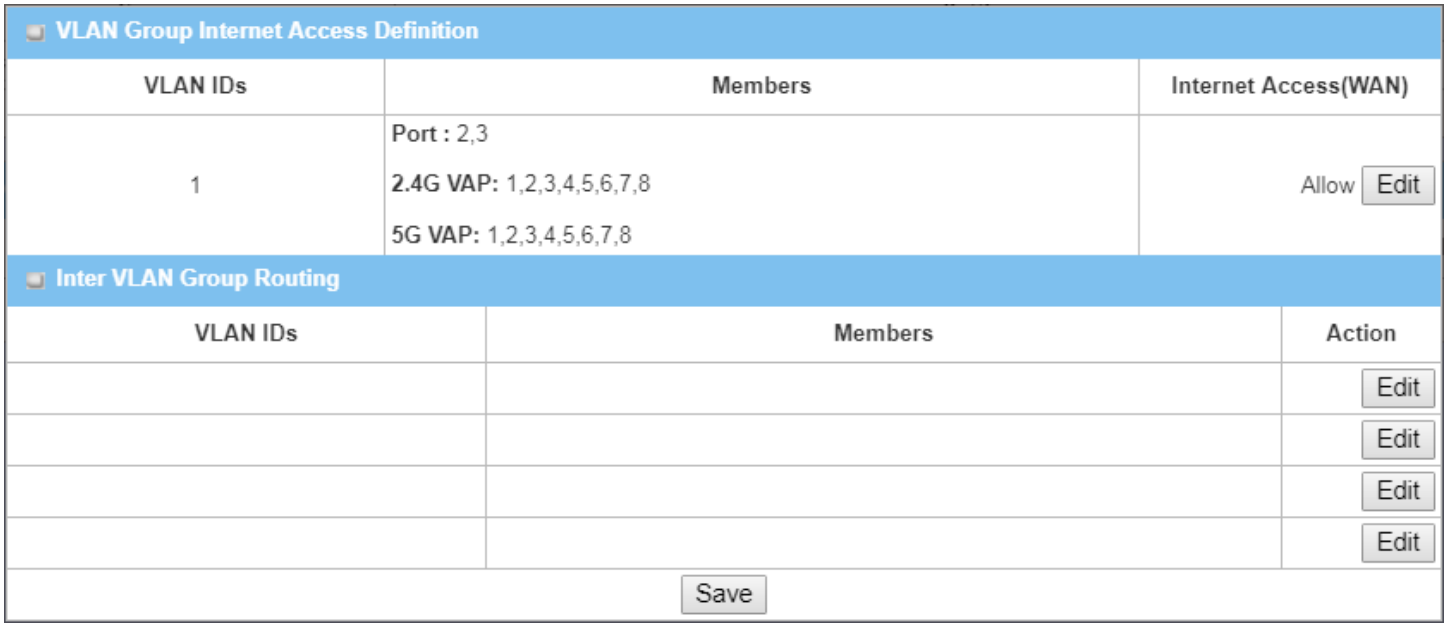
Mapping Rule Configuration		
Item	**Value setting**	**Description**
MAC Address	A must-filled setting	Define the **MAC Address** of the host requesting for DHCP assignment.
IP Address	A must-filled setting	Define the **IP Address** that the DHCP Server will assign. The DHCP Server will assign this **IP Address** to the client whose **MAC Address** matches the rule.
Enable	The box is unchecked by default.	Click **Enable** to activate this rule.
Save	NA	Save the configuration.

Click **Apply** on the Port-based VLAN List page to apply the changes.

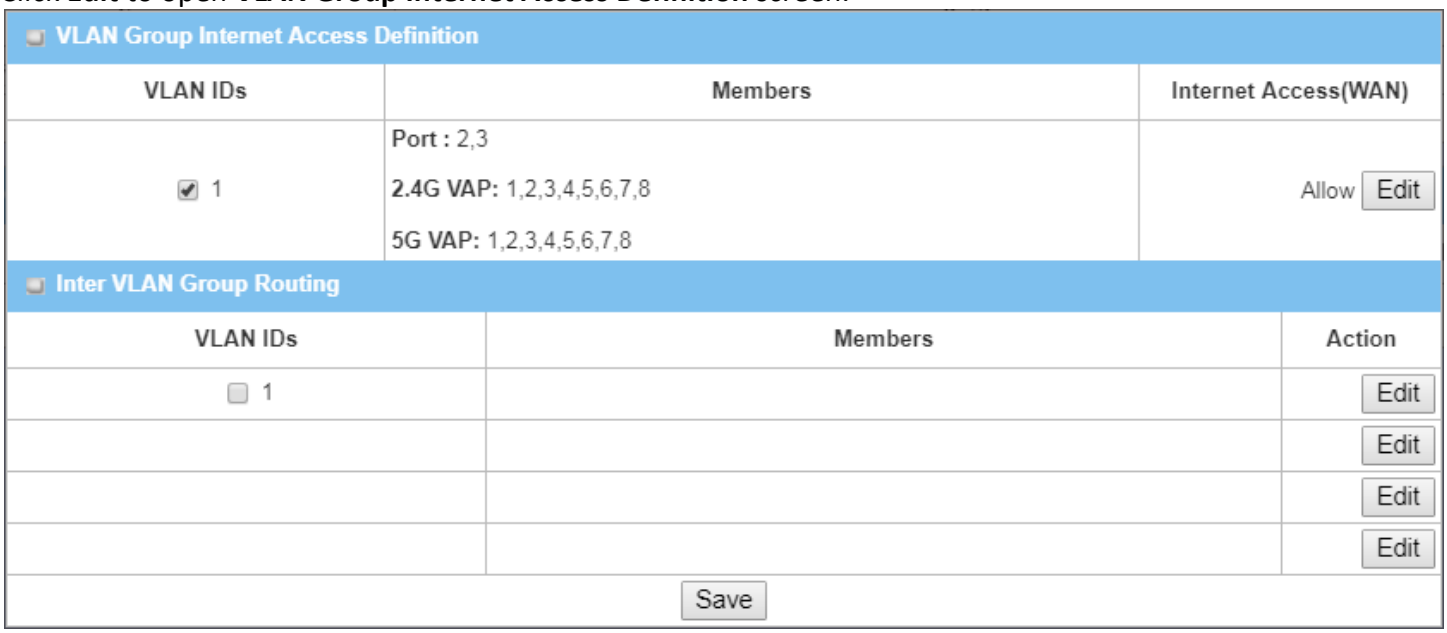


Port-based VLAN – Inter VLAN Group Routing

Click **VLAN Group Routing** to open the **VLAN Group Internet Access Definition** and **Inter VLAN Group Routing** screens.



Click **Edit** to open **VLAN Group Internet Access Definition** screen.

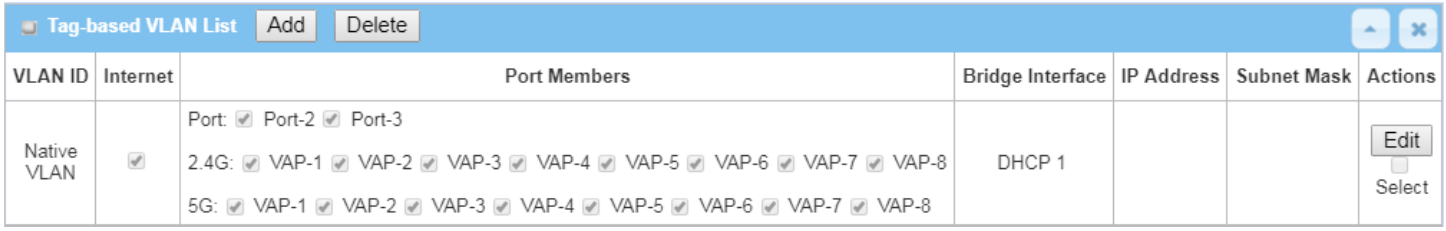


Inter VLAN Group Routing		
Item	**Value setting**	**Description**
VLAN Group Internet Access Definition	Checked by default.	All members of the same VLAN ID group can access the Internet by default. If a VLAN is not selected, members of this VLAN group cannot access the Internet. **Note: VLAN ID 1** is available always; it is the default VLAN ID for the **LAN** rule.
Inter VLAN Group Routing	The box is unchecked by default.	Select the VLAN IDs to enable the Inter-VLAN access function. By default, members of different VLAN IDs can't communicate with one another. Enable this function to allow members in different VLANs to communicate with each other. The gateway supports up to 4 rules for **Inter-**

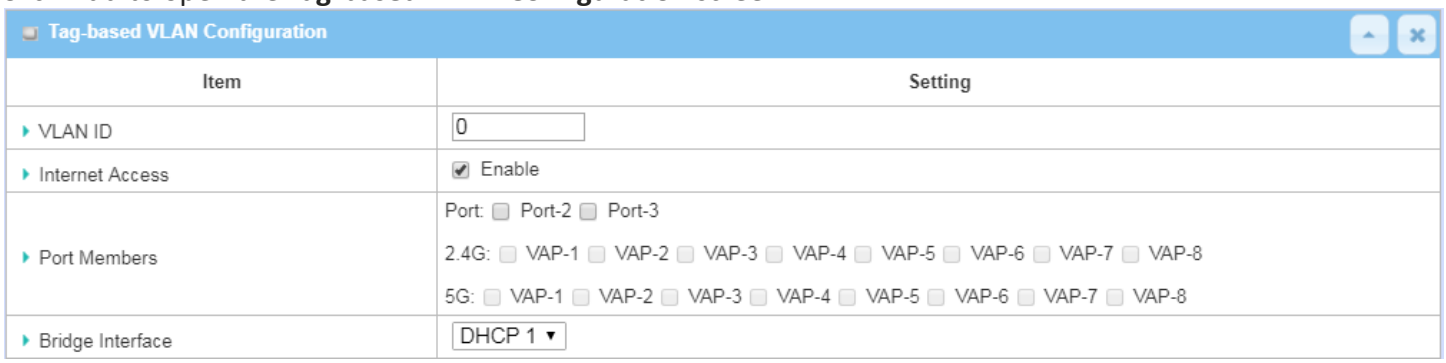
		VLAN Group Routing.
Save	N/A	Save the configuration

Tag-based VLAN – Create/Edit VLAN Rules

The **Tag-based VLAN** allows you to customize each LAN port with a VLAN ID. You can see the configuration of all LAN ports and VAPs in a default rule. If your device has a DMZ port, you can also edit the DMZ configuration. The gateway supports a maximum of 128 VLAN rule sets.

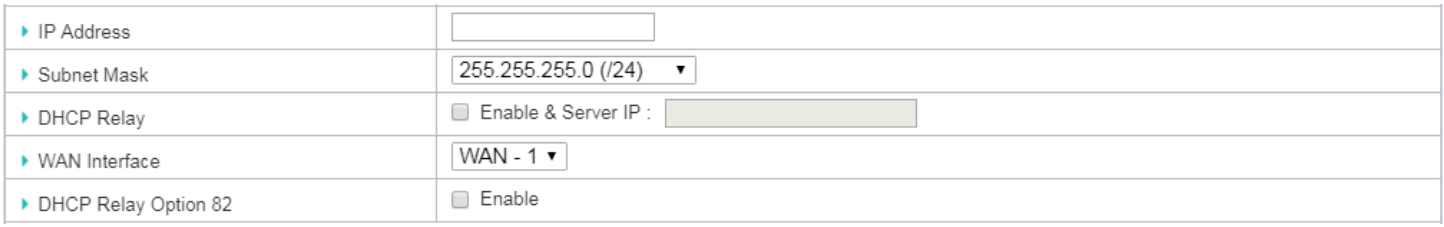


Click **Add** to open the **Tag-based VLAN Configuration** screen.



Tag-based VLAN Configuration (Part-I)		
Item	**Value setting**	**Description**
VLAN ID	A must-filled setting	Define the **VLAN ID** number, which should be outside the system reserved range. *Value Range*: 1 ~ 4095.
Internet Access	Checked by default.	**Enable** this to allow the members in the VLAN group to access the Internet.
Port Members	Unchecked by default.	Check the LAN ports to join the VLAN group. Check the VAP ports to join the VLAN group. **Note**: VAP list is only available for models with a wireless module.
Bridge Interface	**DHCP 1** is selected by default.	Select a pre-defined **DHCP Server** or select **New** to define a new DHCP server for this VLAN group.
Save	N/A	Click **Save** then click the **Apply** button.

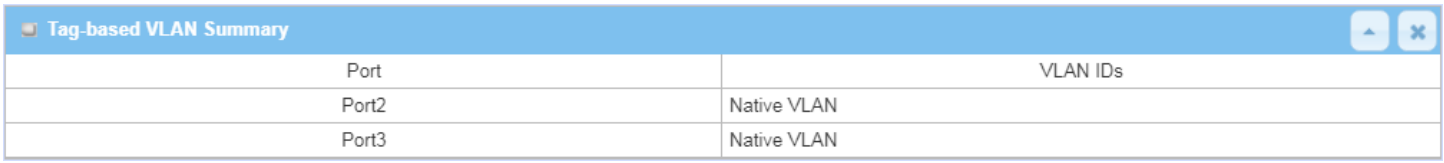
If you select **New** to create a new DHCP server for the VLAN group, configure the following:



Tag-based VLAN Configuration (part-II)		
Item	**Value setting**	**Description**
IP Address	A must-filled setting	Assign an **IP Address** for the DHCP Server.
Subnet Mask	**255.255.255.0(/24)** is selected by default.	Select a **Subnet Mask** for the DHCP Server.
DHCP Relay	The box is unchecked by default.	Check the box to enable the DHCP Relay function for the VLAN group and enter the **DHCP Server IP Address**.
WAN Interface	**WAN-1** is selected by default.	Select the **WAN** interface for Internet connection.
DHCP Option 82	An optional setting	If you select **DHCP Relay**, enable the DHCP Option 82 setting if the DHCP server supports it.
Save	NA	Save the configuration
Undo	NA	Restore to the previous settings.

Tag-based VLAN Summary

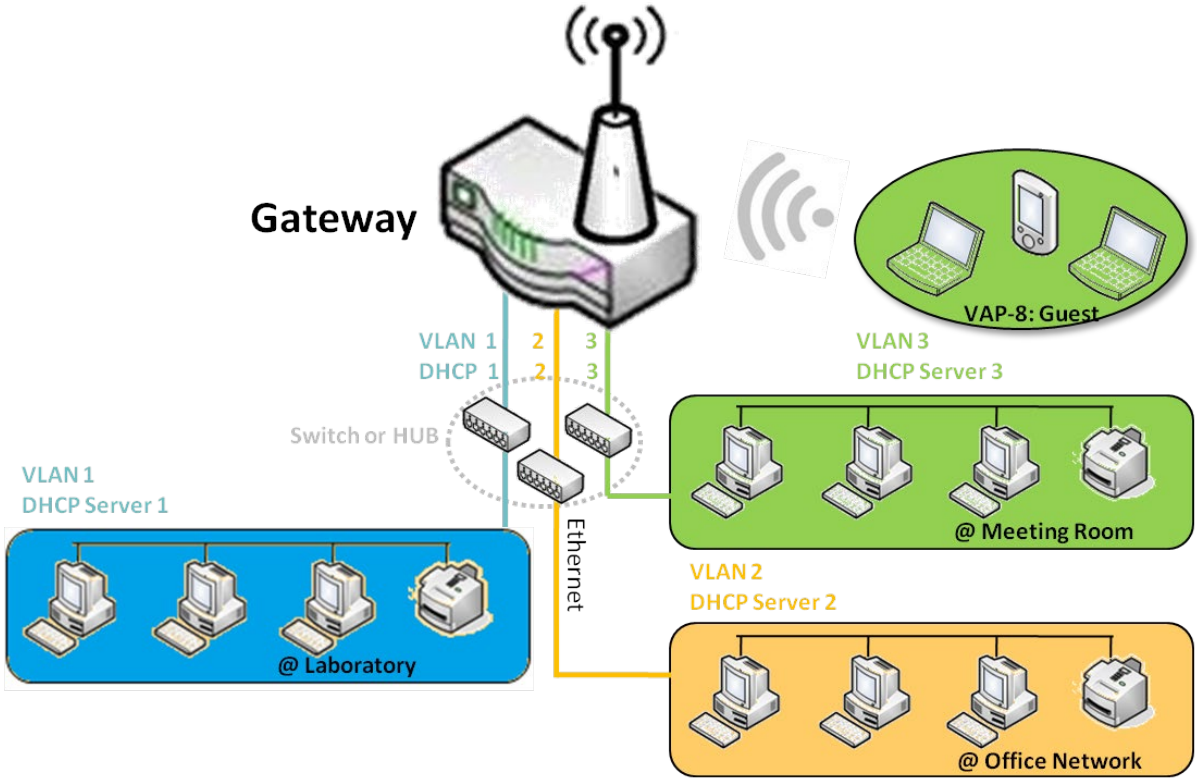
The tagged VLAN group information will be displayed as shown below.



2.2.3 DHCP Server

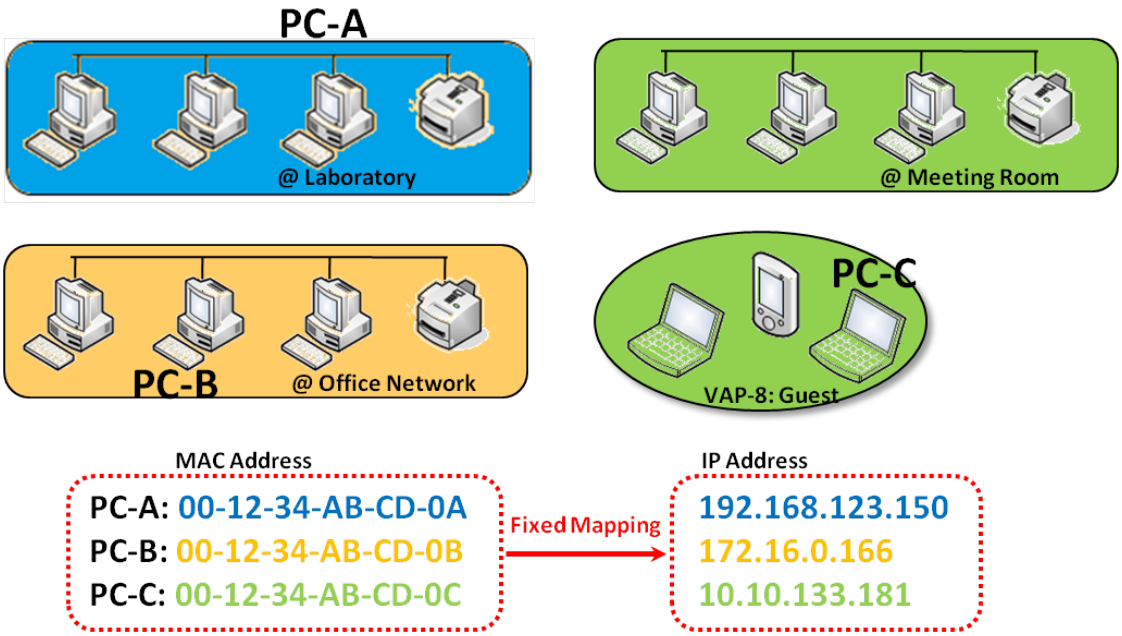
➢ DHCP Server

The gateway supports up to 4 DHCP servers for DHCP assignment for VLAN groups configuration (please refer to the above VLAN section for more information).



➢ Fixed Mapping

With fixed mapping, you can assign a fixed IP address to a DHCP client with a specific MAC address. And if a client is not listed in the DHCP Client List, you can manually create the mapping rule.

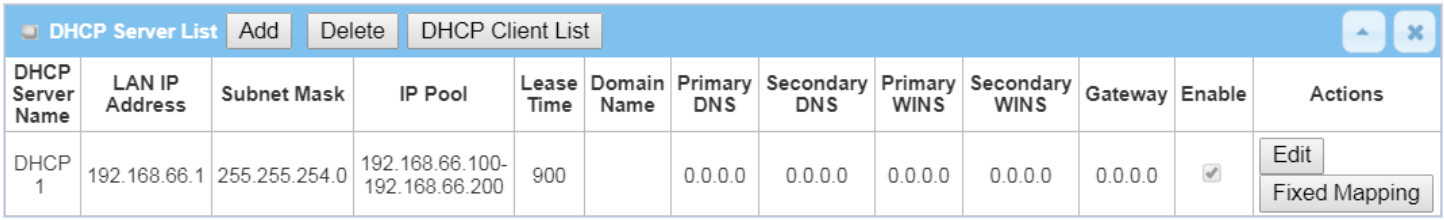


DHCP Server Setting

The DHCP Server setting allows you to create DHCP Server policies to assign IP addresses to clients on the local area network (LAN).
Go to **Basic Network > LAN & VLAN > DHCP Server** to access the DHCP Server Setting.

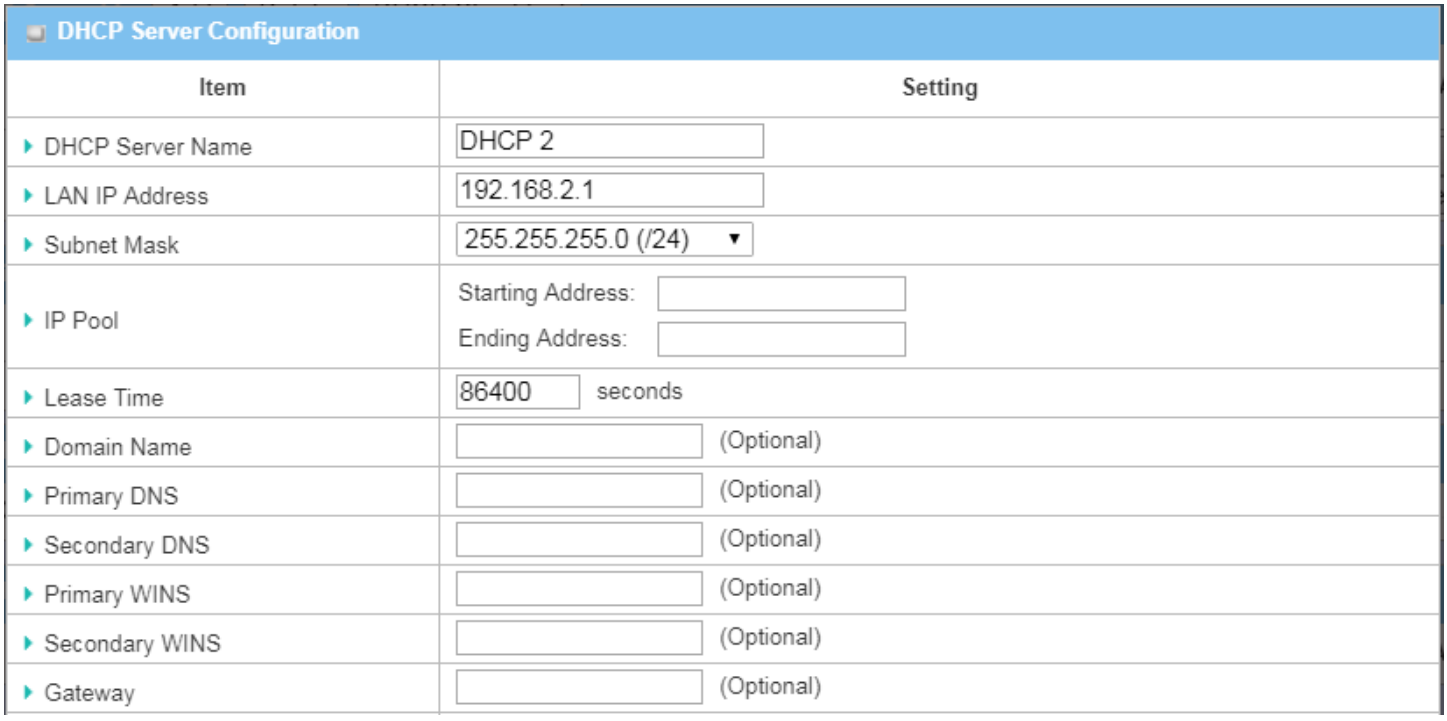
Create / Edit DHCP Server Policy

The page allows you to configure your DHCP Server settings. If multiple LAN ports are available, you can define policies for these LANs (or VLAN group). The default DHCP server IP is the LAN IP address of the gateway's LAN interface, with its default Subnet Mask setting as "255.255.255.0", and its default IP Pool range from ".100" to ".200". The system supports a maximum of 4 policies.



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	☑	Edit Fixed Mapping

Click **Add** to open the **DHCP Server Configuration** screen.



DHCP Server Configuration		
Item	**Value setting**	**Description**
DHCP Server Name	1. String format can be any text 2. A must-filled setting	Enter a descriptive name for the DHCP Server.
LAN IP Address	1. IPv4 format. 2. A must-filled setting	Enter the LAN IP Address of this DHCP Server.
Subnet Mask	255.0.0.0 (/8) is set by default	Select the Subnet Mask of this DHCP Server.
IP Pool	1. IPv4 format. 2. A must-filled setting	Enter a Start and End Address of the IP Pool.
Lease Time	1. Numberic string format. 2. A must-filled setting	Enter the Lease Time for this DHCP Server. *Value Range*: 300 ~ 604800 seconds.
Domain Name	String format can be any text	Enter the Domain Name of this DHCP Server.
Primary DNS	IPv4 format	Enter the Primary DNS server's IP address.
Secondary DNS	IPv4 format	Enter the Secondary DNS server's IP address.
Primary WINS	IPv4 format	Enter the Primary WINS server's IP address.
Secondary WINS	IPv4 format	Enter the Secondary WINS server's IP address.
gateway	IPv4 format	gatewayEnter the gateway's IP address.
Server	The box is unchecked by default.	Click **Enable** box to activate this DHCP Server.
Save	N/A	Save the configuration
Undo	N/A	Restore to the previous settings.
Back	N/A	Return to the previous page.

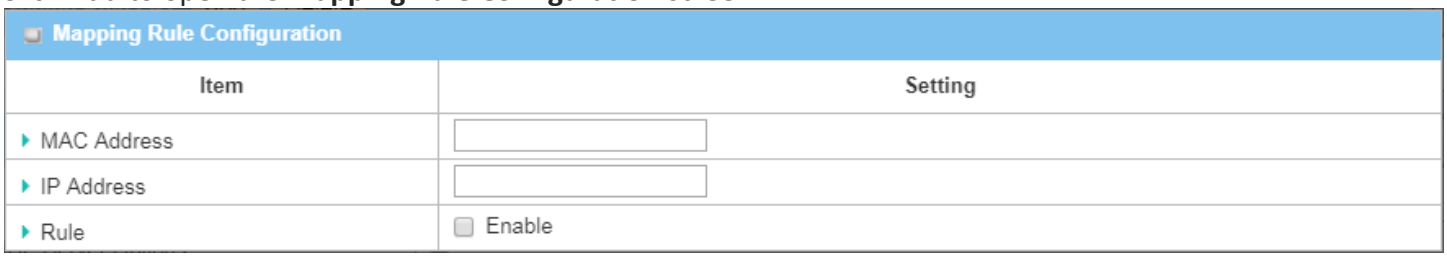
Create / Edit Mapping Rule List on DHCP Server

The gateway allows you to create up to 64 Mapping Rules for the DHCP Server. Click the **Fixed Mapping** button on the DHCP Server List page to open the **Mapping Rule List** page.



-

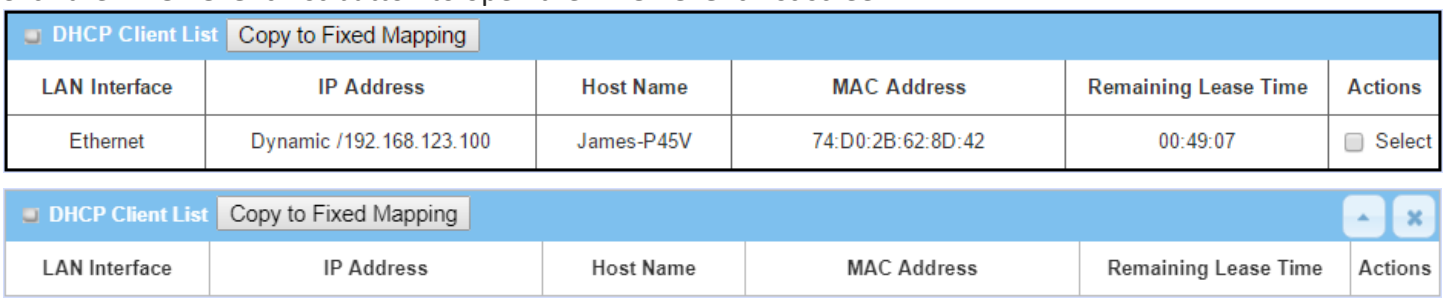
Click **Add** to open the **Mapping Rule Configuration** screen.



Mapping Rule Configuration		
Item	**Value setting**	**Description**
MAC Address	1. MAC Address string format 2. A must-filled setting	Enter a MAC Address for DHCP mapping rule.
IP Address	1. IPv4 format. 2. A must-filled setting	Enter a corresponding IP Address for this rule.
Rule	The box is unchecked by default.	Click **Enable** to activate this rule.
Save	N/A	Save the configuration
Undo	N/A	Restore to the previous settings.
Back	N/A	Return to the previous page.

View / Copy DHCP Client List

Click the **DHCP Client List** button to open the **DHCP Client List** screen.

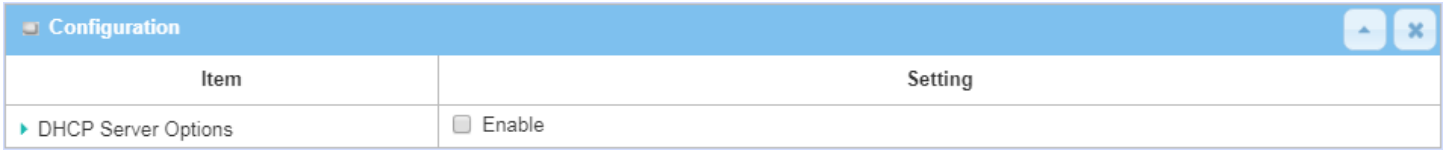


Select a DHCP client and click **Copy to Fixed Mapping** to use the IP and MAC address of the DHCP Client for a new Mapping Rule.

Enable / Disable DHCP Server Options

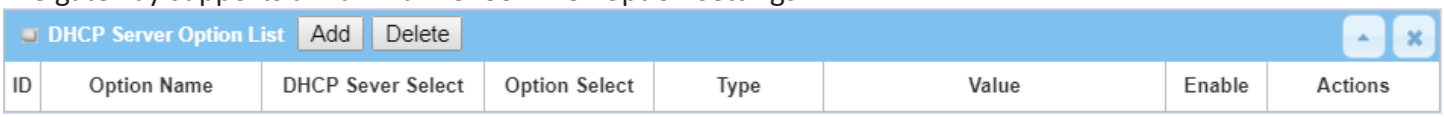
The **DHCP Server Options** setting allows you to set **DHCP OPTIONS 66**, **72**, or **114**. Click the **Enable** button to activate the DHCP option function to let DHCP Server add this information in the DHCPOFFER DHCPACK packets.

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

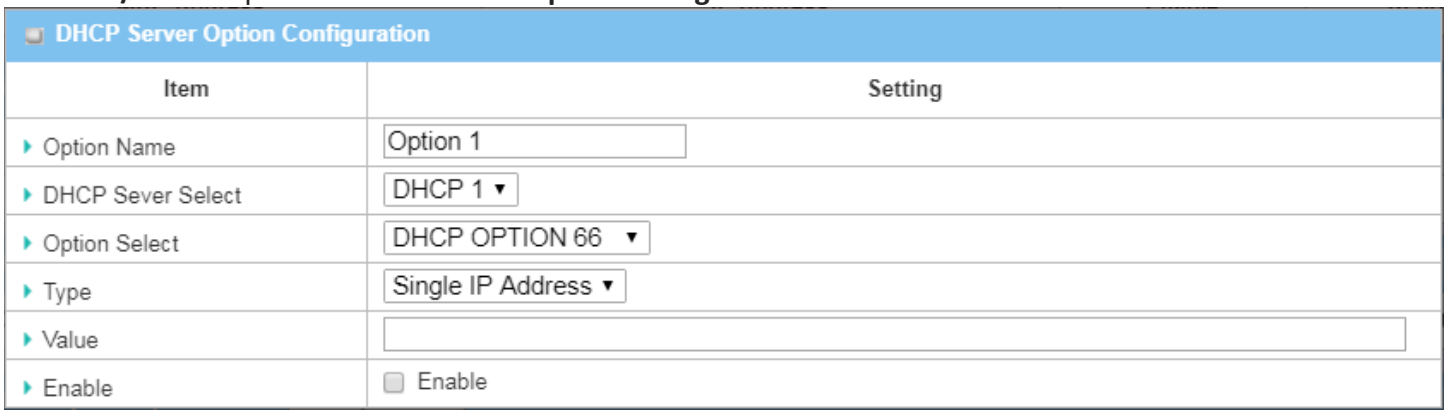


Create / Edit DHCP Server Options

The gateway supports a maximum of 99 DHCP option settings.



Click **Add/Edit** to open the **DHCP Server Option Configuration** screen.



DHCP Server Option Configuration			
Item	**Value setting**	**Description**	
Option Name	1. String format can be any text 2. A must-filled setting.	Enter a descriptive name for the DHCP Server Option.	
DHCP Server Select	Dropdown list of all available DHCP servers.	Choose the DHCP server this option should apply to.	
Option Select	1. A must-filled setting. 2. **Option 66** is selected by default.	Choose an option from the dropdown list: **Option 42** for ntp server; **Option 66** for tftp; **Option 72** for www; **Option 144** for url; **Option 160** for captive-portal.	
Type	Dropdown list of DHCP server option value type	Each option has a unique value type.	
		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 must-filled setting	Type and Value formats :	
		Type	Value
		66	Single IP Address — IPv4 format
			Single FQDN — FQDN format
		72	IP Addresses List, separated by “,” — IPv4 format, separated by “,”

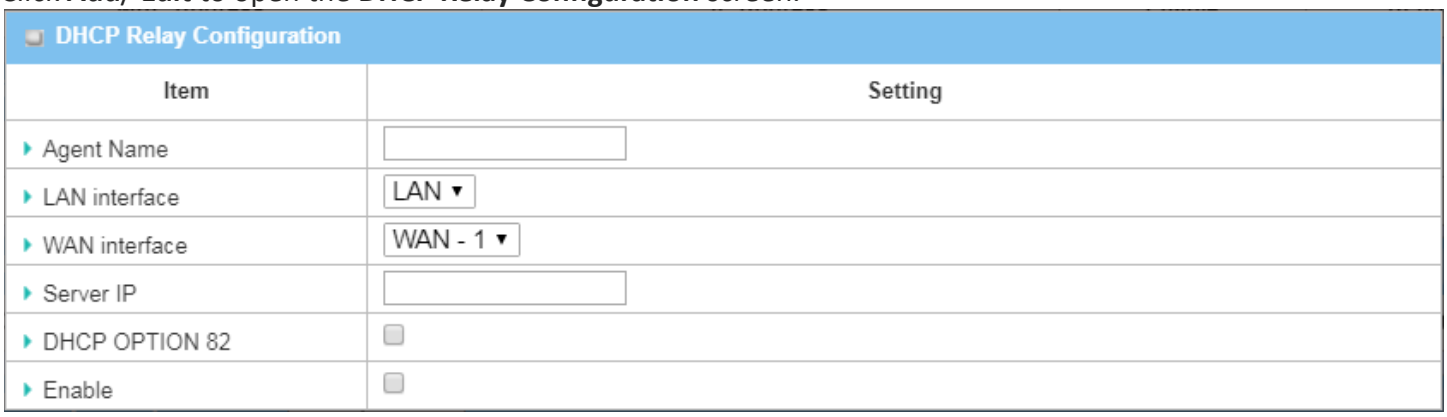
		114	Single URL	URL format
Enable	The box is unchecked by default.	Activate this configuration.		
Save	*NA*	Save the settings.		
Undo	*NA*	Discard all changes.		

Create / Edit DHCP Relay

You can create up to 6 DHCP Relay configurations.

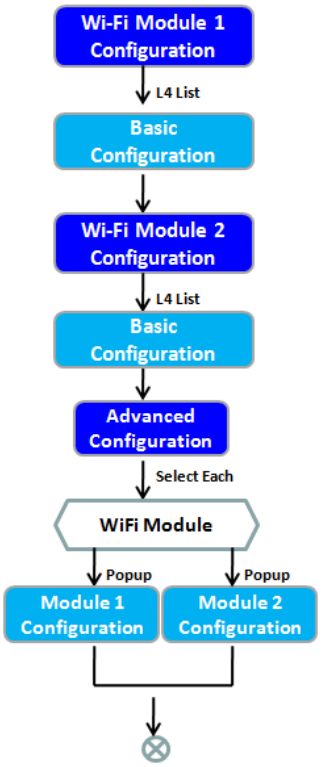


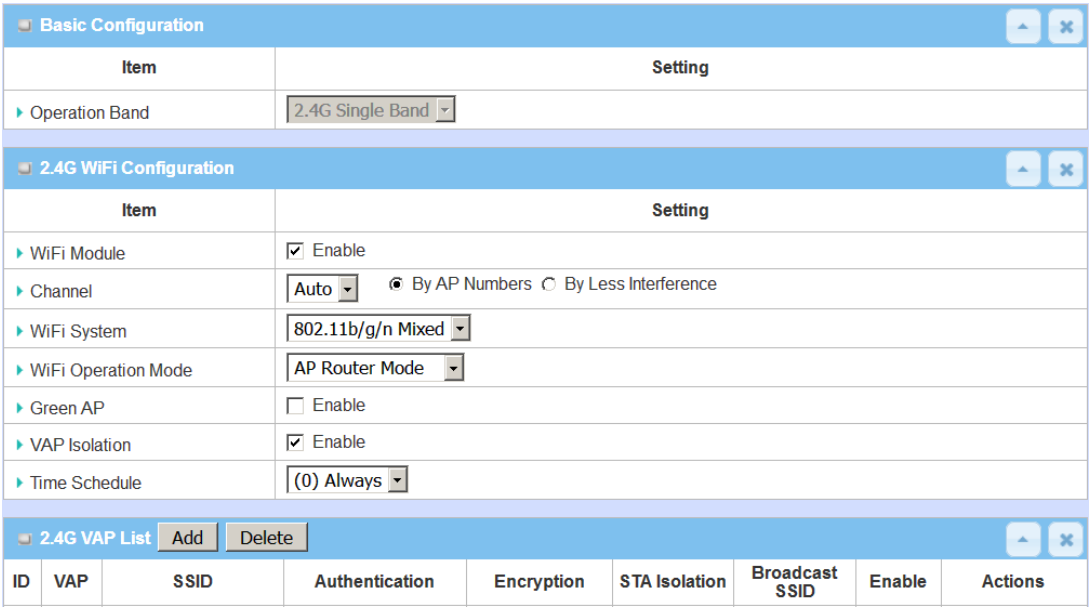
Click **Add**/ **Edit** to open the **DHCP Relay Configuration** screen.



DHCP Relay Configuration		
Item	**Value setting**	**Description**
Agent Name	1. String format can be any text 2. A must-filled setting.	Enter a descriptive name for DHCP Relay name. *Value Range*: 1~64 characters.
LAN Interface	1. A must-filled setting. 2. **LAN** is selected by default.	Choose a LAN Interface to which DHCP Relay will apply.
WAN Interface	1. A must-filled setting. 2. **WAN-1** is selected by default.	Choose a WAN Interface to which DHCP Relay will apply.
Server IP	1. A must-filled setting. 2. **null** by default.	Assign a **DHCP Server IP Address** to which the gateway will relay the DHCP requests via the specified WAN interface.
DHCP OPTION 82	The box is unchecked by default.	Click **Enable** box to activate DHCP OPTION 82 function. Enable this if the relayed DHCP server requires this information for identifying DHCP relay agent.
Enable	The box is unchecked by default.	Activate this setting.
Save	*NA*	Save the setting.
Undo	*NA*	Discard all changes.

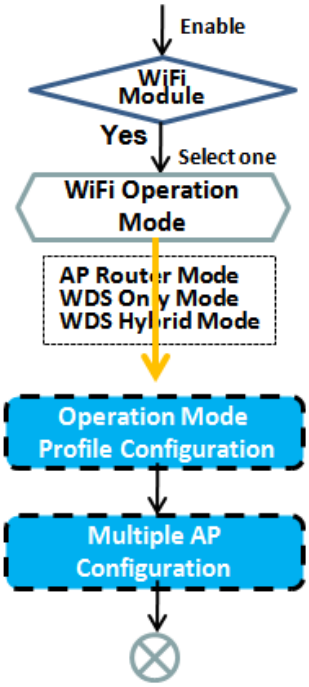
2.3 Wi-Fi





The gateway provides Wi-Fi interfaces for mobile devices that may include **Bring your own device (BYOD)** and guest devices to connect the wireless LAN. The Wi-Fi system in the gateway complies with IEEE 802.11ac/11n/11g/11b/11a standard in 2.4GHz or 5GHz single band or 2.4G/5GHz concurrent dual bands. There are several wireless operation modes provided by this device: "**AP Router Mode**", "**WDS Only Mode**", and "**WDS Hybrid Mode**". The gateway also allows for performance tuning.

2.3.1 Wi-Fi Configuration



2.4G WiFi Configuration

Item	Setting
WiFi Module	Enable
Channel	Auto; By AP Numbers; By Less Interference
WiFi System	802.11b/g/n Mixed
WiFi Operation Mode	AP Router Mode
Green AP	Enable
VAP Isolation	Enable
Time Schedule	(0) Always

2.4G VAP List Add Delete

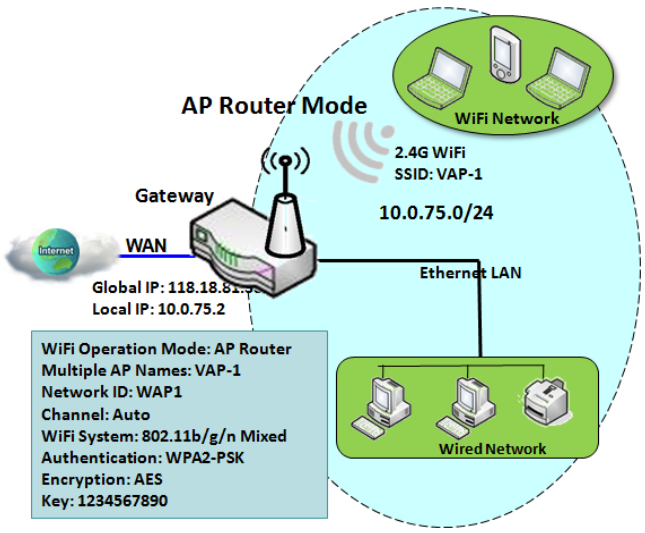
ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	Staff_2.4G	WPA2-PSK	AES				Edit Select
2	VAP 2	default	Open	None				Edit Select

VAP Configuration

Item	Setting
VAP	VAP1
SSID	Staff_2.4G
Max. STA	Enable
Authentication	WPA2-PSK
Encryption	AES
Preshared Key	1234567890
STA Isolation	
Broadcast SSID	
Enable	

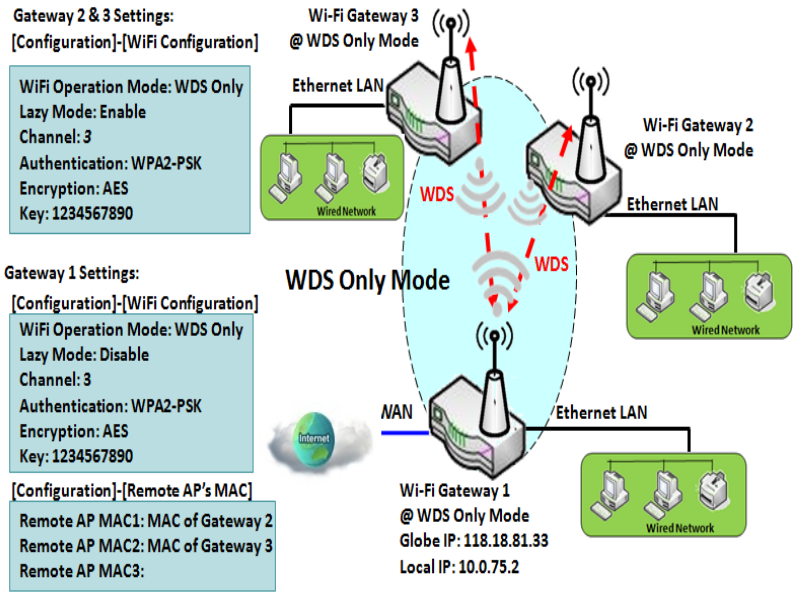
The gateway supports dual frequency bands and you need to configure bands separately according to your desired operation mode. In addition, you can also configure the Wi-Fi Uplink function in the **Basic Network > WAN & Uplink > Physical Interface** tab.

AP Router Mode



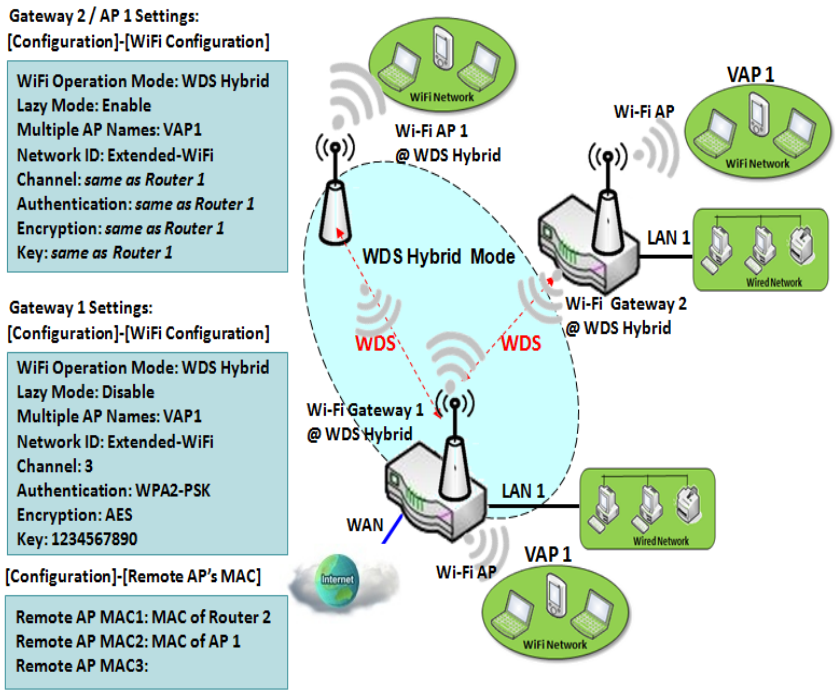
The AP Router Mode allows you to connect your wired and wireless devices to the Internet with the NAT mechanism provided by the gateway. Therefore, this gateway not only works as a Wi-Fi AP, but also a Wi-Fi hotspot for Internet service.

WDS Only Mode



In WDS (Wireless Distributed System) Only Mode, the gateway will serve as a bridge for its wired network and as a repeater to extend the range of the wireless signal. You can chain multiple Wi-Fi gateways using the "WDS Only" mode and configure one of them to provide DHCP service to all DHCP clients.

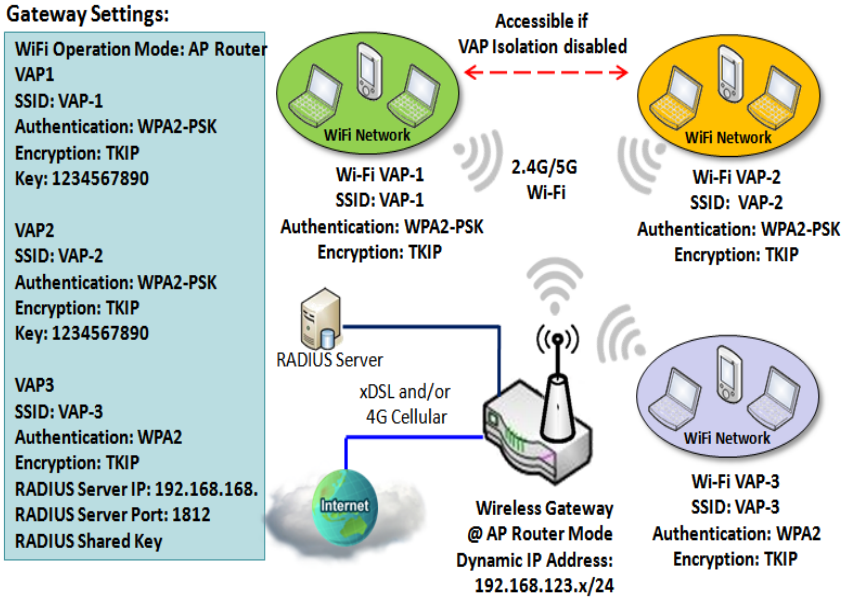
The diagram illustrates that there are two wireless gateways 2, 3 running at "WDS Only" mode and they use channel 3 to link to the local gateway 1 through WDS with gateway 2 and 3 configured as the Remote AP MACs. Then clients of gateway 2, 3 can request an IP address from the DHCP server at gateway 1, which also facilitates Internet access with NAT for the clients.



WDS Hybrid Mode

The WDS Hybrid Mode includes both WDS and AP Router mode. WDS Hybrid mode serves an access point for its wireless network and a bridge for its wired and wireless network at the same time.

The diagram illustrates gateway 1, gateway 2, and AP 1 connected under the WDS hybrid mode. Each gateway provides the access point function for Wi-Fi client connectivity while gateway 1 also offers DHCP service.

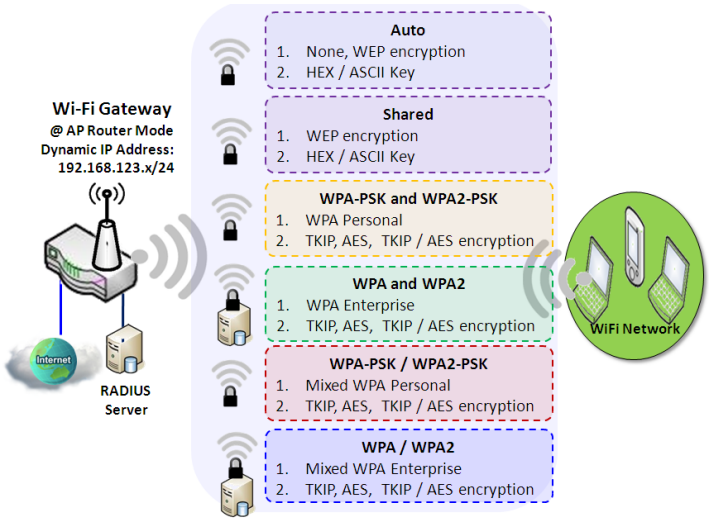


Multiple VAPs

VAP (Virtual Access Point) is the function to partition a wireless network into multiple broadcast domains. This wireless gateway supports up to 8 VAPs. For each VAP, you need to set up SSID, authentication and encryption methos as you would for setting a standalone AP.

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

Wi-Fi Security - Authentication & Encryption



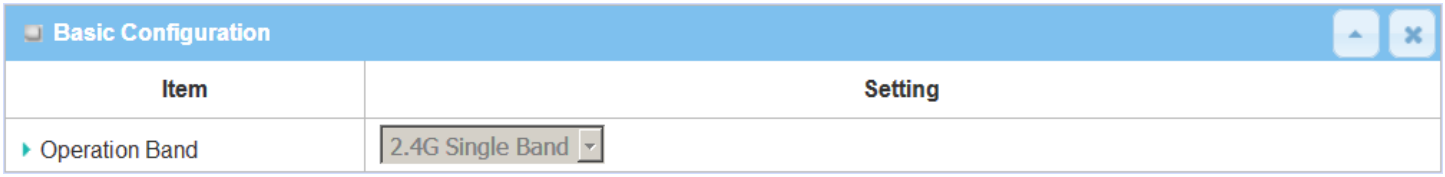
Wi-Fi security provides complete authentication and encryption mechanisms to enhance the data security while your data is transferred wirelessly over the air. The wireless gateway supports Shared, WPA-PSK, WPA2-PSK and WPA/WPA2 authentication with data encryption methods, such as WEP, TKIP and AES.

Wi-Fi Configuration Setting

The Wi-Fi configuration allows you to configure 2.4GHz and 5GHz bands.

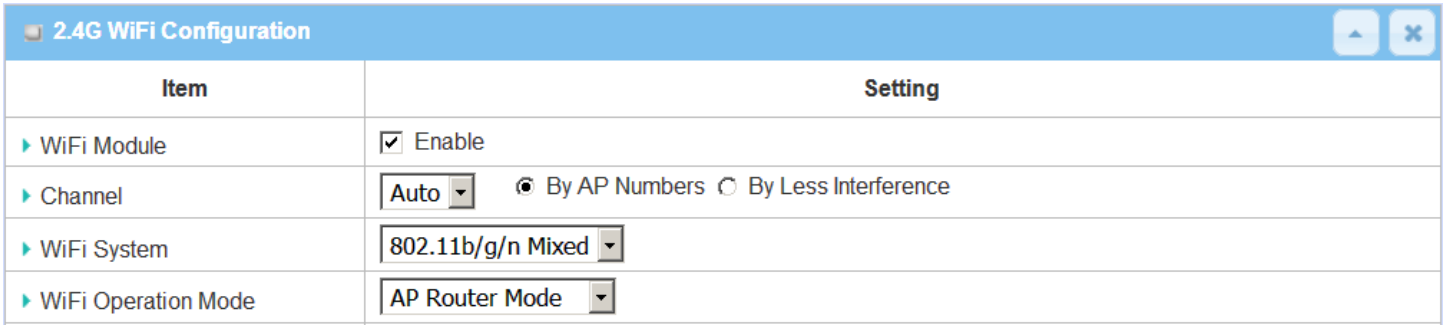
Go to **Basic Network > WiFi > WiFi Module One** Tab. You can configure additional modules using the same procedure if the gateway is equipped with multiple Wi-Fi modules.

Basic Configuration



Basic Configuration		
Item	**Value setting**	**Description**
Operation Band	A must-filled setting	Specify the intended operation band for the Wi-Fi module. Depending on the model, this may be fixed.

Configure Wi-Fi Setting



Configuring Wi-Fi Settings		
Item	**Value setting**	**Description**
Wi-Fi Module	The box is checked by default	Check the **Enable** box to activate Wi-Fi function.
Channel	1. A must-filled setting. 2. **Auto** is selected be default.	Select a radio channel for the VAP compliant with your country's regulations. The permissible channels depend on the **Regulatory Domain**. There are two available options when **Auto** is selected: ● **By AP Numbers** The channel will be selected according to the number of APs detected on the channel (the less, the better). ● **By Less Interference** The channel will be selected according to interference (the lower, the better).
Wi-Fi System	A must-filled setting	Specify the preferred Wi-Fi System. The dropdown list of **Wi-Fi system** is based on **IEEE 802.11** standard. ● Select 802.11 b/g/n only or Mixed for 2.4GHz band. ● Select 802.11 a/n/ac only or Mixed for 5GHz band.
Wi-Fi Operation		Specify the **Wi-Fi Operation Mode** according to your application.

Mode	Go to the following table for **AP gateway Mode**, **WDS Only Mode**, and **WDS Hybrid Mode** settings. **Note:** The available operation modes depend on the product specifications.

The following section describes each Wi-Fi operation mode.

Note: If you activate Wi-Fi uplink, your gateway is automatically in AP Router Mode for your local wireless clients to connect to a wireless network.

AP Router Mode [Wi-Fi Uplink Mode] & VAPs Configuration

For the AP Router Mode and the Wi-Fi Uplink Mode, the device supports both client connectivity and the gateway function. The **WAN** port and the **NAT** function are **enabled**.



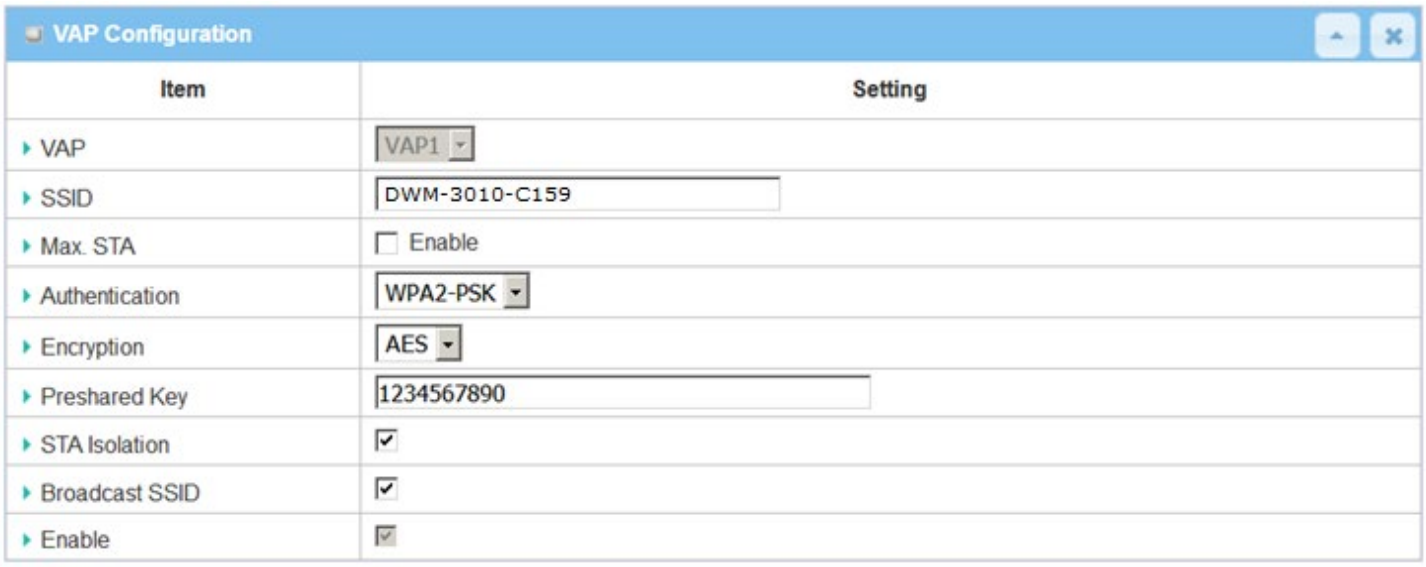
AP gateway Mode		
Item	**Value setting**	**Description**
Green AP	The box is unchecked by default.	Check the **Enable** box to activate **Green AP** function.
VAP Isolation	The box is checked by default.	Check the **Enable** box to activate this function. By default, the box is checked to prevent stations associated to different VAPs from communicating with one another.
Profile	The box is unchecked by default.	Check the **Enable** box to activate the profile setting. **Note:** This setting is only available in Wi-Fi Uplink operation mode.
Time Schedule	A must-filled setting	Apply a specific **Time Schedule** to this rule; otherwise leave it as **(0) Always**. Go to **Object Definition** > **Scheduling > Configuration** tab to configure a schedule.



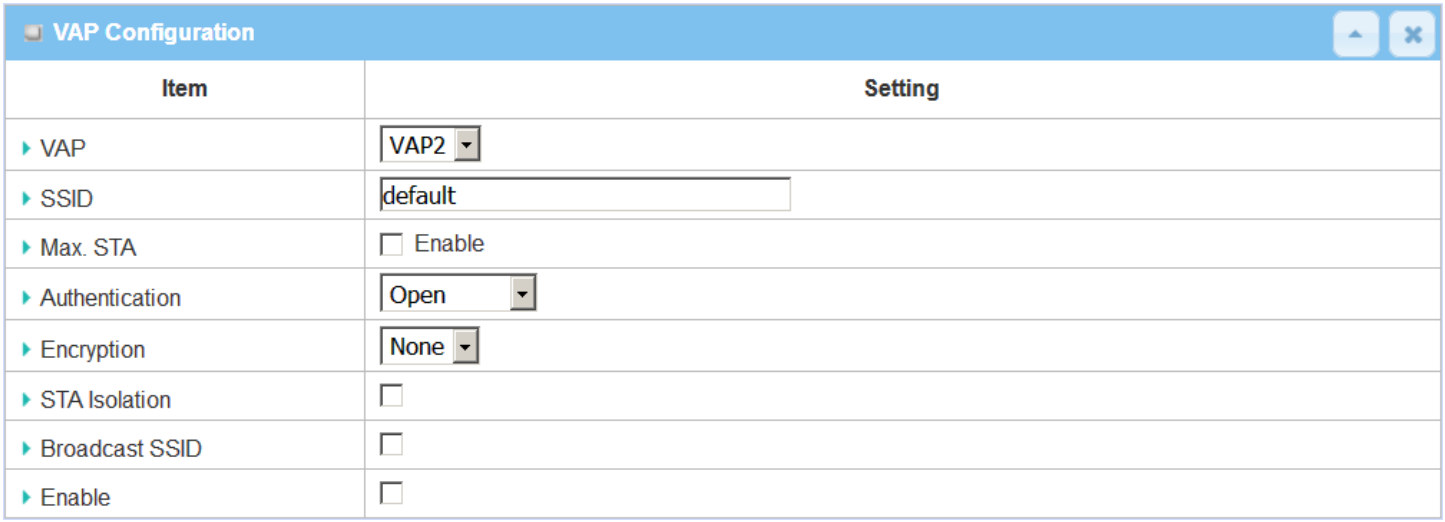
By default, VAP 1 is enabled with security settings to connect to the gateway wirelessly to enhance the security level.
The default Wi-Fi key is printed on both the device label and the Security Card. It is strongly recommanded that you modify the security key.

Click **Add** / **Edit** button in the VAP List screen to open the **VAP Configuration** screen.

For VAP 1:



For others:



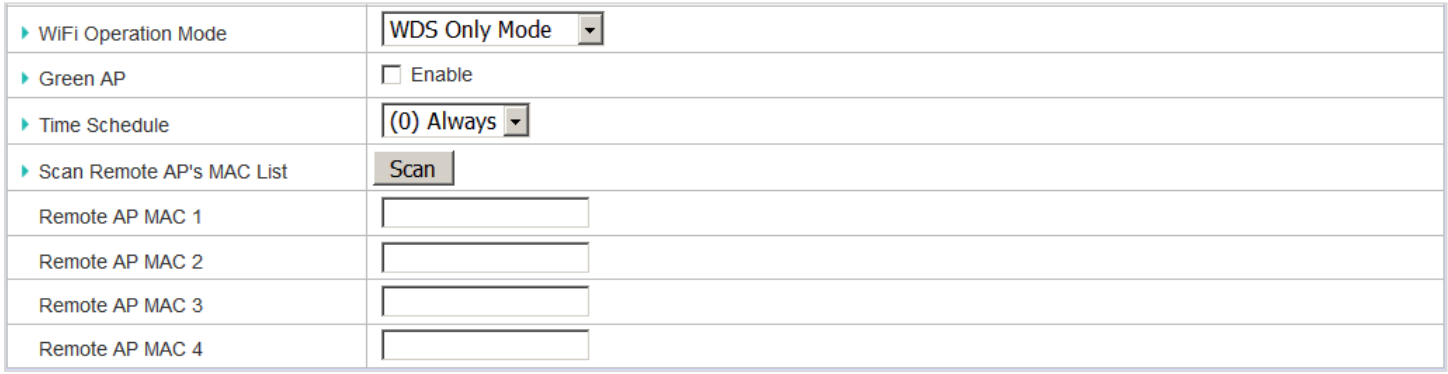
VAP Configuration		
Item	**Value setting**	**Description**
SSID	1. String format : Any text	Enter an SSID for your VAP. You can decide if other APs and clients can identify this SSID with the SSID broadcast function.
Max. STA	Unchecked by default.	Enable Max. STA and specify the maximum available clients.
Authentication	1. A must-filled setting 2. VAP1: **WPA2-PSK** is selected be default; Others: **Open** is selected as the default.	Client stations should provide the key when trying to associate with the device using the correct authentication.
		When **Open** is selected The check box named **802.1x** shows up next to the dropdown list. ● **802.1x** (The box is unchecked by default) When **802.1x** is enabled, all client stations will be authenticated by a RADIUS server. Enter the below RADIUS server settings: **RADIUS Server IP** (The default IP is 0.0.0.0) **RADIUS Server Port** (The default value is 1812) **RADIUS Shared Key**
		When **Shared** is selected, enter the pre-shared WEP key for authentication.
		When **Auto** is selected, the device will select **Open** or **Shared** by requesting the

		clients automatically. The check box named **802.1x** shows up next to the dropdown list. ● **802.1x** (The box is unchecked by default) When **802.1x** is enabled, all client stations will be authenticated by a RADIUS server: **RADIUS Server IP** (The default IP is 0.0.0.0) **RADIUS Server Port** (The default value is 1812) **RADIUS Shared Key**
		WPA and **WPA2** are implementation of IEEE 802.11i. WPA2 fully implements the 802.11i standard and offers better security than WPA while WPA has better compatibility. **WPA2** had ● **RADIUS Server** The client stations will be authenticated by a RADIUS server. Enter the below RADIUS server information: **RADIUS Server IP** (The default IP is 0.0.0.0) **RADIUS Server Port** (The default value is 1812) **RADIUS Shared Key**
		When **WPA** / **WPA2** is selected, the clients can associate with this device via **WPA** or **WPA2**.
		When **WPA-PSK** or **WPA2-PSK** is selected, the clients use pre-shared key instead of RADIUS server for authentication.
		When **WPA-PSK** / **WPA2-PSK** is selected, the clients can associate with this device via **WPA-PSK** or **WPA2-PSK**.
Encryption	1. A must-filled setting. 2. VAP1: **AES** is selected be default; Others: **None** is selected be default.	Select a suitable encryption method and enter the required key(s). The available methods for selection depend on the Authentication type you selected. **None** The device uses no encryption. **WEP** Up to 4 WEP keys can be set, and you have to select one as the current key. The key type can be set to **HEX** or **ASCII**. If **HEX** is selected, the key should consist of (0 to 9) and (A to F). If **ASCII** is selected, the key should consist of alphanumeric characters. **TKIP** Enter a Pre-shared Key with the length from 8 to 63 characters. **AES** Enter a Pre-shared Key with the length from 8 to 63 characters. It is recommended to use **AES** encryption as it offers the best security. **TKIP / AES** **TKIP / AES** mixed mode. Enter a Pre-shared Key with the length from 8 to 63 characters.
STA Isolation	VAP1: The box is checked by default; Others: unchecked by default.	Check the **Enable** box to activate this function. By default, this box is checked; Stations associated to the same VAP cannot communicate with each other.
Broadcast SSID	VAP1: The box is checked by default; Others: unchecked by default.	Check the **Enable** box to activate SSID broadcast function.
Enable	VAP1: The box is checked by default; Others: unchecked by default.	Check the **Enable** box to activate this VAP.
Save	N/A	Save the settings.
Undo	N/A	Restore configuration to previous settings.

Apply	N/A	Apply the saved configuration.

WDS Only Mode

In the WDS Only mode, the gateway bridges its network with another network of WDS-enabled Wi-Fi device. In this mode, no wireless clients can connect to the gateway.

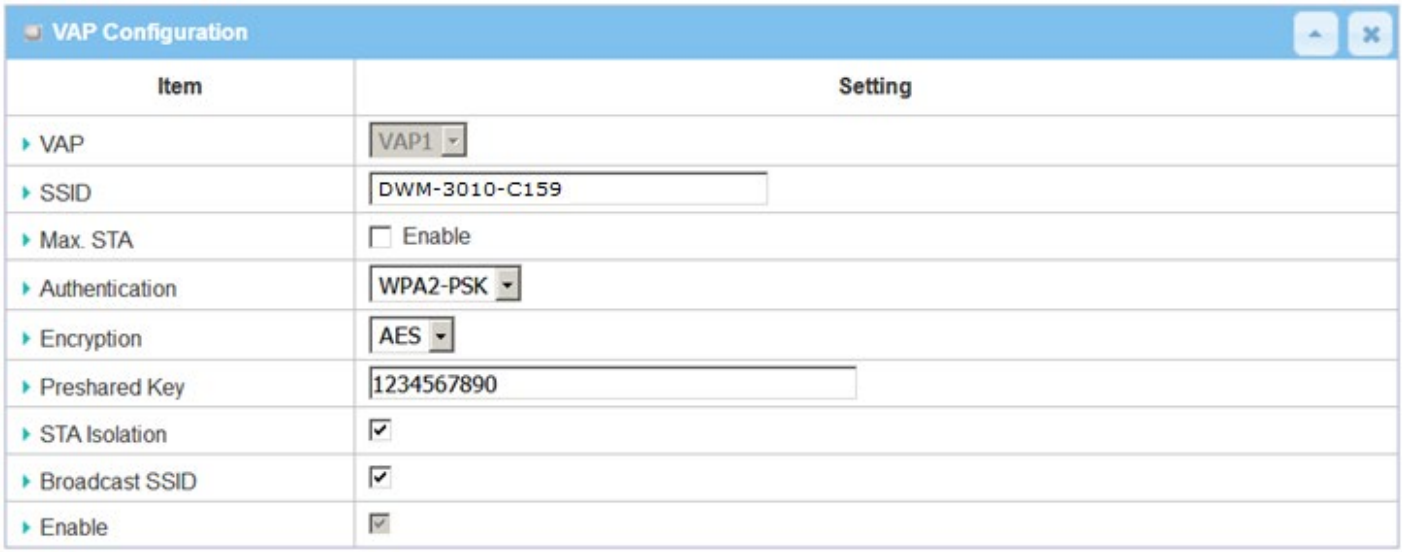


WDS Only Mode		
Item	**Value setting**	**Description**
Green AP	The box is unchecked by default.	Activate **Green AP** function.
Time Schedule	A must-filled setting	Apply a specific **Time Schedule** to this rule; otherwise leave it as **(0) Always**. Go to **Object Definition** > **Scheduling > Configuration** to configure a schedule.
Scan Remote AP's MAC List	N/A	Click **Scan** to scan the spatial AP information, and then select one from the AP list, the MAC of the selected AP will be filled automatically in the following Remote AP MAC table.
Remote AP MAC 1~4	A must-filled setting	Enter the remote AP's MAC manually use the above auto-scan. The gateway will bridge the traffic to the remote AP when associated successfully.



By default, VAP 1 is enabled with security (WPA2-PSK with AES) to prevent access from unauthorized devices. **The default Wi-Fi key is printed on both the device label and the Security Card. It is strongly recommanded that you change the security key**.

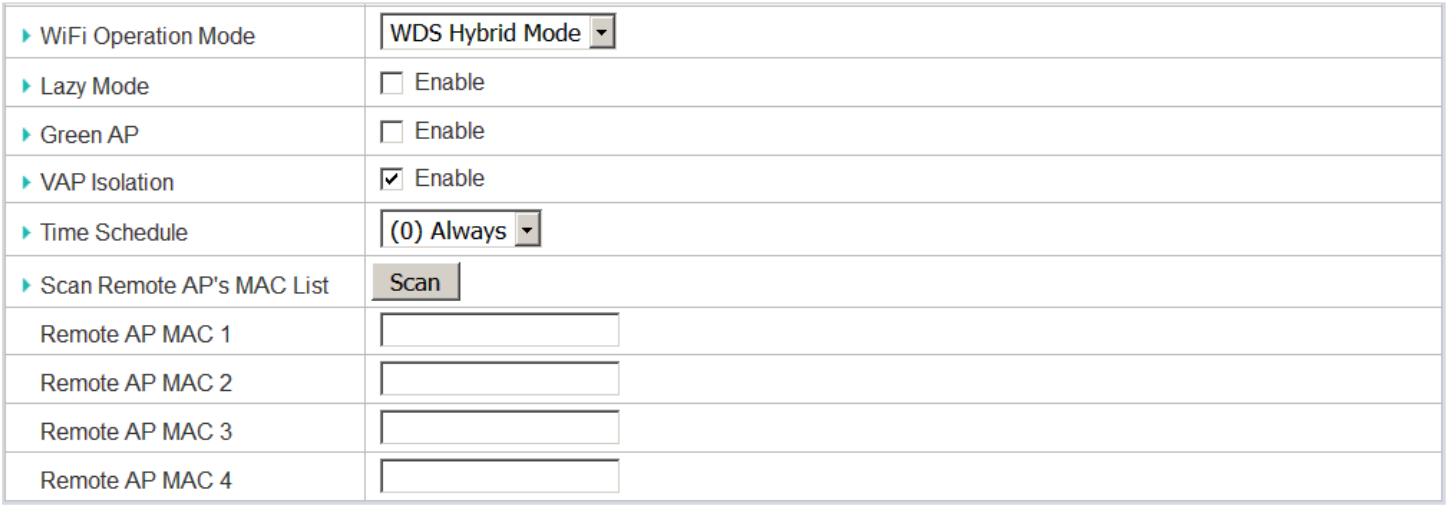
In **WDS Only** mode, only VAP1 will be available for configuration of the required authentication and encryption settings. Click **Edit** in the VAP List to open the **VAP Configuration** screen.



For a detail description of VAP configuration, please refer to the above **AP Router Mode** section.

WDS Hybrid Mode

In the WDS Hybrid mode, the gateway bridges its network with another network of WDS or WDS-hybrid gateway while providing wireless clients connectivity.



WDS Hybrid Mode		
Item	**Value setting**	**Description**
Lazy Mode	The box is checked by default.	Check the **Enable** box to activate this function. The gateway can learn about WDS peers without manual configuration of the other AP's MAC address.
Green AP	The box is unchecked by default.	Check the **Enable** box to activate **Green AP** function.
VAP Isolation	The box is checked by default.	Check the **Enable** box to activate this function. By default, the box is checked; it means that clients associated to different VAPs cannot communicate with one another.
Time Schedule	A must-filled setting	Apply a specific **Time Schedule** to this rule; otherwise leave it as **(0) Always**. Go to **Object Definition** > **Scheduling > Configuration** tab to configure a schedule.
Scan Remote AP's MAC List	Available when Lazy Mode disabled.	Click the **Scan** button to scan the spatial AP information, and select one from the AP list to fill the MAC address of the selected AP automatically in the following Remote AP MAC table.
Remote AP MAC 1~4	Available when Lazy Mode disabled.	Enter the remote AP's MAC address manually or use the auto-scan approach. The gateway will bridge the network with a remote AP.

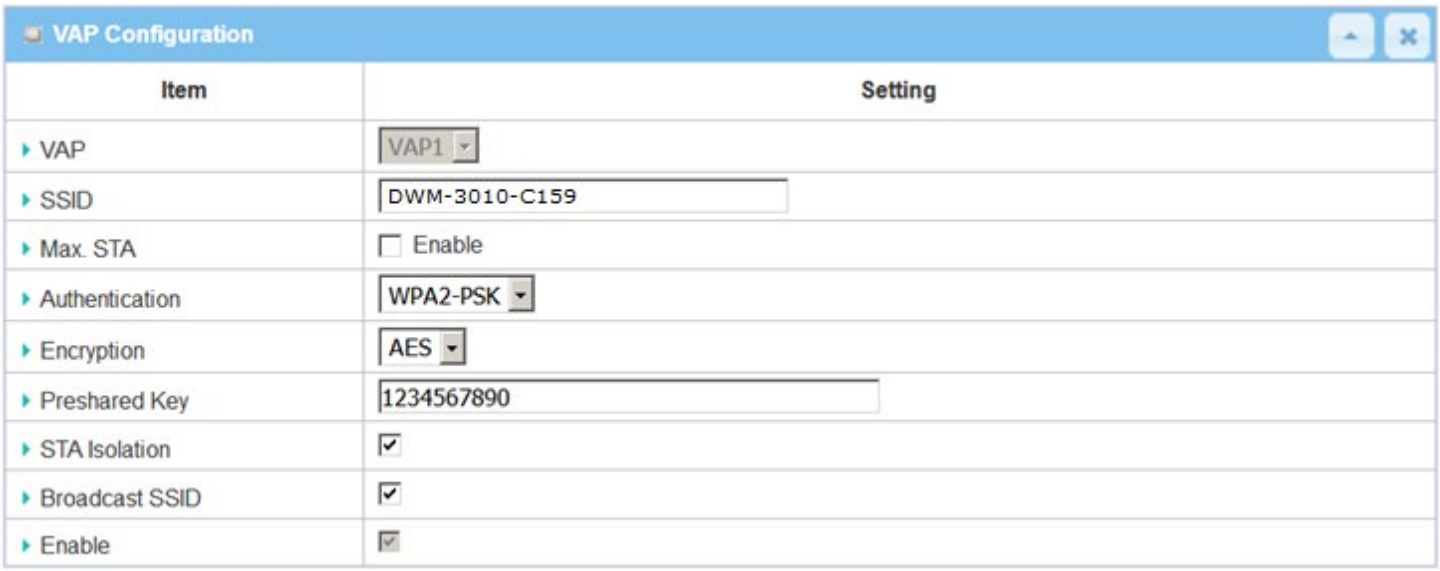


By default, VAP 1 is enabled with security (WPA2-PSK with AES) to prevent access from unauthorized devices. **The default Wi-Fi key is printed on both the device label and the Security Card. It is strongly recommanded that you change the security key**.

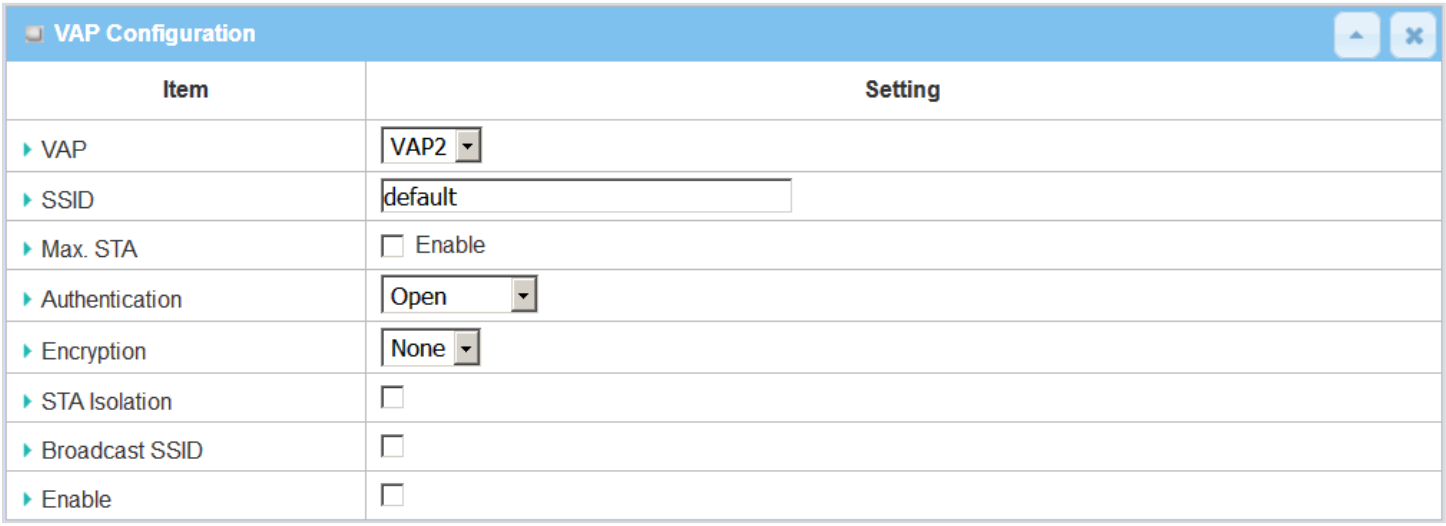
In **WDS Hybrid** mode, you can configure the VAP function for the wireless network.

Click **Add** / **Edit** in the VAP List screen to open the **VAP Configuration** screen.

The configuration screen for VAP 1:



The configuration screen for other VAPs:



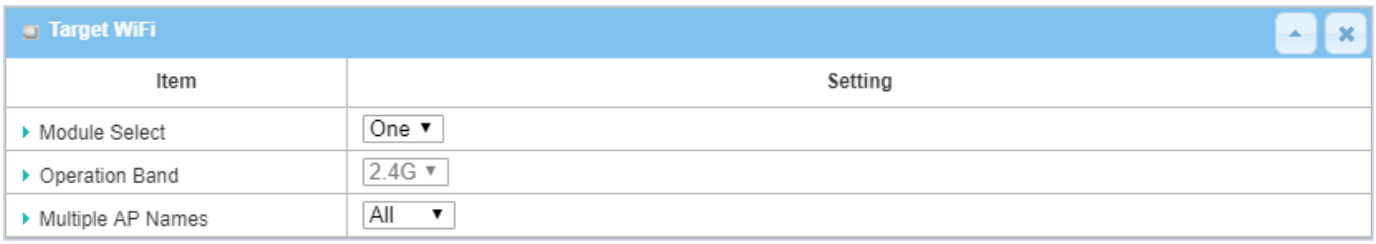
For detailed description of VAP configuration, please refer to the description stated in the above AP gateway section.For a detail description of VAP configuration, please refer to the above **AP Router Mode** section.

2.3.2 Wireless Client List

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

Go to **Basic Network > WiFi > Wireless Client List** to access the **Wireless Client List** page.

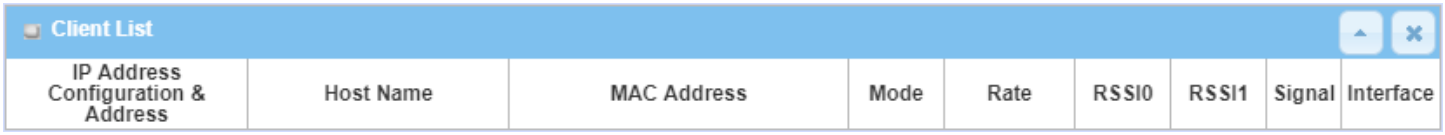
Select Target Wireless Network



Target Configuration		
Item	**Value setting**	**Description**
Module Select	A must-filled setting.	Select the Wi-Fi module to display the information of connected clients. For devices with a single Wi-Fi module, this option is hidden.
Operation Band	A must-filled setting.	Specify the intended operation band for the Wi-Fi module. Basically, this setting is fixed and cannot be changed once the the device is shipped. However, some modules have selectable bands for users to choose according to their network environment.
Multiple AP Names	1. A must-filled setting. 2. **All** is selected by default.	Specify the VAP to show the associated clients' information in the following Client List.

Show Client List

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



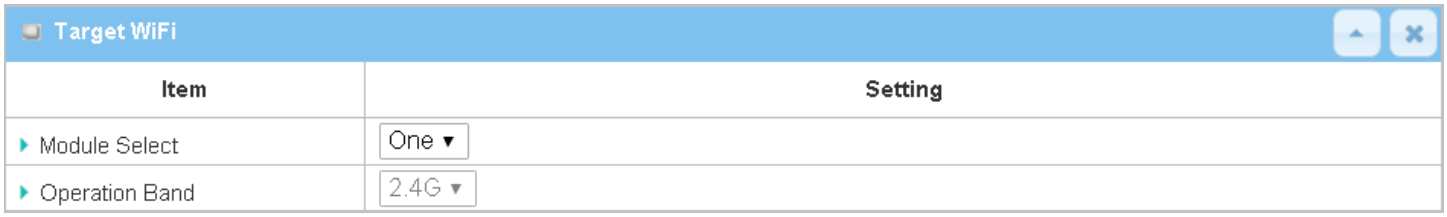
Target Configuration		
Item	**Value setting**	**Description**
IP Address Configuration & Address	N/A	It shows the Client's IP address and the addressing method. **Dynamic** means the IP address is assigned from a DHCP server. **Static** means the IP address is a fixed one filled by the client.
Host Name	N/A	It shows the host name of the client.
MAC Address	N/A	It shows the MAC address of the client.
Mode	N/A	It shows what kind of **wireless mode** (refer to the above Wi-Fi Configuration section for available modes) the client used to associate with this gateway.
Rate	N/A	It shows the **data transmission rate** between the client and this gateway.
RSSI0, RSSI1	N/A	It shows the Received Signal Strength Indication (RSSI) value for each radio path.
Signal	N/A	The **signal strength** between clients and this gateway.
Interface	N/A	It shows the VAP ID that the client associated with.
Refresh	N/A	Update the Client List.

2.3.3 Advanced Configuration

This device provides advanced wireless configuration for professional users to optimize the wireless performance according to application requirements. Please note that if you do not know potential impact of the configuration changes, just leave the advanced configuration with its default values; otherwise, errors may occur.

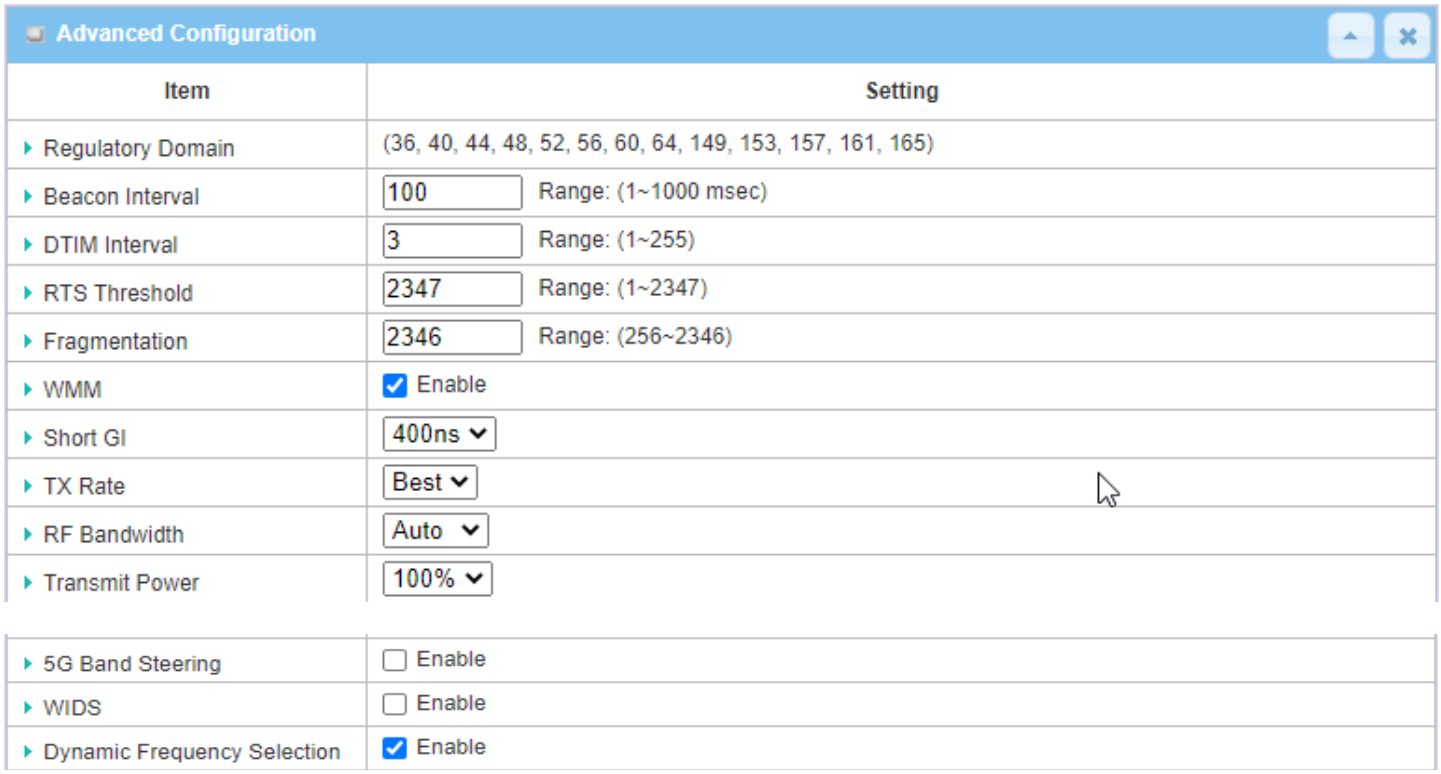
Go to **Basic Network > WiFi > Advanced Configuration** to accesss the **Advanced Configuration** page.

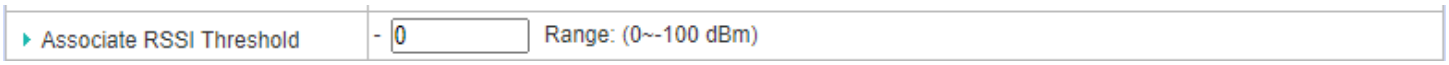
Select Target Wi-Fi



Target Configuration		
Item	**Value setting**	**Description**
Module Select	A must-filled setting.	Select the Wi-Fi module to check the information about connected clients. For devices with a single Wi-Fi module, this option is hidden.
Operation Band	A must-filled setting.	Specify the operation band for the Wi-Fi module. Basically, this setting is fixed and cannot be changed once the device shipped. However, some modules have selectable bands for users to choose according to their network environment.

Advanced Configuration





Advanced Configuration		
Item	**Value setting**	**Description**
Regulatory Domain	The default setting is according to where the product sale to	It limits the available radio channel of this device. The permissible channels depend on your regulatory domain.
Beacon Interval	1. A must-filled setting. 2. **100** is set by default	It shows the time interval between each beacon packet broadcast. The beacon packet contains **SSID**, **Channel ID** and **Security settings**. *Value Range*: 1 ~ 1000 msec.
DTIM Interval	1. A must-filled setting. 2. **3** is set by default	A **DTIM (Delivery Traffic Indication Message)** is a countdown informing clients of the next window to listen to broadcast messages. When the device has buffered broadcast messages for the associated clients, it sends the next DTIM with a DTIM value. *Value Range*: 1 ~ 255.
RTS Threshold	1. A must-filled setting. 2. **2347** is set by default	**Set the RTS (Request to send) Threshold** to activate RTS. RTS/CTS is a **collision avoidance** technique. *Value Range*: 1 ~ 2347.
Fragmentation	1. A must-filled setting. 2. **2346** is set by default	Wireless frames can be divided into smaller units (fragments) to improve performance when RF interference is present. *Value Range*: 256 ~ 2346.
WMM	The box is checked by default	**WMM (Wi-Fi Multimedia)** can help control latency and jitter when transmitting multimedia content over a wireless connection.
Short GI	By default **400ns** is selected	**Short GI (Guard Interval)** is defined to set the sending interval between each packet. Note that a lower **Short GI** could **increase** not only the **transition rate** but also the **error rate**.
TX Rate	By default **Best** is selected	Set the **data transition rate**. When **Best** is selected, the device will choose a proper data rate according to the current **signal strength**.
RF Bandwidth	By default **Auto** is selected	RF bandwidth limits the maximum data rate.
Transmit Power	By default **100%** is selected	Set the **transmit power** to control the Wi-Fi **coverage**.
5G Band Steering	The box is unchecked by default	When a client tries to associate with 2.4GHz Wi-Fi, the device will connect with the client using 5GHz Wi-Fi if the client can use 5G Wi-Fi band. This option is only available for the Wi-Fi modules that supports 5GHz band.
WIDS	The box is unchecked by default	The WIDS (Wireless Intrusion Detection System) will analyze all packets to generate Wi-Fi statistics in Wi-Fi status. Go to **Status** > **Basic Network** > **WiFi** for detailed WIDS status.
Dynamic Frequency Selection	The box is checked by default	**Dynamic Frequency Selection (DFS)** DFS enables gateways to detect radar signals and switch their operating frequency to prevent interference with the radar system. **Note**: Dynamic Frequency Selection (DFS) option is only available for the Wi-Fi module with 5GHz radio.
Associate RSSI Threshold	1. A must-filled setting. 2. **0** is set by default	Specify a connection threshold for the RSSI value. If the RSSI of the Wi-Fi client is less than the threshold, it would be rejected to associate with the AP. And if the average RSSI for data transmission is less than the threshold, the connection would be disconnected directly. The default value **0** means the RSSI threshold checking function is disabled. *Value Range*: 0 ~ -100 dBm.
Save	N/A	Save the current configuration.
Undo	N/A	Restore configuration to previous settings.

2.4 IPv6

The growth of the Internet drives the development of IPv6 to allow more devices to be assigned with Internet addresses. IPv6 (Internet Protocol version 6) is a version of the Internet Protocol (IP) that succeeds IPv4, defining an IP address as a 128-bit value instead of 32-bit. IPv6 implements additional features not present in IPv4, including Stateless address autoconfiguration, network renumbering and router advertisement, which is useful when changing Internet service providers.

2.4.1 IPv6 Configuration



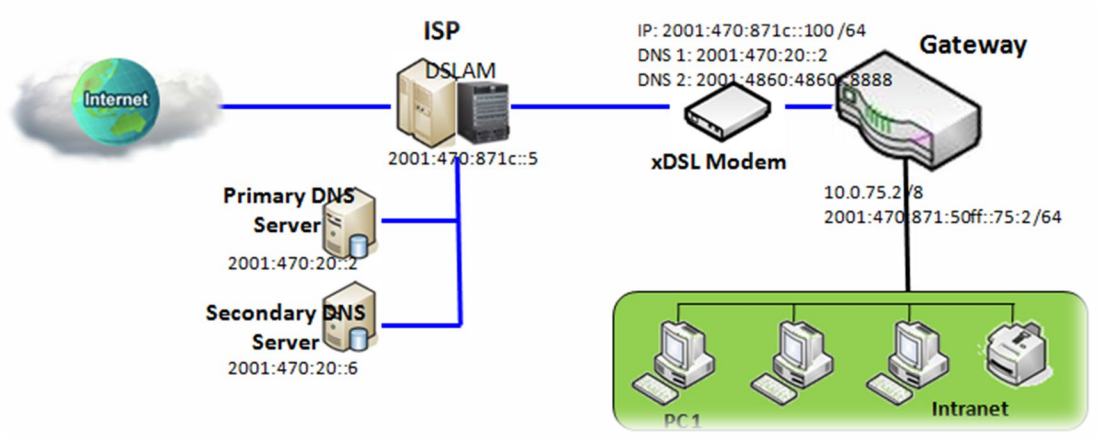
The **IPv6 Configuration** setting allows you to set the IPv6 connection type to access the IPv6 network. This gateway supports various types of IPv6 connection, including **Static IPv6**, **DHCPv6**, and **PPPoEv6**.

Note: The available WAN connection types vary depending on the WAN Interface type.

IPv6 WAN Connection Type

Static IPv6

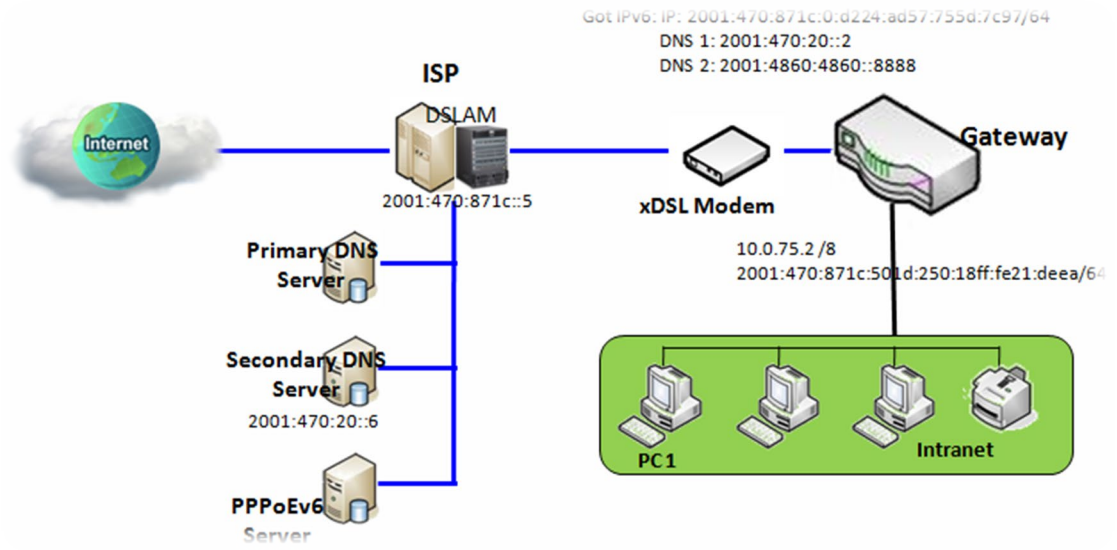
Static IPv6 works the same as static IPv4. The static IPv6 provides manual setting of IPv6 address, IPv6 default gateway address, and IPv6 DNS server address.



The above diagram depicts the IPv6 IP addressing.

DHCPv6

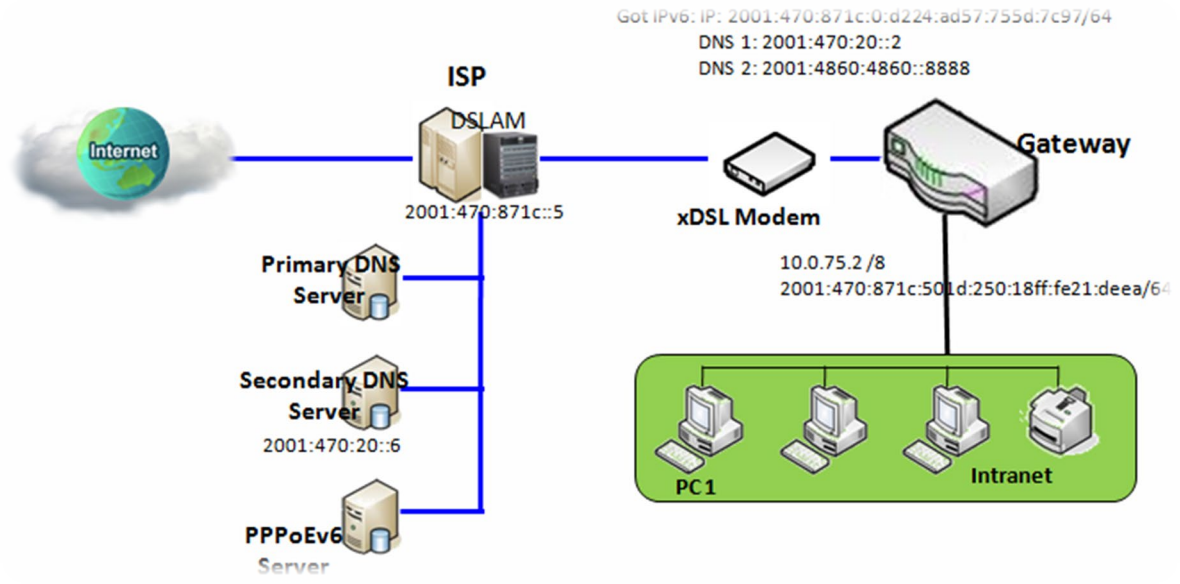
DHCP in IPv6 works the same as DHCP in IPv4. The DHCP server sends IP address, DNS server addresses and other data to the DHCP client for automatic configuration. The server also sends a lease time of the address and time to re-contact the server for IPv6 address renewal. The client then must resend a request to renew the IPv6 address.



The above diagram depicts DHCP IPv6 IP addressing: the DHCPv6 server from the ISP assigns an IPv6 address with the IPv6 default gateway address and IPv6 DNS server address to the client host.

PPPoEv6

PPPoEv6 in IPv6 works the same as PPPoE in IPv4. The PPPoEv6 server provides configuration parameters when the PPPoEv6 clients request for connection. After successful authentication with the client, the server sends IP address, DNS server addresses and other required parameters to the client.

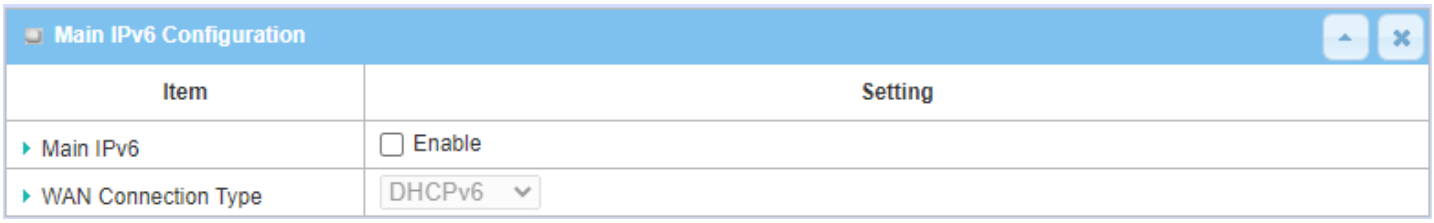


The diagram above depicts the IPv6 addressing through PPPoE. The PPPoEv6 server (DSLAM) from the ISP provides IPv6 configuration (including IP address, DNS server addresses and other required parameters) upon receiving PPPoEv6 client requests.

IPv6 Configuration Setting

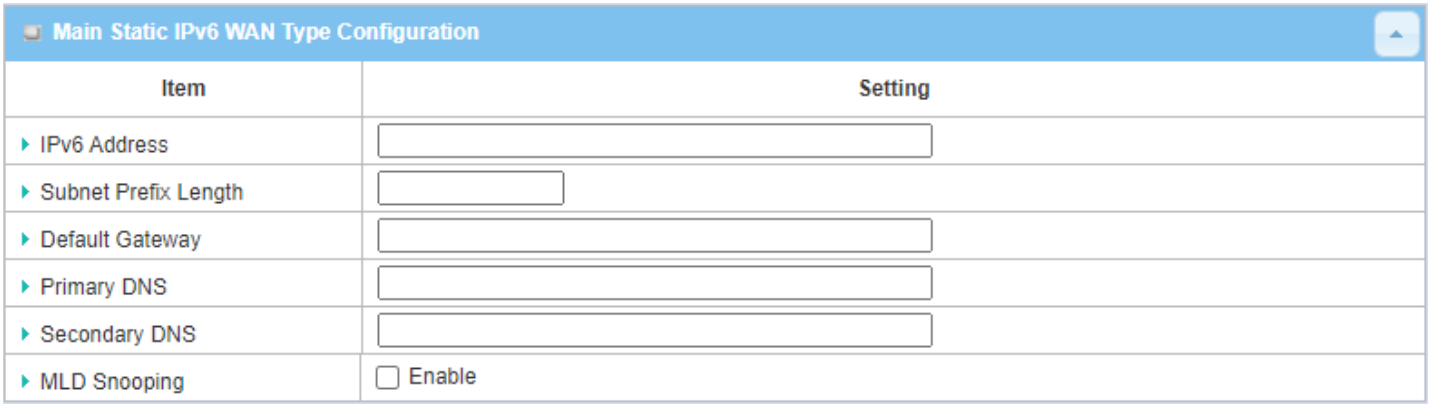
To access IPv6 Configuration page, go to **Basic Network > IPv6 > Configuration**.

The **IPv6 Configuration** setting allows you to set the IPv6 connection type to access the IPv6 network.
The gateway provides two types of IPv6 connections: Main IPv6 connection and Failover IPv6 connection.
Configure the Main IPv6 related settings first and then configure the Failover one to support failover operation.



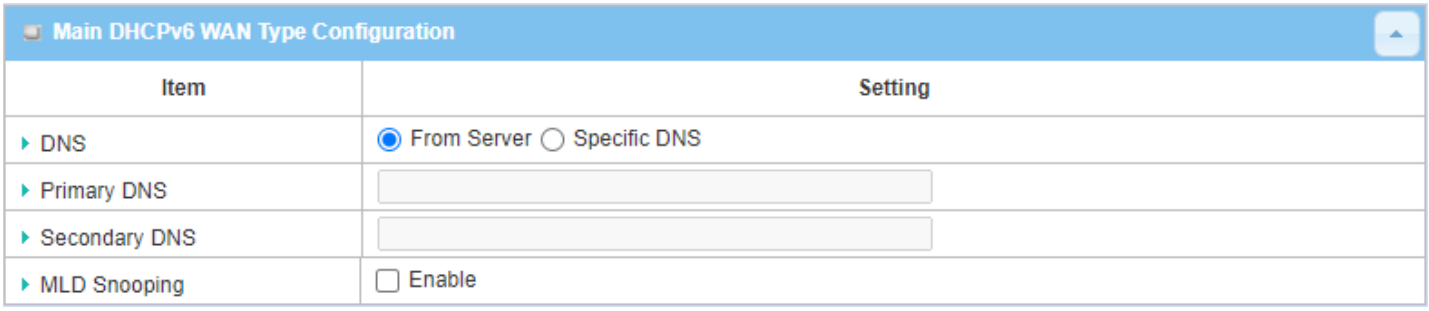
IPv6 Configuration		
Item	**Value setting**	**Description**
IPv6	The box is unchecked by default,	Activate the Main IPv6 function.
WAN Connection Type	1. A must-filled setting 2. DHCPv6 is selected by default	Define the selected IPv6 WAN Connection Type to establish the IPv6 connectivity via Main / Failover WAN Interface. The available WAN connection types are **Static IPv6**, **DHCPv6**, **PPPoEv6**, and **IPv6**. Select **Static IPv6** when your ISP provides you with a IPv6 address. Select **DHCPv6** when your ISP provides DHCPv6 services. Select **PPPoEv6** when your ISP provides you with PPPoEv6 account settings. Select **IPv6** when your ISP provides you with IPv6 (DHCPv6) services. **Note**: The available WAN connection types vary depending on the Interface type of corresponding WAN.

Static IPv6 WAN Type Configuration



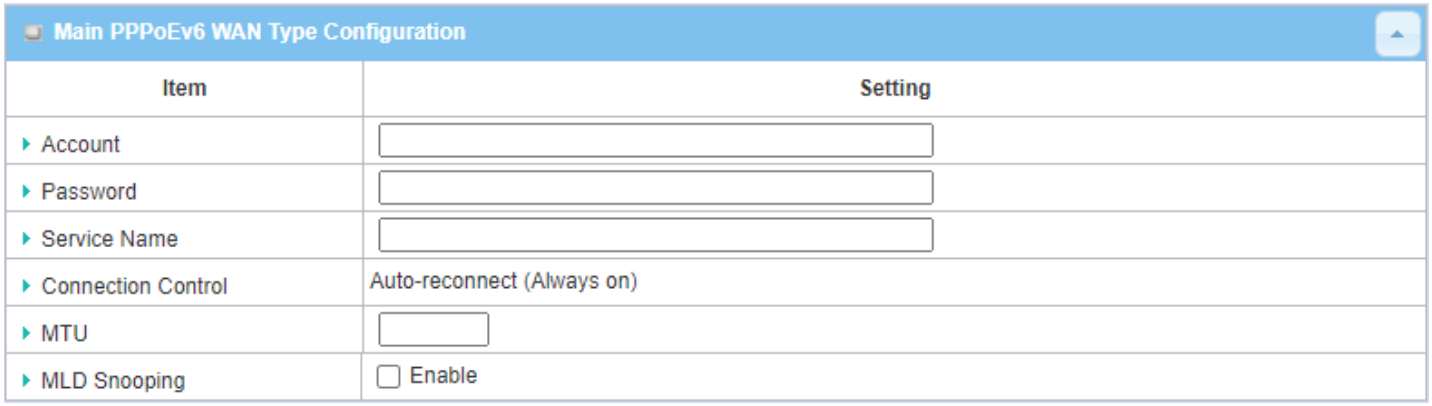
Static IPv6 WAN Type Configuration		
Item	**Value setting**	**Description**
IPv6 Address	A must-filled setting	Enter the **IPv6 Address** for the WAN interface.
Subnet Prefix Length	A must-filled setting	Enter the **Subnet Prefix Length** for the WAN interface.
Default gateway	A must-filled setting	Enter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

DHCPv6 WAN Type Configuration



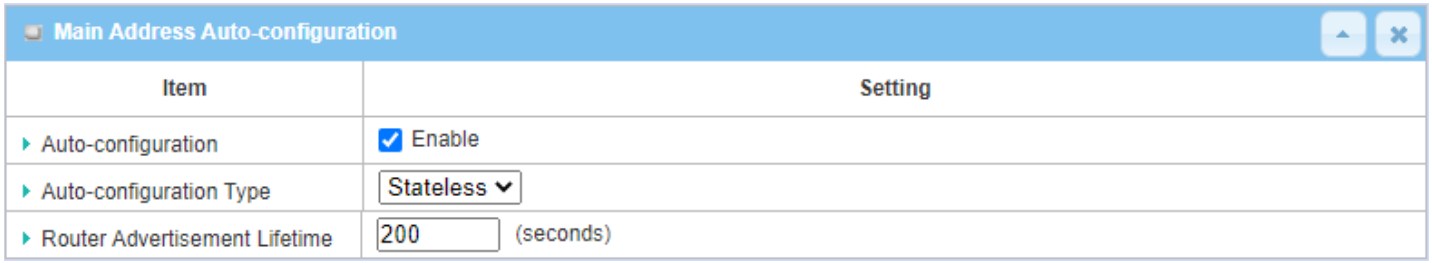
DHCPv6 WAN Type Configuration		
Item	**Value setting**	**Description**
DNS	The option [From Server] is selected by default	Select the [Specific DNS] option to activate the Primary DNS and Secondary DNS. Then fill in the DNS information.
Primary DNS	Can not be modified by default	Enter the **primary DNS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

PPPoEv6 WAN Type Configuration



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

Address Auto-configuration

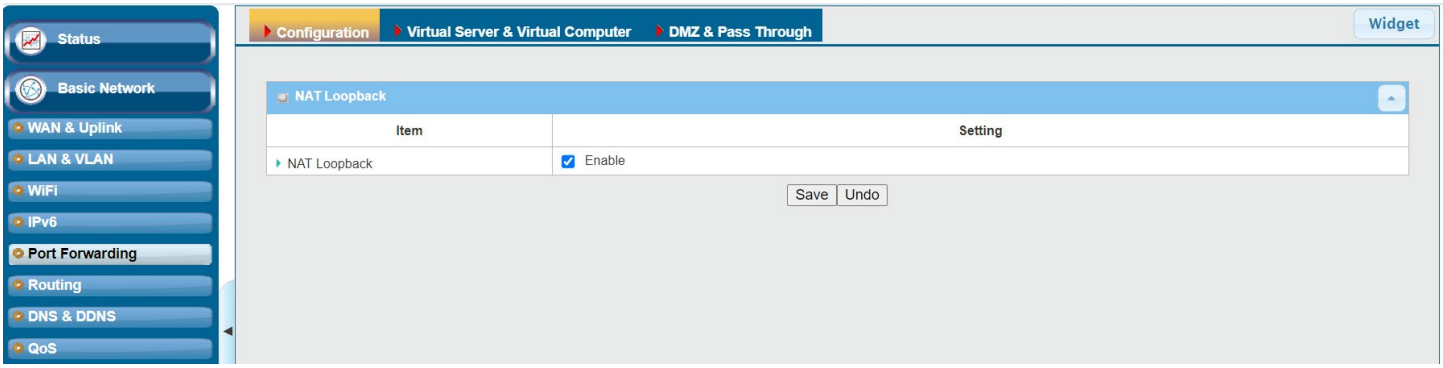


Address Auto-configuration		
Item	**Value setting**	**Description**
Auto-configuration	The box is unchecked by default	Enable the Auto configuration feature.
Auto-configuration Type	1. Only configurable when **Auto-configuration** is enabled	Define the selected IPv6 WAN Connection Type to establish the IPv6 connectivity. Select **Stateless** to manage the LAN using the SLAAC + RDNSS method and enter the below RA information.

	2. Stateless is selected by default	**gateway Advertisement Lifetime** (A must-filled setting): Enter the gateway Advertisement Lifetime (in seconds). 200 is set by default. *Value Range*: 0 ~ 65535. Select **Stateful** to manage the LAN using the **Stateful (DHCPv6)** method and ether the below IP range information. **IPv6 Address Range (Start)** (A must-filled setting): Enter the start IPv6 Address for the DHCPv6 range for your clients. 0100 is set by default. *Value Range*: 0001 ~ FFFF. **IPv6 Address Range (End)** (A must-filled setting): Enter the end IPv6 Address for the DHCPv6 range for your clients. 0200 is set by default. *Value Range*: 0001 ~ FFFF. **IPv6 Address Lifetime** (A must-filled setting): Enter the DHCPv6 lifetime for your clients. 36000 is set by default. *Value Range*: 0 ~ 65535.
Save		Save the configuration.

2.5 Port Forwarding

Network address translation (NAT) is the method of remapping one IP address space into another by modifying network address information in the Internet Protocol (IP) datagram packet headers. It is useful for conserving global address space and this is especially so since the IPv4 address has come to exhaustion. The product you purchased embeds and activates the NAT function. You can disable the NAT function by going to **Basic Network > WAN & Uplink > Connection Setup > WAN Type Configuration** page.



Usually all local hosts or servers behind a corporate gateway are protected a NAT firewall. A NAT firewall can filter unrecognized packets to protect your intranet. Port forwarding or port mapping is the function that redirects a communication request from one address to another. This technique is most commonly used to make services on a host residing on a protected or internal network available to hosts in external network by remapping the destination IP address and port number.

2.5.1 Configuration

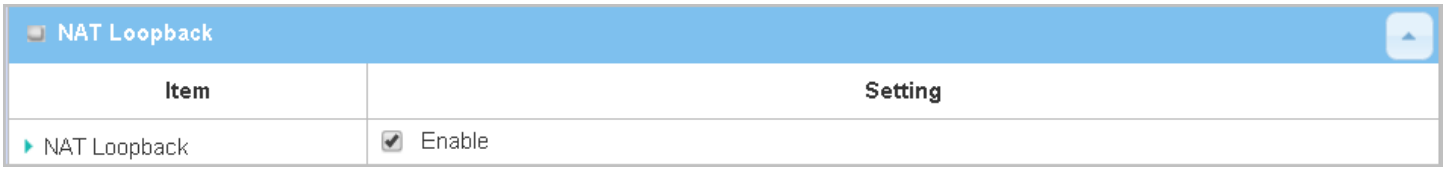
NAT Loopback

This feature allows you to access a WAN IP address from your local network with NAT. It is useful when you run a server on the LAN; you can access this server without changing the IP address no matter from the public Internet or from the LAN.

Configuration Setting

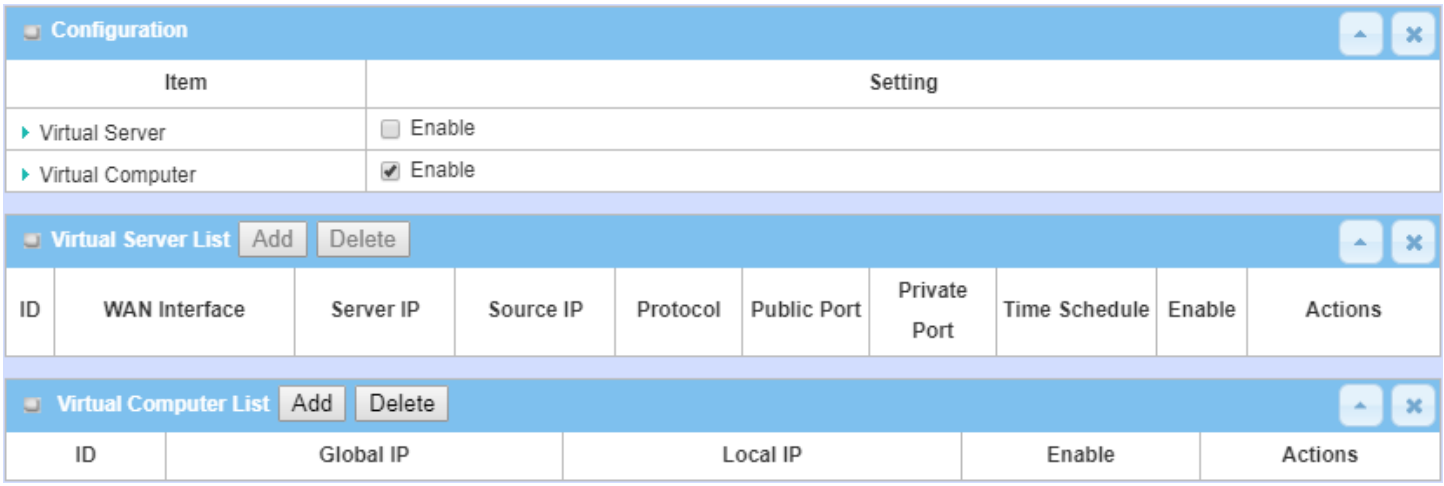
Go to Basic **Network > Port Forwarding > Configuration** to access the NAT Loopback page.

Enable NAT Loopback



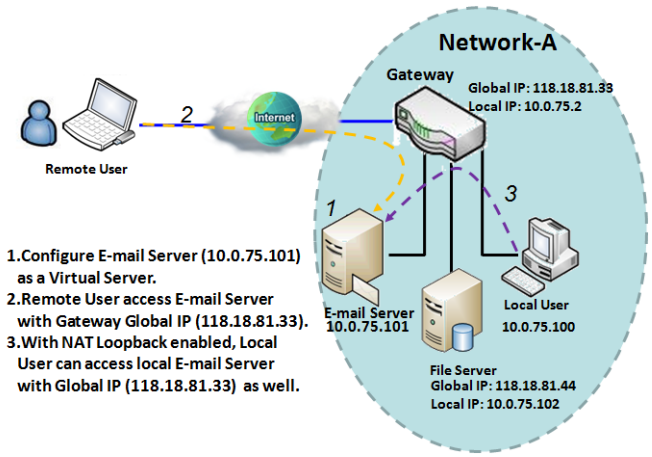
Configuration Item	Value setting	Description
NAT Loopback	The box is checked by default	Activate this NAT function
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings

2.5.2 Virtual Server & Virtual Computer



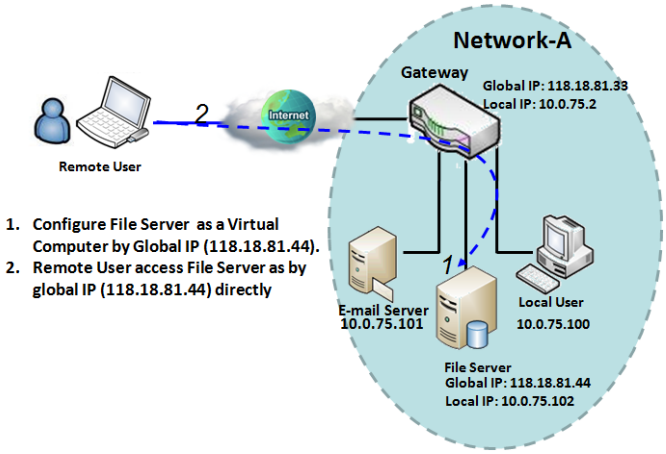
Virtual servers satisfy the need for access to servers behind the gateway from a public network. On the other hand, "Virtual Computer" is a host behind the gateway but with a global IP address. They both are protected by the gateway implemented with NAT and firewall. To configure Virtual Computer, you need to map the local IP of the virtual computer to a global IP.

Virtual Server & NAT Loopback



"Virtual Server" allows you to access servers hosted behind the gateway with a global IP address or FQDN. The gateway serves service requests from the Internet using port forwarding. As shown in the example, an E-mail virtual server having an IP address 10.0.75.101 in the Intranet of Network-A can be accessed using the gateway's global IP address 118.18.81.33. In addition, your local devices an access this mail server using the same global IP address if the NAT loopbck feature is enabled.

Virtual Computer

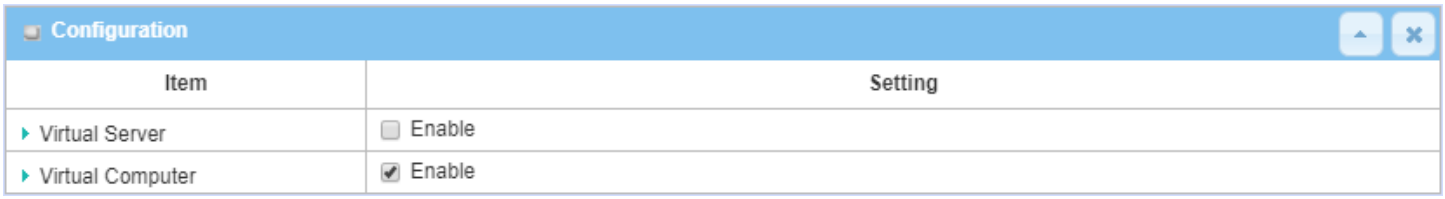


"Virtual Computer" allows you to map LAN hosts to global IP addresses, so that they can be visible to the public network while being protected by the gateway's firewall. For example, if you set an FTP file server with a local IP address (10.0.75.102) and a global IP address (118.18.82.44), a remote user can access the file server using its global IP address even though it is hidden behind the gateway.

Virtual Server & Virtual Computer Setting

Go to **Basic Network > Port Forwarding > Virtual Server & Virtual Computer** to access the Virtual Server and Virtual Computer page.

Enable Virtual Server and Virtual Computer



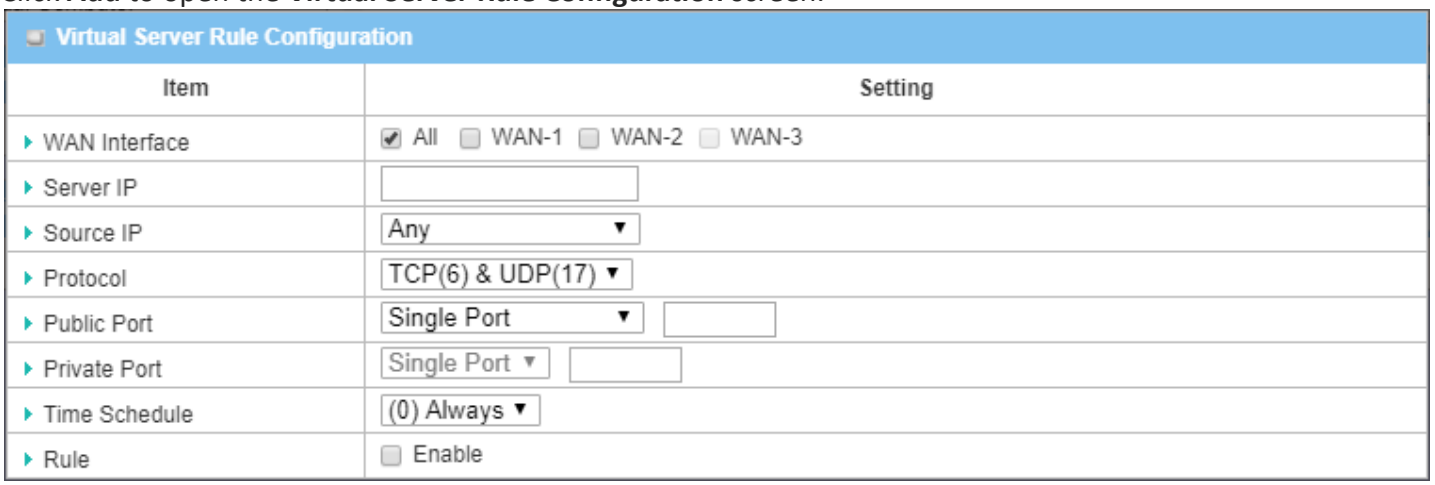
Configuration Item	Value setting	Description
Virtual Server	The box is unchecked by default	Activate Virtual Server to use port forwarding.
Virtual Computer	The box is checked by default	Activate the Virtual Computer function.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings.

Create / Edit Virtual Server

The gateway allows you to create Virtual Server rules. It supports up to a maximum of 20 Virtual Server rules.



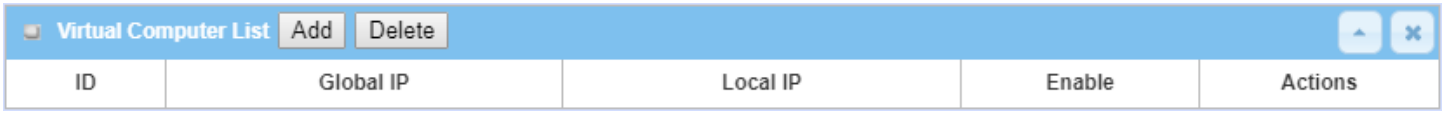
Click **Add** to open the **Virtual Server Rule Configuration** screen.



Virtual Server Rule Configuration Item	Value setting	Description
WAN Interface	1. A must-filled setting 2. Default is **ALL**.	Select an interface to be the one for the incoming packets. Select **ALL** for packets coming into the gateway from any interface. **Note**: The available interfaces depend on the number of available WAN interfaces of the device.
Server IP	A must-filled setting	Specify the IP address of the WAN interface selected.
Source IP	1. A must-filled setting 2. By default **Any** is selected	Specify the **Source IP address**. Select **Any** to allow access coming from any IP address. Select **Specific IP Address** to allow access coming from an IP address. Select **IP Range** to allow access coming from a specified range of IP address.
Protocol	1. A must-filled setting 2. **TCP & UDP** is selected by default.	Select **"ICMPv4"** as the protocol used for packet filtering. Select "TCP" or "UDP" as the protocol used for virtual server. Define the port number used for this service: Specify a **Public Port** pre-defined from **Well-known Service** and a corresponding **Private Port**. Specify a **Single Port** and a correspoing **Private Port**. Specify a **Public Port Range** and a corresponding **Private Port** with a **Single Port** or **Port Range**. *Value Range*: 1 ~ 65535 for Public Port and Private Port. Select **"GRE"** as the protocol for this service.
		Select **"ESP"** as the protocol for this service. When **"SCTP"** as the protocol for this service. Select **"User-defined"** and enter the **Protocol Number** for this service.
Time Schedule	1. An optional setting 2. **(0) Always** Is selected by default.	You can apply **Time Schedule** to this rule, otherwise leave it as **Always** (refer to **Scheduling setting** under **Object Definition**).
Rule	1. An optional setting 2.The box is unchecked by default.	Activate this rule.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings and return to previous page.

Create / Edit Virtual Computer

The gateway allows you to create your Virtual Computer rules. It supports a maximum of 20 rules.



Click **Add** to open the **Virtual Computer Rule Configuration** screen.

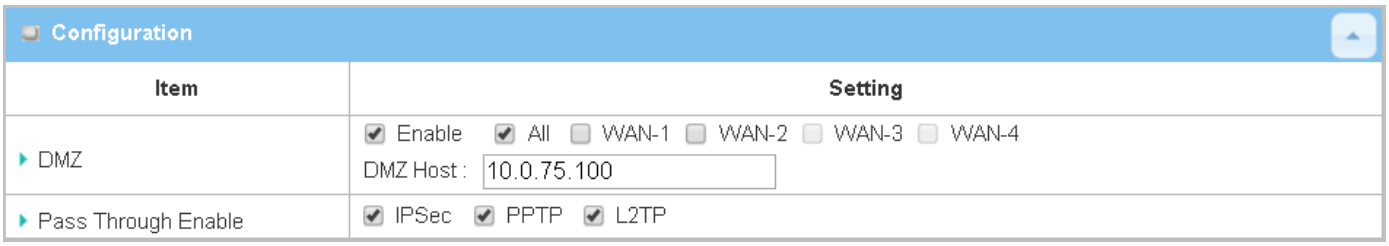


Virtual Computer Rule Configuration

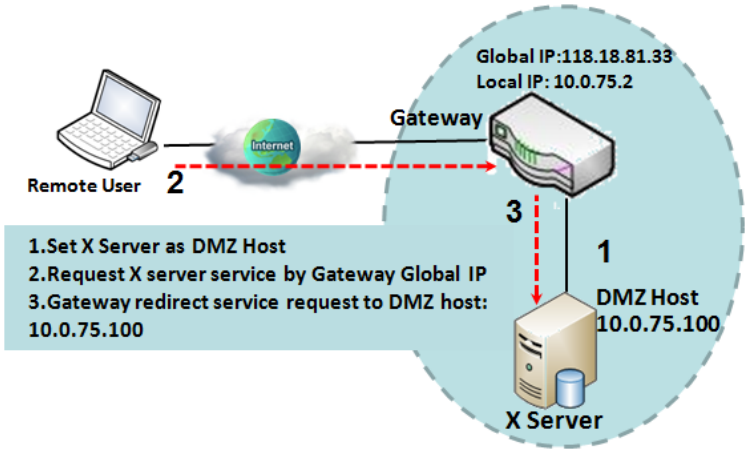
Item	Value setting	Description
Global IP	A must-filled setting	Specify the WAN IP of the virtual computer.
Local IP	A must-filled setting	Specify the LAN IP of the virtual computer.
Enable	N/A	Enable this rule.
Save	N/A	Save the settings.

2.5.3 DMZ & Pass Through

The DMZ (De Militarized Zone) allows a host behind a gateway to be exposed to the Internet but still protected by the gateway's firewall. It allows a computer to execute 2-way communication for Internet games, video conferencing, Internet telephony and other applications.
The DMZ function allows you to direct all packets to the DMZ host protected the gateway when these packets are not to be received by applications in the gateway or by other client hosts.

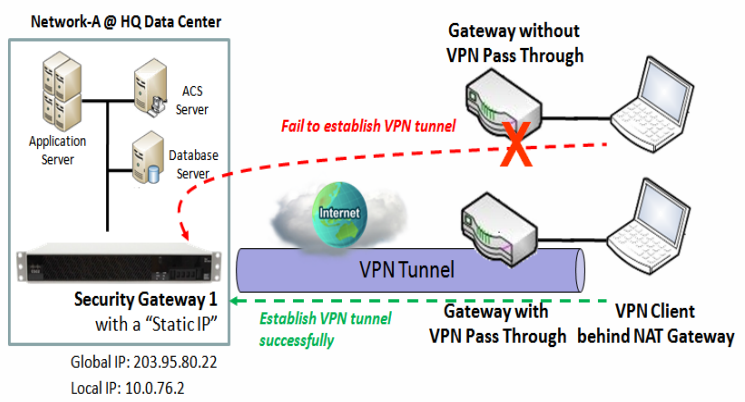


DMZ Scenario



As shown in the diagram, server X is installed as the DMZ host with an IP address of 10.0.75.100. And remote users can request services from X server with a global IP address 118.18.81.33. Packets not destined to any configured virtual server or applications will be directed to the DMZ host.

VPN Pass through Scenario

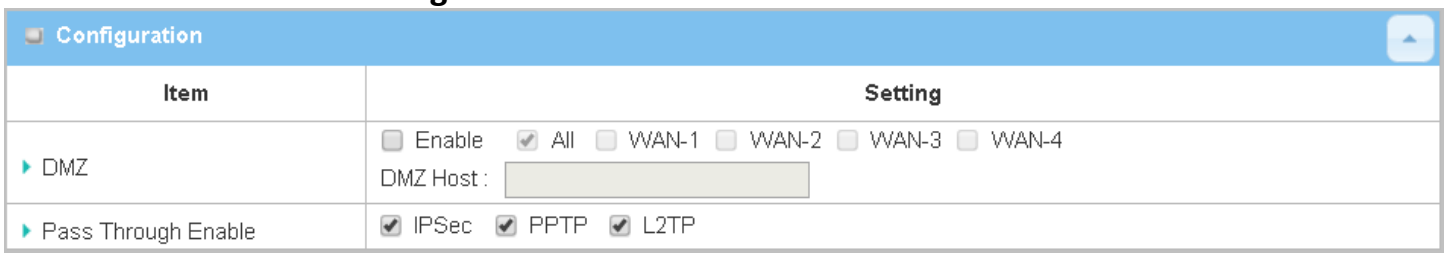


To support for the VPN connections initiating from VPN clients behind NAT gateway, the gateway must implement some kind of VPN pass-through function for such uses. The gateway supports the pass-through function for IPSec, PPTP, and L2TP connections.

DMZ & Pass Through Setting

Go to **Basic Network > Port Forwarding > DMZ & Pass Through** to access the DMZ & Pass Through page.

Enable DMZ and Pass Through



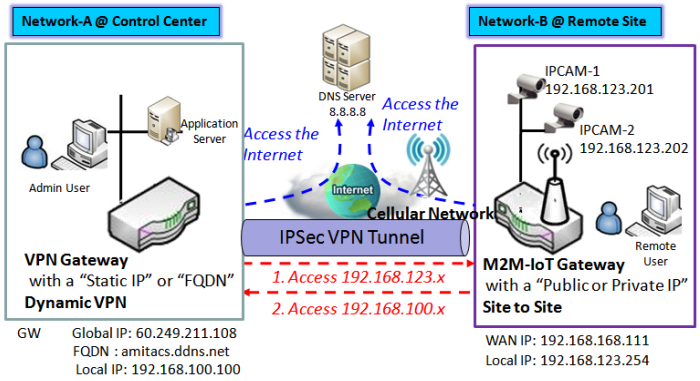
Configuration Item	Value setting	Description
DMZ	1. A must-filled setting 2. Default is **ALL**.	Select an interface to apply the DMZ function. Select **ALL** for packets coming into the gateway from any interface. **Note**: The available interfaces depend on the number of available WAN interfaces of the device.
Pass Through Enable	The boxes are checked by default	Check the box to enable pass-through for **IPSec**, **PPTP**, and **L2TP**. With the pass-through function enabled, the VPN hosts behind the gateway can connect to remote VPN servers.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings

2.5.5 IP Translation

IP Translation is slimier to One-to-One NAT where you can map multiple public IP addresses to individual LAN devices to create a one-to-one mapping between a public IP address and a private IP address of a local host. Note that the availability of this function depends on the product model.

IP Translation | Add | Delete

ID	Mapping Source IP/Domain Name	Mask	Mapping Destination IP/Domain Name	Mask	Physical interface	Description	Enable	Actions
1	1.1.1.8	255.255.255.255	8.8.8.8	255.255.255.255	All	DNS Server	☑	Edit ☐ Select
2	1.1.1.201	255.255.255.255	192.168.123.201	255.255.255.255	All	Remote IPCam-1	☑	Edit ☐ Select
3	1.1.1.202	255.255.255.255	192.168.123.202	255.255.255.255	All	Remote IPCam-2	☑	Edit ☐ Select



From Control Center to Remote Site

1. Admin user can ping DNS Server by mapped IP Address 1.1.1.8 instead of 8.8.8.8
2. Admin User in Control Center also can manage remote IPCam via VPN Tunnel directly by mapped IP Address 1.1.1.201 instead of 192.168.123.201
   IP Address 1.1.1.202 instead of 192.168.123.202

From Remote Site to Control Center

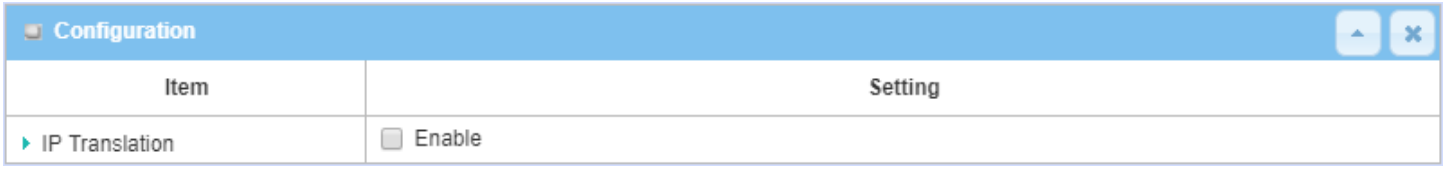
1. Remote User can manage remote VPN Gateway, GUI,SSH directly by mapped specific IP Address 1.1.1.1 instead of FQDN amitacs.ddns.net

As shown in above configuration settings from the VPN gateway at the Control Center, DNS Servers and remote IP Cameras can be accessed with the mapped IP addresses instead of their real IP address 192.168.123.xxx.

IP Translation Setting

Go to Basic **Network > Port Forwarding > IP Translation** to access the IP Translation Setting. Note that the availability of this function depends on product model.

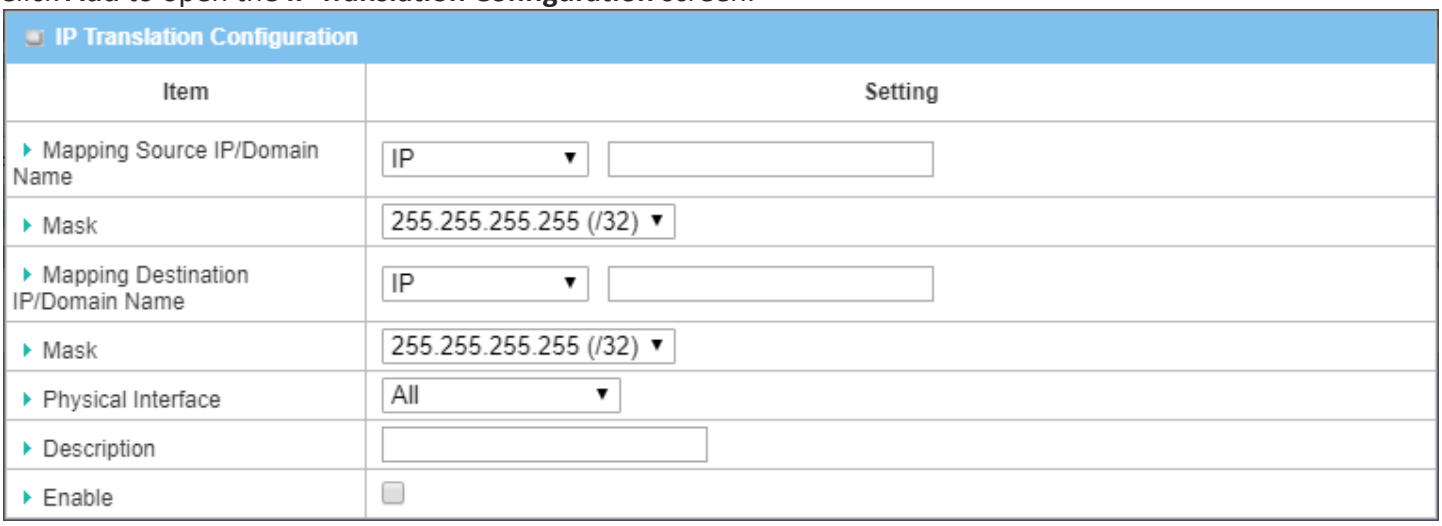
Enable IP Translation



Configuration Item	Value setting	Description
IP Translation	The box is unchecked by default	Activate the IP translation function
Save	N/A	Save the settings.

Create / Edit IP Translation Rule

Click **Add** to open the **IP Translation Configuration** screen.



IP Translation Configuration Item	Value setting	Description
Mapping Source IP/Domain Name	1. A must-filled setting 2.**IP** is selected by default.	Specify the mapped **IP** / **Domain Name** that will be issued from the hosts behind the NAT gateway. The NAT gateway will translate the specified source IP/Domain Name into the real IP/Domain Name.
Mask	1. A must-filled setting 2.**255.255.255.255(/32)** is selected by default.	Enter the required subnet mask if **Source IP** is specified above. Use 255.255.255.255 (/32) to indicate a single IP address.

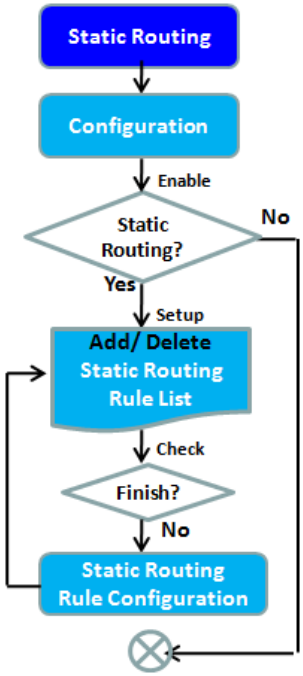
Mapping Destination IP/Domain Name	1. A must-filled setting 2.**IP** is selected by default.	Specify the expected real target IP / **Domain Name** that will be used to replace the original one that is issued by the hosts behind the NAT gateway.
Mask	1. A must-filled setting 2.**255.255.255.255(/32)** is selected by default.	Enter the required subnet mask if **Destination IP** is specified above. Use 255.255.255.255 (/32) to indicate a single IP address.
Physical Interface	1. A must-filled setting 2.**All** is selected by default.	Specify the interface to apply the translation rule. The enabled WAN Interface will be available in the dropdown list. By default, **All** is selected, and the translation rule will be applied to the traffic passing through all WAN interfaces.
Description	An optional setting.	Specify a brief description or rule name for this IP Translation rule.
Enable	The box is unchecked by default	Activate the translation rule.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings

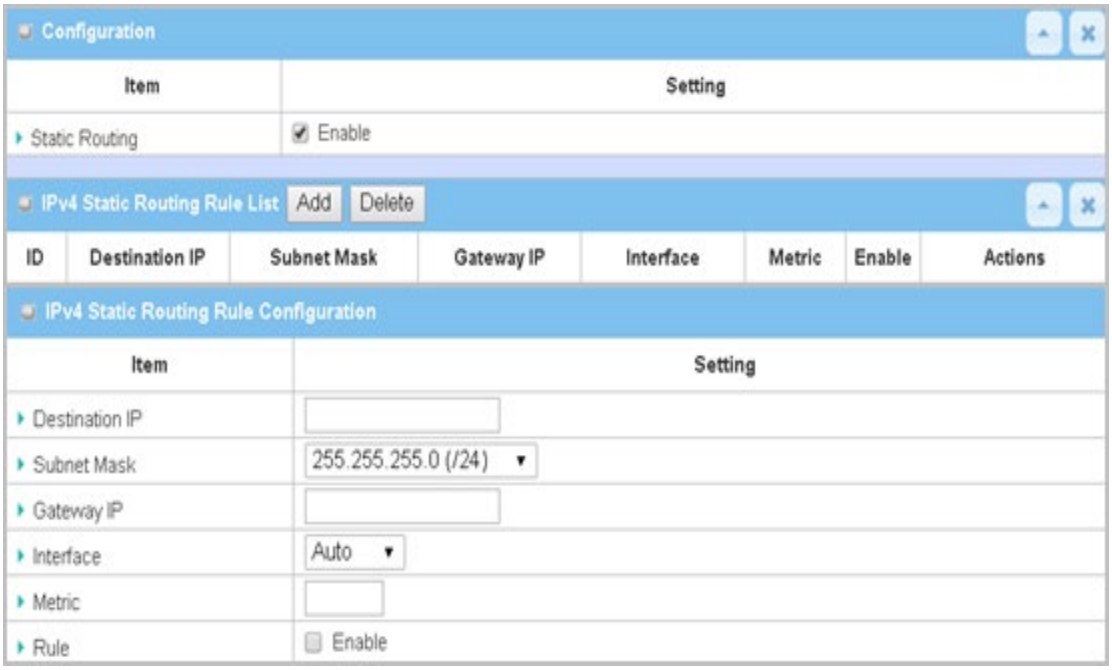
2.6 Routing

Routing allows packets to find proper path among different subnets to facilitate communication across gateways. Routing is the process of selecting best paths in a network. It is performed by different kinds of networks, including electronic data networks (such as the Internet), 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. Efficient routing relies on the correct construction of the routing tables, which are held in the gateway's memory. Most routing algorithms use only one network path at a time.

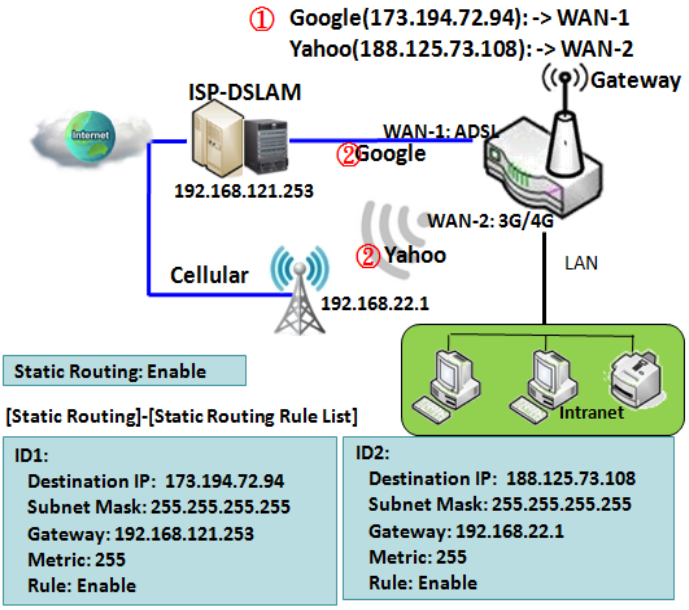
Static routing records your pre-defined routing paths for specific destination subnets. On the other hand, dynamic routing maintains the routing tables with routing paths obtained from neighbor gateways. RIP, OSPF and BGP are all dynamic routing techniques. In addition, the gateway is also built with an advanced routing software called Quagga for more complex routing applications.

2.6.1 Static Routing





"Static Routing" function lets you define the routing paths for dedicated hosts/servers or subnets. The gateway then routes incoming packets to peer gateways according to the records of the routing table.



The "Static Routing" feature allows dedicated traffic flows from the Intranet to be routed to their destination via a designated peer gateway.

As shown in the diagram, rule 1 sets the interface ADSL as the forwarding interface for traffic destined for Google. Rule 2 sets 3G/4G as the forwarding interface for traffic destined for Yahoo.

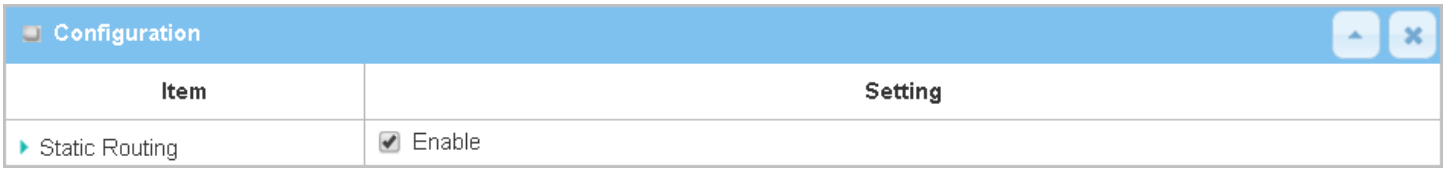
Static Routing Setting

Go to **Basic Network** > **Routing** > **Static Routing** to access the Static Routing Setting page.

There are three configuration windows for static routing feature: "Configuration", "Static Routing Rule List" and "Static Routing Rule Configuration". The "Configuration" window lets you activate the global static routing feature. The "Static Routing Rule List" window lists all your defined static routing rules.

Click **Add** or **Edit** to open the "Static Routing Rule Configuration" window to define a static routing rule.

Enable Static Routing



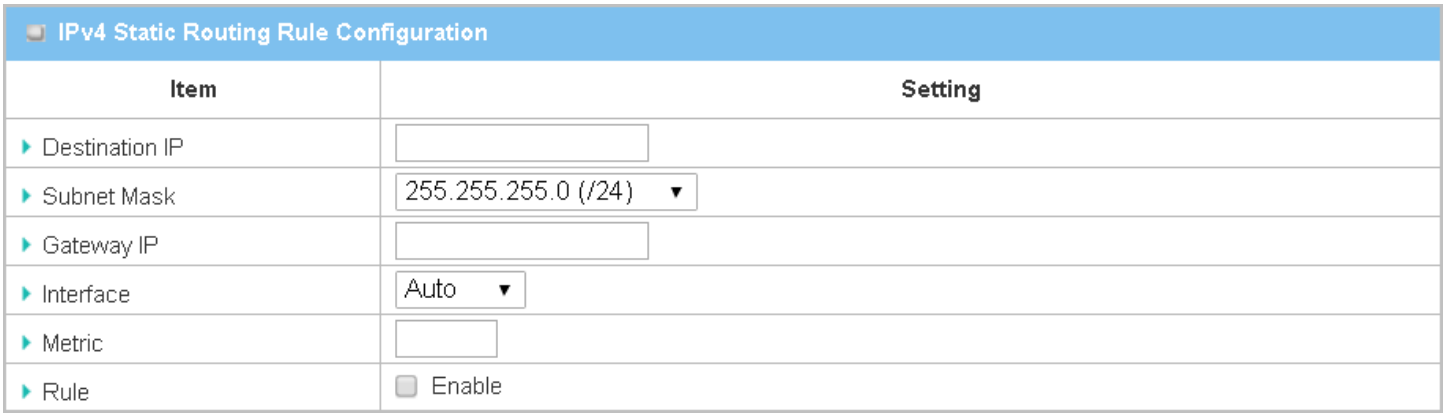
Static Routing Item	Value setting	Description
Static Routing	The box is unchecked by default	Activate this function

Create / Edit Static Routing Rules

The Static Routing Rule List shows the parameters of all static routing rules. To configure a static routing rule, you must specify related parameters including the destination IP address and subnet mask, the IP address of peer gateway, and the metric.

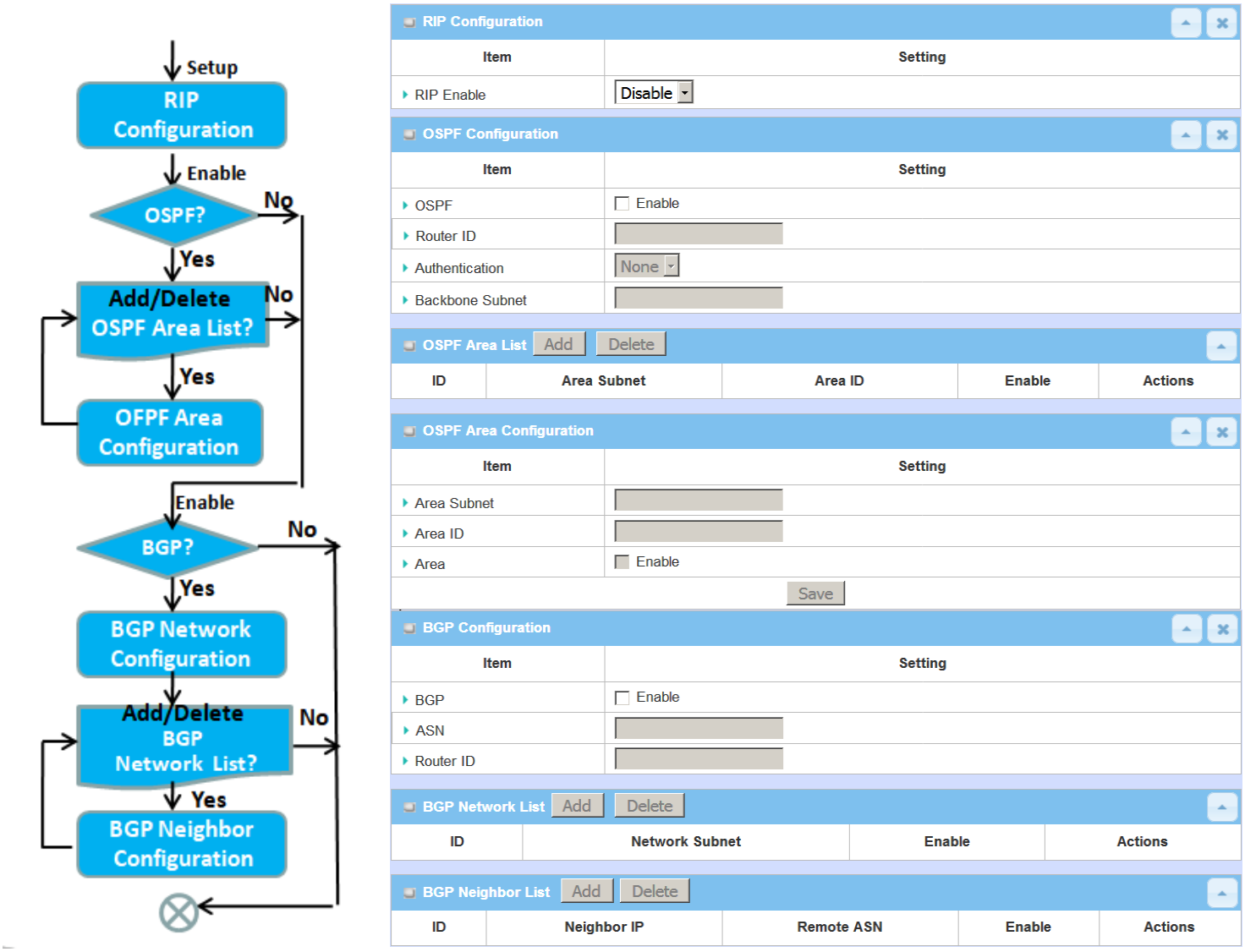


The gateway supports a maximum of 64 rule sets. Click **Add** to open the **Static Routing Rule Configuration** screen.



IPv4 Static Routing		
Item	**Value setting**	**Description**
Destination IP	1. IPv4 Format 2. A must-filled setting	Specify the Destination IP address of this static routing rule.
Subnet Mask	255.255.255.0 (/24) is set by default	Specify the Subnet Mask of this static routing rule.
Gateway IP	1. IPv4 Format 2. A must-filled setting	Specify the gateway IP address of this static routing rule.
Interface	Auto is set by default	Select the Interface to apply this static routing rule. It can be **Auto**, or one of the available WAN / LAN interfaces.
Metric	1. Numberic String Format 2. A must-filled setting	Select the metric of this static routing rule. Value Range: 0 ~ 255.
Rule	The box is unchecked by default.	Activate this rule.
Save	NA	Save the configuration
Undo	NA	Restore to the previous settings.
Back	NA	Return to the Static Routing Configuration page.

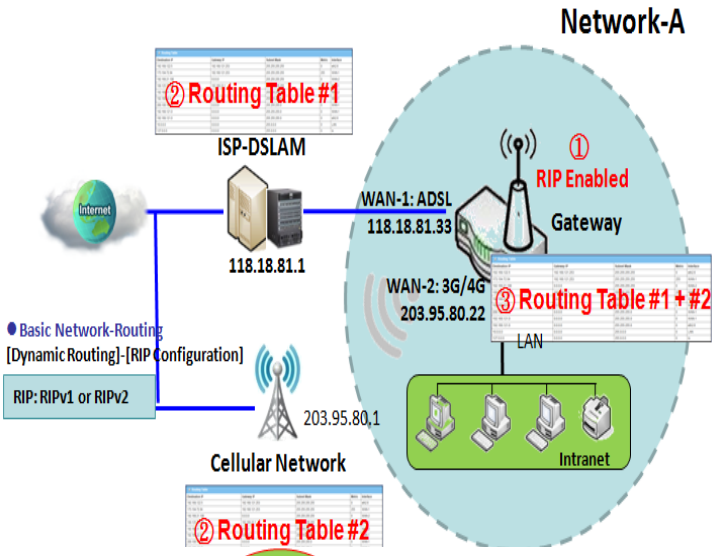
2.6.2 Dynamic Routing



This gateway supports dynamic routing protocols, including RIPv1/RIPv2 (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border gateway Protocol), to establish routing table automatically. Generally speaking, RIP is suitable for small network while OSPF and BGP are more suitable for medium to large network infrastructures.

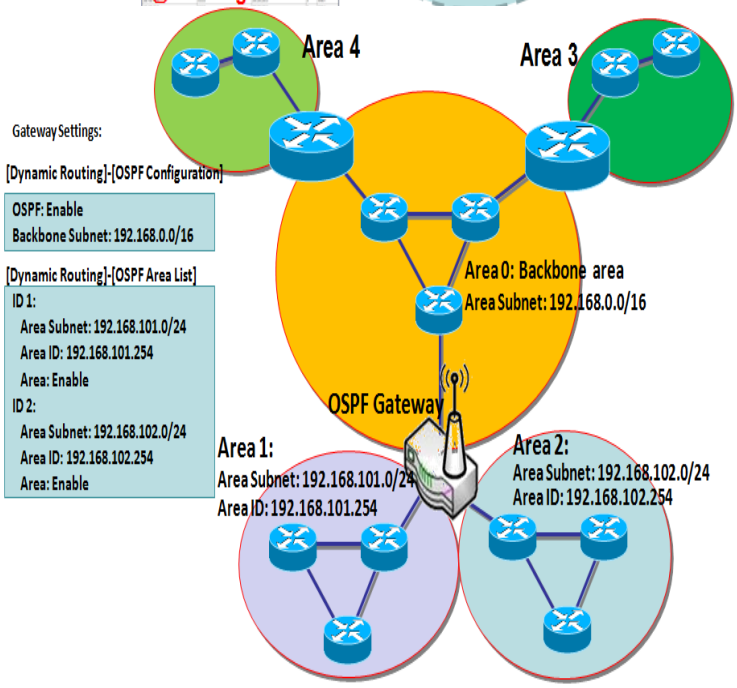
The supported dynamic routing protocols are described as follows.

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, which also means the route is unreachable. RIP also implements the split horizon, route poisoning and hold-down mechanisms to prevent incorrect routing information from being propagated.

OSPF Scenario

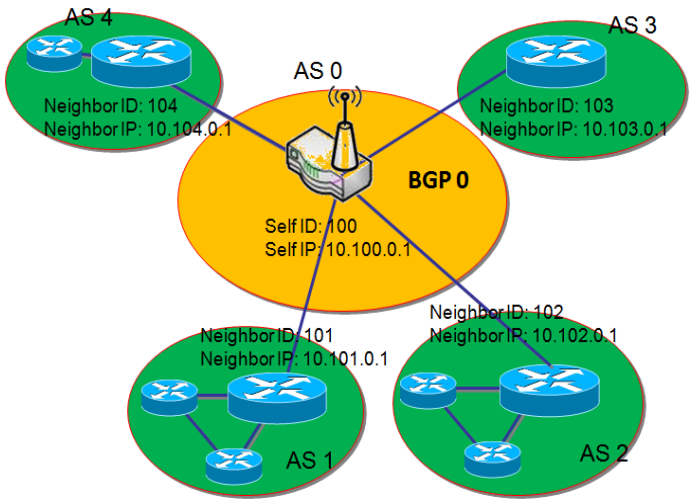


Open Shortest Path First (OSPF) is a routing protocol that uses link state routing algorithm. It is the most widely used interior gateway protocol (IGP) in large enterprise networks. It gathers link state information from available gateways and constructs a topology map of the network. The topology is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

A OSPF gateway in a large enterprise network can obtain routing tables from the enterprise backbone, and forward routing information to other gateways. 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 gateways in area 1 and area 2.

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 forwards traffic on the basis of routing paths, network policies, or rules.

Most ISPs use BGP to establish routing between one another (especially for multi-homed networking). A very large private IP network can also use BGP to link major BGP gateways within one AS to other border gateways for route exchange within a local network.

As shown in the diagram, BGP 0 is a gateway that resides in AS0 (self IP:10.100.0.1 and self ID:100). It also links with other BGP gateways over the Internet. The scenario is used to link subnets from an ISP to other ones in other ISPs. BGP 0 can gather routing information from other BGP gateways. It then forwards the routing data to the gateways in its AS. Finally, the gateways resided in AS 0 know how to route packets to other AS.

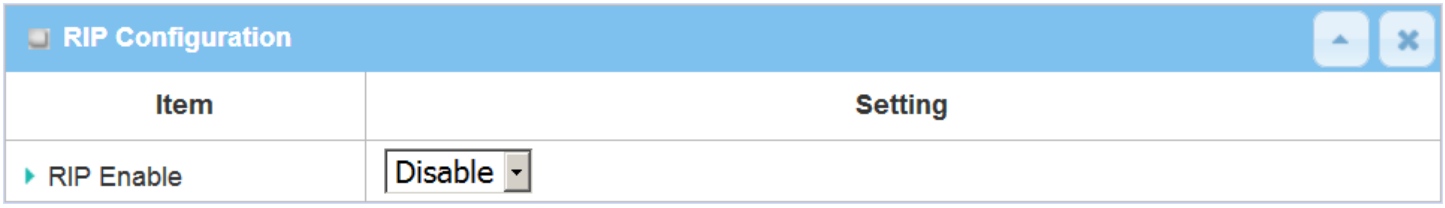
Dynamic Routing Setting

Go to **Basic Network** > **Routing** > **Dynamic Routing** to access the Dynamic Routing Setting page.

The dynamic route setting allows you to enable and configure RIP, OSPF, and BGP on the gateway.
In the "Dynamic Routing" page, there are several configuration windows for dynamic routing: the "RIP Configuration" window, "OSPF Configuration" window, "OSPF Area List", "OSPF Area Configuration", "BGP Configuration", "BGP Neighbor List" and "BGP Neighbor Configuration" window.

RIP Configuration

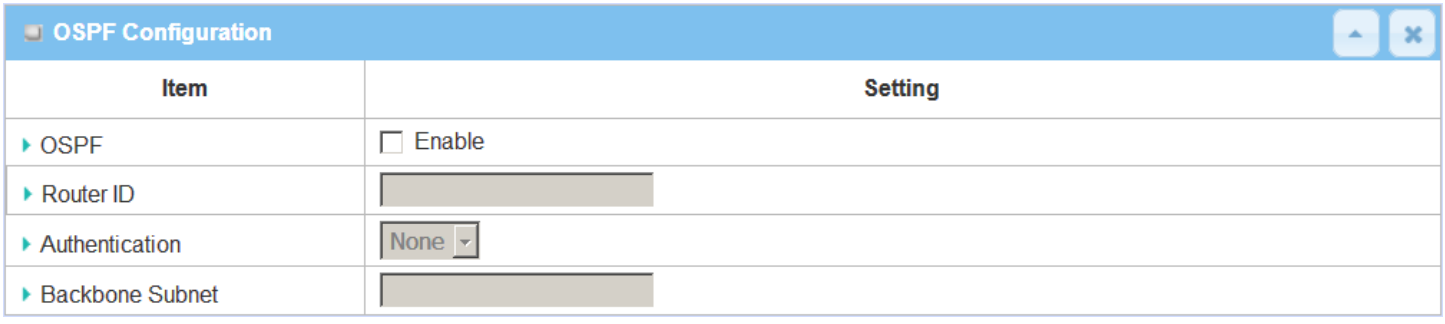
The RIP configuration setting allows you to enable RIP on the gateway.



RIP Configuration		
Item	**Value setting**	**Description**
RIP Enable	Disable is set by default	Select **Disable** or select the corresponding **RIP versions** to be enabled.

OSPF Configuration

The OSPF configuration setting allows you to enable and specify OSPF parameters on the gateway.

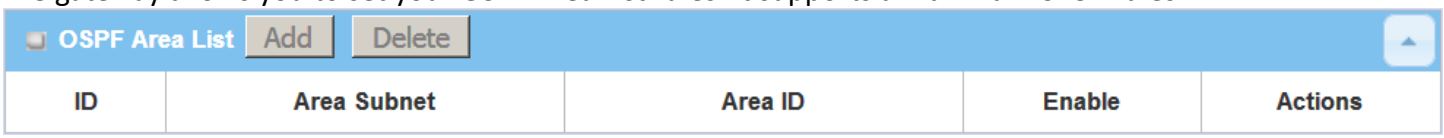


OSPF Configuration		
Item	**Value setting**	**Description**
OSPF	Disable is set by default	Activate the OSPF protocol.
Gateway ID	1. IPv4 Format 2. A must-filled setting	Enter the gateway ID of this gateway.
Authentication	None is set by default	Select **None** to disable Authentication for OSPF.

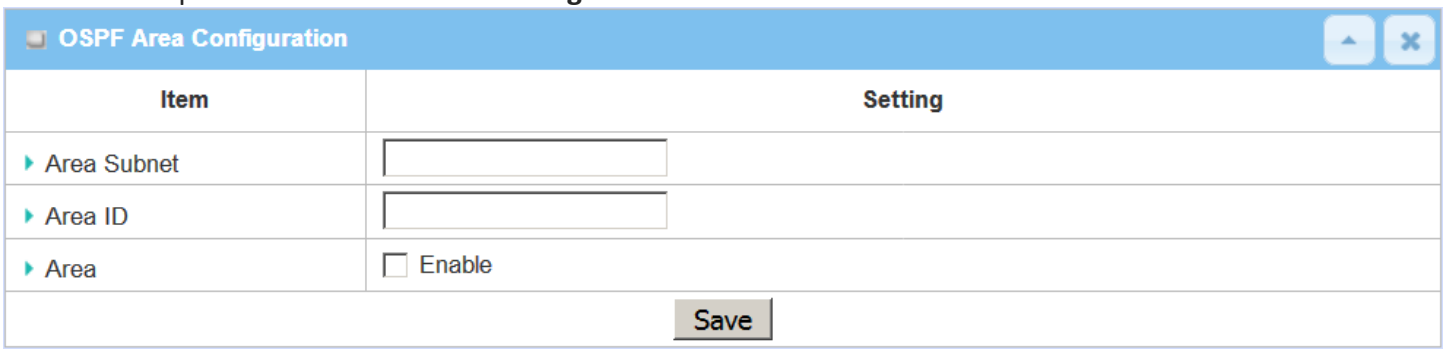
		Select **Text** to enable Text Authentication and enter a Key for OSPF. Select **MD5** to enable MD5 Authentication and enter the ID and Key for OSPF.
Backbone Subnet	1. Backbone Subnet 2. A must-filled setting	Enter the Backbone Subnet (CIDR notation) of this gateway for OSPF, for example, 192.168.1.0/24.

Create / Edit OSPF Area Rules

The gateway allows you to set your OSPF Area List rules. It supports a maximum of 32 rules.



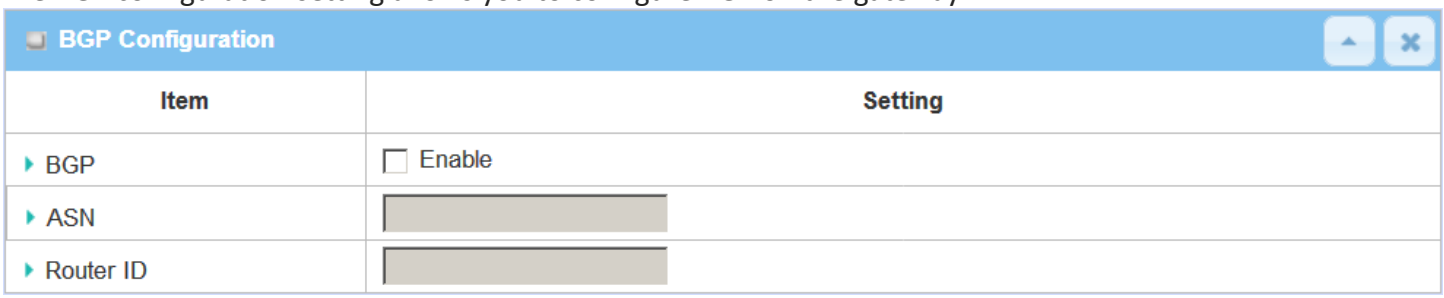
Click **Add** to open the **OSPF Area Rule Configuration** screen.



OSPF Area Configuration		
Item	**Value setting**	**Description**
Area Subnet	1. Subnet Mask Notation. (Ex: 192.168.1.0/24) 2. A must-filled setting	Enter the Area Subnet (CIDR notation) of this gateway for OSPF, for example, 192.168.1.0/24.
Area ID	1. IPv4 Format 2. A must-filled setting	Enter the Area ID for an OSPF Area.
Area	The box is unchecked by default.	Activate this rule.
Save	N/A	Save the configuration.

BGP Configuration

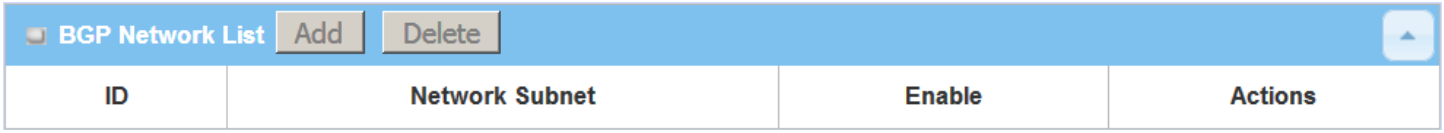
The BGP configuration setting allows you to configure BGP on the gateway.



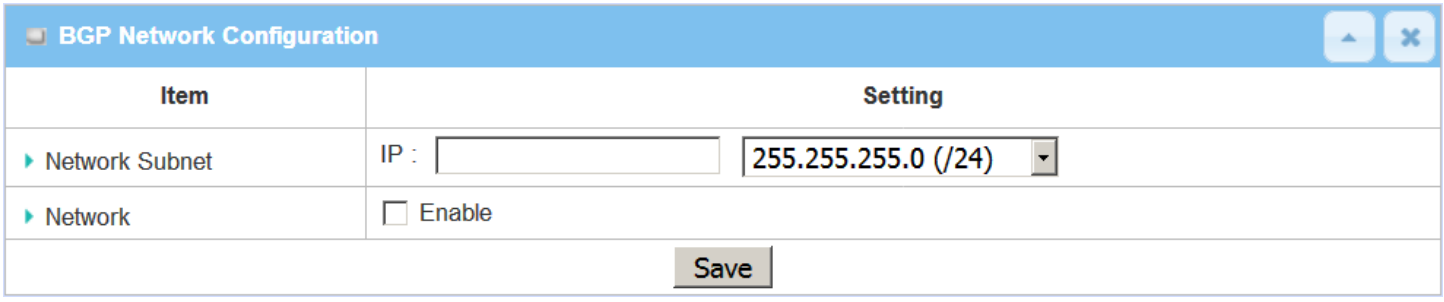
BGP Network Configuration		
Item	**Value setting**	**Description**
BGP	The box is unchecked by default	Activate BGP.
ASN	1. Numberic String format 2. A must-filled setting	Configures a BGP routing process with an autonomous-system-number. *Value Range*: 1 ~ 4294967295.
Gateway ID	1. IPv4 Format 2. A must-filled setting	Enter a fixed 32-bit router ID as the identifier of the local BGP router/gateway.

Create / Edit BGP Network Rules

The gateway allows you to enable BGP and configure BGP parameters. It supports a maximum of 32 rule sets.



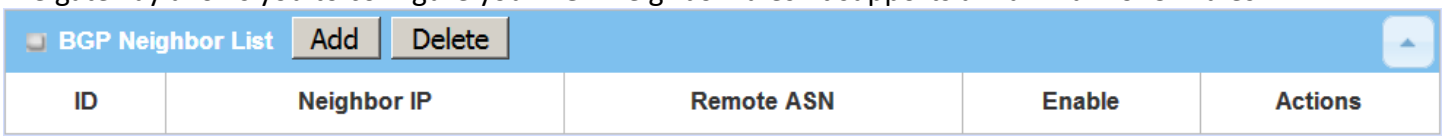
Click **Add** to open the **BGP Network Configuration** screen.



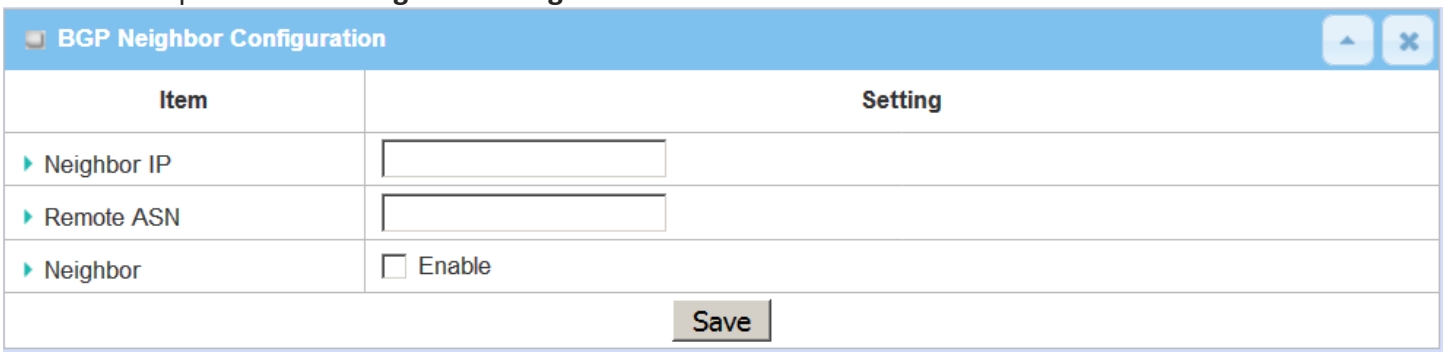
Item	Value setting	Description
Network Subnet	1. IPv4 Format 2. A must-filled setting	Specifies a local network to this autonomous system and adds it to the BGP routing table.
Network	The box is unchecked by default.	Activate this rule.
Save	N/A	Save the configuration

Create / Edit BGP Neighbor Rules

The gateway allows you to configure your BGP Neighbor rules. It supports a maximum of 32 rules.



Click **Add** to open the **BGP Neighbor Configuration** screen.



BGP Neighbor Configuration		
Item	**Value setting**	**Description**
Neighbor IP	1. IPv4 Format 2. A must-filled setting	Adds the IP address of the neighbor in the below specified autonomous system to the BGP neighbor table of the local router.
Remote ASN	1. Numberic String Format 2. A must-filled setting	The Remote autonomous-system-number of the BGP Neighbor. *Value Range*: 1 ~ 4294967295.
Neighbor	The box is unchecked by default.	Activate this rule.
Save	N/A	Save the configuration.

2.6.3 Routing Information

The routing information allows you to view the routing table and policy route information. Policy Routing Information is only available when the Load Balancing function is enabled and the Load Balance Strategy is set as User Policy.

Go to **Basic Network > Routing > Routing Information** to access the Routing Information page.

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	Destination IP in IPv4 format of this route.
Subnet Mask	N/A	Subnet Mask in IPv4 format of this route.
Gateway IP	N/A	The gateway's IP in IPv4 format of this route.
Metric	N/A	The Metric of this route.
Interface	N/A	The Interface Type of this route.

Policy Routing Information

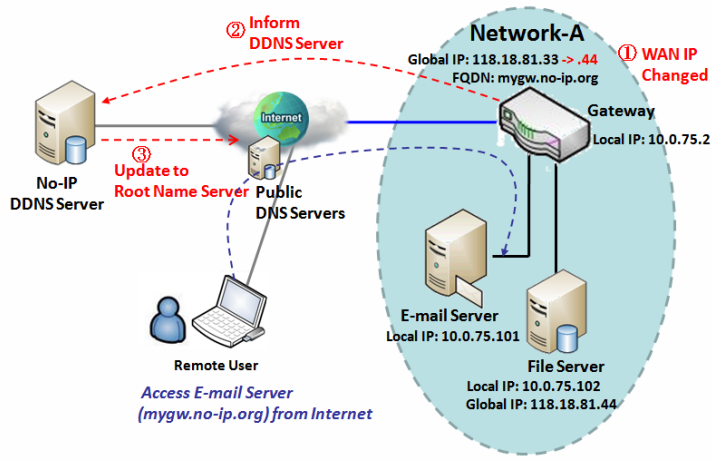
Policy Routing Source	Source IP	Destination IP	Destination Port	WAN Interface
Load Balance	-	-	-	-

Policy Routing Information		
Item	**Value setting**	**Description**
Policy Routing Source	N/A	The Policy Routing strategy.
Source IP	N/A	The Source IP of this Policy Route in IPv4 Format.
Destination IP	N/A	The Destination IP of this Policy Route in IPv4 Format.
Destination Port	N/A	The Destination Port of this Policy Route.
WAN Interface	N/A	The WAN Interface of this Policy Route.

2.7 DNS & DDNS

How can a user access your server if your WAN IP address changes all the time? One way is to register a new domain name and maintain your own DNS server. A simpler way is to apply for a domain name with a third-party DDNS provider. The service can be free or may charge fees. Refer to Wikipedia website[5,6] for more information on DNS and Dynamic DNS.

2.7.1 DNS & DDNS Configuration



Dynamic DNS

To host your server with a changing IP address, you can use dynamic domain name service (DDNS). Dynamic DNS will map the name of your host to your current IP address, which changes dynamically every time you request connection service from your ISP.

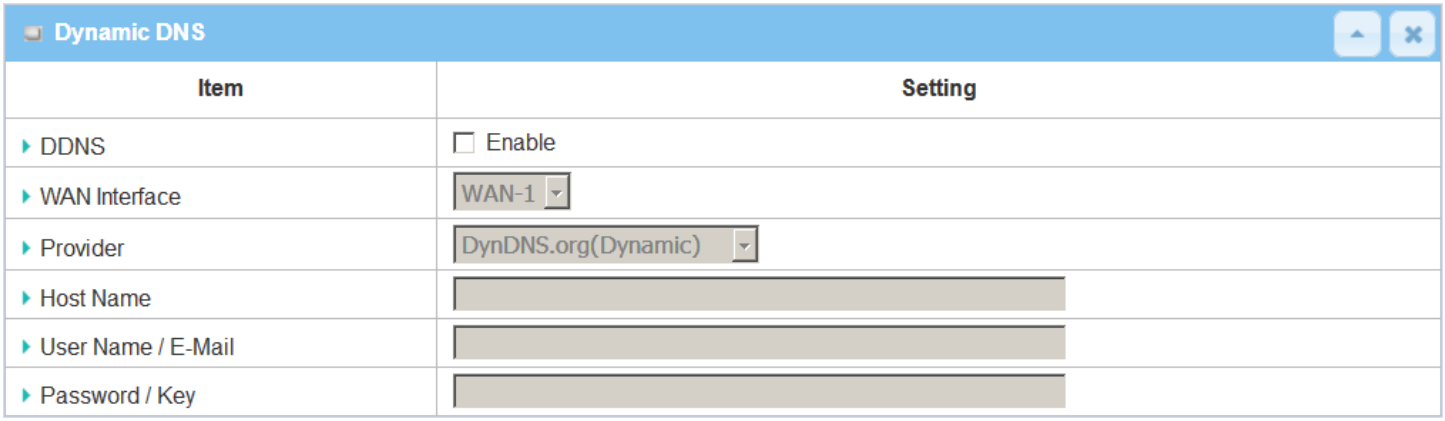
The Dynamic DNS service allows the gateway to map a public dynamic IP address to a static domain name, simplying access of the gateway over the Internet. As shown in the diagram, a domain name is registered through a third-party DDNS ISP (NO-IP). Once the IP address of designated WAN interface has changed, the dynamic DNS agent in the gateway will inform the DDNS server of the new IP address. The server automatically updates your domain name with the changed IP address. Hence, the access to the destined server will not be affected.

5 Wikipedia, “Domain Name System”, Jan 2, 2024, http://en.wikipedia.org/wiki/Domain_Name_System
6 Wikipedia, “Dynamic DNS”, Nov 29, 2023, http://en.wikipedia.org/wiki/Dynamic_DNS

DNS & DDNS Setting

Go to **Basic Network** > **DNS & DDNS** > **Configuration** Tab to set up Dynamic DNS feature and DNS redirect rules.

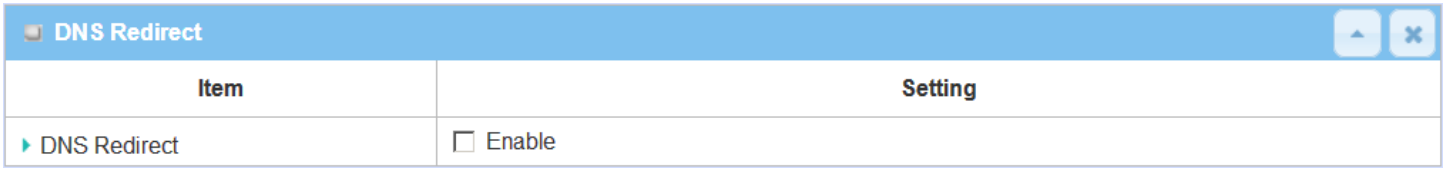
Configure Dynamic DNS



DDNS (Dynamic DNS) Configuration Item	Value setting	Description
DDNS	The box is unchecked by default	Activate this function.
WAN Interface	WAN 1 is set by default	Select the WAN Interface for DDNS.
Provider	DynDNS.org (Dynamic) is set by default	Select your DDNS provider of Dynamic DNS. It can be **DynDNS.org(Dynamic)**, **DynDNS.org**, **NO-IP.com**, etc...
Host Name	1. String format can be any text 2. A must-filled setting	Enter your registered host name of Dynamic DNS. *Value Range*: 0 ~ 63 characters.
Username / E-Mail	1. String format can be any text 2. A must-filled setting	Enter your Username or E-mail addresss of Dynamic DNS.
Password / Key	1. String format can be any text 2. A must-filled setting	Enter your Password or Key of Dynamic DNS.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

Configure DNS Redirect

DNS redirect is a special function to redirect certain traffic to a specified host.

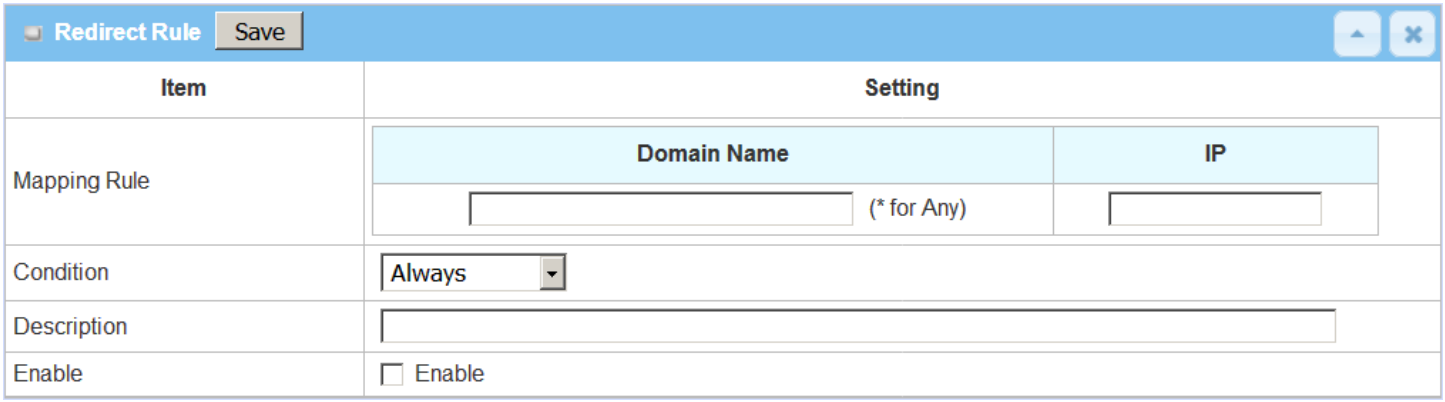


DNS Redirect Configuration		
Item	**Value setting**	**Description**
DNS Redirect	The box is unchecked by default	Activate this function.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

If you enable the DNS Redirect function, you have to further specify the redirection rules. The gateway will redirect the traffic with the matching DNS rule to a pre-defined host.



Click **Add** to open the **Redirect Rule** screen.



Redirect Rule Configuration		
Item	**Value setting**	**Description**
Domain Name	1. String format can be any text 2. A must-filled setting	Enter a domain name for redirection. The traffic destined for the specified domain name will be redirected to the following IP address. *Value Range*: at least 1 character is required; '*' for any.
IP	1. IPv4 format 2. A must-filled setting	Enter a target IP Address for the DNS redirection.
Condition	1. A must-filled setting **2. Always is selected by default.**	Specify when the DNS redirection will be applied. It can be **Always** or **WAN Block**. **Always:** The DNS redirection function is applied to the designated traffic all the time. **WAN Block:** The DNS redirection function is applied to the designated traffic only when the WAN connection is disconneced, or unreachable.
Description	1. String format can be any text	Enter a brief description for this rule. *Value Range*: 0 ~ 63 characters.

	2. A must-filled setting	
Enable	The box is unchecked by default	Activate this rule.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

2.8 QoS

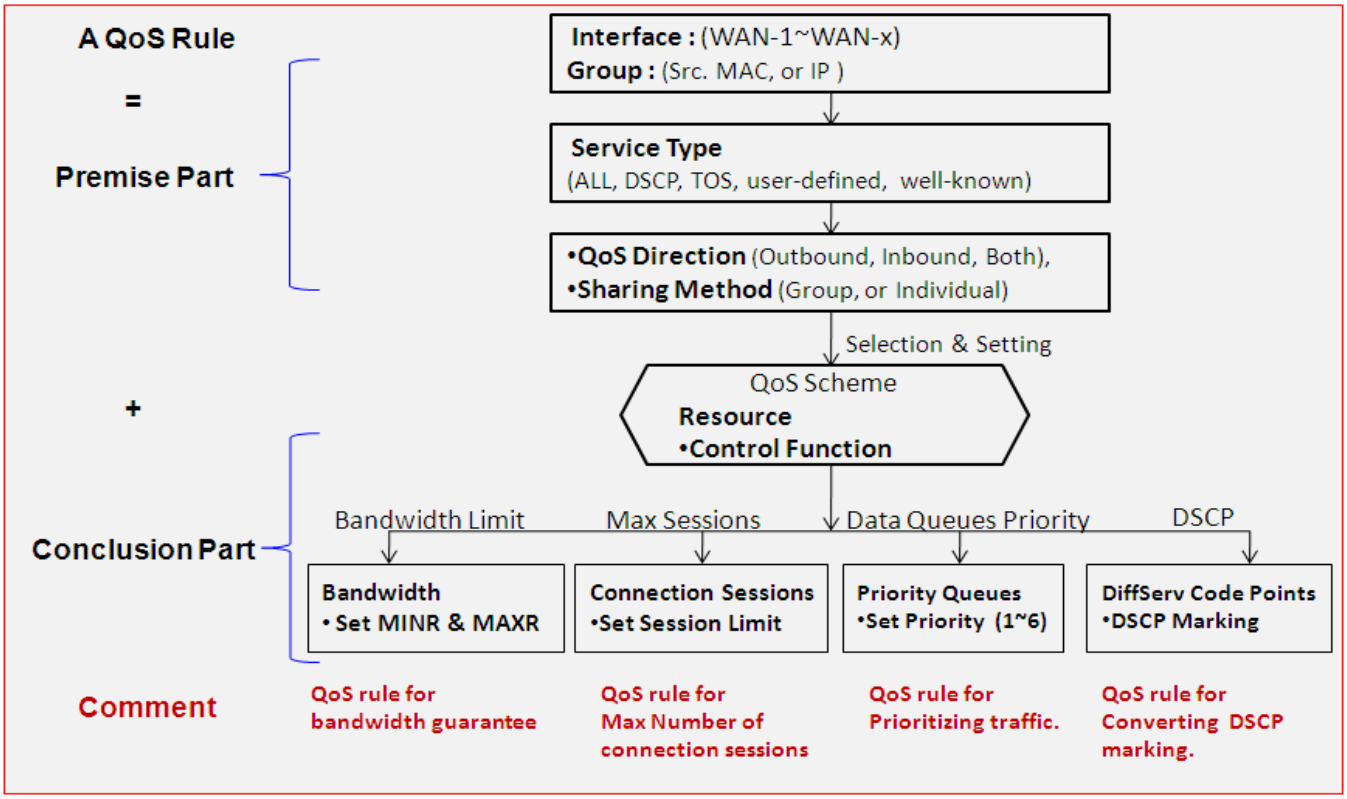
The total amount of data traffic keeps increasing as the bandwidth demand for mobile applications like Game, Chat, VoIP, Video, and web access mounts. New requirements for data transport such as low latency and low data loss emerges to ensure the guarranted quality of service.

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 function of QoS is ensuring that prioritizing data flow doesn’t interfere with other data flows. By marking the incoming packets entering the gateway, QoS determines which queue the packets enter, according to the priority setting. This is useful when there are certain types of data to assign a higher priority to, for example, voice data.

To utilize your network bandwidth effectively, you must define bandwidth rules to balance the utilization of network bandwidth for all client hosts while satisfying the requirements of latency-critical applications, minimum access right guarantee, and fair bandwidth usage. D-LINK Security gateway provides a Rule-based QoS approach.

2.8.1 QoS Configuration

The "QoS Rule Configuration" window allows you to configure QoS rules. 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 resources to be distributed, the corresponding control function for specified resource, the packet flow direction, the sharing method for the control function, the integrated time schedules 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, and the sharing method of group control or individual control. However, in the conclusion part, you must select which kind of system resources that the rule will apply and the control function for the chosen system resource for the rule. The Rule-based QoS has the following features:

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

Differentiated Services:
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), POP3 (TCP:995), NetMeeting (1720), L2TP (UDP:1701) and PPTP (TCP:1723).
Control Functions for resource allocation: bandwidth, connection sessions, priority queues and DiffServ Code Point (DSCP). Control function that acts on specific services of packet flows is based on these resources.

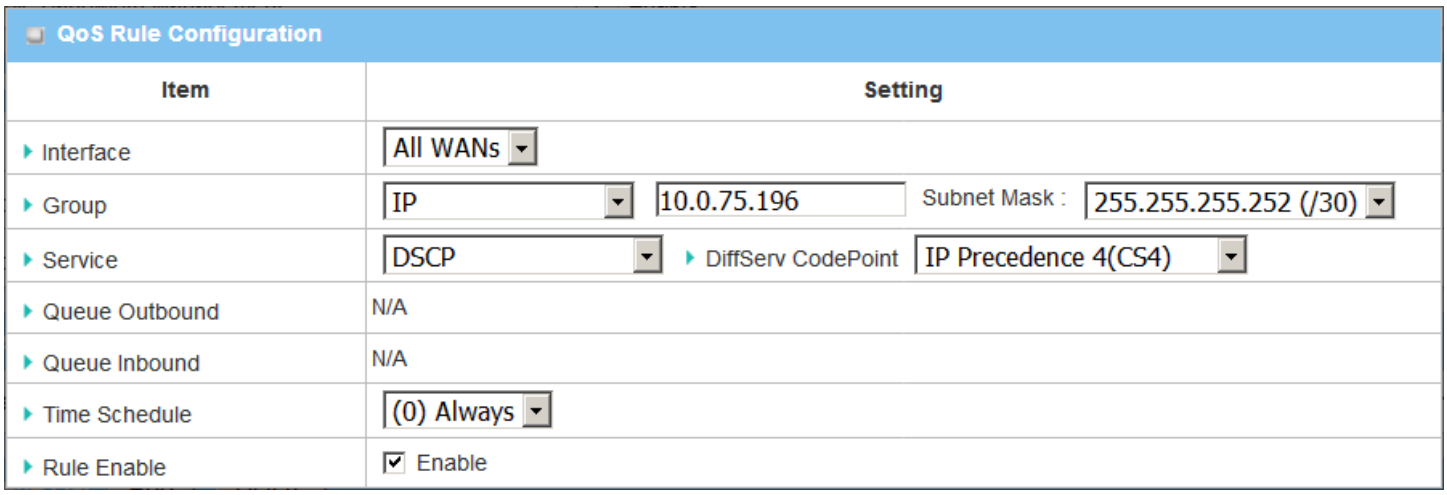
Two QoS rule examples are demonstrated below:

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	Enable

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

QoS Rule Example #2 – DifferServ Code Points



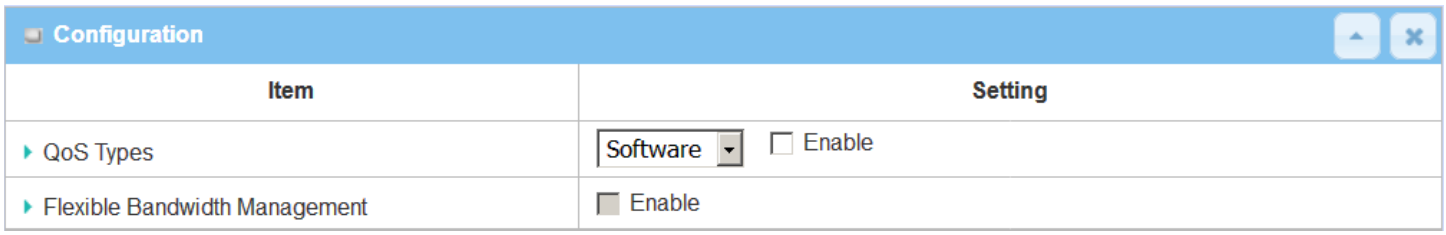
To convert the code point value, "IP Precedence 4(CS4)" to the code value, "AF Class2(High Drop)", in the packets from the specified client hosts (IP 10.0.75.196~199), the "Rule-based QoS" function can be defined as shown in above configuration.

QoS Configuration Setting

Go to **Basic Network > QoS > Configuration** to access the QoS Cofiguration page.
In "QoS Configuration" page, there are configuration windows for QoS function: "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 and enable the "Flexible Bandwidth Management" (FBM) feature for better utilization of system bandwidth by FBM algorithm. The “System Configuration” window lets you configure the total bandwidth and session of each WAN. The "QoS Rule List" window lists all your defined QoS rules. Finally, the "QoS Rule Configuration" window lets you define each QoS rule.

Enable QoS Function

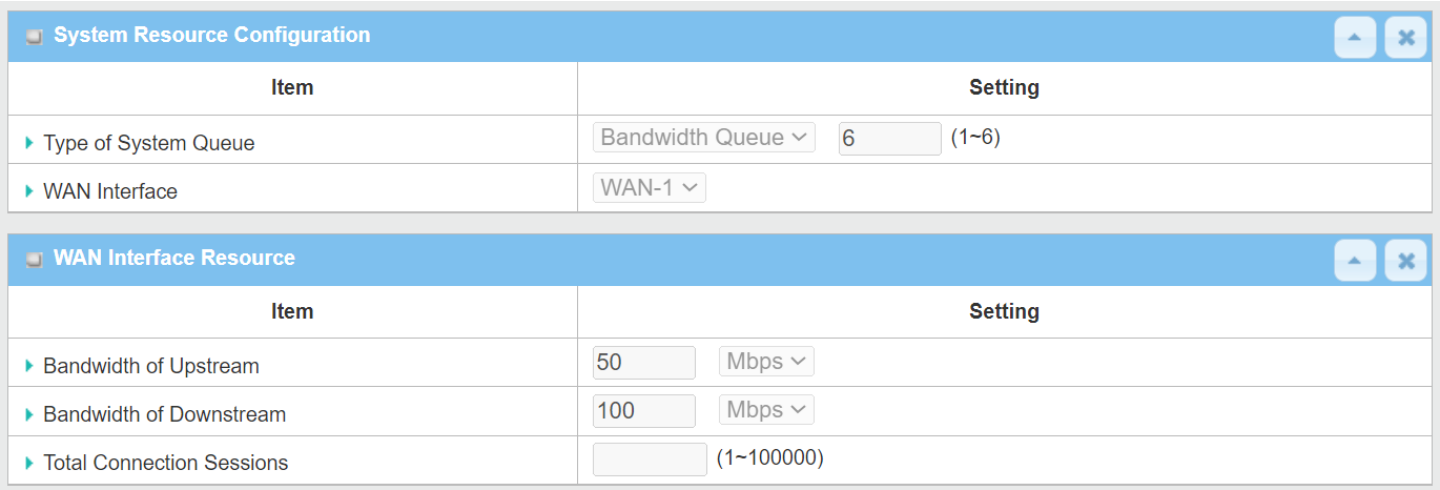
-



Configuration Item	Value Setting	Description
QoS Type	1. **Software** is selected by default. 2. The box is unchecked by default.	Select the QoS Type from the dropdown list: **Software** or **Hardware**, and then click **Enable** box to activate the QoS function.
Flexible Bandwidth Management	The box is unchecked by default	Click **Enable** box to activate the **Flexible Bandwidth Management** function.
Save	N/A	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 will adjust the bandwidth distribution dynamically based on the current bandwidth consumption for the optimal system network performance while taking the users’ bandwidth subscription profiles into account.

Configure System Resource

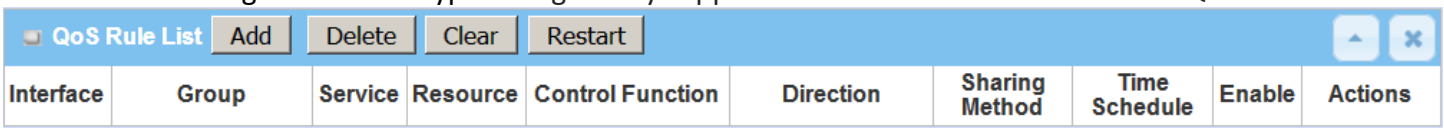


System Resource Configuration		
Item	**Value Setting**	**Description**
Type of System Queue	1. A must-filled setting. 2. **Bandwidth Queue**, and **6** are set by default.	Define the system queues for the QoS settings. The supported type of system queues are **Bandwidth Queue** and **Priority Queues.** *Value Range*: 1 ~ 6.
WAN Interface	**WAN-1** is selected by default.	Specify the WAN interface configuration related resources in the below **WAN Interface Resource** section. ● **Bandwidth of Upstream / Downstream** Specify total upload / download bandwidth of the selected WAN. ● **Total Connection Sessions** Specify total connection sessions allowed for the selected WAN. *Value Range:* 1 ~ 10000.
Save	N/A	Save the settings.

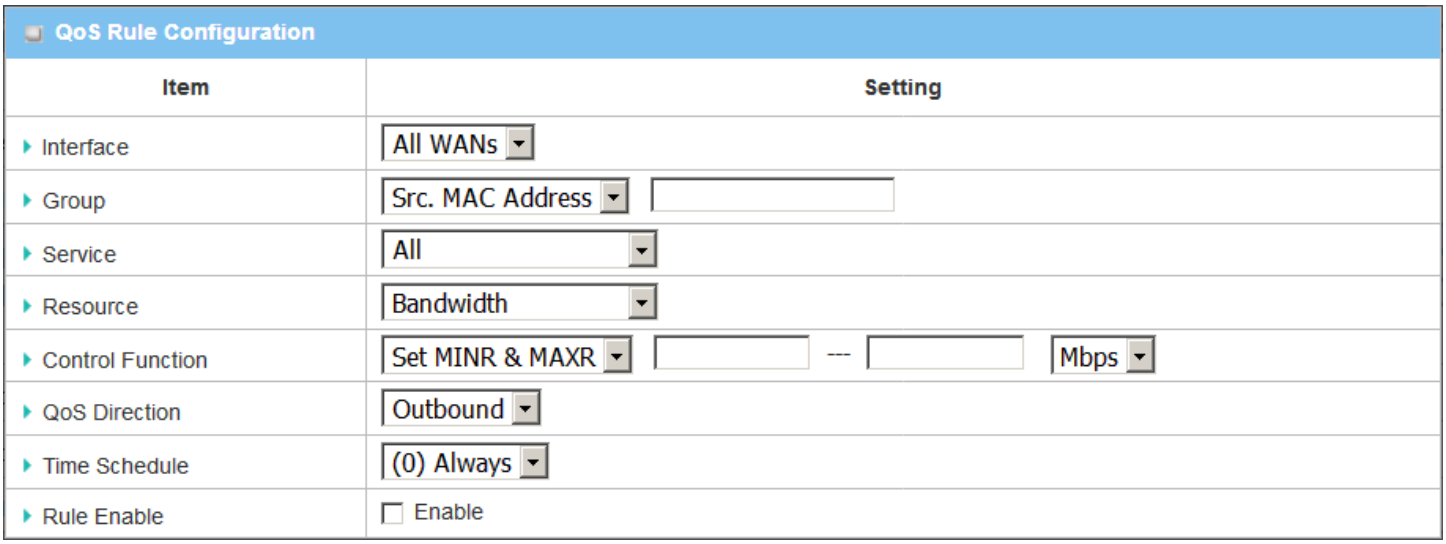
Note: For proper implementation of QoS, the upstream bandwidth, downstream bandwidth, and the maximum number of connection sessions should be configured in advance.

Create / Edit QoS Rules

After enabling and configuring the QoS function and system resources, configure QoS rules to provide better service on the designated traffic type. The gateway supports a maximum of 128 rule-based QoS rules.



Click **Add** to open the **QoS Rule Configuration** screen.



QoS Rule Configuration		
Item	**Value setting**	**Description**
Interface	1. A must-filled setting. 2. **All WANs** is selected by default.	Specify the WAN interface to apply the QoS rule. Select **All WANs** or a certain **WAN-n** to filter the packets entering to or leaving from the interface(s).
Group	1. A must-filled setting. 2. **Src. MAC Address** is selected by default.	Specify the **Group** category for the QoS rule: **Src. MAC Address**, **IP**, or **Host Name.** **Src. MAC Address**: Select **Src. MAC Address** to prioritize packets based on MAC Address. **IP:** Select **IP** to prioritize packets based on IP address and Subnet Mask. **Host Name:** Select **Host Name** to prioritize packets based on a group of a pre-configured group of hosts from the dropdown list. **Note:** The required host groups must be created in advance and the corresponding QoS checkbox in the **Multiple Bound Services** field must be checked to activate the **Host Group** option. Refer to **Object Definition > Grouping > Host Grouping.**
Service	1. A must-filled setting. 2. **All** is selected by default.	Specify the service type of traffic to be applied with the QoS rule: **All**, **DSCP**, **TOS**, **User-defined Service**, or **Well-known Service**. **All:** Select **All** for all packets.

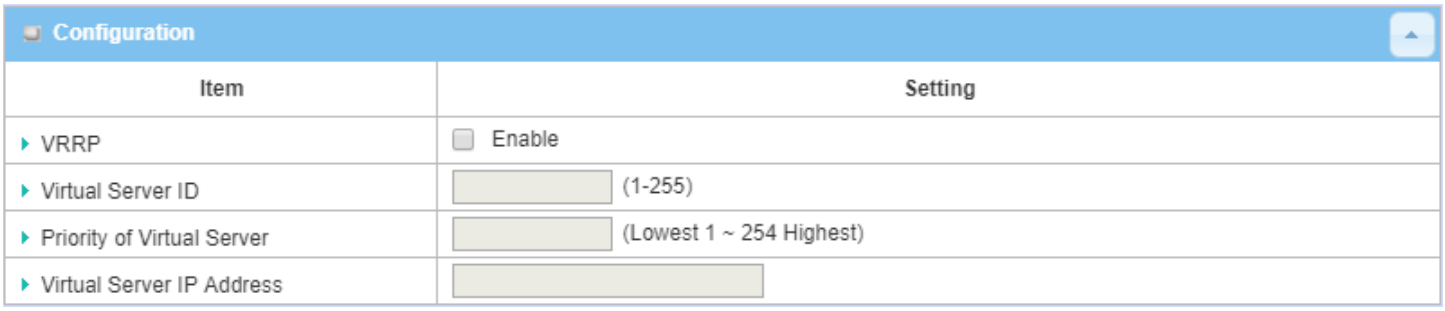
		DSCP: Select **DSCP** for DSCP type packets only. **ToS:** Select **TOS** for TOS type packets only. Then select a service type: **Minimize-Cost**, **Maximize-Reliability**, **Maximize-Throughput**, or **Minimize-Delay** from the dropdown list as well. **User-defined Service**: Select **User-defined Service** for user-defined packets only. You have to define the port range and protocol as well. **Well-known Service**: Select **Well-known Service** for specific application packets only.
Resource and **Control Function**	A must-filled setting	Specify the Resource Type and corresponding Control function for the QoS rule: **Bandwidth**, **Connection Sessions**, **Priority Queues**, and **DiffServ Codepoints**. **Bandwidth**: Select **Bandwidth** as the resource type for the QoS Rule and assign the min rate, max rate and rate unit as the bandwidth settings in the **Control Function** / **Set MINR & MAXR** field. **Connection Sessions**: Select **Connection Sessions** as the resource type for the QoS Rule and assign the supported session number in the **Control Function** / **Set Session Limitation** field. **Priority Queues**: Select **Priority Queues** as the resource type for the QoS Rule, and specify a priority queue in the **Control Function** / **Set Priority** field. **DiffServ Code Points**: Select **DiffServ Code Points** as the resource type for the QoS Rule and select a DSCP marking from the **Control Function** / **DSCP Marking** dropdown list.
QoS Direction	1. A must-filled setting. 2. **Outbound** is selected by default.	Specify the traffic flow direction for the packets to apply the QoS rule: **Outbound**, **Inbound**, or **Both**. **Outbound**: Select **Outbound** to prioritize the traffic traffic going to the Internet via the specified interface. For the Outbound traffic, the hosts specified in the Group field is a source group. **Inbound**: Select **Inbound** to prioritize the traffic traffic coming from the Internet via the specified interface. For the Inbound traffic, the hosts specified in the Group field is a destination group. **Both**: Select **both** to prioritize the traffic traffic passing through the specified interface, both Inbound and Outbound should be considered. For both inbound and outbound traffic, the hosts specified in the Group field can be a source or destination group.
Sharing Method	1. A must-filled setting. 2. **Group Control** is selected by default.	Specify the preferred sharing method for the QoS rule on the selected group: **Individual Control** or **Group Control**. **Individual Control**: If **Individual Control** is selected, each host in the group will have its own QoS service resource as specified in the rule. **Group Control**: If **Group Control** is selected, all the group hosts share the same QoS service resource.
Time Schedule	1. A must-filled setting. 2. **(0) Always** is selected by default.	Apply **Time Schedule** to this rule; otherwise leave it as (0) **Always**. (refer to **Object Definition > Scheduling > Configuration** settings)

Rule Enable	The box is unchecked by default.	Activate this QoS rule.
Save	N/A	Save the settings.

2.9 Redundancy

Redundancy is the duplication of critical components or functions of a system to provide backup or fail-safe. In an IP networking, the gateway can serve as the redundant gateway of the core gateway in the enterprise environment using Virtual gateway Redundancy Protocol (VRRP).

2.9.1 VRRP

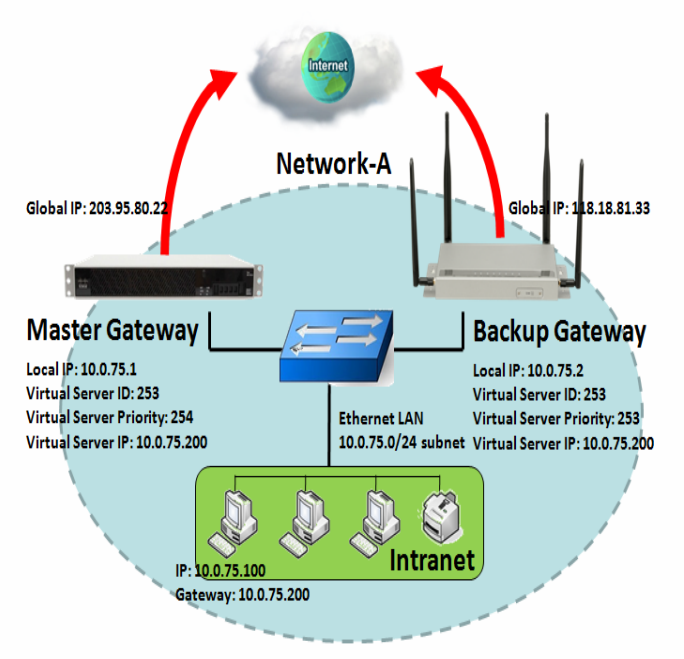


Virtual gateway Redundancy Protocol (VRRP) is a computer networking protocol that provides device redundancy. It allows a backup gateway or switch to automatically take over the job of the master gateway if the primary (master) gateway or switch fails. This increases the availability and reliability of routing paths via automatic default gateway selection in an IP network.

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

A group of physical VRRP gateways combined to serve as a virtual server with one unique virtual server ID and one unique virtual server IP address, with each of the VRRP gateways having a unique priority value for the selection of the master gateway.

The gateway with VRRP function can serve as the backup one for the master gateway with other participated redundant gateways in a VRRP group.



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

At first stage, all data from the LAN will through the master gateway that has the highest priority. Once the master Internet connection is broken, the backup gateway will take over data transmission and serve as the master gateway.

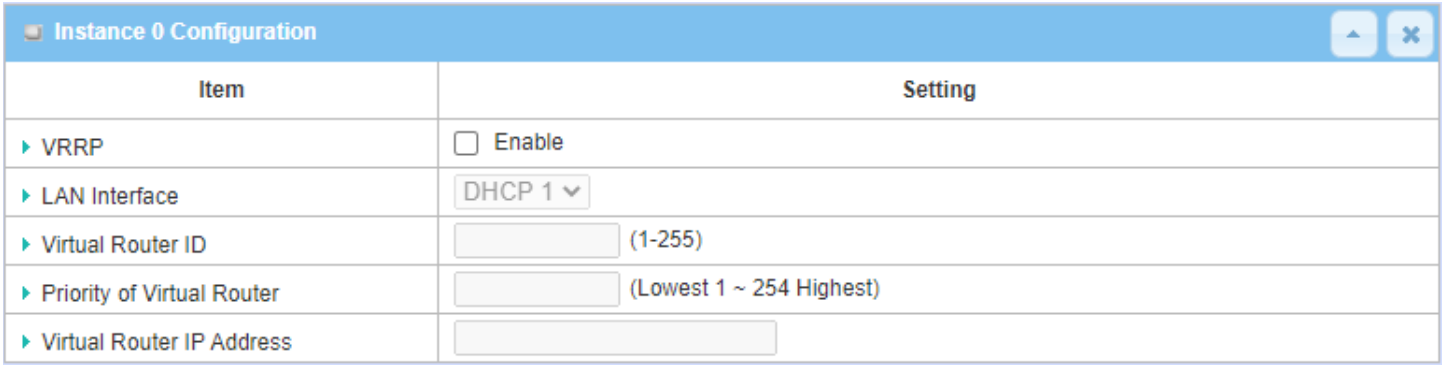
When a gateway with a higher priority value recovers, it will take over data transmittion again.

VRRP Setting

The Virtual gateway Redundancy Protocol (VRRP) setting allows you to assign available gateways as participating hosts automatically. Note that the availability of this function depends on the product model.

Go to Basic Network > Redundancy > VRRP to access VRRP Setting page.

The device provides multiple VRRP instances to accommodate different LAN topologies.



Instance 0 / 1 / 2 / 3 Configuration		
Item	**Value setting**	**Description**
VRRP	The box is unchecked by default.	Activate this VRRP function.
LAN Interface	1. A must-filled setting **2. DHCP 1 is selected by**	Specify the LAN interface that will be applied with the to apply the VRRP configuration: **DHCP 1 ~ DHCP 4**.

	default	
Virtual Server ID	1. Numberic String Format 2. A must-filled setting	Specify the Virtual Server ID of VRRP for the gateway. Value Range: 1 ~ 255.
Priority of Virtual Server	1. Numberic String Format 2. A must-filled setting	Specify the Priority of Virtual Server of VRRP for the gateway. *Value Range*: 1 ~ 254, and 254 is the highest priority.
Virtual Server IP Address	1. IPv4 Format 2. A must-filled setting	Specify the Virtual Server IP Address of VRRP for the gateway.
Save	N/A	Save the configuration.
Undo	N/A	Restore to the previous settings.

Chapter 3 Object Definition

3.1 Scheduling

Scheduling allows you to define activation schedules that can be applied to other functionality, for example, Packet Filters and URL Blocking in Firewall, for time-based control.

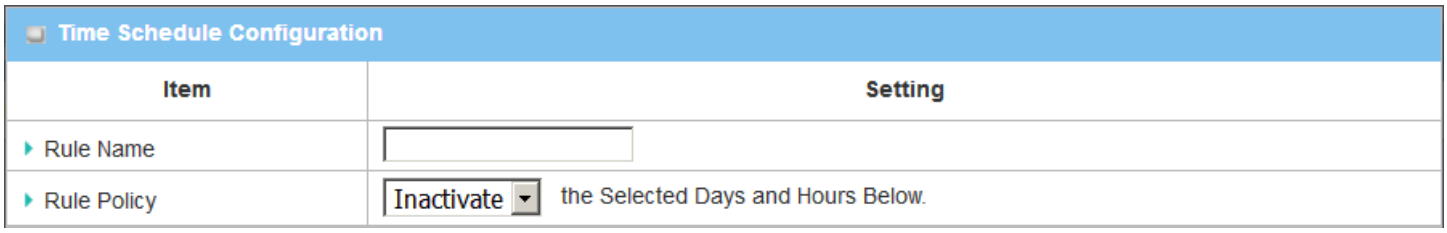
3.1.1 Scheduling Configuration

Go to **Object Definition > Scheduling > Configuration** to access the Time Schedule Configuration page.

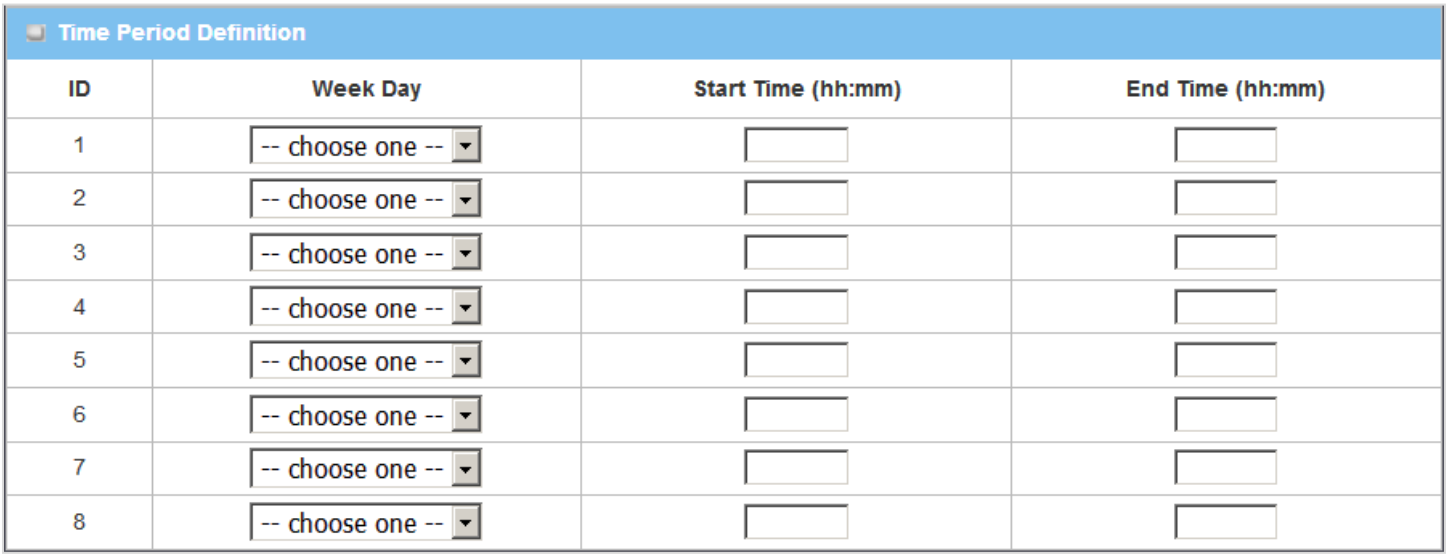


Button description		
Item	**Value setting**	**Description**
Add	N/A	Configure a time schedule rule
Delete	N/A	Delete the selected rule(s)

Click **Add** to open the **Time Schedule Configuration** and **Time Period Definition**.



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



Time Period Definition		
Item	**Value Setting**	**Description**
Week Day	Select from menu	Select everyday or one weekday
Start Time	Time format (hh :mm)	Start time for the selected weekday
End Time	Time format (hh :mm)	End time for the selected weekday
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.
Refresh	N/A	Refresh the time schedule list.

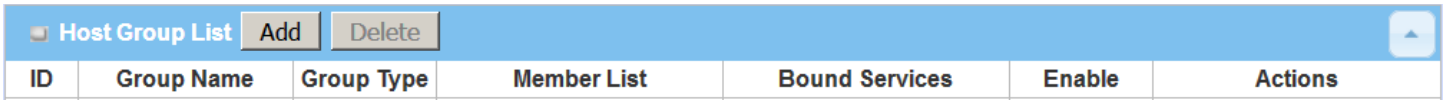
3.2 Grouping

The Grouping function allows you to select hosts for a group. Note that the availability of this function depends on the product model.

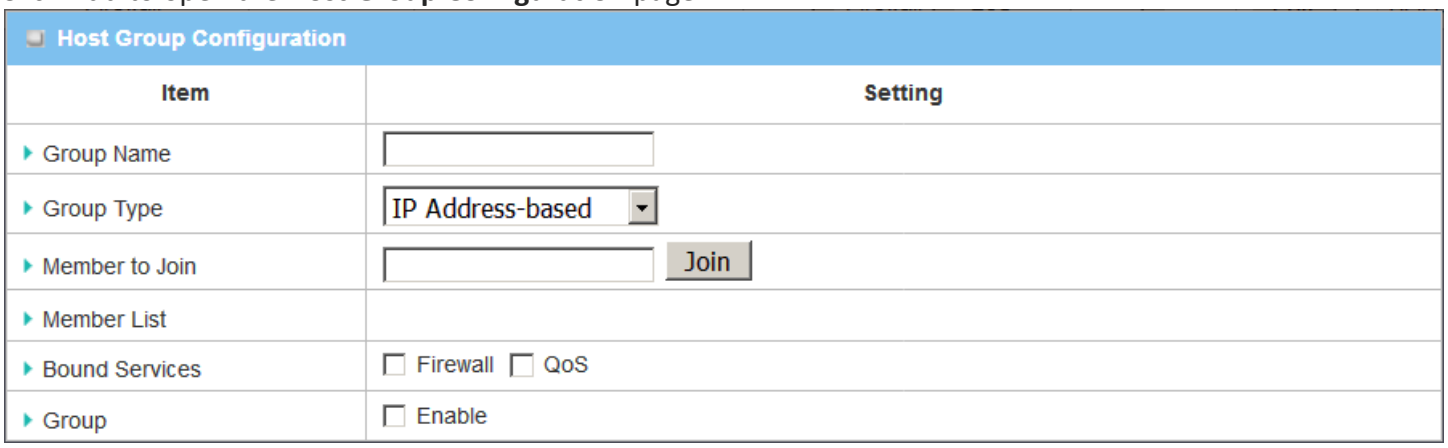
3.2.1 Host Grouping

Go to **Object Definition > Grouping > Host Grouping** tab to define host groups.

This allows you to define a host group for certain functions, such as QoS, Firewall, and Communication Bus. The selection of the members for a host group can be based on IP address, MAC address or host name. Note the availability of this function depends on the product model.



Click **Add** to open the **Host Group Configuration** page.



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

		When **Host Name-based** is selected, only host names can be added in **Member to Join.** **Note**: The available Group Type can be different depening on the product model.
Member to Join	N/A	Add the members to the group. Enter the member information as specified in the Member Type above and click the **Join** button to add.
Member List	NA	This field will indicate the hosts (members) contained in the group.
Bound Services	The boxes are unchecked by default	Bind the services so that the host group can apply for that function. For example, enable **Firewall** to let the group to be applied for Firewall. The available services depend on the supported functions of the gateway.
Group	The box is unchecked by default	Activate the host group rule. So that the group can be bound to selected service(s) for further configuration.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

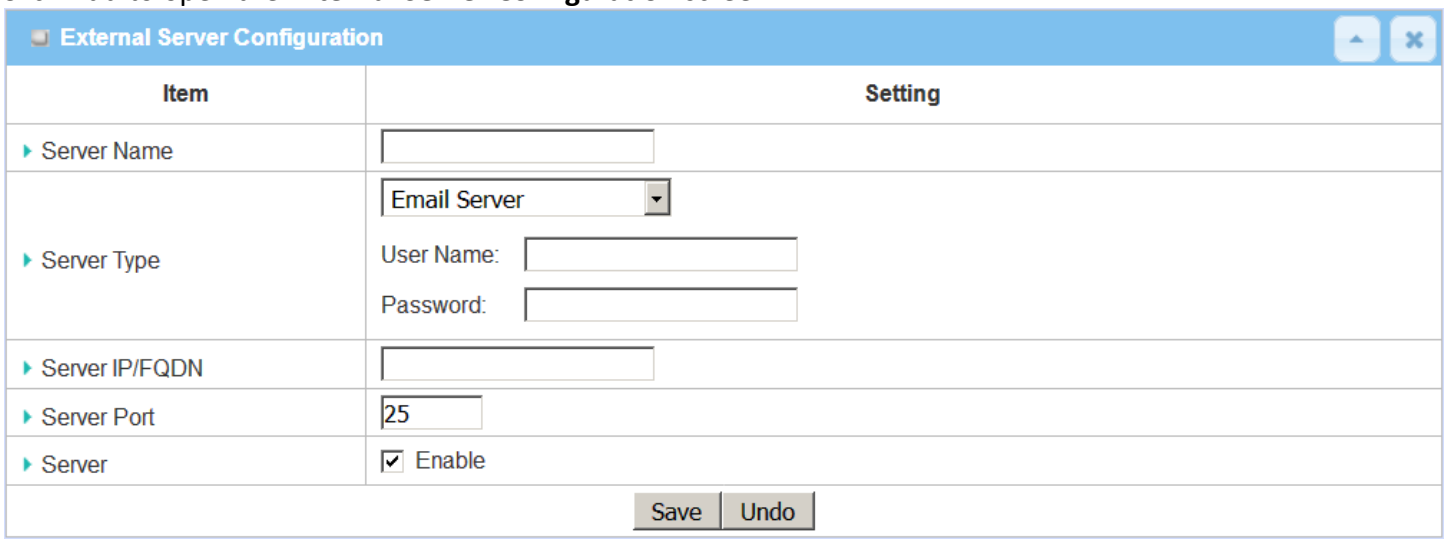
3.3 External Server

The External Server setting allows you to add external servers that the system have permission to access.
Go to **Object Definition > External Servers** to access the External Server page.

Create External Server



Click **Add** to open the **External Server Configuration** screen.



External Server Configuration		
Item	**Value setting**	**Description**
Sever Name	1. String format can be any text 2. A must-filled setting	Enter a descriptive name for the server.
Server Type	A must-filled setting	Specify the Server Type for the external server, and enter the required settings to access the server.
		Email Server (A must-filled setting) : When selecting **Email Server**, specify the follwing: **Username** (String format: any text) **Password** (String format: any text)
		RADIUS Server (A must-filled setting) : When selecting **RADIUS Server**, specify the following settings for both the primary and secondary servers: **Shared Key** (String format: any text) **Authentication Protocol** (Default: CHAP is selected, Options : CHAP, PAP) **Session Timeout** (Default: 1, Range: 1-60) Idle Timeout: (Default: 1, Range: 1-15)
		Active Directory Server (A must-filled setting) : When selecting **Active Directory Server**, specify the following **Domain setting**: **Domain** (String format: any text)
		LDAP Server (A must-filled setting) : When selecting **LDAP Server**, specify the following settings: **Base DN** (String format: any text) **Identity** (String format: any text) **Password** (String format: any text)
		UAM Server (A must-filled setting) : When selecting **UAM Server**, specify the following settings: **Login URL** (String format: any text) **Shared Secret** (String format: any text) **NAS/gateway ID** (String format: any text) **Location ID** (String format: any text) **Location Name** (String format: any text)
		TACACS+ Server (A must-filled setting) : When selecting **TACACS+ Server**, specify the following settings: **Shared Key** (String format: any text) **Session Timeout** (Range : 1-60)
		SCEP Server (A must-filled setting) : When selecting **SCEP Server**, specify the following settings: **Path** (String format: any text, default : **cgi-bin**) **Application** (String format: any text, default : **pkiclient.exe**)
		FTP(SFTP) Server (A must-filled setting) : When selecting **FTP(SFTP) Server,** specify the following settings: **Username** (String format: any text)

		Password (String format: any text) **Protocol** (FTP or SFTP) **Encryption** (Plain, Explicit FTPS or Implicit FTPS) **Transfer mode** (Passive or Active)
Server IP/FQDN	A must-filled setting	Specify the IP address or FQDN used for the external server.
Server Port	A must-filled setting	Specify the Port used for the external server: For **Email Server** 25 will be set by default; For **Syslog Server**, port 514 will be set by default; For **RADIUS Server**, port 1812, 1823 will be set by default; For **Active Directory Server**, port 389 will be set by default; For **LDAP Server**, port 389 will be set by default; For **UAM Server**, port 3990 and 4990 will be set by default; For **TACACS+ Server**, port 49 will be set by default; For **SCEP Server**, port 80 will be set by default; For **FTP (SFTP) Server**, port 21 will be set by default; *Value Range*: 1 ~ 65535.
Account Port	1. A must-filled setting **2. 1813 is set by default**	Specify the accounting port used if you selected an external RADIUS server. *Value Range*: 1 ~ 65535.
Server	The box is checked by default	Activate this External Server.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.
Refresh	N/A	Refresh the external server list.

3.4 Certificate

In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove the ownership of a public key. The certificate includes information about the key, its owner's identity, and the digital signature of an entity that has verified the certificate's content is 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[7].
In a typical public-key infrastructure (PKI) scheme, the signer is a certificate authority (CA), usually a company such as VeriSign which charges customers who acquire certificates. In a web of trust scheme, the signer is either the key's owner (for a self-signed certificate) or other parties whom the person examining the certificate might know of 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) in which they prevent an attacker from impersonating a secure website or other servers. They are also used in other important applications, such as email encryption and code signing. Here, it can be used in IPSec tunneling for user authentication.

3.4.1 Configuration

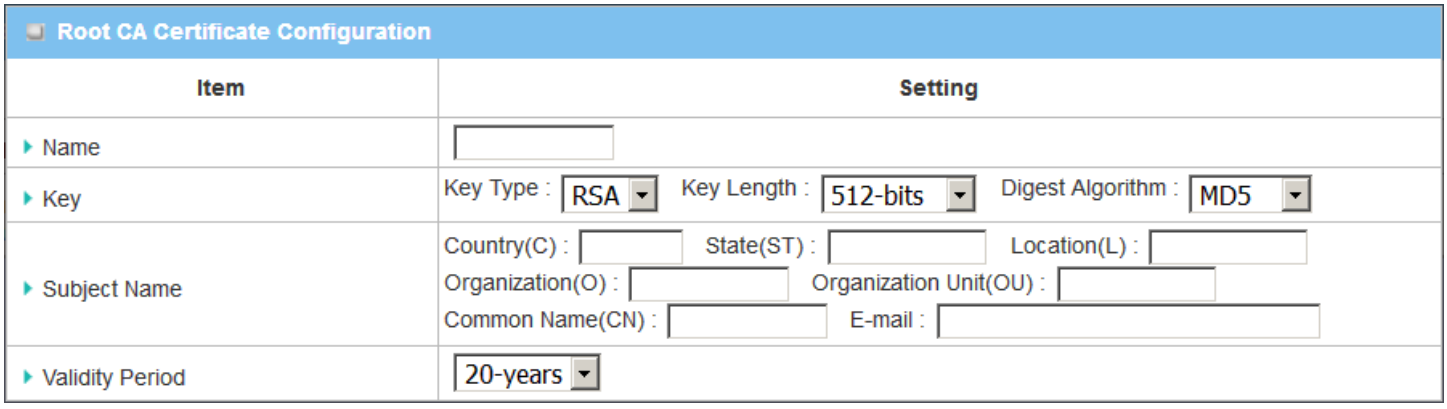
The configuration setting allows you to create Root Certificate Authority (CA) certificates and enable SCEP. Root CA is at the top-most level of the certificate tree, which is the private key used to sign other certificates.

Go to **Object Definition > Certificate > Configuration** to access the configuration page.

Create Root CA



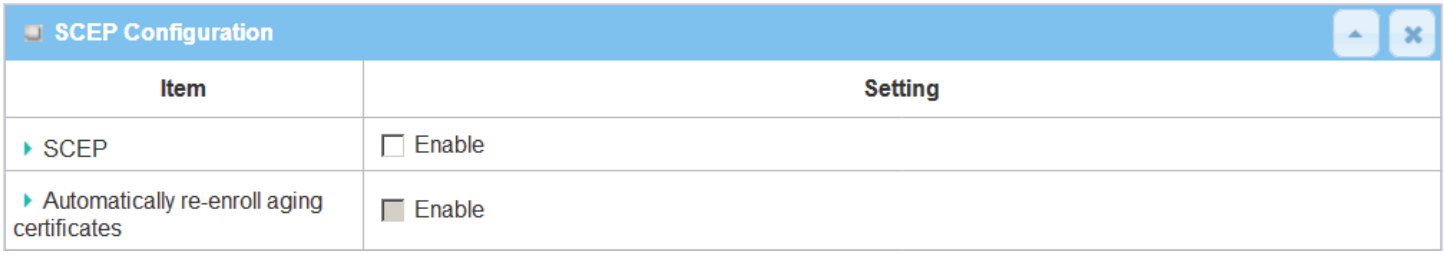
Click **Generate** to open the **Root CA Certificate Configuration** screen.



7 Wikipedia, “Public key certificate”, Dec 12, 2023, http://en.wikipedia.org/wiki/Public_key_certificate.

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

Configure SCEP

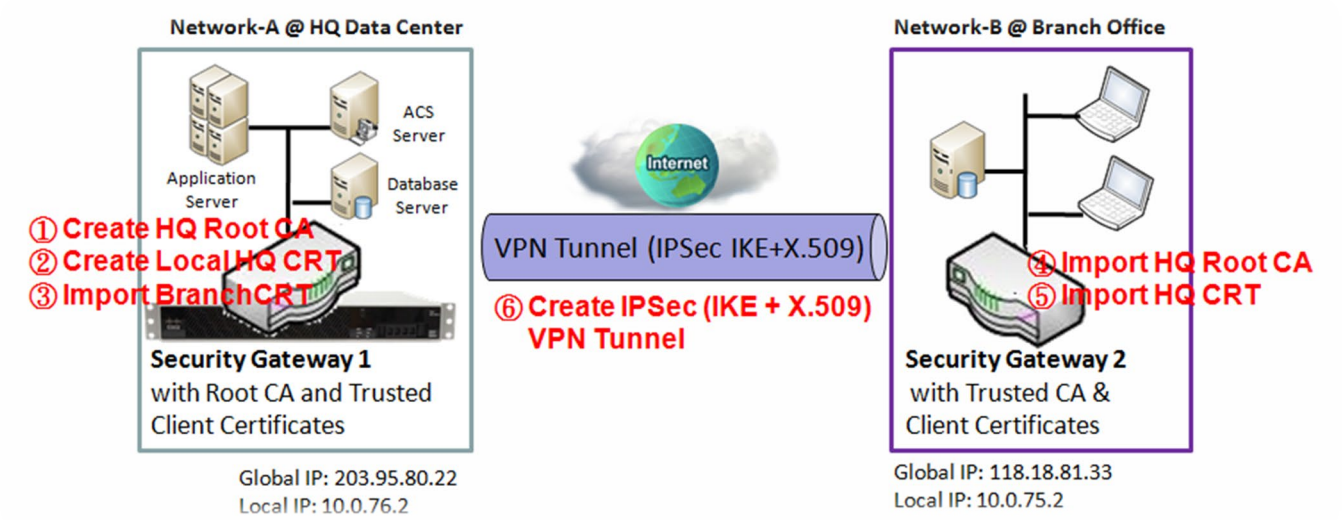


SCEP Configuration		
Item	**Value setting**	**Description**
SCEP	The box is unchecked by default	Activate SCEP function.
Automatically re-enroll aging certificates	The box is unchecked by default	If the certificate has been aged, it will activate the SCEP function to re-enroll it automatically.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

3.4.2 My Certificate

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

Self-signed Certificate Usage Scenario



Scenario

When the gateway is the root CA and needs a certificate for VPN tunneling, it can generate its own local certificates that can be signed by itself or import local certificates that are signed by other CAs. Since it is the root CA, it can create Certificate Signing Requests (CSR) for corresponding certificates for remote connection. These certificates can be used by two remote peers for identity verification when establishing a VPN tunnel.

Scenario Description

gateway 1 generates the root CA and a local certificate (HQCRT) signed by itself. A BranchCSR certificate of gateway 2 signed by root CA of gateway 1 is also imported as the Trusted Client Certificate to the gateway.

gateway 2 creates a CSR (BranchCSR) to issue the BranchCRT certificate that is signed by root CA of the gateway 1. It is then imported into the gateway 2 as a local certificate. In addition, the certificates of the root CA of the gateway 1 are imported into gateway 2 as the Trusted Client Certificate.

Either peer can establish an IPSec VPN tunnel with IKE and X.509 protocols, so that all client hosts in both subnets can communicate with each other.

Parameter Setup Example

For Network-A at HQ

The following tables list the parameter configuration of Network-A for "My Certificate" used for the user authentication of IPSec VPN tunnel for the scenario shown in the above diagram.

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

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

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

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

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

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

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

For Network-B at Branch Office

The following tables list the parameter configuration of Network-B for "My Certificate" used for user authentication of IPSec VPN tunnel for the scenario shown in the above diagram.

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

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

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

Configuration Path	[IPSec]-[Local & Remote Configuration]
Local Subnet	***10.0.75.0***
Local Netmask	***255.255.255.0***
Full Tunnel	***Disable***
Remote Subnet	***10.0.76.0***
Remote Netmask	***255.255.255.0***
Remote gateway	***203.95.80.22***

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

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

Now gateway 2 can establish a Site-to-Site IPSec VPN tunnel with IKE and X.509 protocols to gateway 1. And the client hosts in the two subnets 10.0.75.0/24 and 10.0.76.0/24 can communicate with each other.

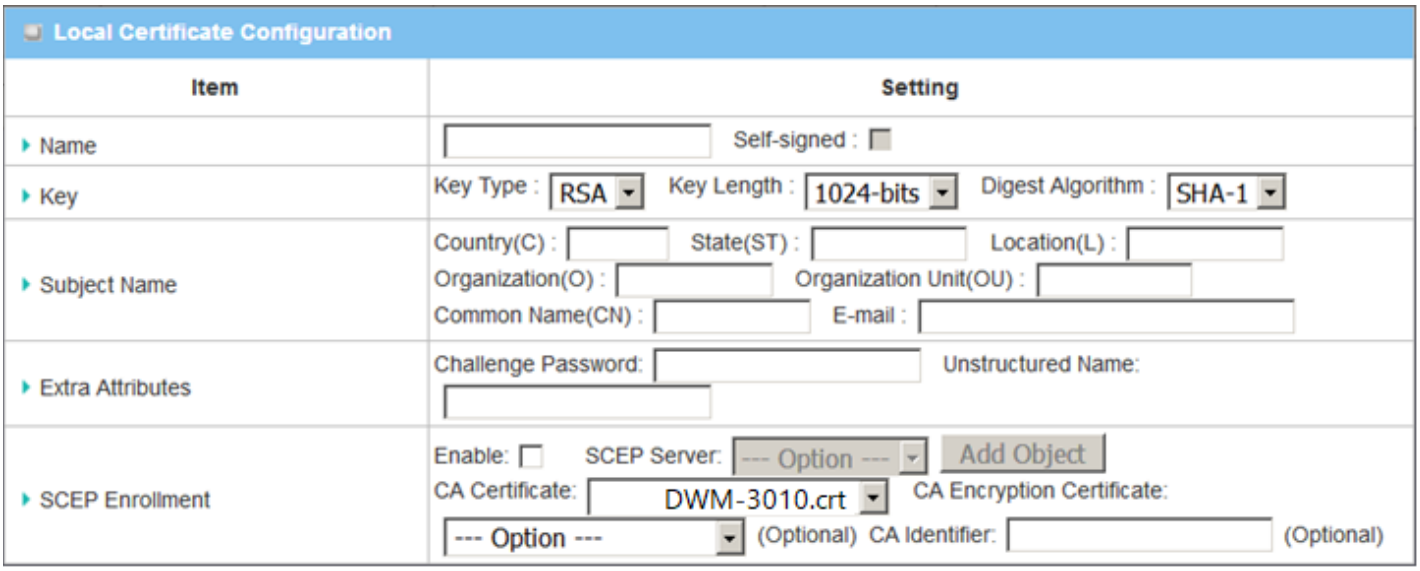
My Certificate Setting

Go to **Object Definition > Certificate > My Certificate** to access the Certificate Setting page.
The My Certificate setting allows you to create local certificates. There are two configuration windows for the "My Certificate" function: Local Certificate List and Local Certificate Configuration windows. The "Local Certificate List" window shows the stored certificates or CSRs. The "Local Certificate Configuration" window lets you fill out information necessary for generating self-certificates or corresponding CSRs to be signed by other CAs.

Create Local Certificate

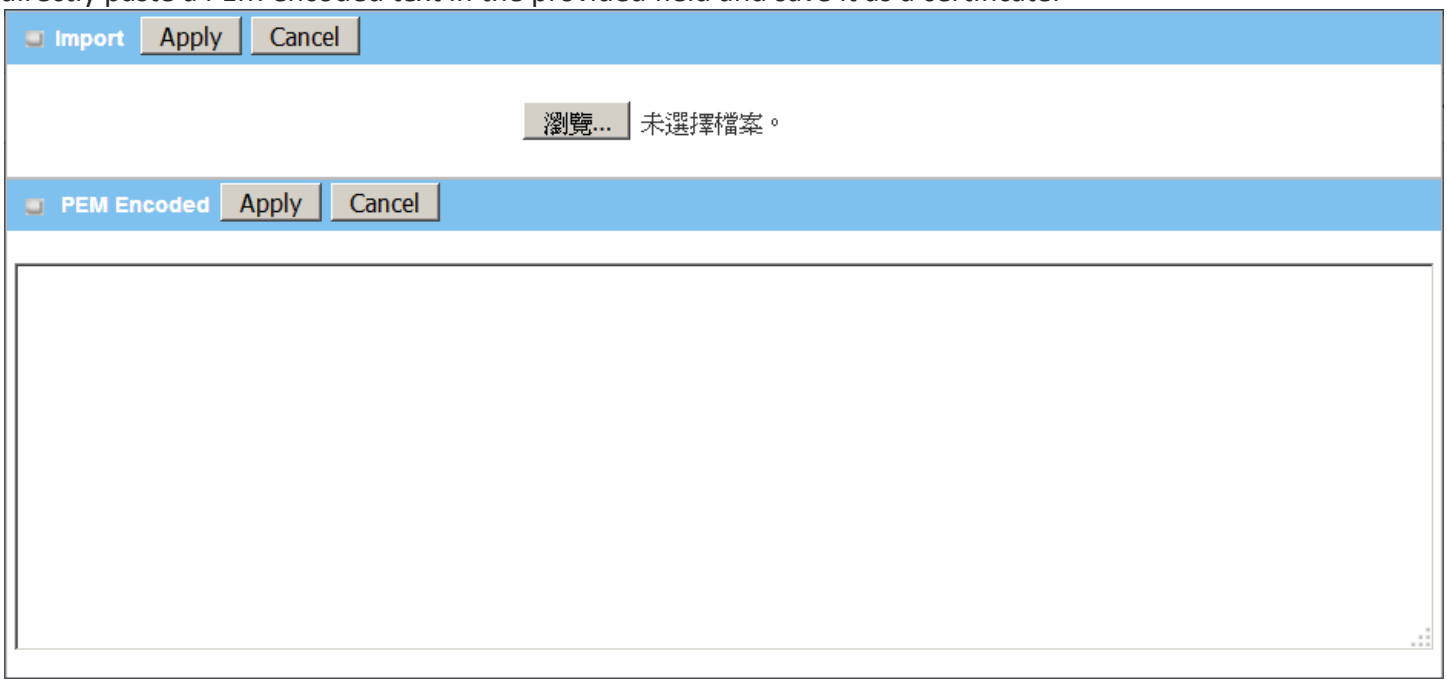


Click **Add** to open the **Local Certificate Configuration** screen.



Local Certificate Configuration		
Item	**Value setting**	**Description**
Name	1. String format can be any text 2. A must-filled setting	Enter a name for the certificate. If **Self-signed** is checked, the certificate will be signed by root CA. If **Self-signed** is not checked, the system will generate a certificate signing request (CSR).
Key	A must-filled setting	Specify the key attributes of certificate. **Key Type**: set public-key cryptosystems. Currently, only RSA is supported. **Key Length**: set the length (in bits) of the key used for cryptography. It can be 512, 768, 1024, 1536 or 2048. **Digest Algorithm:** set identifier in the signature algorithm identifier of the certificate. It can be MD5 or SHA-1.
Subject Name	A must-filled setting	Specify the information of the certificate: **Country(C)**: the two-letter ISO code for the country where your organization is located. **State (ST)**: the state of your organization. **Location (L)**: the location where your organization is located. **Organization (O)**: the name of your organization. **Organization Unit (OU)**: the name of your organization unit. **Common Name (CN)**: the common name of your organization. **Email**: the email of your organization.
Extra Attributes	A must-filled setting	Specify the validity period of the certificate.
SCEP Enrollment	A must-filled setting	Specify the information of SCEP: Check the **Enable** box to generate a certificate signing request (CSR) to be signed by a SCEP server online. Select a **SCEP Server** to identify the SCEP server configured in External Servers (refer to **Object Definition** > **External Server** > **External Server**). You may click **Add Object** to add a new external server. Refer to **3.4 External Server**. Select a **CA Certificate** to identify which certificate could be accepted by SCEP server for authentication. It will be generated as Trusted Certificates. Select an optional **CA Encryption Certificate**, if it is required, to identify which certificate could be accepted by SCEP server for encryption data information. It will be generated as Trusted Certificates. Fill in optional **CA Identifier** to identify which CA could be used for signing certificates.
Save	N/A	Save the configuration.
Back	N/A	Return to the previous page.

Click **Import** to open the **Import** screen. You can then import a certificate from an existing certificate file, or directly paste a PEM encoded text in the provided field and save it as a certificate.



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

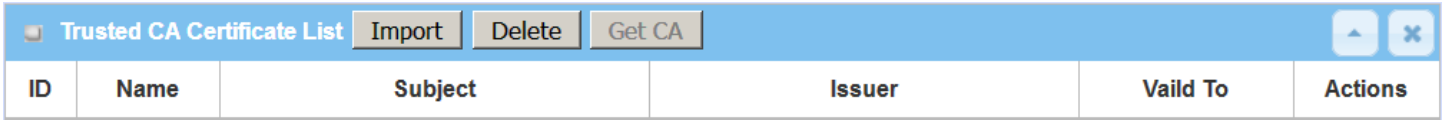
3.4.3 Trusted Certificate

Trusted Certificate includes Trusted CA Certificate List, Trusted Client Certificate List, and Trusted Client Key List. The Trusted CA Certificate List stores all the certificates of external trusted CAs. The Trusted Client Certificate List stores the others' certificates that will be trusted. And the Trusted Client Key List places the others' keys that will be trusted.

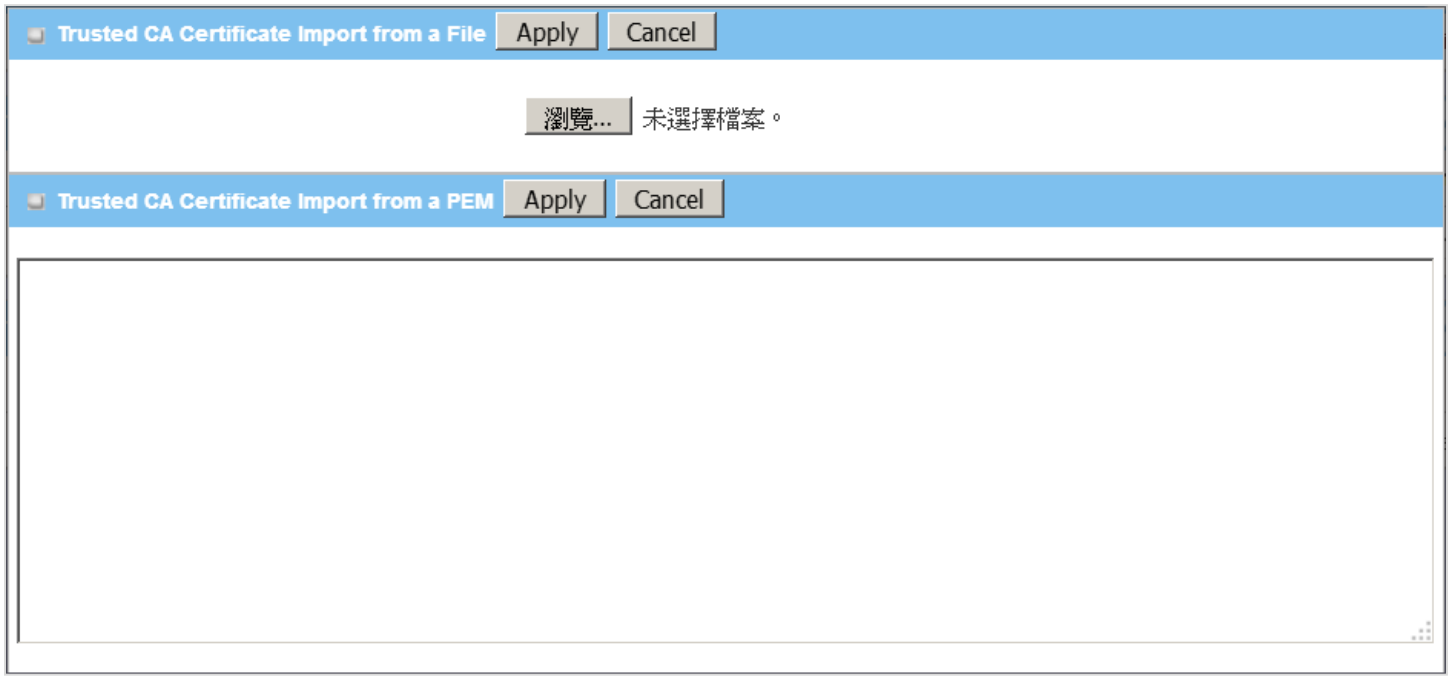
Trusted Certificate Setting

Go to **Object Definition > Certificate > Trusted Certificat**e to access the Trusted Certificate Setting page. The Trusted Certificate setting allows you to import trusted certificates and keys.

Import Trusted CA Certificate



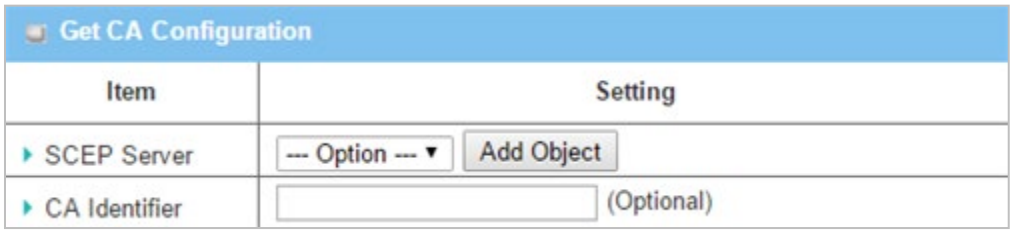
Click **Import** to open the Trusted CA import screen. You can import a Trusted CA certificate from an existing certificate file, or directly paste a PEM encoded text into the provided field.



Trusted CA Certificate List		
Item	**Value setting**	**Description**
Import from a File	A must-filled setting	Select a CA certificate file from your local directory and click the **Apply** button to import the specified CA certificate file to the gateway.
Import from a PEM	1. String format can be any text 2. A must-filled setting	You can directly fill in the PEM encoded CA certificate text, and click the **Apply** button to import the CA certificate to the gateway.
Apply	N/A	Import the certificate.

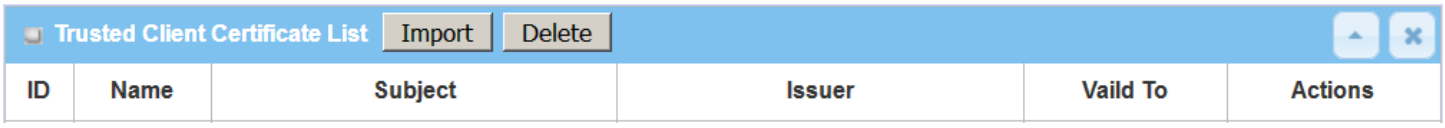
Cancel	N/A	Click the **Cancel** button to discard the import setting to return to the Trusted Certificates page.

Instead of importing a Trusted CA certificate, you can also get a CA certificate from a SECP server.
If **SCEP** is enabled (refer to **Object Definition** > **Certificate** > **Configuration**), click the **Get CA** button to open the **Get CA Configuration** screen.

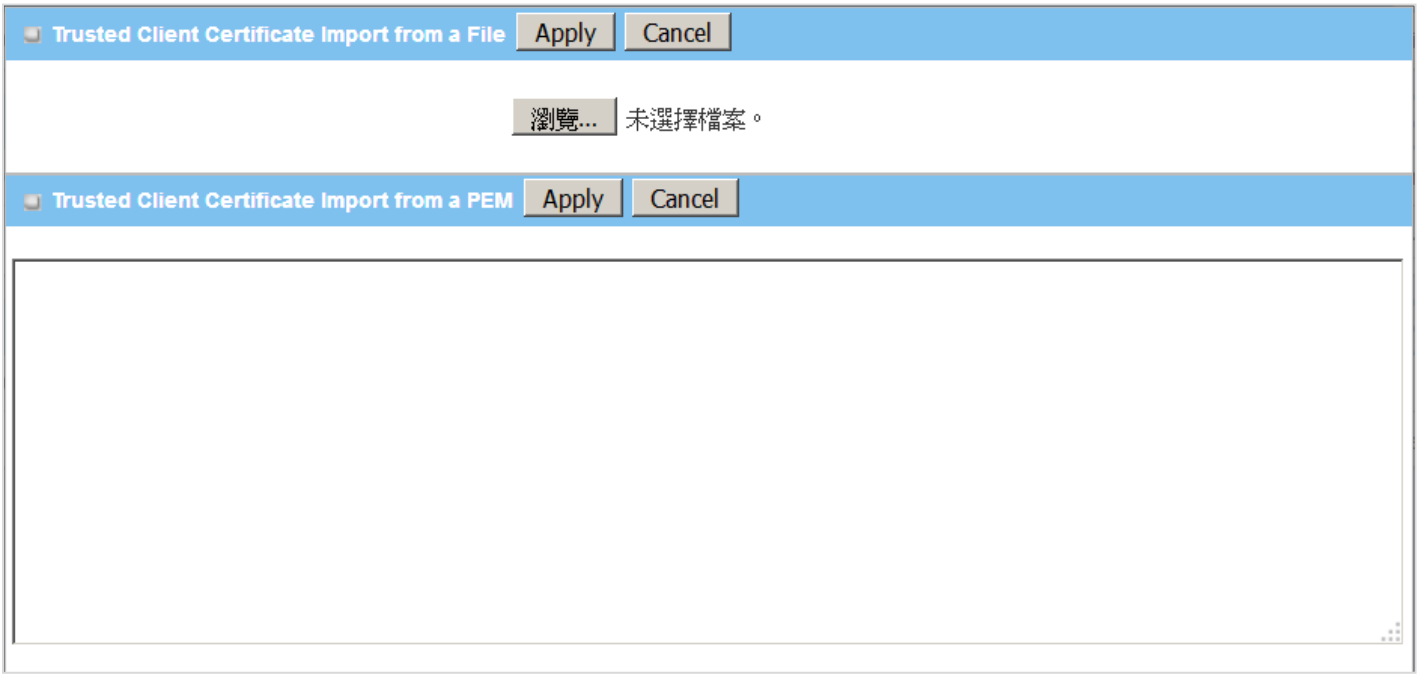


Get CA Configuration		
Item	**Value setting**	**Description**
SCEP Server	A must-filled setting	Select a **SCEP Server** that should be configured in External Servers (refer to **Object Definition** > **External Server** > **External Server**). You may click **Add Object** button to create a new external server.
CA Identifier	1. String format can be any text	Enter optional **CA Identifier** to identify which CA could be used for signing certificates.
Save	N/A	Save the settings.
Close	N/A	Return to the Trusted Certificates page.

Import Trusted Client Certificate



Click **Import** to open the **Trusted Client Certificate Import** screen. You can import a Trusted Client Certificate from an existing certificate file, or directly paste a PEM encoded CA certificate text as the certificate.

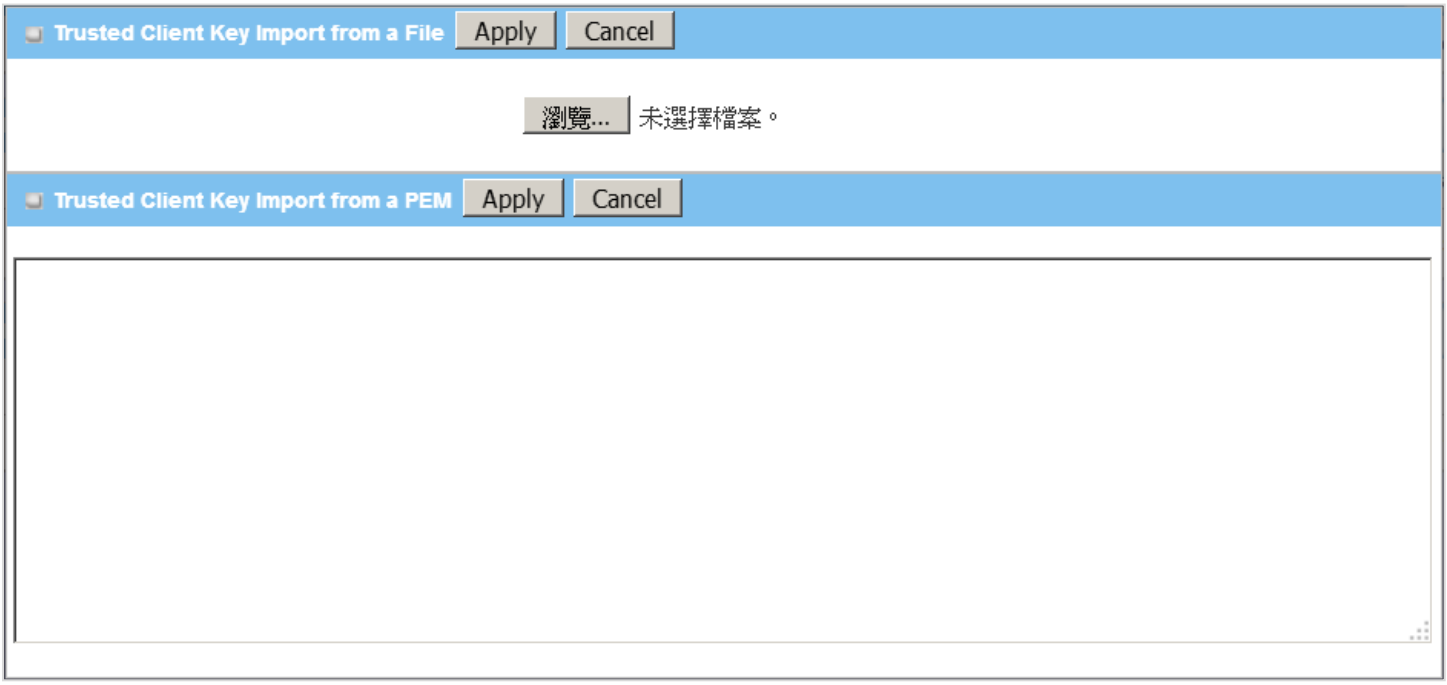


Trusted Client Certificate List		
Item	**Value setting**	**Description**
Import from a File	A must-filled setting	Select a certificate file from the local directory and click the **Apply** button to import the specified certificate file.
Import from a PEM	1. String format can be any text 2. A must-filled setting	You can directly fill in the PEM encoded text, and click the **Apply** button to import it.
Apply	N/A	Click the **Apply** button to import certificate.
Cancel	N/A	Click the **Cancel** button to discard the import setting to return to the Trusted Certificates page.

Import Trusted Client Key



Click **Import** to open the **Trusted Client Key Import** screen. You can import a Trusted Client Key from an existing file, or directly paste a PEM encoded string as the key.



Trusted Client Key List		
Item	**Value setting**	**Description**
Import from a File	A must-filled setting	Select a certificate file from the local directory and click the **Apply** button to import the specified certificate file.
Import from a PEM	1. String format can be any text 2. A must-filled setting	You can directly fill in the PEM encoded text, and click the **Apply** button to import it.
Apply	N/A	Click the **Apply** button to import certificate.
Cancel	N/A	Click the **Cancel** button to discard the import setting to return to the Trusted Certificates page.

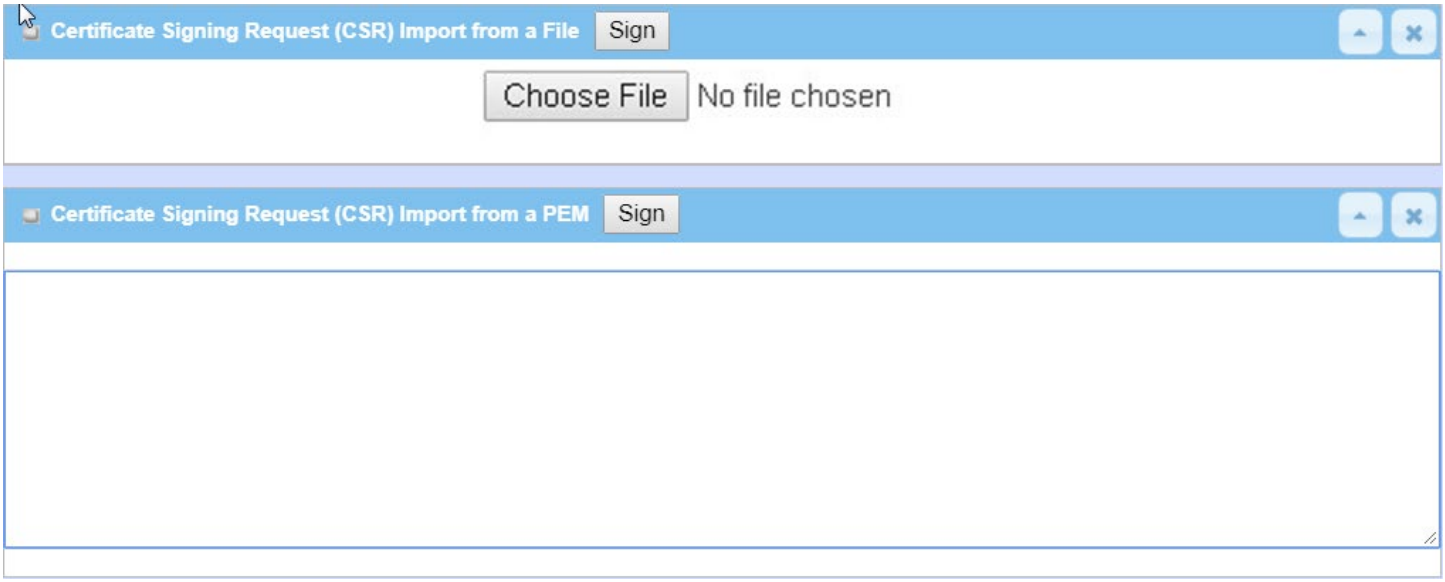
3.4.4 Issue Certificate

When you have a Certificate Signing Request (CSR) that needs to be certificated by the root CA of the device, you can apply for a CSR to be signed by root CA. If the gateway signs a CSR successfully, the "Signed Certificate View" window will show the content of the signed certificate. You may also download the certificate to your local directory.

Issue Certificate Setting

Go to **Object Definition > Certificate > Issue Certificate** to access the Issue Certificate Setting page.
The Issue Certificate setting allows you to import Certificate Signing Request (CSR) to be signed by root CA.

Import and Issue Certificate

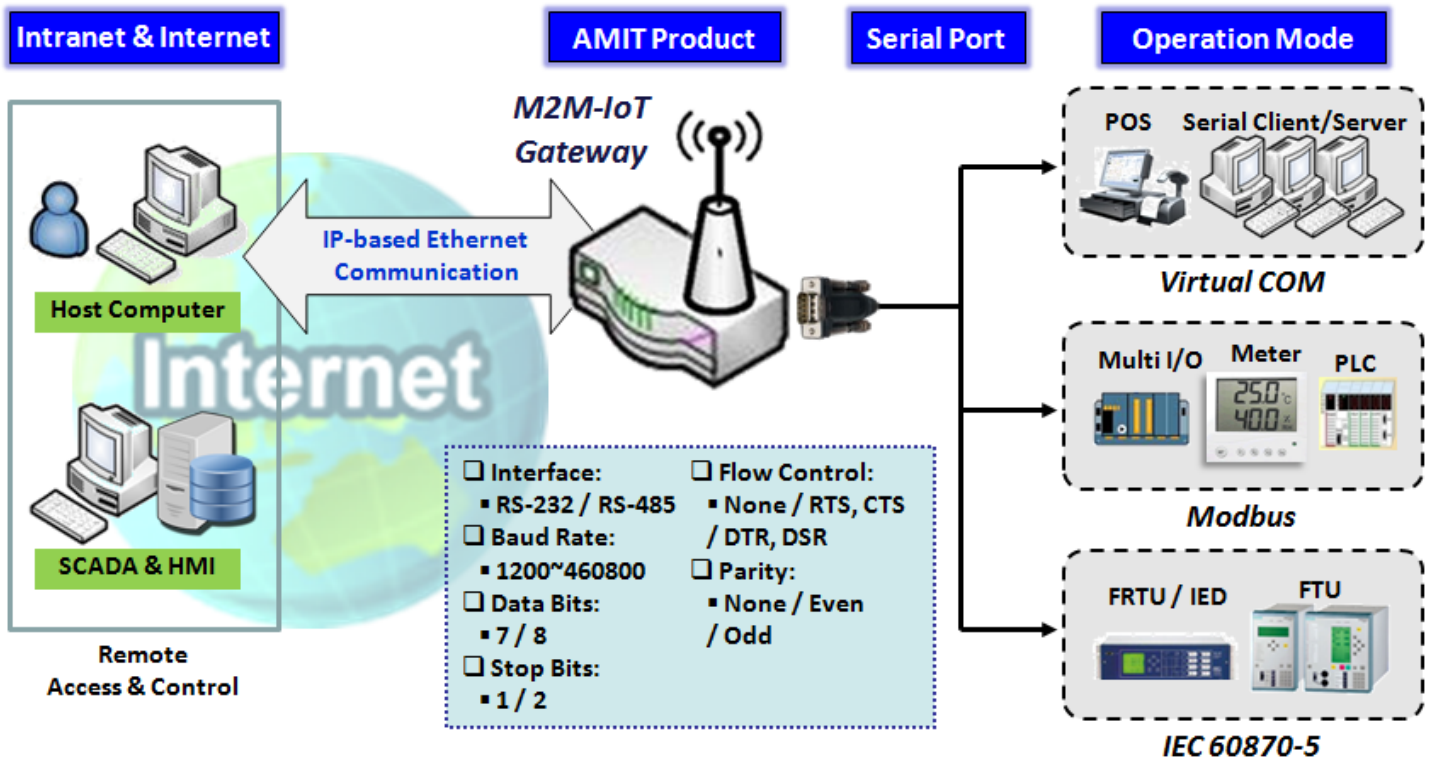


Certificate Signing Request (CSR) Import from a File		
Item	**Value setting**	**Description**
Certificate Signing Request (CSR) Import from a File	A must-filled setting	Select a certificate signing request file from the local directory.
Certificate Signing Request (CSR) Import from a PEM	1. String format can be any text 2. A must-filled setting	Enter the certificate signing request PEM encoded text in the field.
Sign	N/A	Sign the imported certificate by root CA.

Chapter 4 Field Communication

4.1 Bus & Protocol

The gateway may equip one or more serial port(s) for serial communication with RS-232 or RS-485 serial devices to integrate with an IP-based Ethernet LAN, allowing for access to serial devices over a local LAN or the Internet.



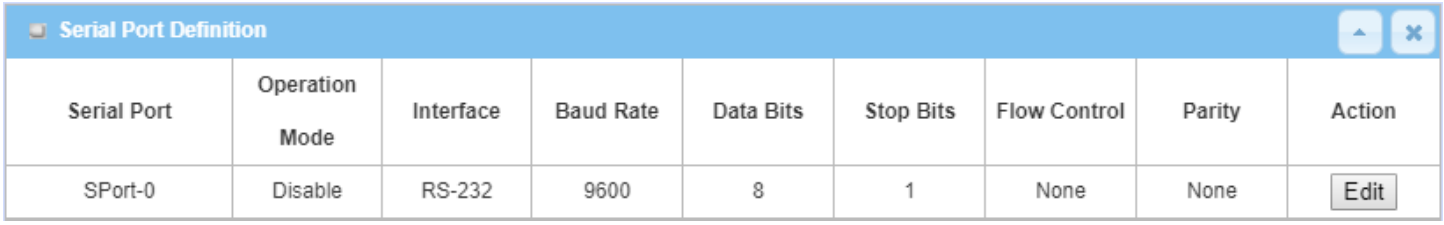
4.1.1 Port Configuration

Before using the supported field communication function, like Virtual COM or Modbus, you need to configure the physical communication ports first.
The port configuration screen allows you to configure the operation mode and physical layer settings for each serial interface and to switch from one communication protocol to another for the serial port. The number of ports and type of the supported protocols could be different depending on the model.

Port Configuration Setting

Go to **Field Communication > Bus & Protocol > Port Configuration** to access the Port Configuration Setting page.

In "Port Configuration" page, you can configure the physical serial ports with settings such as the operation mode and flow control.



Port Configuration Window		
Item	**Value setting**	**Description**
Serial Port	*N/A*	It displays the serial port ID of the serial port. Note the number of serial ports varies depending on the model.
Operation Mode	**Disable** is set by default	Select the operation mode for the serial interface. The available modes are **Disable, Virtual COM** or **Modbus**.
Interface	**RS-232** is set by default	Select the physical interface type for this port: RS-232 or RS-485. Note that the supported interface type depends on the model.
Baud Rate	**9600** is set by default	Select the appropriate baud rate for serial device communication. RS-232: 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200. RS-485 can use higher baud rate: 230400 or 460800. It depends on the cable length and the netowrk environment. The longer the cable, the lower the baud it can support.
Data Bits	**8** is set by default	Select 8 or 7 for data bits.
Stop Bits	**1** is set by default	Select 1 or 2 for stop bits.
Flow Control	**None** is set by default	Select None / RTS, CTS / DTS, DSR for Flow Control in RS-232 mode. The supporting of Flow Control depends on the purchased model.
Parity	**None** is set by default	Select None, Even, or Odd for Parity bit.
Action	N/A	Click **Edit** button to change the operation mode, or modify the parameters mentioned above for the serial interface communication.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings.

4.1.2 Virtual COM

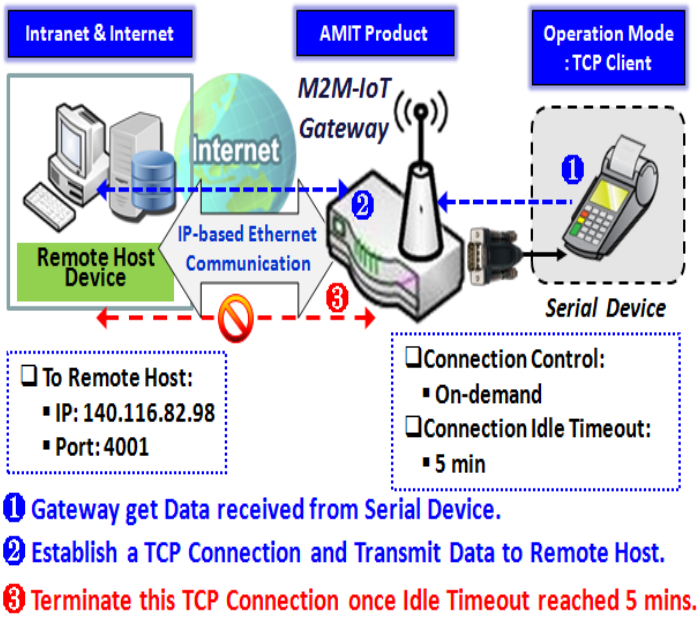
A virtual COM port on a host PC allows access to a serial device connected to a serial port on the gateway. It provides connection flexibility across a network built on different systems to achieve Ethernet pass-through communication.

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	☐	Edit

Virtual COM can operate in different modes: Disable, TCP Client, TCP Server, UDP, and RFC2217 modes for remote access. These operation modes are illustrated below.

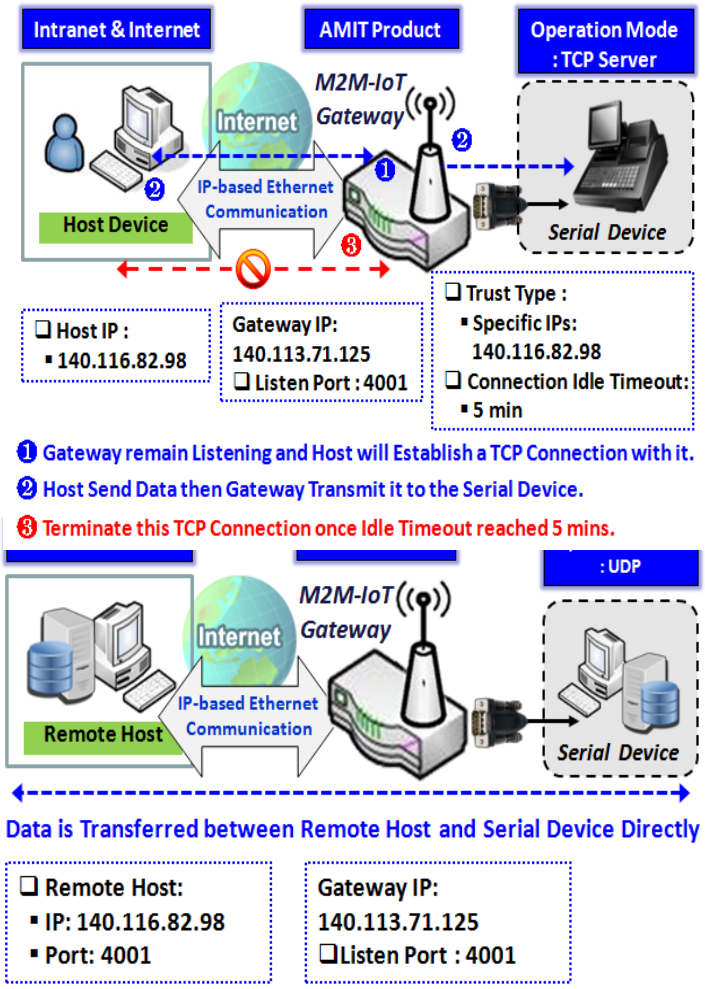
TCP Client Mode



The "TCP Client" mode allows the gateway to establish a TCP connection to a host computer. On the other hand, the “On-demand” mode only establishes a TCP connection when the gateway receives data from a connected serial device. The gateway will automatically disconnect the TCP session according to the settings of the TCP alive check timeout or idle timeout.

TCP Server Mode

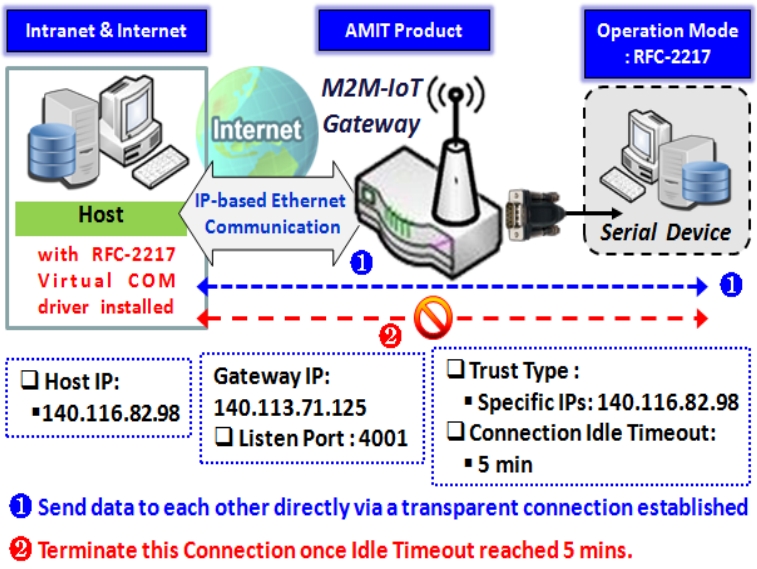
When the gateway waits passively to accept connection request from a host computer, the mode is set as “TCP Server”. In this mode, the gateway provides a unique "IP: Port" address for server connection setting. It allows multiple hosts to collect data from the same serial device at the same time. After the data has been transferred, the TCP connection to the host will be automatically disconnected according to the settings of the TCP alive check timeout or idle timeout.



UDP Mode

The “UDP” mode allows both a remote host and a serial device to establish a TCP connection actively. In this mode, the UDP data can be transferred simultaneously between the gateway and multiple host computers, making this mode ideal for message display applications.

RFC2217 Mode



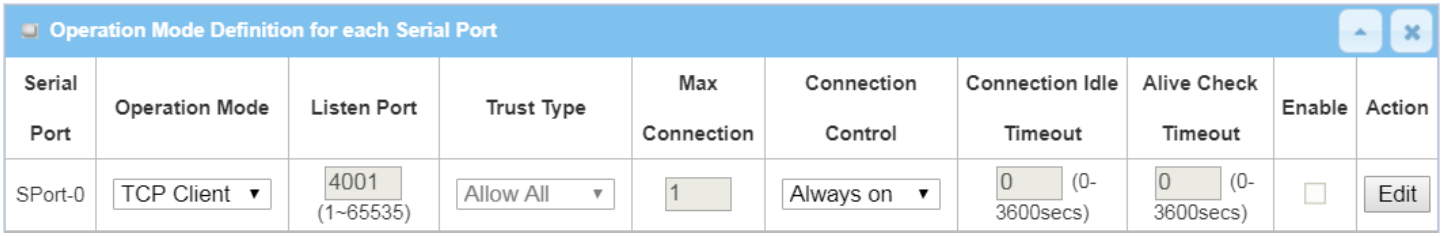
RFC2217 defines general COM port control options on the basis of Telnet. A host computer with RFC2217 driver installed can monitor and manage a remote serial device connected to the gateway's serial port, as though they were directly connected to the host.
This method allows a host computer to directly send data to and receive data from a serial device via the gateway. The gateway supports up to 4 host computers.

Virtual COM Setting

To use the Virtual COM function, specify the operation mode (i.e. Disable, TCP Client, TCP Server, UDP, and RFC2217) on the multi-function serial port first.
Go to **Field Communication > Bus & Protocol > Port Configuration** to access the Operation Mode Definition page.

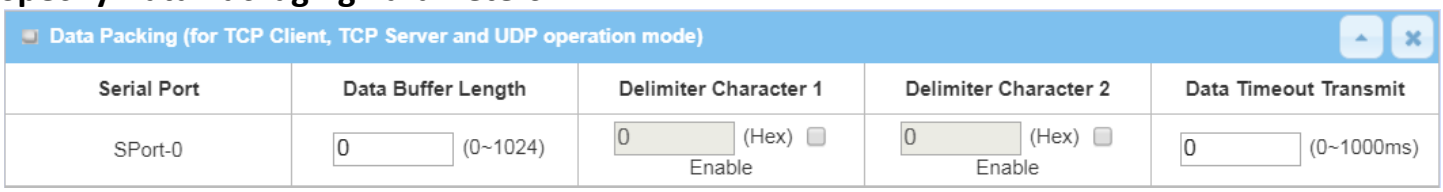
Enable TCP Client Mode

Configure the gateway as the TCP (Transmission Control Protocol) Client. In TCP Client mode, the gateway requests a TCP connection with a TCP server. The gateway disconnects from the server when the connection is idle for a specified period. You may also enable full-time connection with the TCP server.



Enable TCP Client Mode Window		
Item	**Value setting**	**Description**
Operation Mode	A must-filled setting	Select **TCP Client**.
Connection Control	**Always on** is set by default	Choose **Always on** for a TCP full-time connection. Otherwise, choose **On-Demand** to initiate a TCP connection only when needed.
Connection Idle Timeout	1. 0 is set by default 2. Range 0 to 3600 sec.	Enter the idle timeout to specify the length of time that a connection remains idel before it can be deleted. Idle timeout is only available when **On-Demand** is selected as the **Connection Control** method. *Value Range*: 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. It allows the gateway to periodically check the connection and to re-establish the TCP connection when it is disconnected. Alive check timeout is only available when **On-Demand** is selected as the **Connection Control** method. *Value Range*: 0 ~ 3600 seconds.
Enable	The box is unchecked by default.	Activate the corresponding serial port to operate in the specified mode.
Save	*N/A*	Save the configuration

Specify Data Packaging Parameters



Data Packing Configuration		
Item	**Value setting**	**Description**
Data Buffer Length	1.An optional setting 2.Default value is 0	Enter the data buffer length for the serieal port. *Value Range*: 0 ~ 1024.
Delimiter Character 1	1.An optional setting 2.Default value is 0	Activate the Delimiter character 1 in Hexdecimal values. *Value Range*: 0x00 ~ 0xFF.
Delimiter Character 2	1.An optional setting 2.Default value is 0	Activate the Delimiter character 2 in Hex value. *Value Range*: 0x00 ~ 0xFF.
Data Timeout Transmit	1.An optional setting 2.Default value is 0	Enter the data timeout interval for transmitting serial data through the port. By default, it is set to 0 and the timeout function is disabled. *Value Range*: 0 ~ 1000ms.
Save	*N/A*	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	☐	Edit
2		4001	SPort-0	☐	Edit
3		4001	SPort-0	☐	Edit
4		4001	SPort-0	☐	Edit

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

Enable TCP Server Mode

Configure the gateway as the TCP (Transmission Control Protocol) Server. The configuration also allows you to specify specific TCP clients that will be allowed for serial data transmission. The TCP Server supports up to 128 simultaneous connections to receive serial data from multiple TCP clients.

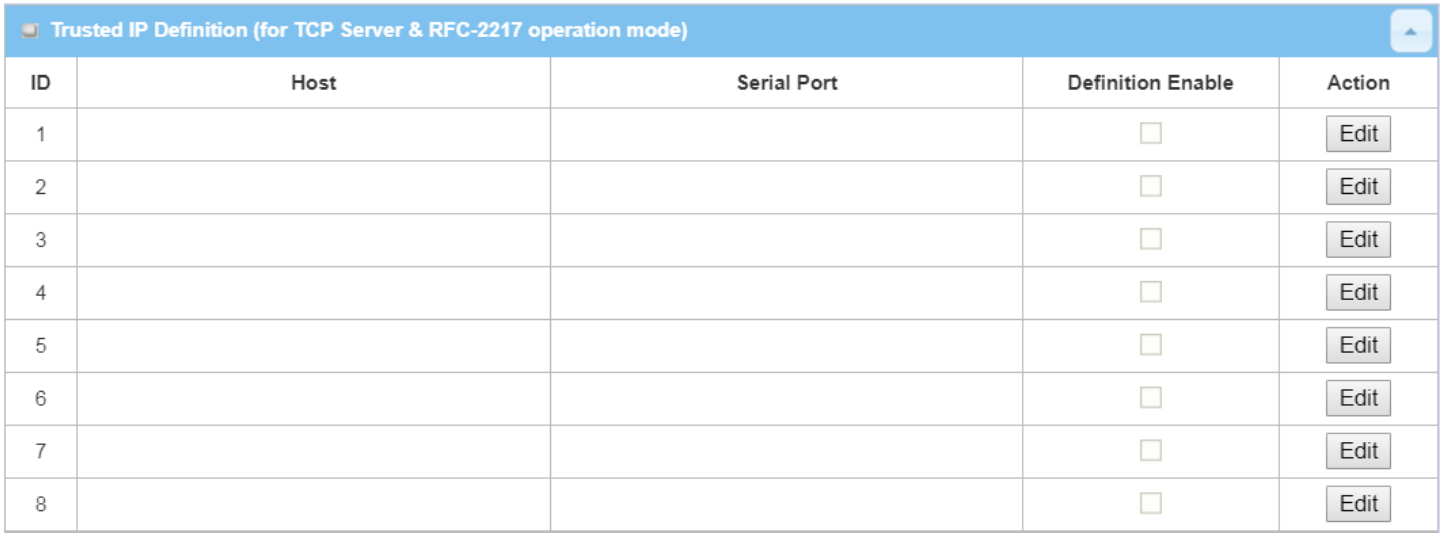
Operation Mode Definition for each Serial Port

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)	☐	Edit

Enable TCP Server Mode Window		
Item	**Value setting**	**Description**
Operation Mode	A must-filled setting	Select **TCP Server** mode.
Listen Port	4001 is set by default	Enter the listening port for TCP connection. *Value Range*: 1 ~ 65535.
Trust Type	**Allow All** is set by default	Choose **Allow All** to allow any TCP clients to connect. Otherwise, choose **Specific IP** to allow only the specified 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. *Value Range*: 1 ~ 128.
Connection Idle Timeout	1. 0 is set by default 2. Range 0 to 3600 sec.	Enter the idle timeout to specify the length of time that a connection remains idel before it can be deleted. Idle timeout is only available when **On-Demand** is selected as the **Connection Control** method. *Value Range*: 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. It allows the gateway to periodically check the connection and to re-establish the TCP connection when it is disconnected. Alive check timeout is only available when **On-Demand** is selected as the **Connection Control** method. *Value Range*: 0 ~ 3600 seconds.
Enable	The box is unchecked by default.	Activate the corresponding serial port to operate in the specified mode.
Save	*N/A*	Save the settings.

Specify TCP Clients for TCP Server Access

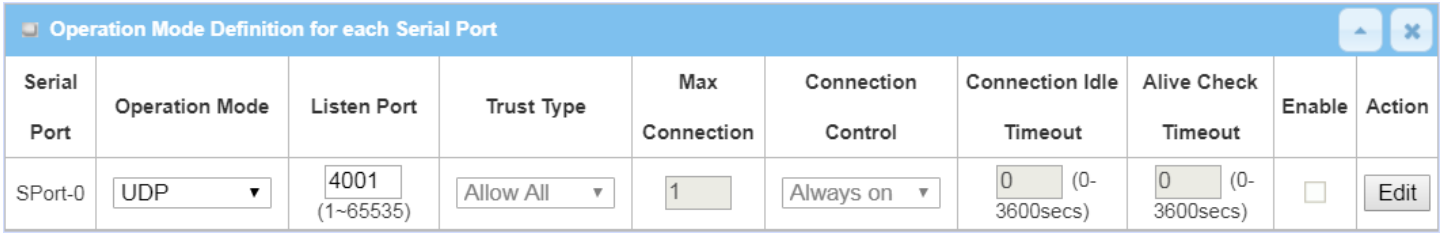
If you select Specific IPs as the trust Type, enter the host information in the Trusted IP Definition window. The settings are valid for both TCP Server and RFC-2217 modes.



Specify TCP Clients Window		
Item	**Value setting**	**Description**
Host	A must-filled setting	Enter the IP address range of allowed TCP clients.
Serial Port	The box is unchecked by default	Check the box to apply the rule to the selected serial port.
Definition Enable	The box is unchecked by default	Enable the rule.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

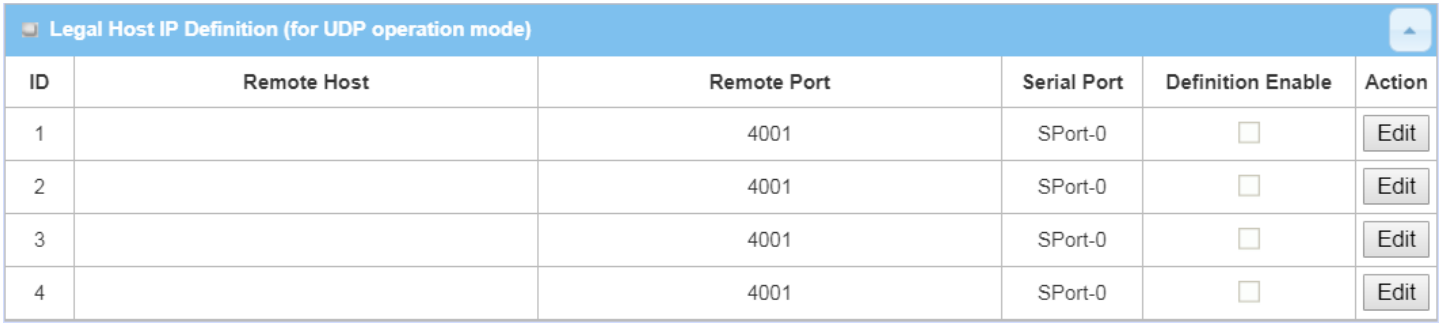
Enable UDP Mode

Unlink TCP, the UDP mode provides connectionless communication, which enables you to forward data from a serial device to multiple host computers in a single transmission, and vice versa, making this mode ideal for message display applications.



Enable UDP Mode Window		
Item	**Value setting**	**Description**
Operation Mode	A must-filled setting	Select **UDP** mode.
Listen Port	4001 is set by default	Enter the listening port of UDP connection. *Value Range*: 1 ~ 65535
Enable	The box is unchecked by default.	Activate the corresponding serial port to operate in the specified mode.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

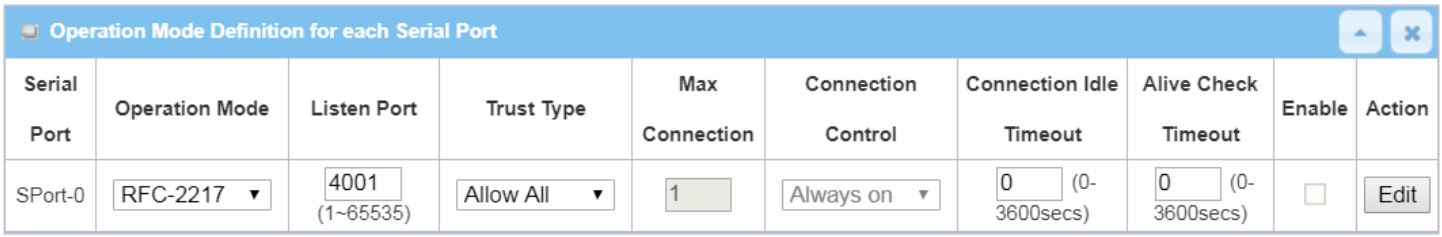
Specify Remote UDP



Specify Remote UDP hosts Window		
Item	**Value setting**	**Description**
Host	A must-filled setting	Click **Edit** to enter the IP address range of remote UDP hosts.
Remote Port	4001 is set by default	Enter the UDP port of peer UDP hosts. *Value Range*: 1 ~ 65535
Serial Port	SPort-0 is set by default	Apply the UDP hosts configuration to the selected serial port. Up to 4 UDP servers can be configured for each serial port.
Definition Enable	The box is unchecked by default	Enable the rule.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

Enable RFC-2217 Mode

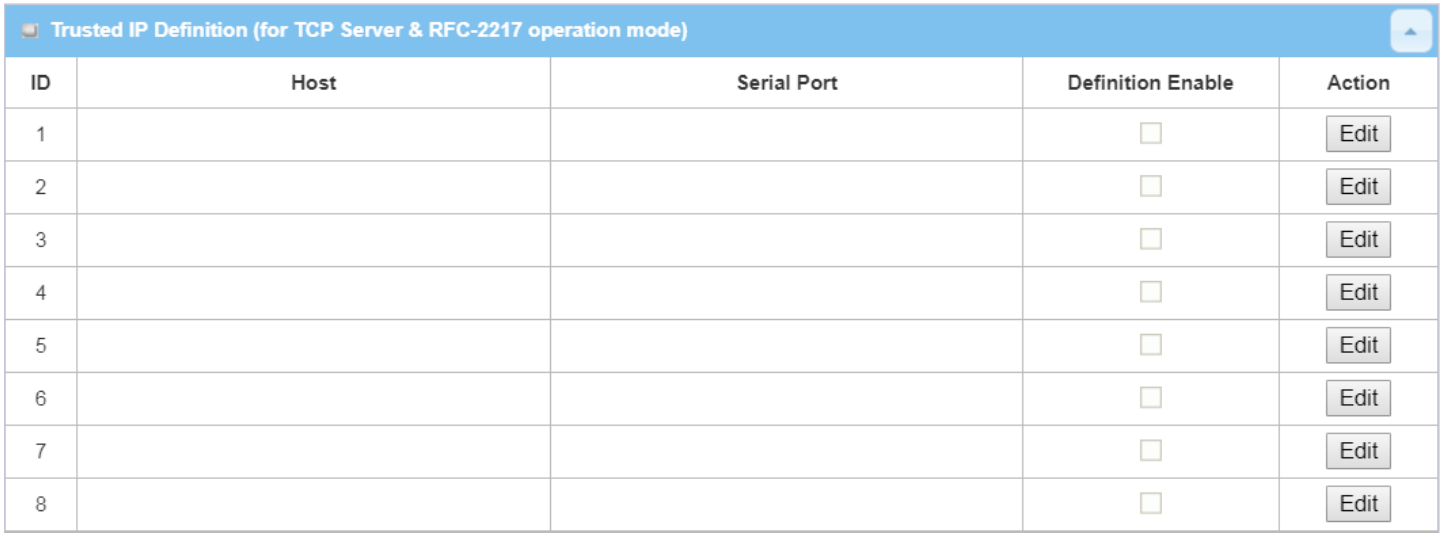
RFC-2217 defines general COM port control options through Telnet. With the RFC-2217 mode, host computers can monitor and manage remote serial devices, as though they were directly connected to the local serial port.



Enable RFC-2217 Mode Window		
Item	**Value setting**	**Description**
Operation Mode	A must-filled setting	Select **RFC-2217** mode.
Listen Port	4001 is set by default	Indicate the listening port of RFC-2217 connection. *Value Range*: 1 ~ 65535
Trust Type	**Allow All** is set by default	Choose **Allow All** to allow any clients to connect. Otherwise choose **Specific IP** to limit certain clients.
Connection Idle Timeout	1. 0 is set by default 2. Range 0 to 3600 sec.	Enter the idle timeout to specify the length of time that a connection remains idel before it can be deleted. Idle timeout is only available when **On-Demand** is selected as the **Connection Control** method. *Value Range*: 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. It allows the gateway to periodically check the connection and to re-establish the TCP connection when it is disconnected. Alive check timeout is only available when **On-Demand** is selected as the **Connection Control** method. *Value Range*: 0 ~ 3600 seconds.
Enable	The box is unchecked by default.	Check the **Enable** box to activate the corresponding serial port in specified operation mode.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

Specify Remote Host for Access

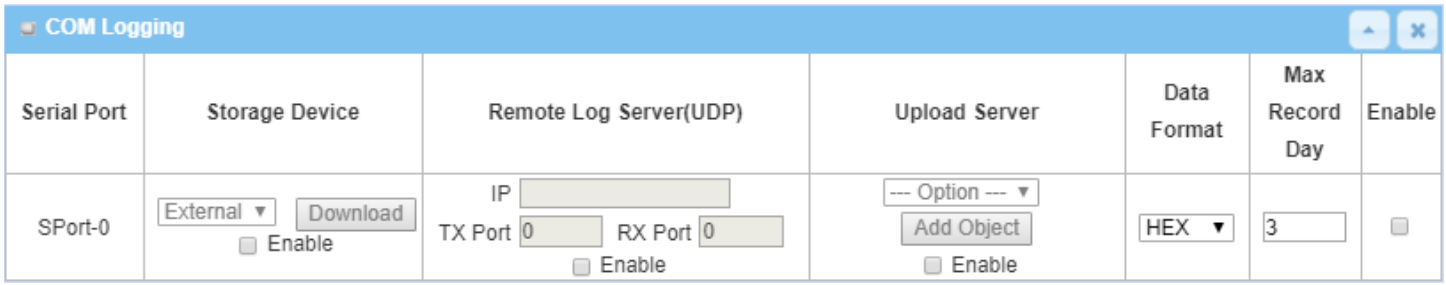
If you select Specific IPs as the trust Type, enter the host information in the Trusted IP Definition window. The settings are valid for both TCP Server and RFC-2217 modes.



Specify TCP Clients Window		
Item	**Value setting**	**Description**
Host	A must-filled setting	Enter the IP address range of allowed hosts.
Serial Port	The box is unchecked by default	Check the box to apply the rule to the selected serial port.
Definition Enable	The box is unchecked by default	Enable the rule.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

Configure VirtualCOM Data Logging

You can monitor the traffic of a serial port by configuring the data logging settings to generate logs. Refer to **4.2 Data Logging** for more information.



COM Logging Configuration Window		
Item	**Value setting**	**Description**
Storage Device	The box is unchecked by default.	Check the **Enable** box and save data logs to the attached storage (USB or SD-card) device. The log files will be stored in the directory with the file names as "*\virtual-com-log\SPort-n\$Date*". Click the **Download** button to download the log files to the local directory (*.csv).
Remote Log Server (UDP)	The box is unchecked by default.	Enable remote logging to send data logs to a remote server. You also need to specify the IP address and port number of the log server. *Value Range*: 1 ~ 65535, and 0 for disabled by default.
Upload Server	The box is unchecked by default.	Check the **Enable** 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 external server. The device will upload the log files (*.csv.gz) every hour to the designated FTP server.
Data Format	**HEX** is set by default	Specify the format for data logs. It can be **HEX** or **ASCII**.
Max Record Day	**3** is set by default	Enter the maximum number of consecutive days to record data logs. *Value Range*: 1 ~ 30 days.
Enable	The box is unchecked by default.	Activate the data logging function for the corresponding serial port with the above specified configuration.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

4.1.3 Modbus

Modbus is one of the most popular protocols used in industry automation, supporting traditional RS-232/422/485 devices and the more recent Ethernet devices. Many industrial devices, such as PLCs, DCSs, HMIs, instruments, and smart meters, adopt the Modbus protocol in a master-slave communication architecture.

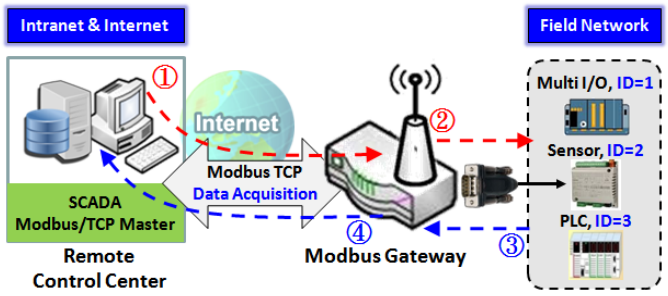
However, the Ethernet-based Modbus protocol is different from the original serial-based protocols. In order to integrate different types of communication systems, the IoT gateway should automatically and intelligently translate between Modbus TCP (Ethernet) and Modbus RTU/ASCII (serial) protocols, allowing Ethernet-based PLCs to control serial devices through RS-232/422/485 without additional programming effort. Note that all Modbus devices must be configured with the same communication protocols and settings.

Serial Port Definition

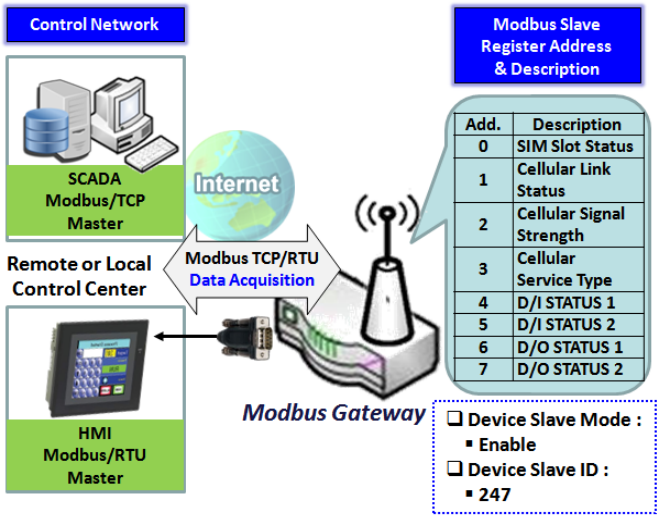
Serial Port	Operation Mode	Interface	Baud Rate	Data Bits	Stop Bits	Flow Control	Parity	Action
SPort-0	Modbus	RS-485	9600	8	1	None	None	Edit

Modbus gateway Scenario

The IoT gateway serves as a Modbus gateway through which the management facilities in the remote control center (e.g. Modbus TCP master, and the SCADA server) Modbus devices can be managed and accessed. Data acquisition and management operation such as configuration modification can be accomplished.



Modbus Slave Scenario



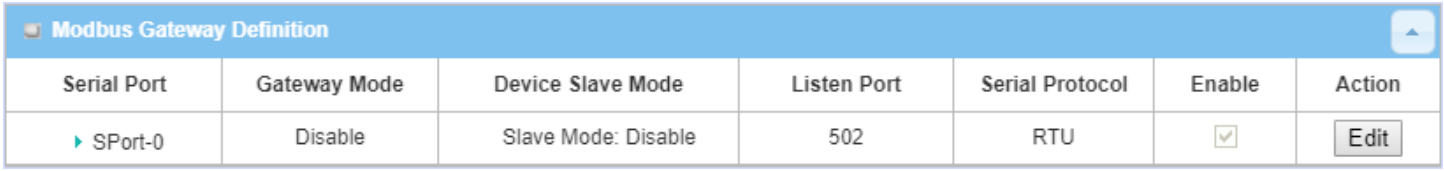
The gateway can also act as a Modus slave, which is capable of executing commands and replying to the Modbus master's request for information, such as device status, DI/DO status, and network status.

Modbus Setting

Go to **Field Communication > Bus & Protocol > Modbus** to access the Modbus Setting page.

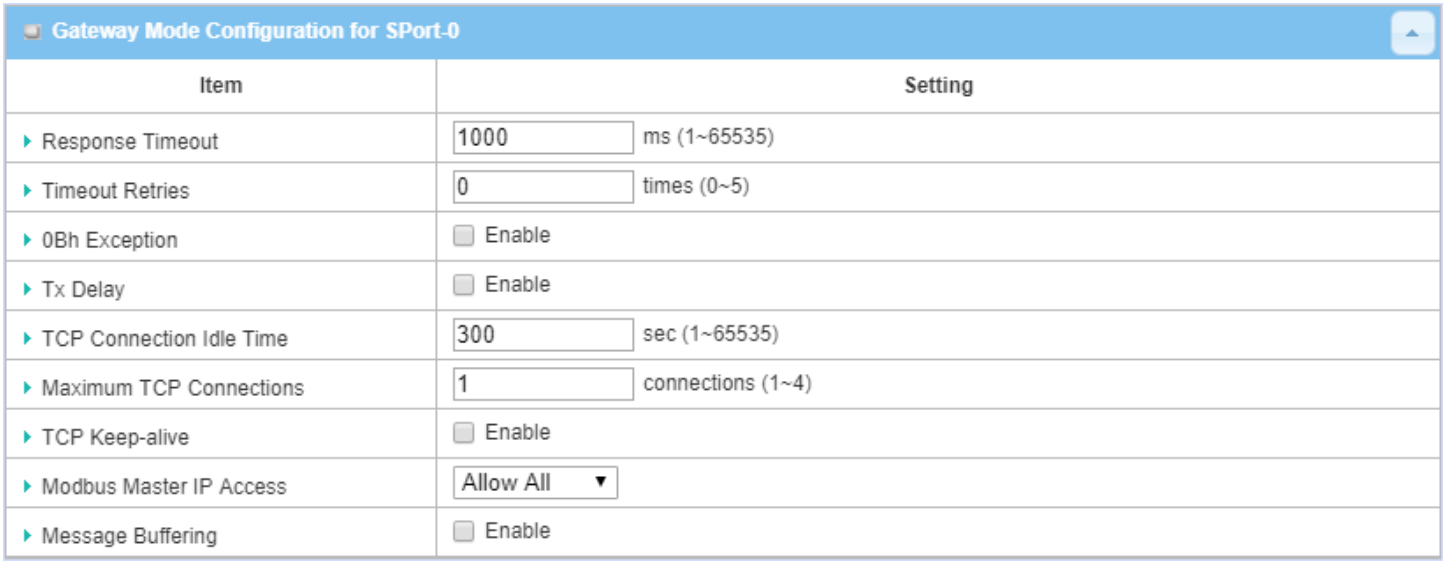
The Modbus Setting page enables you to configure the gateway to operate as a Modbus gateway to allow access to Modbus TCP devices (connected through an Ethernet network) and Modbus RTU/ASCII devices (connected to the serial ports of the gateway). Make sure that Modbus communication is enabled on the designated serial ports on the Port Configuration page (go to **Field Communication > Bus & Protocol > Port Configuration**) as described in the following sections.

Define Modbus Gateway Function for Serial Ports



Modbus gateway Definition		
Item	**Value setting**	**Description**
Serial Port	N/A	Select the name of the serial port to be configured, e.g. SPort-0. The number of serial ports varies depending on the device model.
gateway Mode	**Disable** is set by default	Specify the Modbus gateway mode for the selected serial port: Disable, Serial as Slave, or Serial as Master. A serial port can be attached to only one Modbus master, or daisy-chained a group of Modbus salve devices. **Disable**: Select this to disable the respective Modbus gateway function for the selected serial port. **Serial as Slave**: Select this when the attached serial device(s) are all Modbus slave devices. **Serial as Master**: Select this when the attached serial device is a Modbus master device.
Device Slave Mode	**Disable** is set by default	Activate the integrated Modbus slave function and enter the preferred ID for the integrated Modbus slave. The device can then act as a Modbus slave device and can be accessed with legacy Modbus Function Code from the SCADA management system. Refer to the following table for the Supported Modbus commands. Value Range: 1 ~ 247.
Listen Port	1. **502** is set by default 2. Range 1 to 65535	Specify the Listening Port number if slave device(s) is attached to the selected serial port. Please assign a different number for each serial port. *Value Range*: 1 ~ 65535.
Serial Protocol	**RTU** is set by default	Select the serial protocol for communicating with the attached Modbus device(s). It can be **RTU** or **ASCII**.
Enable	N/A	Shows whether the specific Modbus serial port is enabled or disabled. To enable or disable a Modbus serial port, go to **Field Communication > Bus & Protocol > Port Configuration**, and set the operation mode as **Modbus**.

Specify Gateway Configuration

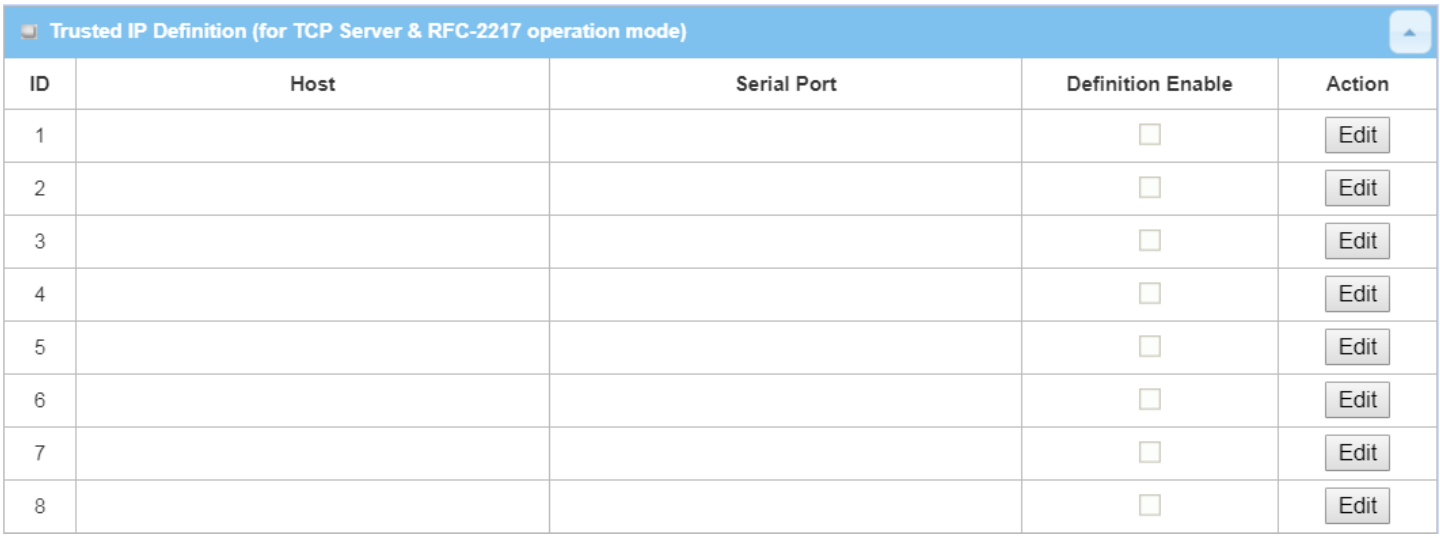


gateway Mode Configuration for SPort-n		
Item	**Value setting**	**Description**
Response Timeout	**1000 ms** is set by default	Set the response timeout of the slave. If the slave does not respond within the specified period, data would be discarded. A master or slave can be a serially attached Modbus device or a remote device connected through the network. *Value Range*: 1 ~ 65535.
Timeout Retries	**0** is set by default	If the slave does not respond to the master's request, the gateway will resend the request saved in the buffer. If Timeout retries is set to 0, the gateway will not buffer master requests. For the retry number other than zero, the gateway will save the master request in the buffer and resend the request according to the specified number of retries. Once the maximum number of retires has been reached, 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 error message will be sent instead. Value Range: 0 ~ 5.
0Bh Exception	The box is unchecked by default.	Send a 0Bh exception code message to notify the Modbus master that the slave device does not respond within the timeout interval.
Tx Delay	The box is unchecked by default.	Enter the minimum amount of time to wait before sending the next message after receiving a response. When Tx Delay is enabled, the gateway would insert a Tx delay between master requests.
You can set up TCP connection settings to allow remote Modbus Master to access the Modbus gateway. You can also configure authorized masters for Modbus communication.		
TCP Connection Idle Time	1. **300** is set by default 2. Range 1 to 65535	Enter the idle timeout in seconds. The TCP session will be terminated automatically if the TCP connection has been idled for the specified amount of time. *Value Range*: 1 ~ 65535.

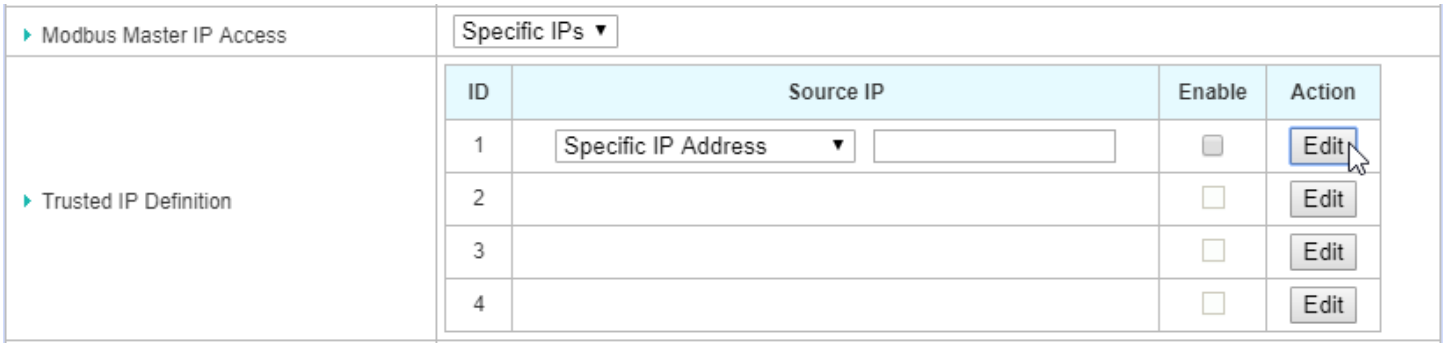
Maximum TCP Connections	1. 4 is set by default 2. Range 1 to 4	Enter the maximum number of simultaneous TCP connections allowed. Value Range: 1 ~ 4.
TCP Keep-alive	The box is unchecked by default.	Enable this to ensure that the TCP session stays connected.
Modbus Master IP Access	**Allow All** is selected by default.	Specify authorized masters on the TCP network. Select **Allow All** to allow any Modbus master to access the attached slave(s). Otherwise, specify the trusted Modbus masters to restrict the access to slave device in the Trusted IP Definition page shown below.

Specify Trusted Modbus Masters on the TCP Network

If you select Specific IPs for Modbus Master IP Access, enter the host information in the Trusted IP Definition table to allow them to access the slave devices.



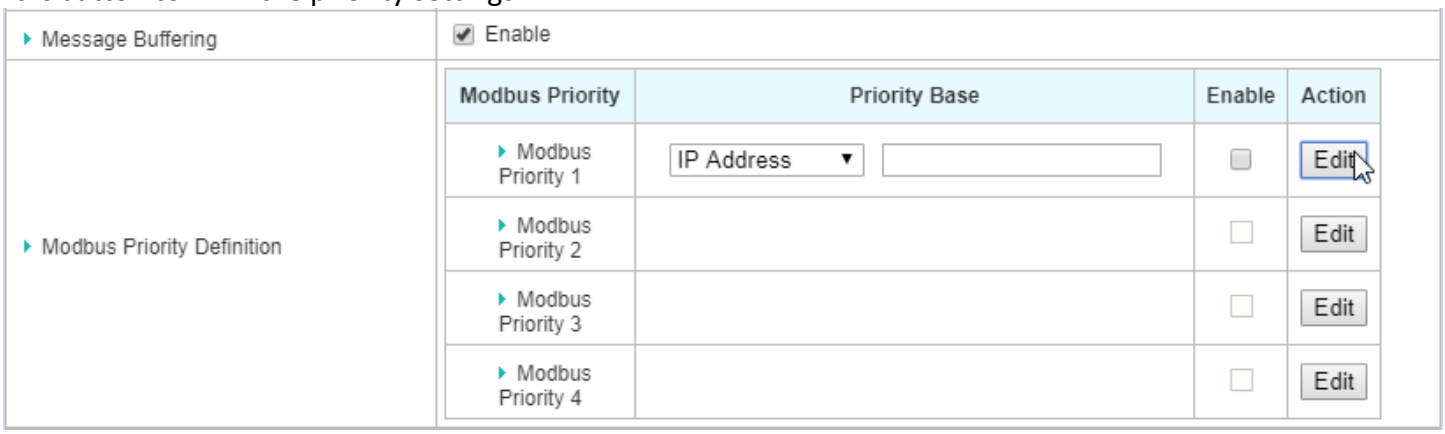
Specify TCP Clients Window		
Item	**Value setting**	**Description**
Host	A must-filled setting	Enter the IP address range of the allowed hosts.
Serial Port	The box is unchecked by default	Check the box to apply the rule to the selected serial port.
Definition Enable	The box is unchecked by default	Enable the rule.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.



Item	Value setting	Description
Source IP	A must-filled setting	Select **Specific IP Address** to allow only a single master with the specified IP address to access the attached slave(s). Select **IP Range** to specify the range of IP addresses of the master devices to access the attached slave(s). Select **IP Address-based Group** to allow only a pre-defined group of master devices to access the attached slave(s). **Note:** Click **Add Rule** to access the Host grouping page. Refer to **Object Definition > Grouping > Host grouping** for the pre-defined group list.
Enable	Unchecked by default	Enable this rule.

Modbus Priority Definition

Enable Message Buffering to prioritize master request queues for transmission to Modbus slaves. Click the **Edit** button to fill in the priority settings.

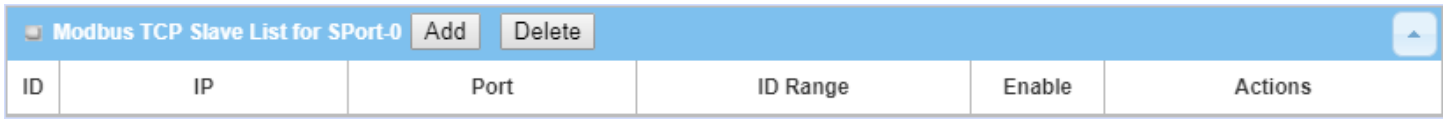


Item	Value setting	Description
Message Buffering	1. Unchecked by default 2. Buffer up to 32 requests	Check the **Enable** box to allow up to 32 requests from a master to be buffered, and the Modbus Priority Definition dialog will appear. The priority of the request queues for buffering messages can be set by the master devices' IP address, remote Slave ID, or Function Code.
Modbus Priority	N/A	Modbus Priority 1 ~ Modbus Priority 4.
Priority Base	IP Address by Default	Specify the priority for a Modbus using one of the following methods: **IP Address**, **Slave ID**, and **Function Code**. The buffered Modbus message that matched the specified method will be handled with given priority.

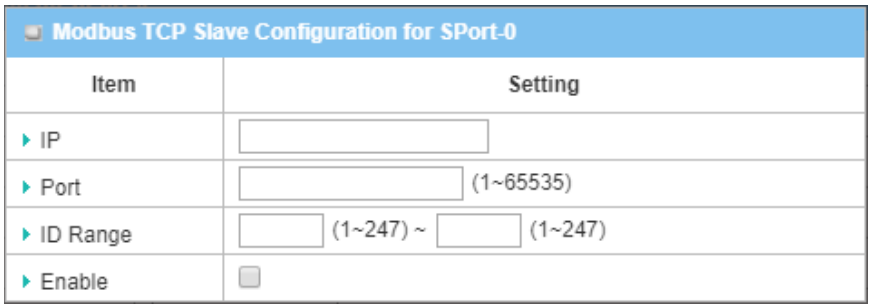
		The Modbus master's requests can be buffered to a priority queue according to the master's IP address if requests are coming from a remote master, or the remote slave's device ID if requests are coming from serially attached device, or the specific Function Code issued by a master device.
Enable	Unchecked by default	Enable the priority settings.
Save	N/A	Save the settings.

Specify Modbus TCP Slave device(s)

If there is a Modbus master device directly attached to a serial port of the Modbus gateway, specify the Modbus TCP slave device(s) to which the requests from the attached Modbus RTU/ASCII master device can be sent.



Click **Add** to open the **Modbus TCP Slave Configuration** screen.



Modbus Remote Slave Configuration		
Item	**Value setting**	**Description**
IP	A must-filled setting	Enter the IP address of the remote Modbus TCP slave device.
Port	1. A must-filled setting 2. Range 1 to 65535	Enter the TCP port of the remote Modbus TCP slave device. *Value Range*: 1 ~ 65535.
ID Range	Range 1 to 247	Enter the Modbus ID range for the Modbus TCP slave(s) that will respond to the Master's request. This is required if the remote Modbus RTU slaves are located behind another Modbus gateway. Value Range: 1 ~ 247.
Enable	It is unchecked by default.	Enable this rule.
Save	N/A	Save the settings.

Supported Function Code for Integrated Modbus Slave

Setting the gateway as a Modbus slave device allows a local SCADA management system to retrieve device information for monitoring.
Currently, the integrated Modbus slave function 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=Diconnected
1	WAN-2 Connection Status	R	0 ~ 6, 0=Disconnected, 1=Connecting…, 2=Connected, 3=Disconnecting…, 5=Wait for Traffic…, 6=Diconnected
2	WAN-3 Connection Status	R	0 ~ 6, 0=Disconnected, 1=Connecting…, 2=Connected, 3=Disconnecting…, 5=Wait for Traffic…, 6=Diconnected
3	WAN-4 Connection Status	R	0 ~ 6, 0=Disconnected, 1=Connecting…, 2=Connected, 3=Disconnecting…, 5=Wait for Traffic…, 6=Diconnected
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=Diconnected
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=Diconnected
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 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	R	0 : Unregistered, 1: Registered

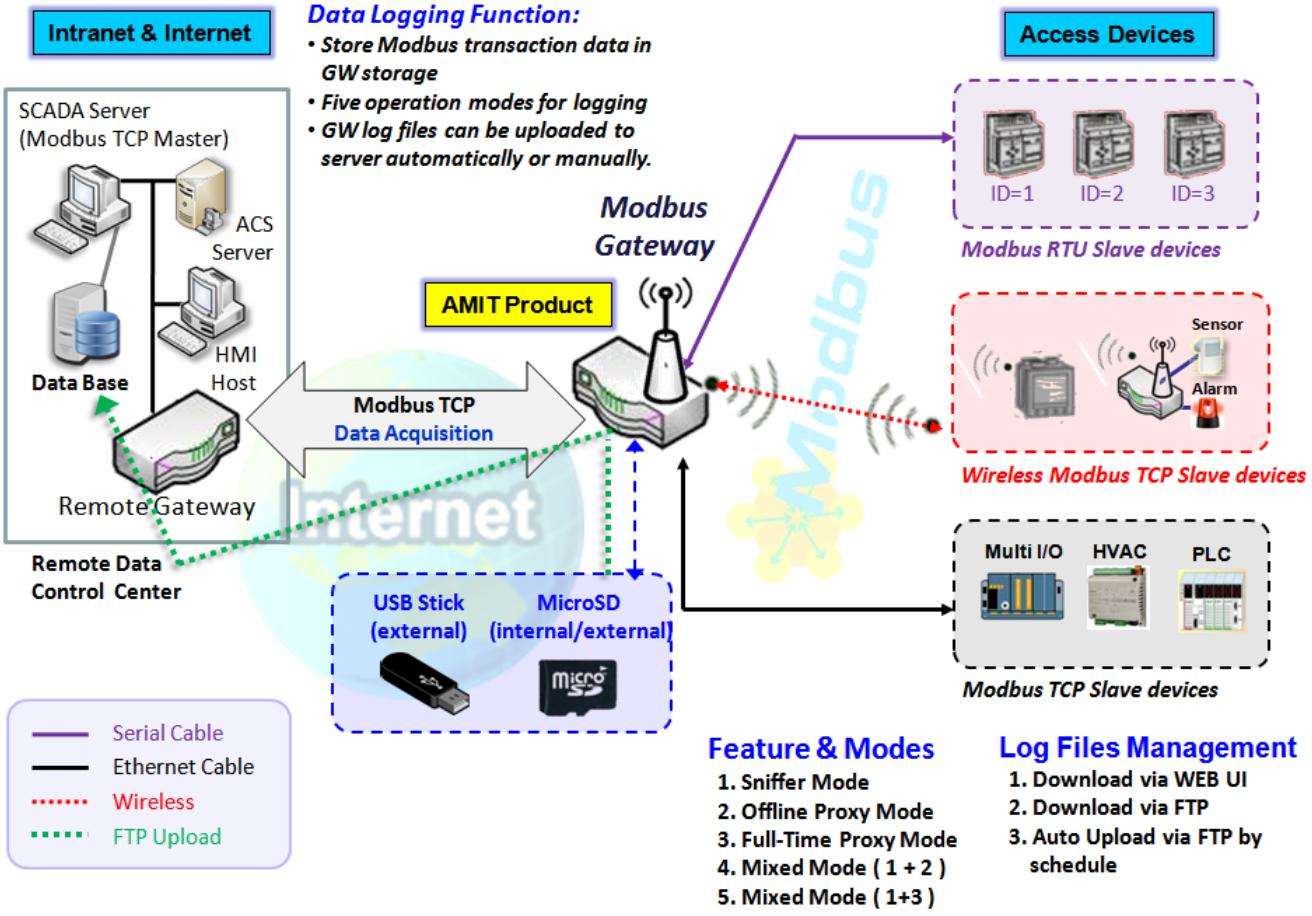
Register Address	Register Name	R / W	Register Range / Description
	Status		
37	3G/4G_Module-2_PS Register Status	R	0 : Unregistered, 1: Registered
38	3G/4G_Module-2_Roaming Status	R	0 : Not Roaming, 1: Roaming
39	3G/4G_Module-2_RSSI	R	RSSI Value
40	3G/4G_Module-2_RSRP	R	RSRP Value
41	3G/4G_Module-2_RSRQ	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
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

Register Address	Register Name	R / W	Register Range / Description
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.

4.2 Data Logging

Data logging is the process of collecting and storing data over a period of time in order to analyze specific trends or record the events/actions of a system. Data logging function is a very useful and also important feature for SCADA telemetry; it makes device monitoring and analysis easier.

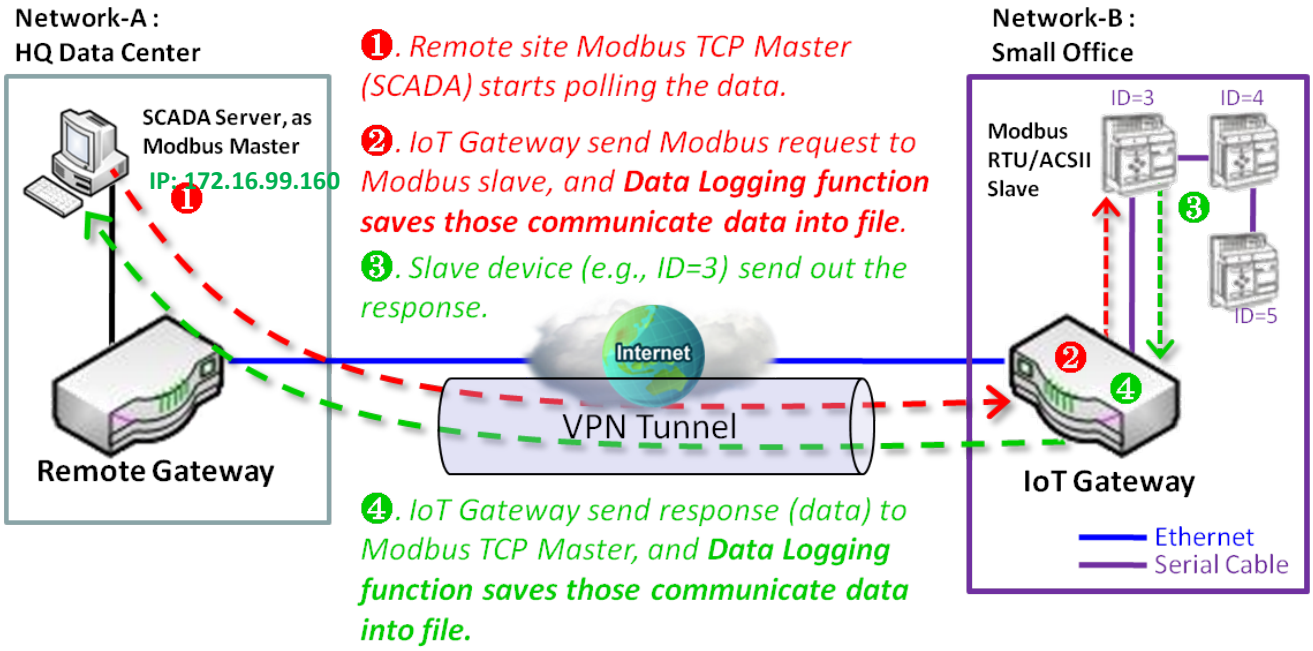
Data logging also provides logging proxy that saves a copy of the data collected to the local file storage (in .CSV file format). And when the network connection recovers, you can retrieve and download the data logs via FTP.



The Modbus gateway provides a complete data logging function for application requirements. There are different data logging schemes to meet different management requirements: Sniffer Mode, Offline Proxy Mode, Full-Time Proxy Mode, and the mixed modes for sniffer and proxy combined. In Sniffer mode, the gateway can monitor and log the communication data between the master and the associated slaves. However, if the Modbus gateway and the remote NOC/SCADA server disconnects, meaning the communication between a remote Modbus server and slave devices cannot be established; hence, no data is recorded.

With the Proxy mode option enabled, when the Modbus gateway lost the connection with a Modbus server, it will take over the data acquisition task and collect the required data from slave devices continuourly. Once the connection is recovered, the Modbus gateway can stop the data logging. The remote Modbus server can resume its data acquisition process; you can also troubleshoot problems by examing the stored data log files. The gateway offers configuration menus for setting data acquisition rules in the Proxy Mode.

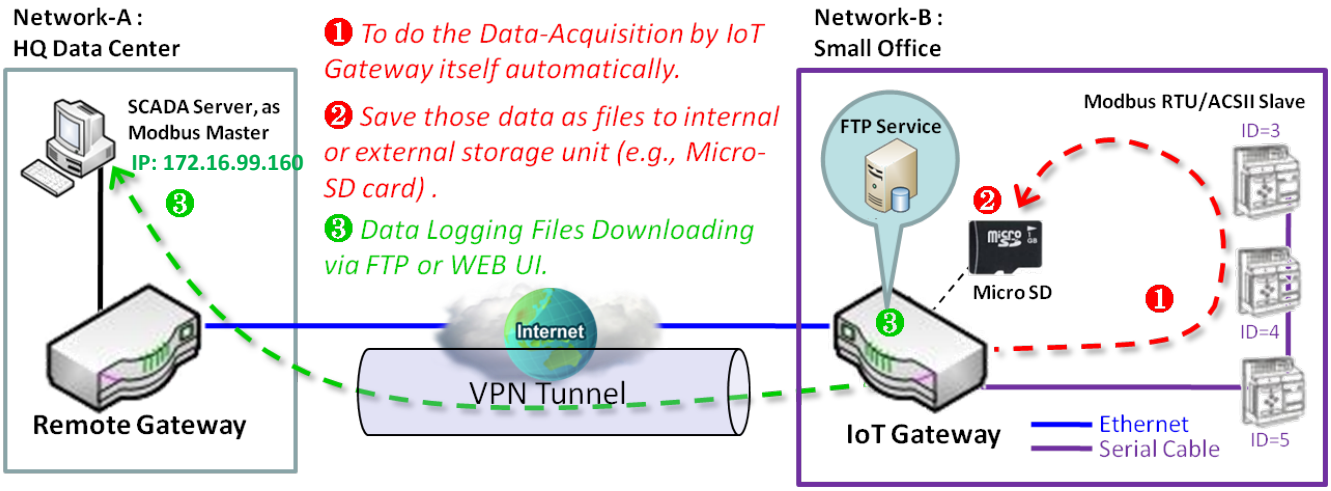
➢ Scenario for Sniffer Mode



As Illustrated in the diagram, the Modbus gateway will log the following Modbus activities:

- The Modbus request sent from a Remote Modbus TCP master.
- The response (data) sent out from the polled slave device (ID=3)

➢ Scenario for Off-Line Proxy Mode



As illustrated above, when the connection to a remote Modbus master breaks, the Modbus gateway will trigger the data logging proxy function to take over the data acquisition task and log the activity data (a repeat process) :

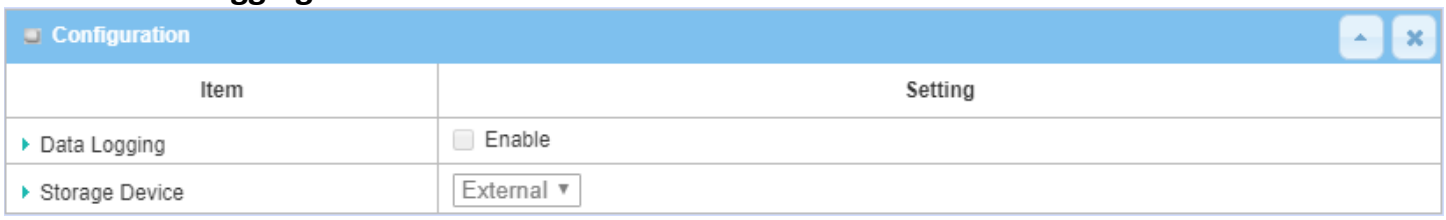
- The Modbus request issued by the Modbus gateway (Data Logging Proxy).
- The response (data) that sent out from the polled Slave device (ID=3)

4.2.1 Data Logging Configuration

The gateway will record Modbus messages according to the specified rules.

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

Enable Data Logging



Configuration		
Item	**Value setting**	**Description**
Data Logging	The box is unchecked by default.	Activate data logging function.
Storage Device	**External** is set by default	Choose the sotrage device to store the log file: **External** or **Internal**.
Save	*NA*	Save the settings.

Notes:

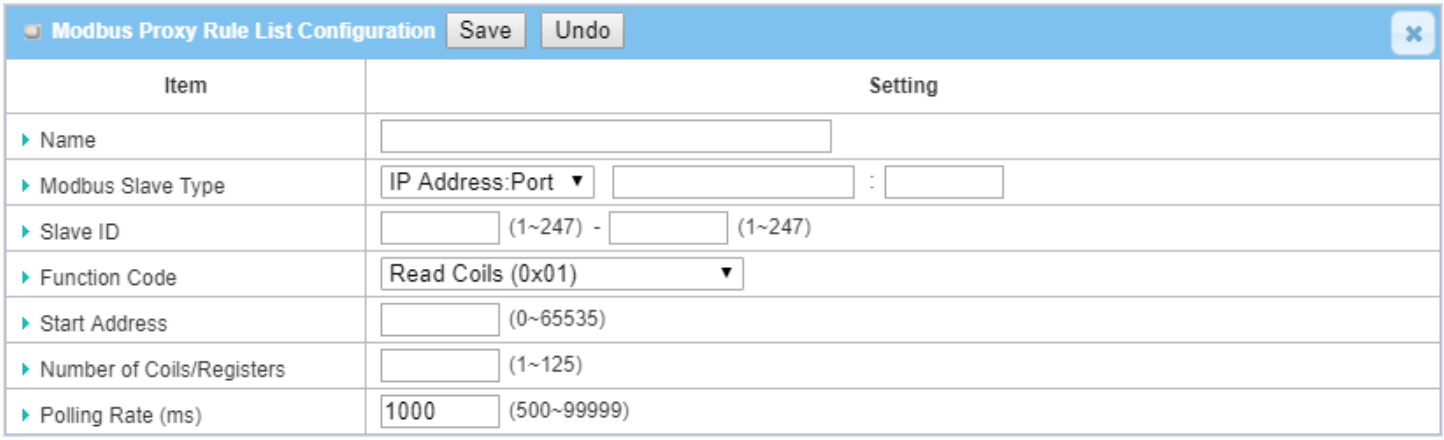
1. To use external storage, insert the external storage devices first and configure the related Data Logging function.
2. Make sure the Modbus Operation Mode is selected and enabled so that Modbus transactions will be logged (go to Field Communication > Bus & Protocol > Port Configuration and Modbus).

Create/Edit Modbus Proxy Rules

The gateway allows you to customize your proxy mode rules. It supports up to a maximum of 30 rules.



Click **Add** to open the **Modbus Proxy Rule Configuration** screen.



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

4.2.2 Scheme Setup

There are five data logging schemes for different management requirements: Sniffer Mode, Offline Proxy Mode, Full-Time Proxy Mode, and the combined mode of sniffer and proxy.

Go to **Field Communication > Data Logging > Scheme Setup** to access the Scheme Setup page.

Create/Edit Data Logging Rules



Click **Add** to open the **Scheme Configuration** screen.



Scheme Configuration		
Item	**Value setting**	**Description**
Name	A must-filled setting.	Specify a name for the data logging rule. *Value Range*: 1 ~ 16 characters.
Mode	**Sniffer** is selected by default.	Select a data logging scheme for the data logging rule. There are five available schemes : **Sniffer**: The Modbus gateway will record all the Modbus transcations between the master and slave devices. **Off-Line Proxy**: When the connection between the Modbus gateway and master is lost, the pre-defined proxy rule will be triggered to send the specified function code to collect and record the data/status from the slave devices. **Full-Time Proxy**: The pre-defined proxy rule will be triggered at all times and the Modbus gateway will issue the specified function code to collect and record the data/status from the slave devices. **Sniffer & Off-Line Proxy**: This is the mixed mode for both Sniffer and Off-Line Proxy. **Sniffer & Full-Time Proxy**: This is a mixed mode for both Sniffer and Full-Time Proxy.
Master Type	**IP Address** is selected by default.	Specify the Modbus master device to apply the data logging rule. It can be an **IP Address** of a Modbus TCP master, or **Local Serial Port** of directly attached Modbus RTU/ASCII master.
Master Query Timeout (sec.)	1. An optional setting. 2. **60** sec is set by default 3. Range 1 to 99999	Specify the timeout value for querying Modbus Master. The designated proxy rule will be triggered with the data logging rule after the specified timeout period. This setting only applied to Off-line proxy scheme.
Proxy Rules	An optional setting.	Select the Proxy rule to be applied with the data logging rule.

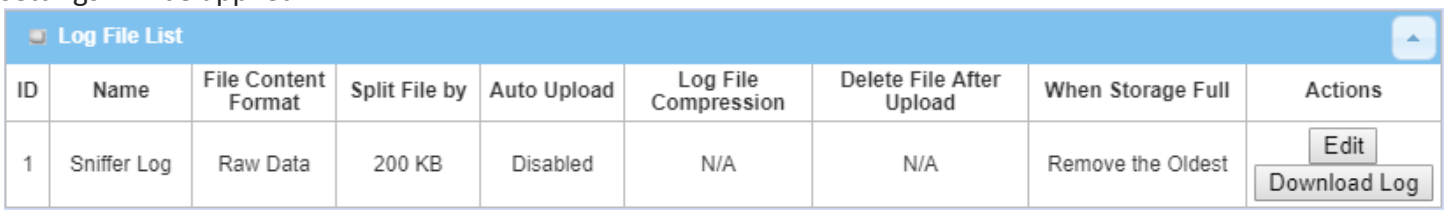
		Note: If any proxy scheme is selected, please create the required Proxy rules in advance, and select from the list.
Enable	The box is unchecked by default.	Activate the data logging rule.
Save	N/A	Save the settings.
Undo	N/A	Cancel the changes.

4.2.3 Log File Management

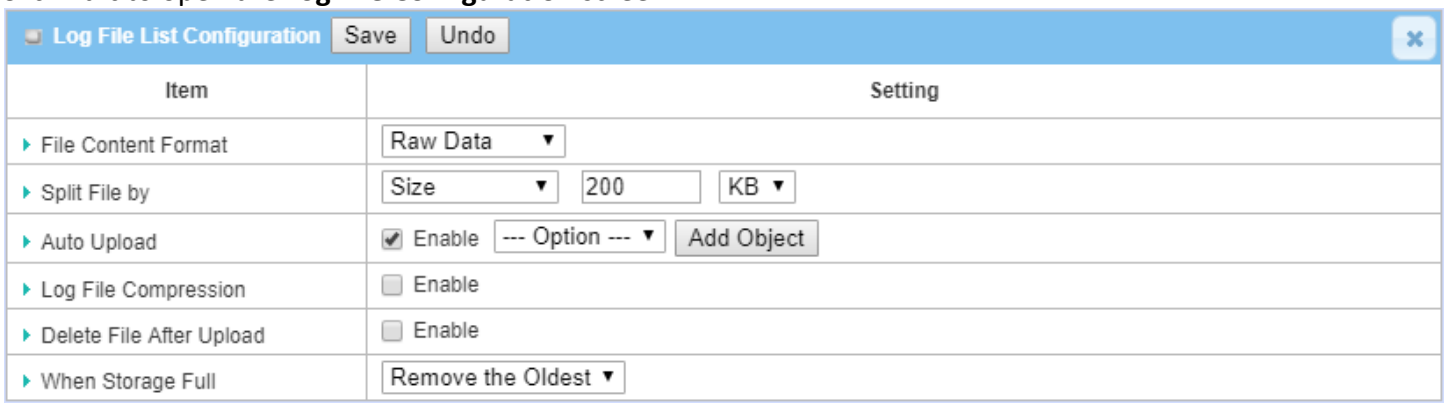
You can configure data logging rules for different data logging schemes.

Go to **Field Communication > Data Logging > Log File Management** to access the Log File Management page.

This table displays all the logging rules created. If you do not create any rules, the default log file management settings will be applied.



Click **Edit** to open the **Log File Configuration** screen.



Log File Configuration		
Item	**Value setting**	**Description**
Name	N/A	The name of the corresponding data log rule will be displayed. The default log file name will be named as ' Name_yyyyMMddHHmmSS.csv '.
File Content Format	**Raw Data** is selected by default	Select the data format for the log files: **Raw Data** or **Modbus Type**.
Split File by	**Size** and **200 KB** are set by default	Specify the method by which files should be created : **Size**, or **Time Interval** and enter the value accordingly. *Value Range*: 1 ~ 99999.
Auto Upload	1. An optional setting 2. The box is unchecked by default.	Activate the auto upload function for logged files. Once enabled, specify an external FTP server for auto uploading the log files to the server. Refer to **Object Definition > External Server > External Server**, or click **Add Object** to create a new FTP server.
Log File Compression	1. An optional setting 2. The box is unchecked by default	If Auto Upload is enabled, specify whether to compress the log file prior to the upload.
Delete File After Upload	1. An optional setting 2. The box is unchecked by default	If Auto Upload is enabled, specify whether to delete the uploaded log from the gateway's storage. Check the **Enable** button to activate the function.
When Storage Full	**Remove the Oldest** is selected by default	Specify the action when the storage is full: **Remove the Oldest** log file or **Stop Recording**. When **Remove the Oldest** is selected, the gateway will delete the oldest files but log data continuously. When **Stop Recording** is selected, the gateway will stop logging the data once

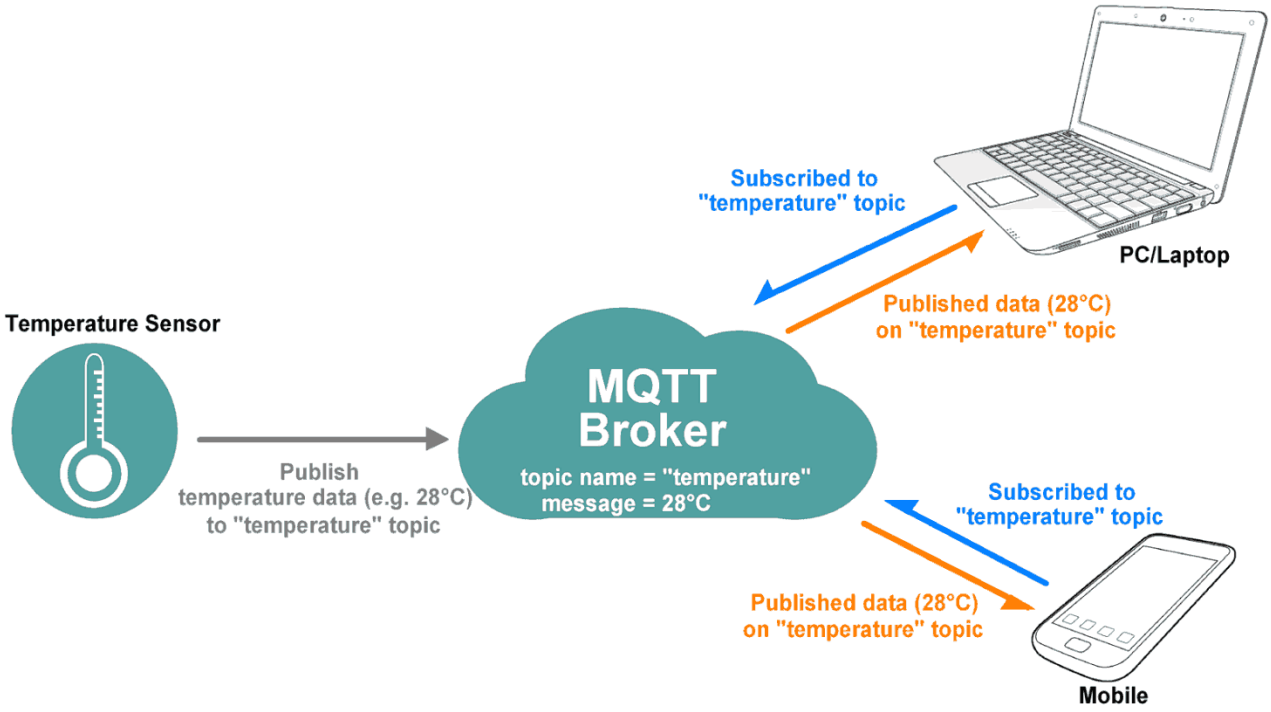
		the storage is full.
Save	*NA*	Save the settings.
Undo	*NA*	Cancel the changes.
Download Log	*NA*	Logs will be downloaded to your browser's default download folder in .tar file format.

4.3 Data Interchange

4.3.1 MQTT

MQTT (Message Queuing Telemetry Transport) is an ISO standard (ISO/IEC PRF 20922) publish-subscribe based messaging protocol. It works on top of the TCP/IP protocol. MQTT is a simple messaging protocol, designed for devices with constraint bandwidth and hence perfect for IoT applications. An MQTT system consists of clients communicating with a server, often called a "broker". And the client may be either a publisher of information or a subscriber. [8]

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 need to be configured in order to reach the publisher. Therefore, it makes it really easy to establish communication among multiple devices. [9]



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 to ensure that new subscribers will always receive the most current value.

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

8 Wikipedia, “MQTT”, Dec 22, 2023, https://en.wikipedia.org/wiki/MQTT.
9 Random Nerd Tutorials, “What is MQTT and How It Works”, https://randomnerdtutorials.com/what-is-mqtt-and-how-it-works/

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

The following briefly describes the terms for MQTT:

MQTT - Publish and Subscribe

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

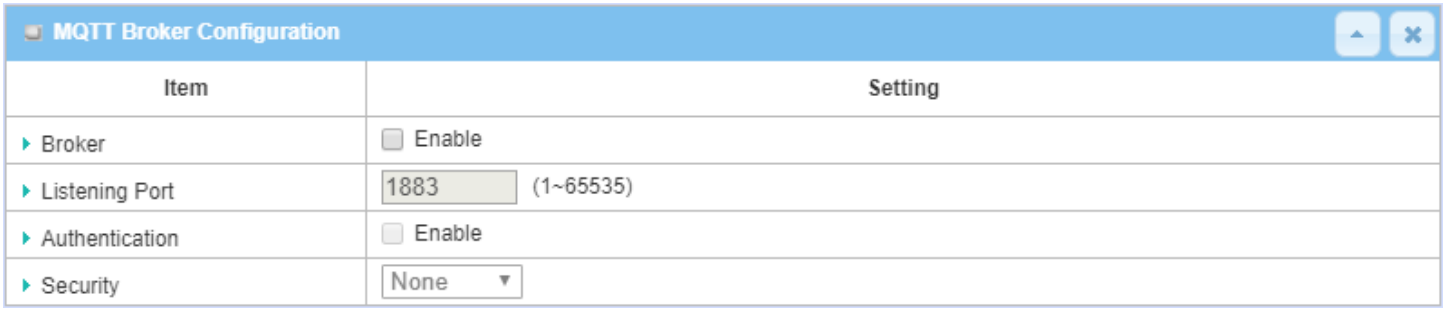
Topics are the way you register interest for incoming messages or how you specify where you want to publish the message.

Topics are represented with strings separated be a forward slash ‘/’. Each forward slash indicates a topic level. Here’s an example on how you would create a topic for controlling a lamp in your home office:

Both MQTT borker and MQTT client functions are supported on the gateway.

Configure the gateway as an MQTT Broker

Go to **Field Communication > Data Interchange > MQTT** to access MQTT Broker Configuration. Note the availability of this function depends on product model.

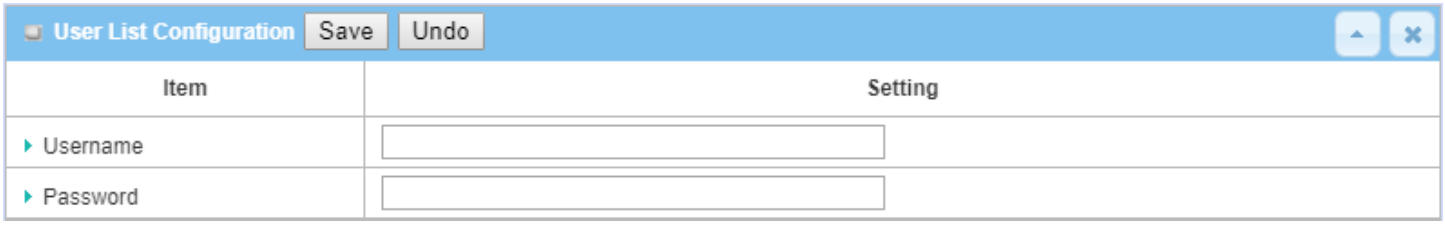


MQTT Broker Configuration		
Item	**Value setting**	**Description**
Broker	The box is unchecked by default.	Activate the MQTT Broker function.
Listening Port	1. An optional setting. 2. **1883** is set by default	Specify the listening port for MQTT broker. The MQTT broker will monitor the activity on that port for messages from MQTT clients. If there is any MQTT client(s) subscribing the received topic, the MQTT broker will forward the topic to the correspoinding subscriber(s). *Value Range*: 1 ~ 65535.
Security	1. An optional setting. 2. **None** is set by default	Select the security scheme for MQTT. **None**: no encryption for MQTT data transmission. **SSL/TLS**: SSL/TLS encryption will be applied for security. You also need to specify required certificate files for SSL/TLS. **Note:** If **SSL/TLS** is selected, the listening port will be changed to the default **8883** port.
Certificate	1. An optional setting. 2. **None** is set by default	Select **CA File** / **CERT File** / **Key File** from the dropdown lists. Go to **Object Definition** > **Certificate** > **Trusted Certificate** to populate the list first. **CA File** is defined in Trusted Certificate List. **CERT File** is defined in Trusted Client Certificate List. **KEY File** is 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 the MQTT messages from the MQTT Broker. Up to 5 user accounts can be defined to have permission.
Save	N/A	Save the settings.

Create/Edit User List



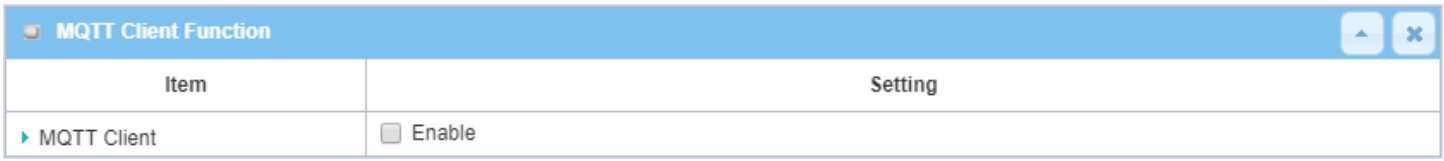
Click **Add** to open the **User List Configuration** screen. Click **Add** to open the **User List Configuration** screen.



Scheme Configuration		
Item	**Value setting**	**Description**
Username	A must-filled setting.	Specify a name for the MQTT subscriber. *Value Range*: 1 ~ 32 characters.
Password	A must-filled setting.	Specify the password for the user account. *Value Range*: 1 ~ 32 characters.
Save	N/A	Save the settings.
Undo	N/A	Cancel the changes.

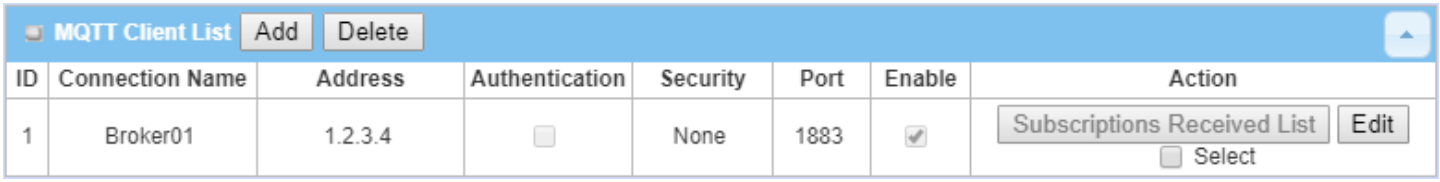
Set up as a MQTT Client

In addition to functioning as an MQTT Borker, the gateway can be set up as an MQTT client.



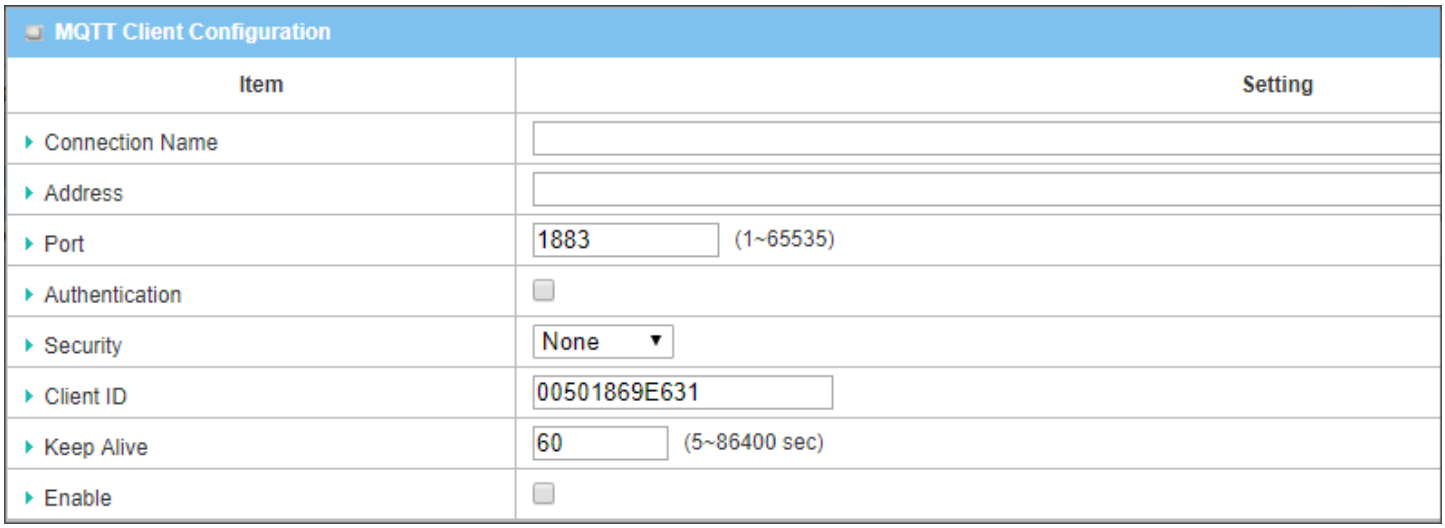
MQTT Broker Configuration		
Item	**Value setting**	**Description**
MQTT Client	The box is unchecked by default.	Activate the MQTT Client function. The gateway will then publish messages to an MQTT borker or subscribe interested topic(s) from MQTT brokers.
Save	N/A	Save the settings.

Create/Edit MQTT Client List



Click **Add** to open the following configuration screens: MQTT Client Configuration, MQTT Message Configuration, Publish Message List, and Subscribe Message List.

Configure MQTT Client Settings

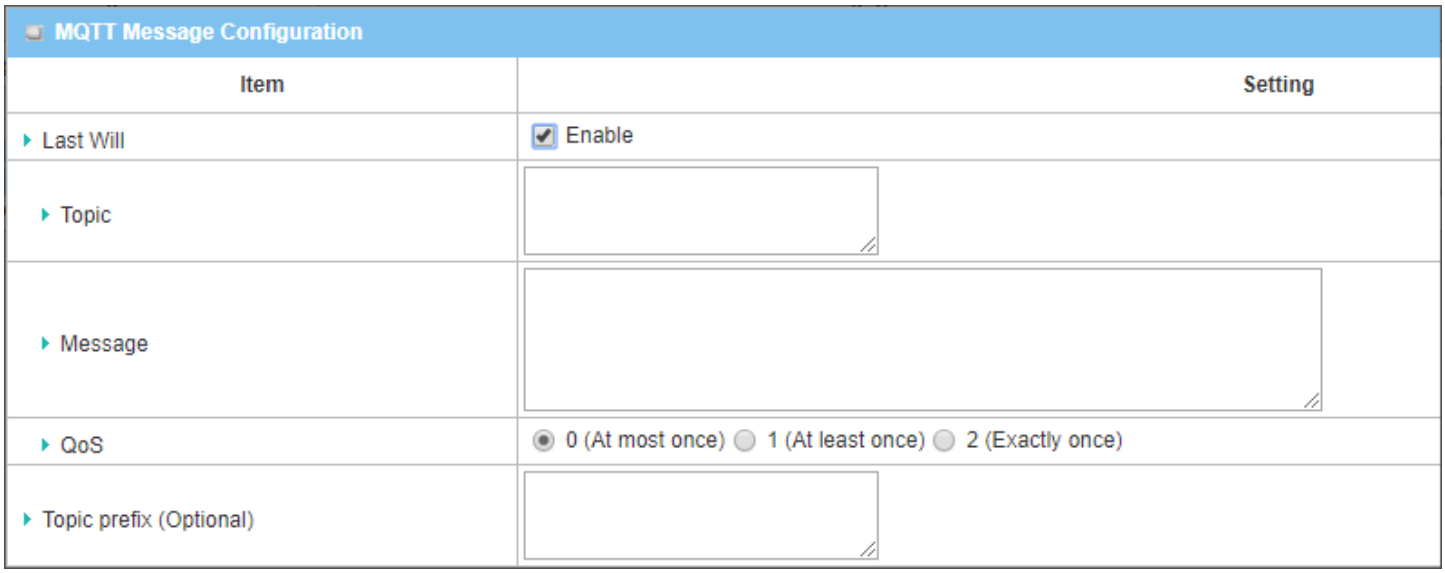


MQTT Client Configuration		
Item	**Value setting**	**Description**
Connection Name	The box is unchecked by default.	Specify a name for the MQTT Client, which can use the Broker name or interested message (topic) *Value Range*: 1 ~ 64 characters.
Address	1. A Must-filled setting. 2. Blank by default	Specify the host name or IP address of the MQTT borker.
Port	1. An optional setting. 2. **1883** is set by default	Specify a port for MQTT connection. *Value Range*: 1 ~ 65535.
Security	1. An optional setting. 2. **None** is set by default	Select the security scheme for MQTT. **None**: no encryption for MQTT data transmission. **SSL/TLS**: SSL/TLS encryption will be applied for security. You have to specify required certificate files for SSL/TLS. **Note**: If **SSL/TLS** is selected, the listening port will be changed to the default **8883** port.
Certificate	1. An optional setting. 2. **None** is set by default	Select **CA File** / **CERT File** / **Key File** from the dropdown lists. If you don't have any items in the dropdown list, you have to define or create it first. Please refer to **Object Definition** > **Certificate** > **Trusted Certificate**. **CA File** is defined in Trusted Certificate List. **CERT File** is defined in Trusted Client Certificate List. **KEY File** is defined in Trusted Client Key List.
Client ID	1. A Must-filled 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.
Authentication	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 from the MQTT Broker.
Username	A must-filled setting.	Specify the name of the MQTT client with the following password for user authentication. *Value Range*: 1 ~ 32 characters.
Password	A must-filled setting.	Specify the password for the user account. *Value Range*: 1 ~ 32 characters.

Keep Alive	1. An optional setting. 2. **60** sec is set by default.	Specify a keep alive interval to ensure that the connection is still alive. *Value Range*: 5 ~ 86400 sec.
Enable	The box is unchecked by default.	Activate this MQTT Client configuration.
Save	N/A	Save the settings.
Undo	N/A	Cancel the changes.
Back	N/A	Go back to previous configuration screen.

Compose MQTT Message

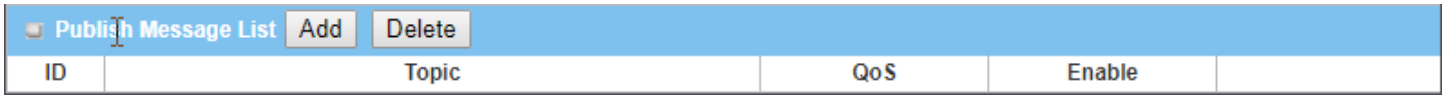
You can define the Last Will Message, and optional Topic Prefix for publishing / subscribing MQTT messages.



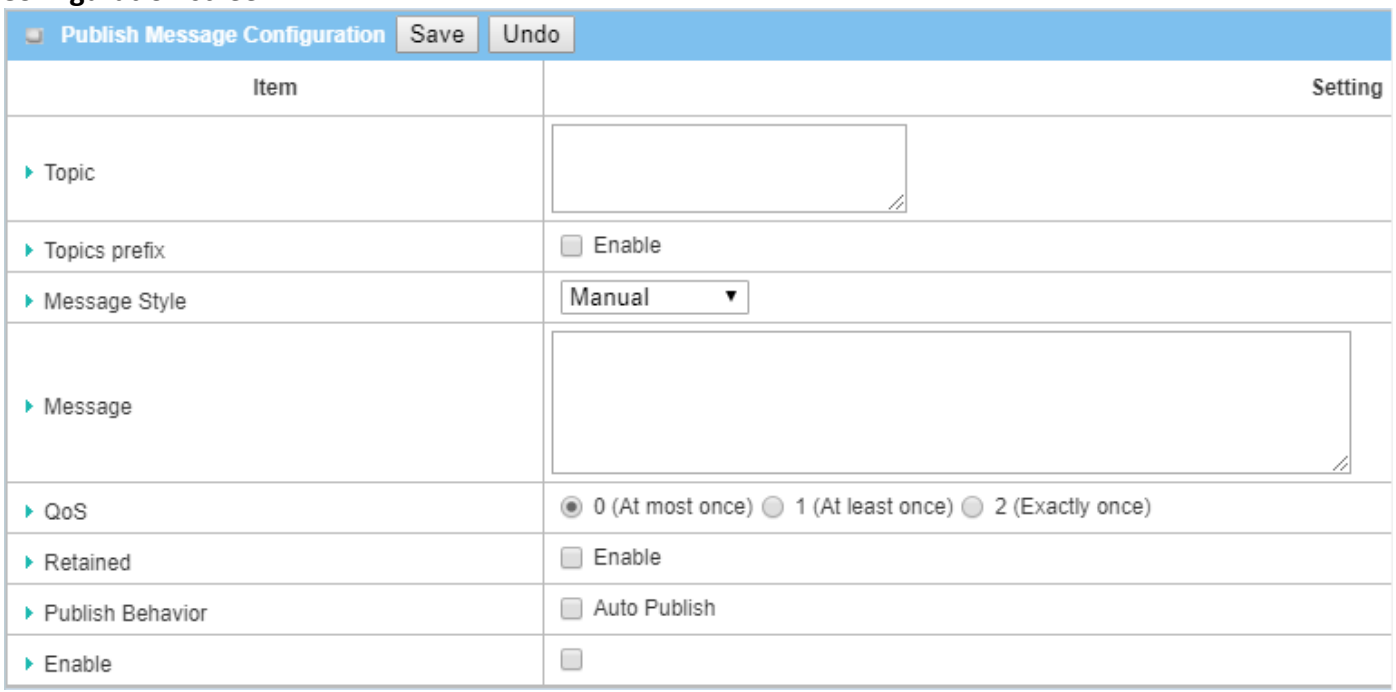
MQTT Message Configuration		
Item	**Value setting**	**Description**
Enable	The box is unchecked by default.	Activate this Last Will message configuration and specify the Topic, Message, and QoS settings. When the MQTT borker detects that the MQTT client is disconnected, it will send the Last Will message to the MQTT clients.
Topic	1. A Must-filled setting. 2. Blank by default	Specify the topic for the Last Will message. *Value Range*: 1 ~ 64 characters, including the topic level separator '/', but excluding the wildcards '+' and '#'.
Message	1. A Must-filled setting. 2. Blank by default	Specify the message content for the Last Will message. *Value Range*: 1 ~ 256 characters.
QoS	1. An optional setting. 2. **0 (At most once)** is set by default	Select the QoS setting for the Last Will message. **0 (At most once)**: 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. **1 (At least once)**: the message will be published at least once until acknowledgement is recevied from the broker or subscribed clent(s). **2 (Exactly once)**: the message will be published to subscribed clent(s) once in a two-level handshake transmission to ensure only one copy of the message is received.

Topic prefix (Optional)	1. An Optional-filled setting. 2. Blank by default	Specify the topic prefix for the MQTT message. *Value Range*: 1 ~ 64 characters.
Save	N/A	Save the settings.
Undo	N/A	Cancel the changes.
Back	N/A	Go back to previous configuration screen.

Publish Message List



Up to 64 published messages will be displayed in the message list. Click **Add** to open the **Publish Message Configuration** screen.



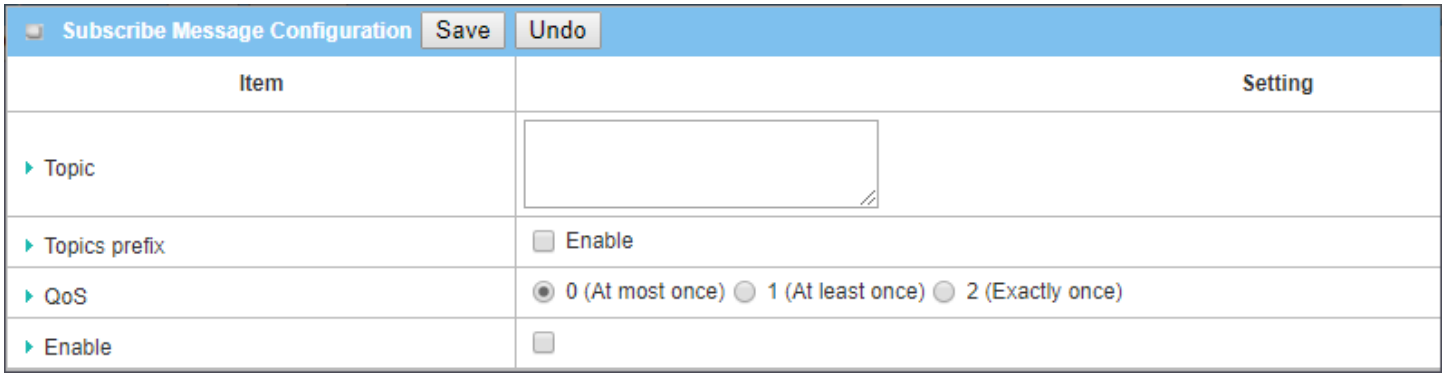
Publish Message Configuration		
Item	**Value setting**	**Description**
Topic	1. A Must-filled setting. 2. Blank by default	Specify the topic for the message to be published. *Value Range*: 1 ~ 64 characters, including the topic level separator '/', but excluding the wildcards '+' and '#'.
Topic prefix	The box is unchecked by default.	Check the box to add the pre-defined topic prefix into a MQTT message.
Message Style	1. An Optional-filled setting. 2. **Manual** is selected by default	Select a message style from the dropdown list. The supported styles are : **Manual**: The message is created manaully, and you can specify the message content below. **System Log**: The messages to be published are the system logs of the device. **Data Logging**: The messages to be published are the data logs recorded in the designated storage.
Message	1. A Must-filled setting. 2. Blank by default	Specify the message content for the Manual publish type. *Value Range*: 1 ~ 256 characters.

QoS	1. An optional setting. 2. **0 (At most once)** is set by default	Select the QoS setting for the Last Will message. **0 (At most once)**: 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. **1 (At least once)**: the message will be published at least once until acknowledgement is recevied from the broker or subscribed clent(s). **2 (Exactly once)**: the message will be published to subscribed clent(s) once in a two-level handshake transmission to ensure only one copy of the message is received.
Retained	The box is unchecked by default.	Activate the message retaining function.
Publish Behavior	The box is unchecked by default.	Specify publish behavior: **Auto Publish**: automatically publish a message with the specified time interval (1~65535 sec). **When the Message or Data variation more than ☐ lines**: publish a new message that differs from the previous one for the specified number of changes. This option is not available for the Manual message style.
Enable	The box is unchecked by default.	Activate this publish message configuration.
Save	N/A	Save the settings.
Undo	N/A	Cancel the changes.
Back	N/A	Go back to previous configuration screen.

Subscribe Message List



Up to 64 subscribed messages will be displayed in the message list. Click **Add** to open the **Subscribe Message Configuration** screen.



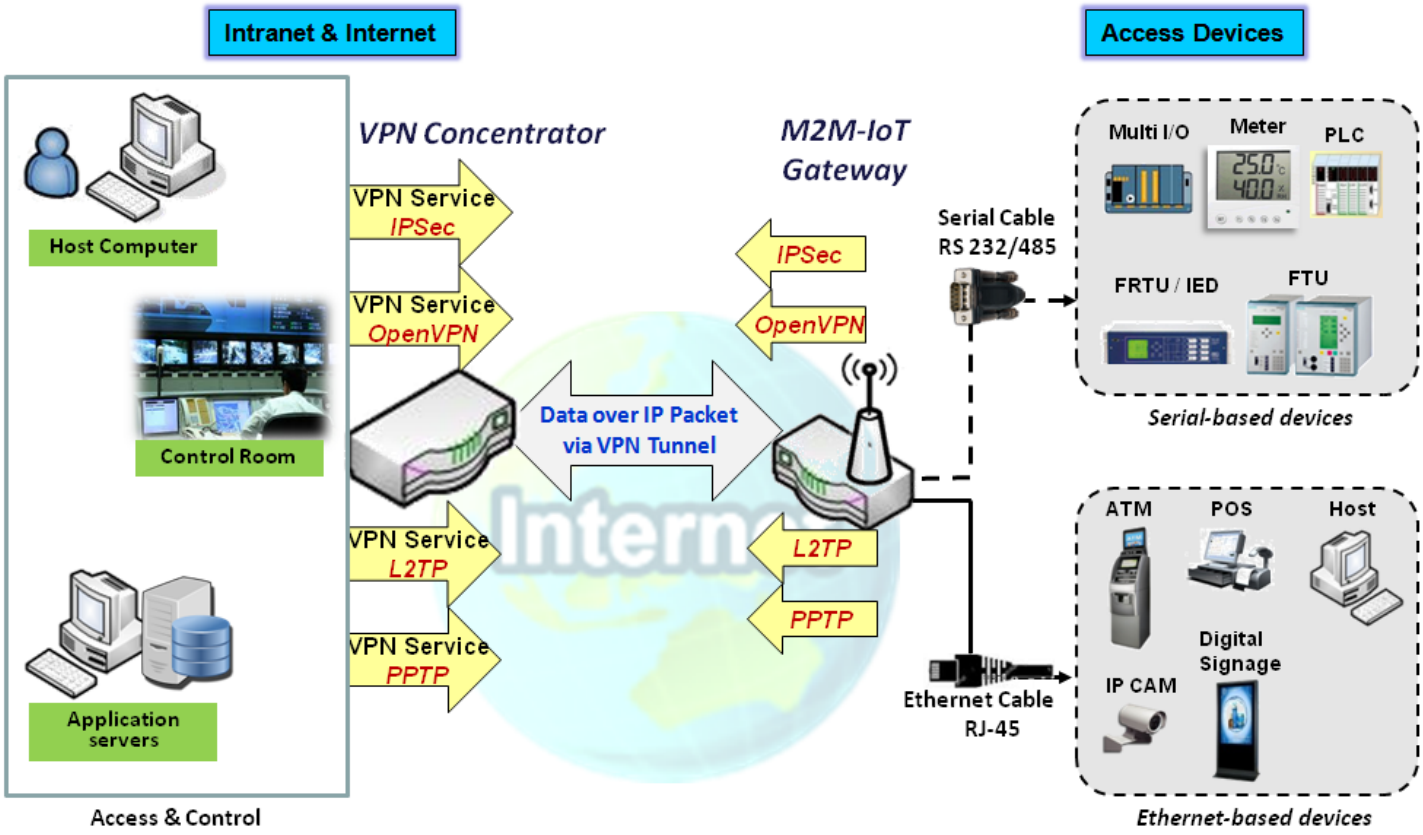
Subscribe Message Configuration		
Item	**Value setting**	**Description**
Topic	1. A Must-filled setting. 2. Blank by default	Specify the topic for the message to be subscribed. *Value Range*: 1 ~ 64 characters, including the topic level separator '/', and wildcards '+', '#'.
Topic prefix	The box is unchecked	Enable the topic prefix for the subscribed message.

	by default.	
QoS	1. An optional setting. 2. **0 (At most once)** is set by default	Select the QoS type for publishing a message. **0 (At most once)**: the message will be published only once, and the broker and subscribed client(s) take no additional steps to acknowledge the develivery, no matter it is received or not. **1 (At least once)**: the message will be published at least once until acknowledgement is recevied from the broker or subscribed clent(s). **2 (Exactly once)**: the message will be published to subscriber(s) once in a two-level handshake to ensure only one copy of the message is received.
Enable	The box is unchecked by default.	Activate this subscribe message configuration
Save	N/A	Save the settings.
Undo	N/A	Cancel the changes.
Back	N/A	Go back to previous configuration screen.

Chapter 5 Security

5.1 VPN

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while offering the functionality as well as security and management features of the private network. A VPN creates a virtual point-to-point connection through dedicated connections with encryption utilizing tunneling technique. The tunnel technology supports data confidentiality and security as well as data integrity by employing encapsulation protocols, encryption algorithms, and hashing algorithms.



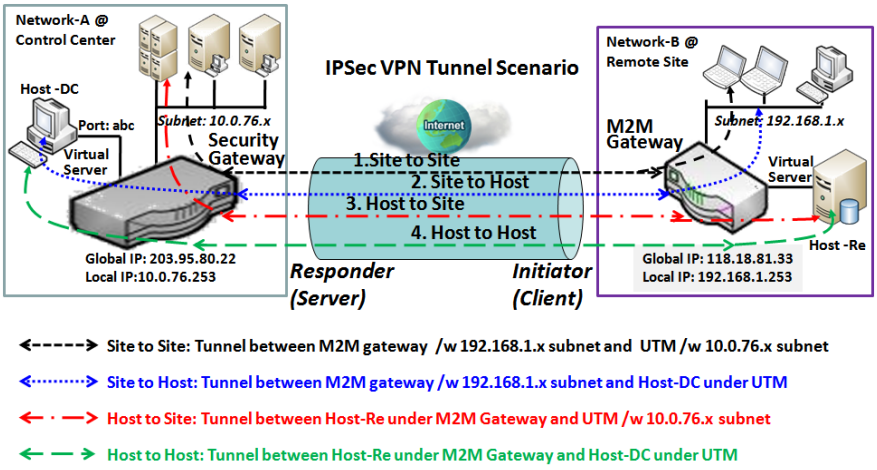
The product series supports different tunneling technologies for building secure tunnels between multiple sites: IPSec, OpenVPN, L2TP (over IPSec), PPTP, and GRE. Advanced functions such as Full Tunnel, Tunnel Failover, Tunnel Load Balance, NetBIOS over IPSec, NAT Traversal and Dynamic VPN, are also supported.

5.1.1 IPSec

Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting IP packets of a communication session. At the begging of a new session, IPSec establishes mutual authentication between agents and negotiates cryptographic keys to be used during the session.

An IPSec VPN tunnel is established between an IPSec client and a server. This gateway can be configured for different roles for building tunnels with remote devices. Before setting a VPN connection, you may need to decide the connection scenario.

IPSec Tunnel Scenarios



To build an IPSec tunnel, you need the remote gateway global IP, and the optional subnet to allow for accessing LAN resources behind the other end of the tunnel.

Under such configuration, there are four scenarios:

Site to Site: You need to set remote gateway IP and subnet of gateways at both ends. After the IPSec tunnel is established, hosts behind both gateways can communicate with one another through the tunnel.

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

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

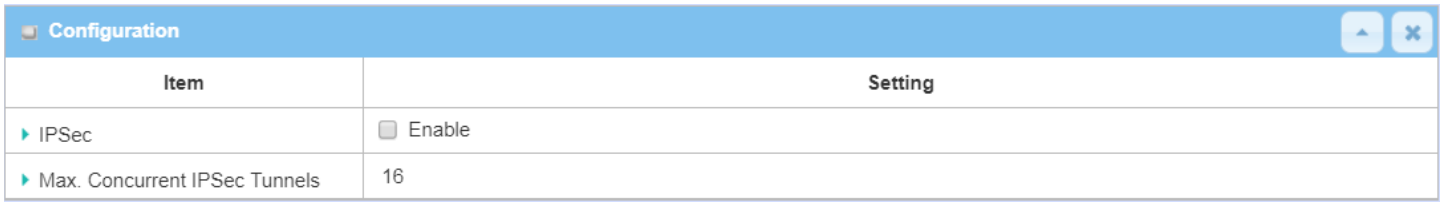
Host-to-Host: Host to Host is a special configuration for building a VPN tunnel between two single hosts.

IPSec Setting

Go to **Security > VPN > IPSec** to access the IPSec configuration page.

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

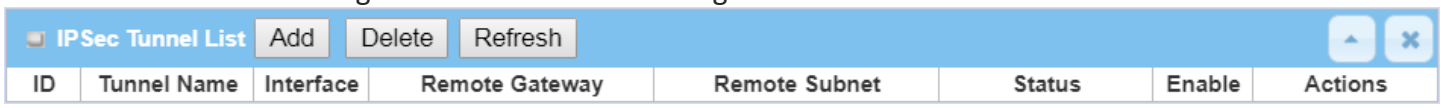
Enable IPSec



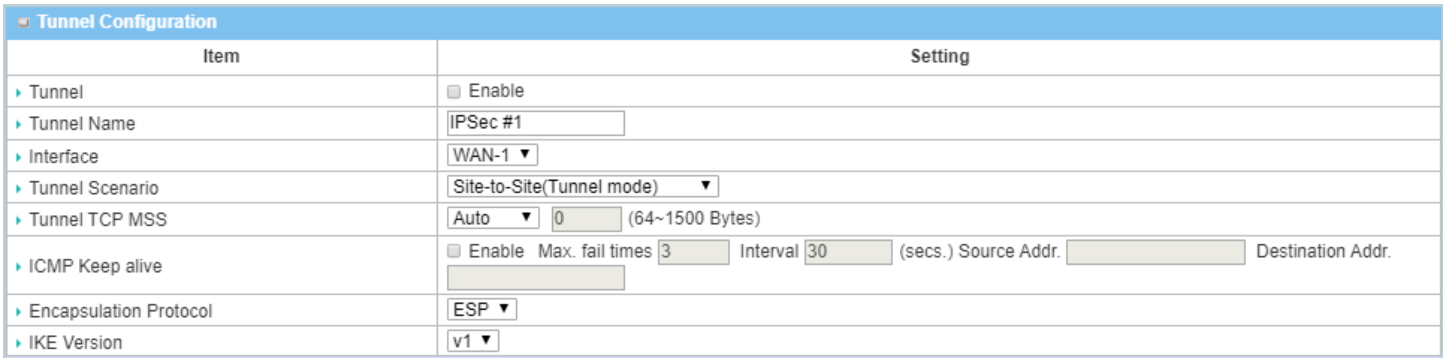
Configuration Window		
Item	**Value setting**	**Description**
IPsec	Unchecked by default	Enable the IPSec function.
Max. Concurrent IPSec Tunnels	Depends on Product specification.	The specified value will limit the maximum number of simultaneous IPSec tunnel connections.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

Create/Edit IPSec Tunnel

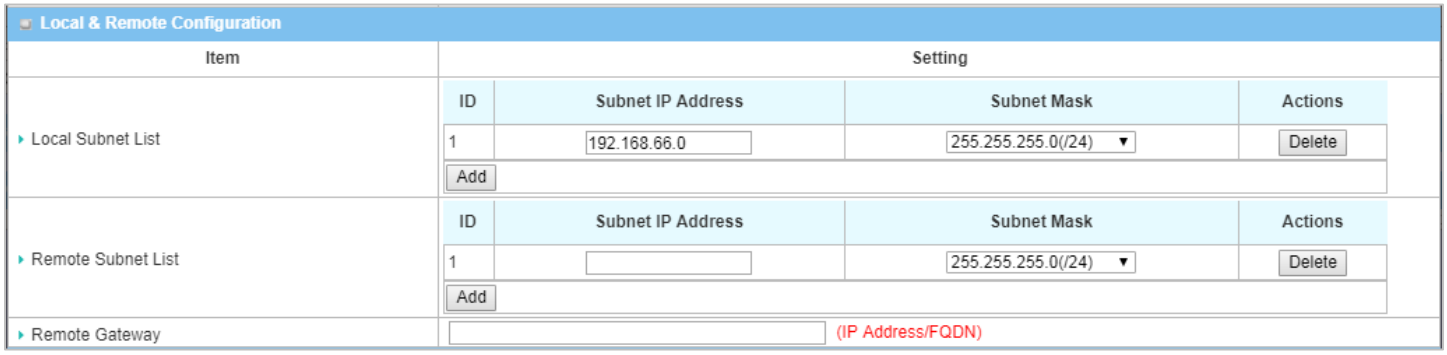
Enable IPSec above to configure the IPSec tunnel settings.



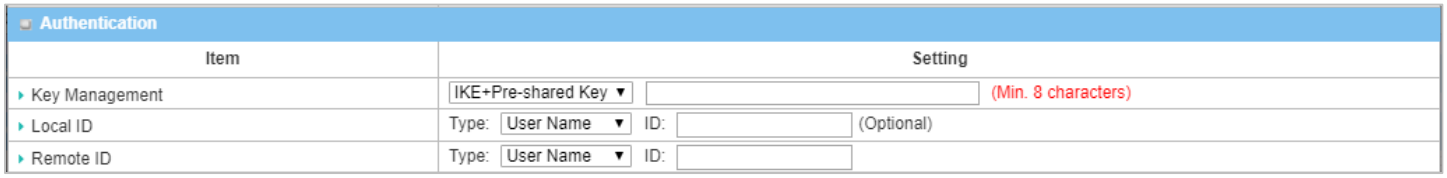
Click **Add/Edit** to open these configuration screens: Tunnel Configuration, Local & Remote Configuration, Authentication, IKE Phase, IKE Proposal Definition, IPSec Phase, and IPSec Proposal Definition. You have to configure the tunnel details for both local and remote VPN devices.



Tunnel Configuration Window		
Item	**Value setting**	**Description**
Tunnel	Unchecked by default	Activate the IPSec tunnel
Tunnel Name	1. A must-filled setting 2. String format can be any text	Enter a name for the tunnel. *Value Range*: 1 ~ 19 characters.
Interface	1. A must-filled setting 2. **WAN 1** is selected by default	Select the interface on which IPSec tunnel is to be established.
Tunnel Scenario	1. A must-filled setting 2. **Site to site** is selected by default	Select an IPSec tunneling scenario from the dropdown box for your application. Select **Site-to-Site**, **Site-to-Host**, **Host-to-Site**, or **Host-to-Host**. If a LAN interface is selected above, only **Host-to-Host** scenario is available. With **Site-to-Site** or **Site-to-Host** or **Host-to-Site**, IPSec operates in tunneling mode, with the difference in the number of subnets. With **Host-to-Host**, IPSec operates in transport mode.
Tunel TCP MSS	1. An optional setting 2. **Auto** is set by default	Select from the size of Tunel TCP MSS. Select **Auto** for automatic adjustment among the devices. Select **Manual** and specify a vaule for Tunel TCP MSS. *Value Range*: 64 ~ 1500 bytes.
ICMP Keep Alive	1. An optional setting 2. **Unchecked** by default	Activate the ICMP keep alive function for the tunnel. If the keep alive function is enabled, define the numner of fail trials, check interval, and source/destination IP address for ICMP transmission. *Value Range*: 1~999 for fail trials and time interval.
Encapsulation Protocol	1. A must-filled setting 2. **ESP** is selected by default	Select the Encapsulation Protocol for this IPSec tunnel: **ESP** and **AH**.
IKE Version	1. A must-filled setting 2. **v1** is selected by default	Specify the IKE version for this IPSec tunnel: **v1** or **v2**.

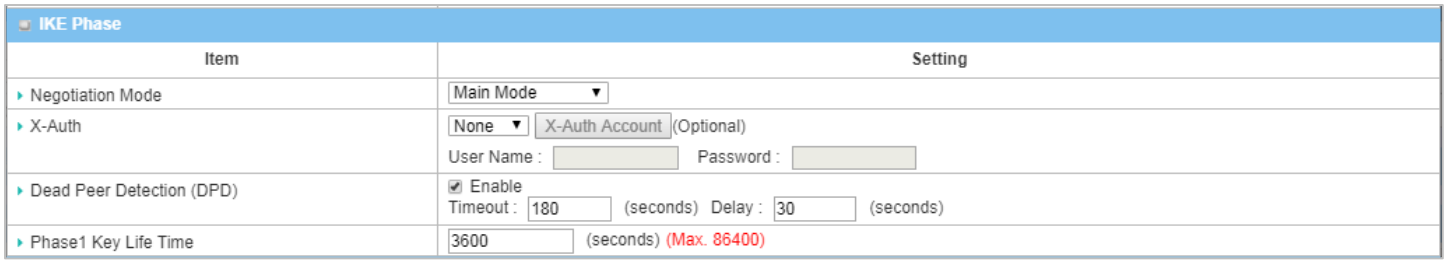


Local & Remote Configuration Window		
Item	**Value setting**	**Description**
Local Subnet List	A must-filled setting	Specify the Local Subnet IP address and Subnet Mask. Click the Add or Delete button to add or delete a Local Subnet. Notes: 1. When Dynamic VPN option in Tunnel Scenario is selected, only one subnet will be available. 2. When Host-to-Site or Host-to-Host is selected for Tunnel Scenario, Local Subnet will not be available. 3. When Hub and Spoke is selected, there will be only one subnet available.
Remote Subnet List	A must-filled setting	Specify the Remote Subnet IP address and Subnet Mask. Click the Add or Delete button to add or delete a remote subnet.
Remote gateway	1. A must-filled setting. 2. Format can be a ipv4 address or FQDN	Specify the remote gateway.

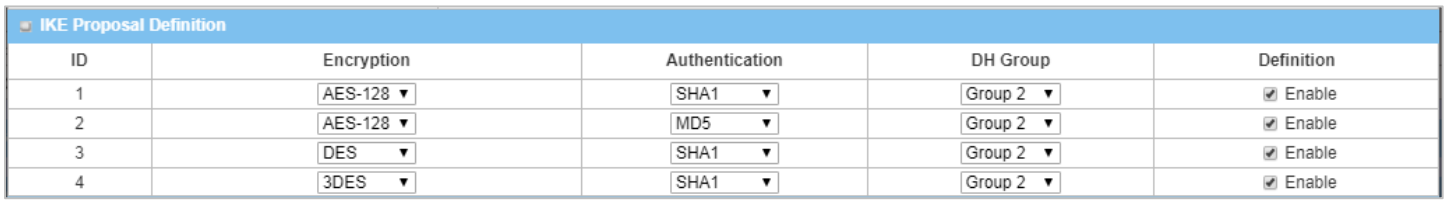


Authentication Configuration Window		
Item	**Value setting**	**Description**
Key Management	1. A must-filled setting 2. Pre-shared Key 8 to 32 characters.	Select Key Management for this IPSec tunnel. **IKE+Pre-shared Key:** Set a key (8 ~ 32 characters). **IKE+X.509:** IKE+X.509 will be available only when Certificate has been configured properly (go to **Object Definition > Certificate**).
Local ID	An optional setting	Specify the Local ID for IPSec tunnel authentication. Select **Username** for Local ID and enter the username. Select **FQDN** for Local ID and enter the FQDN. Select **User@FQDN** for Local ID and enter the ID in the format: User@FQDN. Select **Key ID** for Local ID and enter the Key ID.
Remote ID	An optional setting	Specify the Remote ID for IPSec tunnel authentication. Specify the Local ID for IPSec tunnel authentication. Select **Username** for Local ID and enter the username.

	Select **FQDN** for Local ID and enter the FQDN. Select **User@FQDN** for Local ID and enter the ID in the format: User@FQDN. Select **Key ID** for Local ID and enter the Key ID. **Note:** Remote ID will not be available when Dynamic VPN is selected for Tunnel Scenario.

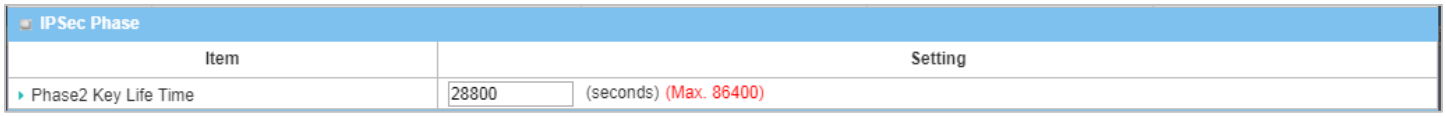


IKE Phase Window		
Item	**Value setting**	**Description**
Negotiation Mode	Main Mode is set by default default	Specify the Negotiation Mode for this IPSec tunnel: **Main Mode** or **Aggressive Mode**.
X-Auth	None is selected by default	Specify the X-Auth role for this IPSec tunnel: Server, Client, or None. Select None if no X-Auth authentication is required. Select Server if the gateway will be an X-Auth server and click on the X-Auth Account button to create a remote X-Auth client account. Select Client to designate this gateway as an X-Auths client. Enter a Username and Password to be authenticated by the X-Auth server gateway. **Note:** X-Auth Client will not be available if Dynamic VPN is selected for Tunnel Scenario.
Dead Peer Detection (DPD)	1. Checked by default 2. Default Timeout 180s and Delay 30s	Enable the **DPD** function. Specify the **Timeout** and **Delay** time in seconds. *Value Range*: 0 ~ 999 seconds for **Timeout** and **Delay**.
Phase1 Key Life Time	1. A must-filled setting 2. Default 3600s 3. Max. 86400s	Specify the Phase1 Key lifetime. *Value Range*: 30 ~ 86400.

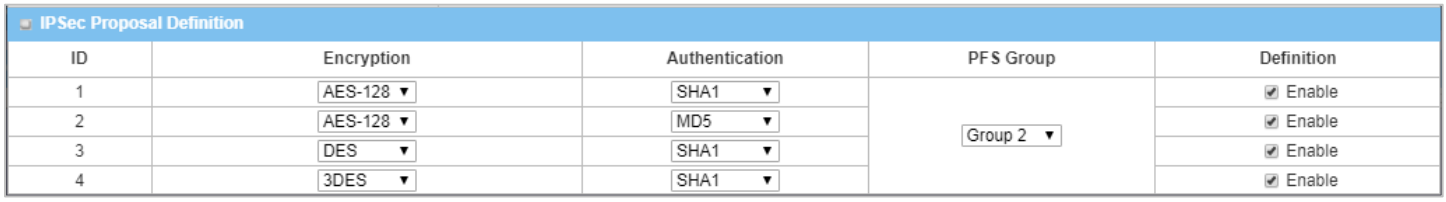


IKE Proposal Definition Window		
Item	**Value setting**	**Description**
IKE Proposal Definition	A must-filled setting	Specify the Phase 1 Encryption method: DES, 3DES, AES-128, AES-192, or AES-256. Specify the Authentication method: None, MD5, SHA1, or SHA2-256. Specify the DH Group: None, Group1, Group2, Group5, Group14, Group15, Group16, Group17, or Group18.

Then chek **Enable.**



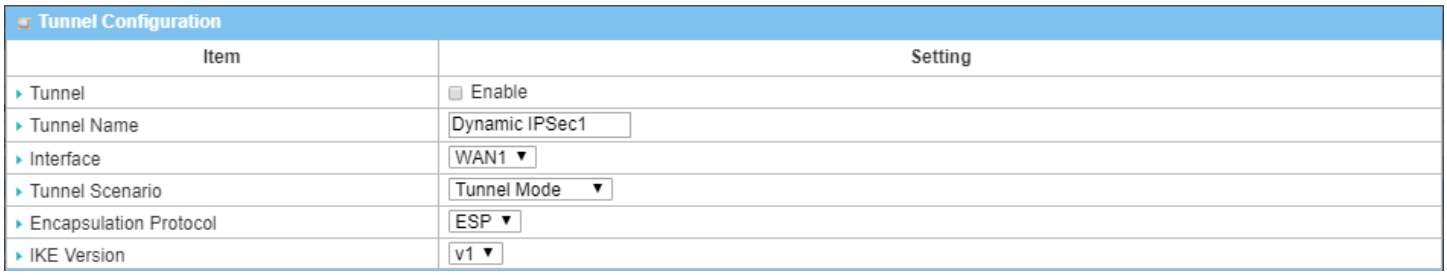
IPSec Phase Window		
Item	**Value setting**	**Description**
Phase2 Key Life Time	1. A must-filled setting 2. 28800s is set by default 3. Max. 86400s	Specify the Phase2 Key lifetime in second. *Value Range*: 30 ~ 86400.



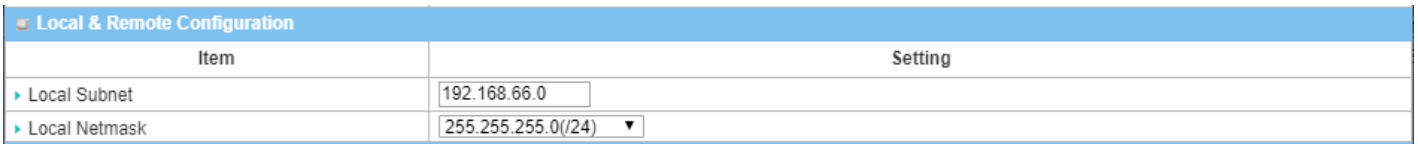
IPSec Proposal Definition Window		
Item	**Value setting**	**Description**
IPSec Proposal Definition	A must-filled setting	Specify the Encryption method: None, DES, 3DES, AES-128, AES-192, or AES-256. **Note:** None is only available when AH is selected for Encapsulation. Specify the Authentication method: None, MD5, SHA1, or SHA2-256. **Note:** None and SHA2-256 are not available if **AH** is selecte for Encapsulation. Specify the PFS Group: None, Group1, Group2, Group5, Group14, Group15, Group16, Group17, or Group18. Then click **Enable**.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.
Back	N/A	Click **Back** to return to the previous page.

Create/Edit Dynamic VPN Server List

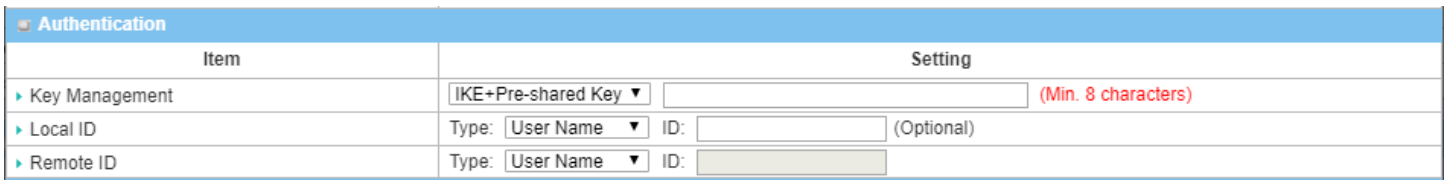
This page allows you to configure the tunnel details of the gateway's Dynamic VPN server. You can specify different VPN servers for multiple WAN interfaces.



Tunnel Configuration Window		
Item	**Value setting**	**Description**
Tunnel	Unchecked by default	Activate the Dynamic IPSec VPN tunnel.
Tunnel Name	1. A must-filled setting 2. String format can be any text	Enter a name for the tunnel. *Value Range*: 1 ~ 19 characters.
Interface	1. A must-filled setting 2. **WAN 1** is selected by default	Select WAN interface on which the IPSec tunnel will be established.
Tunnel Scenario	1. A must-filled setting 2. **Tunnel Mode** is selected by default	Select the Dynamic IPSec tunneling scenario: **Tunnel Mode** or **Transport Mode**.
Encapsulation Protocol	1. A must-filled setting 2. **ESP** is selected by default	Select the Encapsulation Protocol: **ESP** or **AH**.
IKE Version	1. A must-filled setting 2. **v1** is selected by default	Specify the IKE version for this IPSec tunnel: v1 or v2.



Local & Remote Configuration Window		
Item	**Value setting**	**Description**
Local Subnet	A must-filled setting	Specify the Local Subnet IP address.
Local Netmask	A must-filled setting	Specify the Local Subnet Mask.



Authentication Configuration Window		
Item	**Value setting**	**Description**
Key Management	1. A must-filled setting 2. Pre-shared Key 8 to 32 characters.	Select Key Management for this IPSec tunnel. **IKE+Pre-shared Key:** Set a key (8 ~ 32 characters). **IKE+X.509:** IKE+X.509 will be available only when Certificate has been configured in advance (go to **Object Definition > Certificate**).
Local ID	An optional setting	Specify the Local ID for IPSec tunnel authentication. Select **Username** for Local ID and enter the username. Select **FQDN** for Local ID and enter the FQDN. Select **User@FQDN** for Local ID and enter the ID in the format: User@FQDN. Select **Key ID** for Local ID and enter the Key ID.
Remote ID	An optional setting	Specify the Remote ID for IPSec tunnel authentication. Specify the Local ID for IPSec tunnel authentication. Select **Username** for Local ID and enter the username. Select **FQDN** for Local ID and enter the FQDN. Select **User@FQDN** for Local ID and enter the ID in the format: User@FQDN. Select **Key ID** for Local ID and enter the Key ID. **Note:** Remote ID will not be available when Dynamic VPN is selected for Tunnel Scenario.

For IKE Phase, IKE Proposal Definition, IPSec Phase, and IPSec Proposal Definition settings, refer to the above sections of IPSec Tunnel configuration.

5.1.2 OpenVPN

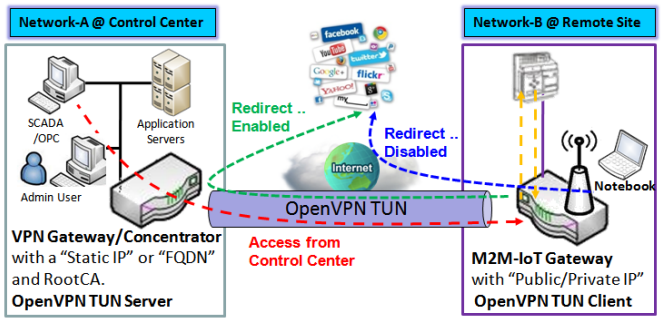
OpenVPN is an application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address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

OpenVPN allows peers to authenticate each other using a Static Key (pre-shared key) or certificate. When used in a server with multiple clients scenario, OpenVPN allows the server to release an authentication certificate for every client. It uses the OpenSSL encryption library based on the SSLv3/TLSv1 protocol to provide a variety of security and control features.

OpenVPN Tunneling is a client and server based tunneling technology. The OpenVPN server must have a static IP or an FQDN. The OpenVPN client may be a mobile user or mobile site with a public IP or private IP for requesting an OpenVPN tunnel connection. The product supports both OpenVPN server and OpenVPN client feature to meet different application requirements.

There are two OpenVPN connection scenarios: TAP and TUN. The gateway 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. The connection scenario is also required along with the server or client configuration.

OpenVPN TUN Scenario



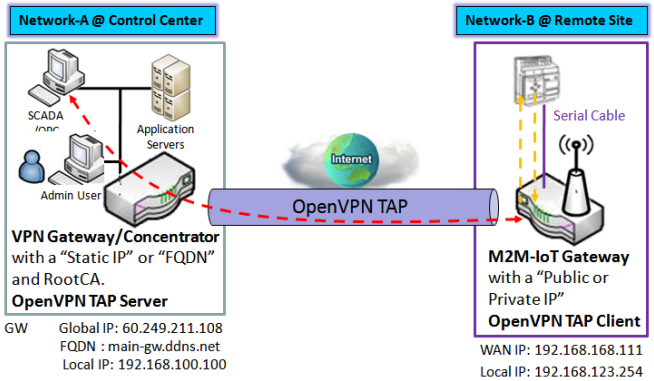
1. M2M-IoT Gateway (as OpenVPN TUN Client) connects to peer VPN Gateway/Concentrator (as OpenVPN TUN Server).
2. M2M-IoT Gateway will be assigned 10.8.0.2 IP Address after OpenVPN TUN Connection estabilshed. (10.8.0.x is a virtual subnet)
3. Local networked device will get a virtual IP 10.8.0.x if its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

The term "TUN" mode is used in routing mode. In routing mode, the VPN client is given an IP address that is different from other subnets in the local LAN. 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 from the local LAN. Remote hosts that connect from the other end will get an IP address in the virtual subnetwork and will have access only to the server where the OpenVPN service runs.

If you want to allow remote connection to a VPN server for access to only restricted resources, OpenVPN TUN mode is the simplest solution.

As shown in the diagram, the M2M-IoT gateway is configured as an OpenVPN TUN Client, which 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) of a virtual subnet that is different from the local subnet in the Control Center. With such connection, the local VPN devices will get a virtual IP 10.8.0.x for traffic to pass through the OpenVPN TUN connection when Redirect Internet Traffic settings is enabled; Besides, the SCADA Server in Control Center can access attached serial device(s) at the remote site with the virtual IP address of 10.8.0.2.

OpenVPN TAP Scenario



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

The term "TAP" is referred to bridge mode and operates with layer 2 packets. In bridge mode, the VPN client is given an IP address that is in the same subnet as the local LAN where the OpenVPN server is located, which allows OpenVPN clients to access the resources in LAN.

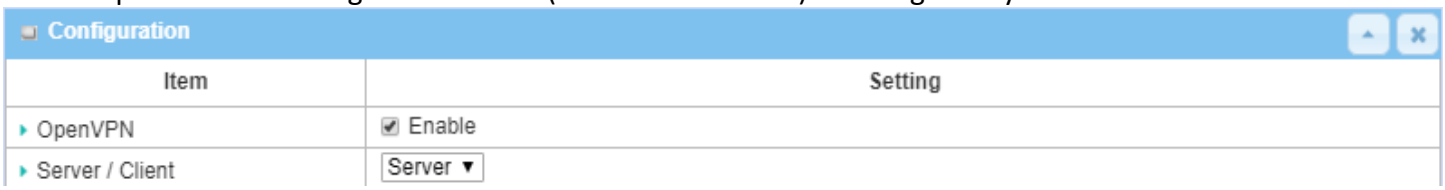
As shown in the diagram, the M2M-IoT gateway is configured as an OpenVPN TAP client and connects to an OpenVPN TAP Server. Once the OpenVPN TAP connection is established, the connected TAP client will be assigned a virtual IP (192.168.100.210) which is in the same subnet as the local subnet of the Control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

Open VPN Setting

Go to Security > VPN > OpenVPN to create and configure **OpenVPN tunnels.**

Enable OpenVPN

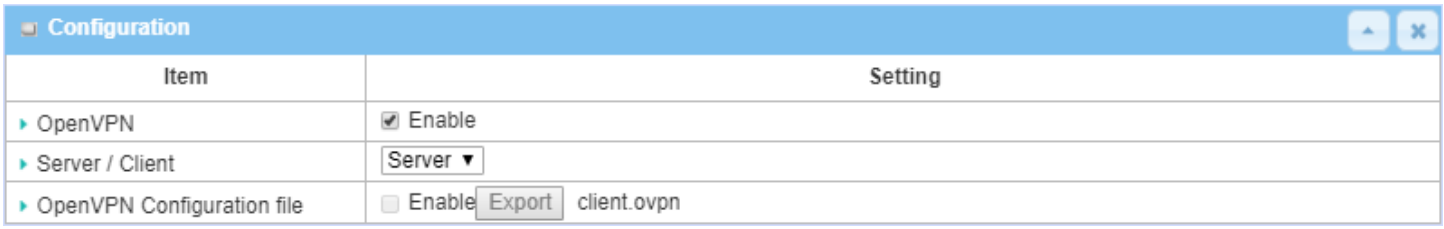
Enable OpenVPN and configure the mode (i.e. server or client) for the gateway.



Configuration Item	Value setting	Description
OpenVPN	The box is unchecked by default	Activate the OpenVPN function.
Server/ Client	Server Configuration is selected by default.	Select **Server** and configure more detailed settings for server configuration. Select **Client** and configure more detailed settings for client configuration.

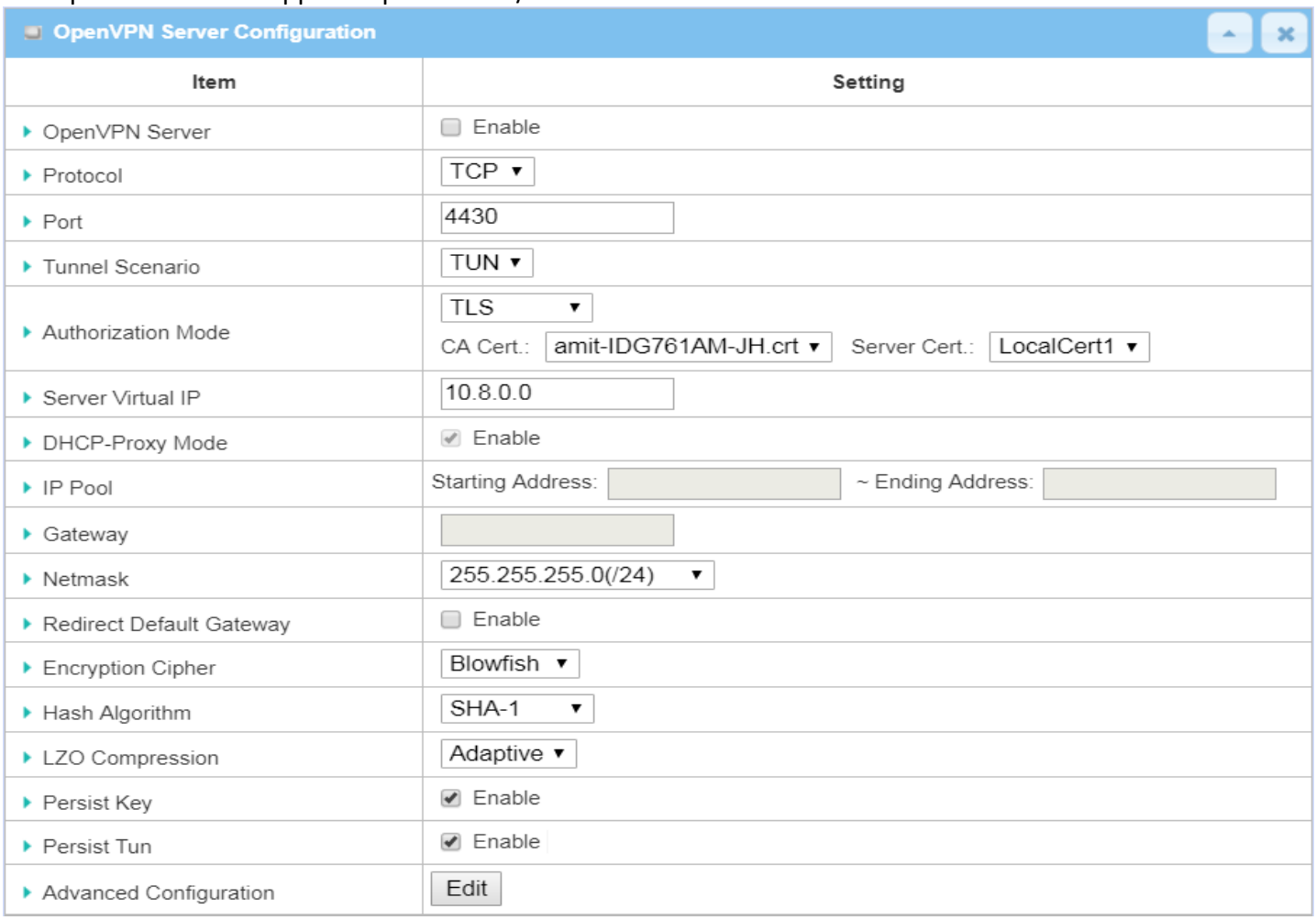
As an OpenVPN Server

Configure the OpenVPN Server settings with a virtual IP address of the OpenVPN server and related tunnel settings.



Configuration		
Item	**Value setting**	**Description**
OpenVPN Configuration File	1. An optional setting. 2. The box is unchecked by default.	Activate the export feature of OpenVPN Client configuration file as a .ovpn file. Click the **Export** button to download the configuration file.

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

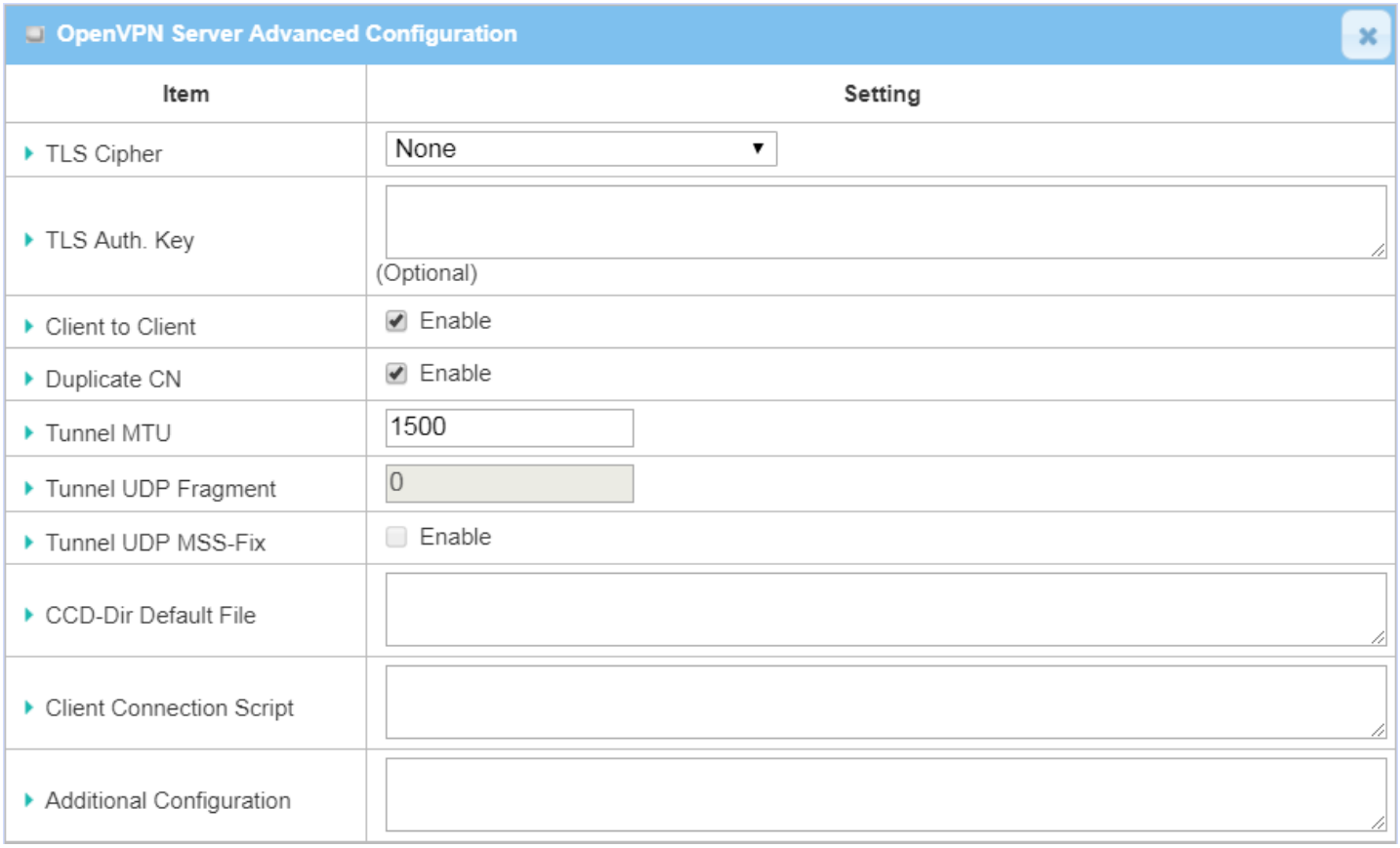


OpenVPN Server Configuration		
Item	**Value setting**	**Description**

OpenVPN Server	The box is unchecked by default.	Activate OpenVPN Server function.
Protocol	1. A must-filled setting 2. By default **TCP** is selected.	Define the **Protocol** for connecting to an OpenVPN Server. • Select **TCP or UDP** The TCP protocol will be used to access the OpenVPN Server with the default **Port** 4430. • Select **UDP** The UDP protocol will be used to access the OpenVPN Server with the default port 1194.
Port	1. A must-filled setting 2. By default **4430** is set.	Specify the **Port** for connecting to the OpenVPN Server. *Value Range*: 1 ~ 65535.
Tunnel Scenario	1. A must-filled setting 2. By default **TUN** is selected.	Specify the **Tunnel Scenario** for connecting to the OpenVPN Server: **TUN** for TUN tunnel scenario or **TAP** for TAP tunnel scenario.
Authorization Mode	1. A must-filled setting 2. By default **TLS** is selected.	Specify the authorization mode for the OpenVPN Server. • **TLS:** The OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Server Cert.** and **DH PEM** will be displayed. **CA Cert:** go to **Object Definition** > **Certificate** > **Trusted Certificate** for certificate generation. **Server Cert:** go to **Object Definition** > **Certificate** > **My Certificate** for certificate generation. • **Static Key:** The OpenVPN will use static key (pre-shared) authorization mode and you need to configure the **Local Endpoint IP Address**, **Remote Endpoint IP Address** and **Static Key**. **Note:** Static Key will be available only when TUN is selected as the Tunnel Scenario.
Local Endpoint IP Address	A must-filled setting	Specify the virtual **Local Endpoint IP Address** of the local OpenVPN gateway. *Value Range*: The IP format is 10.8.0.x, the range of x is 1~254. **Note:** Local Endpoint IP Address will be available only when Static Key is chosen as the Authorization Mode.
Remote Endpoint IP Address	A must-filled setting	Specify the virtual **Remote Endpoint IP Address** of the peer OpenVPN gateway. *Value Range*: The IP format is 10.8.0.x, the range of x is 1~254. **Note:** Remote Endpoint IP Address will be available only when Static Key is chosen as the Authorization Mode.
Static Key	A must-filled setting	Specify the **Static Key**. **Note:** Static Key will be available only when Static Key is chosen as the Authorization Mode.
Server Virtual IP	A must-filled setting	Specify the **Server Virtual IP**. *Value Range*: The IP format is 10.y.0.0, the range of y is 1~254. **Note:** Server Virtual IP will be available only when TLS is chosen as the Authorization Mode.
DHCP-Proxy Mode	1. A must-filled setting 2. The box is checked by default.	Activate the **DHCP-Proxy Mode**. **Note:** DHCP-Proxy Mode will be available only when TAP is chosen as the Tunnel Scenario.
IP Pool	A must-filled setting	Specify the virtual **IP pool** range for the OpenVPN server with the the **Starting Address** and **Ending Address** for the IP address pool of the OpenVPN clients. **Note:** IP Pool will be available only when TAP is chosen as the Tunnel Scenario and DHCP-Proxy Mode is unchecked (disabled).
gateway	A must-filled setting	Specify the **gateway** setting for the OpenVPN server. It will be assigned to the connected OpenVPN clients. **Note:** gateway will be available only when TAP is chosen as the Tunnel Scenario and DHCP-Proxy Mode is unchecked (disabled).
Netmask	By default **- select one -** is selected.	Specify the **Netmask** setting for the OpenVPN server. It will be assigned to the connected OpenVPN clients.

		Value Range: 255.255.255.0/24 (only support class C) **Note:** Netmask will be available when TAP is chosen as the Tunnel Scenario and DHCP-Proxy Mode is unchecked (disabled).
Redirect Default gateway	1. An optional setting. 2. The box is unchecked by default.	Activate the **Redirect Default gateway** function. Activate the **Redirect Default gateway** function. When this is enabled, local VPN devices will get a virtual IP from the IP pool for traffic to pass through the OpenVPN TUN connection.
Encryption Cipher	1. A must-filled setting. 2. By default **Blowfish** is selected.	Specify the **Encryption Cipher**: **Blowfish, AES-256/AES-192/AES-128,** or **None.**
Hash Algorithm	By default **SHA-1** is selected.	Specify the **Hash Algorithm**: **SHA-1, MD5, MD4, SHA2-256/SHA2-512, None,** or **Disable.**
LZO Compression	By default **Adaptive** is selected.	Specify the **LZO Compression** scheme: **Adaptive**, **YES/NO** or **Default.**
Multicast	1. An optional setting. 2. The box is checked by default.	Activate the **Multicast** function. **Note:** Multicast function is only available for TAP tunnel scenario.
Persis Key	1. An optional setting. 2. The box is checked by default.	Activate the **Persis Key** function.
Persis Tun	1. An optional setting. 2. The box is checked by default.	Activate the **Persis Tun** function.
Advanced Configuration	N/A	Click the **Edit** button to specify the **Advanced Configuration** setting for the OpenVPN server.
Save	N/A	Save the settings.
Undo	N/A	Cancel the changes and return to the previous page.

Click Edit **to open the** OpenVPN Server Advanced Configuration **screen.**

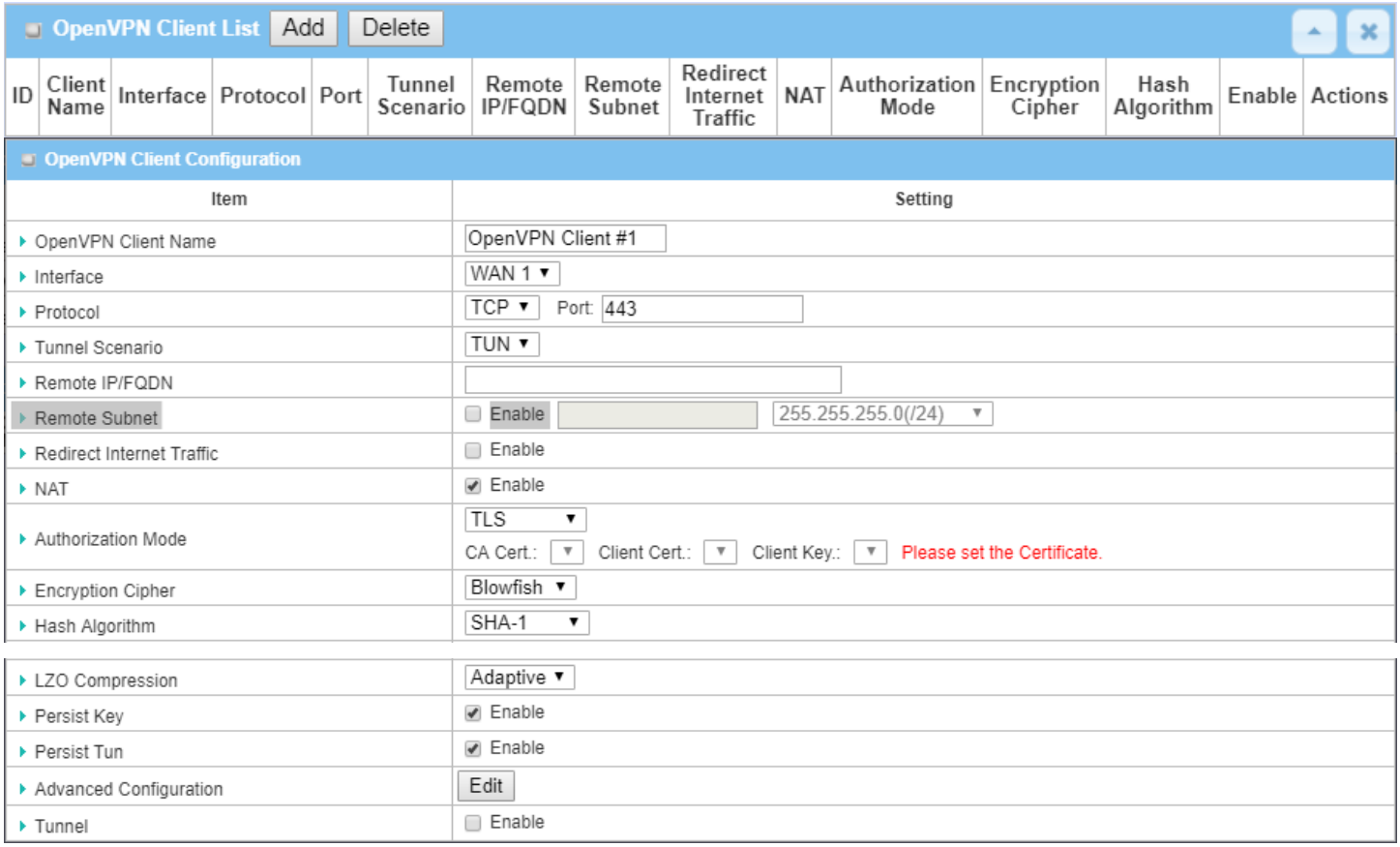


OpenVPN Server Advanced Configuration		
Item	**Value setting**	**Description**
TLS Cipher	1. A must-filled setting. 2. **TLS-RSA-WITH-AES128-SHA** is selected by default	Specify the **TLS Cipher**: **None, TLS-RSA-WITH-RC4-MD5, TLS-RSA-WITH-AES128-SHA, TLS-RSA-WITH-AES256-SHA, TLS-DHE-DSS-AES128-SHA,** or **TLS-DHE-DSS-AES256-SHA.** **Note:** TLS Cipher will be available only when TLS is chosen as the Authorization Mode.
TLS Auth. Key	1. An optional setting. 2. String format: any text	Specify the **TLS Auth. Key.** **Note:** TLS Auth. Key will be available only when TLS is chosen as the Authorization Mode.
Client to Client	The box is checked by default	Enable the traffic among different OpenVPN Clients. **Note:** Client to Client will be available only when TLS is chosen as the Authorization Mode
Duplicate CN	The box is checked by default	Activate the **Duplicate CN** function. **Note:** Duplicate CN will be available only when TLS is chosen as the Authorization Mode
Tunnel MTU	1. A must-filled setting 2. The value is **1500** by default	Specify the **Tunnel MTU.** *Value Range*: 0 ~ 1500.
Tunnel UDP Fragment	1. A must-filled setting 2. The value is **1500** by default	Specify the **Tunnel UDP Fragment.** By default, it is equal to **Tunnel MTU**. *Value Range*: 0 ~ 1500. **Note:** Tunnel UDP Fragment will be available only when UDP is chosen for Protocol.
Tunnel UDP MSS-Fix	1. An optional setting. 2. The box is unchecked	Activate the **Tunnel UDP MSS-Fix** Function. **Note:** Tunnel UDP MSS-Fix will be available only when UDP is chosen for

	by default.	Protocol.
CCD-Dir Default File	1. An optional setting. 2. String format: any text	Specify the **CCD-Dir Default File.** *Value Range*: 0 ~ 256 characters.
Client Connection Script	1. An optional setting. 2. String format: any text	Specify the **Client Connection Script.** *Value Range*: 0 ~ 256 characters.
Additional Configuration	1. An optional setting. 2. String format: any text	Specify the **Additional Configuration.** *Value Range*: 0 ~ 256 characters.

As an OpenVPN Client

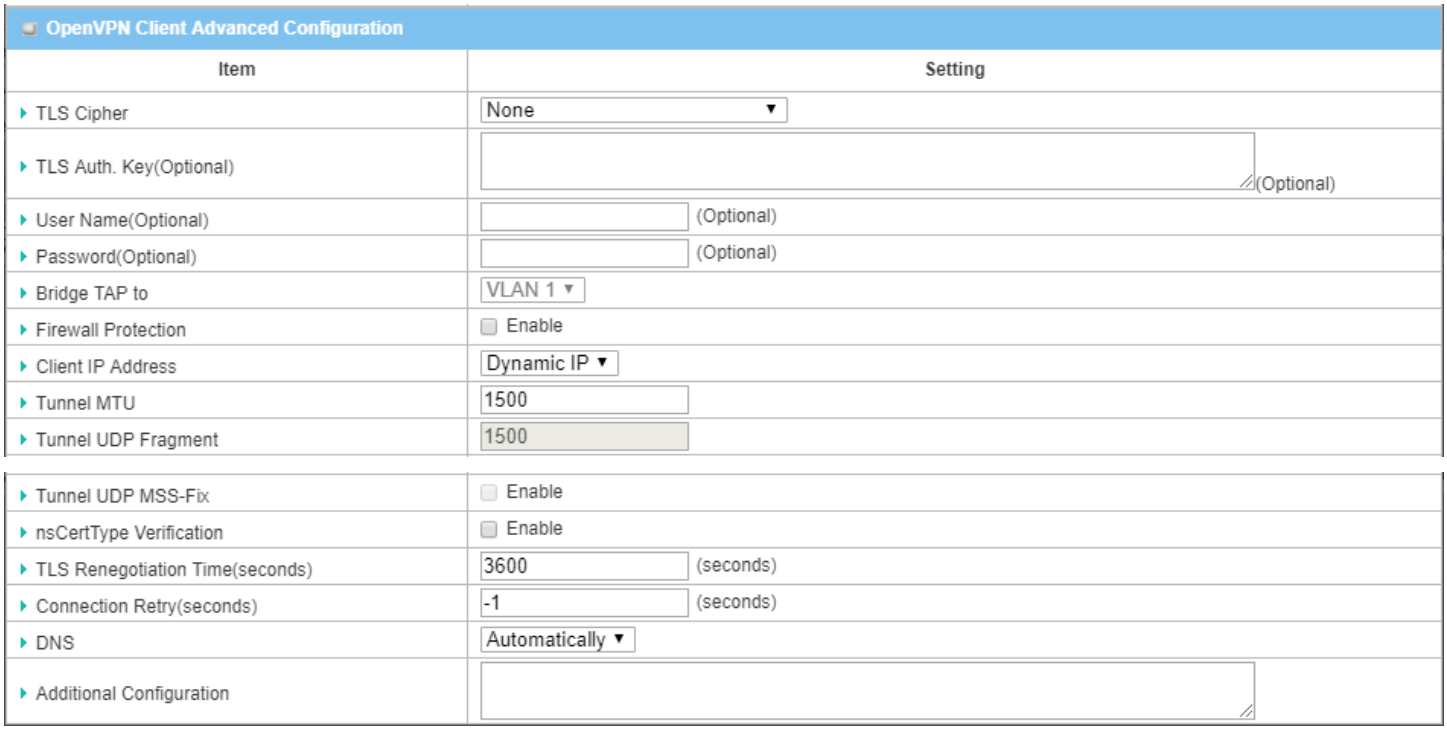
Configure the OpenVPN Client settings and related tunnel settings for OpenVPN client, for example, client name, interface and protocol, and tunnel scenario.



OpenVPN Client Configuration		
Item	**Value setting**	**Description**
OpenVPN Client Name	A must-filled setting	Enter a **OpenVPN Client Name** to be used to identify the client in the tunnel list. *Value Range*: 1 ~ 32 characters.
Interface	1. A must-filled setting 2. By default **WAN-1** is selected.	Define the physical interface to be used for this OpenVPN Client tunnel.
Protocol	1. A must-filled setting 2. By default **TCP** is selected.	Define the **Protocol** for connecting to an OpenVPN Server. • Select **TCP or UDP** The TCP protocol will be used to access the OpenVPN Server with the default **Port** 4430. • Select **UDP** The UDP protocol will be used to access the OpenVPN Server with the default port 1194.
Port	1. A must-filled setting 2. By default **443** is set.	Specify the **Port** for connecting to the OpenVPN Server. *Value Range*: 1 ~ 65535.
Tunnel Scenario	1. A must-filled setting 2. By default **TUN** is selected.	Specify the **Tunnel Scenario** for connecting to the OpenVPN Server: **TUN** for TUN tunnel scenario or **TAP** for TAP tunnel scenario.
Remote IP/FQDN	A must-filled setting	Specify the **Remote IP/FQDN** of the peer OpenVPN Server for this OpenVPN

		Client tunnel.
Remote Subnet	1. An optional setting. 2. The box is unchecked by default.	Activate remote subnet functionand specify **Remote Subnet** of the peer OpenVPN Server for this OpenVPN Client tunnel.
Redirect Internet Traffic	1. An optional setting. 2. The box is unchecked by default.	Activate the **Redirect Internet Traffic** function.
NAT	1. An optional setting. 2. The box is checked by default.	Activate the **NAT** function.
Authorization Mode	1. A must-filled setting 2. By default **TLS** is selected.	Specify the authorization mode for the OpenVPN Server. • **TLS:** The OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Server Cert.** and **DH PEM** will be displayed. **CA Cert:** go to **Object Definition** > **Certificate** > **Trusted Certificate** for certificate generation. **Server Cert:** go to **Object Definition** > **Certificate** > **My Certificate** for certificate generation. • **Static Key:** The OpenVPN will use static key (pre-shared) authorization mode and you need to configure the **Local Endpoint IP Address**, **Remote Endpoint IP Address** and **Static Key**. **Note:** Static Key will be available only when TUN is selected as the Tunnel Scenario.
Local Endpoint IP Address	A must-filled setting	Specify the virtual **Local Endpoint IP Address** of this OpenVPN gateway. *Value Range*: The IP format is 10.8.0.x, the range of x is 1~254. **Note:** Local Endpoint IP Address will be available only when Static Key is chosen as the Authorization Mode.
Remote Endpoint IP Address	A must-filled setting	Specify the virtual **Remote Endpoint IP Address** of the peer OpenVPN gateway. *Value Range*: The IP format is 10.8.0.x, the range of x is 1~254. **Note:** Remote Endpoint IP Address will be available only when Static Key is chosen as the Authorization Mode.
Static Key	A must-filled setting	Specify the **Static Key**. **Note:** Static Key will be available only when Static Key is chosen as the Authorization Mode.
Encryption Cipher	By default **Blowfish** is selected.	Specify the **Encryption Cipher: Blowfish, AES-256/AES-192/AES-128, or None.**
Hash Algorithm	By default **SHA-1** is selected.	Specify the **Hash Algorithm: SHA-1, MD5, MD4, SHA2-256/SHA2-512, None,** or **Disable.**
LZO Compression	By default **Adaptive** is selected.	Specify the **LZO Compression** scheme: **Adaptive, YES/NO,** or **Default.**
Multicast	1. An optional setting. 2. The box is checked by default.	Activate the **Multicast** function. **Note:** Multicast function is only available for TAP tunnel scenario.
Persis Key	1. An optional setting. 2. The box is checked by default.	Activate the **Persis Key** function.
Persis Tun	1. An optional setting. 2. The box is checked by default.	Activate the **Persis Tun** function.
Advanced Configuration	N/A	Click the **Edit** button to specify the **Advanced Configuration** setting for the OpenVPN server.
Tunnel	The box is unchecked by default	Activate this OpenVPN tunnel.
Save	N/A	Save the settings.
Undo	N/A	Cancel the changes and return to the previous page.

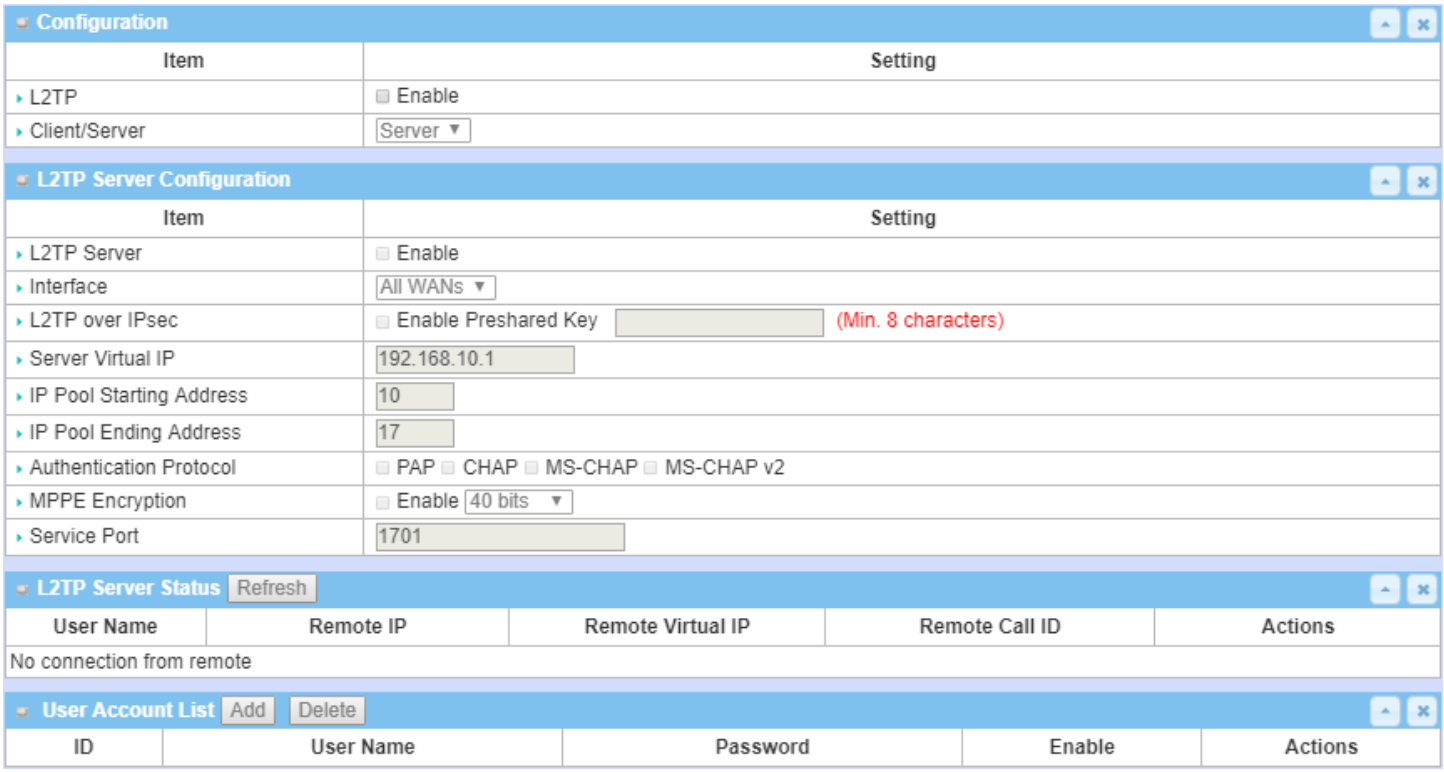
Click **Advanced Configuration** to open the **OpenVPN Client Advanced Configuration** screen.



OpenVPN Advanced Client Configuration		
Item	**Value setting**	**Description**
TLS Cipher	1. A must-filled setting. 2. **TLS-RSA-WITH-AES128-SHA** is selected by default	Specify the **TLS Cipher**: **None, TLS-RSA-WITH-RC4-MD5, TLS-RSA-WITH-AES128-SHA, TLS-RSA-WITH-AES256-SHA, TLS-DHE-DSS-AES128-SHA,** or **TLS-DHE-DSS-AES256-SHA.** **Note:** TLS Cipher will be available only when TLS is chosen as the Authorization Mode.
TLS Auth. Key	1. An optional setting. 2. String format: any text	Specify the **TLS Auth. Key.** **Note:** TLS Auth. Key will be available only when TLS is chosen for the Authorization Mode.
Username	An optional setting.	Enter the **User account** for connecting to an OpenVPN server if required. Note: Username will be available only when TLS is chosen for the Authorization Mode.
Password	An optional setting.	Enter the **Password** of the user account. **Note:** Username will be available only when TLS is chosen for the Authorization Mode.
Bridge TAP to	By default **VLAN 1** is selected	Specify the setting of "**Bridge TAP to**" to bridge the TAP interface to a specific local network interface or VLAN. **Note:** Bridge TAP will be available only when TAP is chosen for Tunnel Scenario and NAT is unchecked.
Firewall Protection	The box is unchecked by default.	Activate the **Firewall Protection** function. **Note:** Firewall Protection will be available only when NAT is enabled.
Client IP Address	By default **Dynamic IP** is selected	Specify the virtual IP Address for the OpenVPN Client:e **Dynamic IP** or **Static IP.**
Tunnel MTU	1.A must-filled setting 2.The value is 1500 by default	Specify the value of **Tunnel MTU.** *Value Range*: 0 ~ 1500.

Tunnel UDP Fragment	The value is 1500 by default	Specify the value of **Tunnel UDP Fragment.** *Value Range*: 0 ~ 1500. **Note:** Tunnel UDP Fragment will be available only when UDP is chosen for Protocol.
Tunnel UDP MSS-Fix	The box is unchecked by default.	Activate the **Tunnel UDP MSS-Fix** function. **Note:** Tunnel UDP MSS-Fix will be available only when UDP is chosen for Protocol.
nsCerType Verification	The box is unchecked by default.	Activate the **nsCerType Verification** function. **Note:** nsCerType Verification will be available only when TLS is chosen for the Authorization Mode.
TLS Renegotiation Time (seconds)	The value is 3600 by default	Specify the time interval of **TLS Renegotiation Time.** *Value Range*: -1 ~ 86400.
Connection Retry(seconds)	The value is -1 by default	Specify the time interval of **Connection Retry.** The default -1 means that this option is disabled. *Value Range*: -1 ~ 86400, and -1 means no retry is required.
DNS	By default **Automatically** is selected	Specify the setting of **DNS: Automatically** or **Manually.**
Additional Configuration	An optional setting.	Enter optional configuration string (up to 256 characters) here. *Value Range*: 0 ~ 256 characters.
Save	N/A	Save the settings.
Undo	N/A	Cancel the changes and return to the previous page.

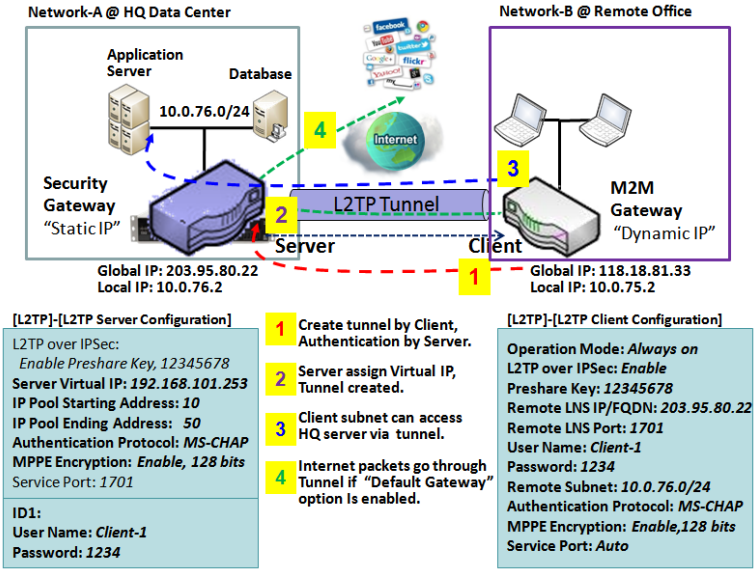
5.1.3 L2TP



Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or service delivery by ISPs. L2TP does't provide encryption and confidentiality and relies on IPSec to provide such security protection. This gateway can be configured as both a server and a client at the same time.

L2TP Server: A server must have a static IP or a FQDN for clients to create L2TP tunnels. It also maintains a "User Account list" (username/ password) for client login authentication. A virtual IP pool can be used to assign a virtual IP address to connected L2TP clients.

L2TP Client: A client can be mobile users or gateways in remote offices with a dynamic IP. To set up a tunnel, you should identify "username", "password", and server's global IP address. In addition, it is required to configure the operation mode (e.g. main connection, failover for another tunnel, or load balance) to optimize bandwidth utilization. The "Default gateway" or "Remote Subnet" should be identified to direct packet flow. Moreover, you can define what kind of traffic can pass through the L2TP tunnel in the "Default gateway/Remote Subnet" parameter.

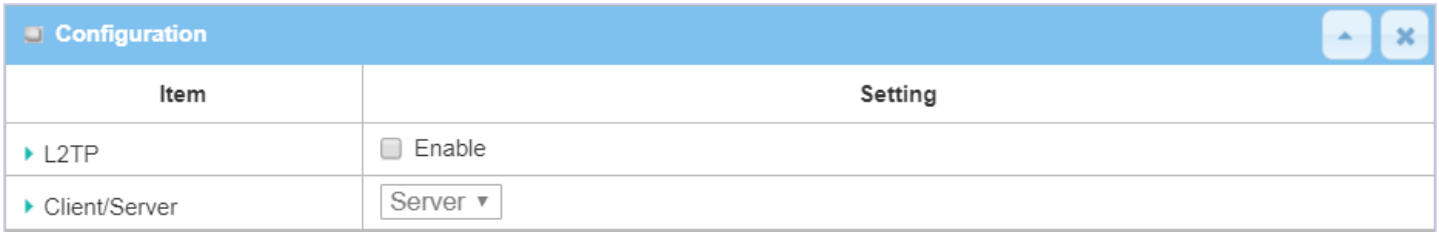


The diagram at the left illustrates how the configuration of the Remote Subnet for an L2TP client peer directs the packet flow. From the L2TP client peer, the packets destined for the dedicated subnet will be transferred via the L2TP tunnel. Other traffic will be transferred based on current routing policy of the gateway. For a Remote Subnet address of 0.0.0.0/0, which will be set as the "Default gateway" for the L2TP client peer, all packets, including the Internet traffic, will go through the established L2TP tunnel.

L2TP Setting

Go to **Security > VPN > L2TP** to create and configure L2TP tunnels.

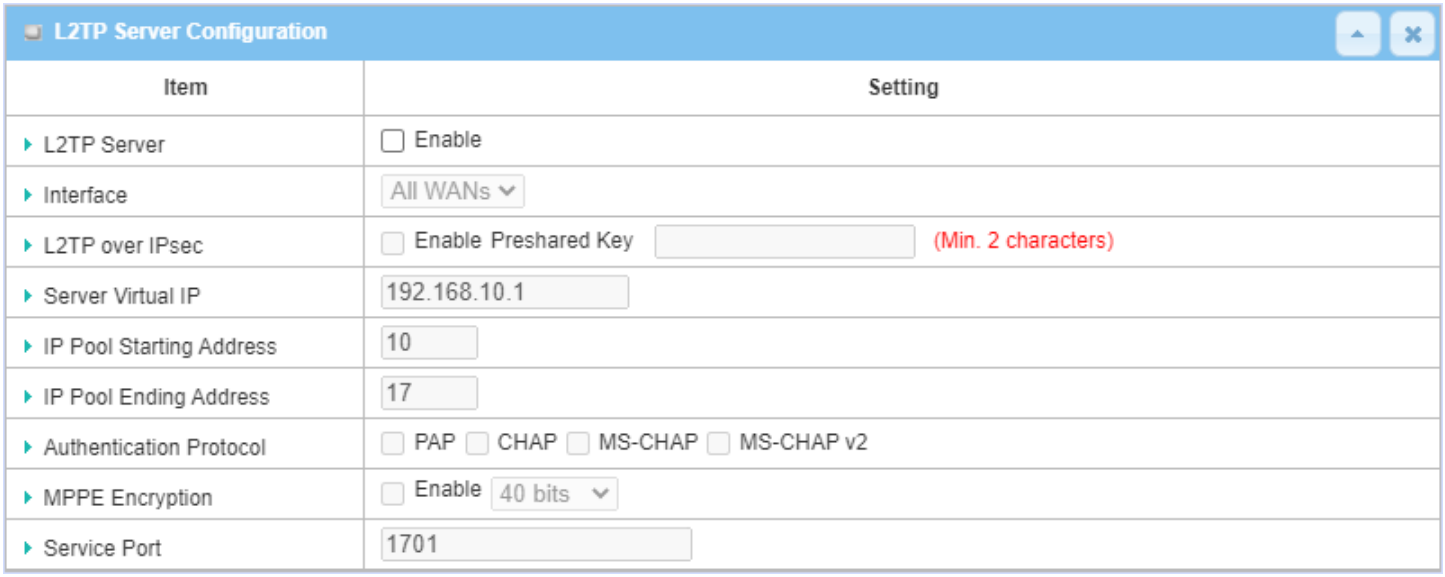
Enable L2TP



Enable L2TP Window		
Item	**Value setting**	**Description**
L2TP	Unchecked by default	Activate L2TP function.
Client/Server	A must-filled setting	Specify the role of L2TP: **Server** or **Client**. Configure the detailed settings for the selected role below.
Save	N/A	Save the settings

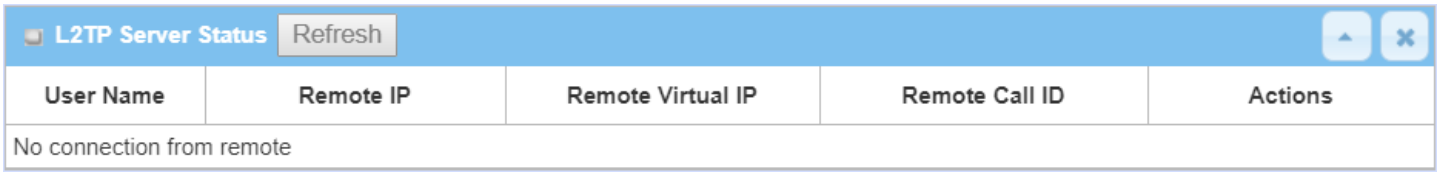
As an L2TP Server

Configure the L2TP server function with related settings such as interface and security features.

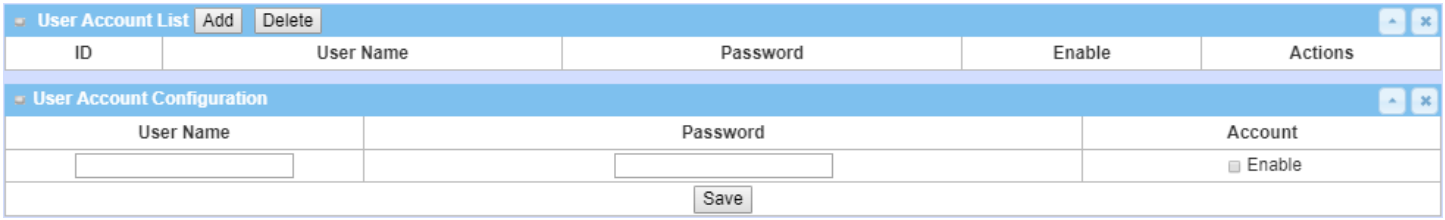


L2TP Server Configuration		
Item	**Value setting**	**Description**
L2TP Server	The box is unchecked by default	Activate the L2TP server.
Interface	1. A must-filled setting	Select the interface on which L2TP tunnel is to be established.

	2. **All WANs** is selected by default	
L2TP over IPSec	The box is unchecked by default	Enable L2TP over IPSec and fill in the Pre-shared Key (2~31 characters).
Server Virtual IP	A must-filled setting	Specify the L2TP local server Virtual IP.
IP Pool Starting Address	1. A must-filled setting **2. 10 is set by default.**	Specify the L2TP server starting IP of the virtual IP pool for client assignment. Value Range: 1 ~ 254.
IP Pool Ending Address	1. A must-filled setting **2. 17 is set by default.**	Specify the L2TP server ending IP of the virtual IP pool for client assignment. *Value Range*: >= Starting Address, and < (Starting Address + 8) or 254.
Authentication Protocol	A must-filled setting	Select the Authentication Protocols for the L2TP server to authenticate L2TP clients: **PAP, CHAP, MS-CHAP,** or **MS-CHAP v2**.
MPPE Encryption	A must-filled setting	Specify whether to support MPPE Protocol and select the key length: **40 bits, 56 bits**, or **128 bits**. **Note:** When MPPE Encryption is enabled, the Authentication Protocol **PAP** and **CHAP** options will not be available.
Service Port	A must-filled setting	Specify the **Service Port** for the L2TP server. *Value Range*: 1 ~ 65535.
Save	N/A	Save the configuration.
Undo	N/A	Discard the configuration.



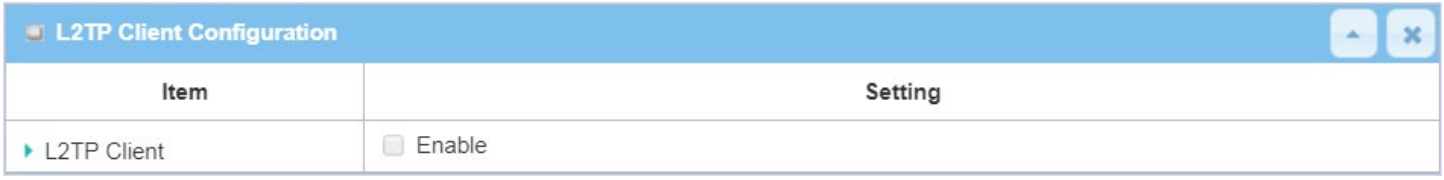
L2TP Server Status		
Item	**Value setting**	**Description**
L2TP Server Status	N/A	It displays the Username, Remote IP, Remote Virtual IP, and Remote Call ID of the connected L2TP clients. Click the **Refresh** button to renew the L2TP client information.



User Account List Window		
Item	**Value setting**	**Description**
User Account List	Max.of 10 user accounts	This is the L2TP authentication user account entry. You can create and add accounts for remote clients to establish L2TP VPN connection to the gateway. Click **Add** button to add a user account and enter the Username and password. The click **Save**. You can activate or delete a user account. *Value Range*: 1 ~ 32 characters.

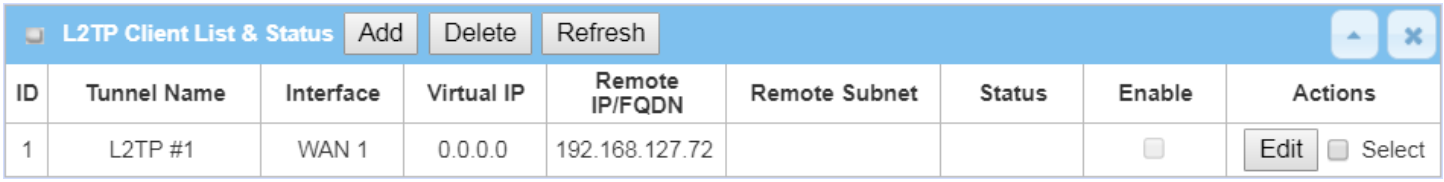
As an L2TP Client

Configure the L2TP Client function with related settings such as Remote IP and Subnet.

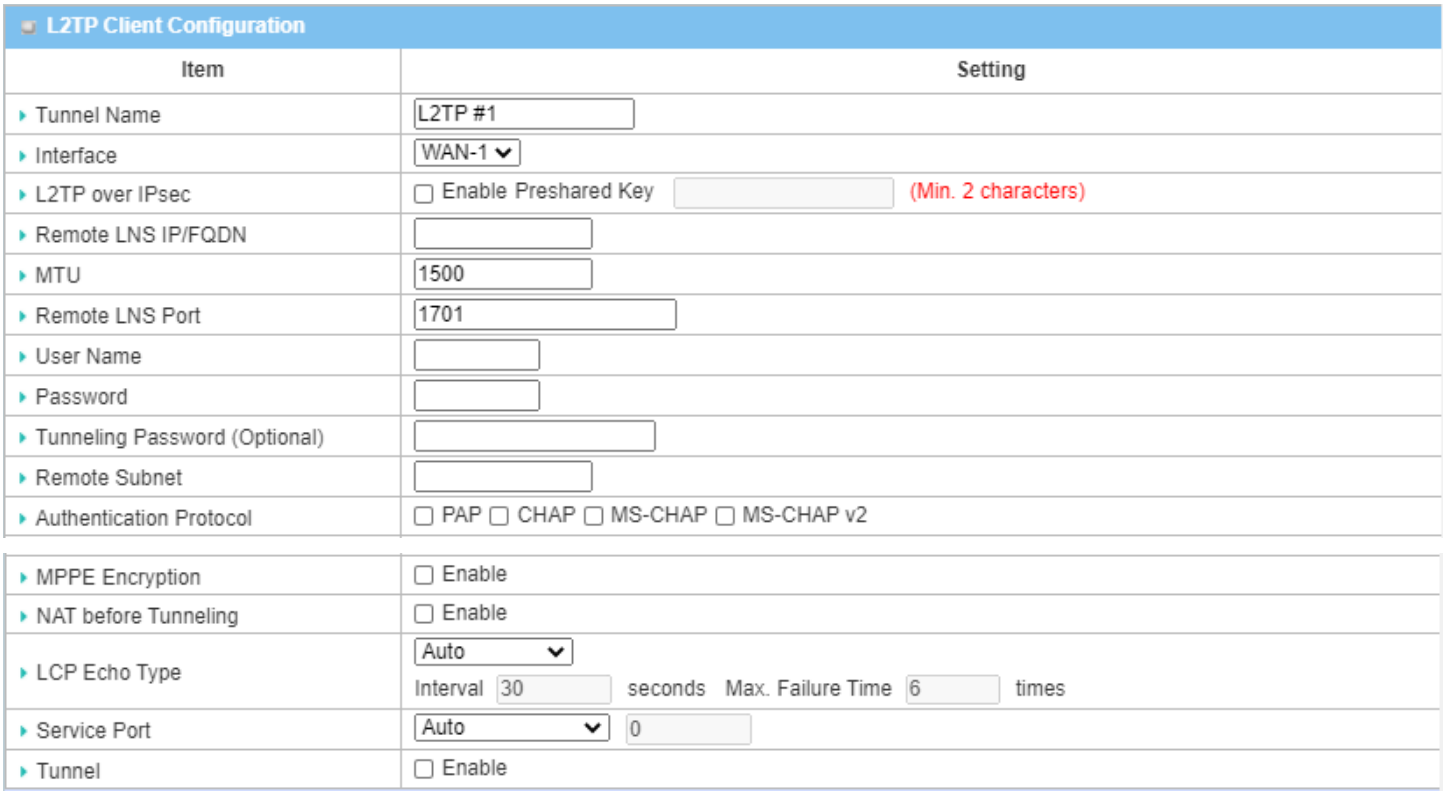


L2TP Client Configuration		
Item Setting	**Value setting**	**Description**
L2TP Client	The box is unchecked by default	Enable L2TP client function of the gateway.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings.

Create/Edit L2TP Client



Click Add/Edit to open the Client Configuration screen. You can add up to 8 L2TP Clients.

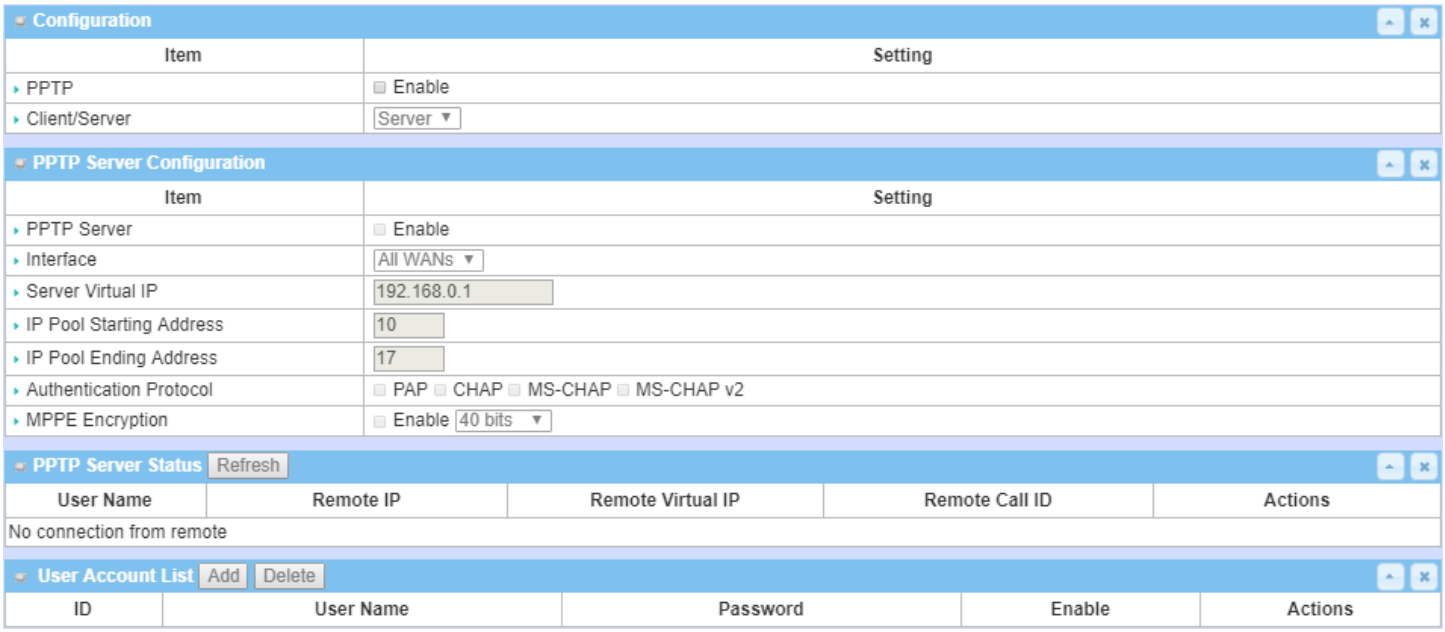


L2TP Client Configuration		
Item Setting	**Value setting**	**Description**

Tunnel Name	A must-filled setting	Enter a name for the tunnel name. *Value Range*: 1 ~ 32 characters.
Interface	A must-filled setting	Select an interface on which the L2TP tunnel will be established. A WAN interface is available only when it has been enabled in advance.
L2TP over IPSec	The box is unchecked by default	Enable L2TP over IPSec and fill in the Pre-shared Key (2~31 characters).
Remote LNS IP/FQDN	A must-filled setting	Enter the public IP address or the FQDN of the remote L2TP server.
MTU	1.A must-filled setting 2.The value is 1500 by default	Specify the **MTU.** *Value Range*: 0 ~ 1500.
Remote LNS Port	1. A must-filled setting 2. **1701** is set by default	Enter the Remote LNS Port for this L2TP tunnel. *Value Range*: 1 ~ 65535.
Username	A must-filled setting	Enter the **Username** for this L2TP tunnel to be authenticated. *Value Range*: 1 ~ 32 characters.
Password	A must-filled setting	Enter the **Password** for this L2TP tunnel to be authenticated.
Tunneling Password(Optional)	An optional setting	Enter the **Tunneling Password** of this user account.
Remote Subnet	A must-filled setting	Specify the remote subnet for this L2TP tunnel to reach L2TP server. Specify the subnet of the remote LAN in CIDR format (e.g. 10.0.0.2/24). From the L2TP client peer, the packets destined for the dedicated subnet will be transferred via the L2TP VPN tunnel. Other traffic will be transferred based on the current routing policy of the gateway. If you entered 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 traffic, will go through the established L2TP VPN tunnel.
Authentication Protocol	1. A must-filled setting 2. Unchecked by default	Specify the Authentication Protocol for this L2TP tunnel: PAP, CHAP, MS-CHAP, or MS-CHAP v2.
MPPE Encryption	1. Unchecked by default 2. An optional setting	Specify whether L2TP server supports **MPPE Protocol**. **Note:** When MPPE Encryption is enabled, the **PAP** / **CHAP** options of the Authentication Protocol will not be available.
NAT before Tunneling	1. A must-filled setting 2. Unchecked by default	Enable or disable NAT.
LCP Echo Type	1. Auto is set by default	Specify the LCP Echo Type for this L2TP tunnel: **Auto**, **User-defined**, or **Disable**. **Auto**: automatic configuration of the Interval and Max. Failure Time. **User-defined:** enter the Interval (default: 30 seconds) and Max. Failure Time (default: 6). **Disable**: disable the LCP Echo. *Value Range*: 1 ~ 99999 for Interval Time, 1~999 for Failure Time.
Service Port	A must-filled setting	Specify the Service Port for this L2TP tunnel: Auto, (1701) for Cisco, or User-defined. **Auto**: automatic configuration of the service port.

		1701 (for Cisco): The system uses port 1701 for connecting with CISCO L2TP Server. **User-defined:** Enter the service port. The default value is 0. *Value Range*: 0 ~ 65535.
Tunnel	Unchecked by default	Enable this L2TP tunnel.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings and back to the previous page.

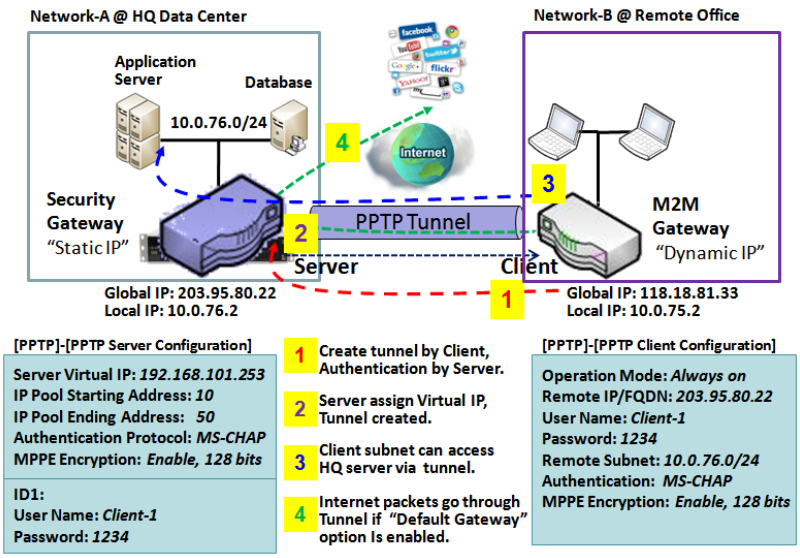
5.1.4 PPTP



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

PPTP Server: A server must have a static IP or a FQDN for clients to create PPTP tunnels. It also maintains a “User Account list” (username/ password) for client login authentication. A virtual IP pool can be used to assign a virtual IP address to connected PPTP clients.

PPTP Client: A client can be mobile users or gateways in remote offices with a dynamic IP. To set up a tunnel, you should identify “username”, “password”, and server’s global IP address. In addition, it is required to configure the operation mode (e.g. main connection, failover for another tunnel, or load balance) to optimize bandwidth utilization. The “Default gateway” or “Remote Subnet” should be identified to direct packet flow. Moreover, you can define what kind of traffic can pass through the PPTP tunnel in the “Default gateway/Remote Subnet” parameter.



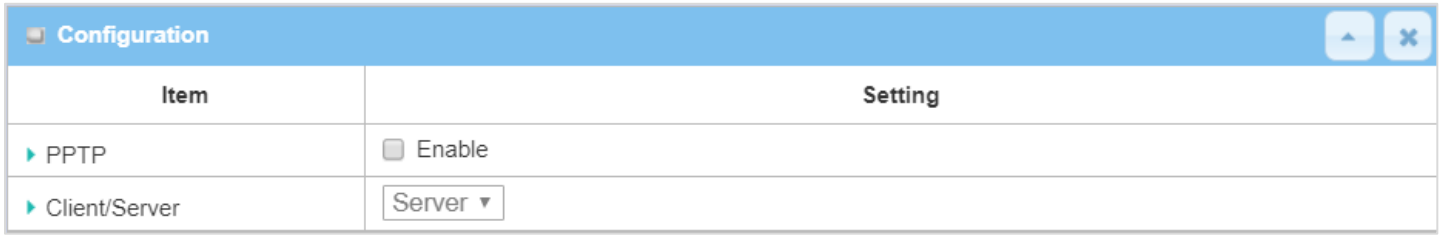
The diagram at the left illustrates how the configuration of the Remote Subnet for an PPTP client peer directs the packet flow. From the PPTP client peer, the packets destined for the designated subnet will be transferred via the PPTP tunnel. Other traffic will be transferred according to current routing policies of the gateway. For a Remote Subnet address of 0.0.0.0/0, which will be set as the "Default gateway" for the PPTP client peer, all packets, including the Internet traffic, will go through the established PPTP tunnel.

PPTP Setting

Go to **Security > VPN > PPTP** to access the PPTP Setting page.

The PPTP setting page allows you to create and configure PPTP tunnels.

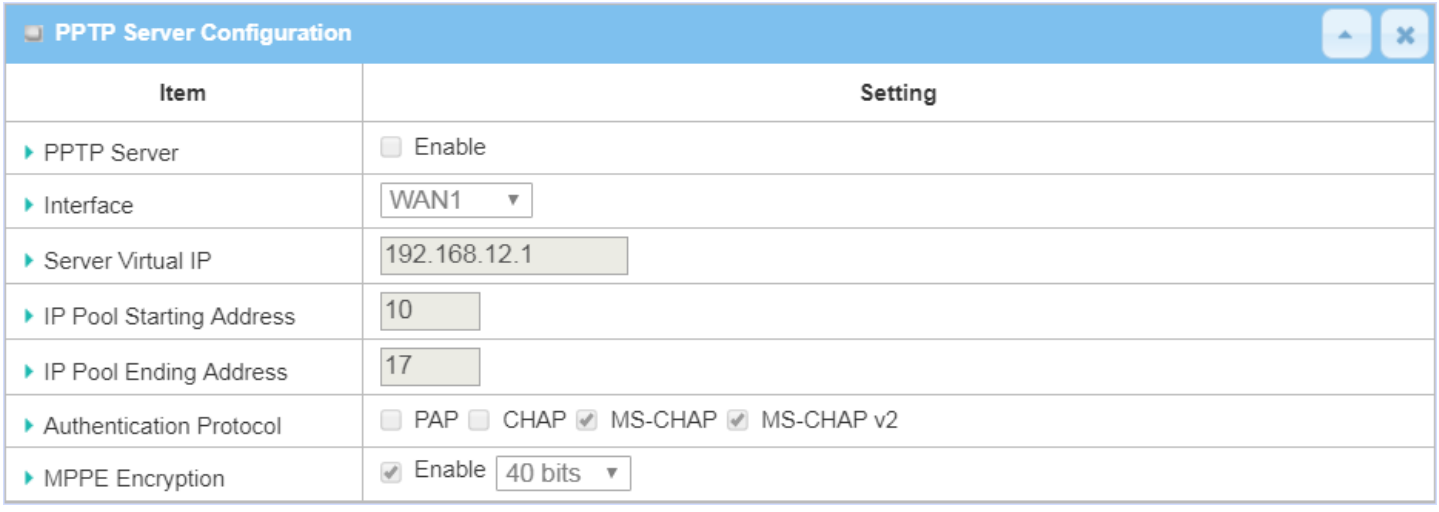
Enable PPTP



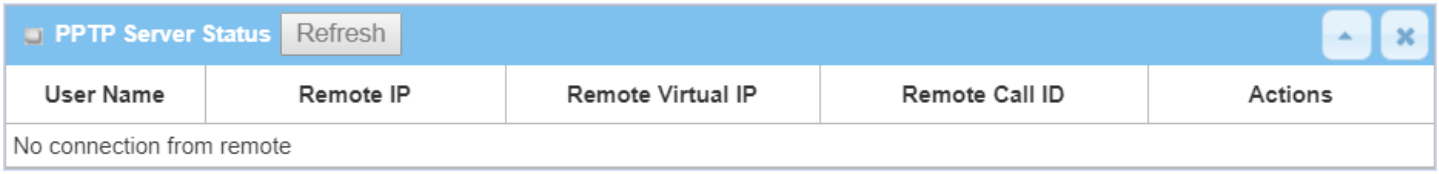
Enable PPTP Window		
Item	**Value setting**	**Description**
PPTP	Unchecked by default	Activate PPTP function.
Client/Server	A must-filled setting	Specify the role of PPTP: **Server** or **Client** role and configure the detailed settings for the selected role.
Save	N/A	Save the settings.

As a PPTP Server

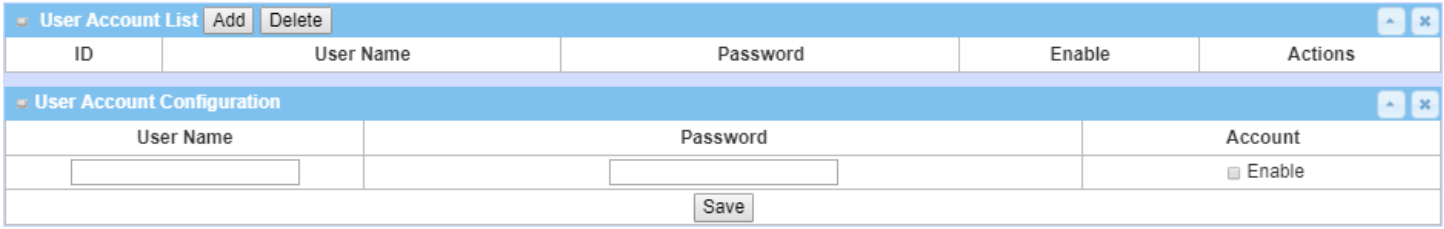
Configure the PPTP Server function with related settings, such as IP address and authentication protocol.



PPTP Server Configuration Window		
Item	**Value setting**	**Description**
PPTP Server	Unchecked by default	Enable PPTP server role of the gateway.
Interface	1. A must-filled setting 2. **All WANs** is selected by default	Select the interface on which PPTP tunnel is to be established.
Server Virtual IP	1. A must-filled setting 2. Default is 192.168.0.1	Specify the Virtual IP address. The virtual IP address will serve as the virtual DHCP server for the PPTP clients.
IP Pool Starting Address	1. A must-filled setting 2. Default is **10**	This is the PPTP server's Virtual IP DHCP assignment setting. Specify the start IP address for the subnet for client assignment. Value Range: 1 ~ 254.
IP Pool Ending Address	1. A must-filled setting 2. Default is **17**	This is the PPTP server's Virtual IP DHCP assignment setting. Specify the end IP address for the subnet for client assignment. It must be greated than or equal to the start value and less than the start value plus 8 or 254. *Value Range*: >= Starting Address, and < (Starting Address + 8) or 254.
Authentication Protocol	1. A must-filled setting 2. Unchecked by default	Select Authentication Protocols for the PPTP server to authenticate PPTP clients: **PAP, CHAP, MS-CHAP,** or **MS-CHAP v2**.
MPPE Encryption	1. A must-filled setting 2. Unchecked by default	Specify whether to support MPPE Protocol and select the key length: **40 bits**, **56 bits,** or **128 bits**. **Note:** when MPPE Encryption is enabled, the **PAP** / **CHAP** options of the Authentication Protocol will not be available.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings.



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

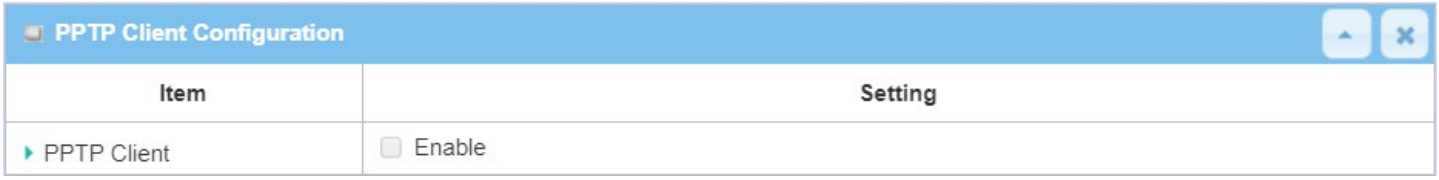


User Account List Window

Item	Value setting	Description
User Account List	Max.of 10 user accounts	This is the PPTP authentication user account entry. The gateway supports up to 10 PPTP user accounts. You can create and add accounts for remote clients to establish PPTP VPN connection to the gateway. Click **Add** button to add a user account and enter the username and password. The click **Save**. You can activate or delete a user account. *Value Range*: 1 ~ 32 characters.

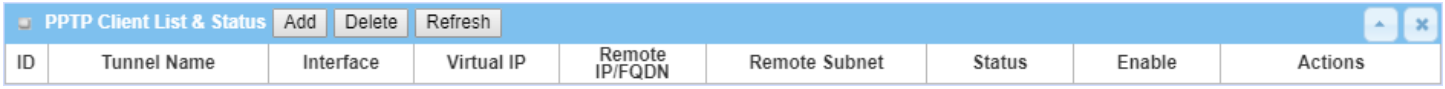
As a PPTP Client

Configure the PPTP Client function with related settings such as Remote IP and Subnet.

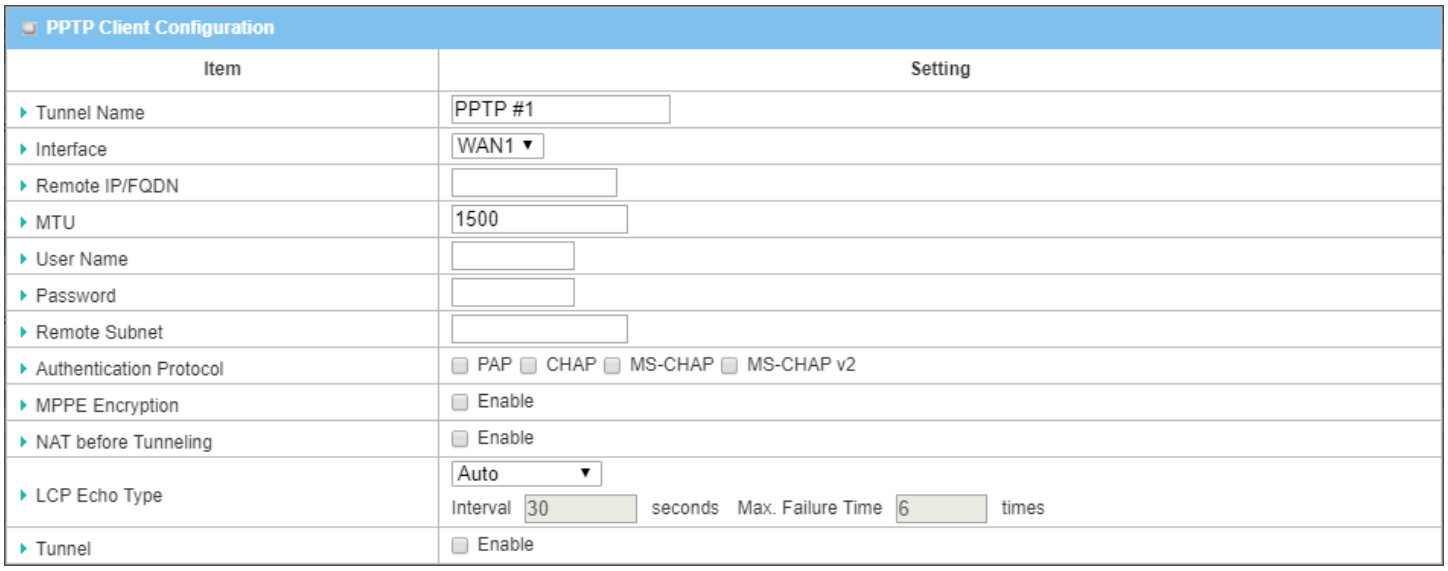


PPTP Client Configuration		
Item	**Value setting**	**Description**
PPTP Client	Unchecked by default	Enable PPTP client role of the gateway.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings.

Create/Edit PPTP Client



Click **Add/Edit** to open the **Client Configuration** screen.



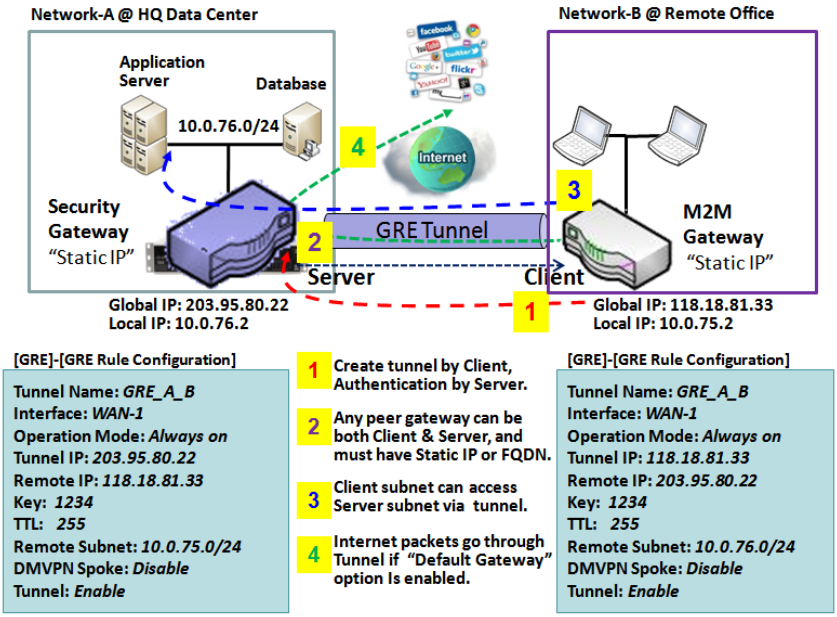
PPTP Client Configuration Window		
Item	**Value setting**	**Description**
Tunnel Name	A must-filled setting	Enter a name for the tunnel. *Value Range*: 1 ~ 32 characters.
Interface	1. A must-filled setting 2. **WAN1** is selected by default	Select an interface on which the PPTP tunnel will be established. A WAN interface is available only when it has been enabled in advance. (Go to **Basic Network > WAN & Uplink > Physical Interface**.)
Remote IP/FQDN	1. A must-filled setting. 2. Format can be a ipv4 address or FQDN	Enter the public IP address or the FQDN of the PPTP server.
MTU	1.A must-filled setting 2.The value is 1500 by default	Specify the **MTU.** *Value Range*: 0 ~ 1500.
Username	A must-filled setting	Enter the **Username** for this PPTP tunnel for authentication. *Value Range*: 1 ~ 32 characters.
Password	A must-filled setting	Enter the **Password** of this PPTP user account.
Remote Subnet	A must-filled setting	Specify the remote subnet for this PPTP tunnel to reach L2TP server. Specify the subnet of the remote LAN in CIDR format (e.g. 10.0.0.2/24). From the PPTP client peer, the packets destined for the dedicated subnet will be transferred via the PPTP VPN tunnel. Other traffic will be transferred based on the current routing policy of the gateway. If you entered 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 traffic, will go through the established PPTP VPN tunnel.
Authentication Protocol	1. A must-filled setting 2. Unchecked by default	Specify the Authentication Protocol for this PPTP tunnel: PAP, CHAP, MS-CHAP, or MS-CHAP v2.
MPPE Encryption	1. Unchecked by default	Specify whether PPTP server supports **MPPE Protocol**.

	2. An optional setting	**Note:** When MPPE Encryption is enabled, the **PAP** / **CHAP** options of the Authentication Protocol will not be available.
NAT before Tunneling	1. A must-filled setting 2. Unchecked by default	Enable or disable NAT.
LCP Echo Type	Auto is set by default	Specify the LCP Echo Type for this L2TP tunnel: **Auto**, **User-defined**, or **Disable**. **Auto**: automatic configuration of the Interval and Max. Failure Time. **User-defined:** enter the Interval (default: 30 seconds) and Max. Failure Time (default: 6). **Disable**: disable the LCP Echo. *Value Range*: 1 ~ 99999 for Interval Time, 1~999 for Failure Time.
Tunnel	Unchecked by default	Enable this PPTP tunnel.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings and go back to the previous page.

5.1.5 GRE

Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco Systems that encapsulates a wide variety of network layer protocols inside virtual point-to-point links over an IP internetwork. GRE Tunneling is similar to IPSec Tunneling by which a client can request a tunnel connection with a server. It allows hosts from a remote site to communicate with servers behind another M2M gateway.

GRE Tunnel Scenario



To set up a GRE tunnel, configure a global IP as the tunnel IP and a remote IP of the gateway at the other side. From a GRE client peer, the packets destined for a dedicated subnet will be transferred via the GRE tunnel. Other traffic will be transferred according to the current routing policies of the gateway. For a Remote Subnet address of 0.0.0.0/0, which will be set as the "Default gateway" for the remote client, all packets, including the Internet traffic, will go through the established tunnel.

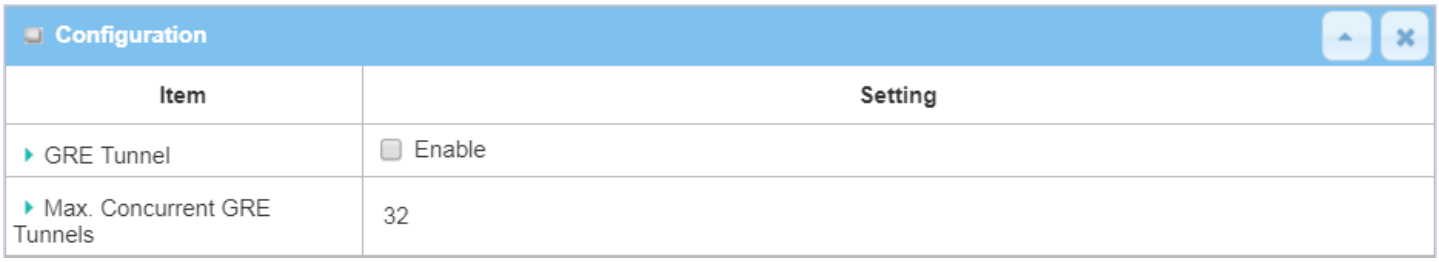
If a GRE server supports DMVPN Hub function, which works as a VPN concentrator on a Cisco gateway, the GRE client can activate the DMVPN spoke function, which is implemented by GRE over IPSec tunneling.

GRE Setting

Go to **Security > VPN > GRE** to access the GRE setting page.

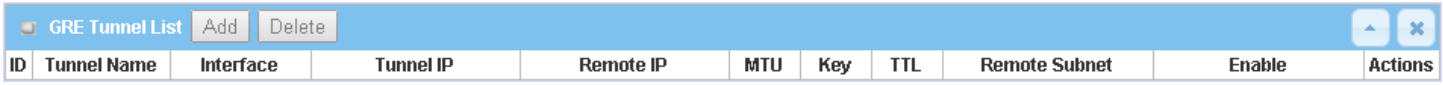
The GRE setting allows you to create and configure GRE tunnels.

Enable GRE

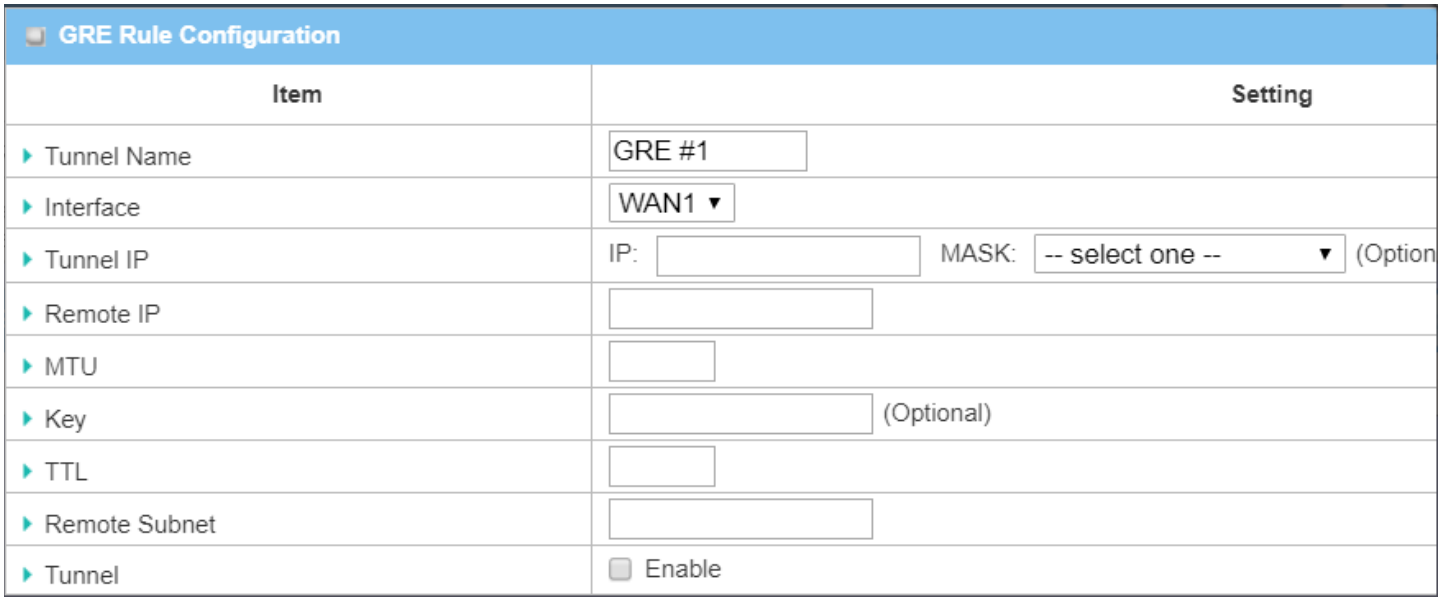


Enable GRE Window		
Item	**Value setting**	**Description**
GRE Tunnel	Unchecked by default	Enable GRE function.
Max. Concurrent GRE Tunnels	Depends on Product specification.	Enter the maximum number of simultaneous GRE tunnel connection.
Save	N/A	Save the settings
Undo	N/A	Cancel the settings

Create/Edit GRE Tunnel



Click **Add/Edit** to open the **GRE Rule Configuration** screen.

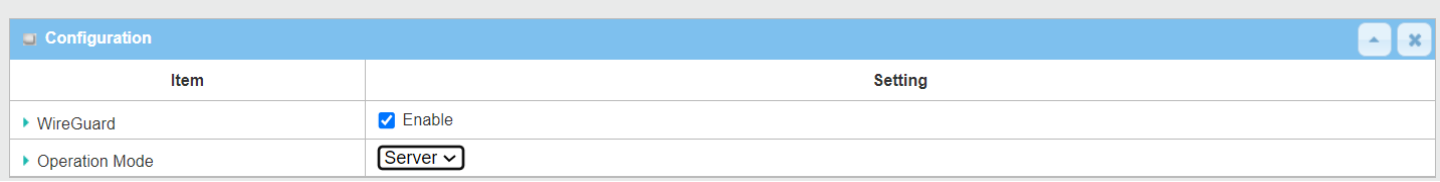


GRE Rule Configuration Window		
Item	**Value setting**	**Description**
Tunnel Name	A must-filled setting	Enter a name for the tunnel. *Value Range*: 1 ~ 9 characters.
Interface	1. A must-filled setting 2. **WAN 1** is selected by default	Select the interface on which GRE tunnel is to be established. It can be any available WAN and LAN interfaces.
Tunnel IP	An optional setting	Enter the Tunnel IP address and corresponding subnet mask.
Remote IP	A must-filled setting	Enter the Remote IP address of remote GRE tunnel gateway. Normally this is the public IP address of the remote gateway.
MTU	1. A must-filled setting 2. **Auto** (value zero or blank) is set by default	**MTU** refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Select Auto (value '0' or blank) to let the gateway configure the best MTU for optimal connection. *Value Range*: 0 ~ 1500.
Key	An optional setting	Enter the Key for the GRE connection. *Value Range*: 0 ~ 9999999999.
TTL	1. A must-filled setting 2. 1 to 255 range	Specify **TTL** hop-count value for this GRE tunnel. Value Range: 1 ~ 255.
Remote Subnet	A must-filled setting	Specify the remote subnet for this GRE tunnel to reach GRE server. Specify the subnet of the remote LAN in CIDR format (e.g. 10.0.0.2/24). From the GRE client peer, the packets destined for the dedicated subnet will be transferred via the GRE tunnel. Other traffic will be transferred according to the current routing policy of the gateway. A subnet setting of 0.0.0.0/0 will be treated as the default gateway setting for the GRE client peer, all packets, including the Internet traffic, will go through the established GRE VPN tunnel.
Tunnel	Unchecked by default	Enable this GRE tunnel.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings and go back to the previous page.

5.1.6 WireGuard

WireGuard® is an efficient and modern VPN tool that creates point-to-point dedicated connections with advanced encryption.
Go to **Security > VPN > WireGuard** to access the WireGuard setting page.

Enable WireGuard

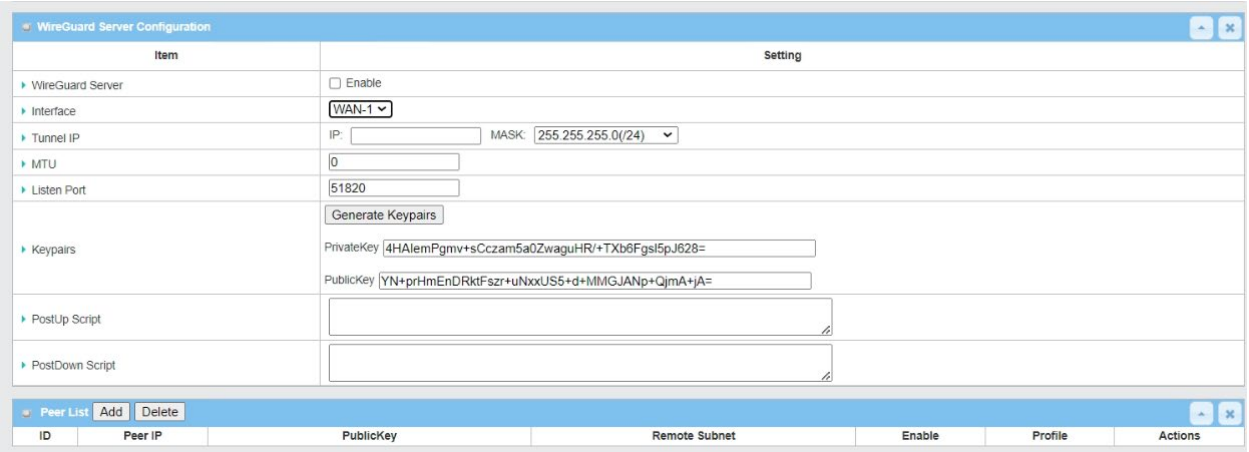


Enable WireGuard® Window		
Item	**Value setting**	**Description**

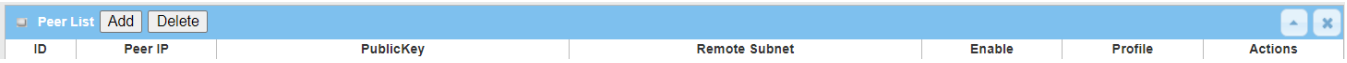
WireGuard	Unchecked by default	Activate WireGuard function.
Client/Server	A must-filled setting	Specify the role of WireGuard: **Server** or **Client** role and configure the detailed settings for the selected role.
Save	N/A	Save the settings.

As a WireGuard Server

Configure the WireGuard Server function with related settings, such as IP address and authentication keys.



WireGuard Server Configuration Window		
Item	**Value setting**	**Description**
WireGuard Server	Unchecked by default	Enable WireGuard server role of the gateway.
Interface	A must-filled setting	Select the interface on which WireGuard tunnel is to be established.
Tunnel IP	A must-filled setting	Specify the Tunneling IP address and Sunet Mask.
MTU	A must-filled setting	Specify the Maximum Transfer Unit. The default is 0.
Listen Port	A must-filled setting	The service port number. The default is 51820.
Keypairs	A must-filled setting	Click the **Generate Keypairs** button to generate both private key and public key for authentication
PostUP/PostDown Script	Optional	Enter custom PostUP/PostDown scripts to execute IP forwarding rules automatically after being connected or disconnected via VPN.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings.



Peer List Window		
Item	**Value setting**	**Description**
Peer IP		Enter the Peer IP address of the peer from the other end.
Private/Public key		The public and private key pairs for the peer to be authenticated.
Pre-sharedKey (Option)	Optional	Enter the optional pre-shared key and enable authentication with a pre-shared key.
Remote Subnet		The subnet address of the remote site.
Enable		Enable this peer to connection.

As a WireGuard Client

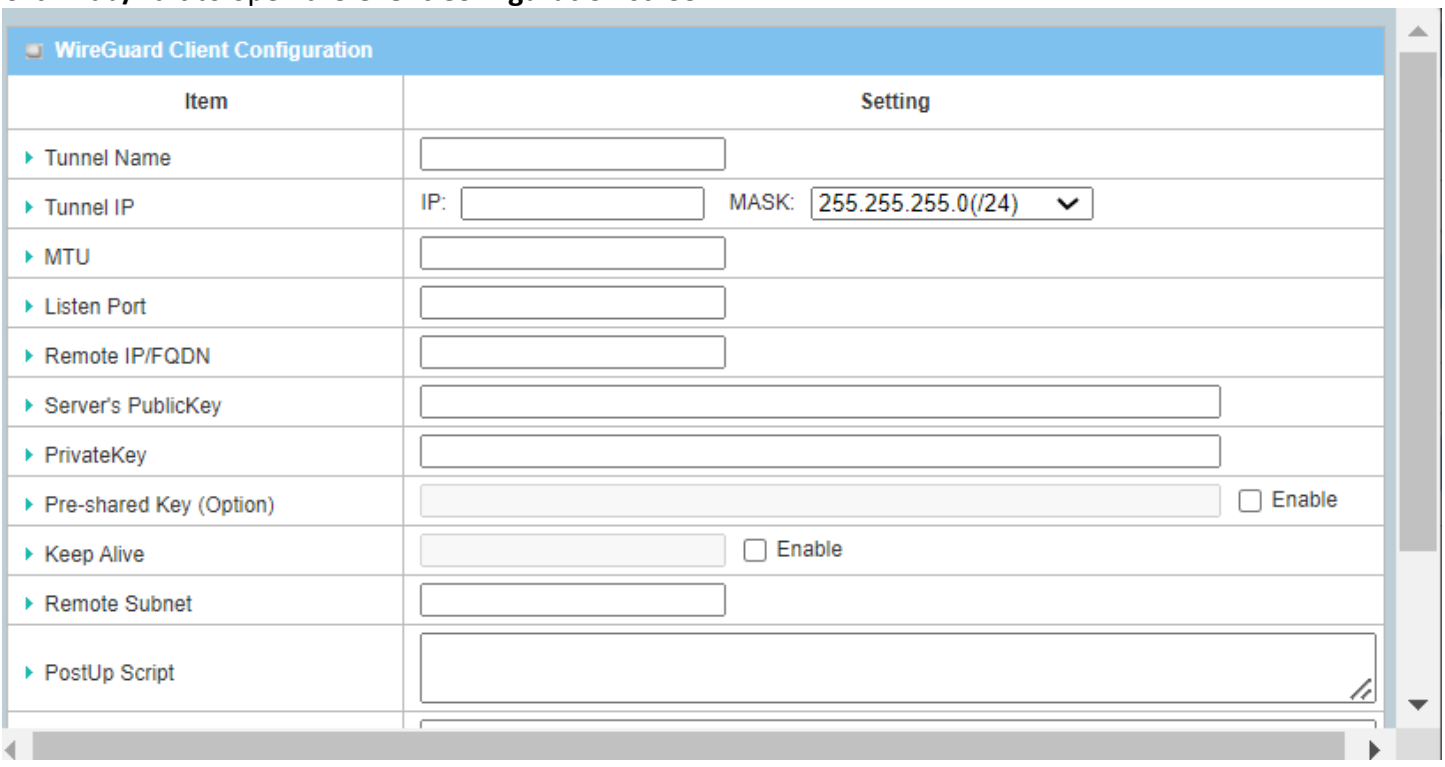
Configure the Client function with related settings for connection to a WireGuard server.



Create/Edit WireGuard Client



Click **Add/Edit** to open the **Client Configuration** screen.



WireGuard Client Configuration Window		
Item	**Value setting**	**Description**
Tunnel Name	A must-filled setting	Enter a name for the tunnel.
Tunnel IP	A must-filled setting	Specify the Tunneling IP address and Sunet Mask.
MTU	A must-filled setting	Specify the Maximum Transfer Unit. The default is 0.
Listen Port	A must-filled setting	The service port number. The default is 51820.
Remote IP/FQDN	1. A must-filled setting. 2. Format can be a ipv4 address or FQDN	Enter the public IP address or the FQDN of the WireGuard server.

Server's PublicKey		Enter the server's public key for authentication.
Private	A must-filled setting	Enter the private key for authentication
Pre-sharedKey (Option)	Optional	Enter the optional pre-shared key and enable authentication with a pre-shared key if the server requires it.
KeepAlive	Optional	Enable this function and enter the number of seconds to monitor the VPN connection to keep it connected.
Remote Subnet	A must-filled setting.	The subnet address of the remote site.
PostUP/PostDown Script	Optional	Enter custom PostUP/PostDown scripts to execute IP forwarding rules automatically after being connected or disconnected via VPN.
Tunnel		Enable or disable this tunnel.
Save	N/A	Save the settings.

5.2 Firewall

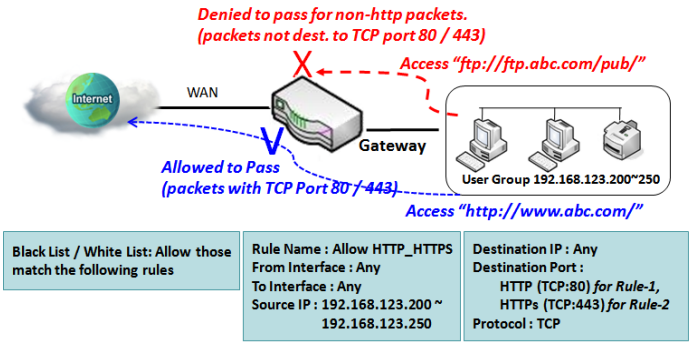
The firewall functions include Packet Filter, URL Blocking, MAC Control, IPS, and other related options. The supported functions can be different depending on the model.

5.2.1 Packet Filter

Packet Filter lets you define filter rules for incoming and outgoing packets. A packet filter rule specifies the criteria for passing or blocking packets, for example, the interface the packet passes through, the source and destination IP addresses, and destination service port type and port number. And together with a time schedule, the rule will be active at a recurring date and time.



Packet Filter with White List Scenario



As shown in the diagram, a "Packet Filter Rule List" is created as an allowed list (*Allow those match the following rules*) with the following criteria: Rule-1 is to allow HTTP packets to pass while Rule-2 is to allow HTTPS packets to pass.

Under such configuration, the gateway will allow only HTTP and HTTPS packets from a source IP address in the ragne of 192.168.123.200 to 250.

Packet Filter Setting

The packet filter setting allows you to create and customize packet filter policies to allow or block specific inbound/outbound traffic.

Go to **Security > Firewall > Packet Filters** to access the Packet Filter Setting page.

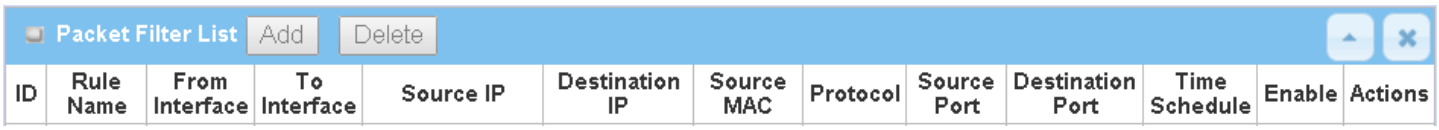
Enable Packet Filter



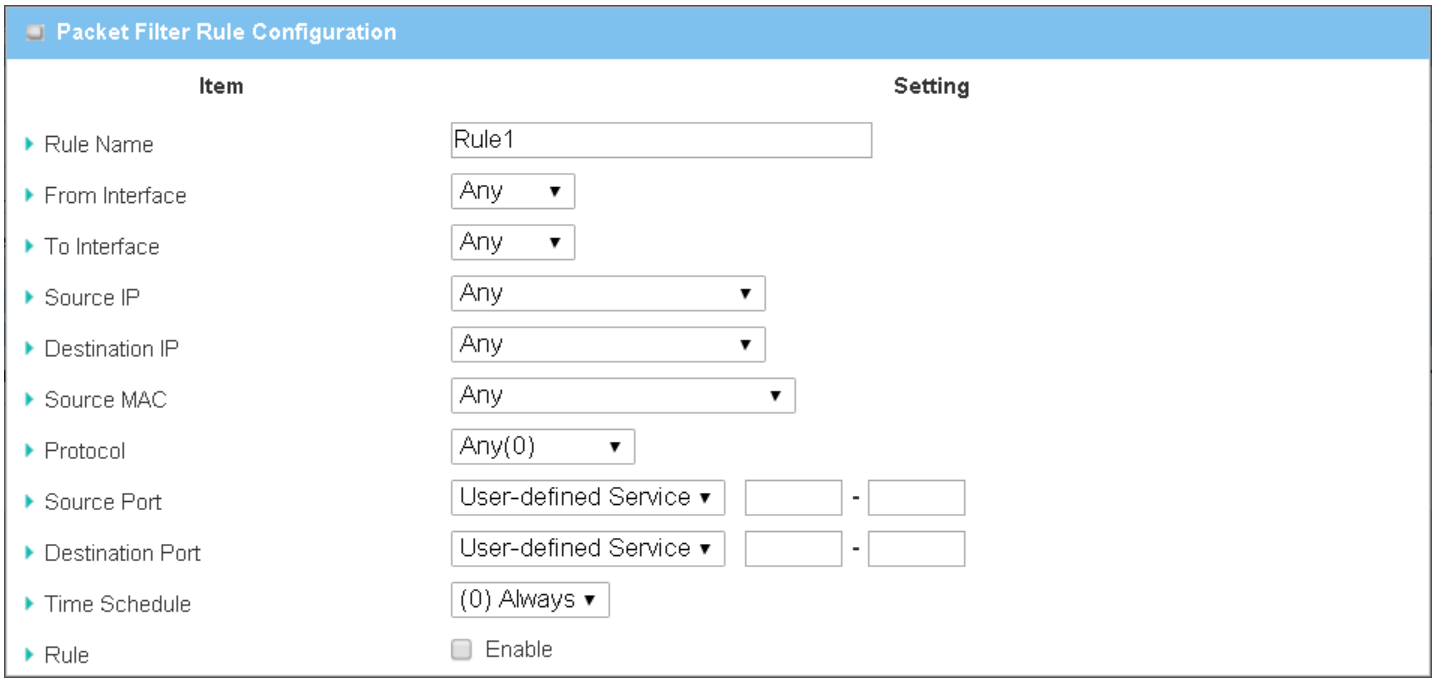
Configuration Window		
Item Name	**Value setting**	**Description**
Packet Filter	The box is unchecked by default	Activate Packet Filter function
Black List / White List	Deny those match the following rules is set by default	When ***Deny those match the following rules*** is selected, packets matching these rules will be blocked. In contrast, for the ***Allow those match the following rules***, packets matching these rules will be allowed to pass while all other packets will be blocked.
Log Alert	The box is unchecked by default	Activate alert logging. Go to **Status > Security > Firewall** to view the logged alerts.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

Create/Edit Packet Filter Rules

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



Click **Add** to open the **Packet Filter Rule Configuration** screen.



Packet Filter Rule Configuration		
Item Name	**Value setting**	**Description**
Rule Name	1. String format can be any text 2. A must-filled setting	Enter a name for the packet filter rule. *Value Range*: 1 ~ 30 characters.
From Interface	1. A must-filled setting **2. By default Any is selected**	Select the source interface to apply the rule. If the packets to be filtered are coming from **LAN to WAN**, select LAN for this field. Select **Any** to filter packets coming into the gateway from any interfaces. Please note that an identical interface for both the incoming and outgoing interface is not allowed. e.g., VLAN-1 to VLAN-1.
To Interface	1. A must-filled setting 2. By default **Any** is selected	Select the interface to be the outgoing interface of the gateway. If the packets to be filtered are entering from **LAN to WAN,** select **WAN** for this field. Select **Any** to filter packets leaving the gateway from any interfaces. Please note that an identical interface for both the incoming and outgoing interface is not allowed. e.g., VLAN-1 to VLAN-1.
Source IP	1. A must-filled setting 2. By default **Any** is selected	Specify the Source IP address. Select **Any** to filter packets with any source IP addresses. Select **Specific IP Address** to filter packets with the specified source IP address. Select **IP Range** to filter packets with the specified range of IP address. Select **IP Address-based Group** to filter packets with the source IP address defined in the pre-defined group. **Note:** Groups must be configured first (go to **Object Definition > Grouping > Host grouping**). Click **Add Rule** to create a new group.
Destination IP	1. A must-filled setting 2. By default **Any** is selected	Specify the Destination IP address. Select **Any** to filter packets with any destination IP addresses. Select **Specific IP Address** to filter packets with the specified destination IP address. Select **IP Range** to filter packets with the specified range of IP address. Select **IP Address-based Group** to filter packets with the destination IP address defined in the pre-defined group.

		Note: Groups must be configured first (go to **Object Definition > Grouping > Host grouping**)**.** Click **Add Rule** to create a new group.
Source MAC	1. A must-filled setting 2. By default **Any** is selected	Specify the Source MAC address. Select **Any** to filter packets coming from any MAC addresses. Select **Specific MAC Address** to filter packets coming from the specified MAC address. Select **MAC Address-based Group** to filter packets coming from the pre-defined group. **Note:** Groups must be configured first (go to **Object Definition > Grouping > Host grouping**)**.** Click **Add Rule** to create a new group.
Protocol	1. A must-filled setting 2. By default **Any(0)** is selected	For Protocol, select the protocol to be filtered: TCP, UDP, GRE, ESP, SCTP, Any, or ICMPv4. For **Source Port**, select a pre-defined port when **Well-known Service** is selected or select **User-defined Service** and specify a port range. For **Destination Port**, select a pre-defined port when **Well-known Service** is selected or select **User-defined Service** and specify a port range. *Value Range*: 1 ~ 65535 for Source Port, Destination Port.
		For **Protocol**, select **ICMPv4** to filter ICMPv4 packets
		For **Protocol**, select **TCP** to filter **TCP** packets Then for **Source Port**, select a pre-defined port when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. Then for **Destination Port**, select a pre-defined port when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. *Value Range*: 1 ~ 65535 for Source Port, Destination Port.
Time Schedule	A must-filled setting	Apply **Time Schedule** for the rule to be in effect. Configure the Time Schedule in advance (go to **Object Definition > Scheduling > Configuration**).
Rule	The box is unchecked by default.	Activate this rule.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings and go back to the previous page.

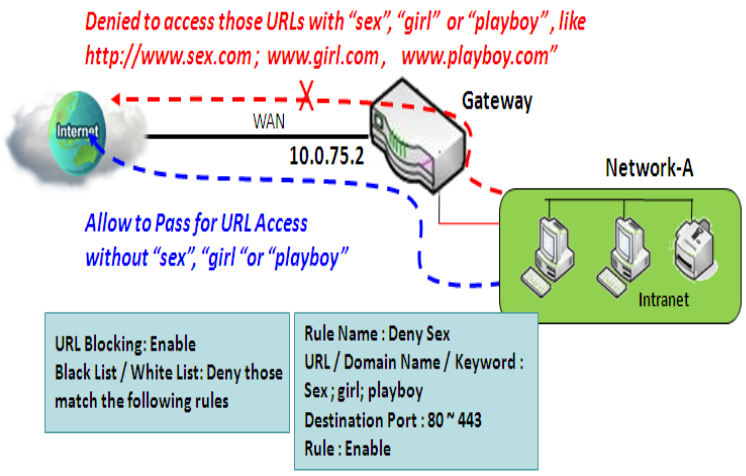
5.2.2 URL Blocking

URL Blocking lets you block or allow incoming and outgoing web request packets on the basis of a complete URL, partial domain name, or pre-defined keywords. For example, you can filter out or allow only the web requests based on domain names like .com or .org or keywords like “bct” or “mpe”.

An URL blocking rule should consist of URLs, partial domain names, or keywords in the web requests passing through the gateway. A time-based rule can be accomplished by applying a schedule.

The gateway will also log and display the blocked web requests that match the defined URL blocking rules.

URL Blocking Rule with Black List

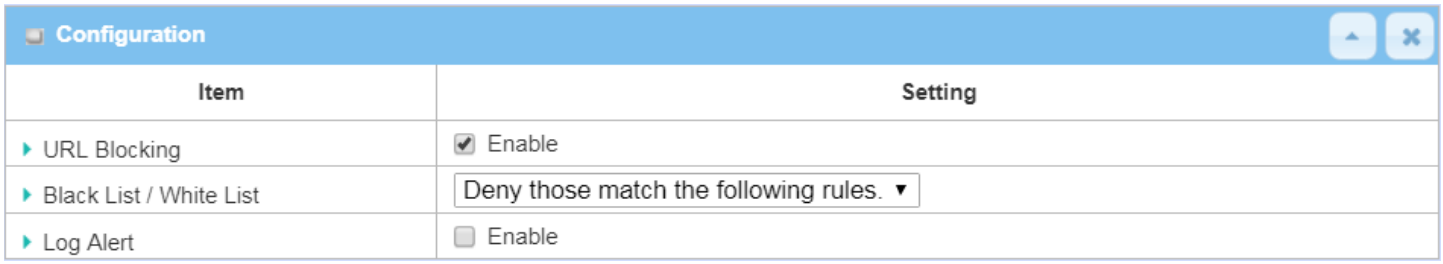


The "URL Blocking" function prevents specific web requests by defining a blacklist as shown in the diagram. On the other hand, a whitelist allows only web requests matching the defined rules. The example defines the URL keywords: "sex", "sexygirl", and "sexygirl" to block such web content.

URL Blocking Setting

Go to **Security > Firewall > URL Blocking** to access the URL Blocking Setting page.

Enable URL Blocking



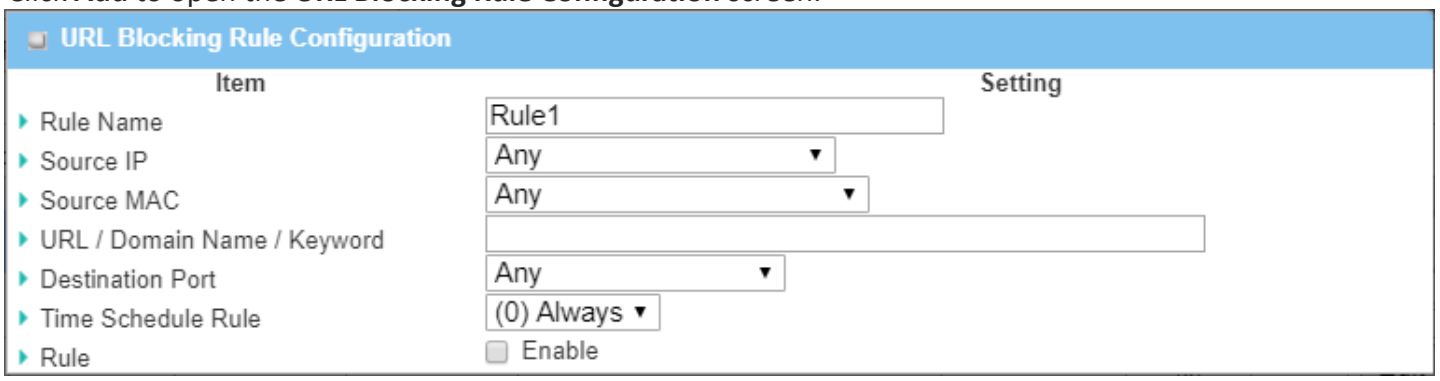
Configuration		
Item	**Value setting**	**Description**
URL Blocking	The box is unchecked by default	Activate URL Blocking function.
Black List / White List	**Deny those match the following rules** is set by default	Specify the URL Blocking Policy, either Black List or White List. Black List: When **Deny those match the following rules** is selected, the matched web request packets will be blocked. White List: When **Allow those match the following rules** is selected, the matched web request packets can pass through the gateway, while all other packets will be blocked.
Log Alert	The box is unchecked by default	Activate alert logging. Go to **Status > Security > Firewall** to view the logged alerts.
Save	NA	Save the settings
Undo	NA	Cancel the settings

Create/Edit URL Blocking Rules

The gateway supports a maximum of 20 URL blocking rules. Ensure that the URL Blocking is enabled first.



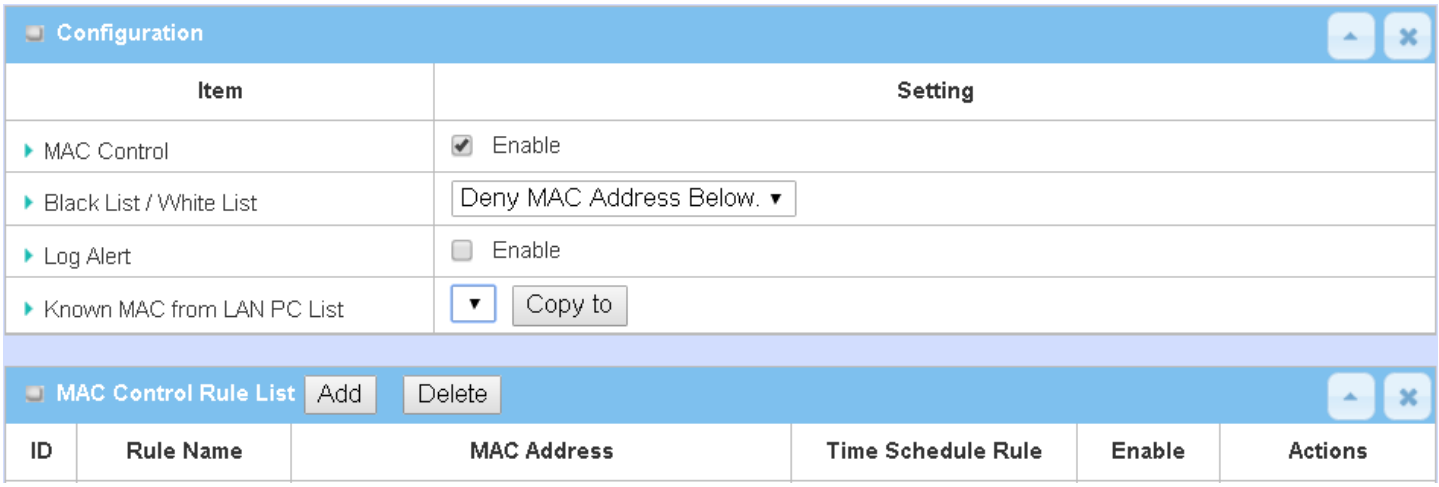
Click **Add** to open the **URL Blocking Rule Configuration** screen.



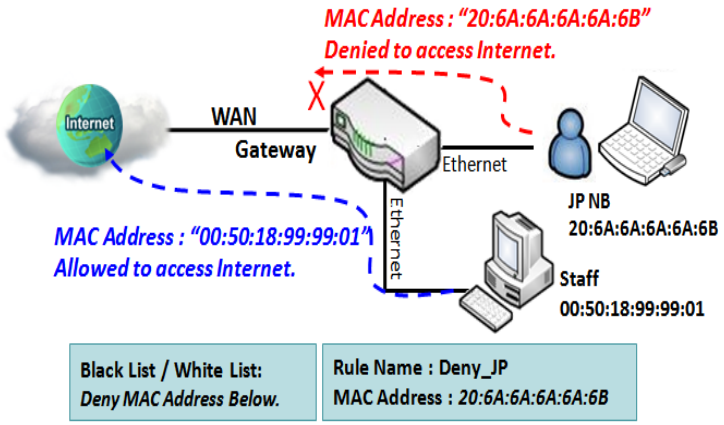
URL Blocking Rules Configuration

Item	Value setting	Description
Rule Name	1. String format can be any text 2. A must-filled setting	Specify a name for the URL Blocking rule name.
Source IP	1. A must-filled setting 2. **Any** is set by default	Specify the Source IP address. Select **Any** to filter packets with any source IP addresses. Select **Specific IP Address** to filter packets with the specified source IP address. Select **IP Range** to filter packets with the specified range of IP address. • Select **IP Address-based Group** to filter packets with the source IP address defined in the pre-defined group. **Note:** Groups must be configured first (go to **Object Definition > Grouping > Host grouping**)**.** Click **Add Rule** to create a new group.
Source MAC	1. A must-filled setting 2. **Any** is set by default	Specify the Source MAC address. Select **Any** to filter packets coming from any MAC addresses. Select Specific MAC Address to filter packets coming from the specified MAC address. • Select MAC Address-based Group to filter packets coming from the pre-defined group. **Note:** Groups must be configured first (go to **Object Definition > Grouping > Host grouping**). Click **Add Rule** to create a new group.
URL / Domain Name / Keyword	1. A must-filled setting 2. Supports up to a maximum of 10 Keywords in a rule by using the delimiter ";".	Specify URL, Domain Name, or Keyword list for URL checking. • In the **Black List** mode, when matched, the packets will be dropped. • In the **White List** mode, when matched, the packets will be accepted and other packets that don't match any rule will be dropped.
Destination Port	1. A must-filled setting 2. **Any** is set by default	This field is to specify the **Destination Port number**. • Select **Any** to filter packets going to any Port. • Select **Specific Service Port** to filter packets going to a specific Port. • Select **Port Range** to filter packets going to a specific range of Ports.
Time Schedule Rule	A must-filled setting	Apply Time Schedule for the rule to be in effect. Configure a schedule in advance to allow selection in Time Schedule. Refer to **Object Definition > Scheduling > Configuration.**
Rule	The box is unchecked by default.	Activate this rule.
Save	*NA*	Save the settings.
Undo	*NA*	Cancel the changes and go back to the previous page.

5.2.3 MAC Control



The "MAC Control" function allows you to control the access to the gateway for different users according to device's MAC address.



MAC Control with Black List Scenario

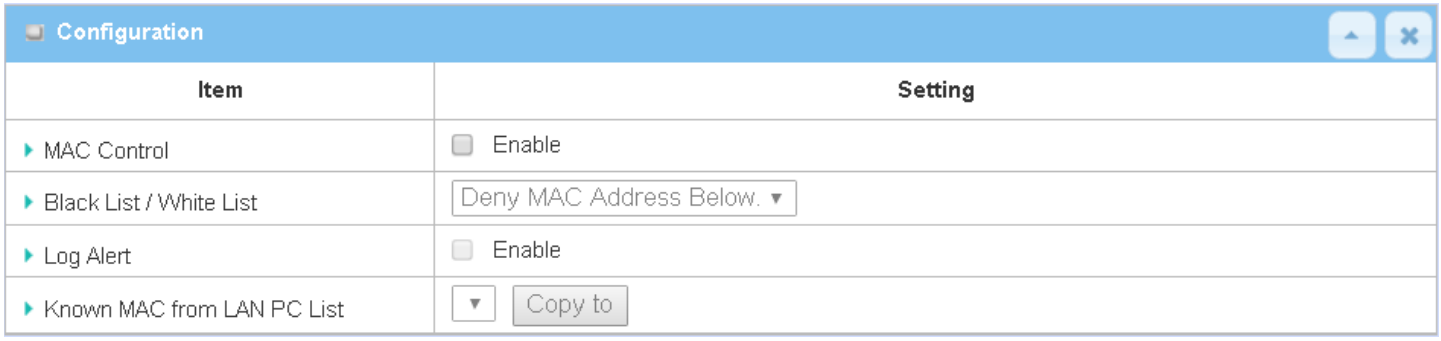
As shown in the diagram, enable the MAC control function and define a blocked "MAC Control Rule List". You also need to configure MAC control rules to deny the connection request from the "JP NB" with its MAC address 20:6A:6A:6A:6A:6B.
The gateway will block access from the "JP NB" but allow others.

MAC Control Setting

The MAC control setting allows you to create MAC address policies to allow or reject packets with specific source MAC addresses.

Go to **Security > Firewall > MAC Control** to access the MAC Control Setting page.

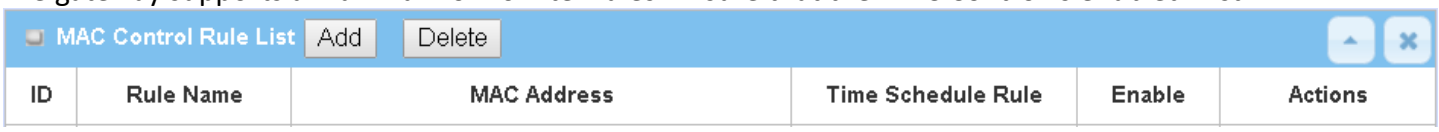
Enable MAC Control



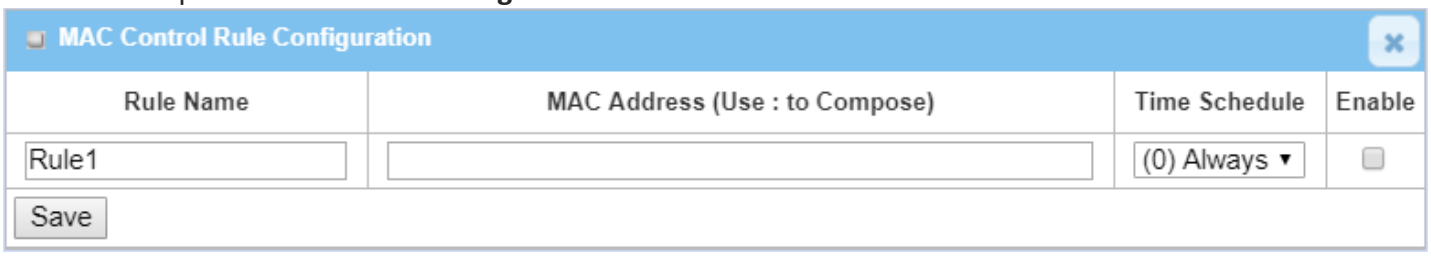
Configuration Window		
Item	**Value setting**	**Description**
MAC Control	The box is unchecked by default	Activate the MAC filter function
Black List / White List	Deny MAC Address Below is set by default	When ***Deny MAC Address Below*** is selected, packets matching the rules will be blocked. In contrast, the ***Allow MAC Address Below*** allow packets matching the rules to pass the gateway while blocking all other traffic.
Log Alert	The box is unchecked by default	Activate alert logging. Go to **Status > Security > Firewall** to view the logged alerts.
Known MAC from LAN PC List	N/A	Select a MAC Address from the LAN Client List and click **Copy to** to copy the selected **MAC Address** to the filter rule.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

Create/Edit MAC Control Rules

The gateway supports a maximum of 20 filter rules. Ensure that the MAC Control is enabled first.



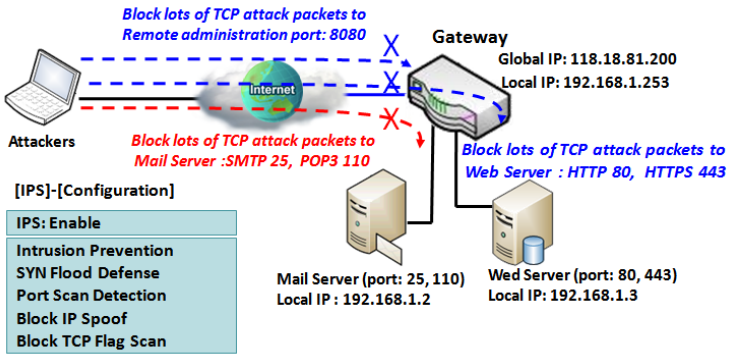
Click **Add** to open the **Filter Rule Configuration** screen.



MAC Control Rule Configuration		
Item	**Value setting**	**Description**
Rule Name	1. String format can be any text 2. A must-filled setting	Enter a name for the MAC Control rule.
MAC Address (Use: to Compose)	1. MAC Address string Format 2. A must-filled setting	Specify the **Source MAC Address** to filter rule using Colon-Hexadecimal notation, e.g. 00:1B:44:11:3A:B7.
Time Schedule	A must-filled setting	Apply **Time Schedule** for the rule to be in effect. Configure a schedule in advance to allow selection in **Time Schedule**. Refer to **Object Definition** > **Scheduling > Configuration**.
Enable	The box is unchecked by default.	Activate this rule.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

5.2.6 IPS

Intrusion Prevention System (IPS) is a network security application that monitors network as well as system activities for malicious events. The IPS function not only identifies malicious activities but also stops the attempts. You can also enable the alert logging function so that the system will record intrusion events.



IPS Scenario

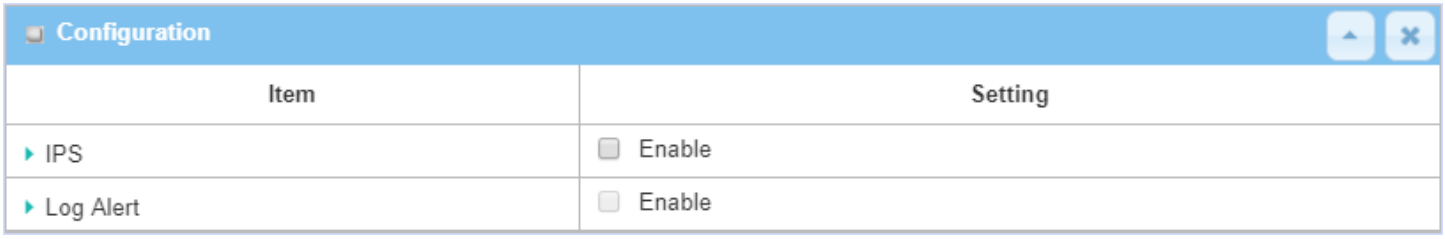
As shown in the diagram, the gateway provides email service and web service as well as remote administration through port 8080. So remote users or unknown users can request those services from the Internet. With IPS enabled, the gateway can detect incoming attack packets targeting all TCP ports, including the above-mentioned service ports 25, 80, 110, 443 and 8080. It will block malicious packets while allowing legitimate traffic to pass through the gateway.

IPS Setting

Go to **Security > Firewall > IPS** to access IPS Setting page.

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

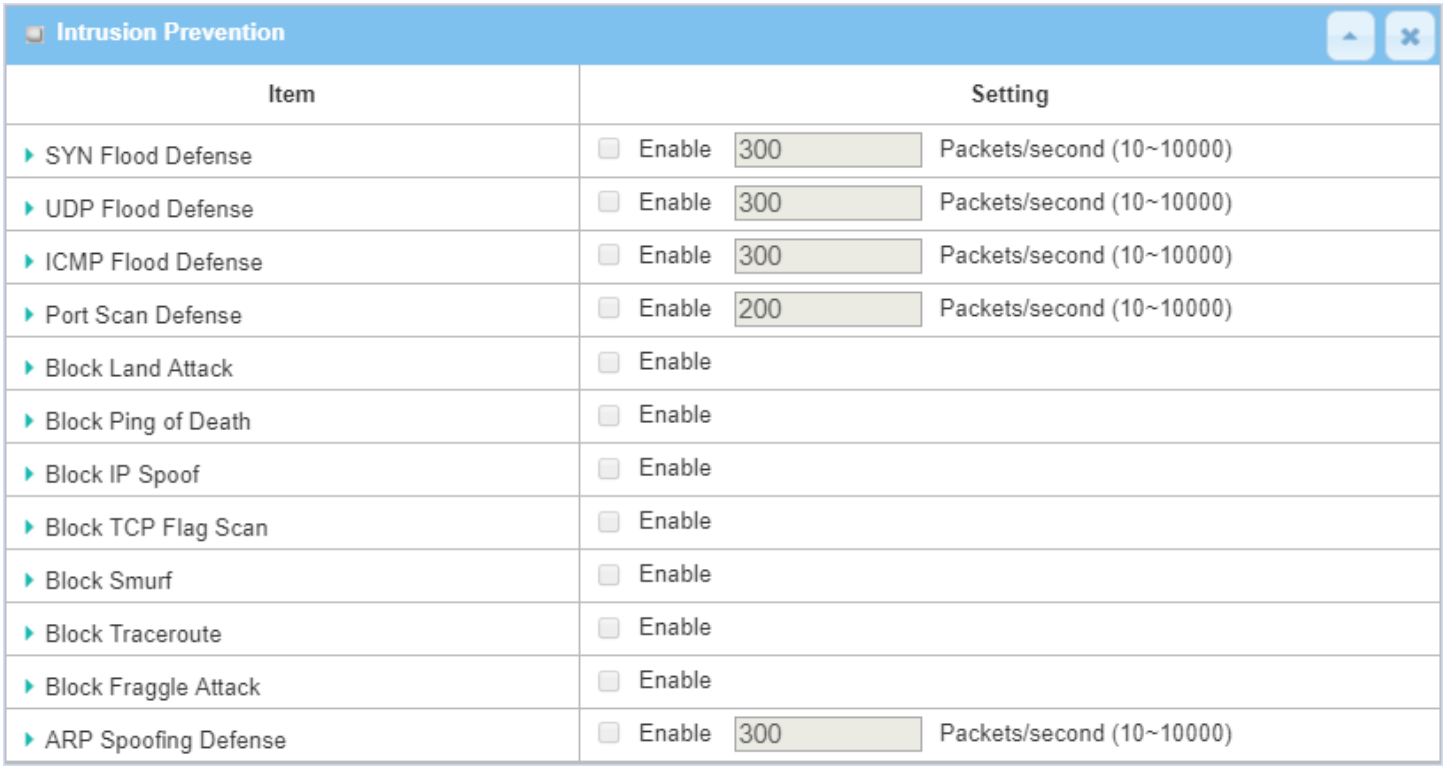
Enable IPS Firewall



Configuration Window		
Item	**Value setting**	**Description**
IPS	The box is unchecked by default	Activate IPS function
Log Alert	The box is unchecked by default	Activate alert logging. Go to **Status > Security > Firewall** to view the logged alerts.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

Configure Intrusion Prevention Rules

The gateway allows you to enable specific intrusion prevention functions. Ensure that IPS is enabled first.

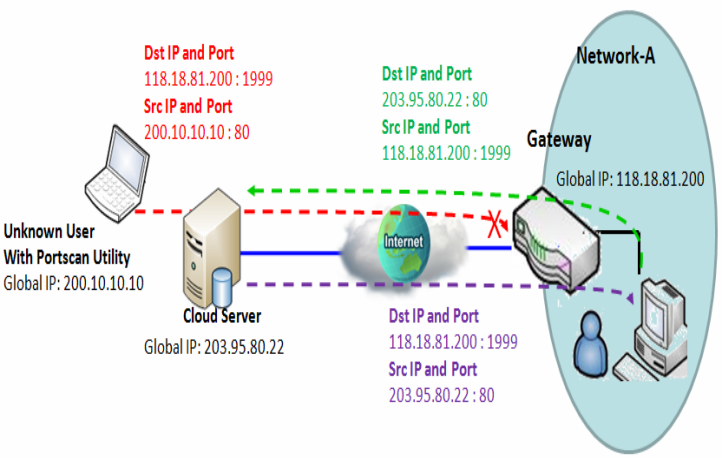


Setup Intrusion Prevention Rules		
Item Name	**Value setting**	**Description**
SYN Flood Defense **UDP Flood Defense** **ICMP Flood Defense**	1. A must-filled setting 2. The box is unchecked by default. 3. Traffic threshold is set to 300 by default 4. The value range can be from 10 to 10000.	Activate SYN Flood Defense and enter the traffic threshold in this field. If the number of inbound SYN packets exceeds the threshold, system will identify the traffic as a SYN flood. Activate UDP Flood Defense and enter the traffic threshold Activate ICMP Flood Defense and enter the traffic threshold. *Value Range*: 10 ~ 10000.
Port Scan Defense	1. A must-filled setting 2. The box is unchecked by default. 3. Traffic threshold is set to 200 by default 4. The value range can be from 10 to 10000.	Activate the Port Scan Defense and enter the traffic threshold. *Value Range*: 10 ~ 10000.
Block Land Attack **Block Ping of Death** **Block IP Spoof** **Block TCP Flag Scan** **Block Smurf** **Block Traceroute** **Block Fraggle Attack**	The box is unchecked by default.	Activate a specific defense function: The LAND attack crashes the targeted machine by sending a TCP SYN spoofed packet with identical IP/ports of the source and destination. The Ping of Death attack aims to disrupt a targeted network device by sending abnormally large packets. The IP Spoof floods the network with spoofed IP address. The Smurf attack overwhelms a targeted machine with ICMP reply packets. The Fraggle attack overwhelms a targeted machine with UDP packets.

ARP Spoofing Defence	1. A must-filled setting 2. The box is unchecked by default. 3. Traffic threshold is set to 300 by default 4. The value range can be from 10 to 10000.	An ARP spoofing is a type of man-in-the-middle attack which allows an attacker to alter ARP packets. Activate this defense and enter the traffic threshold. *Value Range*: 10 ~ 10000.
Save	NA	Save the settings.
Undo	NA	Discard the settings.

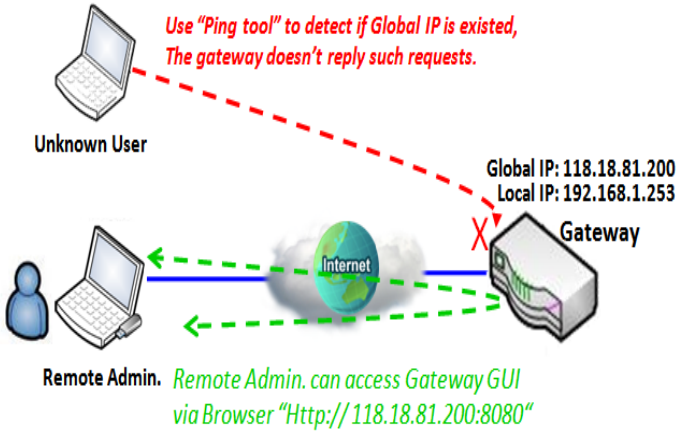
5.2.7 Options

There are some additional useful firewall options offered on the gateway.
“Stealth Mode” allows the gateway not to respond to port scans from the WAN to make it less susceptible to discovery and attacks from the Internet. Stateful packet inspection is a dynamic approach to protecting against attacks, which exams the content of the inbound packets and tracks connection state. “Discard Ping from WAN” disregards ICMP packets from the WAN. And finally, “Remote Administrator Hosts” enables you to perform administrative tasks from remote hosts with specified IP address(es).



Enable SPI Scenario

As shown in the diagram, the gateway has been configured with a WAN IP address of 118.18.81.200 and a LAN IP address of 192.168.1.253. An unknown user sends a forged packet to the cloud server through the gateway. The SPI frewall of the gateway will block such malicious packets.



Discard Ping from WAN & Remote Administrator Hosts Scenario

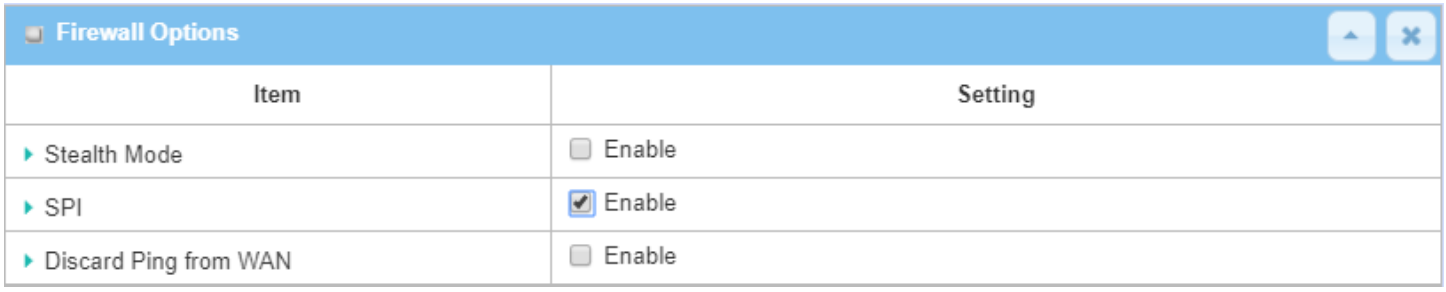
When the “Discard Ping from WAN” option is enabled, the gateway will not reply any ICMP packets from the WAN. With the “Remote Administrator Hosts” enabled, you will be able to log in to the gateway remotely.

Firewall Options Setting

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

The firewall options setting allows you to modify the behavior of the firewall and to enable Remote Gateway Access Control.

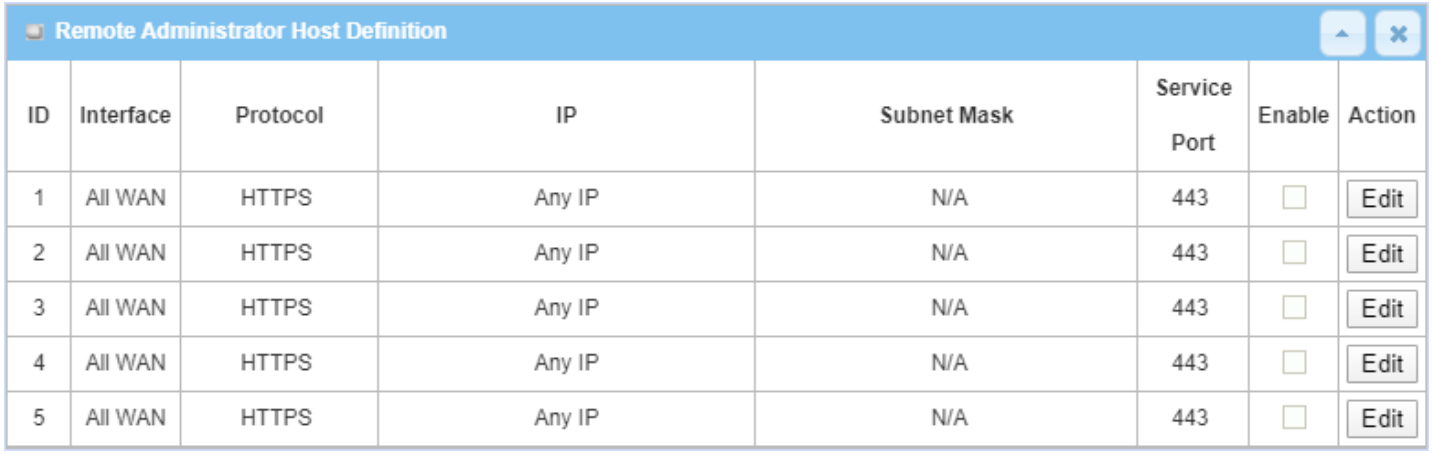
Enable Firewall Options



Firewall Options		
Item	**Value setting**	**Description**
Stealth Mode	The box is unchecked by default	Activate the Stealth Mode function
SPI	The box is checked by default	Activate the SPI function
Discard Ping from WAN	The box is unchecked by default	Activate the Discard Ping from WAN function

Define Remote Administrator Host

The gateway allows you to manage gateway remotely. The gateway can be assigned with a specific IP address and service port to facilitate remote management.

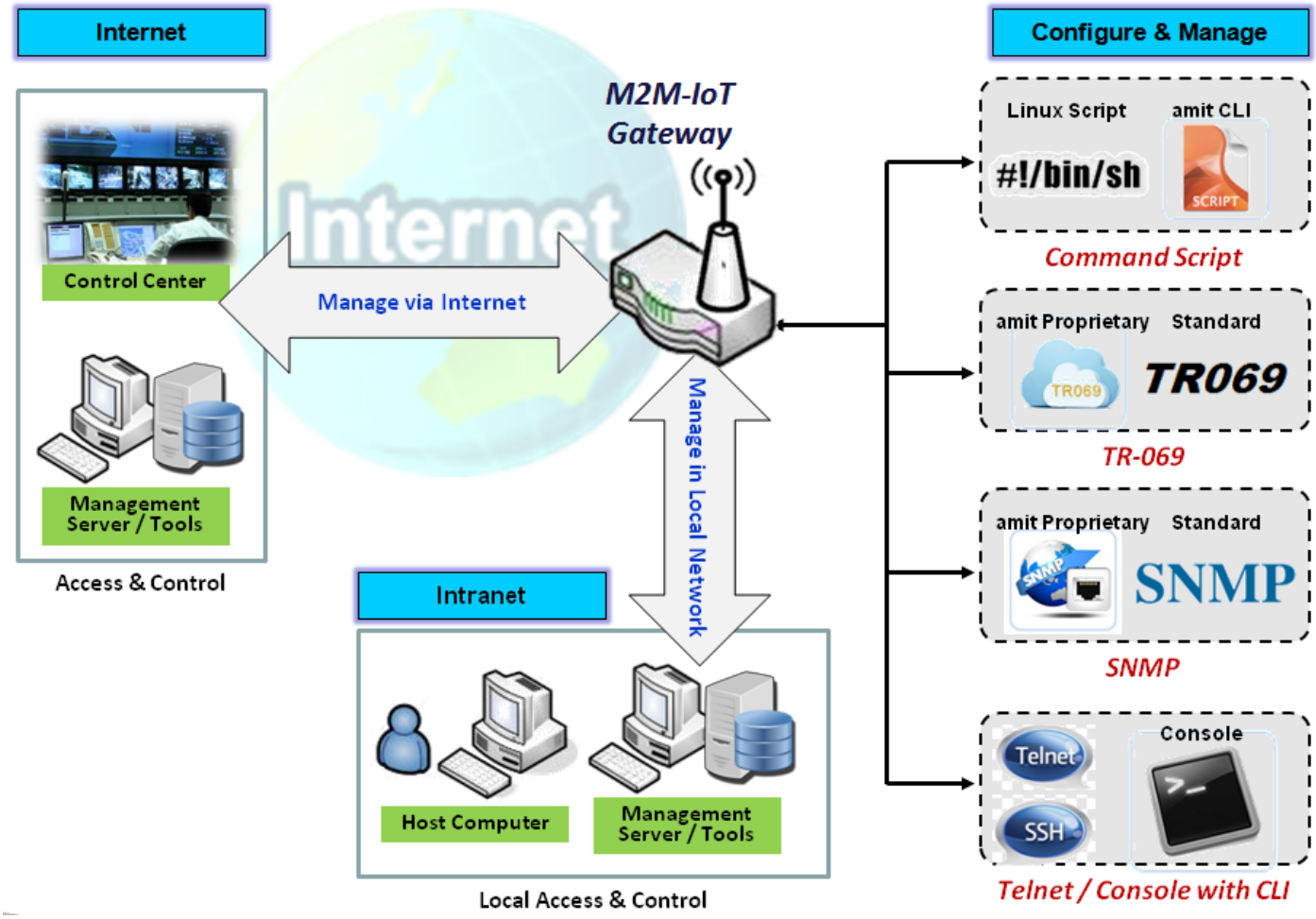


Remote Administrator Host Definition		
Item	**Value setting**	**Description**

Protocol	**HTTPS** is set by default	Select **HTTP** or **HTTPS** method for remote administration.
IP	A must-filled setting	Specify the remote host to assign access right for remote access. Select **Any IP** to allow any remote hosts. Select **Specific IP** to allow remote hosts in a specific subnet: enter an IP address with a **Subnet Mask**.
Service Port	1. 80 for HTTP by default 2. 443 for HTTPS by default	This field is to specify a Service Port to HTTP or HTTPS connection. *Value Range*: 1 ~ 65535.
Enabling the rule	The box is unchecked by default.	Activate this rule.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

Chapter 6 Administration

6.1 Configure & Manage



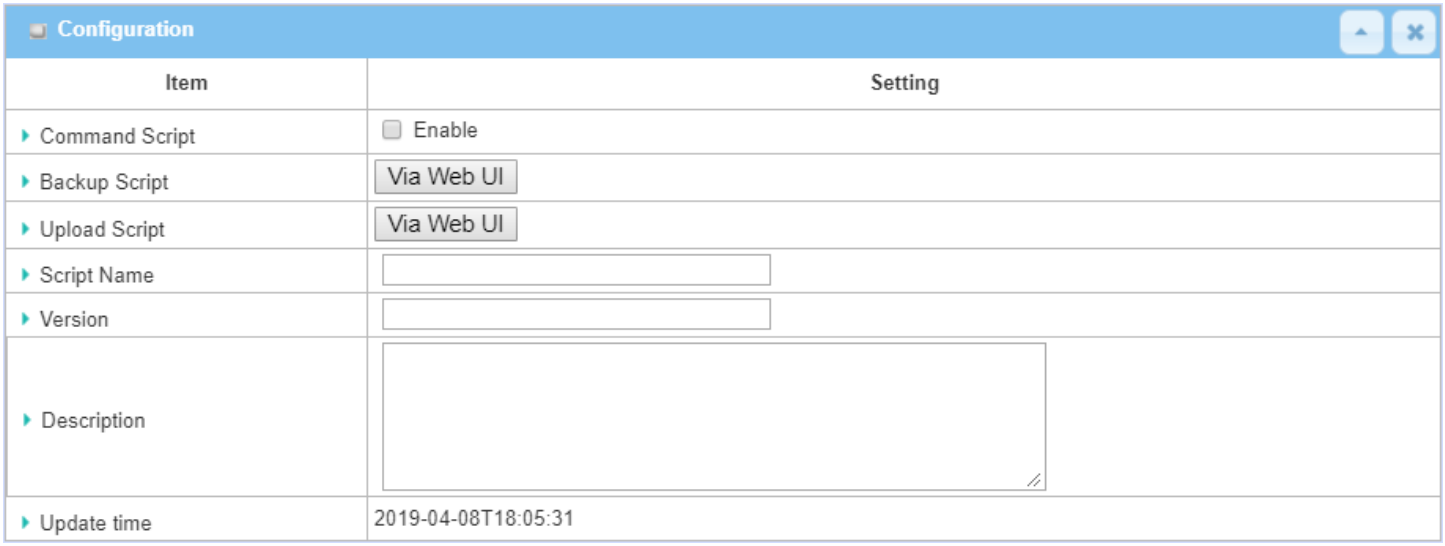
Configure & Manage provides enterprise-wide administration of distributed systems across geographical areas. It allows you to monitor the network and devices and troubleshoot in time. This device supports many system management protocols, such as Command Script, TR-069, SNMP, and Telnet with CLI.

6.1.1 Command Script

Command script allows you to set up pre-defined configuration in plain text and apply the configuration on system startup.

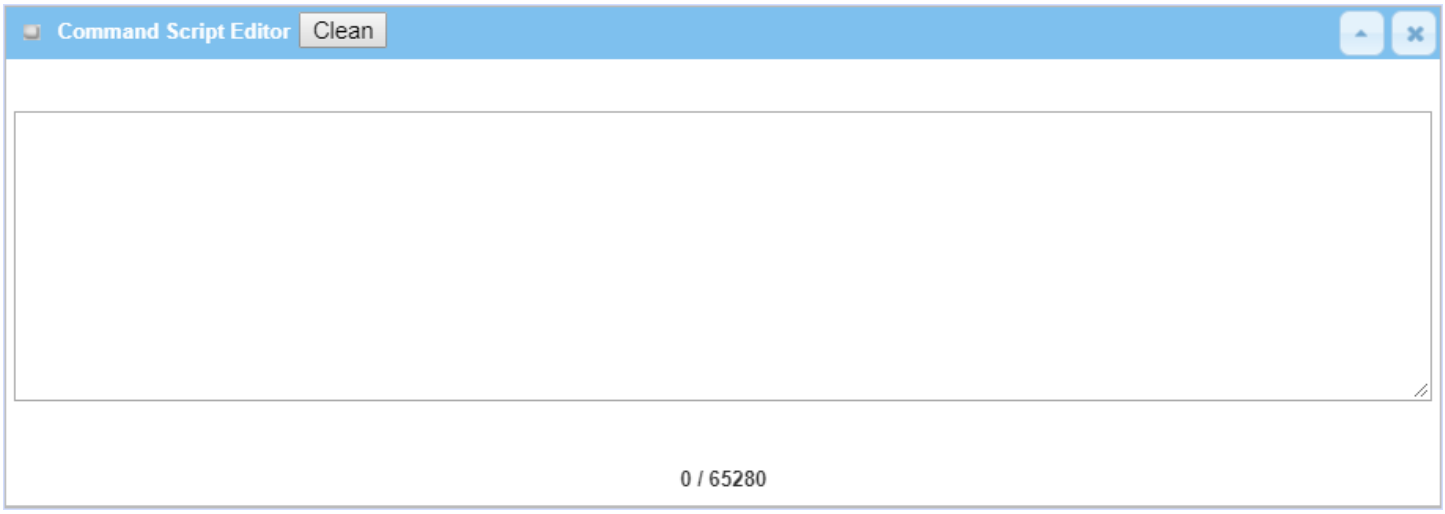
Go to **Administration > Configure & Manage > Command Script > Configuration** to access the Command Script page.

Enable Command Script Configuration



Configuration		
Item	**Value setting**	**Description**
Command Script	The box is unchecked by default	Activate the Command Script function.
Backup Script	N/A	Click the Via Web UI button to save the existing command script in a .txt file. You can specify the script file name in Script Name below.
Upload Script	N/A	Click the Via Web UI button to upload command script from a .txt file.
Script Name	1.An optional setting **2.Any valid file name**	Specify a script file name for script backup or display the selected script file name to be uploaded. *Value Range*: 0 ~ 32 characters.
Version	1.An optional setting 2.Any string	Specify the version number for the applied Command script. *Value Range*: 0 ~ 32 characters.
Description	1.An optional setting 2.Any string	Enter a short description for the applied Command script.
Update time	N/A	It records the upload time for the previous commad script upload.

Edit/Back up Plain Text Command Script



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

Plain Text Configuration		
Item	**Value setting**	**Description**
Clean	*NA*	Clean text area.
Backup	*NA*	Back up and download the configuration.
Save	*NA*	Save the configuration

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

Configuration Content		
Key	**Value setting**	**Description**
OPENVPN_ENABLED	1 : enable 0 : disable	Enable or disable OpenVPN client function.
OPENVPN_DESCRIPTION	A must-filled Setting	Specify the tunnel name for the OpenVPN client connection.
OPENVPN_PROTO	udp tcp	Define the **Protocol** for the OpenVPN Client. • Select **TCP** or **TCP /UDP** The OpenVPN will use TCP protocol, and **Port** will be set as 443 automatically. • Select **UDP** The OpenVPN will use UDP protocol, and **Port** will be set as 1194 automatically.
OPENVPN_PORT	A must-filled Setting	Specify the **Port** for the OpenVPN connection.
OPENVPN_REMOTE_IPADDR	IP or FQDN	Specify the **Remote IP/FQDN** of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the IP address or FQDN.
OPENVPN_PING_INTVL	seconds	Specify the time interval for OpenVPN keep-alive mechanism.
OPENVPN_PING_TOUT	seconds	Specify the timeout value for OpenVPN Client keep-alive mechanism.
OPENVPN_COMP	Adaptive	Specify the **LZO Compression** algorithm for OpenVPN client.
OPENVPN_AUTH	Static Key/TLS	Specify the authorization mode for the OpenVPN tunnel.

		• **TLS** The OpenVPN will use TLS authorization mode. You need also specify these items: **CA Cert.**, **Client Cert.** and **Client Key**.
OPENVPN_CA_CERT	A must-filled Setting	Specify the Trusted CA certificate for the OpenVPN client. Base64 Conversion will be applied automatically.
OPENVPN_LOCAL_CERT	A must-filled Setting	Specify the local certificate for OpenVPN client. Base64 Conversion will be applied automatically.
OPENVPN_LOCAL_KEY	A must-filled Setting	Specify the local key for the OpenVPN client. Base64 Conversion will be applied automatically.
OPENVPN_EXTRA_OPTS	Options	Specify the extra options setting for the OpenVPN client.
IP_ADDR1	Ip	Ethernet LAN IP.
IP_NETM1	Net mask	Ethernet LAN subnet mask.
PPP_MONITORING	1 : enable 0 : disable	When the Network Monitoring feature is enabled, the gateway will use DNS Query or ICMP to periodically check Internet connection – connected or disconnected.
PPP_PING	0 : DNS Query 1 : ICMP Query	With **DNS Query,** the system checks the connection by sending DNS Query packets to the destination specified in PPP_PING_IPADDR. With **ICMP Query,** the system will check connection by sending ICMP request packets to the destination specified in PPP_PING_IPADDR.
PPP_PING_IPADDR	IP	Specify an IP address to which DNS query/ICMP requests will be sent.
PPP_PING_INTVL	seconds	Specify the time interval that should elapse between two DNS Query or ICMP checking packets.
STARTUP	Script file	For the settings 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 system also allows configuration via Telnet CLI. You can use the proprietary telnet command “***txtConfig***” and related action items to perform the plain system configuration.

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

Action	Option	Description
clone	*Output file*	Duplicate the configuration content from database and store it as a configuration file. (ex: *txtConfig clone /tmp/config*) The content in the configuration file is the same as the plain text commands mentioned above.
commit	a existing file	Commit the configuration content to the database. (ex: *txtConfig commit /tmp/config*)
enable	*NA*	Enable plain-text system configuration. (ex: *txtConfig enable*)
disable	*NA*	Disable plain-text system configuration. (ex: *txtConfig disable*)
run_immediately	*NA*	Apply the configuration content that has been committed in database. (ex: *txtConfig run_immediately*)

run_immediately	a existing file	Assign a configuration file to apply. (ex: *txtConfig run_immediately /tmp/config*)

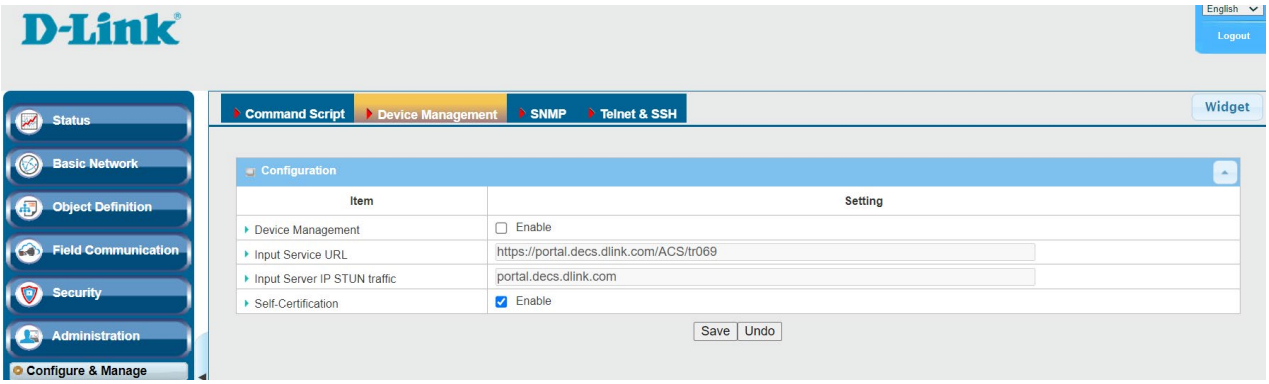
6.1.2 D-ECS (D-LINK EDGE CLOUD SOLUTION)

D-ECS is a cloud management platform that allows you to manage 4G/5G devices, including DOM-550-GSO anytime, anywhere. In order for the D-ECS system to communicate with individual devices, device registration must be done with device configuration on each device.

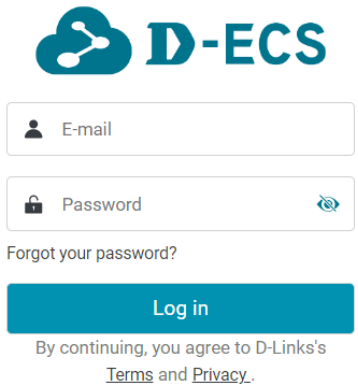
To Enable Remote D-ECS Service:

1. Register the device to D-ECS by configuring the relevant settings in the device management page (go to **Configure & Manage > Device Management**) as shown below:

Item	Setting
Device Management	Select Enable to allow management by D-ECS
Input Local Service URL	Input the management service URL: https://portal.decs.dlink.com/ACS/tr069
Input Local Server IP STUN Traffic	Input the server address for processing STUN traffic: portal.decs.dlink.com
Note: The service URL and Server IP STUN Traffic should be modified accordingly depending on the deployment architecture of the D-ECS system.	



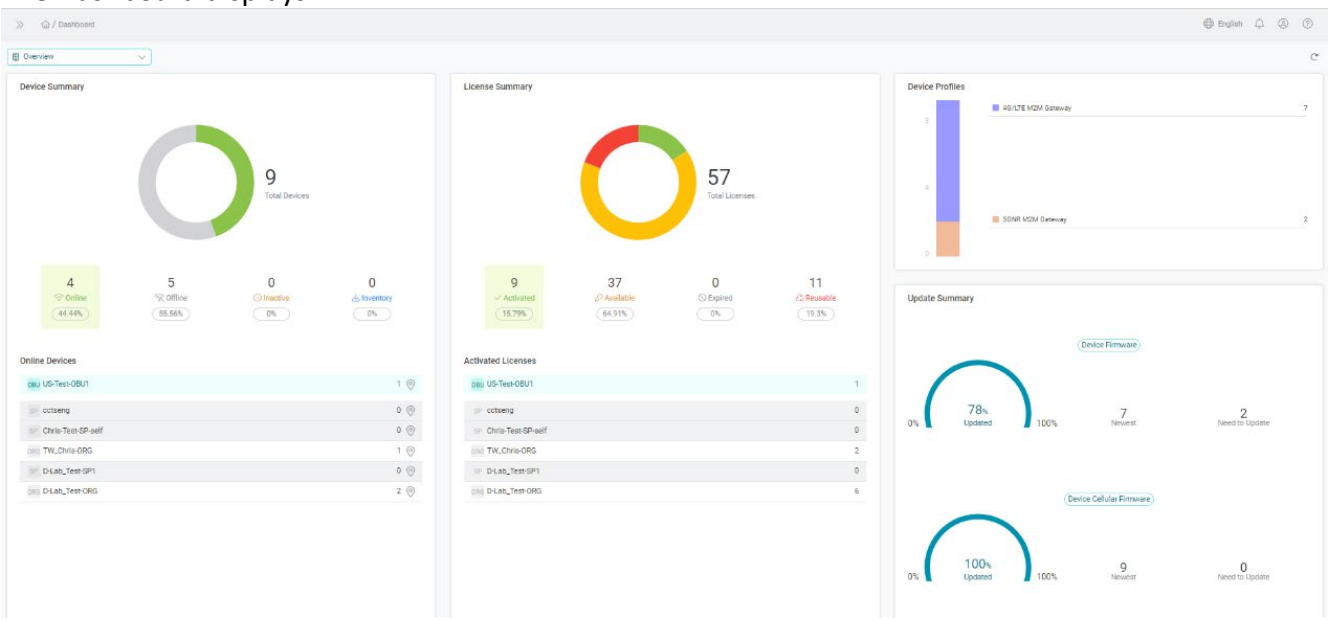
2. Log in to the D-ECS Management Interface by typing the URL in your browser's address field: https://portal.decs.dlink.com/login.



Note that the URL varies depending on the deployment architecture of the D-ECS system (i.e. on-premises or cloud version).

3. Log in using your ID and password.

4. The Dashboard displays.



6.1.3 SNMP

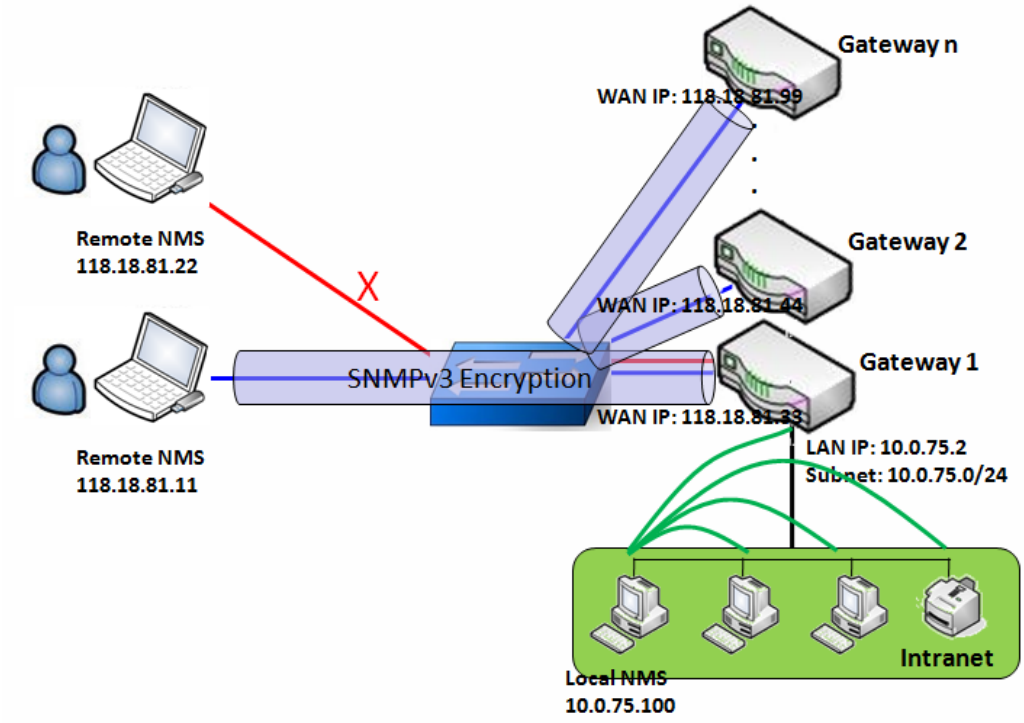
In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to enable users to remotely manage a computer network by polling and setting system values and monitoring network events.

In typical SNMP uses, one or more administrative computers, called managers, monitor and manage a group of hosts or devices on a computer network. Each managed system executes a software component called agent, which reports information to the manager.

SNMP agents display management data on the managed systems as variables. The variables accessible via SNMP are organized in hierarchies. These variables along with their 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 follows: **MIB-II (RFC 1213, Include IPv6), IF-MIB, IP-MIB, TCP-MIB, UDP-MIB, SMIv1 and SMIv2, SNMPv2-TM and SNMPv2-MIB, and AMIB (a proprietary MIB).**

SNMP Management Scenario



Application Scenarios

There are two application scenarios of SNMP Network Management Systems (NMS): local and remote. Local NMS is in the Intranet and manages all devices supporting SNMP protocol. Remote NMS manages devices through the WAN using UDP forwarding. The NMS server can monitor and configure the managed devices through SNMP protocol. The managed devices also report configured alert events through SNMP traps to the NMS servers.

Parameter Setup Example

The following tables list the parameter configuration for gateway 1 with "SNMP" enabled at LAN and WAN interfaces as shown in the above diagram. "gateway 1" is one of the managed devices configured with a LAN IP address of 10.0.75.2 and a WAN IP address of 118.18.81.33 for the WAN-1 interface. It serves as an NAT gateway.

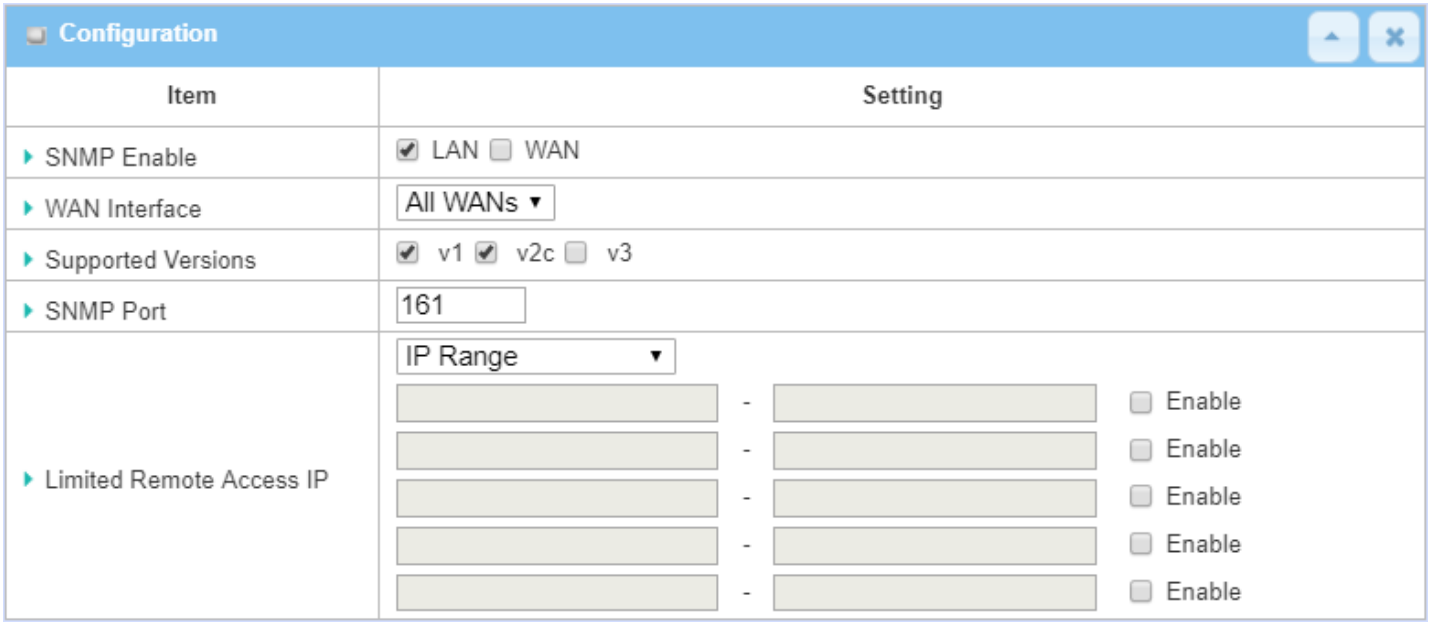
Configuration Path	[SNMP]-[Configuration]
SNMP Enable	■ ***LAN*** ■ ***WAN***
Supported Versions	■ ***v1*** ■ ***v2c*** ■ ***v3***
Get / Set Community	***ReadCommunity / WriteCommunity***
Trap Event Receiver 1	***118.18.81.11***
WAN Access IP Address	***118.18.81.11***

Configuration Path	[SNMP]-[User Privacy Definition]		
ID	1	2	3
Username	***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***

SNMP Setting

Go to **Administration > Configure & Manage > SNMP** to access SNMP Setting page.
The SNMP allows you to configure SNMP related settings, including interface, version, access control, and trap receiver.

Enable SNMP



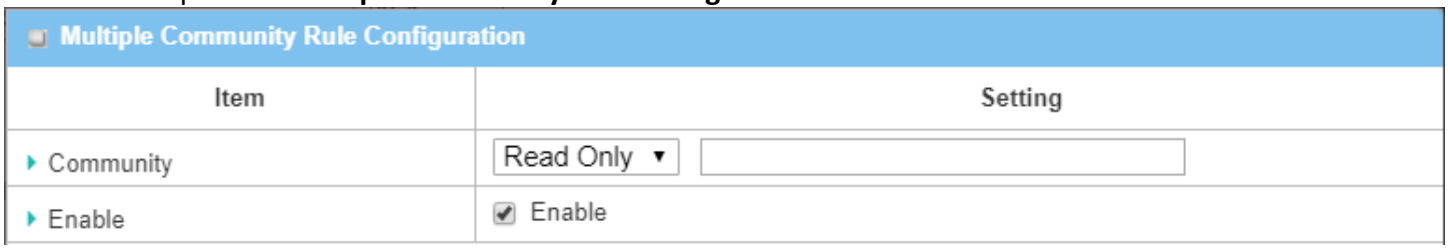
SNMP Item	Value setting	Description
SNMP Enable	1.The boxes are unchecked by default	Select the interface to enable SNMP: **LAN** or **WAN**.
WAN Interface	1.A must-filled setting **2. ALL WANs are selected by default**	Specify the WAN interface that a remote SNMP host can access through the device. By default, **All WANs** interfaces are selected.
Supported Versions	1.A must-filled setting 2.The boxes are unchecked by default	Select the version for the SNMP: **v1, v2c,** or **v3**.
SNMP Port	1. String format: any port number 2. The default SNMP port is **161**. 3. A must-filled setting	Specify the **SNMP Port**. *Value Range*: 1 ~ 65535.
Limited Remote Aceess IP	1. String format: any IPv4 address 2. It is an optional item.	Specify the **Remote Access IP** for WAN and check the box to enable it. Select **Specific IP Address** or **IP Range** and enter a single IP address or a range of IP addresses to permit management using SNMP through the WAN.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

Create/Edit Multiple Community

Customize the SNMP access control for version 1 and version 2 users. The gateway supports up to 10 communities.



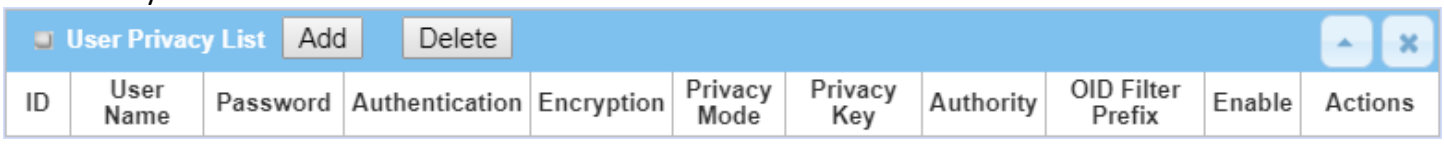
Click **Add** to open the **Multiple Community Rule Configuration** screen.



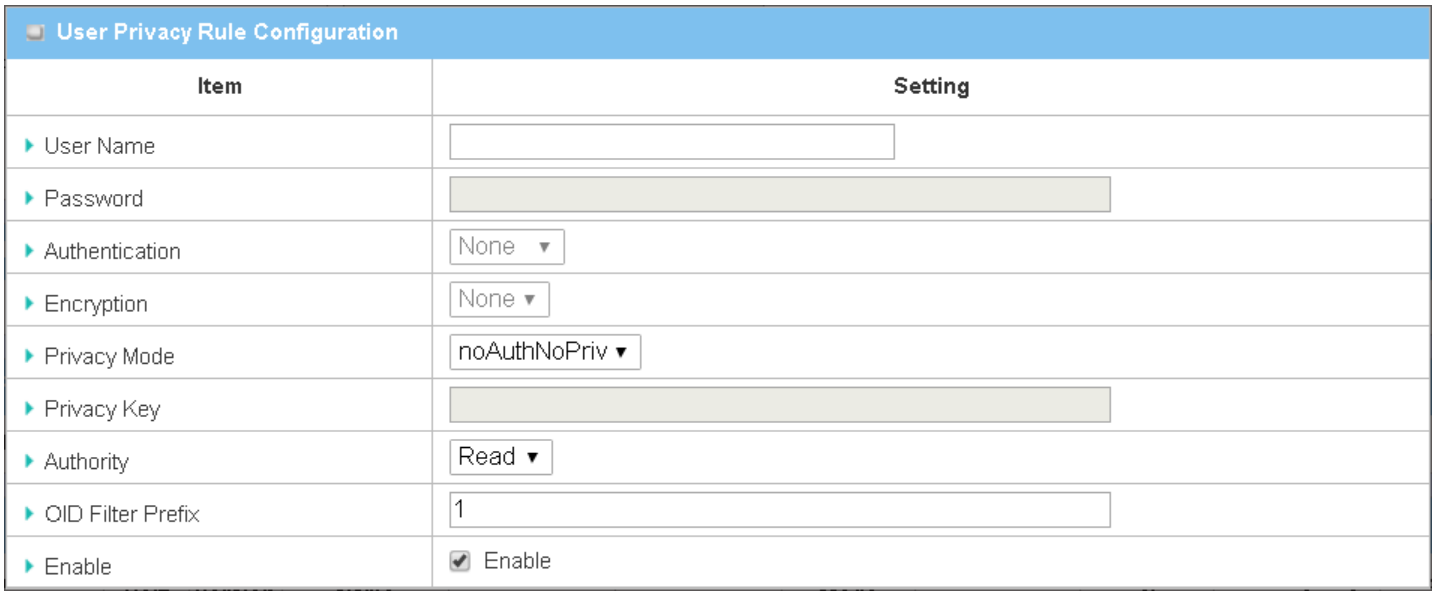
Multiple Community Rule Configuration		
Item	**Value setting**	**Description**
Community	1. **Read Only** is selected by default 2. A must-filled setting 3. String format: any text	Specify the privilege for the community: **Read Only** (GET and GETNEXT commands) or **Read-Write** (GET, GETNEXT and SET commands) access respectively. The maximum length for the community string is 32 characters.
Enable	1.The box is checked by default	Enable version 1 or version v2c user.
Save	N/A	Save the configuration.
Undo	N/A	Cancel the settings.
Back	N/A	Return to the previous page.

Create/Edit User Privacy

Customize the SNMP access control for version 1 and version 2 users. The gateway supports a maximum of 128 User Privacy rules.



Click **Add** to open the **User Privacy Rule Configuration** screen.



User Privacy Rule Configuration		
Item	**Value setting**	**Description**
Username	1. A must-filled setting 2. String format: any text	Specify the **Username** for this version 3 user. *Value Range*: 1 ~ 32 characters.
Password	1. String format: any text	For **Privacy mode** of **authNoPriv** or **authPriv**, specify the **Password** for this version 3 user. *Value Range*: 8 ~ 64 characters.
Authentication	1. **None** is selected by default	For Privacy Mode of authNoPriv or authPriv, specify the Authentication type: MD5/ SHA-1 to use.
Encryption	1. **None** is selected by default	For **Privacy Mode** of **authPriv**, specify the **Encryption** protocol: DES or AES.
Privacy Mode	1. **noAuthNoPriv** is selected by default	Specify the **Privacy Mode** for this version 3 user. Select **noAuthNoPriv**, if you do not use any authentication types and encryption protocols. For authNoPriv, specify the Authentication and Password. For authPriv, specify the Authentication, Password, Encryption and Privacy Key.
Privacy Key	1. String format: any text	If you select **authPriv** for **Privacy Mode**, you must specify the **Privacy Key** (8 ~ 64 characters) for this user.
Authority	1. **Read** is selected by default	Select the privilege: **Read Only** (GET and GETNEXT) or **Read-Write** (GET, GETNEXT and SET) access.
OID Filter Prefix	1. The default value is 1 2. A must-filled setting 3. String format: any legal OID	The **OID Filter Prefix** restricts access to the sub-tree rooted at the given OID. *Value Range*: 1 ~2080768.
Enable	1.The box is checked by default	Enable this version 3 user.

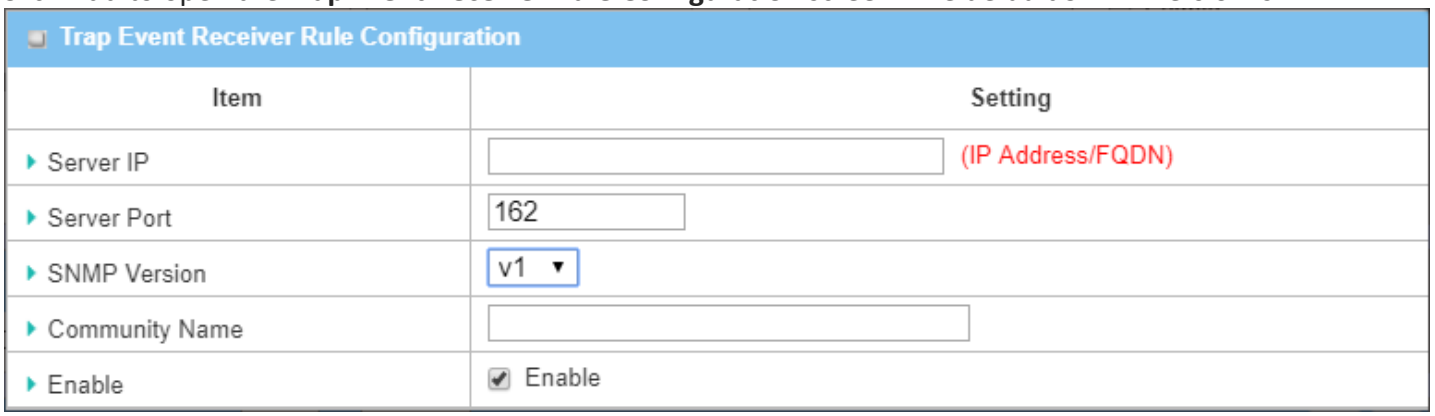
Save	N/A	Save the configuration.
Undo	N/A	Cancel the settings
Back	N/A	Return to the previous page.

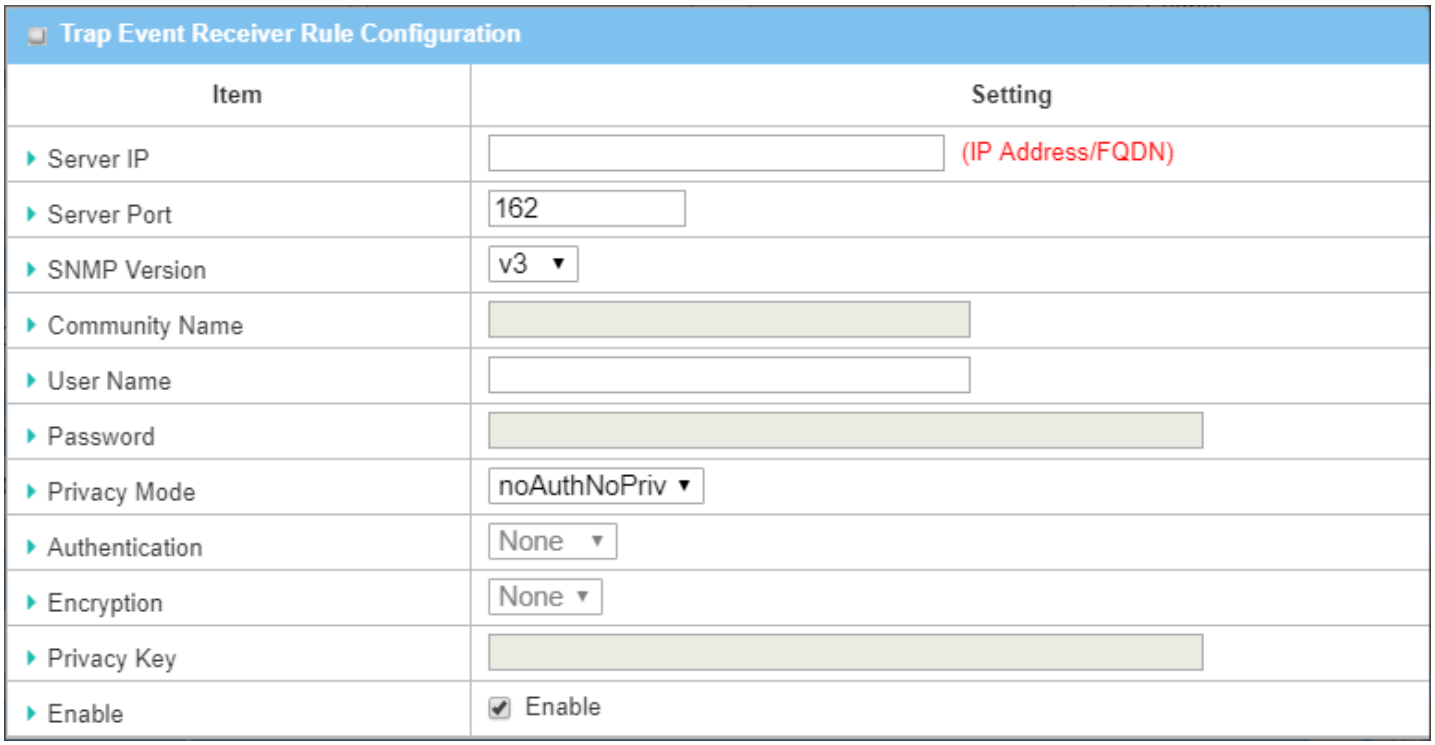
Create/Edit Trap Event Receiver

The SNMP allows you to add your trap event receiver. The gateway supports up to a maximum of 4 Trap Event Receivers.



Click **Add** to open the **Trap Event Receiver Rule Configuration** screen. The default SNMP Version is v1.





Trap Event Receiver Rule Configuration

Item	Value setting	Description
Server IP	1. A must-filled setting 2. String format: any IPv4 address or FQDN	Specify the trap **Server IP** or **FQDN**. The DUT will send traps to the server IP/FQDN.
Server Port	1. String format: any port number 2. The default SNMP trap port is 162 3. A must-filled setting	Specify the trap **Server Port**. Make sure that this port is not assigned for other functions. *Value Range*: 1 ~ 65535.
SNMP Version	1. **v1** is selected by default	Select the version for the trap: **v1, v2c,** or **v3.**
Community Name	1. A **v1** and **v2c** Must filled setting 2. String format: any text	Specify the **Community Name** for version 1 or version v2c traps. *Value Range*: 1 ~ 32 characters.
Username	1. A **v3** Must filled setting 2. String format: any text	Specify the **Username** for version 3. *Value Range***:** 1 ~ 32 characters.
Password	1. A **v3** Must filled setting 2. String format: any text	For **Privacy mode** of **authNoPriv** or **authPriv**, specify the **Password** for version 3. *Value Range*: 8 ~ 64 characters.
Privacy Mode	1. A **v3** Must filled setting 2. **noAuthNoPriv** is selected by default	For **Privacy Mode** of **authNoPriv** or **authPriv**, specify the Authentication type: MD5/ SHA-1 to use.
Authentication	1. A **v3** Must filled setting 2. **None** is selected by default	For **Privacy Mode** of **authPriv**, specify the **Encryption** protocol: DES or AES.
Encryption	1. A **v3** Must filled setting 2. **None** is selected by default	Specify the **Privacy Mode** for version 3. Select **noAuthNoPriv** if you do not use any authentication types and encryption protocols. For authNoPriv, specify the Authentication and Password. For authPriv, specify the Authentication, Password, Encryption and Privacy Key.
Privacy Key	1. A **v3** Must filled setting 2. String format: any text	If you select **authPriv** for **Privacy Mode**, you must specify the **Privacy Key** (8 ~ 64 characters) for this user.
Enable	1.The box is checked by default	Enable this trap receiver.
Save	N/A	Save the configuration.
Undo	N/A	Cancel the settings.
Back	N/A	Return to the previous page.

Specify SNMP MIB-II System

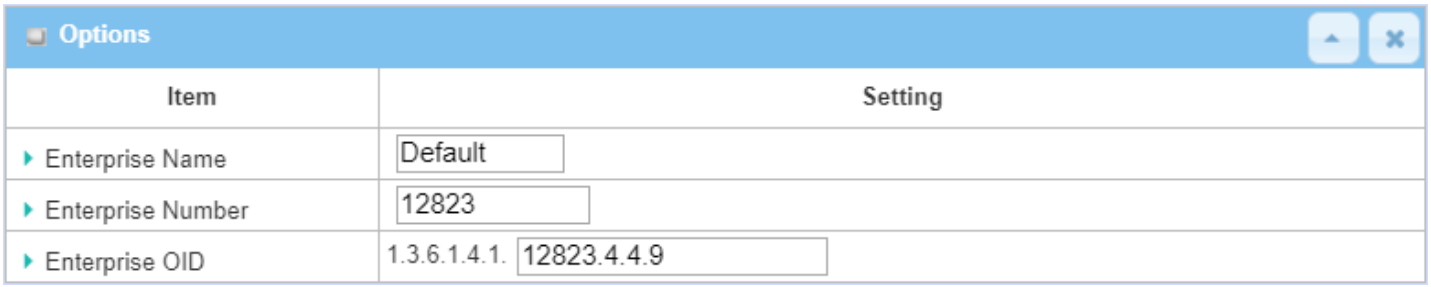
Specify the required information for the MIB-II System.



SNMP MIB-2 System Configuration		
Item	**Value setting**	**Description**
sysContact	1. An optional setting 2. String format: any text	Specify the contact information for MIB-II system. *Value Range*: 0 ~ 64 characters.
sysLocation	1. An optional setting 2. String format: any text	Specify the location information for MIB-II system. *Value Range*: 0 ~ 64 characters.

Edit SNMP Options

If the device uses private MIBs, enter the enterprise name, number, and OID.



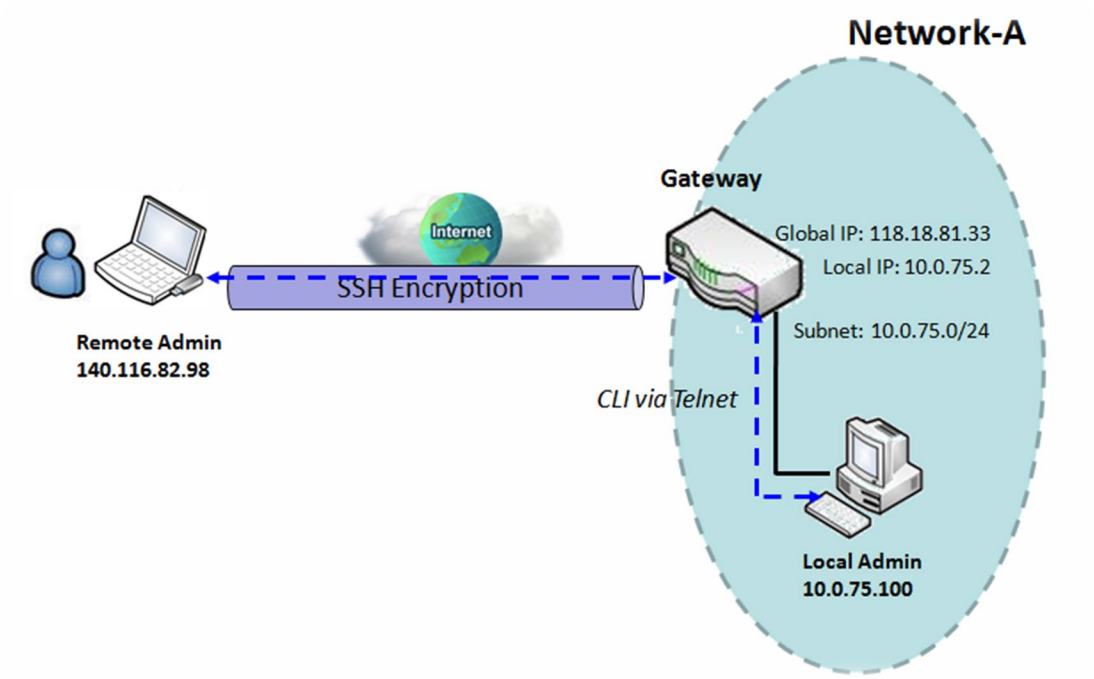
Options		
Item	**Value setting**	**Description**
Enterprise Name	1. The default value is **Default** 2. A must-filled setting 3. String format: any text	Specify the **Enterprise Name** for the private MIB. *Value Range*: 1 ~ 10 characters, and only string with A~Z, a~z, 0~9, '–', '_'.
Enterprise Number	The default value is **12823** (Default Enterprise Number) 2. A must-filled setting 3. String format: any number	Specify the **Enterprise Number** for the private MIB. *Value Range*: 1 ~2080768.
Enterprise OID	1. The default value is 1.3.6.1.4.1.**12823.4.4.9**	Specify the **Enterprise OID** for the private MIB. The range of the each OID number is 1 to 2080768.

	(Default Enterprise OID) 2. A must-filled setting 3. String format: any legal OID	The maximum length of the enterprise OID is 31. The seventh number must be identical with the enterprise number.
Save	N/A	Save the configuration and apply your changes.
Undo	N/A	Cancel the settings.

6.1.4 Telnet & SSH

A command-line interface (CLI), also known as command-line user interface and console user interface, is a method of interacting with a computer program where a 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 control and configure via scripting. The device supports both Telnet and SSH (Secure Shell) CLI with default service port 23 and 22, respectively.

Telnet & SSH Scenario



Application Scenario

If you want to manage the gateway from a remote site, you can enable "Telnet with CLI" and use a "Telnet" or "SSH" utility to connect to the gateway.

Parameter Setup Example

The following table lists the parameter configuration for the gateway as the example illustrated in the above diagram with "Telnet with CLI" enabled at LAN and WAN interfaces. The "gateway" is the gateway of Network-A and has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. It serves as an NAT gateway for the Network-A subnet (10.0.75.0/24).

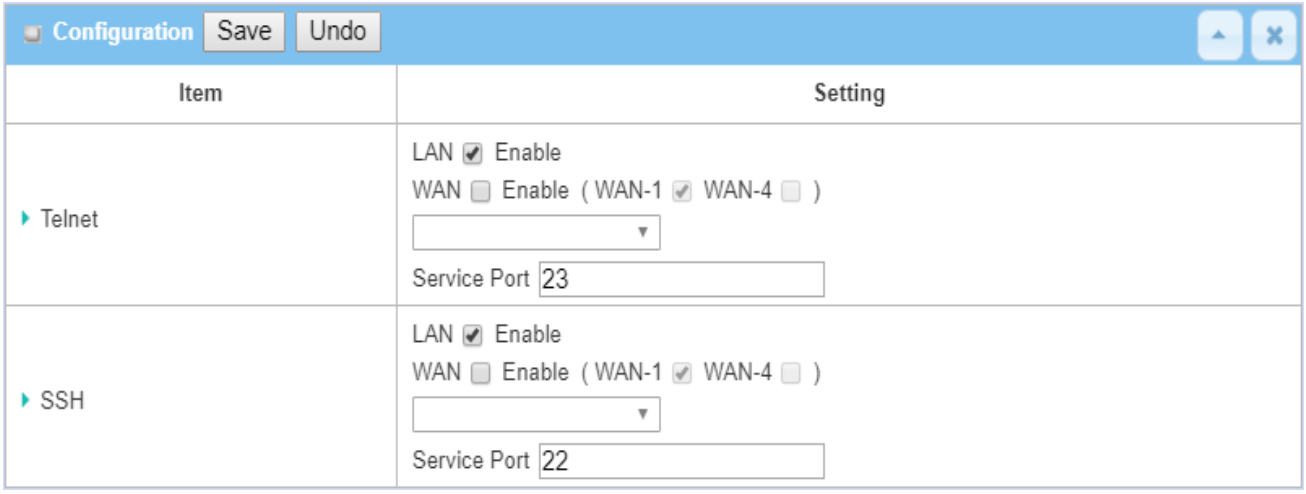
Configuration Path	[Telnet & SSH]-[Configuration]
Telnet	LAN: ■ ***Enable*** WAN: ☐ ***Enable*** Service Port: ***23***

SSH	LAN: ■ ***Enable*** WAN: ■ ***Enable*** Service Port: ***22***

Telnet & SSH Setting

Go to **Administration > Configure & Manage > Telnet & SSH** to access the Telnet & SSH setting page.

The Telnet & SSH setting allows you to access this device through the traditional Telnet or SSH Telnet program. Configure related settings before connecting to the device with Telnet.



Configuration		
Item	**Value setting**	**Description**
Telnet	1. The LAN Enable box is checked by default. 2. By default **Service Port** is 23.	Activate the Telnet function for the specified LAN or WAN interface. Specify the **Service Port** for the corresponding service. *Value Range*: 1 ~65535.
SSH	3. The LAN Enable box is checked by default. 4. By default **Service Port** is 22.	Activate the SSH Telnet function for the specified LAN or WAN interface. Specify the **Service Port** for the corresponding service. *Value Range*: 1 ~65535.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.
Note: The Telnet/SSH login password is the same as the admin login password for the device's Web UI.		

6.2 System Operation

System Operation allows you to manage system related information and settings such as admin account, system time and logging. It also allows you to perform essential administration and maintenance tasks such as firmware or configuration backup and restore, as well as reset & reboot.

6.2.1 Password & MMI

Go to **Administration > System Operation > Password & MMI** to access the Password & MMI page.

Configure Host Name

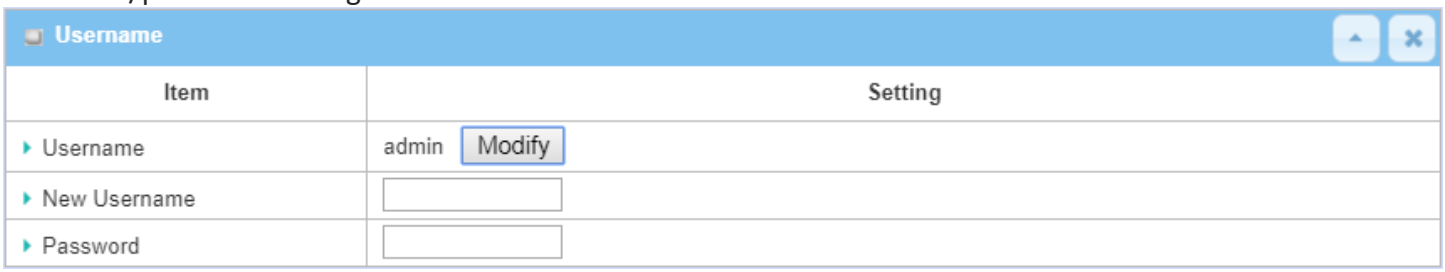
The Host Name screen allows you to configure the hostname of the gateway.

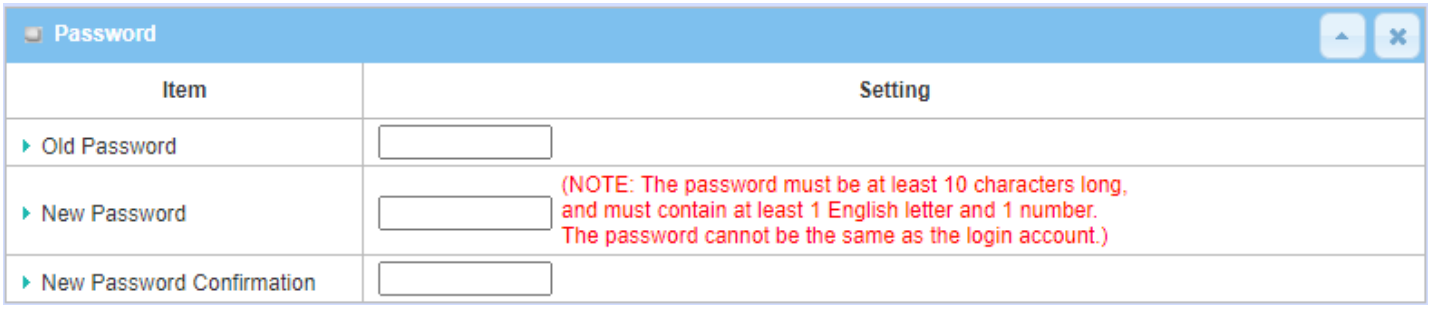


Username Configuration		
Item	**Value setting**	**Description**
Host Name	1. An optional setting 2. It is blanked by default	Enter the hostname of the gateway.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings.

Change Username & Password

You can change the web-based MMI login account and password. Click the **Modify** button and provide the new username/password setting.

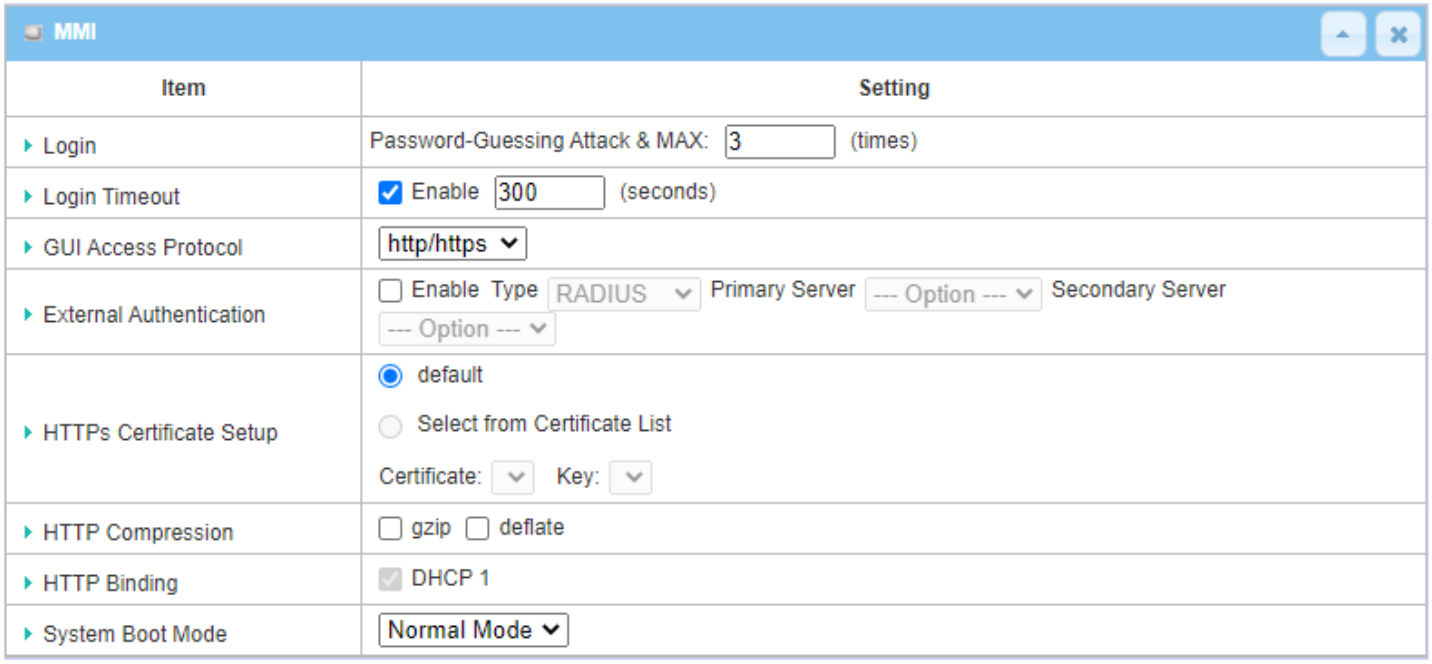




Username Configuration		
Item	**Value setting**	**Description**
Username	1. The default Username for web-based MMI is '**admin**'.	Display the current MMI login account (username).
New Username	String: any text	Enter a new username to replace the current setting.
Password	String: any text	Enter current password to make changes.
Old Password	1. String: any text 2. The default password for web-based MMI is 'admin'.	Enter the current password to make changes.
New Password	String: any text	Enter a new password that is different from the existing one. **Note**: The password length must be at least 10 characters and contains at least one letter and one number.
New Password Confirmation	String: any text	Enter the new password again to confirm it.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings.

Change MMI Basic Setting

The web-based MMI access allows you to access the gateway for management. The MMI related settings include automatic logout timer and protocols for web access.



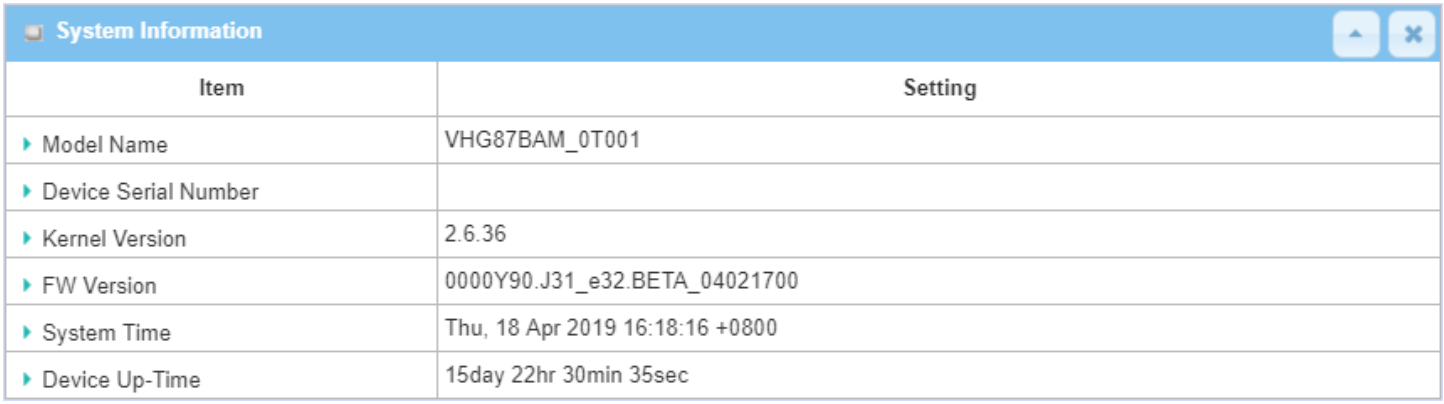
MMI Configuration Item	Value setting	Description
Login	3 times is set by default	Enter the login trial value. Value Range: 3 ~ 10. If someone tries to log into the Web UI with an incorrect password for the maximum trials, an warning message "***Already reaching maximum Password-Guessing times, please wait a few seconds!***" will be displayed.
Login Timeout	The Enable box is checked, and 300 is set by default.	Activate the auto logout function and specify the maximum idle time. *Value Range*: 30 ~ 65535.
GUI Access Protocol	**http/https** is selected by default.	Select the protocol that will be used for GUI access. It can be **http/https**, **http only**, or **https only**.
HTTPs Certificate Setup	The **default** box is selected by default	If the https Access Protocol is selected, configure HTTPs Certificate. Go to **Object Definition > Certificate** for certificate configuration.
HTTP Compression	The box is unchecked by default.	Select the compression method: **gzip or deflate.**
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	**Normal Mode** is selected by default.	Select the system boot mode to boot up the device. **Normal Mode**: It takes a longer bootup time, with complete firmware image checking during the device boot. **Fast Mode**: It takes a shorter bootup time, without checking the firmware image during the device boot. **Quick Mode**: It takes the shortest bootup time, without checking the firmware image and creating the internal database for User/Group/Captive Portal functions. **Note**: The **Quick Mode** will render the User/Group/Captive Portal function unusable.

Save	N/A	Save the settings
Undo	N/A	Cancel the settings

6.2.2 System Information

The System Information page provides a a snapshot of the device information.

Go to **Administration > System Operation > System Information** to access the System Information page.



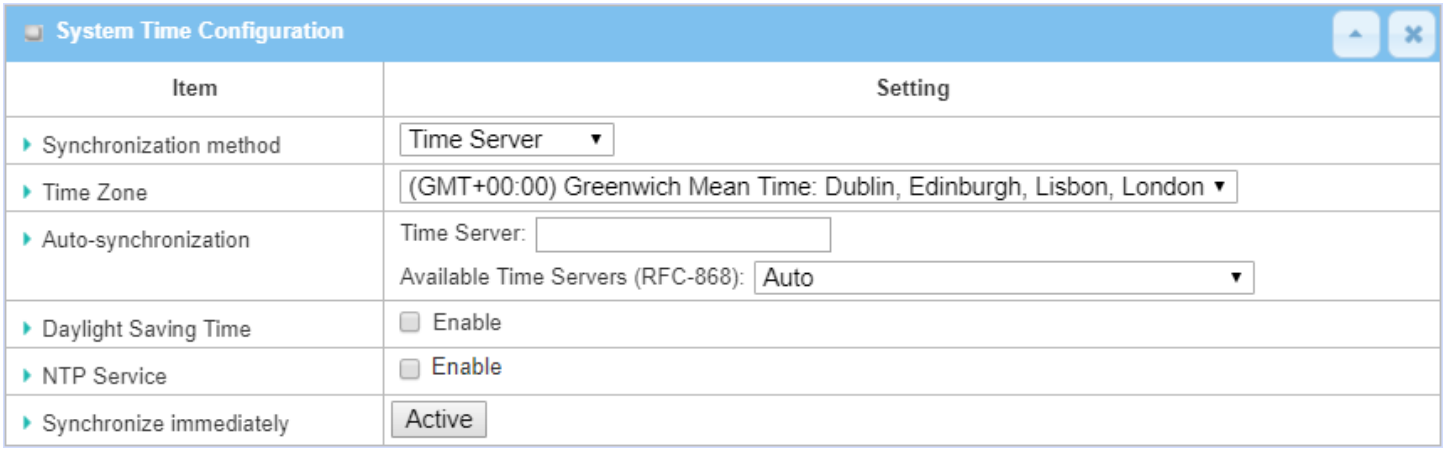
System Information		
Item	**Value Setting**	**Description**
Model Name	N/A	It displays the model name of the device.
Device Serial Number	N/A	It displays the serial number of the device.
Kernel Version	N/A	It displays the Linux kernel version of the system
FW Version	N/A	It displays the firmware version of the device.
Memory Usage	N/A	It displays the device memory utilization in percentage.
System Time	N/A	It displays the current system time.
Device Up-Time	N/A	It displays the device uptime since the last system start.
Refresh	N/A	Update the system Information.

6.2.3 System Time

You can set the system time either manually or using automatic time synchronization provided by the gateway. The two quick methods of time synchronization are “Sync with Time Server” and “Sync with my PC”. With Sync with Time Server, the system will communicate with a time server by NTP Protocol to set the time. With “Sync with my PC”, the system will update its date and time to accord with the time of the administration PC.

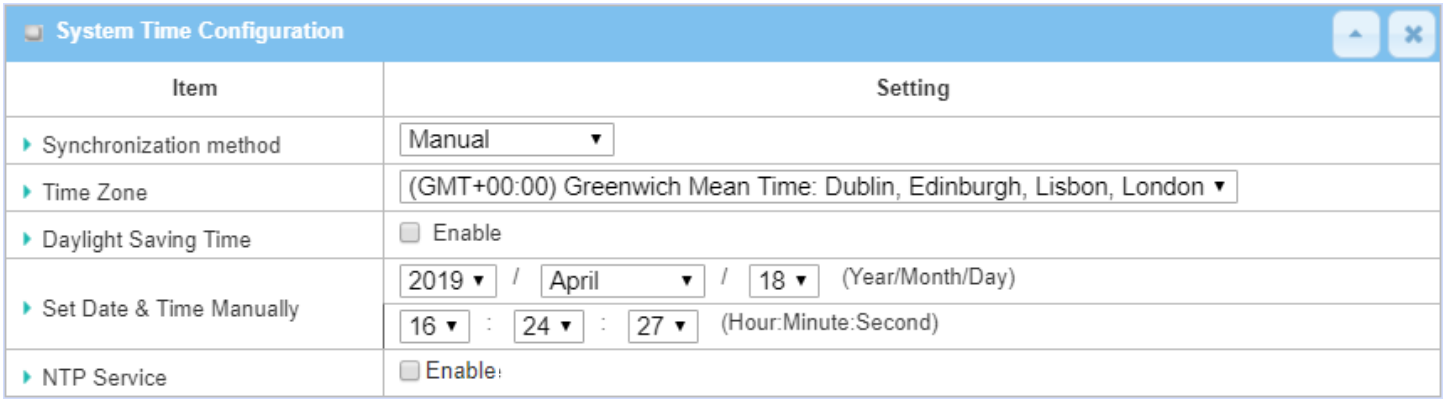
Go to **Administration > System Operation > System Time** to access the System Time page.

Synchronize with Time Server



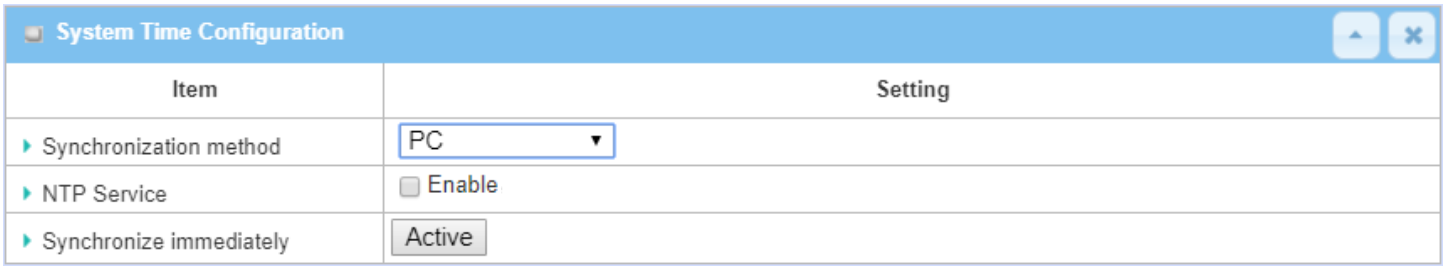
System Time Information		
Item	**Value Setting**	**Description**
Synchronization method	1. A Must-filled item. **2. Time Server is selected by default.**	Select the **Time Server** as the synchronization method for setting the system time.
Time Zone	1. A Must-filled item. 2. **GMT+00 :00** is selected by default.	Select a time zone where this device locates.
Auto-synchronization	1. A Must-filled item. 2. Auto is selected by default.	Enter the IP or FQDN of the NTP time server or leave it as auto for automatic selection.
Daylight Saving Time	1. It is an optional item. 2. Un-checked by default	Activate the daylight saving function and specify the start date and end date for the daylight saving time duration.
NTP Service	1. It is an optional item. 2. Un-checked by default	Activate the NTP Service function on the gateway to let the gateway provide NTP server service for its local connected devices.
Synchronize immediately	N/A	Click the **Active** button to synchronize the system time with the specified time server immediately.
Save	N/A	Save the settings.
Refresh	N/A	Update the system time immediately.
Note: The system will obtain the UTC (Coordinated Universal Time) time instead of the local time for the device without a correct time zone setting.		

Synchronize Manually



System Time Information		
Item	**Value Setting**	**Description**
Synchronization method	1. A Must-filled item. **2. Time Server is selected by default.**	Select the **Manual** as the synchronization method for the system time and set the Date & Time manually.
Time Zone	1. A Must-filled item. 2. **GMT+00 :00** is selected by default.	Select a time zone where this device locates.
Daylight Saving Time	1. It is an optional item. 2. Un-checked by default	Activate the daylight saving function and specify the start date and end date for the daylight saving time duration.
Set Date & Time Manually	1. It is an optional item.	Manually set the date (Year/Month/Day) and time (Hour:Minute:Second) as the system time.
NTP Service	1. It is an optional item. 2. Un-checked by default	Activate the NTP Service function on the gateway to let the gateway provide NTP service for its local connected devices.
Save	N/A	Save the settings.

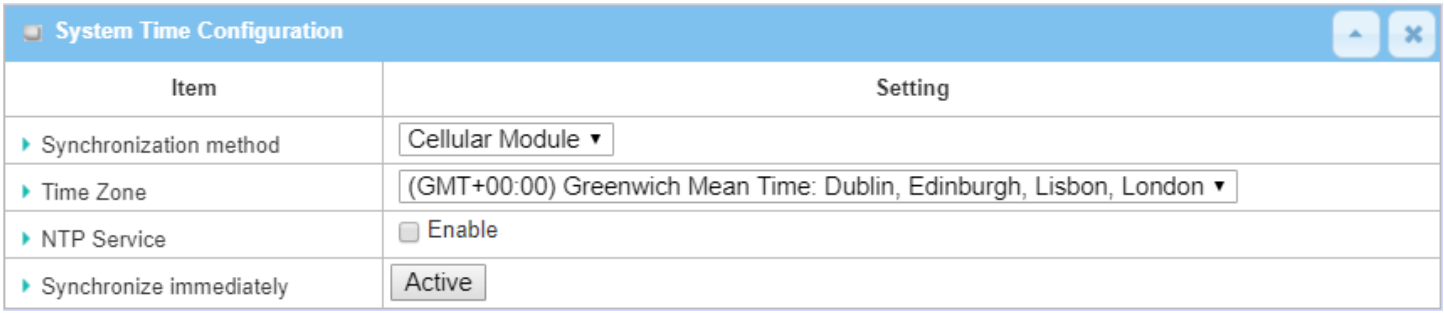
Synchronize with PC



System Time Information		
Item	**Value Setting**	**Description**

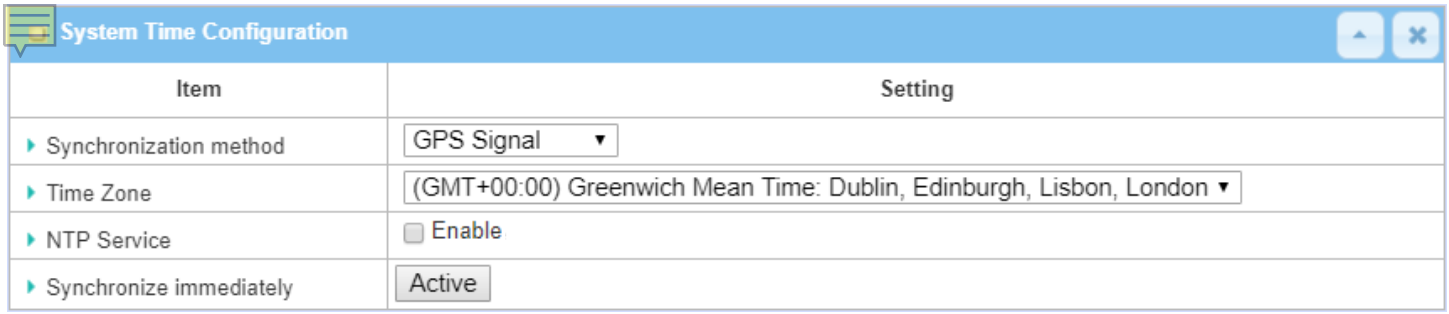
Synchronization method	1. A Must-filled item. **2. Time Server is selected by default.**	Select **PC** as the synchronization method to let system synchronize its date and time to the time of the administration PC.
NTP Service	1. It is an optional item. 2. Un-checked by default	Check the **Enable** button to activate the NTP Service function. When you enabled this function, the gateway can provide NTP server for its local connected devices.
Synchronize immediately	N/A	Click the **Active** button to synchronize the system time with specified time server immediately.
Save	N/A	Save the settings.
Refresh	N/A	Update the system time immediately.

Synchronize with Cellular Time Service



System Time Information		
Item	**Value Setting**	**Description**
Synchronization method	1. A Must-filled item. **2. Time Server is selected by default.**	Select Cellular Module as the synchronization method to let the system synchronize its date and time to the time provided by the connected mobile ISP. **Note:** This option is only available for device models with a Cellular WAN interface.
Time Zone	1. A Must-filled item. 2. GMT+00 :00 is selected by default.	Select a time zone where this device locates.
NTP Service	1. It is an optional item. 2. Un-checked by default	Check the Enable button to activate the NTP Service function. When you enabled this function, the gateway can provide NTP server for its local connected devices.
Synchronize immediately	N/A	Click the Active button to synchronize the system time with specified time server immediately.
Save	N/A	Save the settings.
Refresh	N/A	Update the system time immediately.

Synchronize with GPS Time Service

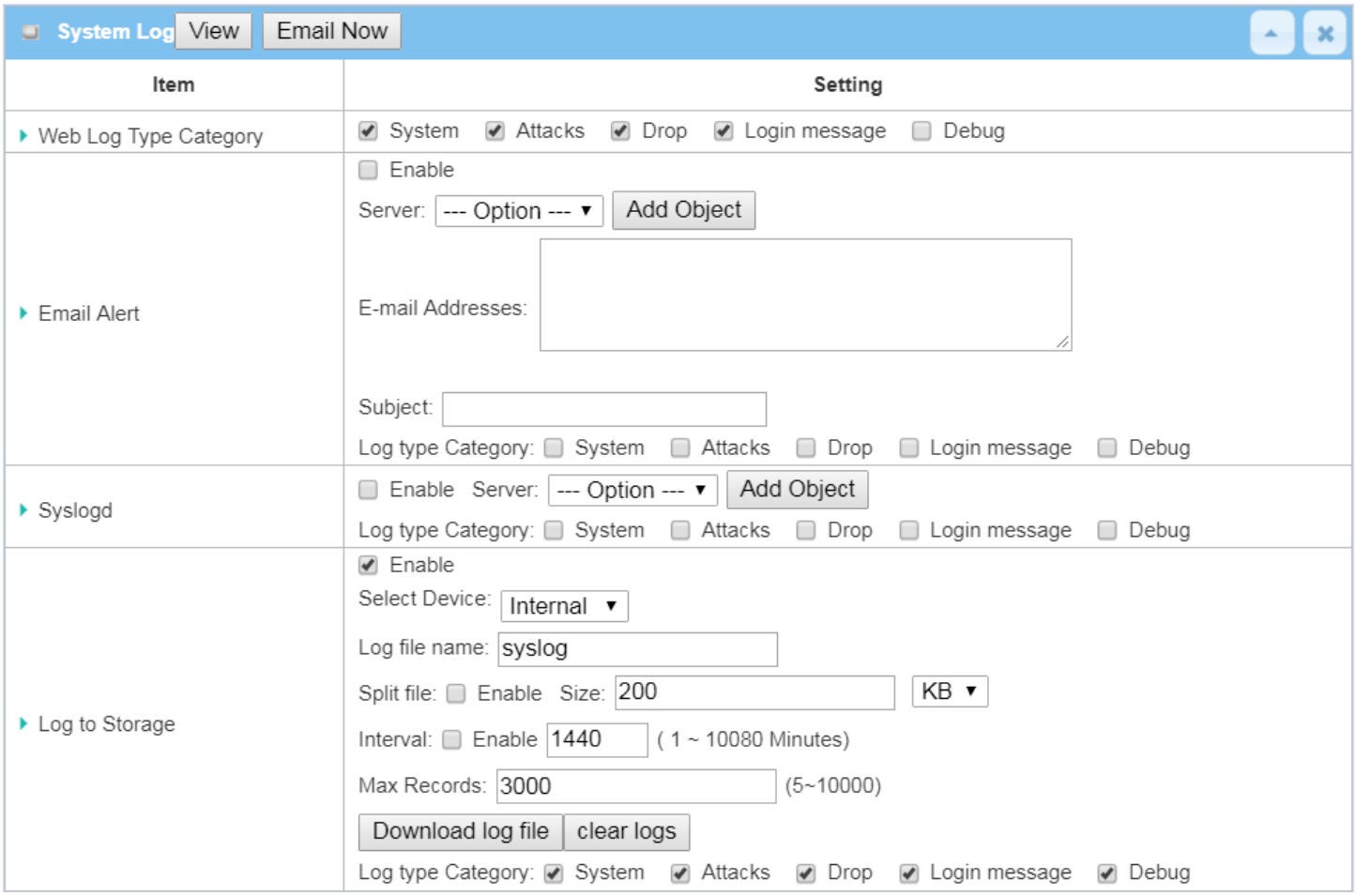


System Time Information		
Item	**Value Setting**	**Description**
Synchronization method	1. A Must-filled item. **2. Time Server is selected by default.**	Select GPS Signal as the synchronization method to let system synchronize its date and time to the time provided by the GNSS service. **Note:** This option is only available for device models with a GPS Time Service.
Time Zone	1. A Must-filled item. 2. GMT+00 :00 is selected by default.	Select a time zone where this device locates.
NTP Service	1. It is an optional item. 2. Un-checked by default	Check the Enable button to activate the NTP Service function. When you enable this function, the gateway can provide NTP server for its local connected devices.
Synchronize immediately	N/A	Click the Active button to synchronize the system time with specified time server immediately.
Save	N/A	Save the settings.
Refresh	N/A	Update the system time immediately.

6.2.4 System Log

The System Log page allows you to perform local event logging and remote reporting.

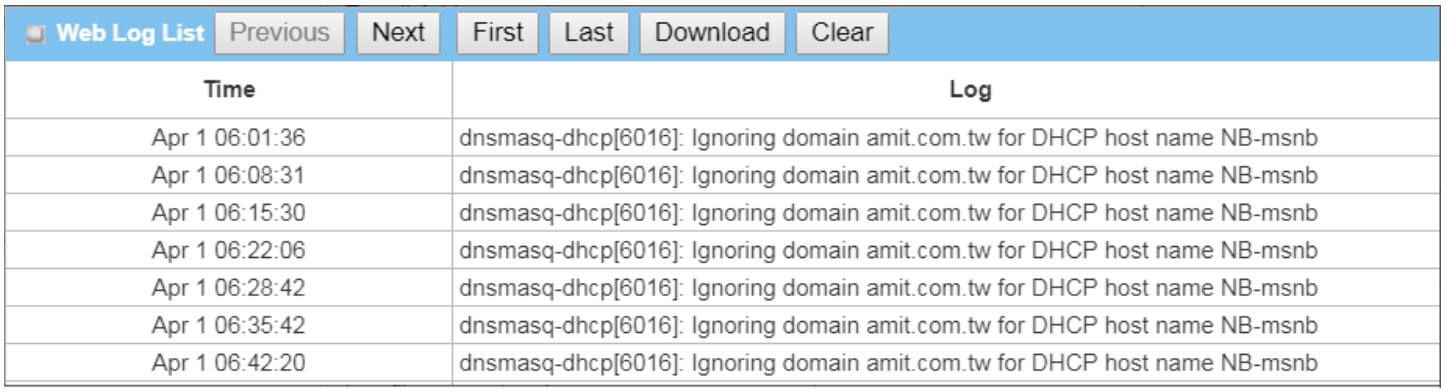
Go to **Administration > System Operation > System Log** tab.



View & Email Log History

Click **View** to view log history on the gateway. Click **Email Now** to send instant email for analysis.

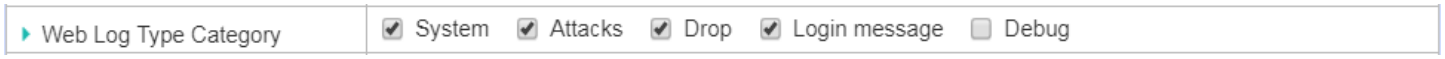
View & Email Log History		
Item	**Value setting**	**Description**
View button	N/A	Click the **View** button to view Log History in Web Log List Window.
Email Now button	N/A	Click the **Email Now** button to send Log History via email immediately.



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
Previous	N/A	Go to the previous page.
Next	N/A	Go to the next page.
First	N/A	Jump to the first page.
Last	N/A	Jump to the last page.
Download	N/A	Download log to your PC in tar file format.
Clear	N/A	Clear all loga.
Back	N/A	Return to the previous page.

Web Log Type Category

The Web Log Type Category screen allows you to select the type of events to be logged and displayed in the Web Log List window.



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

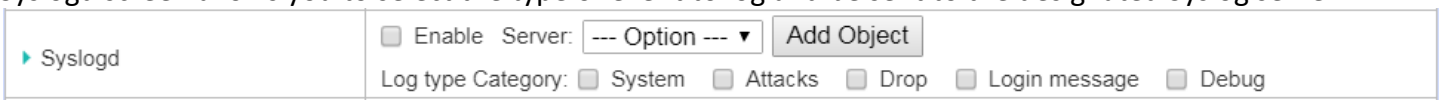
Configure Email Alert and select the type of event to be logged and sent to the configured email account.



Email Alert Setting Window		
Item	**Value Setting**	**Description**
Enable	Un-checked by default	Check **Enable** box to enable sending event log messages to destined Email account defined in the E-mail Addresses blank space.
Server	N/A	Select one email server from the Server dropdown box to send Email. If none has been available, click the Add Object button to create an outgoing Email server. You may also add an outgoing Email server from **Object Definition > External Server** 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

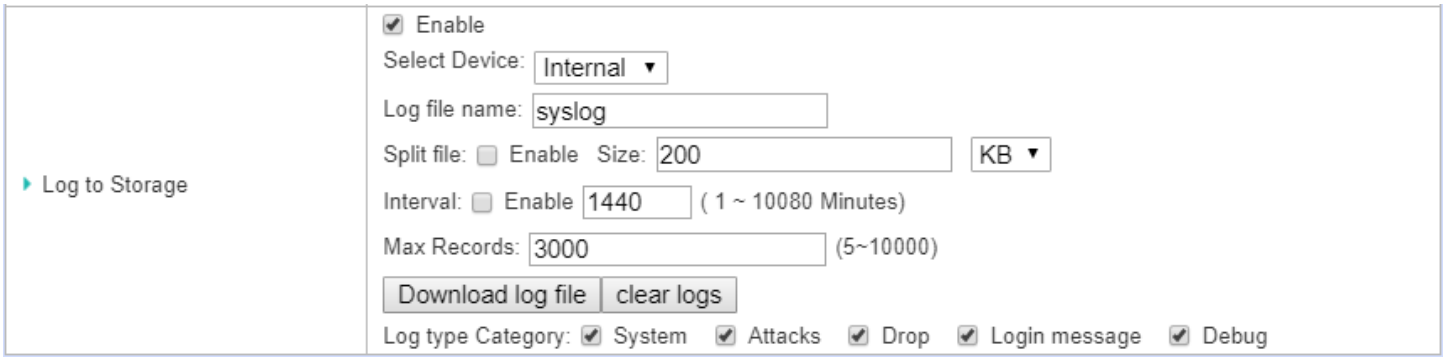
Syslogd screen allows you to select the type of event to log and be sent to the designated Syslog server.



Syslogd Setting Window		
Item	**Value Setting**	**Description**
Enable	Un-checked by default	Check Enable box to activate the Syslogd function, and send event logs to a syslog server
Server	N/A	Select one syslog server from the Server dropdown box to send event logs to. If none has been available, click the **Add Object** button to create a system log server. You may also add a system log server from the Object Definition > External Server > External Server tab.
Log type category	Un-checked by default	Select the type of event to log and be sent to the destined syslog server. Available events are System, Attacks, Drop, Login message, and Debug.

Log to Storage

Configure the type of events to be logged and be saved to an internal storage volume or external storage device.



Log to Storage Setting Window		
Item	**Value Setting**	**Description**
Enable	Un-checked by default	Check to enable logging to storage.
Select Device	Internal is selected by default	Select internal or external storage.
Log file name	Un-checked by default	Enter a file name to save logs.
Split file Enable	Un-checked by default	Check **enable** box to split a file when it reaches the specified limit.
Split file Size	**200 KB** is set by default	Enter the file size limit for each split log file. *Value Range*: 10 ~ 1000.
Interval Enable	Un-checked by default	Check **enable** box to enable the log interval setting.
Log Interval	**1440** is set by default	Enter the log interval setting. *Value Range*: 1 ~ 10080 Minute.
Max Records	**3000** is set by default	Enter the maximum number of records to be stored in the log storage. *Value Range*: 5 ~ 10000.
Log type category	Un-checked by default	Check the types of logs to send: System, Attacks, Drop, Login message, Debug

Log to Storage Button Description		
Item	**Value setting**	**Description**
Download log file	N/A	Download log files in a log.tar file format.
Clear Logs	N/A	Delete the log files from the storage.

6.2.5 Backup & Restore

The Backup & Restore lets you upgrade the device firmware and save and restore the device configuration. You can also restore the device with a default configuration besides the factory default settings.

Go to **Administration > System Operation > Backup & Restore** to access the Backup & Restore page.



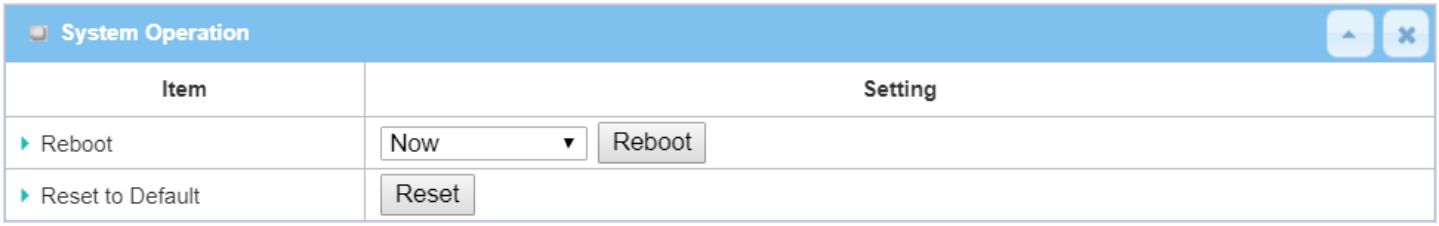
FW Backup & Restore		
Item	**Value Setting**	**Description**
FW Upgrade	**Via Web UI** is selected by default	Click the FW Upgrade button to upgrade the device firmware via Web UI, or Via Storage. Then click Browse to locate the new firmware file. After selecting the firmware file for upgrade, click Upgrade to start the FW upgrade process. If you want to upgrade a version of firmware licensed with GPL, please check "Accept unofficial firmware".
Backup Configuration Settings	**Download** is selected by default	Back up or restore the device configuration settings by clicking the Via Web UI button. Download: back up device configuration to a config.bin file. Upload: restore a designated configuration file to the device.
Auto Restore Configuration	The **Enable** box is unchecked by default	Activate automatic restoration using the most recent configuration saved in the gateway's memory. Click the **Conf.Info** to view details about the saved configuration file. You can save your current configuration by clicking **Save Conf.** or erase the stored configuration by clicking the **Clean Conf.** button.
Self-defined Logo		Use this function to define a customized logo on the Web UI by clicking the Via Web UI button. **Download:** download the current logo. **Upload:** upload a new logo. **Reset: Reset the logo**
Clean Userdata		Use this function to clear all user configuration changes made on this page, e.g. the self-defined logo and saved configuration files.

CAUTION: During a firmware upgrade, do not interrupt the process in any way such as closing the webpage or turning off the device. Interrupting the upgrade process will damage the device and further RMA service may be required.

6.2.6 Reboot & Reset

The Reboot & Reset allows you to reboot the device or reset the device configuration to its factory defaults.

Go to **Administration > System Operation > Reboot & Reset** to access the Reboot & Reset page.



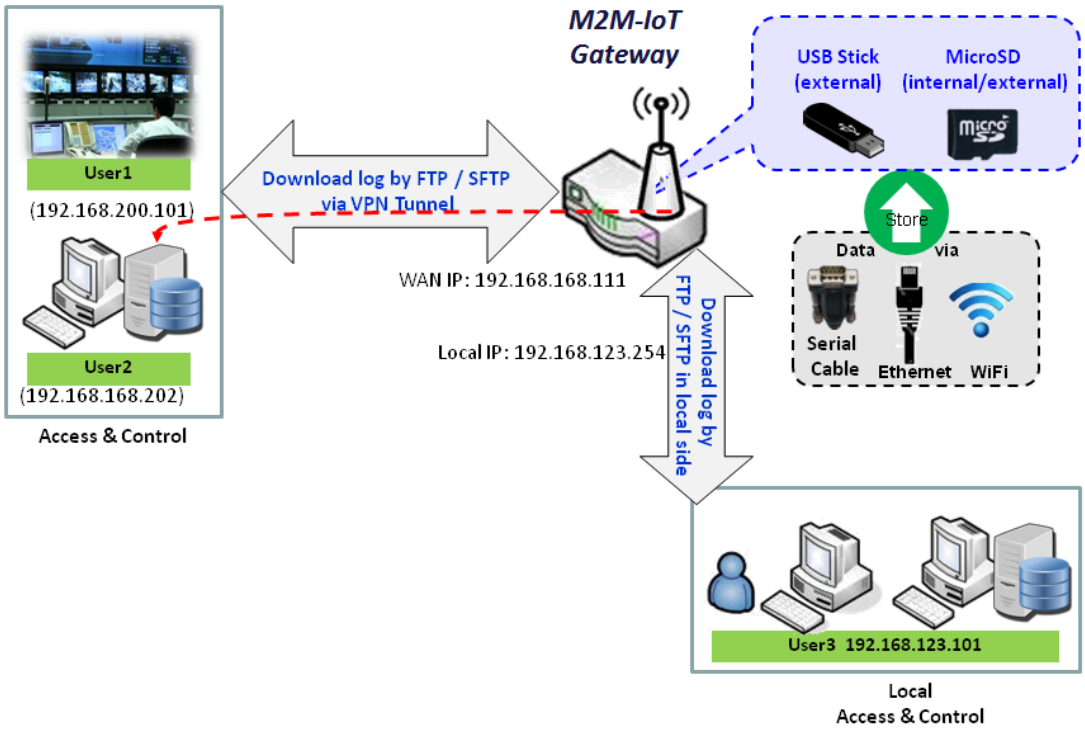
System Operation Window		
Item	**Value Setting**	**Description**
Reboot	**Now** is selected by default	Chick the **Reboot** button to reboot the gateway immediately or schedule a auto reboot. **Now**: Reboot immediately.s **Time Schedule**: Select a pre-defined schedule to reboot the device. To define a schedule, go to **Object Definition > Scheduling > Configuration** tab.
Reset to Default	N/A	Reset the device configuration to its default settings.

6.3 FTP

The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files between a client and server on a computer network. FTP is built on a client-server model architecture and uses separate control and data connections. FTP users may authenticate themselves with a sign-in protocol, normally in the form of a username and password, as well as connect anonymously if the server allows it.

For secure transmission that protects the username and password and encrypts the content, FTP is often used with SSL/TLS (FTPS).

This gateway has a built-in FTP / SFTP server for file download. You can download different types of log files for troubleshooting and system analysis purposes: 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).

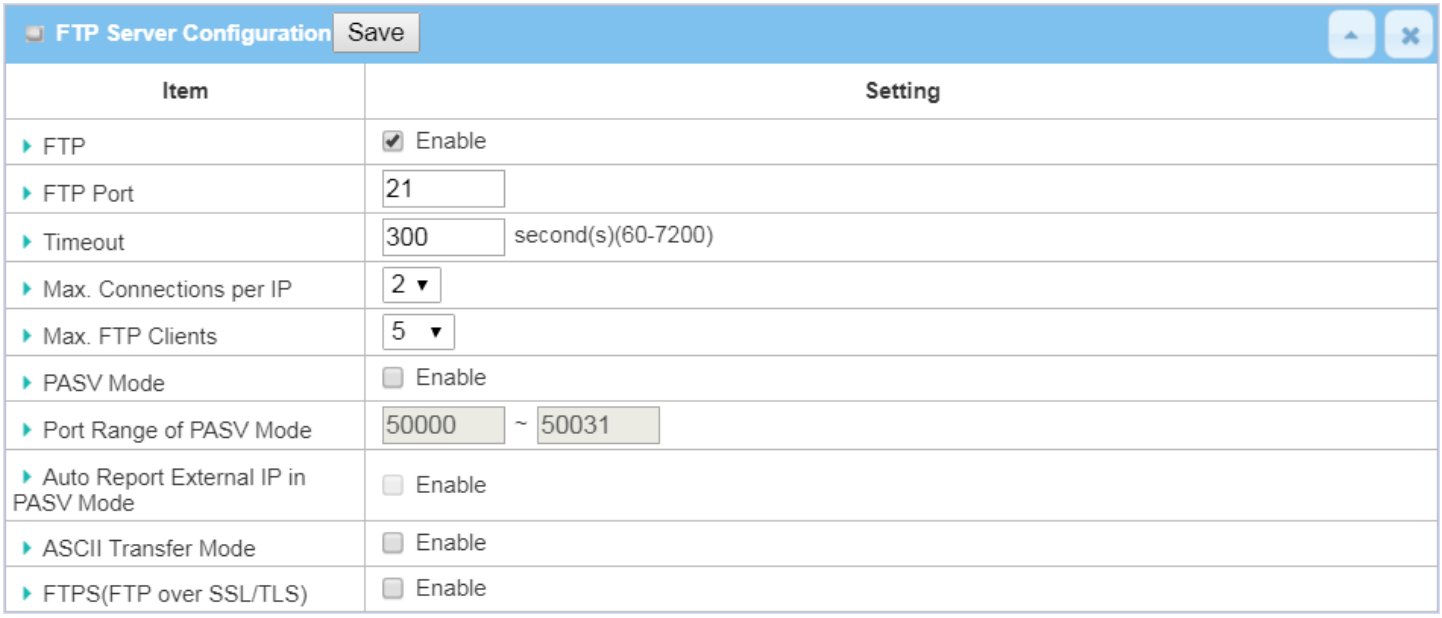


6.3.1 Server Configuration

The Server Configuration page allows you to set up the embedded FTP and SFTP server for retrieving log files.

Go to Administration > FTP > Server Configuration to access the configuration page.

Enable FTP Server



Configuration Item	Value setting	Description
FTP	The box is unchecked by default.	Activate the embedded FTP Server function. You can retrieve or delete the stored log files via FTP. **Note**: The embedded FTP Server is only for log downloading, but not for file upload.
FTP Port	Port **21** is set by default	Specify a port number for FTP connection. *Value Range*: 1 ~ 65535.
Timeout	**300** seconds is set by default.	Specify the maximum timeout interval for the FTP connection. *Value Range:* 60 ~ 7200 seconds.
Max. Connections per IP	**2** Clients are set by default.	Specify the maximum number of clients from the same IP address. A total of 5 concurrent connections from the same IP address is supported.
Max. FTP Clients	**5** Clients are set by default.	Specify the maximum number of clients for the FTP connection. A total of 32 clients is supported.
PASV Mode	Optional setting	Activate the support of PASV mode.
Port Range of PASV Mode	Port **50000** ~ **50031** is set by default.	Specify the port range to allocate for PASV style data connection. *Value Range*: 1024 ~ 65535.
Auto Report External IP in PASV Mode	Optional setting	Activate the support for overriding the IP address advertisement in response to the PASV command.
ASCII Transfer	Optional setting	Activate the support of ASCII mode data transfers.

Mode		Binary mode is supported by default.
FTPS (FTP over SSL/TLS)	Optional setting	Activate the support for secure connections via SSL/TLS.

Enable SFTP Server



Configuration Item	Value setting	Description
SFTP	The box is unchecked by default.	Activate the embedded SFTP Server function and select an interface for SFTP: **LAN**, **WAN**, or **both**. For a WAN interface, limit the hosts that can access to the WAN port via SFTP. Specify the hosts with the following options: **any** to allow any hosts, **Specific IP Address** for a single host, or **IP Range** for a range of IP addresses. You can retrieve or delete the stored log files via secure SFTP connection.
SFTP Port	Default 22	Specify a port number for SFTP connection. *Value Range*: 1 ~ 65535.

6.3.2 User Account

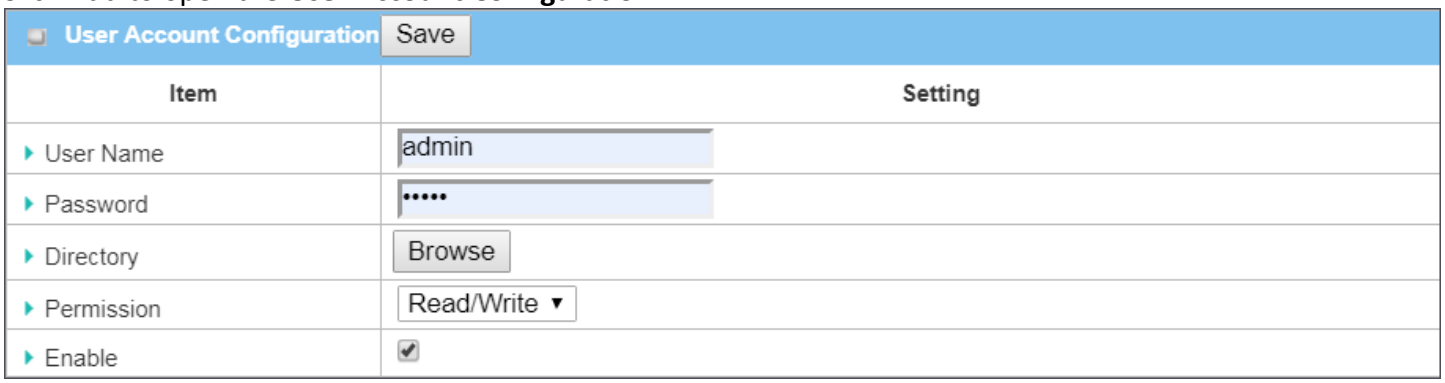
This section allows you to configure user accounts for logging to the embedded FTP and SFTP server to retrieve the fog files.

Go to **Administration > FTP > User Account** to access the Uer Account page.

Create/Edit FTP User Accounts



Click **Add** to open the **User Account Configuration**.



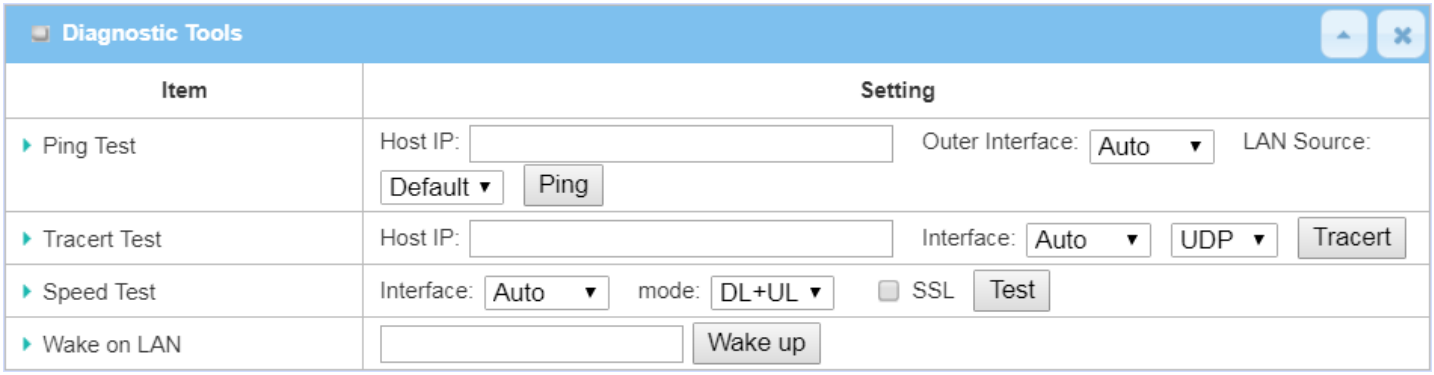
Configuration Item	Value setting	Description
Username	String : non-blank string	Enter the user account for FTP login. *Value Range*: 1 ~ 15 characters.
Password	String : no blank	Enter the user password.
Directory	N/A	Select a root directory for user access.
Permission	**Read/Write** is selected by default.	Select the Read/write permission. **Note**: The embedded FTP Server is only for log downloading, but not for file upload.
Enable	The box is checked by default.	Activate the FTP user account.

6.4 Diagnostic

This gateway offers some common network diagnostic tools for diagnosing the system and troubleshooting causes of connection problems. The Packet Analyzer helps record the packets while Ping and Tracert help testing the network connectivity.

6.4.1 Diagnostic Tools

Go to **Administration > Diagnostic > Diagnostic Tools** to access the tools.

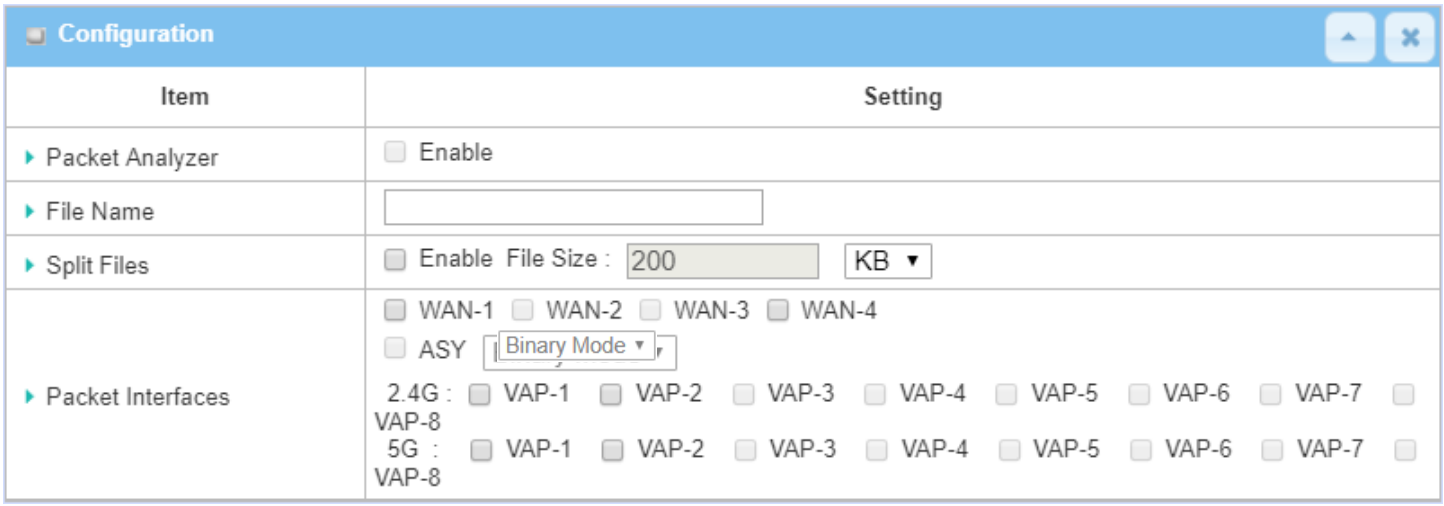


Diagnostic Tools		
Item	**Value setting**	**Description**
Ping Test	Optional Setting	Specify the host IP / FQDN and the Outer interface (auto, WAN, LAN, or VLAN) and LAN source (default, LAN, or VLAN), so the system will ping the specified device to test whether it is alive. The results will be displayed below.
Tracert Test	Optional setting	Traceroute (tracert) command is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets transmitted in an IP network. Specify an IP / FQDN, the test interface (LAN, WAN, or Auto) and the protocol (UDP or ICMP), so the system will try to traceroute the specified host. The results will be displayed below.
Speed Test	Optional setting	Perform a quick speed test for verifying the connectivity of a specific interface.
Wake on LAN	Optional setting	Wake on LAN (WOL) is an Ethernet networking standard that allows a computer to be turned on by a network message. Specify a MAC address of the computer, in your LAN network, to be remotely turned on.
Save	N/A	Save the configuration.

6.4.2 Packet Analyzer

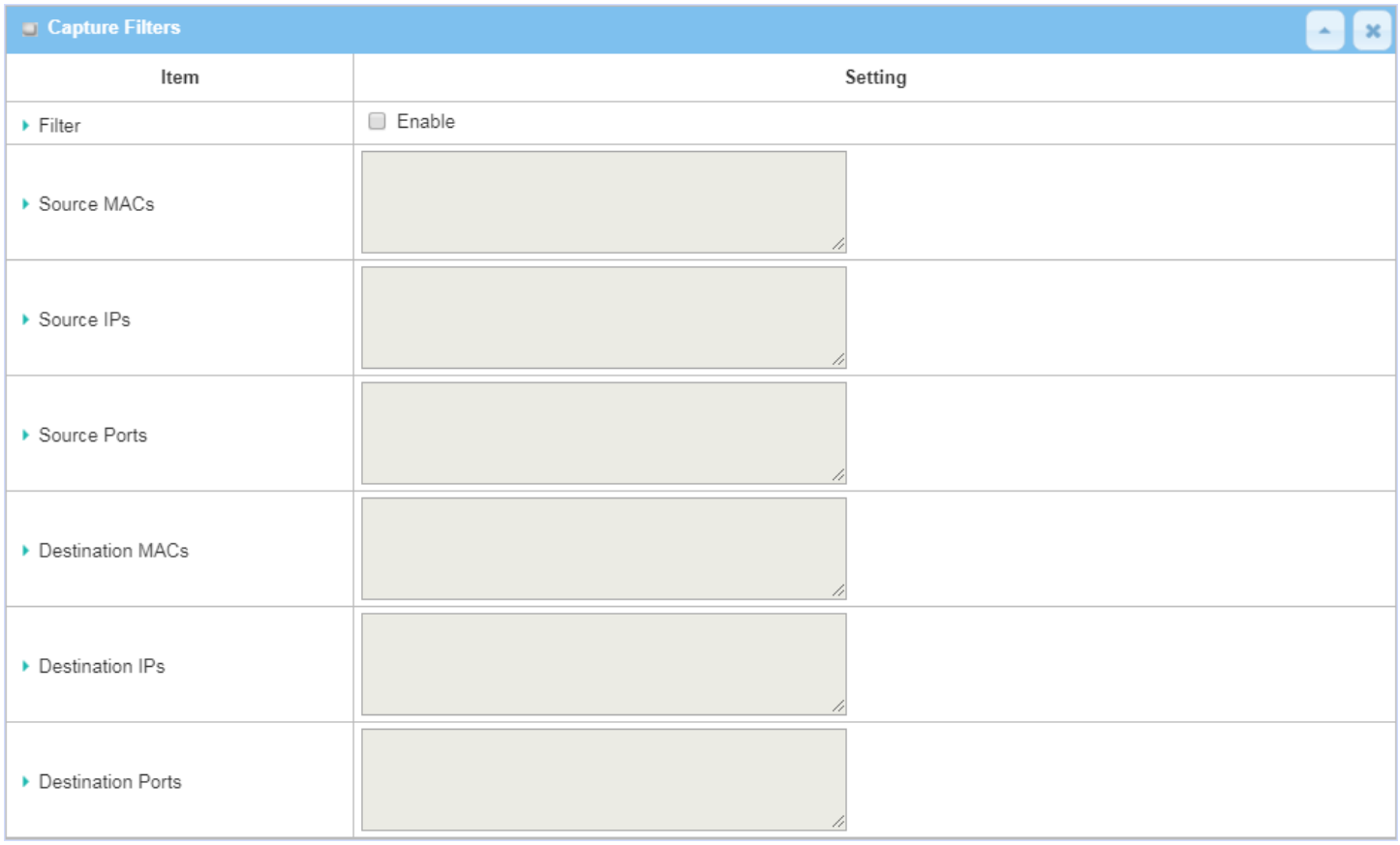
The Packet Analyzer captures packets. You can specify interfaces to enable packets capture and filter them by setting rules. Make sure that the log storage is available (either embedded SD Card or an external USB Storage device) to enable Packet Analyzer.

Go to Administration > Diagnostic > Packet Analyzer to access the configuration page.



Configuration		
Item	**Value setting**	**Description**
Packet Analyzer	The box is unchecked by default.	Activate the Packet Analyzer function. Make sure that a USB storage device is present to enable the Package Analyzer function.
File Name	1. An optional setting 2. Blank is set by default, and the default file name is **<Interface>_<Date>_<index>.**	Enter the file name to save the captured packets in the log storage. If the **Split Files** option is enabled, the file name will be appended with an index code "**_<index>**". The extension of the file name is **.pcap**.
Split Files	1. An optional setting 2. The default value of **File Size** is 200 KB.	Check **enable** box to split the file when the size of the log file reaches the specified limit. If the **Split Files** option is enabled, specify the **File Size** and **Unit** for the split files. *Value Range*: 10 ~ 99999. **Note: File Size** cannot be less than 10 KB
Packet Interfaces	An optional setting	Define the interface(s) to enable **Packet Analyzer**. The supported interfaces are: ● **WAN**: When a specific WAN interface is enabled at **Physical Interface**, it can be selected here. ● **ASY**: This indicates the serial communication interface. It is used to capture packets of the interfaces appearing in the **Field Communication**. Select **Binary mode** or **String mode** for the serial interface. ● **VAP**: This means the virtual AP interface. When Wi-Fi is enabled on the gateway, it can be selected here.
Save	N/A	Save the configuration.
Undo	N/A	Discard the changes.

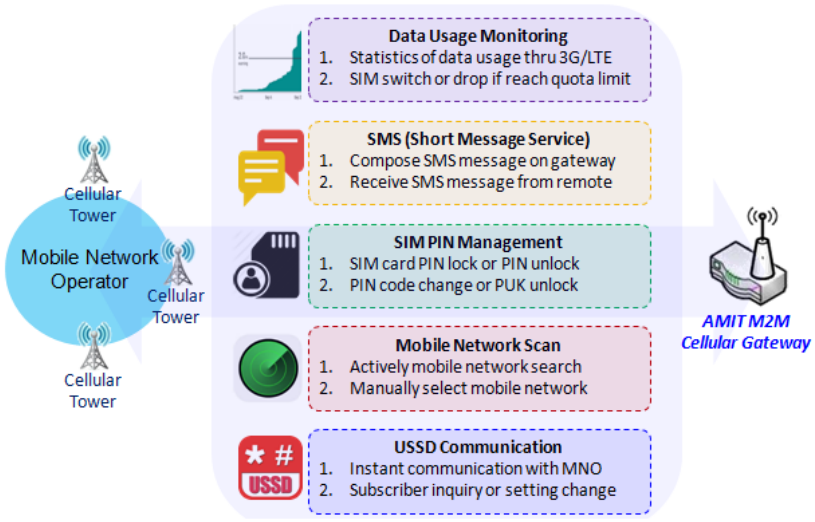
Once you enable the Packet Analyzer function, you can specify filter rules to capture packets that match the specified criteria.



Capture Fitters		
Item	**Value setting**	**Description**
Filter	Optional setting	Activate the Capture Filter function.
Source MACs	Optional setting	Define the filter rule with **Source MACs**. Up to 10 MACs are supported and they must be separated by "**;**", e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66
Source IPs	Optional setting	Define the filter rule with **Source IPs.** Up to 10 IP addresses are supported and they must be separated by "**;**", e.g. 192.168.1.1; 192.168.1.2.
Source Ports	Optional setting	Define the filter rule with **Source Ports**. Up to 10 ports are supported and they must be separated by "**;**", e.g. 80; 53 *Value Range*: 1 ~ 65535.
Destination MACs	Optional setting	Define the filter rule with **Destination MACs.** Up to 10 MACs are supported and they must be separated by "**;**", e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66
Destination IPs	Optional setting	Define the filter rule with **Destination IPs**. Up to 10 IPs are supported and they must be separated by "**;**", e.g. 192.168.1.1; 192.168.1.2
Destination Ports	Optional setting	Define the filter rule with **Destination Ports**. Up to 10 ports are supported and they must be separated by "**;**", e.g. 80; 53 *Value Range*: 1 ~ 65535.

Chapter 7 Service

7.1 Cellular Toolkit



The system provides tools for you to monitor data usage of cellular WAN, send text messages through SMS, change PIN code of SIM card, send USSD command to a carrier/ISP, and perform mobile network scan to search for available mobile networks.

Please note a valid SIM card is required for proper configurations of the mobile network.

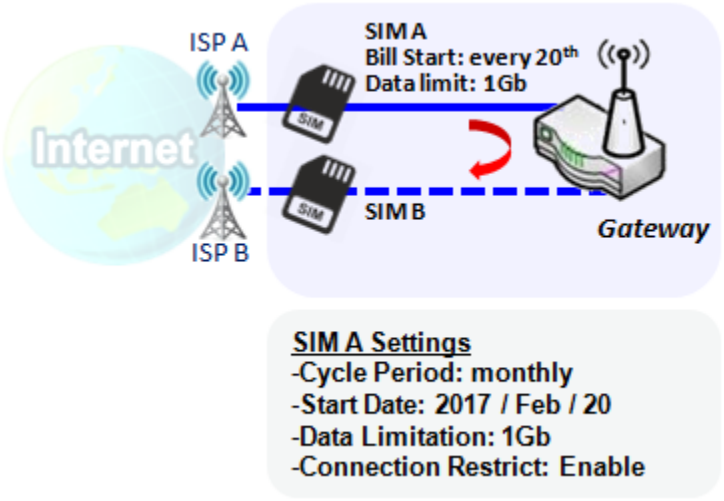
7.1.1 Data Usage

Most cellular data service sets a limit on data usage. If the cellular data usage has been over the data limit, the connection throughput will be reduced or extra charges will incur.

The Data Usage feature continuously monitors data consumption and automatically drops the active connection if the usage reaches the set limit. It will also start failover if a second SIM card is installed to avoid network disruption.

If Data Usage is enabled, go to **Status** > **Statistics & Reports** > **Cellular Usage** to view the history of cellular data usage.

Cellular Data Usage



Data Usage enables the gateway to continuously monitor cellular data usage. In the diagram, data limit of SIM A is 1GB per month and billing starts at 20th of every month, which is the date the device resets the counter for data consumption. The Connection Restrict feature will also force the gateway to drop cellular connection of SIM A when data usage reaches the limit (1GB in this case). And if SIM failover is configured in **Connection Setup** (refer to **2.1.2 Connection Setup**), then the gateway will switch to SIM B to continue the mobile service.

Data Usage Setting

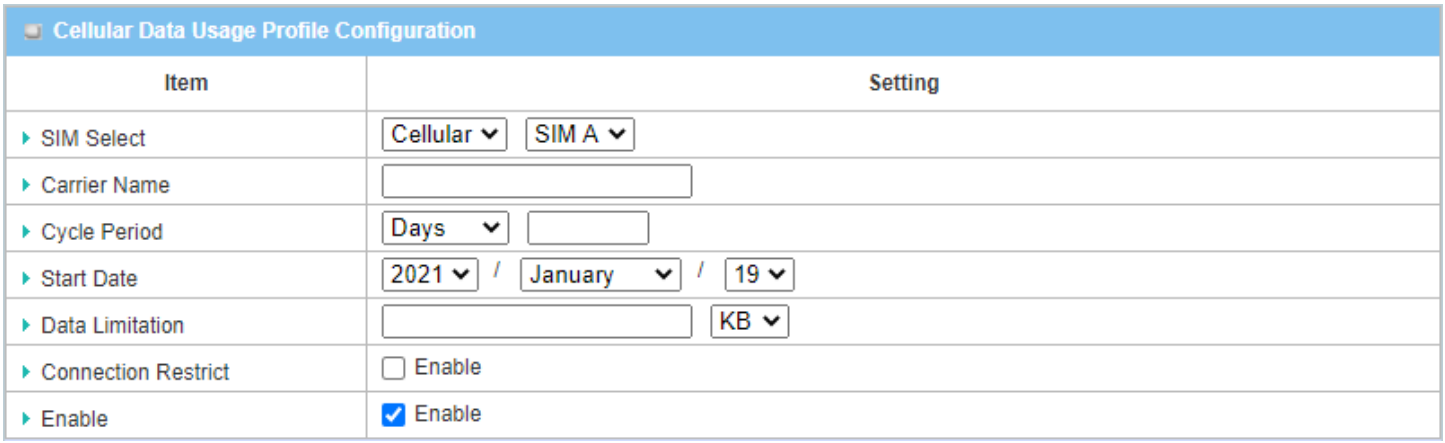
Go to **Service** > **Cellular Toolkit** > **Data Usage** to access the Data Usage Profile Setting page.

To set up data usage settings, obtain related information such as bill start date, bill period, and data limit of your data plan from your carrier or ISP.

Create / Edit Cellular Data Usage Profile



Click **Add** to open the **Cellular Data Usage Profile Configuration** screen. You can create up to 4 data usage profiles, one profile for each SIM card used in the gateway.



Cellular Data Usage Profile Configuration		
Item Setting	**Value setting**	**Description**
SIM Select	**Cellular-1** and **SIM A** by default.	Choose a cellular interface (**Cellular-**1 or **Cellular-2**) and a SIM card bound to the selected cellular interface to configure its data usage profile. **Note: Cellular-2** is only available for for the product with dual cellular modules.
Carrier Name	It is an optional item.	Fill in the Carrier Name for the selected SIM card for identification.
Cycle Period	**Days** by default	The first box has three types for cycle period: **Days**, **Weekly** and **Monthly**. **Days**: Specify the number of days for per Days cycle periods. **Weekly**, **Monthly**: The cycle period is one week or one month. *Value Range*: 1 ~ 90 days.
Start Date	N/A	Specify the date to start measuring network traffic. Please do not select a day before the current day; otherwise, the traffic statistics will be incorrect.
Data Limitation	N/A	Limit the amount of data consumption for the defined cycle period.
Connection Restrict	Un-Checked by default.	Activate the connection restriction function. During the specified cycle period, if the actual data usage exceeds the data limit, the cellular connection will be forced to disconnect.
Enable	Checked by default.	Activate the data usage profile.

7.1.2 SMS

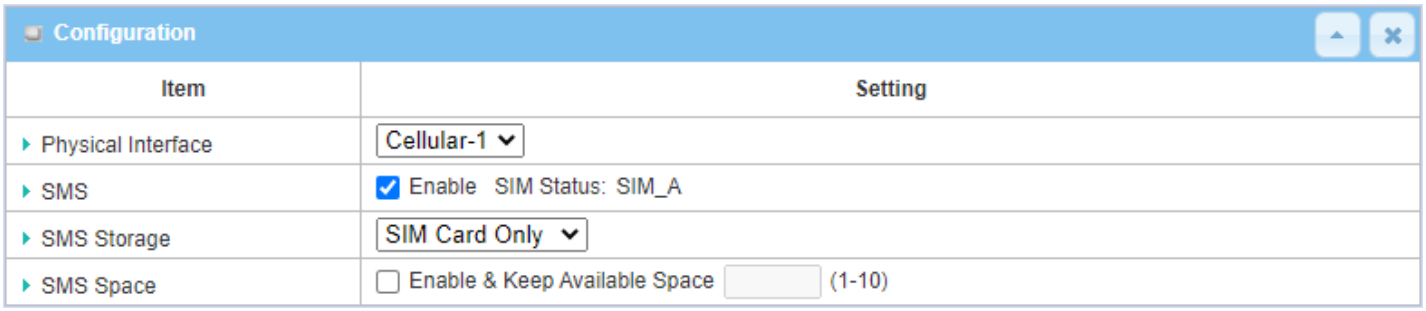
Short Message Service (SMS) is a text messaging service, which allows mobile phones or tablets to send short text messages instantly.

SMS Setting

Go to **Service** > **Cellular Toolkit** > **SMS** to access the SMS page.

You can send SMS text messages or read read SMS messages in the inbox as you would on a cellular phone.

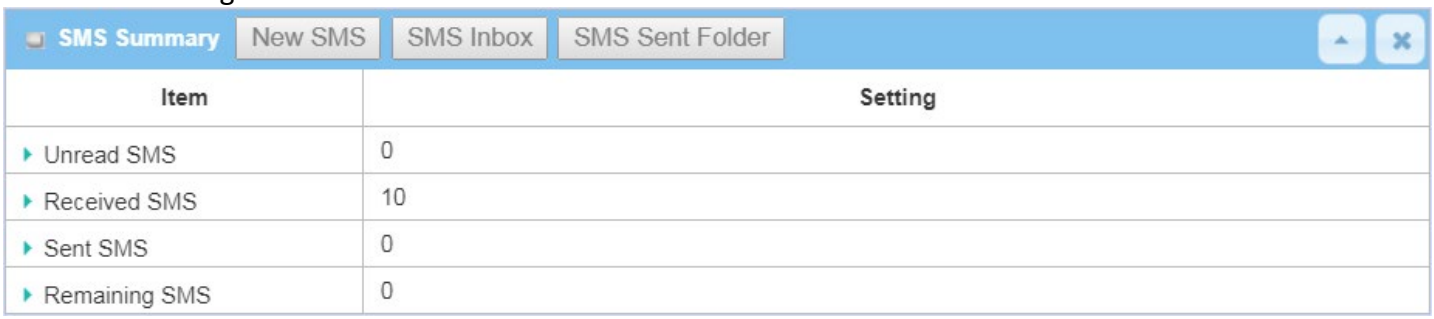
Configure SMS Configuration



Configuration Item	Value setting	Description
Physical Interface	The box is **Cellular-1** by default	Choose a cellular interface (**Cellular**-1 or **Cellular-2**) for the following SMS function configuration. **Note:** Cellular-2 is only available for models with dual SIM.
SMS	The box is checked by default	Enable or disable the SMS function.
SIM Status	N/A	Depending on the currently SIM status, the possible values are: **SIM_A** or **SIM_B**.
SMS Storage	The box is **SIM Card Only** by default	This is the SMS storage location.
SMS Space	The box is unchecked by default	Specify a number (1-10) as the number of messages for storage reservation. The oldest message(s) will be deleted when the SMS storage becomes full.
Save	N/A	Save the settings

SMS Summary

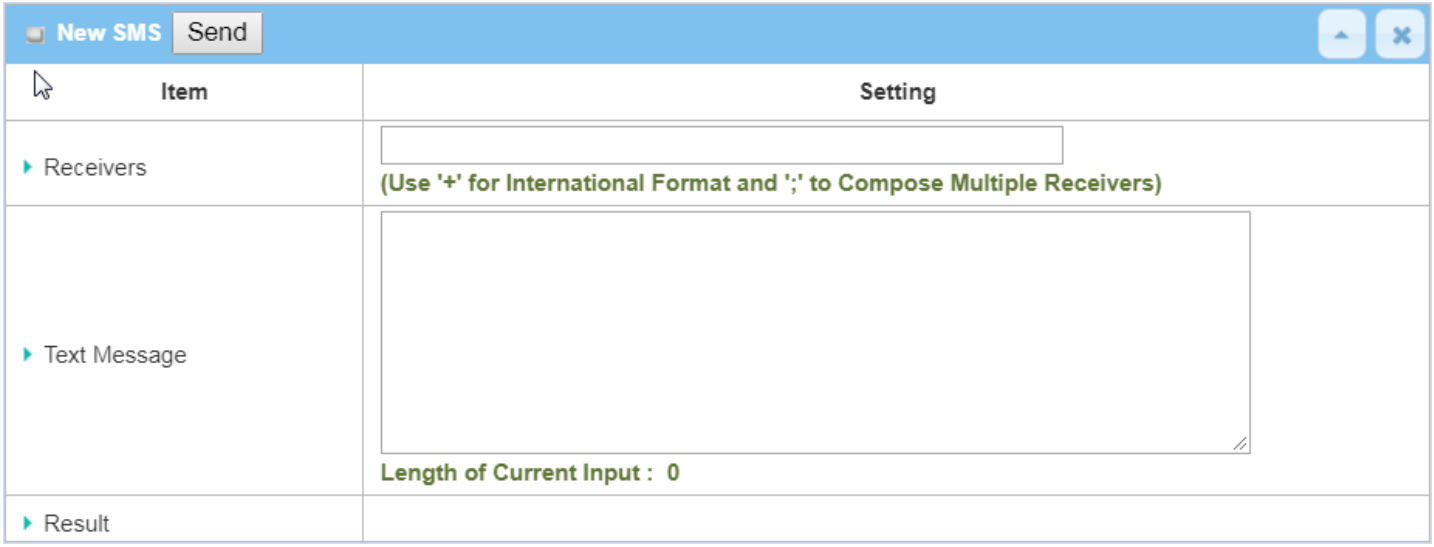
The summary displays **Unread SMS**, **Received SMS**, **Sent SMS**, and **Remaining SMS.** You can also read and write SMS messages.



SMS Summary Item	Value setting	Description
Unread SMS	N/A	Displays unread messages.
Received SMS	N/A	Displays the number of received messages. This value increments by one when a new message is received.
Sent SMS	N/A	Displays the number of sent messages.
Remaining SMS	N/A	Displays the number of remaining messages to receive as the storage permits. This value decreases by one when a new message is received.
New SMS	N/A	Click **New SMS** button to open the **New SMS** screen. You can write a new message from this screen. Refer to New SMS in the next page.
SMS Inbox	N/A	Click **SMS Inbox** to open the **SMS Inbox List** screen. You can read or delete messages and reply or forward messages from this screen. Refer to SMS Inbox on the next page.
Refresh	N/A	Update the SMS summary immediately.

New SMS

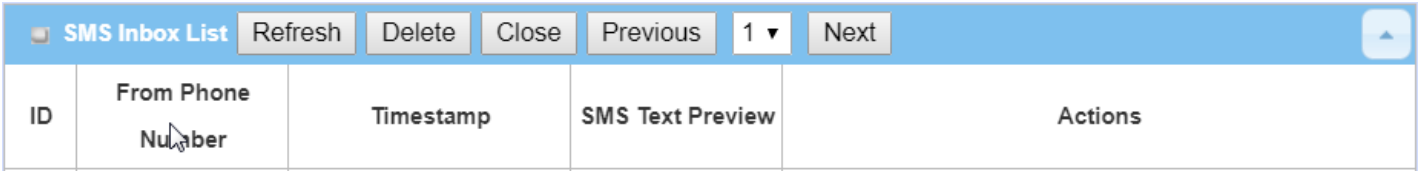
You can write messages from this screen.



New SMS		
Item	**Value setting**	**Description**
Receivers	N/A	Enter the recipients of the message; separate the recipient by a semicolon.
Text Message	N/A	Write an SMS message. Up to 1023 characters are allowed.
Send	N/A	Send the text message via SMS.
Result	N/A	If the message has been sent successfully, it will show **Send OK;** otherwise, **Send Failed** will be displayed.

SMS Inbox List

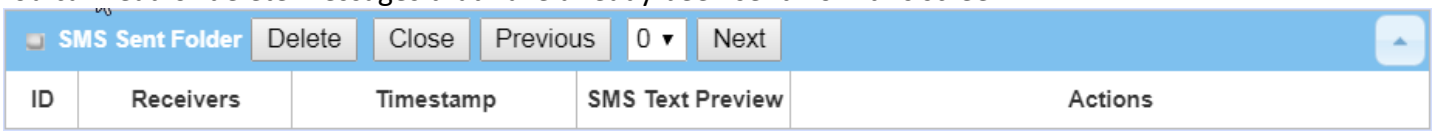
You can read or delete and reply or forward messages from this screen.



SMS Inbox List		
Item	**Value setting**	**Description**
ID	N/A	The number that identifies the SMS message.
From Phone Number	N/A	Sender List (Phone Number) for the received SMS.
Timestamp	N/A	The time that the message is received.
SMS Text Preview	N/A	Preview the SMS text. Click the **Detail** button to read a specific message.
Action	The box is unchecked by default	Click the **Detail** button to read the message in detail. Or click the **Reply** / **Forward** button to reply/forward a message.
Refresh	N/A	Refresh the SMS Inbox List.
Delete	N/A	Delete the selected messages.
Close	N/A	Close the Detail SMS Message screen.

SMS Sent Folder

You can read or delete messages that have already been sent from this screen.



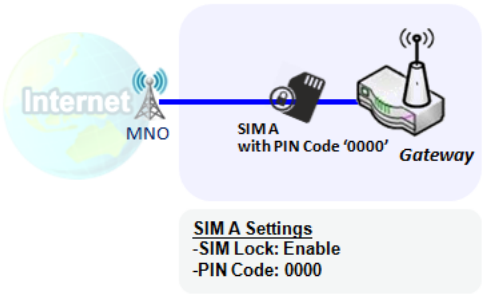
SMS Sent Folder		
Item	**Value setting**	**Description**
ID	N/A	The number that identifies the SMS message.
Receivers	N/A	The recipients of the sent message.
Timestamp	N/A	The time that the message is sent.
SMS Text Preview	N/A	Preview the SMS text. Click the **Detail** button to read a specific message.
Action	The box is unchecked by default	Click the **Detail** button to read the message in detail; Click the **Reply** / **Forward** button to reply or forward a message.
Refresh	N/A	Refresh the SMS Sent Folder.
Delete	N/A	Delete the selected messages.
Close	N/A	Close the Detail SMS Message screen.

7.1.3 SIM PIN

The SIM card is usually released by mobile operators or ISPs. Each SIM card has a unique number or ICCID for network owners or ISPs to identify each subscriber. Therefore, it is imperative that a SIM card employs security mechanisms to prevent unauthorized access.

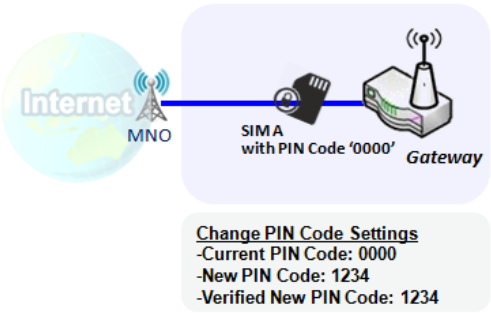
A PIN code on a SIM card has been used widely and the gateway allows you to activate and manage PIN code on a SIM card through the Web UI.

Activate PIN code on SIM Card



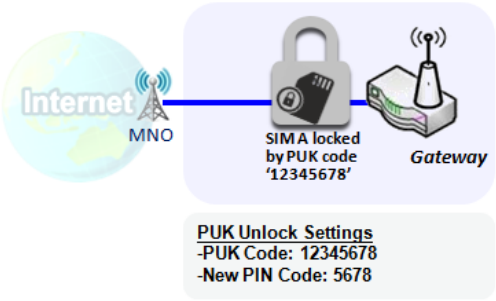
This example shows how to activate PIN code on SIM-A for 3G/4G-1 with the default PIN code "**0000**".

Change PIN code on SIM Card



The exampls shows how to change PIN code on the SIM card. You need to type original PIN code "**0000**" and then type the new PIN code.

Unlock SIM card by PUK Code



If you entered incorrect PIN code for more than three times, then the SIM card will be locked by PUK code. Then you have to call the service number to get a PUK code to unlock the SIM card. In the diagram, the PUK code is "**12345678**" and new PIN code is "**5678**".

SIM PIN Setting

Go to **Service** > **Cellular Toolkit** > **SIM PIN** to access the SIM PIN setting.

You can enable or disable SIM lock with a PIN code. You can also change the PIN code. You can also see the remaining times of failure trials. A PUK code will be required to unlock the SIM card.

Select a SIM Card



Configuration Window		
Item	**Value setting**	**Description**
Physical Interface	The box is **Cellular-1** by default	Choose a cellular interface (**Cellular-**1 or **Cellular-2**) to change the SIM PIN setting for the selected SIM Card. **Note: Cellular-2** is only available for models with dual SIM card.
SIM Status	N/A	Displays the selected SIM card and the SIM card status. The status could be **Ready**, **Not Insert**, or **SIM PIN**. **Ready** -- SIM card is inserted and ready to use. It can be a SIM card without PIN protection or that SIM card is already unlocked by a correct PIN code. **Not Insert** -- No SIM card is inserted in that SIM slot. **SIM PIN** -- SIM card is protected by PIN code, and the SIM card is still at locked state.
SIM Selection	N/A	Select the SIM card for PIN configuration. Click the **Switch** button to switch the SIM card to the selected one.

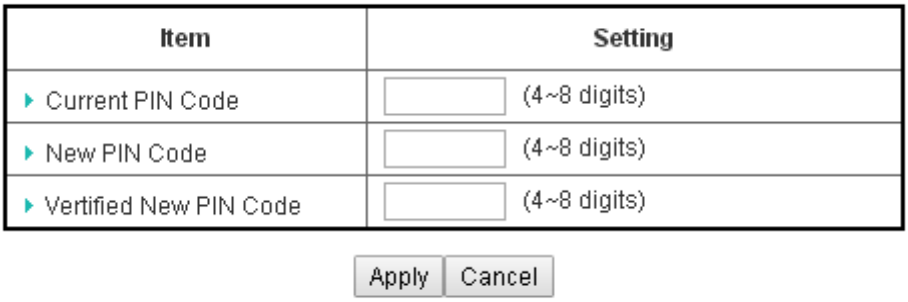
Enable / Change PIN Code

Enable or Disable the SIM lock function with PIN code (password).



SIM function Window		
Item Setting	**Value setting**	**Description**
PIN lock	Depend on SIM card	Acctivate the PIN lock function. The first time you enable PIN lock, you have to enter the PIN code, and then click **Save** to apply the setting.
Remaining times	Depend on SIM card	Indicates the remaining trials for unlocing the SIM PIN code.
Save	N/A	Apply the settings.
Change PIN Code	N/A	Click the **Change PIN code** button to change the PIN code. If the **SIM Lock** function is not enabled, the **Change PIN code** button is disabled. To enable SIM Lock, enter the PIN code, then click **Save** to enable the SIM Lock.

Click Change PIN Code to open the Change PIN Code Screen.



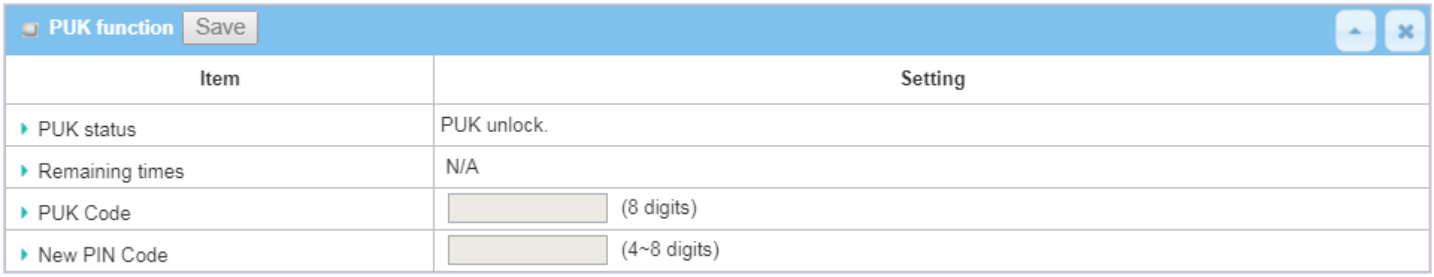
Item	Value Setting	Description
Current PIN Code	A must-filled setting	Enter the current (old) PIN code of the SIM card.
New PIN Code	A must-filled setting	Enter the new PIN Code.
Verified New PIN Code	A must-filled setting	Confirm the new PIN Code.
Apply	N/A	Change the PIN code with the specified new PIN code.
Cancel	N/A	Cancel the changes and keep current PIN code.

Note: If you have changed the PIN code for a SIM card, you must also change the corresponding PIN code specified on the Connection Setup page (go to **Basic Network > WAN & Uplink > Connection Setup > Connection with SIM Card**). Otherwise, it may result in wrong SIM PIN trials using an invalid (old) PIN code.

Unlock with a PUK Code

The PUK Function is only available if the SIM card is locked by a PUK code. It means that the SIM card is locked and needs additional PUK code to unlock it. It happens when the allowed PIN trials exceed. In this situation, you

need to contact your ISP and request a PUK code for your SIM card. After a SIM card is unlocked by the PUK code successfully, the SIM lock function will be activated automatically.



PUK Function Window		
Item	**Value setting**	**Description**
PUK status	**PUK Unlock** / **PUK Lock**	Indication for the PUK status. The status could be **PUK Lock** or **PUK Unlock**. As mentioned earlier, the SIM card will be locked by PUK code after too many failed attempts. In this case, the PUK Status shows **PUK Lock**. In a normal situation, it will display **PUK Unlock**.
Remaining times	Depend on SIM card	Indicate the remaining trials for PUK unlocking. **Note: Beware of the "0" remaining times, it will damage the SIM card permanently !** Call your ISP for help with a correct PUK to unlock the SIM.
PUK Code	A must-filled setting	Enter the PUK code (8 digits) to unlock the SIM card.
New PIN Code	A must-filled setting	Enter the New PIN Code (4~8 digits) for the SIM card. Save the new pin code for latter uses.
Save	N/A	Apply the settings.

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.

7.1.5 Network Scan

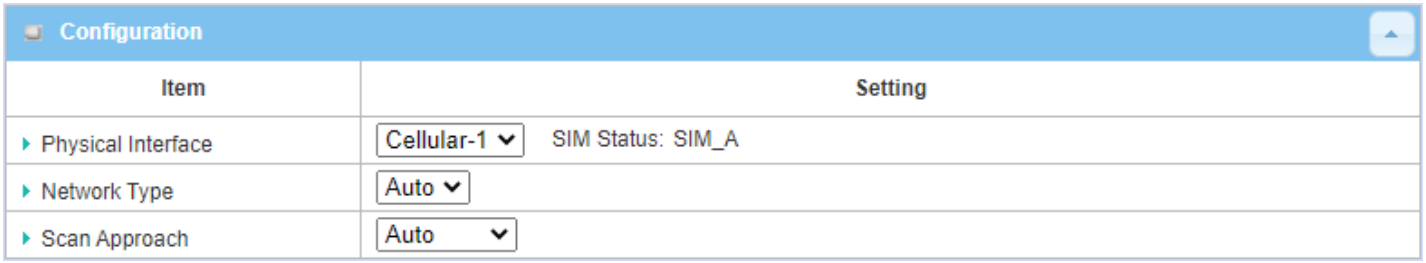
The Network Scan lets you configure the device to connect to a mobile network. You can specify which generation of mobile network will be used for connection: 3G, 4G or 5G. You can also scan for available mobile networks manually.

Network Scan Setting

Go to **Service** > **Cellular Toolkit** > **Network Scan** tab.

On the "Network Scan" page, there are two windows for the Network Scan function: the "Configuration" window, which lets you select the Cellular module (physical interface) to perform Network Scan and the "Network Provider List" window, which lists all mobile networks from manual scan.

Configure Network Scan



Configuration Item	Value setting	Description
Physical Interface	The box is **Cellular-1** by default	Choose a cellular interface (**Cellular-**1 or **Cellular-2**) for the network scan function. **Note: Cellular-2** is only available for models with dual SIM.
SIM Status	N/A	Show the connected cellular service (identified with **SIM_A** or **SIM_B**).
Network Type	**Auto** is selected by default.	Specify the network type for the network scan function. When **Auto** is selected, the network will be registered automatically;
Scan Approach	**Auto** is selected by default.	When **Auto** is selected, the cellular module will be registered automatically. If the **Manually** option is selected, the **Network Provider List** appears. Click the **Scan** button to scan for nearby base stations. Select the preferred base stations then **Apply** to apply the settings.
Save	N/A	Save the settings.

Select **Manually** as the **Scan Approach** to open the **Network Provider List** window. Click the **Scan** button and wait for 1 to 3 minutes to show the found mobile systems. Click the **Apply** button to connect to the selected mobile operator system for the dedicated cellular interface.

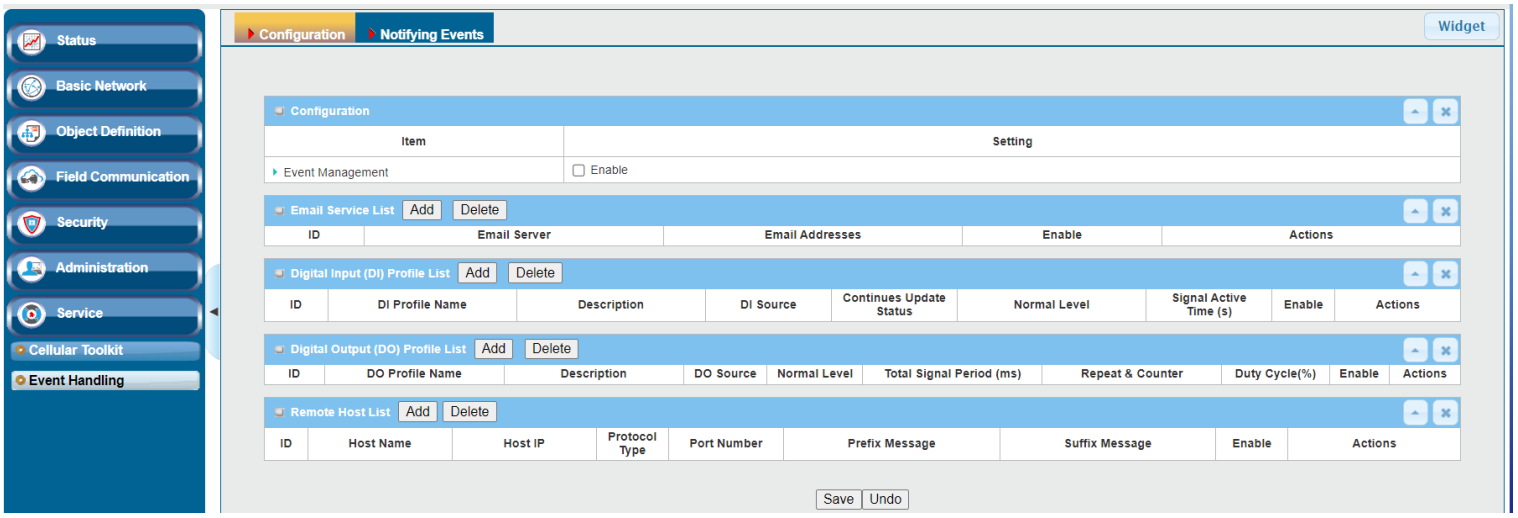
Network Provider List Scan Apply

Provider Name	Mobile System	Network Status	Action
Chunghwa Telecom	4G	Available	Select
T Star	4G	Available	Select
T Star	3G	Available	Select
TW Mobile	3G	Available	Select
Far EasTone	3G	Available	Select
Far EasTone	4G	Available	Select
TWN APT	4G	Available	Select
TW Mobile	4G	Available	Select
TWN APT	4G	Available	Select
Chunghwa Telecom	3G	Available	Select

Network Provider List Scan Apply

Provider Name	Mobile System	Network Status	Action

7.2 Event Handling

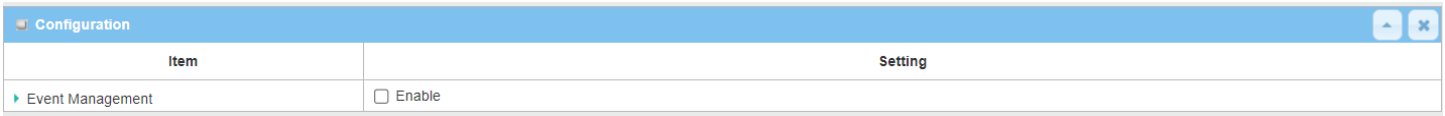


7.2.1 Configuration

The Configuration page allows you to set profiles for triggering actions when the defined events occur. To define notifying events, go to **Service > Event Handling> Notifying Events**.

Go to **Service > Event Handling > Configuration** to access the Event Handling Configuration page.

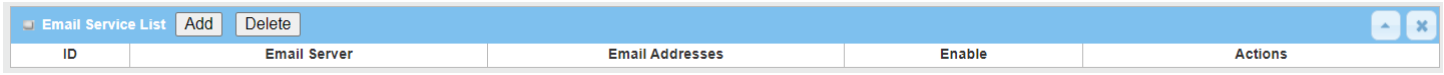
Enable Event Management Configuration



Configuration		
Item	**Value setting**	**Description**
Event Management	N/A	Enable the event management function to set actions for the corresponding events.

Configure Email Servers

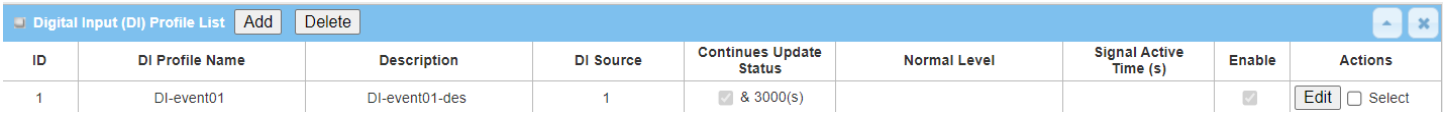
Configure emails for sending notifications.



Email Service List		
Item	**Value setting**	**Description**
Email Server	A must-filled setting	Select a pre-configured email server from the drop-down list. To configure an email server, go to **Object Definition > External Servers**.
Email Addresses	A must-filled setting	Enter the email address of the notification receipient.
Enable	The default is not eanbled.	Enable this event handling rule.
Save	N/A	Save the settings.

Digital Input (DI) Profile List

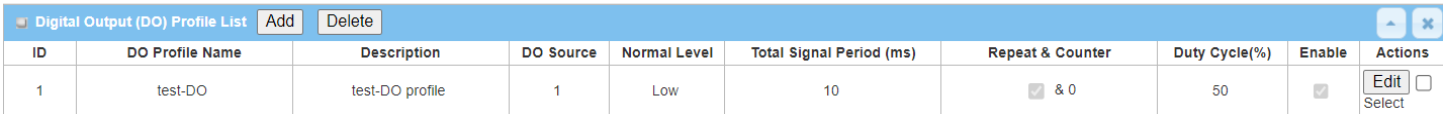
Configure DI profiles for defining conditions that can initiate event triggers.



Email Service List		
Item	**Value setting**	**Description**
DI Profile Name	A must-filled setting	Enter a name for the profile.
Description	A must-filled setting	Describes the profile for identification purposes.
DI Source	The default is ID1.	Select the digital input (DI) as the event trigger.
Continues Update Status	The default is disabled.	Enable the continuous update function to keep sending update signals in the defined interval (2~86400 seconds).
Normal Level	Low or High	Define the power level for the normal state: low or high.
Signal Active Time	The default is 1 second.	Enter the active time for the signal in seconds.
Profile	The default is enabled.	Enable or disable the DI profile.
Save	N/A	Save the settings.

Digital Output (DO) Profile List

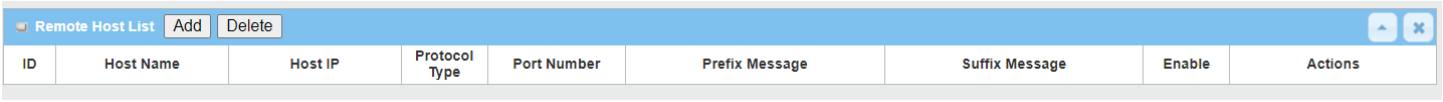
Configure profiles for Digital Output (DO) triggers for the predefined events.



Email Service List		
Item	**Value setting**	**Description**
DO Profile Name	A must-filled setting	Enter a name for the profile.
Description	A must-filled setting	Describes the profile for identification purposes.
DO Source	The default is ID1.	Select the digital output (DO) to be triggered.
Normal Level	Low or High	Define the power level for the normal state: low or high.
Total Signal Period	The default is 10 millisecond.	Enter the active time for the signal in milliseconds.
Repeat & Counter	The default is disabled.	Enter the counter and enter the number of times to send signals repeatedly.
Duty Cycle		Enter the duty cycle in percentage.
Profile	The default is enabled.	Enable or disable the DO profile.
Save	N/A	Save the settings.

Remote Host List

Configure remote hosts for sending notifications when certain events occur.



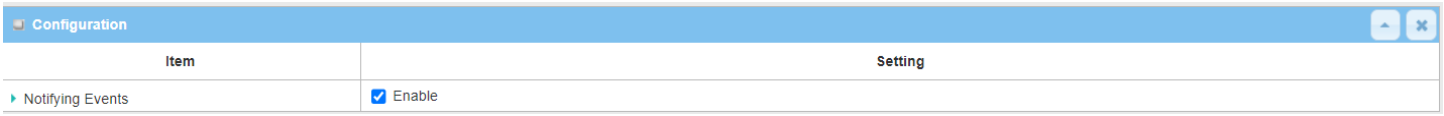
Remote Host List		
Item	**Value setting**	**Description**
Host Name	A must-filled setting	Enter a name for the remote host.
Host IP	A must-filled setting	Enter the IP address of the remote host.
Protocol Type	A must-filled setting	Select the protocol for communicating with the remote host: TCP or UDP.
Port Number	A must-filled setting	Enter the corresponding service port number for the above protocol type.
Prefix Message	A must-filled setting	Enter a messaget o proceed the notification.
Suffix Message	A must-filled setting	Enter a message to append to the end of the notification
Enable	The default is disabled.	Enable or disable the remote host.
Save	N/A	Save the settings.

7.2.2 Notifying Events

The Notifying Events page allows you to define events that will trigger corresponding actions.

Go to **Service > Event Handling> Notifying Events** to define the type of events that should generate notifications.

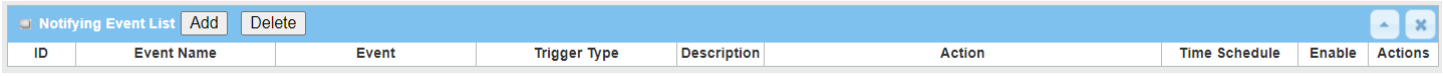
Configure Event Notifications



Configuration		
Item	**Value setting**	**Description**
Notifying Events	N/A	Enable the event notification function to set event triggers for the designated events.

Notifying Events List

Configure the events that will trigger actions configured in the Configuration page of the Event Handling (refer to **7.2.1 Configuration**).



Click **Add** to add a new event trigger:

Notifying Event Configuration		
Item	**Value setting**	**Description**
Event Name	A must-filled setting	Enter a name for the event.
Event	A must-filled setting	Select the event trigger. For Digitnal Input, configure a DI profile first in the Configuration page firs (refer to **7.2.1 Configuration**). For Administration category, the following events can be selected: Login Fail by Web, Login Fail by Telnet, Login Fail by SSH, System Password Changed, FW Upgrade is under

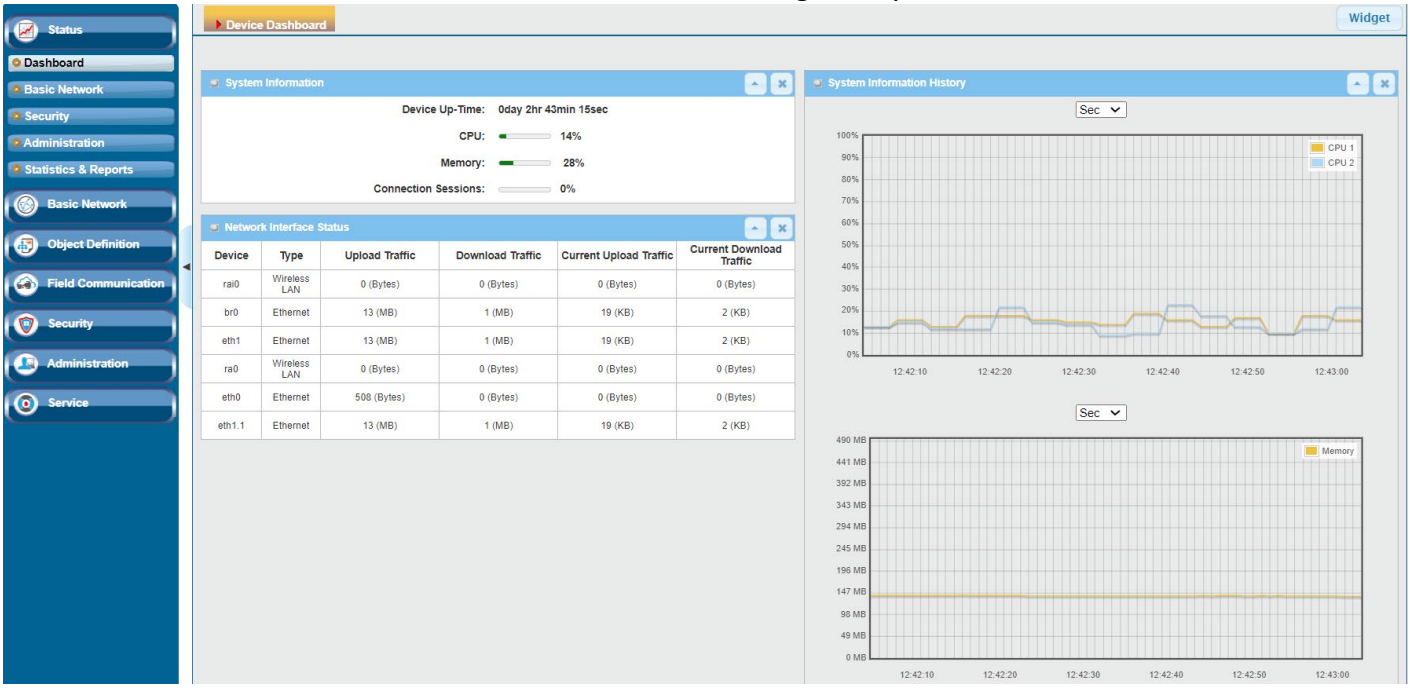
		Processing. For system category, the following events can be selected: System heavy duty (>90%) and system memory low (<10%) for 5 times in a row and with each event lasts for 10 seconds.
Trigger Type	A must-filled setting	Select the triggering frequency: Period or Once.
Interval	A must-filled setting	Select the interval in seconds if triggering periodically (0~86400 seconds)
Description	A must-filled setting	Enter a description for the event notification message.
Action	A must-filled setting	Enter the corresponding action for an event trigger. Refer to **7.2.1 Configuration** for the configured event management actions. For the System category, you can select the reboot function to reboot the system after 30 seconds.
Notifying Events	The default is enabled.	Enable or disable event notification.
Save	N/A	Save the settings.
Undo	N/A	Discard the settings.

Chapter 8 Status

8.1 Dashboard

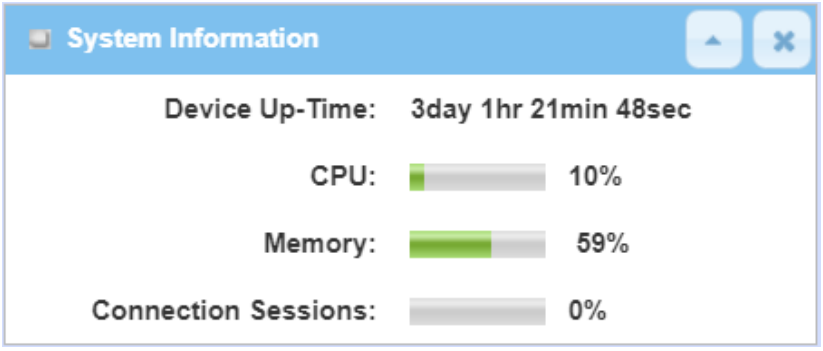
The Device Dashboard window shows the status in graph or tables for a quick overview of the operation status of the gateway. The display will be refreshed very second.

Go to **Status > Dashboard > Device Dashboard** to access the gateway status.



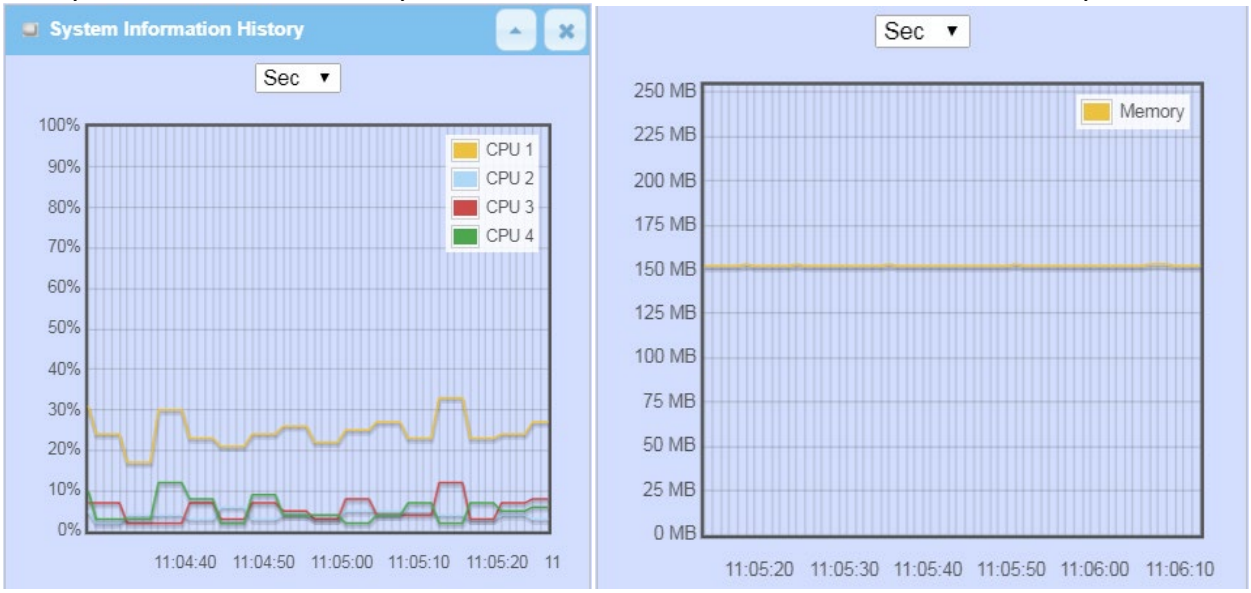
System Information Status

The System Information screen shows the device uptime and the resource utilization of the CPU, memory, and connection sessions.



System Information History

The System Information History screen shows the statistics for the CPU and memory.



Network Interface Status

The Network Interface Status screen shows the statistics for each network interface of the gateway. The information includes the Interface Type, Upload Traffic (total), Download Traffic (total), 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)

8.2 Basic Network

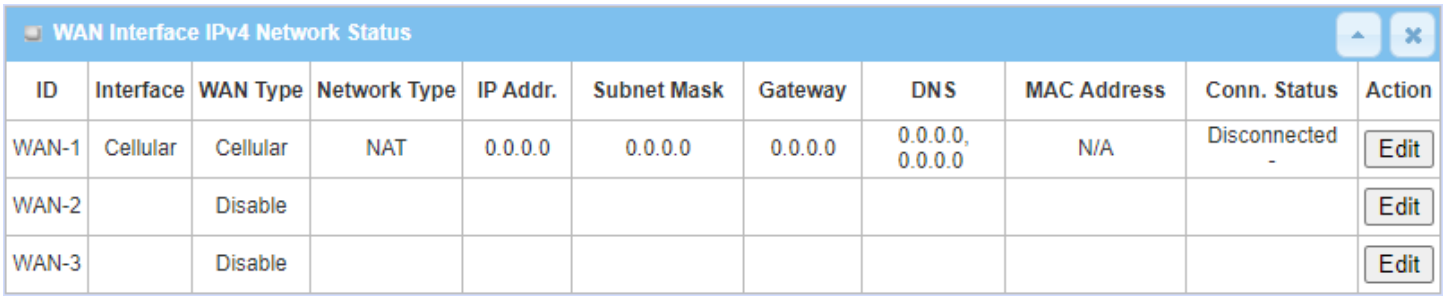
8.2.1 WAN & Uplink Status

The WAN & Uplink Status window shows the current status for different network types, including network configuration, connection information, modem status, and traffic statistics. The display will be refreshed every 5 seconds.

Go to **Status > Basic Network > WAN & Uplink** to access the connection status information.

WAN Interface IPv4 Network Status

The WAN interface IPv4 Network Status screen shows status information about IPv4 network.



WAN Interface IPv4 Network Status

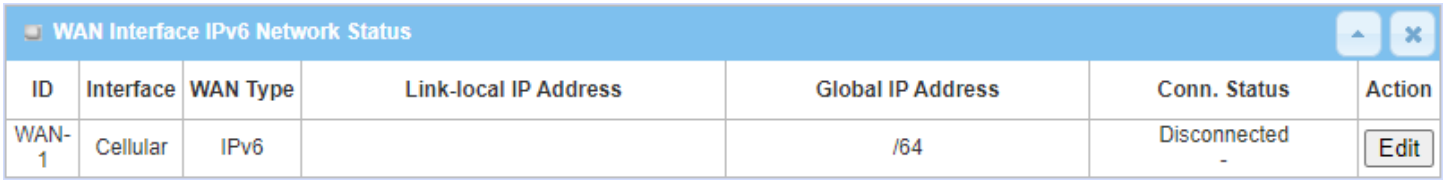
ID	Interface	WAN Type	Network Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Action
WAN-1	Cellular	Cellular	NAT	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	N/A	Disconnected -	Edit
WAN-2		Disable								Edit
WAN-3		Disable								Edit

WAN interface IPv4 Network Status		
Item	**Value setting**	**Description**
ID	N/A	Displays corresponding WAN interface WAN IDs.
Interface	N/A	Displays the type of WAN physical interface. It can be Ethernet or Cellular depending on the device model.
WAN Type	N/A	Displays the method the public IP address is obtained from your ISP. It can be Static IP, Dynamic IP, PPPoE, PPTP, L2TP, Cellular depending on the device model.
Network Type	N/A	Displays the network type for the WAN interface(s). It can be NAT, Routing, Bridge, or IP Pass-through depending on the device model.
IP Addr.	N/A	Displays the public IP address obtained from your ISP for Internet connection. The default value is 0.0.0.0.
Subnet Mask	N/A	Displays the Subnet Mask for the public IP address obtained from your ISP for Internet connection. The default value is 0.0.0.0.
Gateway	N/A	Displays the gateway IP address obtained from your ISP for Internet connection. The default value is 0.0.0.0.
DNS	N/A	Displays the IP address of DNS server obtained from your ISP for Internet connection. The default value is 0.0.0.0.
MAC Address	N/A	Displays the MAC Address required by your ISP for Internet access. Not all ISPd require this information.
Conn. Status	N/A	Displays the connection status with your ISP.
Action	N/A	This area provides functional buttons. **Renew** button gets an IP address from a DHCP server.

	Note: Renew button is available when DHCP WAN Type is configured as the connection type and the WAN connection is disconnected. **Release** button clears the current IP address setting. **Note: Renew** button is available when DHCP WAN Type is configured as the connection type and the WAN connection status is disconnected. **Connect** button manually connect the device to the Internet. **Note**: Connect button is available when **Connect Manually** is set as the Connection Control in WAN Type setting (go to **Basic Network > WAN & Uplink > Internet Setup**) and WAN connection status is disconnected. **Disconnect** button disconnects the device from the Internet. **Note: Disconnect** button is available when **Connect Manually** is set as the Connection Control in WAN Type setting (go to **Basic Network > WAN & Uplink > Internet Setup**) and WAN connection status is disconnected.

WAN Interface IPv6 Network Status

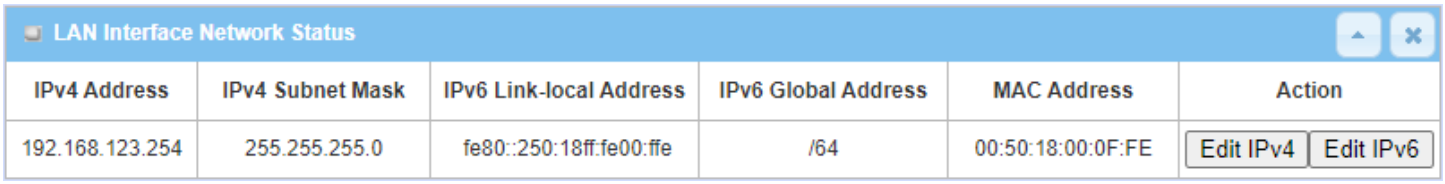
The **WAN interface IPv6 Network Status** screen shows status information about IPv6 network.



WAN interface IPv6 Network Status		
Item	**Value setting**	**Description**
ID	N/A	Displays corresponding WAN interface WAN IDs.
Interface	N/A	Displays the type of WAN physical interface. It can be Ethernet or Cellular depending on the device model.
WAN Type	N/A	Displays the method that the public IP address is obtained from your ISP: Static IP, Dynamic IP, PPPoE, PPTP, L2TP, or Cellular. The types depend on the device model.
Link-local IP Address	N/A	Displays the LAN IPv6 Link-Local address.
Global IP Address	N/A	Displays the IPv6 global IP address assigned by your ISP for your Internet connection.
Conn. Status	N/A	Displays the connection status. The status can be connected, disconnected, or connecting.
Action	N/A	This area provides functional buttons. Click the **Edit Button** to go to the IPv6 configuration page. (**Basic Network > IPv6 > Configuration**.)

LAN Interface Network Status

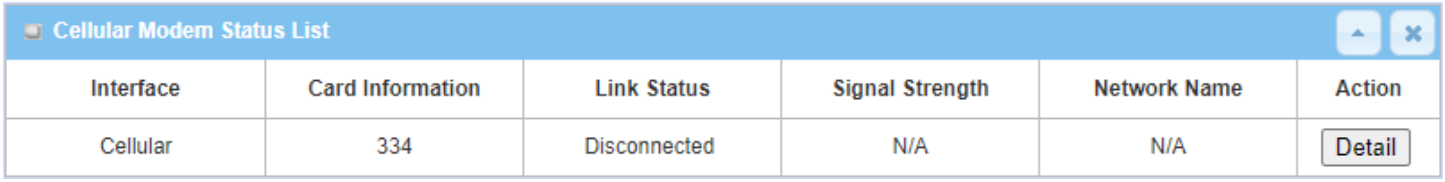
The **LAN Interface Network Status** screen shows IPv4 and IPv6 information of LAN network.



LAN Interface Network Status		
Item	**Value setting**	**Description**
IPv4 Address	N/A	Displays the current IPv4 IP Address of the gateway. This is also the IP Address for accessing the gateway's Web UI.
IPv4 Subnet Mask	N/A	Displays the current mask of the subnet.
IPv6 Link-local Address	N/A	Displays the current LAN IPv6 Link-Local address. This is also the IPv6 IP Address for accessing the gateway's Web UI.
IPv6 Global Address	N/A	Displays the current IPv6 global IP address assigned by your ISP for your Internet connection.
MAC Address	N/A	Displays the LAN MAC Address of the gateway
Action	N/A	This area provides functional buttons. Click the **Edit IPv4** Button to go to the Ethernet LAN configuration page (**Basic Network > LAN & VLAN > Ethernet LAN**). Click the **Edit IPv6** Button to go to the IPv6 configuration page (**Basic Network > IPv6 > Configuration**.)

Cellular Modem Status

The **Cellular Modem Status List** screen shows the status information for Cellular WAN network(s).

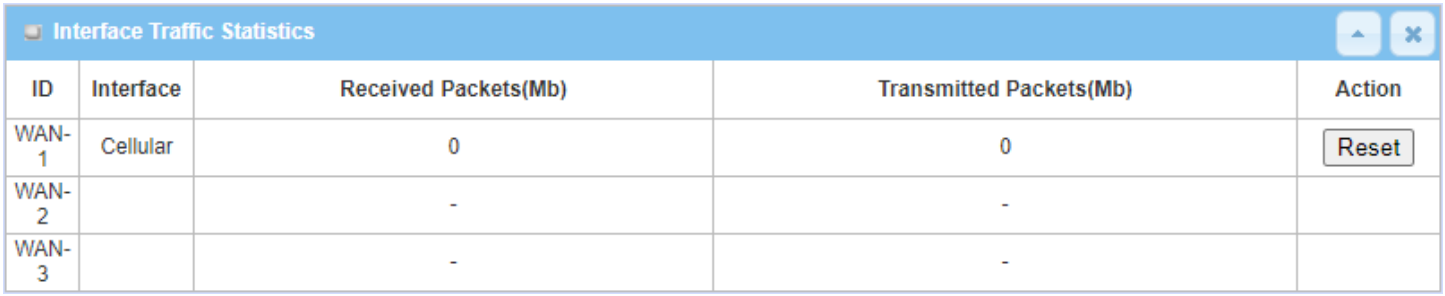


5G/LTE Modem Status List		
Item	**Value setting**	**Description**
Physical Interface	N/A	Displays the type of WAN physical interface.
Card Information	N/A	Displays the vendor's cellular modem model.
Link Status	N/A	Displays the cellular connection status. The status can be Connecting, Connected, Disconnecting, or Disconnected.
Signal Strength	N/A	Displays the cellular wireless signal level.
Network Name	N/A	Displays the name of the service network carrier.
Refresh	N/A	Click the **Refresh** button to renew the information.
Action	N/A	This area provides functional buttons. Click **Detail Button** to display detailed information: Modem Information, SIM Status, and Service Information.

Click **Detail** to display modem Information, SIM Status, Service Information, Signal Strength / Quality, and Error Message.

Interface Traffic Statistics

The **Interface Traffic Statistics** screen displays the Interface's total transmitted packets.



Interface Traffic Statistics		
Item	**Value setting**	**Description**
ID	N/A	Displays corresponding WAN interface's WAN IDs.
Interface	N/A	Displays the type of WAN physical interface. It can be Ethernet or Cellular depending on the device model.
Received Packets (Mb)	N/A	Displays the downstream packets (Mb). It will reset when the device is rebooted.
Transmitted Packets (Mb)	N/A	Displays the upstream packets (Mb). It will reset when the device is rebooted.

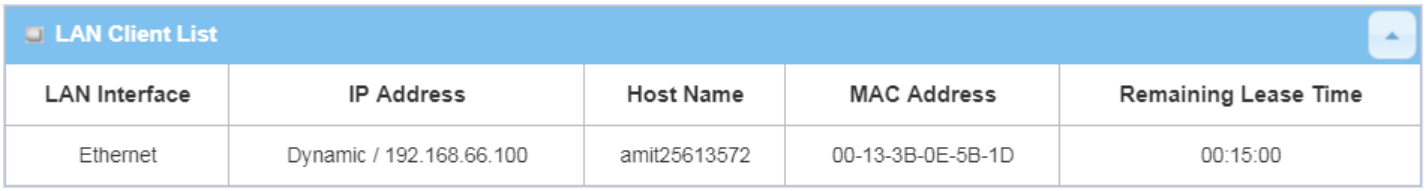
8.2.2 LAN & VLAN Status

The **LAN & Uplink Status** window shows the LAN clients' information, including network configuration and DHCP lease information. The display will be refreshed every 5 seconds.

Go to **Status > Basic Network > LAN & VLAN** to access the status page.

Client List

The Client List shows you the LAN Interface, IP address, Host Name, MAC Address, and Remaining Lease Time of all client devices connected to this gateway.



LAN Client List

LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time
Ethernet	Dynamic / 192.168.66.100	amit25613572	00-13-3B-0E-5B-1D	00:15:00

LAN Client List Item	Value setting	Description
LAN Interface	N/A	Displays the client's LAN Interface.
IP Address	N/A	Displays the client's IP Address in IPv4 Format.
Host Name	N/A	Displays the client's Host Name.
MAC Address	N/A	Displays the client's MAC Address.
Remaining Lease Time	N/A	Displays the client's Remaining Lease Time for DHCP.

8.2.3 Wi-Fi Status

The Wi-Fi Status window shows the overall statistics of Wi-Fi VAP entries.

Go to **Status > Basic Network > Wi-Fi** to access the Wi-Fi status page.

Wi-Fi Virtual AP List

The Wi-Fi Virtual AP List shows all the virtual AP information on each Wi-Fi module. The Edit button allows for quick configuration changes. The QR Code can be used for quick connection of the selected wireless network.

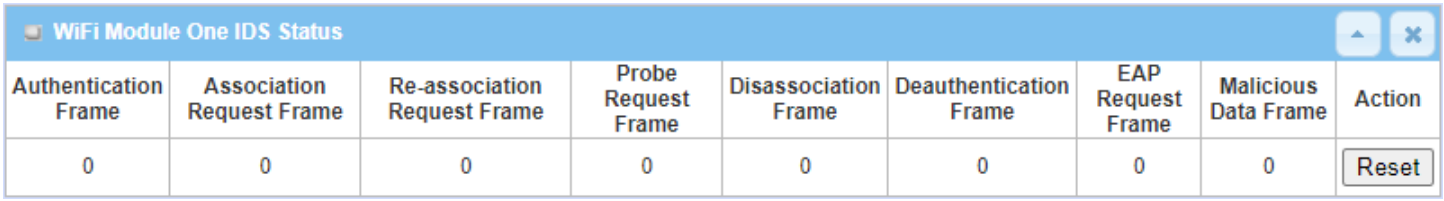
WiFi Module One Virtual AP List

Op. Band	ID	WiFi Enable	Op. Mode	SSID	Channel	WiFi System	Auth.&Security	MAC Address	Action
2.4G	VAP-1	☑	AP Router	Staff_2.4G	Auto(3)	b/g/n Mixed	WPA2-PSK(AES)	00:50:18:00:07:F0	Edit QR Code
2.4G	VAP-2	☐	AP Router	default	Auto(3)	b/g/n Mixed	WPA2-PSK(AES)	02:50:18:10:07:F0	Edit QR Code
2.4G	VAP-3	☐	AP Router	default	Auto(3)	b/g/n Mixed	WPA2-PSK(AES)	02:50:18:20:07:F0	Edit QR Code
2.4G	VAP-4	☐	AP Router	default	Auto(3)	b/g/n Mixed	WPA2-PSK(AES)	02:50:18:30:07:F0	Edit QR Code
2.4G	VAP-5	☐	AP Router	default	Auto(3)	b/g/n Mixed	WPA2-PSK(AES)	02:50:18:40:07:F0	Edit QR Code
2.4G	VAP-6	☐	AP Router	default	Auto(3)	b/g/n Mixed	WPA2-PSK(AES)	02:50:18:50:07:F0	Edit QR Code
2.4G	VAP-7	☐	AP Router	default	Auto(3)	b/g/n Mixed	WPA2-PSK(AES)	02:50:18:60:07:F0	Edit QR Code
2.4G	VAP-8	☐	AP Router	Guest_2.4G	Auto(3)	b/g/n Mixed	WPA2-PSK(AES)	02:50:18:70:07:F0	Edit QR Code

Wi-Fi Virtual AP List		
Item	**Value setting**	**Description**
Op. Band	N/A	Displays the Wi-Fi Operation Band (2.4G or 5G) of VAP.
ID	N/A	Displays the ID of VAP.
Wi-Fi Enable	N/A	Displays whether the VAP wireless signal is enabled or disabled.
Op. Mode	N/A	Displays the Wi-Fi Operation Mode of VAP.
SSID	N/A	Displays the network ID of VAP.
Channel	N/A	Displays the wireless channel used.
Wi-Fi System	N/A	The supported Wi-Fi standards of the VAP.
Auth. & Security	N/A	Displays the authentication and encryption type used.
MAC Address	N/A	Displays MAC Address of VAP.
Action	N/A	Click the **Edit** button to go to the Wi-Fi configuration page (go to **Basic Network > Wi-Fi > Configuration** tab). The **QR Code** button allows you to generate a QR code for quick connect to the VAP by scanning the QR code.

Wi-Fi IDS Status

The Wi-Fi IDS Status shows all the wireless intrusion detection system (WIDS) statistics on each Wi-Fi module.



Wi-Fi IDS Status		
Item	**Value setting**	**Description**
Authentication Frame	N/A	Displays the number of Authentication Frame received.
Association Request Frame	N/A	Displays the number of Association Request Frame received.
Re-association Request Frame	N/A	Displays the number of Re-association Request Frame received.
Probe Request Frame	N/A	Displays the number of Probe Request Frame received.
Disassociation Frame	N/A	Displays the number of Disassociation Frame received.
Deauthentication Frame	N/A	Displays the number of Deauthentication Frame received.
EAP Request Frame	N/A	Displays the number of EAP Request Frame received.
Malicious Data Frame	N/A	Displays the number of unauthorized wireless packets received.
Action	N/A	Click the **Reset** button to clear the statistics and reset the counter to 0.

To enable WIDS, go to **Basic Network > WiFi > Advanced Configuration** and configure the WIDS function for 2.4 GHz and 5 GHz Operation Band separately.

Wi-Fi Traffic Statistics

The Wi-Fi Traffic Statistic shows all the received and transmitted packets on each Wi-Fi module.

WiFi Module One Traffic Statistics

Op. Band	ID	Received Packets	Transmitted Packets	Action
2.4G	VAP-1	11592	3617	Reset
2.4G	VAP-2	0	0	Reset
2.4G	VAP-3	0	0	Reset
2.4G	VAP-4	0	0	Reset
2.4G	VAP-5	0	0	Reset
2.4G	VAP-6	0	0	Reset
2.4G	VAP-7	0	0	Reset
2.4G	VAP-8	0	0	Reset

Wi-Fi Traffic Statistic		
Item	**Value setting**	**Description**
Op. Band	N/A	Displays the Wi-Fi Operation Band (2.4G or 5G) of VAP.
ID	N/A	Displays the VAP ID.
Received Packets	N/A	Displays the number of reveived packets.
Transmitted Packet	N/A	Displays the number of transmitted packets.
Action	N/A	Click the **Reset** button to clear individual VAP statistics.
Refresh Button	N/A	Click the **Refresh** button to update the VAP Traffic Statistics instantly.

8.2.4 DDNS Status

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.

Go to **Status > Basic Network > DDNS** to access the DDNS Status page.

DDNS Status



DDNS Status Item	Value Setting	Description
Host Name	N/A	Displays the host name for DDNS.
Provider	N/A	Displays the DDNS server (or service provider).
Effective IP	N/A	Displays the public IP address updated to the DDNS server
Last Update Status	N/A	Displays whether the last update of the device's public IP address to the DDNS server has been successful (Ok) or failed (Fail).
Last Update Time	N/A	Displays the timestamp of the last update of public IP address to the DDNS server.
Refresh	N/A	Rrefresh the information.

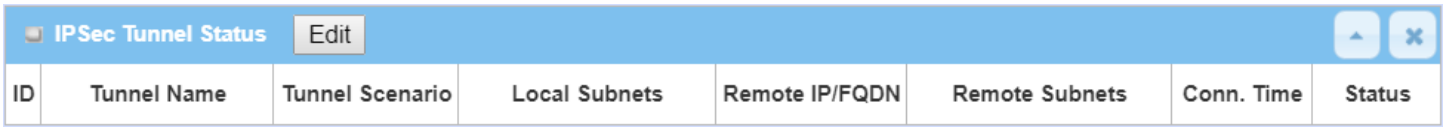
8.3 Security

8.3.1 VPN Status

The VPN Status widow shows the VPN connection status. The display will be refreshed every five seconds. Go to **Status > Security > VPN** to access VPN status page.

IPSec Tunnel Status

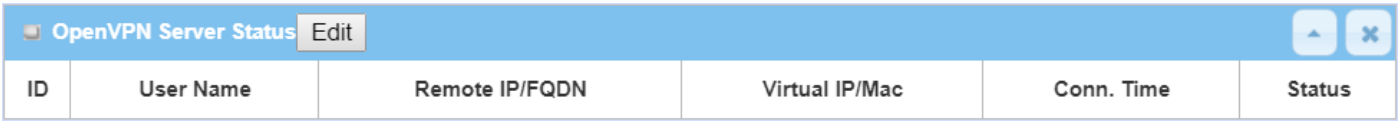
The IPSec Tunnel Status window displays the tunnel status of the established IPSec VPN connection and the current connection status. To configure IPSec VPN, go to **Security > VPN** and select the **IPSec tab**.



IPSec Tunnel Status		
Item	**Value setting**	**Description**
Tunnel Name	N/A	Displays the tunnel name.
Tunnel Scenario	N/A	Displays the tunnel scenario: Tunnel or Transport mode.
Local Subnets	N/A	Displays the local subnets of the VPN tunnel.
Remote IP/FQDN	N/A	Displays the remote IP/FQDN of the VPN tunnel.
Remote Subnets	N/A	Displays the remote subnets of the VPN tunnel.
Conn. Time	N/A	Displays the connection time of the IPSec tunnel.
Status	N/A	Displays the status of the VPN connection: Connected, Disconnected, Wait for traffic, or Connecting.
Edit Button	N/A	Click **Edit** to change the IPSec setting. You will be directed to the IPSec configuration page (go to **Security > VPN > IPSec**).

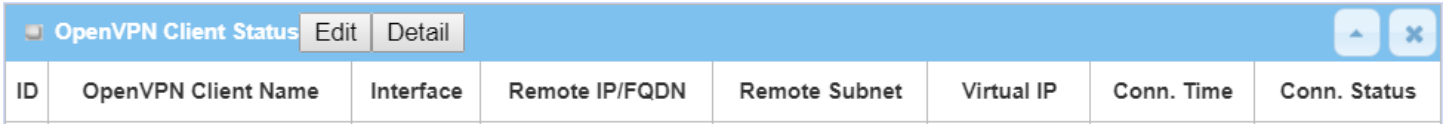
OpenVPN Server Status

The OpenVPN Server/Client Status shows the status and statistics of the OpenVPN connection. To configure IPSec VPN, go to **Security > VPN** and select the **OpenVPN tab**.



OpenVPN Server Status		
Item	**Value setting**	**Description**
Username	N/A	Displays the client's name.
Remote IP/FQDN	N/A	Displays the public IP address (the WAN IP address) of the connected OpenVPN client.
Virtual IP/MAC	N/A	Displays the virtual IP/MAC address assigned to the connected OpenVPN client.
Conn. Time	N/A	Displays the connection time of the OpenVPN tunnel.
Status	N/A	Displays the connection status of the OpenVPN tunnel: Connected or Disconnected.

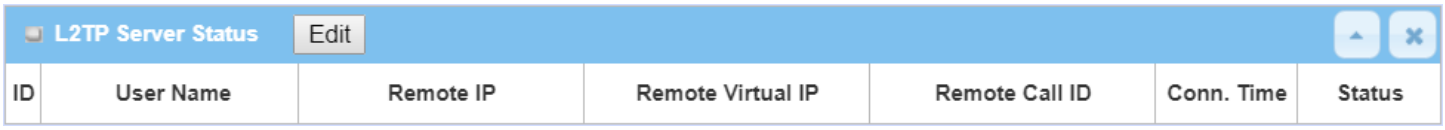
OpenVPN Client Status



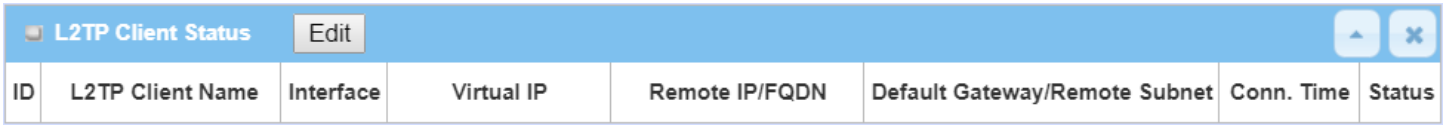
OpenVPN Client Status		
Item	**Value setting**	**Description**
OpenVPN Client Name	N/A	Displays the client's name.
Interface	N/A	Displays the WAN interface configured for the OpenVPN client connection.
Remote IP/FQDN	N/A	Displays the peer OpenVPN server's public IP address (the WAN IP address) or FQDN.
Remote Subnet	N/A	Displays the remote subnet of the OpenVPN tunnel.
TUN/TAP Read(bytes)	N/A	Click **Detail** to display the TUN/TAP read bytes of OpenVPN client.
TUN/TAP Write(bytes)	N/A	Click **Detail** to display the TUN/TAP write bytes of OpenVPN client.
TCP/UDP Read(bytes)	N/A	Click **Detail** to display the TCP/UDP read bytes of OpenVPN client.
TCP/UDP Write(bytes)	N/A	Click **Detail** to display the TCP/UDP write bytes of the OpenVPN client.
Conn. Time	N/A	Displays the connection time of the OpenVPN tunnel.
Conn. Status	N/A	Displays the connection status of the OpenVPN tunnel: Connected or Disconnected.

L2TP Server/Client Status

The LT2TP Server/Client Status shows the connection status of the established L2TP tunnels.



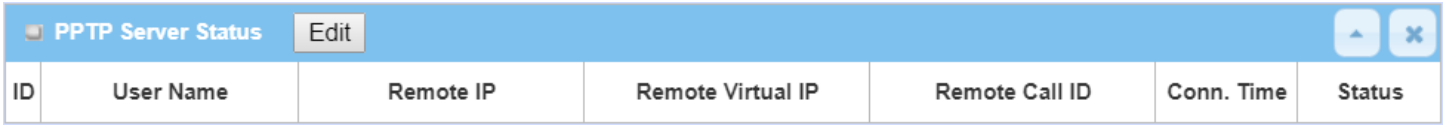
L2TP Server Status		
Item	**Value setting**	**Description**
Username	N/A	Displays the login name of the user.
Remote IP	N/A	Displays the public IP address (the WAN IP address) of the connected L2TP client.
Remote Virtual IP	N/A	Displays the IP address assigned to the connected L2TP client.
Remote Call ID	N/A	Displays the L2TP client Call ID.
Conn. Time	N/A	Displays the connection time of the L2TP tunnel.
Status	N/A	Displays the Status of each of the L2TP client connection: Connected, Disconnect, Connecting.
Edit	N/A	Click **Edit** to change L2TP server setting. You will be directed to the L2TP server page (go to **Security > VPN > L2TP**).



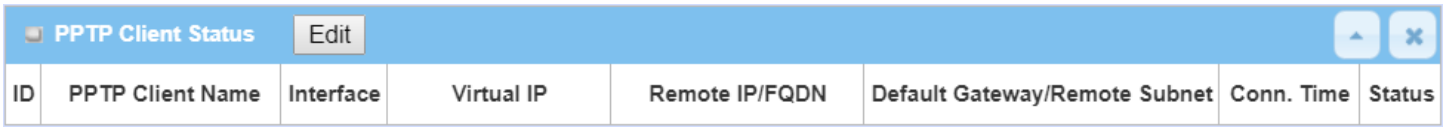
L2TP Client Status Item	Value setting	Description
Client Name	N/A	Displays the name of the L2TP client.
Interface	N/A	Displays the WAN interface activated with the PPTP tunneling connection.
Virtual IP	N/A	Displays the IP address assigned by the virtual L2TP server.
Remote IP/FQDN	N/A	Displays the L2TP Server's public IP address (the WAN IP address) or FQDN.
Default gateway/Remote Subnet	N/A	Displays the IP address of the gateway device used to connect to an L2TP server – the default gateway. Or a subnet if the default gateway is not used to connect to an L2TP server – the remote subnet.
Conn. Time	N/A	Displays the connection time for the L2TP tunnel.
Status	N/A	Displays the status of the VPN connection: Connected, Disconnect, and Connecting.
Edit	N/A	Click on **Edit** Button to change L2TP client setting. You will be directed to the L2TP client page (**Security > VPN > L2TP**).

PPTP Server/Client Status

The PPTP Server/Client Status shows the connection status of the established PPTP tunnel.



PPTP Server Status		
Item	**Value setting**	**Description**
Username	N/A	Displays the login name of the user for connection.
Remote IP	N/A	Displays the public IP address (the WAN IP address) of the connected PPTP client.
Remote Virtual IP	N/A	Displays the IP address assigned to the connected PPTP client.
Remote Call ID	N/A	Displays the PPTP client Call ID.
Conn. Time	N/A	Displays the connection time for the PPTP tunnel.
Status	N/A	Displays the status of each PPTP client connection: Connected, Disconnect, and Connecting.
Edit Button	N/A	Click **Edit** to change PPTP server setting. You will be directed to the PPTP configuration page (**Security > VPN > PPTP**).



PPTP Client Status		
Item	**Value setting**	**Description**
Client Name	N/A	Displays the PPTP client's name.
Interface	N/A	Displays the WAN interface activated with the PPTP tunneling connection.
Virtual IP	N/A	Displays the IP address assigned by the virtual L2TP 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	Displays the IP address of the gateway device used to connect to an L2TP server – the default gateway. Or a subnet if the default gateway is not used to connect to an L2TP server – the remote subnet.
Conn. Time	N/A	Displays the connection time of the PPTP tunnel.
Status	N/A	Displays the status of the VPN connection: Connected, Disconnect, or Connecting.
Edit Button	N/A	Click **Edit** to change PPTP client setting. You will be directed to the PPTP configuration page (**Security > VPN > PPTP**).

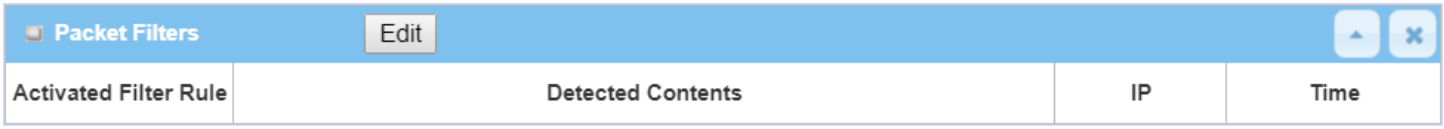
8.3.2 Firewall Status

The Firewall Status provides a quick view of the firewall status and current firewall settings. It also keeps a log history of the dropped packets or blocked websites or MAC addresses by the firewall rules, including the admin's remote login settings. The display will be refreshed every five seconds.

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

Click the icon [+] to display log history. Click the Edit button to display the configuration page.

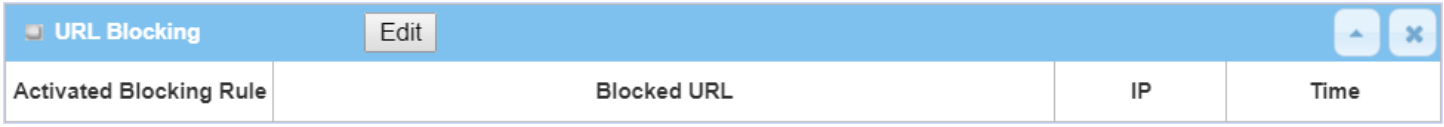
Packet Filter Status



Packet Filter Status		
Item	**Value setting**	**Description**
Activated Filter Rule	N/A	The name of the packet filter rule.
Detected Contents	N/A	This is the logged packet information, including the source IP, destination IP, protocol, and destination port –the TCP or UDP in the following 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 timestamp of the logged packet in the Date & time format ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure **Packet Filter Log Alert** is enabled (go to **Security > Firewall > Packet Filter**).

URL Blocking Status



URL Blocking Status		
Item	**Value setting**	**Description**
Activated Blocking Rule	N/A	This name of the URL blocking rule.
Blocked URL	N/A	This is the logged URL information.
IP	N/A	The Source IP (IPv4) of the blocked URL connection.
Time	N/A	The timestamp of the logged URL connection in the Date & time format ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure URL Blocking is enabled (go to **Security > Firewall > URL Blocking**).

MAC Control Status



MAC Control Status		
Item	**Value setting**	**Description**
Activated Control Rule	N/A	The name of the MAC control rule.
Blocked MAC Addresses	N/A	The MAC address of the logged packets.
IP	N/A	The source IP (IPv4) of the logged packets.
Time	N/A	The timestamp of the logged packet in the Date & time format ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure **MAC Control Status** is enabled (go to **Security > Firewall > MAC Control**).

IPS Status



IPS Firewall Status		
Item	**Value setting**	**Description**
Detected Intrusion	N/A	This violation type of IPS.
IP	N/A	The source IP (IPv4) address of the logged packets.
Time	N/A	The timestamp of the logged packet in the Date time format ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure IPS Log Alert is enabled (go to **Security > Firewall > IPS**).

Firewall Options Status



Firewall Options Status		
Item	**Value setting**	**Description**
Stealth Mode	N/A	The status of the Stealth Mode of the firewall.
SPI	N/A	The status of SPI of the firewall.
Discard Ping from WAN	N/A	The status of Discard Ping from WAN of the firewall.
Remote Administrator Management	N/A	The status of Remote Administrator. If Remote Administrator is enabled, it will display the currently logged in administrator's source IP address and username as well as the login time.

Note: Ensure **Firewall Options Log Alert** is enabled (go to **Security > Firewall > Options**).

8.4 Administration

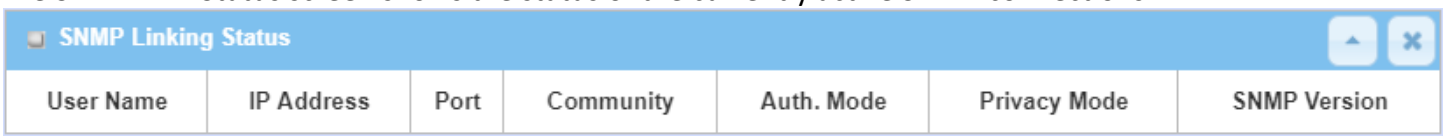
8.4.1 Configure & Manage Status

The Configure & Manage Status window shows the status of remote management. The set of management features depends on the device model. The display will be refreshed on every five seconds.

Go to **Status > Administration > Configure & Manage** to access the Configure & Manage Status page.

SNMP Linking Status

The SNMP Link Status screen shows the status of the currently active SNMP connections.



SNMP Link Status Item	Value setting	Description
Username	N/A	Displays the username for authentication. This is only available for SNMP version 3.
IP Address	N/A	Displays the IP address of the SNMP manager.
Port	N/A	Displays the port number used for connecting with the SNMP manager.
Community	N/A	Displays the community name for SNMP version 1 or version 2c only.
Auth. Mode	N/A	Displays the authentication method required for SNMP version 3 only.
Privacy Mode	N/A	Displays the privacy mode required for version 3 only.
SNMP Version	N/A	Displays the SNMP version.

SNMP Trap Information

The SNMP Trap Information screen shows SNMP traps received.



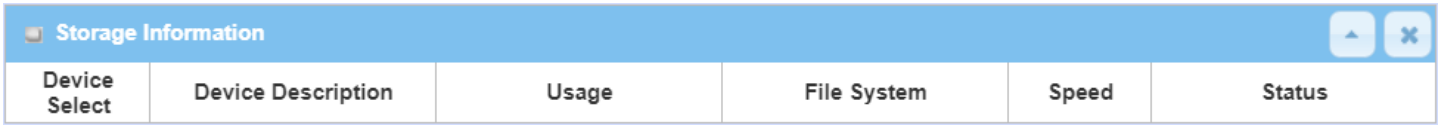
SNMP Trap Information Item	Value setting	Description
Trap Level	N/A	Displays the trap level.
Time	N/A	Displays the timestamp of trap event.
Trap Event	N/A	Displays the IP address of the trap sender and event type.

8.4.2 Log Storage Status

The **Log Storage Status** screen shows the information of device storage, such as the file system type and data speed.

Go to **Status > Administration > Log Storage** to access the Log Storage page.

Log Storage Status

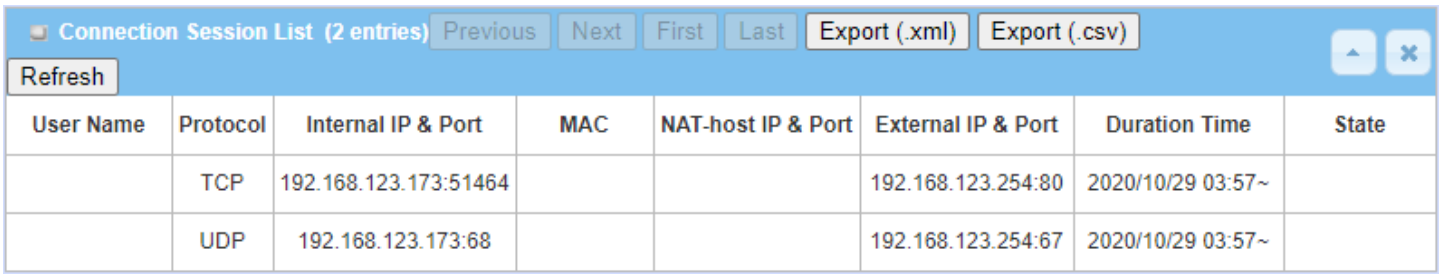


8.5 Statistics & Report

8.5.1 Connection Session

The Connection Session List shows the connection history of devices through the gateway.

Go to **Status > Statistics & Reports > Connection Session** to access the connection history page.



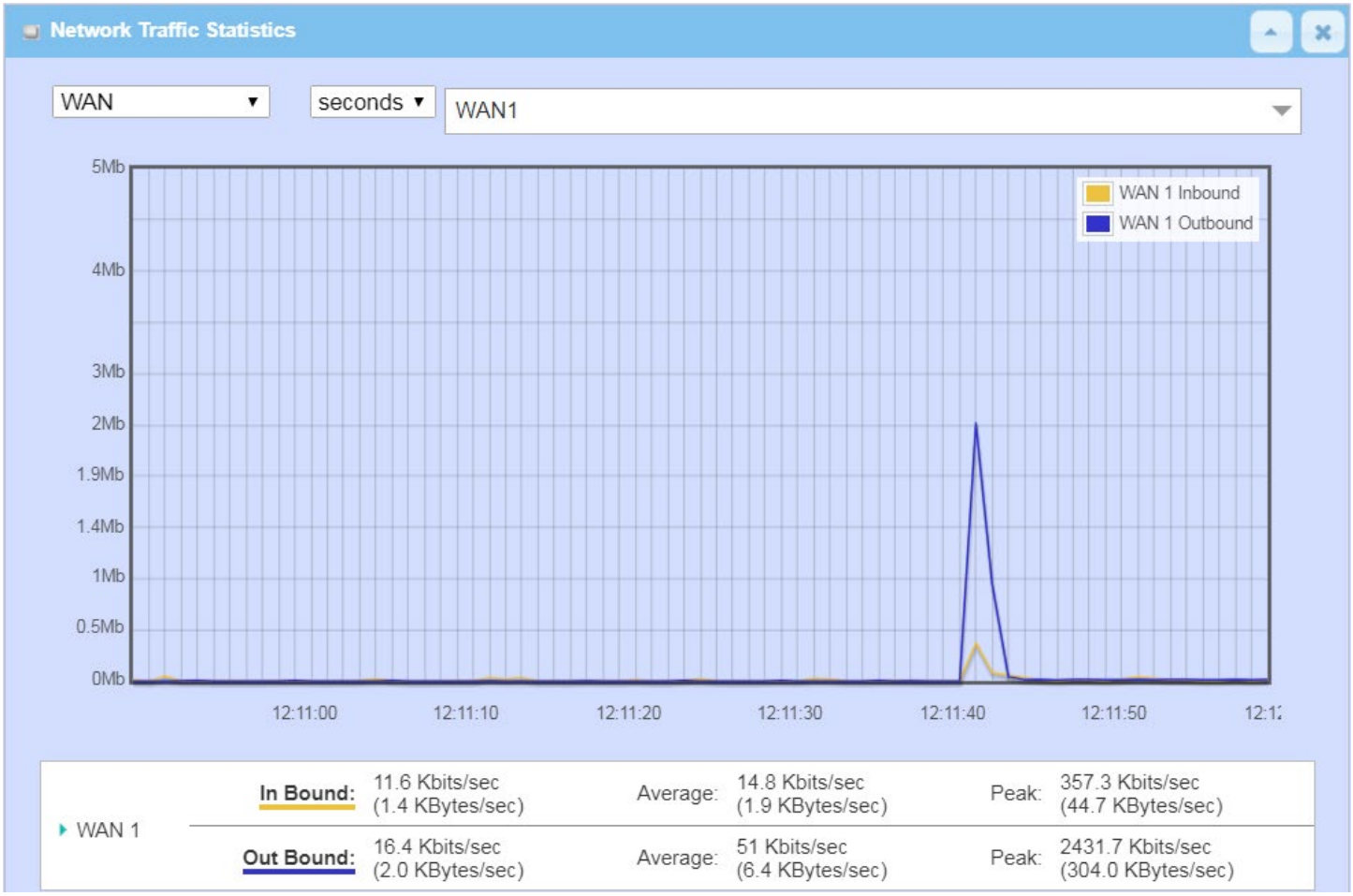
Connection Session List		
Item	**Value setting**	**Description**
Previous	N/A	Click **Previous** to view the previous page of the connection history.
Next	N/A	Click **Next** to view the next page of the connection history.
First	N/A	Click **First** to view the first page of the connection history.
Last	N/A	Click **Last** to view the last page of the connection history.
Export (.xml)	N/A	Click **Export (.xml)** to export the list as an xml file.
Export (.csv)	N/A	Click **Export (.csv)** to export the list as a csv file.
Refresh	N/A	Click **Refresh** to refresh the list.

8.5.2 Network Traffic

Network Traffic Statistics screen shows the status and statistics of the interfaces of the gateway.

Go to **Status > Statistics & Reports > Network Traffic** to access the Network Traffic Statistics page.

Select the interface list and the sampling time unit.

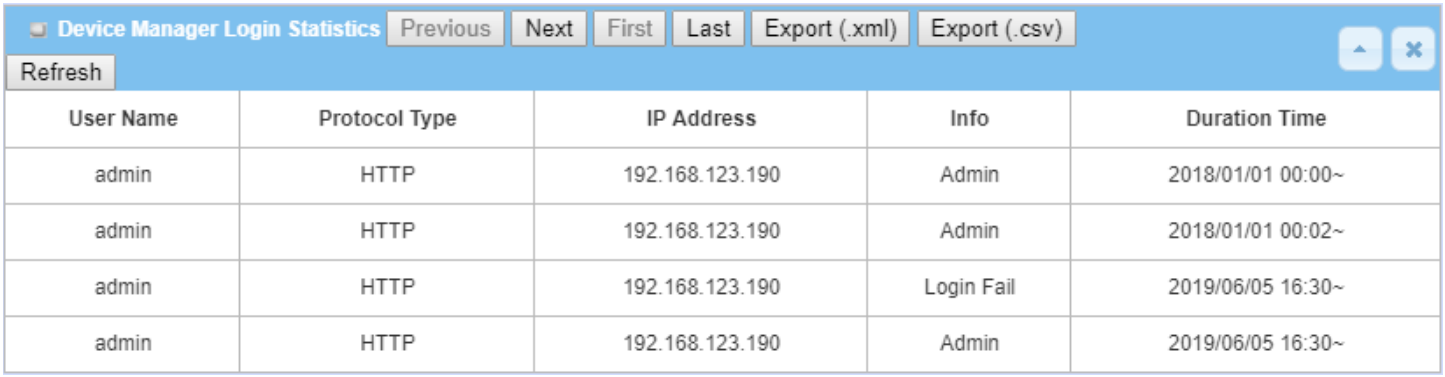


8.5.3 Login Statistics

The Login Statistics screen shows the login history.

Go to **Status > Statistics & Reports > Login Statistics** to access the login history of the gateway.

s



Device Manager Login Statistic		
Item	**Value setting**	**Description**
Previous	N/A	Click **Previous** to view the previous page of login details.
Next	N/A	Click **Next** to view the the next page of login details.
First	N/A	Click **First** to view the first page of login details.
Last	N/A	Click **Last** to view the last page of login details.
Export (.xml)	N/A	Click **Export (.xml)** to export the login history as an xml file.
Export (.csv)	N/A	Click **Export (.csv)** to export the login history as an csv file.
Refresh	N/A	Click **Refresh** to refresh the login history.

8.5.4 Cellular Usage

The Cellular Usage screen shows statistics of cellular data usage. The cellular data usage can be presented by hour or by day.

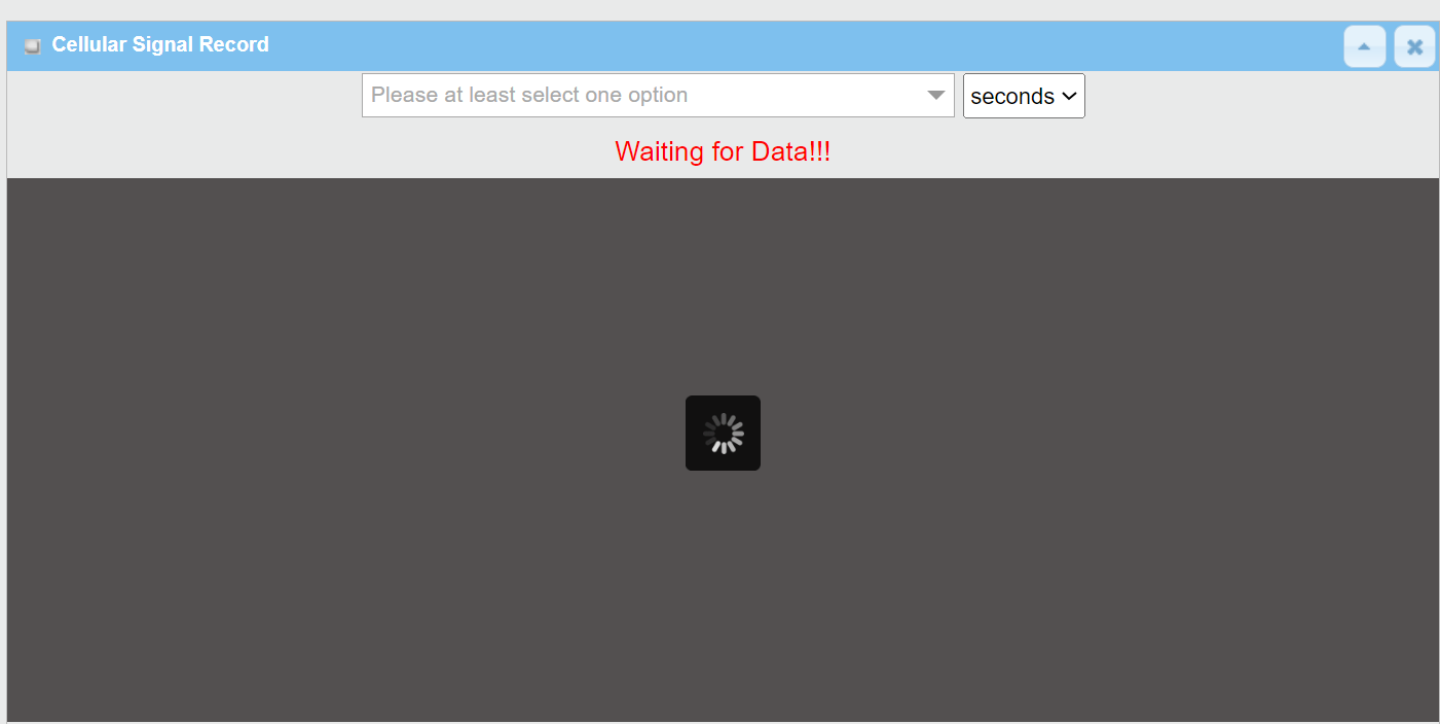
Go to Status > Statistics & Reports > Cellular Usage to access the Cellular Usage page.



8.5.5 Cellular Signal

The Cellular Signal screen shows information about cellular signal quality. The information can be presented by seconds, minutes, or hours.

Go to **Status > Statistics & Reports > Cellular Signal** to access the Cellular Signal page.



Regulatory Information

European Community Declaration of Conformity:

Česky [Czech]	Tímto D-Link Corporation prohlašuje, že tento produkt, jeho příslušenství a software jsou v souladu se směrnicí 2014/53/EU. Celý text ES prohlášení o shodě vydaného EU a o firmwaru produktu lze stáhnout na stránkách k produktu www.dlink.com.
Dansk [Danish]	D-Link Corporation erklærer herved, at dette produkt, tilbehør og software er i overensstemmelse med direktiv 2014/53/EU. Den fulde tekst i EU-overensstemmelseserklæringen og produktfirmware kan wnloades fra produktsiden hos www.dlink.com.
Deutsch [German]	Hiermit erklärt die D-Link Corporation, dass dieses Produkt, das Zubehör und die Software der Richtlinie 2014/53/EU entsprechen. Der vollständige Text der Konformitätserklärung der Europäischen Gemeinschaft sowie die Firmware zum Produkt stehen Ihnen zum Herunterladen von der Produktseite im Internet auf www.dlink.com zur Verfügung.
Eesti [Estonian]	Käesolevaga kinnitab D-Link Corporation, et see toode, tarvikud ja tarkvara on kooskõlas direktiiviga 2014/53/EL. Euroopa Liidu vastavusdeklaratsiooni täistekst ja toote püsivara on allalaadimiseks saadaval tootelehel www.dlink.com.
English	Hereby, D-Link Corporation, declares that this product, accessories, and software are in compliance with directive 2014/53/EU. The full text of the EU Declaration of Conformity and product firmware are available for download from the product page at www.dlink.com
Español [Spanish]	Por la presente, D-Link Corporation declara que este producto, accesorios y software cumplen con las directivas 2014/53/UE. El texto completo de la declaración de conformidad de la UE y el firmware del producto están disponibles y se pueden descargar desde la página del producto en www.dlink.com.
Ελληνική [Greek]	Με την παρούσα, η D-Link Corporation δηλώνει ότι αυτό το προϊόν, τα αξεσουάρ και το λογισμικό συμμορφώνονται με την Οδηγία 2014/53/ΕΕ. Το πλήρες κείμενο της δήλωσης συμμόρφωσης της ΕΕ και το υλικολογισμικό του προϊόντος είναι διαθέσιμα για λήψη από τη σελίδα του προϊόντος στην τοποθεσία www.dlink.com.
Français [French]	Par les présentes, D-Link Corporation déclare que ce produit, ces accessoires et ce logiciel sont conformes aux directives 2014/53/UE.Le texte complet de la déclaration de conformité de l'UE et le icroprogramme du produit sont disponibles au téléchargement sur la page des produits à www.dlink.com.
Italiano [Italian]	Con la presente, D-Link Corporation dichiara che questo prodotto, i relativi accessori e il software sono conformi alla direttiva 2014/53/UE. Il testo completo della dichiarazione di conformità UE e il firmware del prodotto sono disponibili per il download dalla pagina del prodotto su www.dlink.com.
Latviski [Latvian]	Ar šo uzņēmums D-Link Corporation apliecina, ka šis produkts, piederumi un programmatūra atbilst direktīvai 2014/53/ES. ES atbilstības deklarācijas pilno tekstu un produkta aparātprogrammatūru var lejupielādēt attiecīgā produkta lapā vietnē www.dlink.com.
Lietuvių [Lithuanian]	Šiuo dokumentu „D-Link Corporation“ pareiškia, kad šis gaminys, priedai ir programinė įranga atitinka

	direktyvą 2014/53/ES. Visą ES atitikties deklaracijos tekstą ir gaminio programinę aparatinę įrangą galima atsisiųsti iš gaminio puslapio adresu www.dlink.com.
Nederlands [Dutch]	Hierbij verklaart D-Link Corporation dat dit product, accessoires en software voldoen aan de richtlijnen 2014/53/EU. De volledige tekst van de EU conformiteitsverklaring en productfirmware is beschikbaar voor download van de productpagina op www.dlink.com.
Malti [Maltese]	Bil-preżenti, D-Link Corporation tiddikjara li dan il-prodott, l-aċċessorji, u s-software huma konformi mad-Direttiva 2014/53/UE. Tista' tniżżel it-test sħiħ tad-dikjarazzjoni ta' konformità tal-UE u l-firmware tal-prodott mill-paġna tal-prodott fuq www.dlink.com.
Magyar [Hungarian]	Ezennel a D-Link Corporation kijelenti, hogy a jelen termék, annak tartozékai és szoftvere megfelelnek a 2014/53/EU sz. rendeletek rendelkezéseinek. Az EU Megfelelőségi nyilatkozat teljes szövege és a termék firmware a termék oldaláról tölthető le a www.dlink.com címen.
Polski [Polish]	D-Link Corporation niniejszym oświadcza, że ten produkt, akcesoria oraz oprogramowanie są zgodne z dyrektywami 2014/53/EU. Pełen tekst deklaracji zgodności UE oraz oprogramowanie sprzętowe do produktu można pobrać na stronie produktu w witrynie www.dlink.com.
Português [Portuguese]	Desta forma, a D-Link Corporation declara que este produto, os acessórios e o software estão em conformidade com a diretiva 2014/53/UE. O texto completo da declaração de conformidade da UE e do firmware
Slovensko[Slovenian]	Podjetje D-Link Corporation s tem izjavlja, da so ta izdelek, dodatna oprema in programnska oprema skladni z direktivami 2014/53/EU. Celotno besedilo izjave o skladnosti EU in vdelana programska oprema sta na voljo za prenos na strani izdelka na www.dlink.com.
Slovensky [Slovak]	Spoločnosť D-Link týmto vyhlasuje, že tento produkt, príslušenstvo a softvér sú v súlade so smernicou 214/53/EÚ. Úplné znenie vyhlásenia EÚ o zhode a firmvéri produktu sú k dispozícii na prevzatie zo stránky produktu www.dlink.com.
Suomi [Finnish]	D-Link Corporation täten vakuuttaa, että tämä tuote, lisävarusteet ja ohjelmisto ovat direktiivin 2014/53/EU vaatimusten mukaisia. Täydellinen EU-vaatimustenmukaisuusvakuutus samoin kuin tuotteen laiteohjelmisto ovat ladattavissa osoitteesta www.dlink.com.
Svenska[Swedish]	D-Link Corporation försäkrar härmed att denna produkt, tillbehör och programvara överensstämmer med direktiv 2014/53/EU. Hela texten med EU-försäkran om överensstämmelse och produkt-firmware kan hämtas från produktsidan på www.dlink.com.
Íslenska [Icelandic]	Hér með lýsir D-Link Corporation því yfir að þessi vara, fylgihlutir og hugbúnaður eru í samræmi við tilskipun 2014/53/EB. Sækja má ESB-samræmisyfirlýsinguna í heild sinni og fastbúnað vörunnar af vefsíðu vörunnar á www.dlink.com.
Norsk [Norwegian]	Herved erklærer D-Link Corporation at dette produktet, tilbehøret og programvaren er i samsvar med direktivet 2014/53/EU. Den fullstendige teksten i EU-erklæring om samsvar og produktets fastvare er tilgjengelig for nedlasting fra produktsiden på www.dlink.com.

Warning Statement:

The power outlet should be near the device and easily accessible.

Notice of Wireless Radio LAN Usage in The European Community (For Wireless Product Only):

- This device is restricted to indoor use when operated in the European Community using channels in the 5.15-5.35 GHz band to reduce the potential for interference.
- This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries. This equipment may be operated in AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, and CY.

Usage Notes:

- To remain in conformance with European National spectrum usage regulations, frequency and channel limitations will be applied on the products according to the country where the equipment will be deployed.
- This device is restricted from functioning in Ad-hoc mode while operating in 5 GHz. Ad-hoc mode is direct peer-to-peer communication between two client devices without an Access Point.
- Access points will support DFS (Dynamic Frequency Selection) and TPC (Transmit Power Control) functionality as required when operating in 5 GHz band within the EU.

HINWEIS ZUR VERWENDUNG VON DRAHTLOS-NETZWERK (WLAN) IN DER EUROPÄISCHEN GEMEINSCHAFT (NUR FÜR EIN DRAHTLOSES PRODUKT)

- Der Betrieb dieses Geräts in der Europäischen Gemeinschaft bei Nutzung von Kanälen im 5,15-5,35 GHz Frequenzband ist ausschließlich auf Innenräume beschränkt, um das Interferenzpotential zu reduzieren.
- Bei diesem Gerät handelt es sich um ein zum Einsatz in allen EU-Mitgliedsstaaten und in EFTA-Ländern - ausgenommen Frankreich. Der Betrieb dieses Geräts ist in den folgenden Ländern erlaubt: AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Gebrauchshinweise:

- Um den in Europa geltenden nationalen Vorschriften zum Nutzen des Funkspektrums weiterhin zu entsprechen, werden Frequenz und Kanalbeschränkungen, dem jeweiligen Land, in dem das Gerät zum Einsatz kommt, entsprechend, auf die Produkte angewandt.
- Die Funktionalität im Ad-hoc-Modus bei Betrieb auf 5 GHz ist für dieses Gerät eingeschränkt. Bei dem Ad-hoc-Modus handelt es sich um eine Peer-to-Peer-Kommunikation zwischen zwei Client-Geräten ohneeinen Access Point.
- Access Points unterstützen die Funktionen DFS (Dynamic Frequency Selection) und TPC (Transmit Power Control) wie erforderlich bei Betrieb auf 5 GHz innerhalb der EU.
- Bitte schlagen Sie im Handbuch oder Datenblatt nach nach, ob Ihr Gerät eine 2,4 GHz und / oder 5 GHz Verbindung nutzt.

AVIS CONCERNANT L'UTILISATION DE LA RADIO SANS FIL LAN DANS LA COMMUNAUTÉ EUROPÉENNE (UNIQUEMENT POUR LES PRODUITS SANS FIL)

- Cet appareil est limité à un usage intérieur lorsqu'il est utilisé dans la Communauté européenne sur les canaux de la bande de 5,15 à 5,35 GHz afin de réduire les risques d'interférences.
- Cet appareil est un système de transmission à large bande (émetteur-récepteur) de 2,4 GHz, destiné à être utilisé dans tous les États-membres de l'UE et les pays de l'AELE. Cet équipement peut être utilisé dans les pays suivants : AL, AD, BE , BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT , MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Notes d'utilisation:

- Pour rester en conformité avec la réglementation nationale européenne en matière d'utilisation du spectre, des limites de fréquence et de canal seront appliquées aux produits selon le pays où

l'équipement sera déployé.
- Cet appareil ne peut pas utiliser le mode Ad-hoc lorsqu'il fonctionne dans la bande de 5 GHz. Le mode Adhoc fournit une communication directe pair à pair entre deux périphériques clients sans point d'accès.
- Les points d'accès prendront en charge les fonctionnalités DFS (Dynamic Frequency Selection) et TPC (Transmit Power Control) au besoin lors du fonctionnement dans la bande de 5 GHz au sein de l'UE.
- Merci de vous référer au guide d'utilisation ou de la fiche technique afin de vérifier si votre produit utilise 2.4 GHz et/ou 5 GHz sans fil.

AVISO DE USO DE LA LAN DE RADIO INALÁMBRICA EN LA COMUNIDAD EUROPEA (SOLO PARA EL PRODUCTO INALÁMBRICO)
- El uso de este dispositivo está restringido a interiores cuando funciona en la Comunidad Europea utilizando canales en la banda de 5,15-5,35 GHz, para reducir la posibilidad de interferencias.
- Este dispositivo es un sistema de transmisión (transceptor) de banda ancha de 2,4 GHz, pensado para su uso en todos los estados miembros de la UE y en los países de la AELC. Este equipo se puede utilizar en AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Notas de uso:
- Para seguir cumpliendo las normas europeas de uso del espectro nacional, se aplicarán limitaciones de frecuencia y canal en los productos en función del país en el que se pondrá en funcionamiento el equipo.
- Este dispositivo tiene restringido el funcionamiento en modo Ad-hoc mientras funcione a 5 Ghz. El modo Ad-hoc es la comunicación directa de igual a igual entre dos dispositivos cliente sin un punto de acceso.
- Los puntos de acceso admitirán la funcionalidad DFS (Selección de frecuencia dinámica) y TPC (Control de la potencia de transmisión) si es necesario cuando funcionan a 5 Ghz dentro de la UE.
- Por favor compruebe el manual o la ficha de producto para comprobar si el producto utiliza las bandas inalámbricas de 2.4 GHz y/o la de 5 GHz.

AVVISO PER L'USO DI LAN RADIO WIRELESS NELLA COMUNITÀ EUROPEA (SOLO PER PRODOTTI WIRELESS)
- Nella Comunità europea, l'uso di questo dispositivo è limitato esclusivamente agli ambienti interni sui canali compresi nella banda da 5,15 a 5,35 GHz al fine di ridurre potenziali interferenze. Questo dispositivo è un sistema di trasmissione a banda larga a 2,4 GHz (ricetrasmittente), destinato all'uso in tutti gli stati membri dell'Unione europea e nei paesi EFTA.
- Questo dispositivo può essere utilizzato in AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Note per l'uso
- Al fine di mantenere la conformità alle normative nazionali europee per l'uso dello spettro di frequenze, saranno applicate limitazioni sulle frequenze e sui canali per il prodotto in conformità alle normative del paese in cui il dispositivo viene utilizzato.
- Questo dispositivo non può essere attivato in modalità Ad-hoc durante il funzionamento a 5 Ghz. La modalità Ad-hoc è una comunicazione diretta peer-to-peer fra due dispositivi client senza un punto di accesso.
- I punti di accesso supportano le funzionalità DFS (Dynamic Frequency Selection) e TPC (Transmit Power Control) richieste per operare a 5 Ghz nell'Unione europea.
- Ti invitiamo a fare riferimento al manuale del prodotto o alla scheda tecnica per verificare se il tuo prodotto utilizza le frequenze 2,4 GHz e/o 5 GHz.

KENNISGEVING VAN DRAADLOOS RADIO LAN-GEBRUIK IN DE EUROPESE GEMEENSCHAP (ALLEEN VOOR DRAADLOOS PRODUCT)
- Dit toestel is beperkt tot gebruik binnenshuis wanneer het wordt gebruikt in de Europese Gemeenschap gebruik makend van kanalen in de 5.15-5.35 GHz band om de kans op interferentie te beperken.
- Dit toestel is een 2.4 GHz breedband transmissiesysteem (transceiver) dat bedoeld is voor gebruik in alle

EU lidstaten en EFTA landen. Deze uitrusting mag gebruikt worden in AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Gebruiksaanwijzingen:

- Om de gebruiksvoorschriften van het Europese Nationale spectrum na te leven, zullen frequentie- en kanaalbeperkingen worden toegepast op de producten volgens het land waar de uitrusting gebruikt zal worden.
- Dit toestel kan niet functioneren in Ad-hoc mode wanneer het gebruikt wordt in 5 GHz. Ad-hoc mode is directe peer-to-peer communicatie tussen twee klantenapparaten zonder een toegangspunt.
- Toegangspunten ondersteunen DFS (Dynamic Frequency Selection) en TPC (Transmit Power Control) functionaliteit zoals vereist bij gebruik in 5 GHz binnen de EU.
- Raadpleeg de handleiding of de datasheet om te controleren of uw product gebruik maakt van 2.4 GHz en/of 5 GHz.