



User Manual

5G Transit Gateway

DTM-550-G

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.....	7
1.1 Introduction	7
1.2 Contents List.....	8
1.2.1 Package Contents	8
1.3 Hardware Configuration.....	9
1.4 Indicator LEDs.....	11
1.5 Installation & Maintenance Notice	12
1.5.1 System Requirements	12
1.5.2 WARNING	12
1.5.3 HOT SURFACE CAUTION	14
1.5.4 Product Information for CE RED ReSquirements	15
1.6 Hardware Installation.....	19
1.6.1 Mount the Unit	19
1.6.2 Insert the SIM Card	19
1.6.3 Connecting Power	20
1.6.4 Connecting to the Network or a Host	21
1.6.5 Connecting the Web UI	22
Chapter 2 Basic Network.....	24
2.1 WAN & Uplink	24
2.1.1 Physical Interface	25
2.1.2 Connection Setup.....	29
2.1.3 Load Balance	51
2.2 LAN & VLAN.....	56
2.2.1 Ethernet LAN	56
2.2.2 VLAN.....	58
2.2.3 DHCP Server	71
2.3 WiFi	78
2.3.1 WiFi Configuration	79
2.3.2 Wireless Client List	85
2.3.3 Advanced Configuration.....	86
2.3.4 Uplink Profile.....	89
2.4 IPv6.....	91

2.4.1 IPv6 Configuration.....	91
2.5 Port Forwarding.....	93
2.5.1 Configuration.....	94
2.5.2 Virtual Server & Virtual Computer.....	95
2.5.3 DMZ & Pass Through.....	100
2.5.4 Special AP & ALG.....	100
2.6 Routing.....	106
2.6.1 Static Routing.....	107
2.6.2 Dynamic Routing.....	110
2.6.3 Routing Information.....	117
2.7 DNS & DDNS.....	118
2.7.1 DNS & DDNS Configuration.....	118
2.8 QoS.....	122
2.8.1 QoS Configuration.....	122
Chapter 3 Object Definition.....	131
3.1 Scheduling.....	131
3.1.1 Scheduling Configuration.....	131
3.2 Grouping.....	133
3.2.1 Host Grouping.....	133
3.3 External Server.....	135
3.4 Certificate.....	137
3.4.1 Configuration.....	137
3.4.2 My Certificate.....	139
3.4.3 Trusted Certificate.....	145
3.4.4 Issue Certificate.....	148
Chapter 4 Security.....	149
4.1 VPN.....	149
4.1.1 IPSec.....	150
4.1.2 OpenVPN.....	156
4.1.3 L2TP.....	169
4.1.4 PPTP.....	177
4.1.5 GRE.....	183

4.1.6 EoGRE	186
4.1.7 WireGuard	189
4.2 Firewall	192
4.2.1 Packet Filter	192
4.2.2 URL Blocking.....	196
4.2.3 MAC Control	199
4.2.4 IPS.....	202
4.2.5 Options.....	205
4.3 Authentication	208
4.3.1 MAC Authentication.....	208
Chapter 5 Administration	210
5.1 Configure & Manage	210
5.1.1 Command Script.....	211
5.1.2 Device Management	215
5.1.3 RESTful.....	217
5.1.4 SNMP	218
5.1.5 Telnet & SSH	226
5.2 System Operation	229
5.2.1 Password & MMI	229
5.2.2 System Information	232
5.2.3 System Time	233
5.2.4 System Log	238
5.2.5 Backup & Restore	243
5.2.6 Reboot & Reset	244
5.3 FTP	245
5.3.1 Server Configuration	246
5.3.2 User Account	248
5.4 Diagnostic.....	249
5.4.1 Diagnostic Tools.....	249
5.4.2 Ethernet Port Setup	250
Chapter 6 Service	251
6.1 Cellular Toolkit.....	251

6.1.1 Data Usage	252
6.1.2 SMS.....	254
6.1.3 SIM PIN.....	258
6.1.4 Network Scan	262
6.2 Event Handling	264
6.2.1 Configuration.....	265
6.2.2 Notifying Events	266
6.3 Location Tracking.....	268
6.3.1 GNSS.....	269
6.4 Power Control	274
6.4.1 Ignition Sense.....	274
Chapter 7 Status.....	277
7.1 Dashboard	277
7.2 Basic Network	279
7.2.1 WAN & Uplink Status	279
7.2.2 LAN & VLAN Status.....	283
7.2.3 WiFi Status	284
7.2.4 DDNS Status	287
7.3 Security.....	288
7.3.1 VPN Status.....	288
7.3.2 Firewall Status	292
7.4 Administration.....	296
7.4.1 Configure & Manage Status	296
7.4.2 Log Storage Status.....	296
7.4.3 GNSS Status	298
7.5 Statistics & Report.....	299
7.5.1 Connection Session	299
7.5.2 Network Traffic.....	300
7.5.3 Login Statistics.....	301
7.5.4 Cellular Usage.....	302
7.5.5 Cellular Signal.....	303
Appendix A GPL WRITTEN OFFER	304

Chapter 1 Introduction

1.1 Introduction

The DTM-550-G is a 5G Transit Gateway. It is designed to support a variety of IoT applications such as in-vehicle WiFi connectivity, in-vehicle telematics, and M2M (machine-to-machine) applications in smart manufacturing and smart cities.

The system is equipped with a superior 5G NR module to facilitate Internet connection with a SIM card from your local mobile carrier. With a built-in VPN tunneling technology, remote sites can connect to the control center securely utilizing 256-bit AES encryption. Besides VPN, features for enhanced security such as firewall, NAT, port forwarding, and DHCP server are geared to the demands of advanced applications in smart automotive and industrial automation.

The design of a wide power input range (DC 9-36V) allows for electrical transient in vehicles. The design with a terminal block secures the power cord into the connector on the device when it is deployed in vehicles.

The following highlights the capabilities of the DTM-550-G:

- :
- A high-speed 5G NR cellular module for high bandwidth and low latency connectivity.
- 4 gigabit Ethernet ports to connect with other IP-based devices in the application field.
- WiFi 6 AX1800 dual-band, dual-concurrent access point compliant with 802.11b/g/a/n/ac/ax standards.
- Dual-SIM connector for redundant WAN connections.
- Support for RADIUS server for user authentication and authorization or push advertisements.
- Solid and yet flexible metal case design for versatile mount in industrial environments.
- Designed by solid and easy-to-mount metal body for industrial environment to work with a variety of IoT applications
- Global Positioning System (GPS) technology enables GPS-capable smart transportation

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

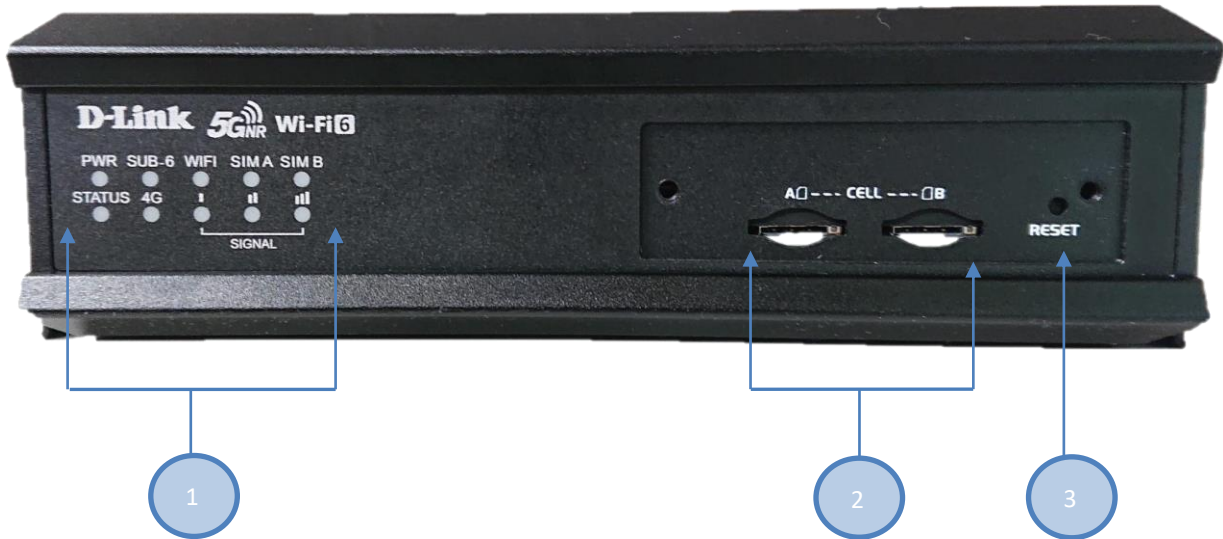
1.2.1 Package Contents

#Standard Package

Items	Description	Contents	Quantity
1	DTM-550-G		1 device
2	3-pin Terminal Block		1 terminal block
3	RJ45 Cable		1 cable
4	5G NR RF1 Antenna		4 antennae
5	WiFi 2.4G/5G Antenna		2 antennae
6	Mounting Bracket		2 brackets

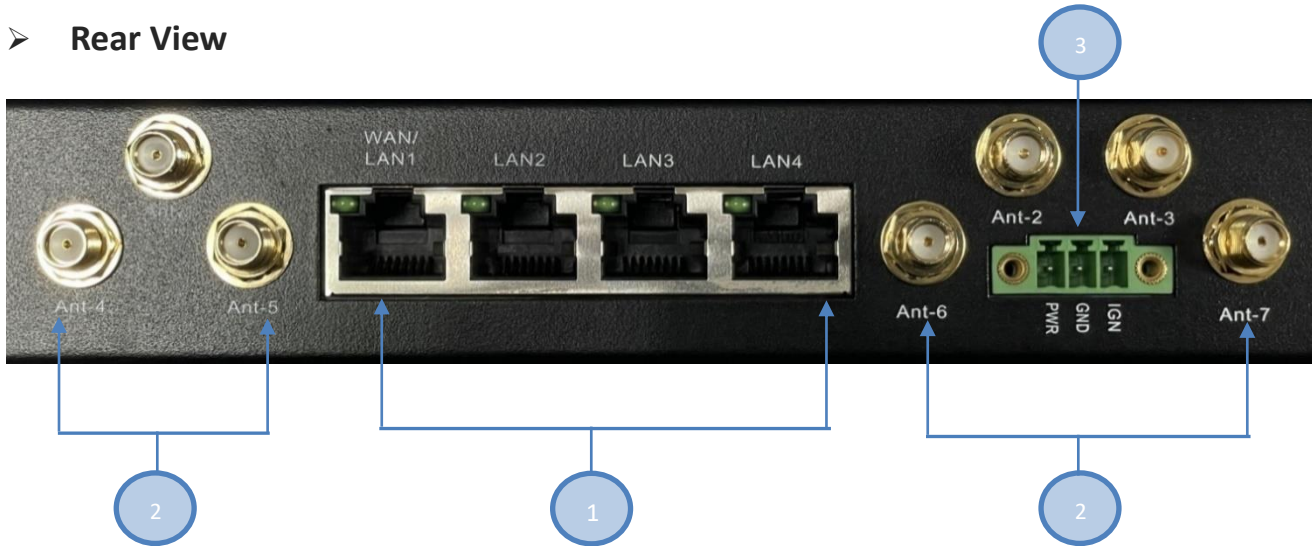
1.3 Hardware Configuration

➤ Front View



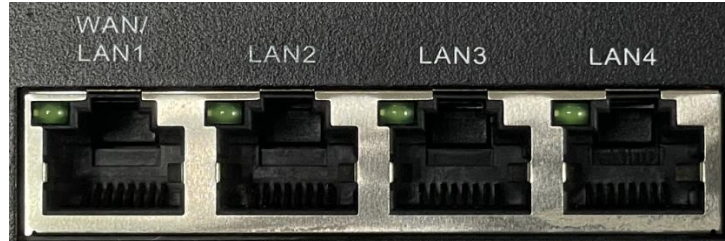
No	Indicator, button, or connector	Description
1	Indicator LEDs	LEDs indicate the operating status of the device. Refer to 1.4 Indicator LEDs for the LEDs and their meaning.
2	SIM Slot A/B (with a slot cover)	SIM slots. Refer to 1.6.2 Insert the SIM Card for installation instructions.
3	Reset Button	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 10 seconds (when the Status LED starts blinking rapidly), and then release it (During the reset, all LEDs will light up.) Note that all configuration changes will be erased.

➤ Rear View



No	Connector	Description
1	Auto MDI/MDIX Port 3x 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 LAN1 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.
2	5G NR & WiFi Antenna	Install antennas for 5G and WiFi networks. Note that 5G NR and WiFi antennas are optional accessories, and not included in the standard package. You need to purchase suitable antennas and RF cables for your application. When installing antennae, install the RF cables and antennas according to your application requirements. The following specifies the receptacles on the panel: Ant-1: GNSS Ant-2: WiFi 2.4G/5G Ant-3: WiFi 2.4G/5G Ant-4: 5G_Ant-0 Ant-5: 5G_An5-1 Ant-6: 5G_Ant-2 Ant-7: 5G_Ant-3
3	DC Power Terminal Block	A terminal block for connecting with power supply. Refer to 1.6.3 Connecting Power for power input voltage and pin assignments.

1.4 Indicator LEDs



LED Icon	Indication	LED Color	Description
PWR	Power Source	Blue	Off: Device is powered off. Steady ON : Device is powered ON
Status	Status	Blue	Flash (slow): Device is working properly. Flash (very fast): Device is in Recovery Mode or is not working properly.
WiFi	WiFi	Blue	OFF : WiFi function is disabled. Steady On : WiFi (2.4GHz) is enabled. Flash: Data is being transmitted via the WiFi 1 LAN interface.
Sub-6G	Sub-6	Blue	OFF : 5G mobile is not in service. Steady On: 5G is enabled.
4G LTE	4G LTE	Blue	OFF : 4G LTE is not in service. Steady On : 4G LTE is enabled.
SIMA	SIM A	Blue	OFF: No SIM card is inserted or operational Steady On : SIM A slot is in use.
SIMB	SIM B	Blue	OFF: No SIM card is inserted or operational Steady On : SIM B slot is in use.
SIGNAL	Low	Blue	OFF: No signal Steady On : Signal Strength is 0~30% (CSQ 0-9) or RSRP < -104 dBm
	Medium	Blue	Steady On : Signal Strength is 31~60% (CSQ 10-18) or RSRP is in the range: -104~-93 dBm
	High	Blue	Steady On : Signal Strength is 61~100% (CSQ 19-31) or RSRP is less than or equal to -92 dBm
WAN/LAN1~3	WAN/LAN1 LAN2~4	Green	OFF : Ethernet port is not connected. 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 or DSL modem • 5G/4G cellular service subscription • Devices with IEEE 802.11b/g/n/a/ac/ax wireless network adaptor • PC with 10/100/1000 Ethernet adaptor
Web-based Configuration Utility 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

- This gateway can be powered by DC12V or DC24V car system. If this gateway is not installed in vehicle, a DC12V/2A power adapter is recommended.
- 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 (<20m 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 (>20cm/low power)

Radiation Exposure Statement:s

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 WiFi 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 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 latest CE RED requirements.¹

(1) Frequency Band & Maximum Power

1. Frequency Band for 5G NR /4G LTE /3G Connection (for RM520N-GL version)²

Band number	Operating Frequency	Max output power
5G NR bands (n1/n3/5/n7/n8/n20/ n28/n38/n40/n41/n75/ n76/n77/n78)	N1 Uplink:1920-1980 MHz Downlink:2110-2170 MHz N3 Uplink:1710-1785 MHz Downlink:1805-1880 MHz N5 Uplink: 824-849 MHz Downlink: 869-894 MHz N7 Uplink:2500-2570 MHz Downlink:2620-2690 MHz N8 Uplink:880-915 MHz Downlink:925-960 MHz N20 Uplink:832-862 MHz Downlink:791-821 MHz N28 Uplink: 703-748 MHz Downlink: 758-803 MHz N38 Uplink: 3550-3700MHz Downlink: 3550-3700MHz N40 Uplink: 2300-2400MHz Downlink: 2300-2400MHz N41 Uplink: 2496-2690MHz Downlink: 2496-2690MHz N75 Downlink: 1432-1517MHz N76 Downlink: 1427-1432MHz N77 Uplink: 3300-4200MHz Downlink: 3300-4200MHz N78 Uplink: 3550-3700MHz Downlink: 3550-3700MHz	n1/n3/n5/n7/n8/n20/n28/n 38/n40: 25dBm n41/n77/n78 (class 2): 28dBm
LTE Bands E-UTRA FDD Band:1/3/5/7/8/20/28/ 32 E-UTRA TDD Band: 34/38/40/41/42/43/46	B1 Uplink:1920-1980 MHz Downlink:2110-2170 MHz B3 Uplink:1710-1785 MHz Downlink:1805-1880 MHz B5 Uplink: 824-849 MHz Downlink: 869-894 MHz	E-UTRA FDD 1/3/5/7/8/20/28: 25 dBm E-UTRA TDD 34/38/40/41/42/43: 25 dBm UL CA: 25 dBm

1 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.

2. There can be different cellular module integrated in the device for EU/EFTA regional version. Refer to the cellular module identifier printed on the device label for the purchased device.

	B7 Uplink:2500-2570 MHz Downlink:2620-2690 MHz B8 Uplink:880-915 MHz Downlink:925-960 MHz B20 Uplink:832-862 MHz Downlink:791-821 MHz B28 Uplink: 703-748 MHz Downlink: 758-803 MHz B32 Downlink: 1452-1496 MHz B34 Uplink: 2010-2025 MHz Downlink: 2010-2025 MHz B38 Uplink: 2570-2620 MHz Downlink: 2570-2620 MHz B40 Uplink: 2300-2400 MHz Downlink: 2300-2400 MHz B41 Uplink: 2496-2690 MHz Downlink: 2300-2400 MHz B42 Uplink: 3400-3600 MHz Downlink: 3400-3600 MHz B43 Uplink: 3600-3800 MHz Downlink: 3600-3800 MHz B46 Downlink: 5150-5925 MHz	
WCDMA BANDs Band I/V/VIII	B1 Uplink:1920-1980 MHz Downlink:2110-2170 MHz B5 Uplink: 824-849 MHz Downlink: 869-894 MHz B8 Uplink:880-915 MHz Downlink:925-960 MHz	25 dBm

2. Frequency Band for 5G NR /4G LTE /3G Connection (for RM520N-EU version)²

Band number	Operating Frequency	Max output power
5G NR bands (n1/n3/n5/n7/n8/n20/ n28/n38/n40/n41/n77/ n78)	N1 Uplink:1920-1980 MHz Downlink:2110-2170 MHz N3 Uplink:1710-1785 MHz Downlink:1805-1880 MHz N5 Uplink: 824-849 MHz Downlink: 869-894 MHz N7 Uplink:2500-2570 MHz Downlink:2620-2690 MHz N8 Uplink:880-915 MHz Downlink:925-960 MHz N20 Uplink:832-862 MHz Downlink:791-821 MHz N28 Uplink: 703-748 MHz Downlink: 758-803 MHz B38 Uplink: 2570-2620 MHz	n1/n3/n5/n7/n8/n20/n 28/n40: 23 dBm n38: 26 dBm n41/n77/n78 (class 2): 29 dBm

	Downlink: 2570-2620 MHz B40 Uplink: 2300-2400 MHz Downlink: 2300-2400 MHz B41 Uplink: 2496-2690 MHz Downlink: 2496-2690 MHz N77 Uplink: 3300-4200MHz Downlink: 3300-4200MHz N78 Uplink: 3550-3700MHz Downlink: 3550-3700MHz	
LTE bands E-UTRA FDD Band:1/3/5/7/8/20/28/ 32 E-UTRA TDD Band: 38/40/41/42/43	B1 Uplink:1920-1980 MHz Downlink:2110-2170 MHz B3 Uplink:1710-1785 MHz Downlink:1805-1880 MHz B5 Uplink: 824-849 MHz Downlink: 869-894 MHz B7 Uplink:2500-2570 MHz Downlink:2620-2690 MHz B8 Uplink:880-915 MHz Downlink:925-960 MHz B20 Uplink:832-862 MHz Downlink:791-821 MHz B28 Uplink: 703-748 MHz Downlink: 758-803 MHz B32 Downlink: 1452-1496 MHz B38 Uplink: 2570-2620 MHz Downlink: 2570-2620 MHz B40 Uplink: 2300-2400 MHz Downlink: 2300-2400 MHz B41 Uplink: 2496-2690 MHz Downlink: 2496-2690 MHz B42 Uplink: 3400-3600 MHz Downlink: 3400-3600 MHz B43 Uplink: 3600-3800 MHz Downlink: 3600-3800 MHz	E-UTRA FDD 1/3/5/7/8/20/28: 23 dBm E-UTRA TDD 38/41/42/43: 26 dBm 40: 23 dBm
WCDMA bands Band I/V/VIII	B1 Uplink:1920-1980 MHz Downlink:2110-2170 MHz B5 Uplink: 824-849 MHz Downlink: 869-894 MHz B8 Uplink:880-915 MHz Downlink:925-960 MHz	24 dBm

(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 In Door Use Only.

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

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) DoC Information

Please contact your sales representative for DoC information of this product.

(5) RF Exposure Statements

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

(6) Unit Mounting Notice

The product is suitable for mounting at heights $\leq 2\text{m}$ (approx. 6 ft), or in a cabinet.

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

(7) Manufacture Information

Manufacture Name: D-Link Corporation

Manufacture Address: No.289, Xinhua 3rd Rd., Neihu District, Taipei 11494, Taiwan, R.O.C.

1.6 Hardware Installation

This chapter describes how to install and configure the hardware.

1.6.1 Mount the Unit

The DTM-550-G can be mounted on a wall, or a horizontal plane with the mounting accessories (optional brackets). The mounting accessories are not attached to the device when the product is shipped. Please install the mounting brackets on the device first.

1.6.2 Insert the SIM Card

WARNING: Before inserting or changing the SIM card, turn off the device.

The SIM card slots are located at the front side of the device housing. You need to unscrew and remove the outer SIM card cover before installing or removing the SIM card. Please follow the instructions to insert or eject a SIM card. When inserting the SIM card, push the SIM card to secure it in place.

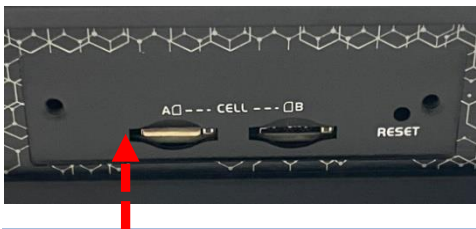
Step 1:

Loosen the screws as shown below and remove the SIM cover.

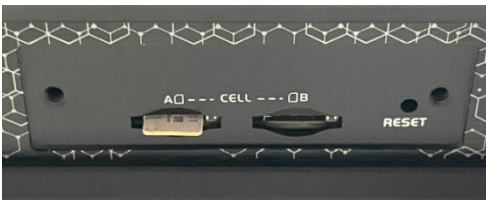


Step 2:

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).

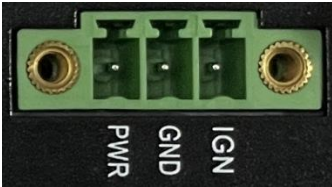


To eject the SIM card, push the inserted SIM card again.



1.6.3 Connecting Power

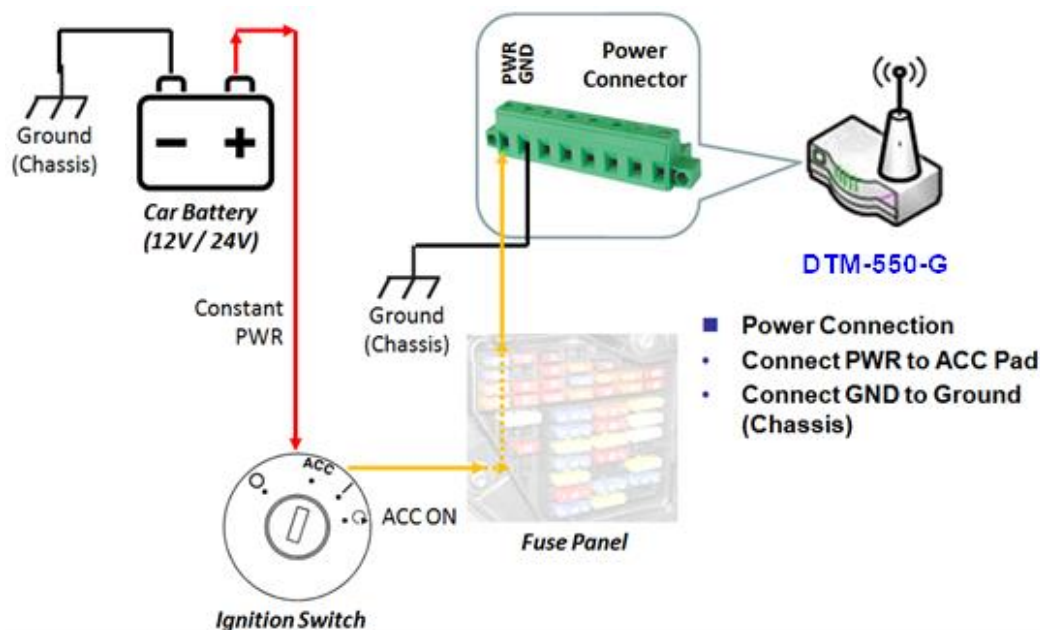
The DTM-550 can be powered by connecting a power source to the 3-pin terminal block. **It supports 9V to 36V DC power input.** Please connect the power supply according to the following pin assignments with correct polarity.



In-vehicle Power Connection:

Depending on the employment of the ignition sensing feature, power connection to the DTM-550 will be different.

When ignition sensing is disabled (the IGN pin is not used), use the following diagram to connect power from the car battery to DTM-550-G.

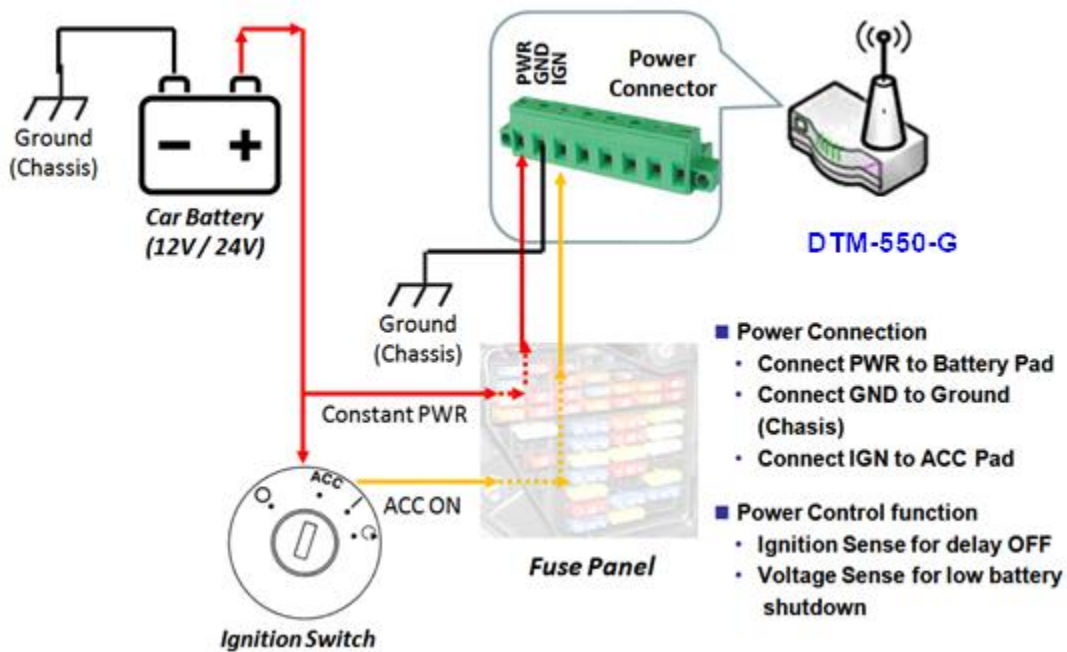


Attention

The **ignition sense** feature is **DISABLED** by default. With this default setting, power pin should be connected to ACC power. **DO NOT** connect power pin to constant power from car battery. Otherwise, this device will drain a car battery.

When ignition sensing (IGN) is enabled, the DTM-55-G can be powered on/off with car ignition function. It can utilize the delay-off and low battery shutdown function provided by in-vehicle power control. With the delay-off feature, the device can continue operating for a certain period of time after the car engine has been turned off.

To use in-vehicle power control, please connect the PWR/GND /IGN connectors to the pads located in the vehicle fuse panel (refer the the following diagram), and activate the **Power Control** function through Web UI configuration. If the ignition sensing (IGN) is enabled, the device won't be turned on until voltage is detected on the IGN pin.



Attention

If the PWR pin is connected to the constant power from a car battery, please make sure IGN pin of the terminal block is connected to ACC pad and the Ignition Sense feature (go to **Service > Power Control > Ignition Sense**) is ENABLED. Otherwise, this device can drain a car battery.

1.6.4 Connecting to the Network or a Host

The DTM-550-G provides four RJ45 ports with 10/100/1000Mbps Ethernet (with one port for LAN or WAN) 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.

1.6.5 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>)³ 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**'.



Welcome to the device's configuration UI.
Enter your Username & Password, then
click 'Login'.

Username

Password

Login

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

³ The default LAN IP address of this device is 192.168.0.1. If you change it, you need to log in using the new IP address.

Change Password

For security consideration, you are being asked to change the password while the first time login to the device.

Enter the new password below.

(NOTE: The password must be at least 10 characters long, and must contain at least 1 English letter and 1 number. The password cannot be the same as the login account.)

Please setup your local country area follow below path :

Basic Network -> WiFi -> Advanced Configuration to select your country area.

New Password:

New Password Confirmation:

OK

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 **5.2.5 Backup & Restore**.

Chapter 2 Basic Network

2.1 WAN & Uplink

Basic Network

↓

WAN& Uplink

↓

Physical Interface

↓

Internet Setup

↓

Loading Balance

↓

End

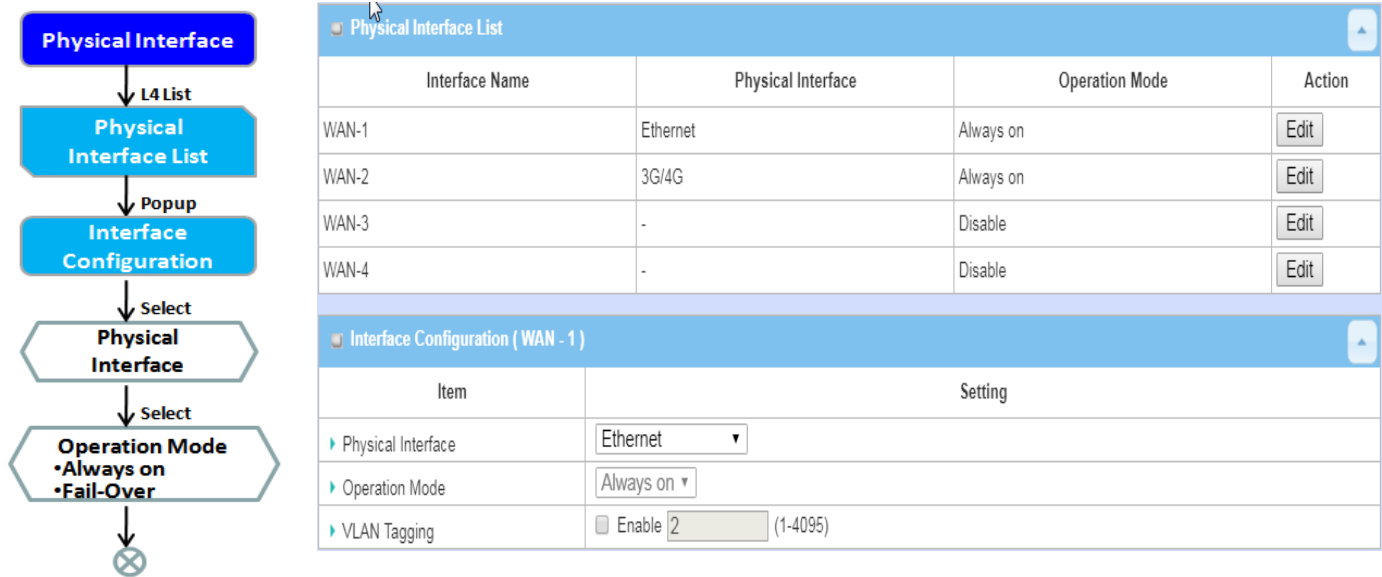
▶ **Physical Interface** ▶ **Internet Setup** ▶ **Load Balance**

Physical Interface List

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

The gateway provides multiple WAN interfaces to achieve redundant Internet connections. Since ISPs in the world require different connection methods for Internet connectivity via different transmission media, you need to configure WAN Connection 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, there are two configuration windows: "Physical Interface List" and "Interface Configuration". "Physical Interface List" window shows all the available physical interfaces. To configure a WAN interface, click **Edit** 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, 1 or dual SIM cards can be installed to allow for failover.



Attention

- 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.

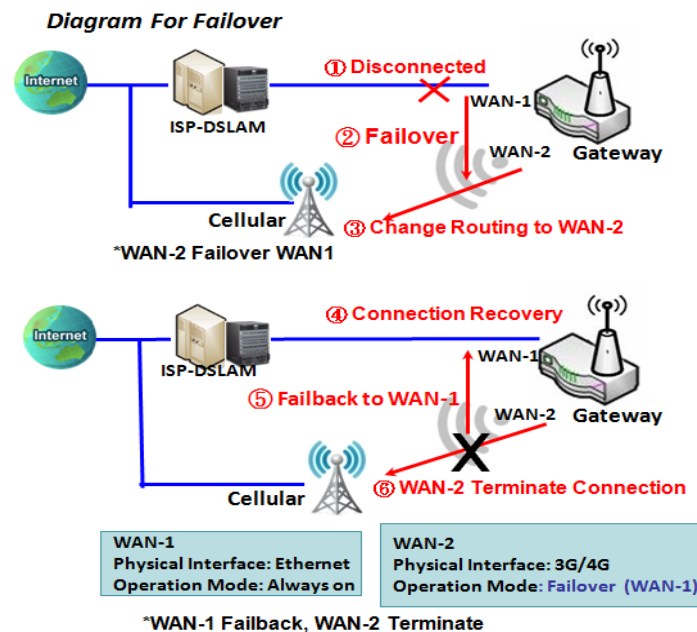
- **WiFi Uplink WAN:** For devices with WiFi Uplink function, one WiFi module can be configured for WAN connection.

Operation Mode:

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

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

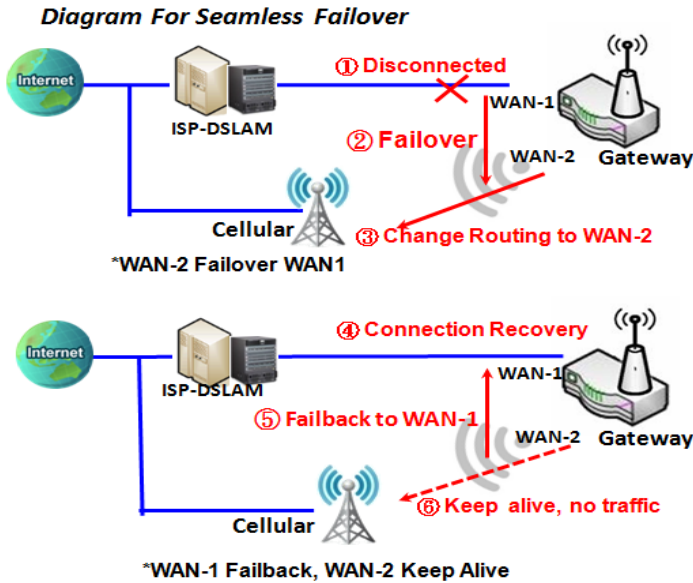
Failover:



A failover interface is a backup connection to the primary. When the 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 the 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 since 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 a tag number 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. After configuring the WAN physical interface, go to the **Connection Setup** tab to configure the Internet connection method.

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	Cellular(5G/LTE)	Always on	<button>Edit</button>
WAN-2	Ethernet	Always on	<button>Edit</button>
WAN-3	-	Disable	<button>Edit</button>

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

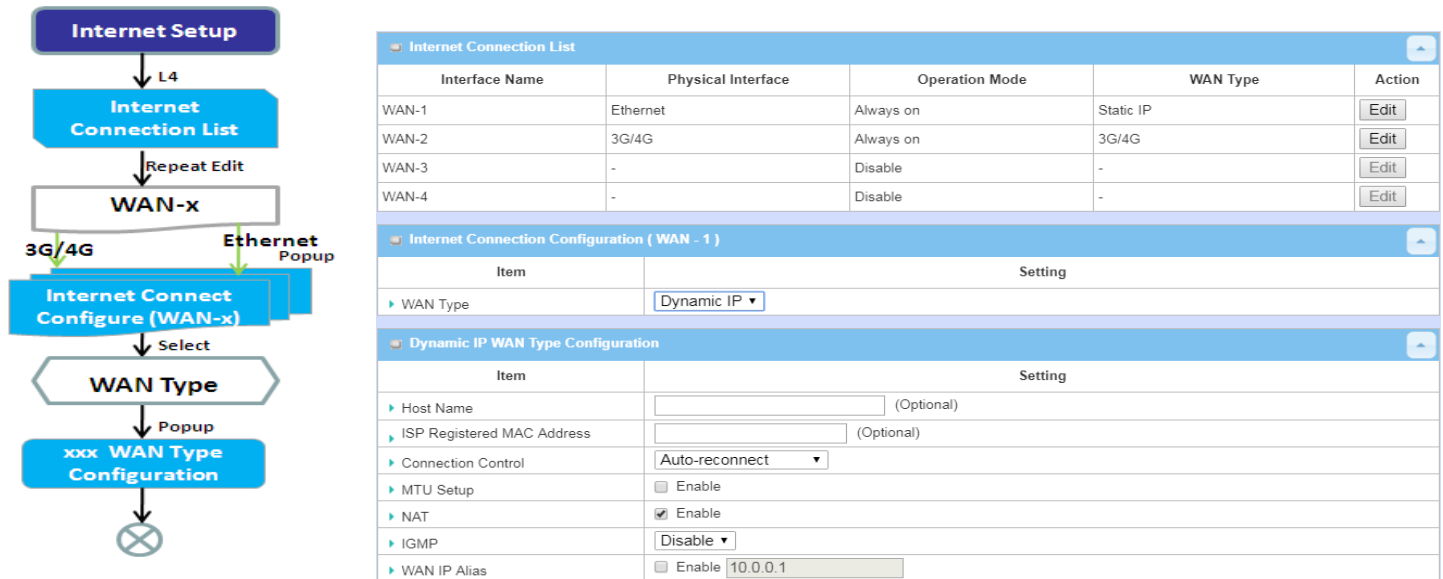
Interface Configuration:

Interface Configuration (WAN-1)	
Item	Setting
▶ Physical Interface	Cellular(5G/LTE) ▾
▶ Operation Mode	Always on ▾
▶ VLAN Tagging	☐ Enable 0 (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 , WiFi Module , and Ethernet . The Disable and Failover options will be available only for models with multiple WAN interfaces. Note: If you want to configure Wi-Fi uplink, select WiFi Module to allow for configuration to connect with a Wi-Fi router for uplink. Go to Basic Network > WiFi > Uplink Profile (refer to 2.3.4 Uplink Profile).
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. <u>Value Range:</u> 1 ~ 4095.

Note: This feature is NOT available for cellular WAN connection.

2.1.2 Connection Setup



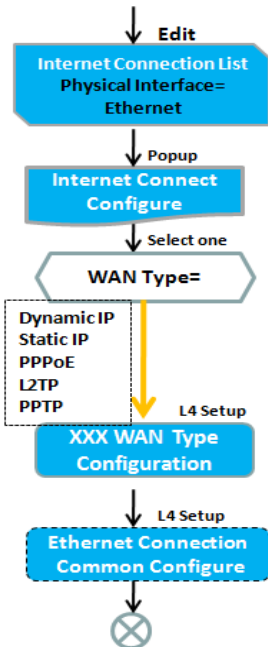
After specifying the physical interface for each WAN connection, you must configure their connection profile according to the ISP's connection requirement to access the Internet.

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 connection of each WAN interface, you must specify its WAN type and then its related connection method for that 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



Internet Connection Configuration (WAN - 1)	
Item	Setting
▶ WAN Type	Dynamic IP ▼ Static IP Dynamic IP PPPoE PPTP L2TP
Dynamic IP WAN Type Conf	
Item	Setting
▶ Host Name	(Optional)
▶ ISP Registered MAC Address	Clone (Optional)
▶ Connection Control	Auto-reconnect ▼
▶ MTU Setup	☐ Enable
▶ NAT	☒ Enable
▶ IGMP	Disable ▼
▶ WAN IP Alias	☐ Enable 10.0.0.1
Network Monitoring Configuration	
Item	Setting
▶ Network Monitoring Configuration	☒ Enable
▶ Checking Method	DNS Query ▼
▶ Loading Check	☒ Enable
▶ Query Interval	5 (seconds)
▶ Latency Threshold	3000 (ms)

WAN Type for Ethernet Interface:

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 subscribe 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.
- 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

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

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

Dynamic IP WAN Type Configuration	
Item	Setting
▶ Host Name	(Optional)
▶ ISP Registered MAC Address	Clone (Optional)

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

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

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

Static IP WAN Type Configuration	
Item	Setting
▶ WAN IP Address	
▶ WAN Subnet Mask	255.255.255.0 (/24) ▼
▶ WAN Gateway	
▶ Primary DNS	
▶ Secondary DNS	(Optional)

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.

WAN Type: PPPoE

Internet Connection Configuration (WAN - 1)

Item	Setting
▶ WAN Type	PPPoE ▼

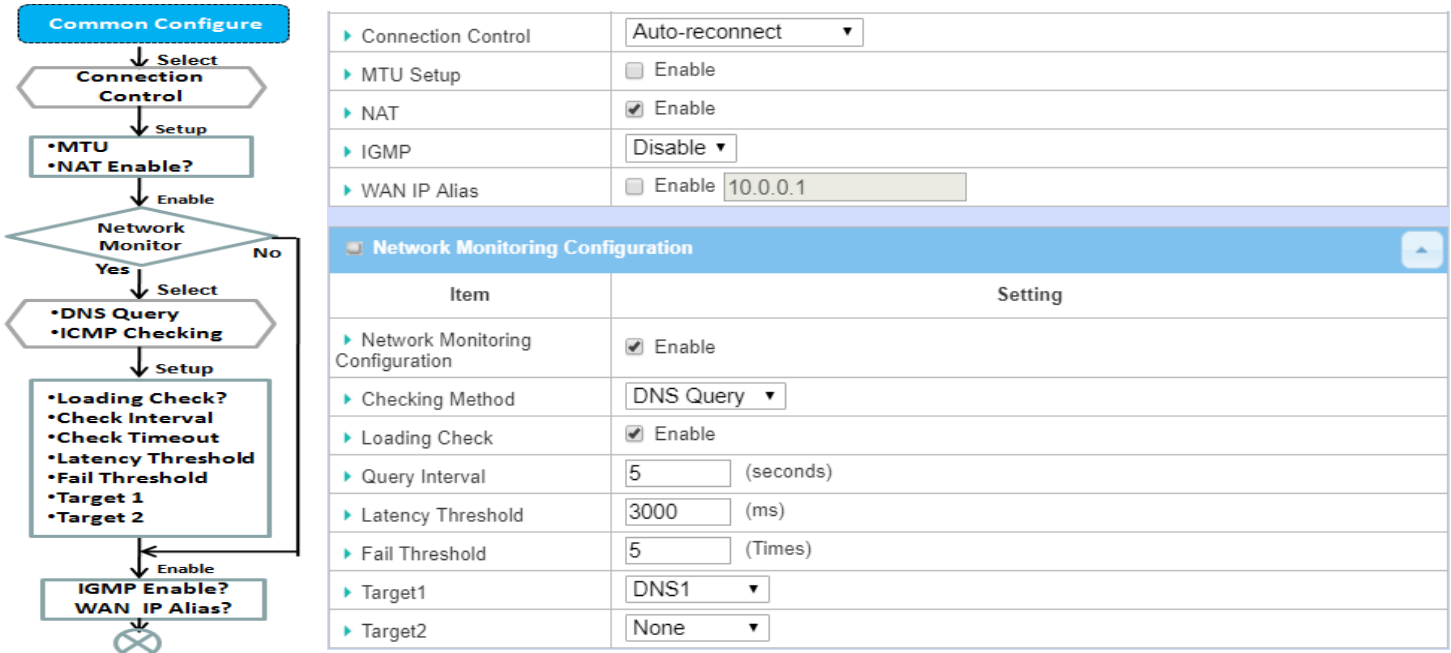
Select **PPPoE** to open **PPPoE WAN Type Configuration**.

PPPoE WAN Type Configuration

Item	Setting
▶ IP Type	IPv4 ▼
▶ PPPoE Account	
▶ PPPoE Password	
▶ Primary DNS	(Optional)
▶ Secondary DNS	(Optional)
▶ Service Name	(Optional)
▶ Assigned IP Address	(Optional)

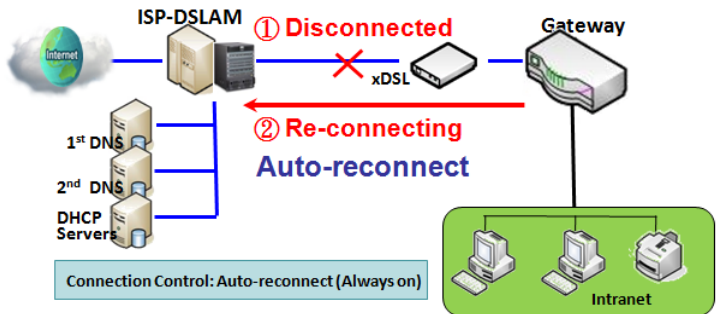
PPPoE WAN Type Configuration		
Item	Value setting	Description
PPPoE Account	A must-filled setting	Enter the PPPoE username provided by your ISP.
PPPoE Password	A must-filled setting	Enter the PPPoE password provided by your ISP.
Primary DNS	An optional setting	Enter the IP address of Primary DNS server.
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.

Ethernet Connection Common Configuration

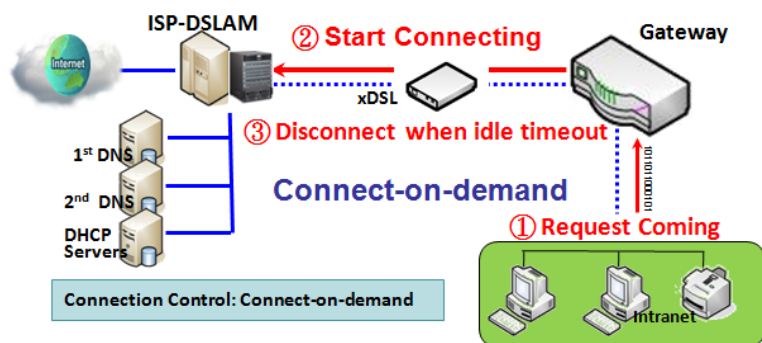


Some parameters need to be configured properly no matter the configured Ethernet WAN type.

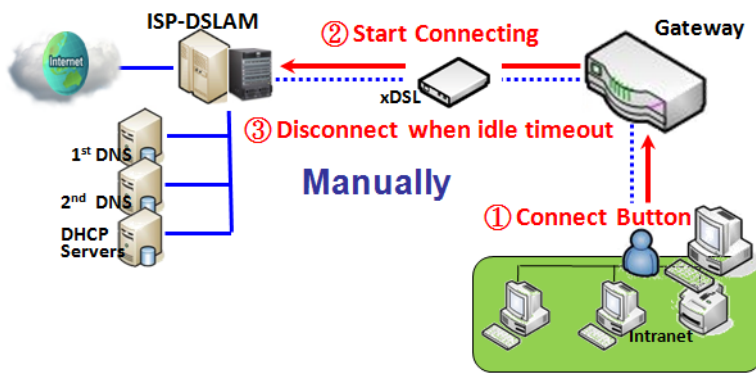
Connection Control.



Auto-reconnect: The gateway will establish an Internet connection automatically once it starts, and try to reconnect. It's recommended to choose this connection type for mission critical applications to ensure uninterrupted Internet connection.



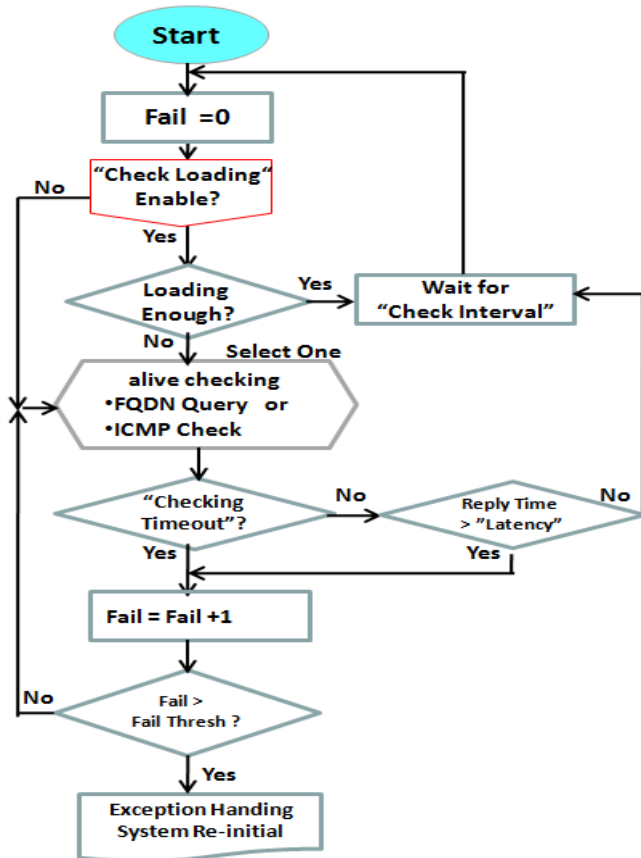
Connect-on-demand: The gateway won't start to establish an Internet connection until local data is detected on the WAN side. And the gateway will disconnect the established WAN connection once it reaches the Maximum Idle Time.



Manually: This gateway won't start to establish an Internet connection until you click the "Connect" button on Web UI. And the gateway will disconnect the established WAN connection once it reaches the Maximum Idle Time.

Note that if a WAN interface serves as the primary connection in Failover role, the connection control will automatically be set to "Auto-reconnect (Always on)".

Network Monitoring



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

Ethernet WAN Common Configuration		
Item	Value setting	Description
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. By default 600 seconds is filled-in	Specify the maximum Idle time after which the Internet will be disconnected. <u>Value Range:</u> 300 ~ 86400. Note: This field is available only when Connect-on-demand or Connect Manually is selected as the connection control scheme.
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. <u>Value Range:</u> 1200 ~ 1500.
MTU Setup	1. A must-filled setting 2. Auto (value zero) is set by default 3. Manual set range 1200~1500	MTU refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. When set to Auto (value '0'), the router selects the best MTU for best Internet connection performance.
NAT	1. An optional setting 2. 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 IP Alias	1. An optional setting 2. Uncheck by default	Enable WAN IP Alias then enter the IP address provided by your service provider. WAN IP Alias assigns dual WAN IP addresses.

 Network Monitoring Configuration


Item	Setting
▶ Network Monitoring Configuration	☒ Enable
▶ Checking Method	DNS Query ▼
▶ Loading Check	☒ Enable
▶ Query Interval	5 (seconds)
▶ Latency Threshold	3000 (ms)
▶ Fail Threshold	5 (Times)
▶ Target1	DNS1 ▼
▶ Target2	None ▼

Network Monitoring Configuration

Item	Value setting	Description
Network Monitoring Configuration	1. 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 usings 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. <u>Value Range:</u> 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. <u>Value Range:</u> 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. <u>Value Range:</u> 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. <u>Value Range:</u> 1 ~ 10 times.
Target 1	1. An optional setting	Target1 specifies the first target of sending a DNS query/ICMP request.

	2. DNS1 is selected by default	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.
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

Physical Interface
Connection Setup
Load Balance
Widget

Internet Connection List

Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Cellular(5G/LTE)	Always on	Cellular	Edit
WAN-2	-	Disable	-	Edit
WAN-3	-	Disable	-	Edit

Internet Connection Configuration (WAN-1)

Item	Setting
WAN Type	Cellular

Cellular WAN Type Configuration

Item	Setting
Preferred SIM Card	SIM-A First Failback : ☐ Enable
Auto Flight Mode	☐ Enable
SIM Switch Policy	Policy Setting

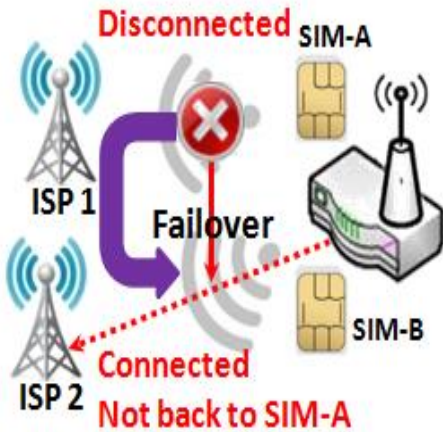
Connection with SIM-A Card

Item	Setting
Network Type	Auto
Dial-Up Profile	Manual-configuration
APN	
IP Type	IPv4
PIN Code	(Optional)
Dial Number	(Optional)
Account	(Optional)
Password	(Optional)
Authentication	Auto
IP Mode	Dynamic IP
Primary DNS	(Optional)
Secondary DNS	(Optional)
Roaming	☐ Enable

Preferred SIM Card – Dual SIM Fail Over

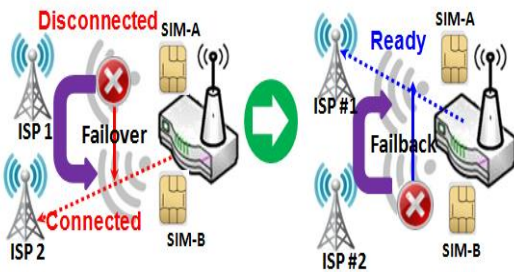
For devices with mobile connectivity, one embedded cellular module can be used for only one WAN interface. This device uses dual SIM cards with advanced failover mechanism. This feature is useful for switching between different mobile network carriers when the location is changed. The “Dual SIM Failover” 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 is used for connection, and when the connection is broken, the gateway will switch to SIM-B. When SIM-A connection is recovered, it will switch back to 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.

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

Cellular WAN Type Configuration	
Item	Setting
▶ Preferred SIM Card	SIM-A First ▼ Fallback : ☐ Enable
▶ Auto Flight Mode	☐ Enable
▶ SIM Switch Policy	Policy Setting

Cellular WAN Type Configuration		
Item	Value setting	Description
WAN Type	1. A must-filled setting 2. 3G/4G is set by default.	From the dropdown box, select Internet connection method for 3G/4G WAN Connection. Only Cellular (5G/LTE) is available.
Preferred SIM Card	1. A must-filled setting 2. By default SIM-A First is selected 3. Fallback 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 Fallback 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: Fallback 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, <i>"Flight mode will cause cellular function to be malfunctioned when the data session is offline."</i>, 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	Setting
▶ Failed connection	0 (1-10) times
▶ RSSI Monitor	☐ Enable Threshold: - 0 (-90~-113 dBm)
▶ Network Service	☐ Enable Loss LTE signal: 0 (1~30 minutes)
▶ Roaming Service	☐ Enable Timeout: 0 (1~30 minutes)

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

Connection with SIM-A Card	
Item	Setting
▶ Network Type	Auto ▼
▶ Dial-Up Profile	Manual-configuration ▼
▶ APN	
▶ IP Type	IPv4 ▼
▶ PIN Code	(Optional)
▶ Dial Number	(Optional)
▶ Account	(Optional)
▶ Password	(Optional)
▶ Authentication	Auto ▼
▶ IP Mode	Dynamic IP ▼
▶ Primary DNS	(Optional)
▶ Secondary DNS	(Optional)
▶ Roaming	☐ Enable

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	Select Auto to register a network automatically, regardless of the network

	2. By default Auto is selected	type. Select LTE only to register the 4G LTE network only. Select 5G SA to register the 5G network. 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 automatically configure the required information 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 provides 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. Select None not to use any authentication method. Note: This setting is only available when Manual-configuration is selected.
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 automatically. Select Static IP mode and fill in all the following settings: IP address, subnet mask, and gateway. Note: IP Subnet Mask is a must-filled setting. Please be sure to set up the configuration correctly.
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	Enter the IP address of the secondary DNS (Domain Name Server) setting

	2. String format : IP address (IPv4 type)	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**.

SIM-A APN Profile List Add Delete									
ID	Profile Name	APN	IP Type	Account	Password	Authentication	Priority	Enable	Actions

Click Add to open the APN Profile Configuration screen.

SIM-A APN Profile Configuration	
Item	Setting
▶ Profile Name	Profile-1
▶ APN	
▶ IP Type	IPv4 ▼
▶ Account	(Optional)
▶ Password	(Optional)
▶ Authentication	Auto ▼
▶ Priority	
▶ Profile	☐ Enable

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. <i>Value Range:</i> 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 2. String format: integer	Enter a value (from 1-16) for the dial-up process where a dial-up will start from a profile of the smallest number. <i>Value Range:</i> 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.

Set up Cellular Connection Common Configuration

Here you can change common configurations for cellular WAN.

Cellular Connection Common Configuration	
Item	Setting
▶ Connection Control	Connect Manually ▾
▶ Maximum Idle Time	600 (seconds)
▶ Time Schedule	(0) Always ▾
▶ MTU Setup	☐ Enable
▶ IP Passthrough (Cellular Bridge)	☐ Enable
▶ NAT	☐ Enable
▶ IGMP	Disable ▾

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 Disconnect 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. <u>Value Range:</u> 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. <u>Value Range:</u> 1200 ~ 1500.
IP Pass-through (Cellular Bridge)	1. The box is unchecked by default 2. String format for Fixed MAC: MAC address, e.g. 00:50:18:aa:bb:cc	Enable this function to assign a WAN IP to the first connected local LAN client. Note: When the IP Pass-through is enabled, NAT will be unavailable.
NAT	Check by default	Enable or disable the 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.

Network Monitoring Configuration

Item	Setting
▶ Network Monitoring Configuration	☒ Enable
▶ Checking Method	DNS Query ▼
▶ Loading Check	☒ Enable
▶ Query Interval	5 (seconds)
▶ Latency Threshold	3000 (ms)
▶ Fail Threshold	5 (Times)
▶ Target1	DNS1 ▼
▶ Target2	None ▼

Network Monitoring Configuration

Item	Value setting	Description
Network Monitoring Configuration	1. 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 connection liveness by sending DNS query to the destination specified in Target 1 and Target 2. With ICMP Checking , the system checks connection liveness by sending ICMP requests to the destination specified in Target 1 and Target 2. With Traffic Check , the system checks connection liveness by detecting the traffic flow coming through the interface.
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 packets. With DNS Query , the system checks the connection by sending DNS query packets to the destination specified in Target 1 and Target 2 . <u>Value Range:</u> 2 ~ 14400.
Check Interval	1. An Optional setting 2. 5 seconds is selected by default.	Specify a time interval for the ICMP Checking or Traffic Check . For ICMP Check, specify an ICMP Checking interval to define the transmitting interval between two ICMP check packets. For Traffic Check, enter how often the system should perform this check method. <u>Value Range:</u> 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. <u>Value Range:</u> 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. <u>Value Range:</u> 1 ~ 10 times.
Target 1	1. An Optional filled setting 2. DNS1 is selected by default	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 filled setting 2. None is selected by default	Target1 specify 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.

Internet Connection – WiFi Uplink WAN

Go to Basic Network > WAN & Uplink > Connection Setup.

WiFi Uplink Interface: The device can connect to a Uplink network through the current WiFi connection.

The device can be connected to another network through the WiFi Uplink connection function. This device supports 802.11ac/n/g/b WiFi standards to connect to a wireless network (access point).

Internet Connection List				
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet	Always on	Static IP	Edit
WAN-2	WiFi Module One	Always on	Uplink	Edit
WAN-3	-	Disable	-	Edit
WAN-4	-	Disable	-	Edit

Configure WiFi Uplink Setting

The **Internet Connection Configuration** screen will appear when you click the **Edit** button. WAN-2 interface is used in this example.

Internet Connection Configuration (WAN - 2)	
Item	Setting
WAN Type	Uplink ▼

Internet Connection Configuration		
Item	Value setting	Description
WAN Type	1. A must-filled setting. 2. Uplink is selected by default.	Select Internet connection method for WiFi Uplink Connection: Uplink .

WiFi Uplink

WiFi Uplink WAN Type Configuration

Item	Setting
▶ Connect to AP	Only_For_Monkey-Ch#1-WPA2-PSK (AES) Scan Edit
▶ Network Type	NAT Mode ▼
▶ IP Mode	Dynamic IP ▼
▶ Host Name	(Optional)
▶ Connection Control	Connect Manually ▼
▶ Maximum Idle Time	86400 (seconds)
▶ Fast Roaming	☐ Enable Signal Threshold 40 %
▶ Fast Roaming Channels	N/A ▼ N/A ▼ N/A ▼

WiFi Uplink WAN Type Configuration		
Item	Value setting	Description
Connect to AP	N/A	Display the information of AP for connecting. You can Click the Scan button and select a AP for the uplink network.
Network Type	1. A must-filled setting 2. NAT Mode is selected by default.	Select the expected network type for the WiFi Uplink connection. It can be NAT Mode , Bridge Mode , or NAT Disable . When NAT Mode is selected, the NAT function is activated on the Wireless Uplink connection; When Bridge Mode is selected, the bridge function is activated on the Wireless Uplink connection; The supporting of bridge mode depends on the product specification, if the purchased device doesn't support the bridge mode, it will be greyed out from selection. When NAT Disable is selected, the NAT function is deactivated on the Wireless Uplink connection, and it can function as a router with manually configured routing setting.
IP Mode	1. A must-filled setting 2. Dynamic IP is selected by default.	Specify the IP mode for the wireless uplink Interface. It can be Dynamic IP or Static IP . When Dynamic IP is selected, the device will request a IP from the Uplink Network as the IP for the uplink interface ; When Static IP is selected, you have to manually configure the IP address settings for the uplink interface. The settings include IP address, subnet mask, gateway, and primary/secondary DNS.
Connection Control	A must-filled setting	There are three connection modes: • Auto-reconnect (Always on) keeps the Internet connection on whenever a physical link is connected. • Connect-on-demand establishes the Internet connection whenever data traffic is detected. Internet connection will be disconnected when it has been inactive for the specified idle time. • Connect Manually establishes the Internet connection through manual dial-up settings.
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. <u>Value Range</u> : 300 ~ 86400. Note: This field is available only when Connect-on-demand or Connect

		Manually is selected as the connection control scheme.
Fast Roaming	1. An Optional setting 2. Unchecked is selected by default.	Click the Enable checkbox to activate the fast roaming function. You can also specify a threshold value for changing from one AP to another near-by AP. The default threshold value is 40%. <u>Value Range:</u> 30 ~ 60%.
Fast Roaming Channels	1. An Optional setting 2. N/A is selected by default.	You can specify up to three channels for WiFi Uplink fast roaming function. If you didn't specify a channel, the WiFi uplink will just use the currently connected channel.

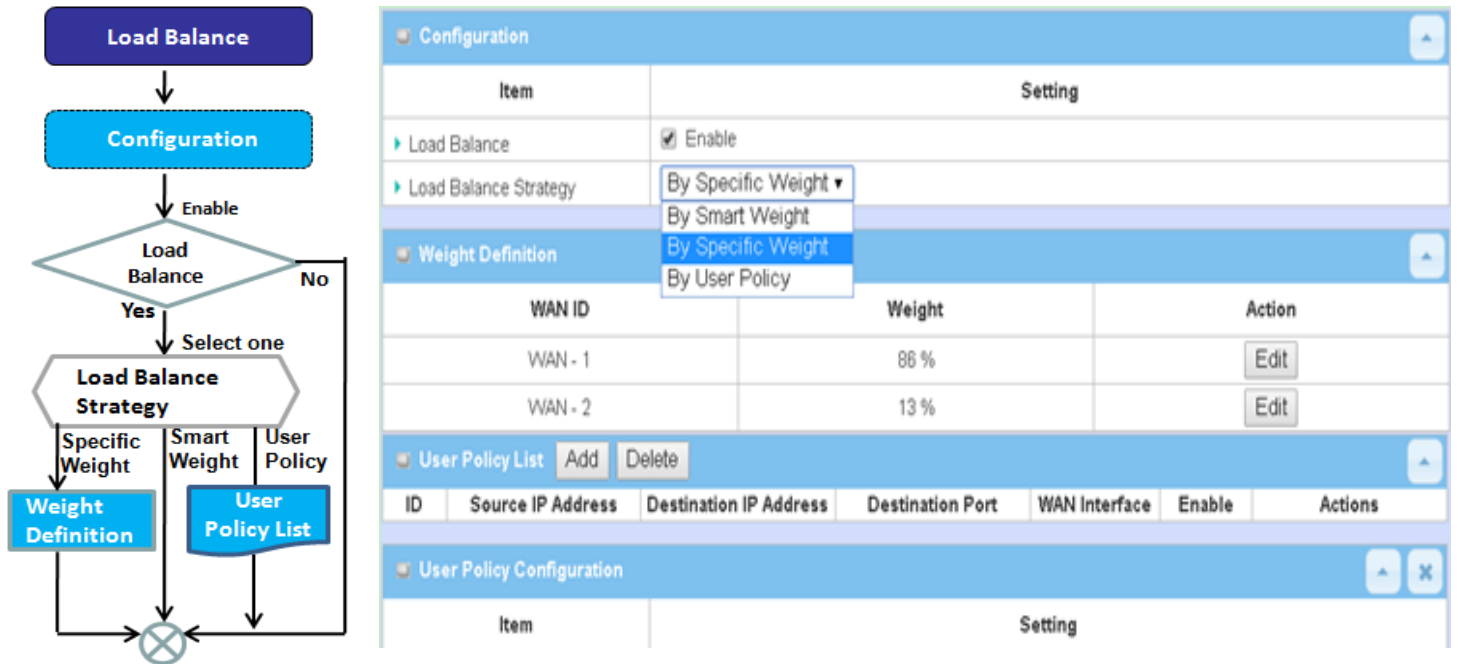
Network Monitoring

Network Monitoring Configuration	
Item	Setting
▶ Network Monitoring Configuration	☒ Enable
▶ Checking Method	DNS Query ▼
▶ Loading Check	☒ Enable
▶ Query Interval	5 (seconds)
▶ Latency Threshold	3000 (ms)
▶ Fail Threshold	5 (Times)
▶ Target1	DNS1 ▼
▶ Target2	None ▼

Network Monitoring Configuration		
Item	Value setting	Description
Network Monitoring Configuration	1. 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 . <u>Value Range:</u> 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. <u>Value Range:</u> 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. <u>Value Range:</u> 2000 ~ 3000 seconds.
Fail Threshold	1. An Optional setting 2. 5 times is set by default	Specify a number as the threshold times for disconnection detection before disconnection is acknowledged. Fail Threshold specifies the number of detected disconnection checks before the gateway recognizes the WAN link down status. <u>Value Range:</u> 1 ~ 10 times.
Target 1	1. An Optional filled setting 2. DNS1 is selected by default	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. gateway: the current gateway is set as the target. Other Host: enter an IP address to be the target.
Target 2	1. An Optional filled setting 2. None is selected by default	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. gateway: the Current gateway 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.

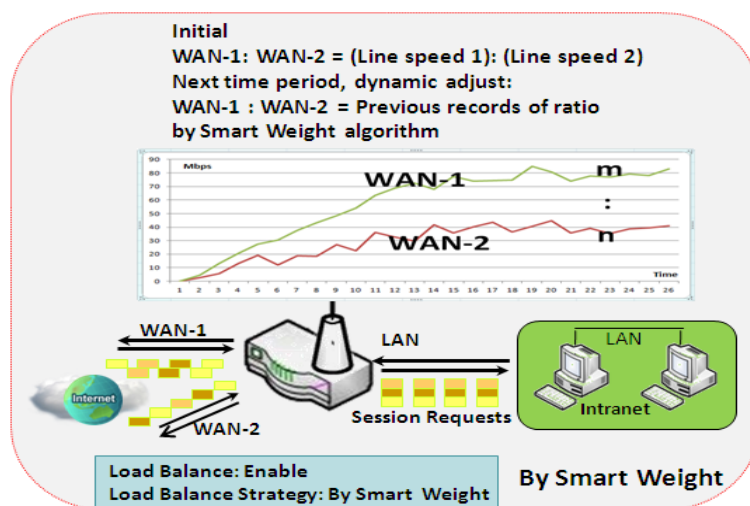
2.1.3 Load Balance



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.

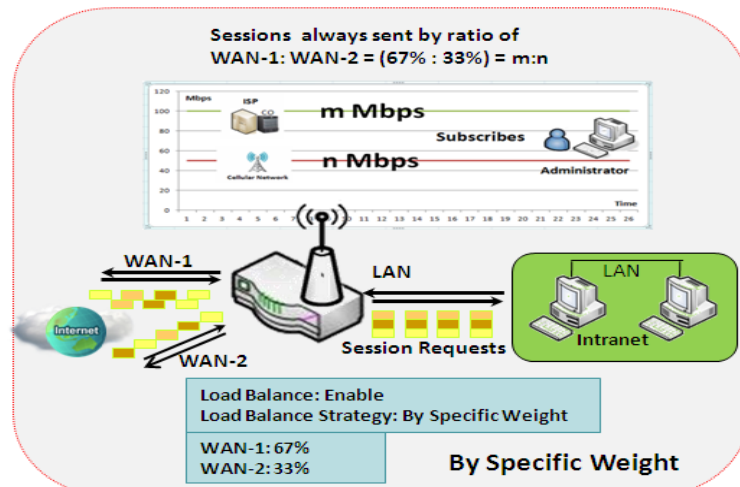
Load Balance Strategy

There are three optional strategies for load balance: **"By Smart Weight"**, **"By Specific Weight"**, and **"By User Policy"**. You can select strategy according to application requirement and environment status. The strategies are explained as below.



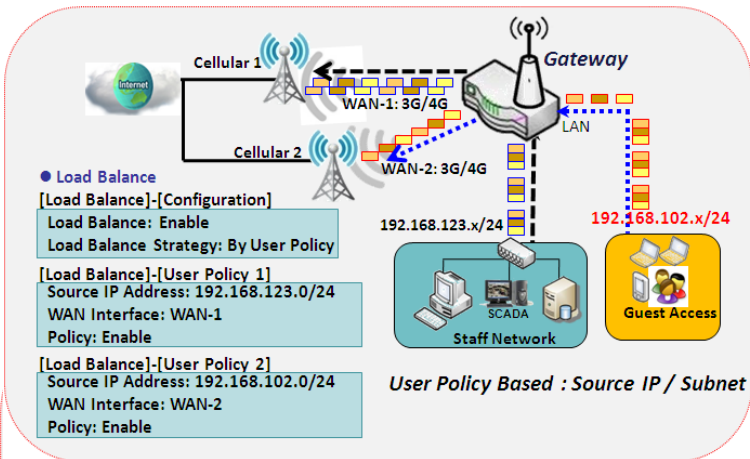
By Smart Weight

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.



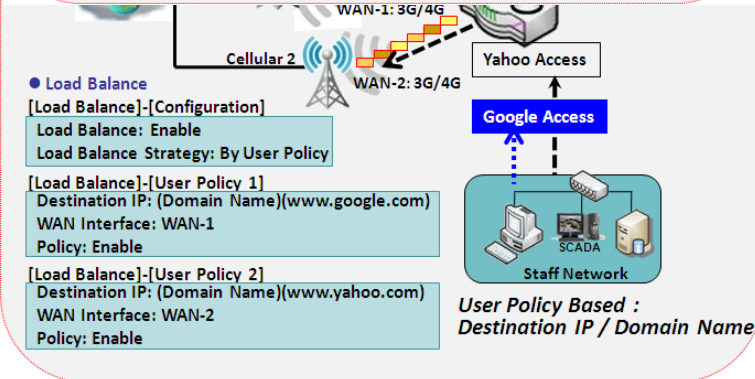
By Specific Weight

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 interface. 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 Strategy

Configuration		
Item	Setting	
▶ Load Balance	☐ Enable	
▶ Load Balance Strategy	By Specific Weight ▼	

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

Weight Definition		
Item	Value setting	Description
WAN ID	NA	The Identifier for each available WAN interface.

Weight	1. A must-filled setting 2. Set with bandwidth ratio of each WAN by default.	Enter a weight for each WAN interface by clicking Edit . <u>Value Range</u> : 1 ~ 99. Note : The sum of all weights can't be greater than 100%.
Save	NA	Save the configuration
Undo	NA	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

User Policy List Add Delete ⬆						
ID	Source IP Address	Destination IP Address	Destination Port	WAN Interface	Enable	Actions

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

User Policy Configuration ⬆ ✕	
Item	Setting
▶ Source IP Address	Any ▼
▶ Destination IP Address	Any ▼
▶ Destination Port	All ▼
▶ Protocol	Both ▼
▶ WAN Interface	WAN - 1 ▼
▶ Policy	☐ Enable

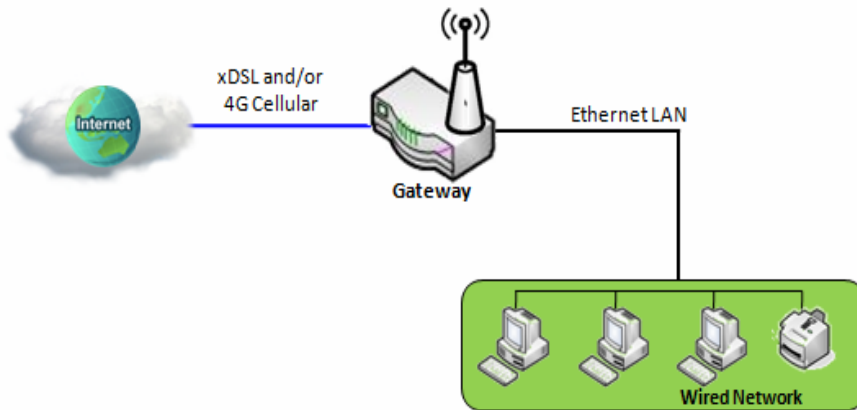
User Policy Configuration		
Item	Value setting	Description
Source IP Address	1. A must-filled setting 2. Any is selected by default.	There are four options for Source IP Address: Any : Select this option for traffic that comes from any source. Subnet : Specify the subnetwork of the source address. Input 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	Setting
IP Mode	Static IP
LAN IP Address	192.168.0.1
Subnet Mask	255.255.255.0 (/24)

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).

<u>Value Range:</u> 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.

Additional IP Add Delete ↑ ×						
ID	Name	Interface	IP Address	Subnet Mask	Enable	Action

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

Additional IP Configuration ↑ ×	
Item	Setting
▶ Name	
▶ Interface	lo ▼
▶ IP Address	
▶ Subnet Mask	255.255.255.0 (/24) ▼
▶ Enable	☐
Save	

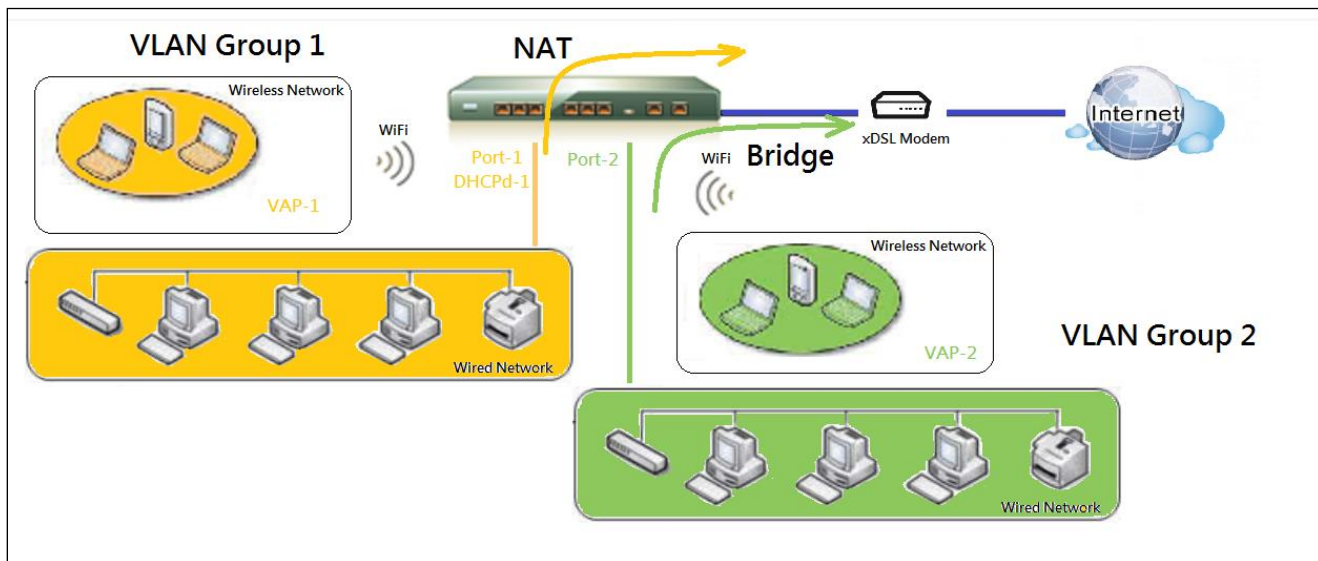
Configuration		
Item	Value setting	Description
Name	1 An optional setting	Enter a name for the alias IP address.
Interface	1. A must-filled setting 2. lo is set by default	Specify the Interface type : lo or br0 .
IP Address	1. An optional setting 2. 192.168.0.1 is the default IP address of this gateway	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). <u>Value Range:</u> 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 requirements. 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.

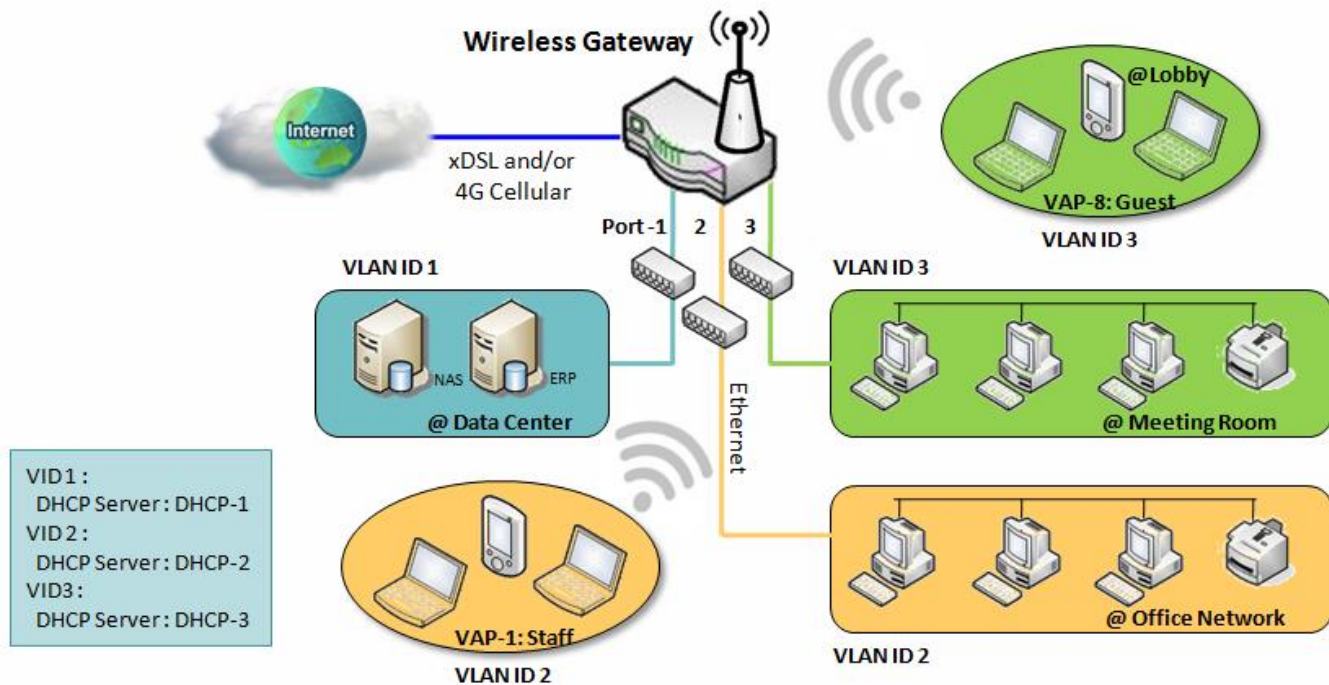
➤ Port-based VLAN

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 assignment 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.



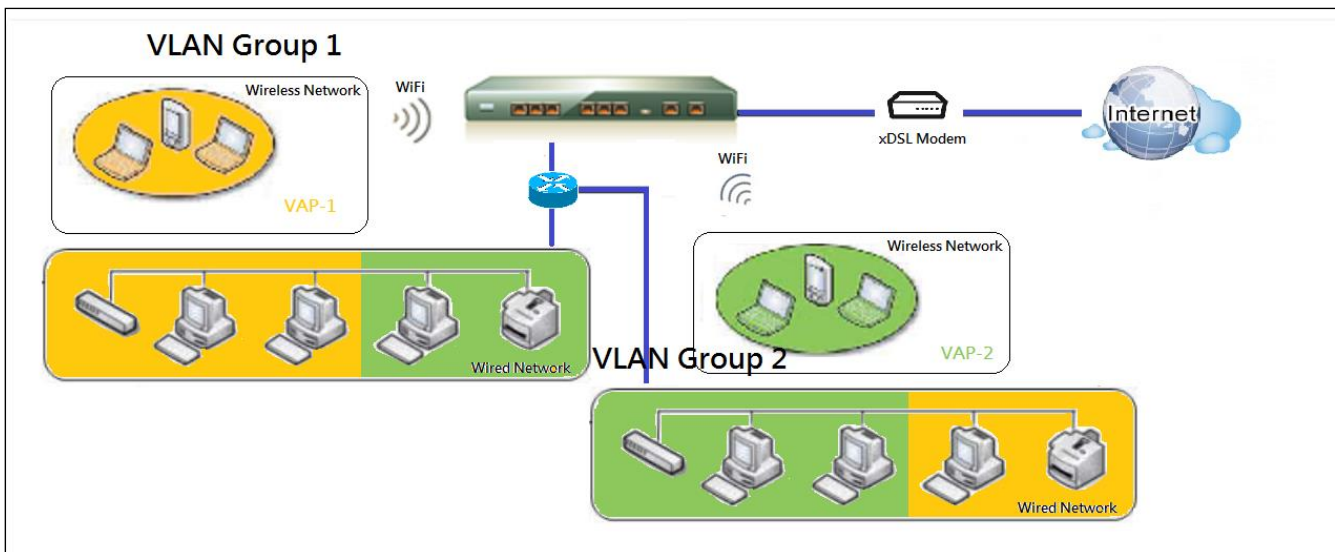
A port-based VLAN is a group of ports on a gateway that forms a logical LAN segment.

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.

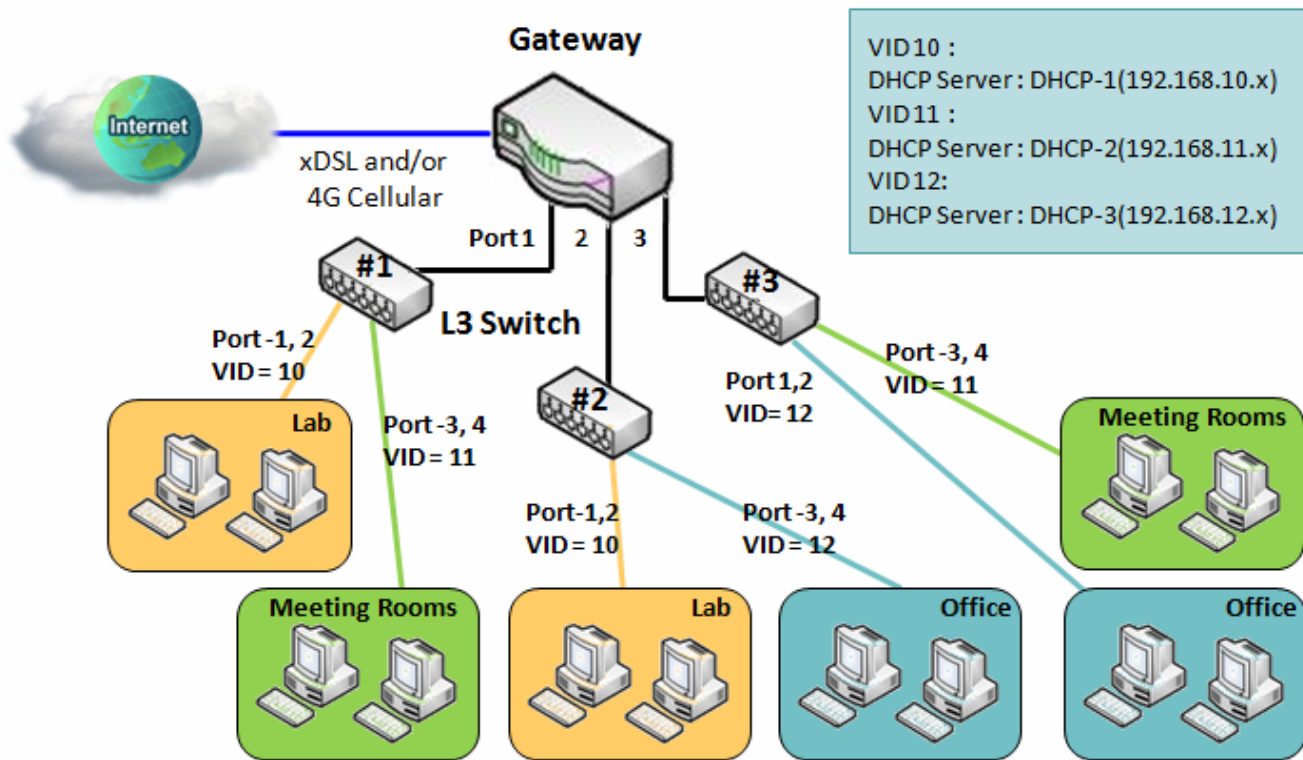


➤ Tagged VLAN

Tagged VLAN function allows you to group hosts from different geographic 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).

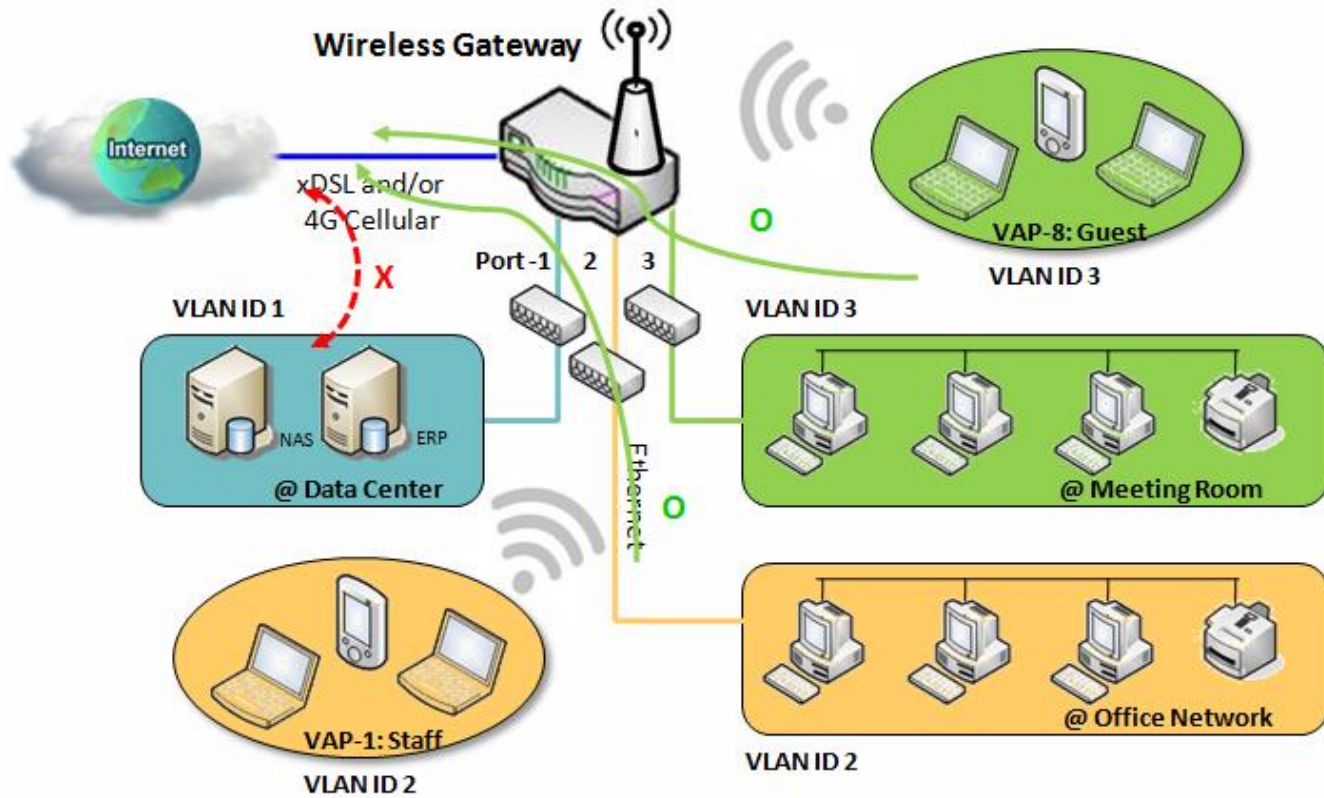


➤ VLAN Groups Access Control

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.

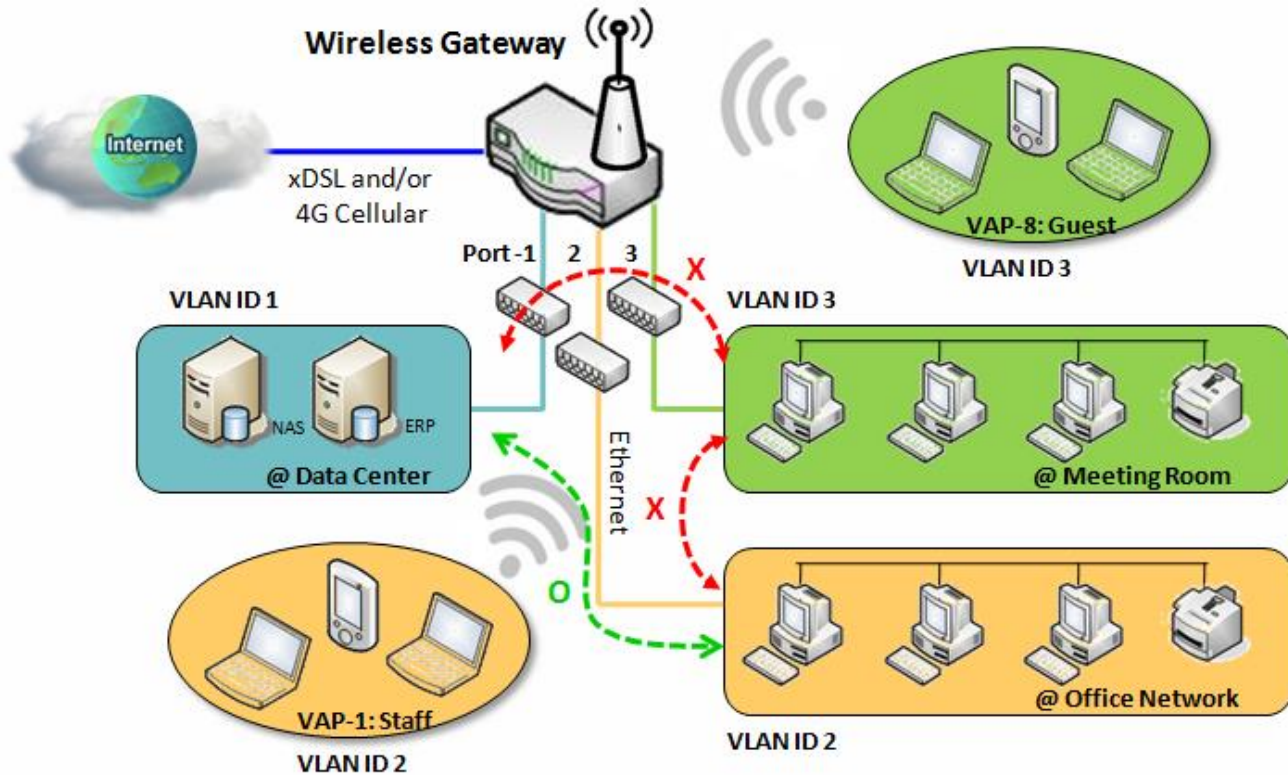
VLAN Group Internet Access

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	Setting
VLAN Types	Port-based ▼
System Reserved VLAN ID	Start ID 1 (1-4091) ~ End ID 5

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. <u>Value Range:</u> 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.

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

Apply Inter VLAN Group Routing

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	
Item	Setting
▶ Name	VLAN - 1
▶ VLAN ID	
▶ VLAN Tagging	Disable ▼
▶ NAT / Bridge	NAT ▼
▶ Port Members	Port: ☐ Port-2 ☐ Port-3 2.4G: ☐ VAP-1 ☐ VAP-2 ☐ VAP-3 ☐ VAP-4 ☐ VAP-5 ☐ VAP-6 ☐ VAP-7 ☐ VAP-8 5G: ☐ VAP-1 ☐ VAP-2 ☐ VAP-3 ☐ VAP-4 ☐ VAP-5 ☐ VAP-6 ☐ VAP-7 ☐ VAP-8
▶ LAN to Join	☐ Enable DHCP 1 ▼

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.

▶ WAN & WAN VID to Join	All WANs ▼ None
▶ LAN IP Address	192.168.2.254
▶ Subnet Mask	255.255.255.0 (/24)
▶ DHCP Server / Relay	Server ▼
▶ DHCP Server Name	
▶ IP Pool	Starting Address: 192.168.2.100 Ending Address: 192.168.2.200
▶ Lease Time	86400 seconds
▶ Domain Name	(Optional)
▶ Primary DNS	(Optional)
▶ Secondary DNS	(Optional)
▶ Primary WINS	(Optional)
▶ Secondary WINS	(Optional)
▶ Gateway	(Optional)
▶ Enable	☐

Port-based VLAN Configuration (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. <u>Value Range:</u> 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.

IP Fixed Mapping Rule List Add Delete			
MAC Address	IP Address	Enable	Actions

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 List

Add

Delete

⬆

✖

Name	VLAN ID	VLAN Tagging	NAT / Bridge	Port Members	LAN IP Address	Subnet Mask	Joined WAN	WAN VID	Enable	Actions
LAN	Native VLAN Tag 1	X	NAT	Detail	192.168.66.1	255.255.254.0	All WANs	0	☒	Edit

Apply

Inter VLAN Group Routing

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.

VLAN Group Internet Access Definition		
VLAN IDs	Members	Internet Access(WAN)
1	Port : 2,3 2.4G VAP: 1,2,3,4,5,6,7,8 5G VAP: 1,2,3,4,5,6,7,8	Allow Edit

Inter VLAN Group Routing		
VLAN IDs	Members	Action
		Edit
		Edit
		Edit
		Edit

[Save](#)

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

VLAN Group Internet Access Definition		
VLAN IDs	Members	Internet Access(WAN)
☒ 1	Port : 2,3 2.4G VAP: 1,2,3,4,5,6,7,8 5G VAP: 1,2,3,4,5,6,7,8	Allow Edit

Inter VLAN Group Routing		
VLAN IDs	Members	Action
☐ 1		Edit
		Edit
		Edit
		Edit

[Save](#)

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.

Tag-based VLAN List Add Delete						
VLAN ID	Internet	Port Members	Bridge Interface	IP Address	Subnet Mask	Actions
Native VLAN	☒	Port: ☒ Port-2 ☒ Port-3 2.4G: ☒ VAP-1 ☒ VAP-2 ☒ VAP-3 ☒ VAP-4 ☒ VAP-5 ☒ VAP-6 ☒ VAP-7 ☒ VAP-8 5G: ☒ VAP-1 ☒ VAP-2 ☒ VAP-3 ☒ VAP-4 ☒ VAP-5 ☒ VAP-6 ☒ VAP-7 ☒ VAP-8	DHCP 1			Edit Select

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

Tag-based VLAN Configuration	
Item	Setting
VLAN ID	0
Internet Access	☒ Enable
Port Members	Port: ☐ Port-2 ☐ Port-3 2.4G: ☐ VAP-1 ☐ VAP-2 ☐ VAP-3 ☐ VAP-4 ☐ VAP-5 ☐ VAP-6 ☐ VAP-7 ☐ VAP-8 5G: ☐ VAP-1 ☐ VAP-2 ☐ VAP-3 ☐ VAP-4 ☐ VAP-5 ☐ VAP-6 ☐ VAP-7 ☐ VAP-8
Bridge Interface	DHCP 1

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. <u>Value Range:</u> 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:

▶ IP Address	
▶ Subnet Mask	255.255.255.0 (/24) ▼
▶ DHCP Relay	☐ Enable & Server IP :
▶ WAN Interface	WAN - 1 ▼
▶ DHCP Relay Option 82	☐ Enable

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

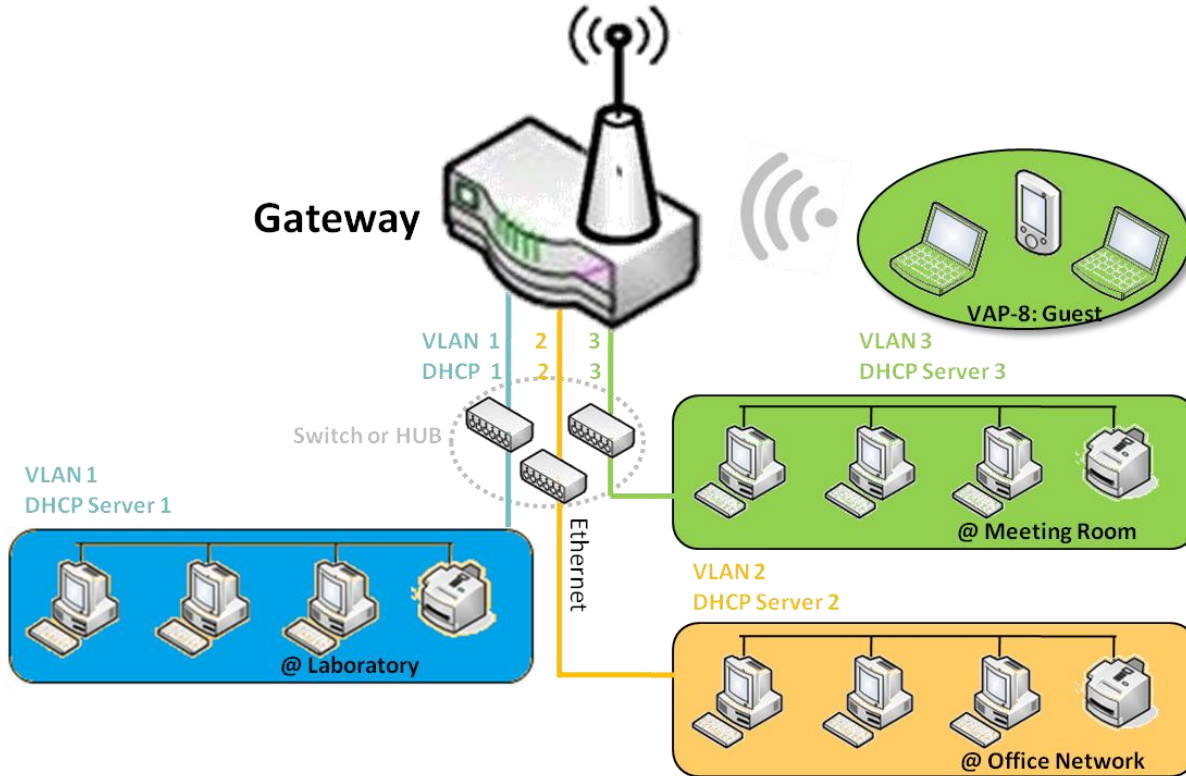
The tagged VLAN group information will be displayed as shown below.

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

2.2.3 DHCP Server

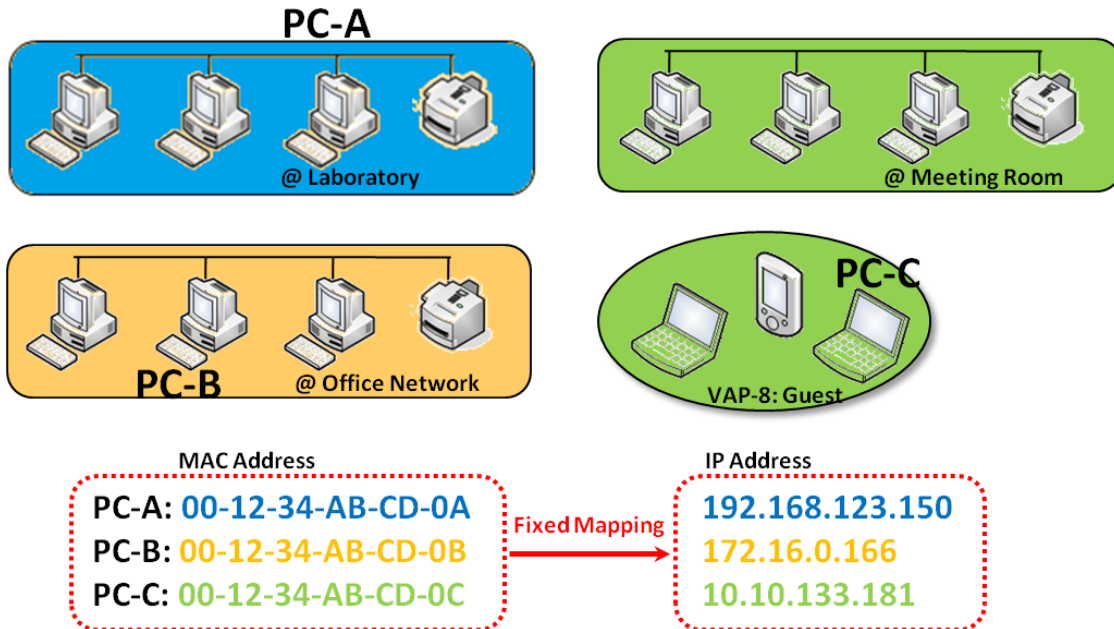
➤ DHCP Server

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 gateway page allows you to configure your DHCP Server settings. If multiple LAN ports are available, you can custom 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 List Add Delete DHCP Client List												
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	Setting
▶ DHCP Server Name	DHCP 2
▶ LAN IP Address	192.168.2.1
▶ Subnet Mask	255.255.255.0 (/24) ▼
▶ IP Pool	Starting Address: Ending Address:
▶ Lease Time	86400 seconds
▶ Domain Name	(Optional)
▶ Primary DNS	(Optional)
▶ Secondary DNS	(Optional)
▶ Primary WINS	(Optional)
▶ Secondary WINS	(Optional)
▶ Gateway	(Optional)

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. Numeric string format. 2. A must-filled setting	Enter the Lease Time for this DHCP Server. <i>Value Range:</i> 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.

Mapping Rule List Add Delete ⬆ ✕			
MAC Address	IP Address	Enable	Actions

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

Mapping Rule Configuration	
Item	Setting
▶ MAC Address	
▶ IP Address	
▶ Rule	☐ Enable

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.

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

DHCP Client List Copy to Fixed Mapping ⬆ ✕					
LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time	Actions

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 DHCP OFFER/DHCPACK packets.

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

Configuration ⬆ ✕	
Item	Setting
▶ DHCP Server Options	☐ Enable

Create / Edit DHCP Server Options

The gateway supports a maximum of 99 DHCP option settings.

DHCP Server Option List Add Delete ↑ ×							
ID	Option Name	DHCP Server Select	Option Select	Type	Value	Enable	Actions

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

DHCP Server Option Configuration	
Item	Setting
▶ Option Name	Option 1
▶ DHCP Server Select	DHCP 1 ▼
▶ Option Select	DHCP OPTION 66 ▼
▶ Type	Single IP Address ▼
▶ Value	
▶ Enable	☐ Enable

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 :		
		TypeValue		
		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.

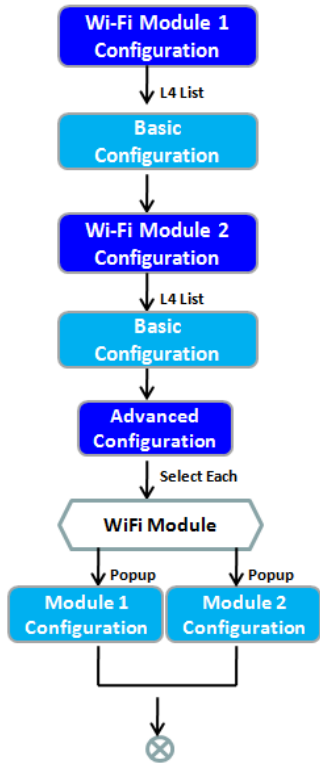
DHCP Relay Configuration List Add Delete ▲ ✕							
ID	Agent Name	LAN interface	WAN interface	Server IP	DHCP Relay Option 82	Enable	Actions

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

DHCP Relay Configuration	
Item	Setting
▶ Agent Name	
▶ LAN interface	LAN ▼
▶ WAN interface	WAN - 1 ▼
▶ Server IP	
▶ DHCP OPTION 82	☐
▶ Enable	☐

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. <u>Value Range:</u> 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 WiFi



Basic Configuration	
Item	Setting
Operation Band	2.4G Single Band

2.4G WiFi Configuration	
Item	Setting
WiFi Module	☒ Enable
Channel	Auto ☒ By AP Numbers ☐ By Less Interference
WiFi System	802.11b/g/n/ax Mixed
Green AP	☐ Enable
VAP Isolation	☒ Enable
Time Schedule	(0) Always

2.4G VAP List								
ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	DTM-550-EEBA	WPA-PSK / WPA2-PSK	TKIP/AES	☐	☒	☒	Edit Select

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 802.11b/g/n/ax standard in 2.4GHz or IEEE 802.11a/n/ac/ax in 5GHz band or 2.4G/5GHz concurrent dual bands.

2.3.1 WiFi Configuration

```

graph TD
    Enable[Enable] --> WiFiModule{WiFi Module}
    WiFiModule -- Yes --> SelectOne[Select one]
    SelectOne --> Modes[AP Router Mode  
WDS Only Mode  
WDS Hybrid Mode]
    Modes --> Profile[Operation Mode Profile Configuration]
    Profile --> APConfig[Multiple AP Configuration]
    APConfig --> End((X))
  
```

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

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
Preshaed 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. To connect your devices wirelessly, choose the operation mode that suits your application needs.

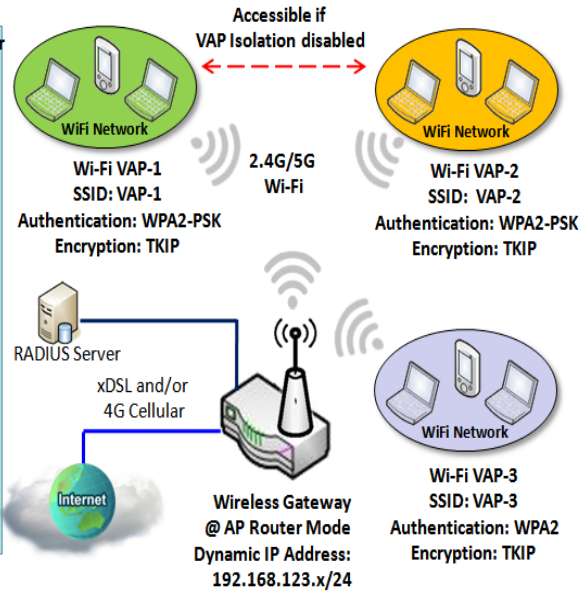
Multiple VAPs

Gateway Settings:

WiFi Operation Mode: AP Router
VAP1
 SSID: VAP-1
 Authentication: WPA2-PSK
 Encryption: TKIP
 Key: 1234567890

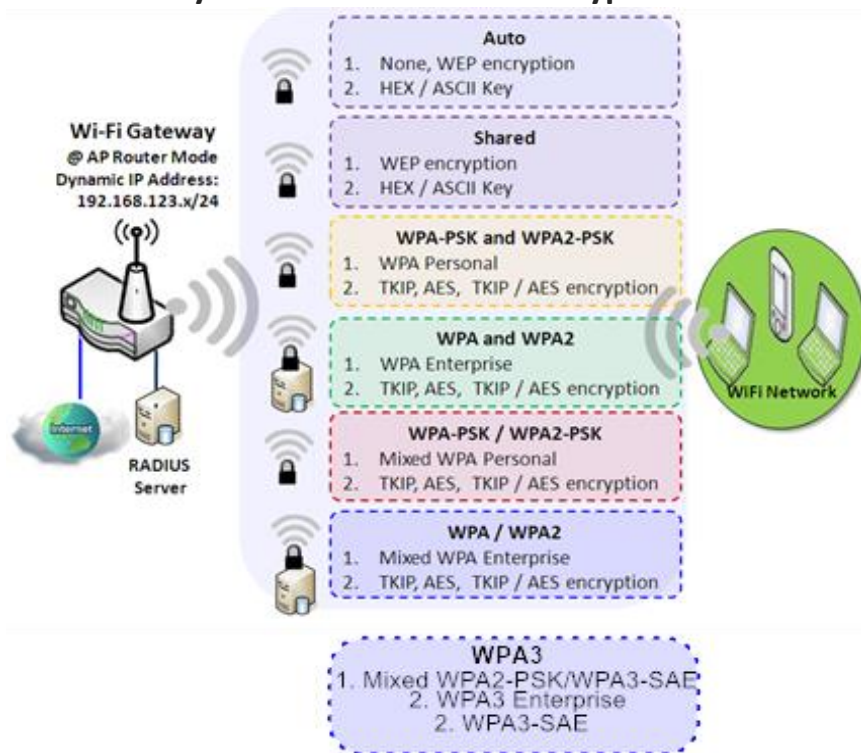
VAP2
 SSID: VAP-2
 Authentication: WPA2-PSK
 Encryption: TKIP
 Key: 1234567890

VAP3
 SSID: VAP-3
 Authentication: WPA2
 Encryption: TKIP
 RADIUS Server IP: 192.168.168.
 RADIUS Server Port: 1812
 RADIUS Shared Key



VAP (Virtual Access Point) is 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 methods as you would for setting a standalone AP. Besides, the VAP Isolation option can 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.

WiFi 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 Open, Shared, WPA-PSK, WPA2-PSK and WPA/WPA2, WPA3-SAE, and WPA3-Enterprise authentication with data encryption methods and RADIUS server authentication and authorization.

WiFi Configuration

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	Setting
▶ Operation Band	2.4G Single Band ▾

Basic Configuration		
Item	Value setting	Description
Operation Band	A must-filled setting	Specify the intended operation band for the Wi-Fi module. The availability of the Operation Band depends on product model.

Configure WiFi Setting

2.4G WiFi Configuration	
Item	Setting
▶ WiFi Module	☒ Enable
▶ Channel	Auto ▾ ☒ By AP Numbers ☐ By Less Interference
▶ WiFi System	802.11b/g/n/ax Mixed ▾
▶ Green AP	☐ Enable
▶ VAP Isolation	☒ Enable
▶ Time Schedule	(0) Always ▾

Configuring WiFi Settings		
Item	Value setting	Description
WiFi 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 by 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).
WiFi 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 the operating wireless standards for the 2.4GHz band:

802.11ax/n/g/b mixed, 802.11 n/g/b mixed, 802.11 g/b mixed, or 802.11b only.

- Select the operating wireless standards for the 5GHz band:
802.11ax/ac/n/a mixed, 802.11ac/n/a mixed, 802.11 n/a mixed, or 802.11a only.

VAPs Configuration

For the AP Router mode, the device supports both client connectivity and the gateway function. The **WAN** port and the **NAT** function are also **enabled** for the **AP Router mode**.

▶ WiFi Operation Mode	AP Router Mode ▾
▶ Green AP	☐ Enable
▶ VAP Isolation	☒ Enable
▶ Time Schedule	(0) Always ▾

AP Router 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.
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.

2.4G VAP List Add Delete								
ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	DTM-550-EEBA	WPA-PSK / WPA2-PSK	TKIP/AES	☐	☒	☒	Edit ☐ Select

By default, VAP 1 is enabled with security settings (WPA-PSK / WPA2-PSK) to connect to the gateway wirelessly to enhance the security level.

Note: The default Wi-Fi key is printed on both the device label and the Security Card. It is strongly recommended that you modify the security key.

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

For VAP 1:

2.4G VAP Configuration	
Item	Setting
VAP	VAP1 ▾
SSID	DTM-550-EE96
Max. STA	☐ Enable
Authentication	WPA2-PSK ▾
Encryption	AES ▾
Preshared Key	
STA Isolation	☐
Broadcast SSID	☒
Enable	☒
Save	

For others:

VAP Configuration	
Item	Setting
VAP	VAP2 ▾
SSID	default
Max. STA	☐ Enable
Authentication	Open ▾
Encryption	None ▾
STA Isolation	☐
Broadcast SSID	☐
Enable	☐

VAP Configuration		
Item	Value setting	Description
SSID	1. String format : Any text	Enter an SSID for your VAP.
Max. STA	The box is unchecked by default.	Enable Max. STA and specify the maximum number of allowed clients.
Authentication/Encryption	1. A must-filled setting 2. VAP1: WPA2-PSK is selected by default; Others: Open is selected by default.	Client stations should provide the key when trying to associate with the device using the correct authentication. When Open is selected ● None: The device uses no encryption. ● WEP: 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. ● 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 WEP key for authentication. HEX: Enter 10 hexadecimal digits (0-9 and A-F).

ASCII: Enter 13 alphanumerical characters. When Auto is selected, the device will use Open or Shared. ● 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, WPA2, and WPA3-Enterprise can be implemented with a RADIUS server. ● 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-PSK or WPA2-PSK is selected, select one of the following encryption method, then enter a pre-shared key. AES Enter a Pre-shared Key with a length from 8 to 63 characters. It is recommended to use AES encryption as it offers the best security. TKIP / AES mixed mode Enter a Pre-shared Key with a length from 8 to 63 characters. When WPA2-PSK is selected, enter a pre-shared key. When WPA3-SAE is selected, enter a preshared key. When mixed WPA2-PSK/WPA3-SAE is selected, wireless clients can associate with this device using either WPA3 or WPA2 with a preshared key.		
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 so that other APs and clients can identify this SSID with wireless scan.
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.

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

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).

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

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.
----------------	-----	-------------------------

Target WiFi
⬆ ✕

Item	Setting
▶ Module Select	One ▼
▶ Operation Band	2.4G ▼
▶ Multiple AP Names	All ▼

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.

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, do not modify these settings; otherwise, errors may occur.

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

Select Target WiFi

Target WiFi
⬆ ✕

Item	Setting
▶ Module Select	One ▼
▶ Operation Band	2.4G ▼

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.

Set up Advanced Configuration

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

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 . <u>Value Range</u> : 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. <u>Value Range</u> : 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. <u>Value Range</u> : 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. <u>Value Range</u> : 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	This option is checked by default	Enable this option use either DFS channel or non-DFS channel according to channel availability. DFS is only available for 5 GHz.
Associate RSSI Threshold	Default is -75	Set the Received Signal Strength Indicator (RSSI) to set the minimum signal strength to keep client connection. <u>Value Range</u> : 0~-100 dBm (10 log P1/1mW). A higher negative value means weaker signal strength.
Save	N/A	Save the current configuration.
Undo	N/A	Restore configuration to previous settings.

2.3.4 Uplink Profile

This device can be connected to an uplink AP or router.

Go to **Basic Network > WiFi > Uplink Profile** to access the **Uplink Profile** page.

Enable Uplink Profile

Note: Configure an Uplink Profile first before enabling it (refer to the below **Add a Profile** section).

Setting Item	Value setting	Description
Profile	Disabled by default	Enable the selected profile setting from the below Profile List. Note: To enable a Wi-Fi profile, you must have configured a profile (refer to below Add a Profile) correctly and apply this configured WiFi module to a WAN interface (go to Basic Network > WAN & Uplink > Physical Interface and click Edit on the selected WAN interface to configure its uplink or Internet connection).
Module Select		It is configurable if multiple modules are present.
Operation Band	A must-filled setting.	Select the band to be used for uplink: 2.4G or 5G .
Priority	A must-filled setting.	Select how profiles should be listed and chosen for uplink connection: by signal strength or with a user-defined priority.
Save	N/A	Save the current configuration.
Undo	N/A	Restore configuration to previous settings.

Add a Profile

Profile Configuration	
Item	Setting
▶ Profile Name	
▶ Network ID (SSID)	Scan
▶ Channel	Auto
▶ Authentication	Open
▶ Encryption	None
▶ MAC Address	
▶ Priority	16
▶ Enable	☒
Save Undo	

Setting Item	Value setting	Description
Profile Name	A must-filled setting	Name this profile.
Network ID (SSID)	A must-filled setting	Enter a network ID (SSID) or click Scan to start scanning available networks.
Channel		Select a channel to use for Wi-Fi uplink.
Authentication	Open, Shared, WPA-PSK, WPA2-PSK, WPA3-SAE	Select the authentication method for connecting with the intended uplink network.
Encryption		Depending on the the above authentication method selected, choose the corresponding encryption method. Then enter the Preshared key for WPA or WEP key for WEP encryption.
MAC Address		Enter the MAC address of the uplink AP.
Priority		Choose the priority for this uplink profile if user-defined is selected in Profile Setting.
Enable		Enable or disable this profile.
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.

2.4.1 IPv6 Configuration

The **IPv6 Configuration** setting allows you to configure IPv6 settings to access the IPv6 network.

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

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 connection to support failover operation.

Main IPv6 Configuration	
Item	Setting
▶ Main IPv6	☒ Enable
▶ WAN Connection Type	IPv6 ▾

Main DHCPv6 WAN Type Configuration	
Item	Setting
▶ DNS	☒ From Server ☐ Specific DNS
▶ Primary DNS	
▶ Secondary DNS	
▶ MLD Snooping	☐ Enable

Main Address Auto-configuration	
Item	Setting
▶ Auto-configuration	☒ Enable
▶ Auto-configuration Type	Stateless ▾
▶ Router Advertisement Lifetime	200 (seconds)

IPv6 Configuration		
Item	Value setting	Description
IPv6	The box is unchecked by default,	Check the Enable box to activate the IPv6 function.
WAN Connection Type	1. A must-filled setting 2. IPv6 is selected by	Define the selected IPv6 WAN Connection Type to establish the IPv6 connectivity via Main / Failover WAN Interface.

default

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

Main IPv6 WAN Type Configuration

DHCPv6 WAN Type Configuration ⬆ ⬇

DNS	☒ From Server ☐ Specific DNS
Primary DNS	
Secondary DNS	
MLD Snooping	☐ Enable

DHCPv6 WAN Type Configuration		
Item	Value setting	Description
DNS	The option [From Server] is selected by default	Select From Server to let the ISP server assign the DNS server automatically. Select the [Specific DNS] option to manually configure 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. MLD snooping prevents flooding of IPv6 multicast packets.

Address Auto-configuration

Address Auto-configuration ⬆ ⬇

Auto-configuration	☒ Enable
Auto-configuration Type	Stateless ▾
Router Advertisement Lifetime	(seconds)

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 2. Stateless is selected by default	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. Router Advertisement Lifetime (A must-filled setting): Enter the gateway Advertisement Lifetime (in seconds). 200 is set by default. <u>Value Range</u> : 0 ~ 65535.
Save		Save the configuration.

2.5 Port Forwarding

Network address translation (NAT) is the method of remapping one IP address 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 let internal servers answer requests from 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 using the same IP address no matter from the a public network or from the LAN.

Configuration Setting

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

Enable NAT Loopback

NAT Loopback	
Item	Setting
▶ NAT Loopback	☒ Enable

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

2.5.2 Virtual Server & Virtual Computer

Configuration

Item	Setting
▶ Virtual Server	☐ Enable
▶ Virtual Computer	☒ Enable

Virtual Server List
 Add Delete

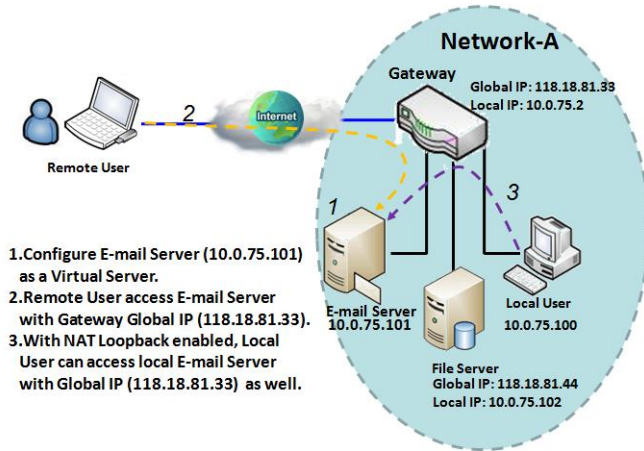
ID	WAN Interface	Server IP	Source IP	Protocol	Public Port	Private Port	Time Schedule	Enable	Actions
----	---------------	-----------	-----------	----------	-------------	--------------	---------------	--------	---------

Virtual Computer List
 Add Delete

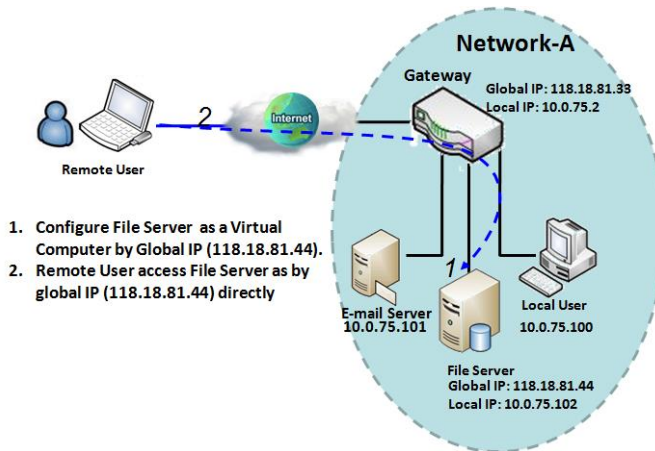
ID	Global IP	Local IP	Enable	Actions
----	-----------	----------	--------	---------

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 can access this mail server using the same global IP address if the NAT loopback 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	Setting
▶ Virtual Server	☐ Enable
▶ Virtual Computer	☒ Enable

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.

Virtual Server List Add Delete									
ID	WAN Interface	Server IP	Source IP	Protocol	Public Port	Private Port	Time Schedule	Enable	Actions

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

Virtual Server Rule Configuration	
Item	Setting
▶ WAN Interface	☒ All ☐ WAN-1 ☐ WAN-2 ☐ WAN-3
▶ Server IP	
▶ Source IP	Any
▶ Protocol	TCP(6) & UDP(17)
▶ Public Port	Single Port
▶ Private Port	Single Port
▶ Time Schedule	(0) Always
▶ Rule	☐ Enable

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 a specified 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 for virtual . Select "TCP" or "UDP" as the protocol used for virtual server. Define the port number used for this service: Specify a Public Port defined from Well-known Service and use it for the corresponding Private Port . Specify a Single Port and enter a correspoing Private Port . Specify a Public Port Range and enter a corresponding Private Port with a Single Port or Port Range. <u>Value Range:</u> 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.

Virtual Computer List Add Delete ↑ ×				
ID	Global IP	Local IP	Enable	Actions

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

Virtual Computer Rule Configuration		
Global IP	Local IP	Enable
		☐

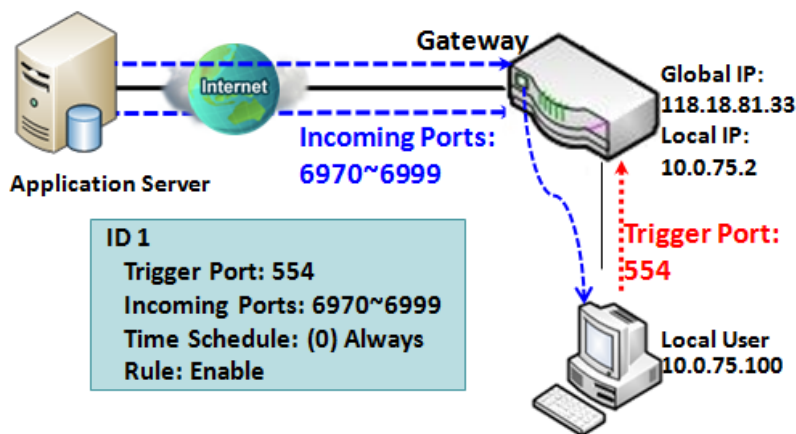
Virtual Computer Rule Configuration		
Item	Value setting	Description
Global IP	A must-filled setting	Specify the WAN IP of the virtual computer.
Local IP	A must-filled setting	Specify the LAN IP of the virtual computer.
Enable	N/A	Enable this rule.
Save	N/A	Save the settings.

2.5.3 Special AP & ALG

The NAT gateway blocks connection requests from an external network. The "Special AP (application)" feature allows applications that require multiple connections such as Internet games, video conferencing, Internet telephony to pass through the NAT gateway. The application-level gateway (ALG) further provides special technique utilizing dynamic address and port translation for specific protocols or applications such as FTP, BitTorrent, Session Initiation Protocol (SIP), Real Time Streaming Protocol (RTSP), and file transfer in Instant messaging (IM) applications.

Special AP

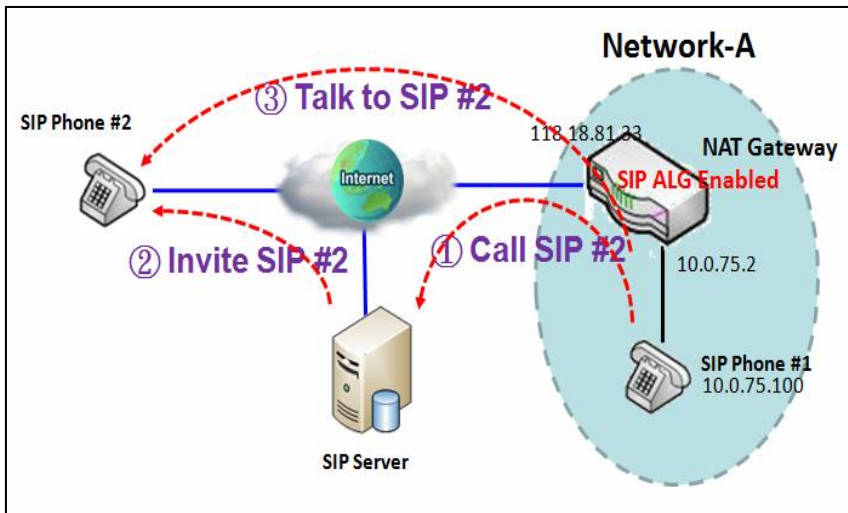
Special AP List Add Delete ▲ ✕						
ID	WAN Interface	Trigger Port	Incoming Ports	Time Schedule	Enable	Actions
1	ALL	554	6970-6999	(0) Always	☒	Edit ☐ Select
2	ALL	47624	2300-2400,28800-29000	(0) Always	☒	Edit ☐ Select



The Special AP feature opens pre-defined service ports for incoming packets to pass through once a port is triggered by local hosts. As shown in the diagram, a special AP rule defines port **554** as the trigger port and **6970~6999** as incoming ports. Thus, the host with the IP address of 10.0.75.100 can use the Quick Time application powered by a media server located over the Internet.

SIP ALG

This gateway supports the SIP ALG feature to allow one SIP phone behind the NAT gateway to call another SIP phone in the Internet. The NAT gateway monitors the traffic and opens the ports dynamically as requested for SIP application layer "control/data" protocols as shown in following diagram.



As shown in the diagram, the SIP Phone #1 initiates a call to the SIP server through the NAT gateway. Then the SIP server invites the SIP Phone #2 to allow calls between SIP Phone #1 and SIP Phone #2. As opposed to a NAT gateway without the SIP ALG function, the gateway will monitor the control SIP traffic for the SIP communication instead of blocking it.

Special AP & ALG Setting

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

The Special AP setting allows applications that require multiple connections to work in NAT mode. The ALG setting permits SIP ALG traffic to pass through the gateway.

Enable Special AP & ALG

Configuration		
Item	Setting	
▶ Special AP	☒ Enable	
▶ ALG Enable	☒ SIP ALG	

Configuration Item	Value setting	Description
Special AP	The box is checked by default	Activate the Special AP function.
ALG Enable	The box is checked by default	Activate the SIP ALG function.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings.

Create / Edit Special AP Rule

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

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

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

Special AP Rule Configuration

Item	Setting
▶ WAN Interface	☒ ALL ☐ WAN-1 ☐ WAN-2 ☐ WAN-3 ☐ WAN-4
▶ Trigger Port	Port : Popular Applications : User-defined
▶ Incoming Ports	
▶ Time Schedule	(0) Always
▶ Rule	☐

Save

Special AP Rule Configuration		
Item	Value setting	Description
WAN Interface	1. A must-filled setting 2. All is checked by default.	Check the interface box(es) to apply the Special AP rule. By default, All is checked, and the Special AP rule will be applied to all WAN interfaces.
Trigger Port	1. A must-filled setting 2. User-defined is selected by default.	Enter the expected trigger port (or port range) if User-defined is selected. If you select other applications, the corresponding trigger port(s) and incoming ports will be defined automatically. <u>Value Range:</u> 1 ~ 65535.
Incoming Ports	1. A must-filled setting	Enter the expected Incoming ports if User-defined is selected in the Trigger Port list. If you select other application from the list, the corresponding incoming ports will be defined automatically. <u>Value Range:</u> 1 ~ 65535; It can be a single port, multiple ports separated by ",", or port range.
Time Schedule	1. An Must-filled setting 2. (0) Always is selected by default.	Apply Time Schedule to this rule, otherwise leave it as Always. If the dropdown list is empty ensure Time Schedule is pre-configured. Refer to Object Definition > Scheduling > Configuration tab.
Rule	The box is unchecked by default	Check the Enable box to activate the special AP rule.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings

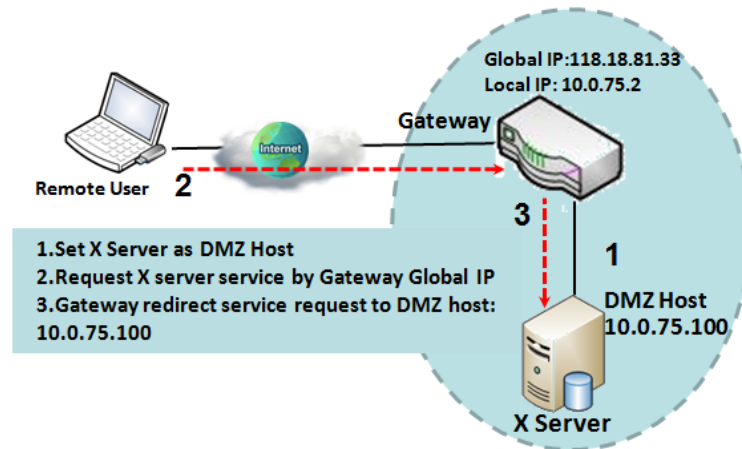
2.5.4 DMZ & Pass Through

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.

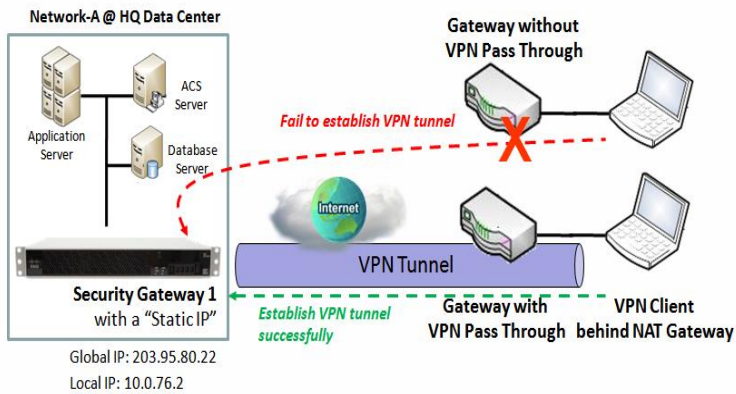
Configuration	
Item	Setting
DMZ	☒ Enable ☒ All ☐ WAN-1 ☐ WAN-2 ☐ WAN-3 ☐ WAN-4 DMZ Host : 10.0.75.100
Pass Through Enable	☒ IPSec ☒ PPTP ☒ L2TP

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 for 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	Setting
DMZ	☐ Enable ☒ All ☐ WAN-1 ☐ WAN-2 ☐ WAN-3 ☐ WAN-4 DMZ Host :
Pass Through Enable	☒ IPSec ☒ PPTP ☒ L2TP

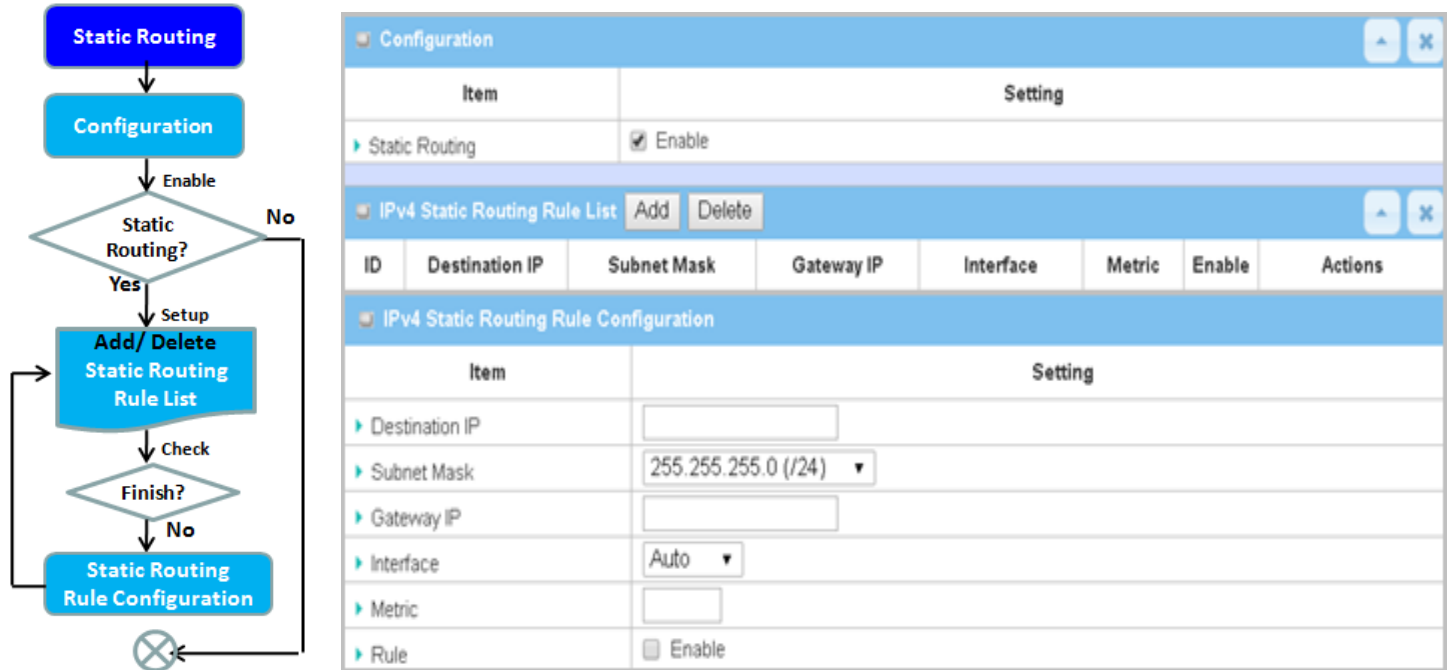
Configuration Item	Value setting	Description
DMZ	1. A must-filled setting 2. Default is ALL .	Select an interface to apply the DMZ function. Select ALL for packets coming into the gateway from any interface. Note: The available interfaces depend on the number of available WAN interfaces of the device.
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

2.6 Routing

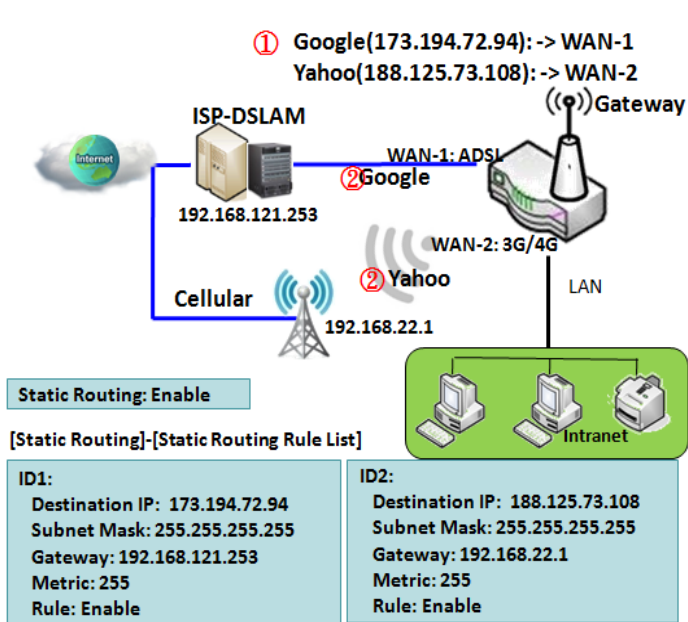
Routing allows packets to find proper path among different subnets to facilitate communication across gateways. Routing is the process of selecting best paths in a network. It is performed by different kinds of networks, including electronic data networks (such as the Internet), using packet switching 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 examples of dynamic routing techniques.

2.6.1 Static Routing



The Static Routing 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

Configuration	
Item	Setting
Static Routing	☒ Enable

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.

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

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

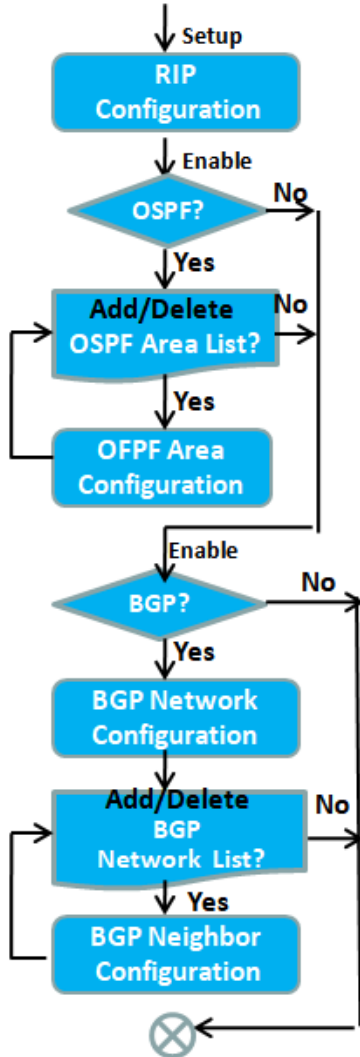
IPv4 Static Routing Rule Configuration

Item	Setting
▶ Destination IP	
▶ Subnet Mask	255.255.255.0 (/24) ▼
▶ Gateway IP	
▶ Interface	Auto ▼
▶ Metric	
▶ Rule	☐ Enable

IPv4 Static Routing

Item	Value setting	Description
Destination IP	1. IPv4 Format 2. A must-filled setting	Specify the Destination IP 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. Numeric 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



RIP Configuration				
Item	Setting			
▶ RIP Enable	Disable			

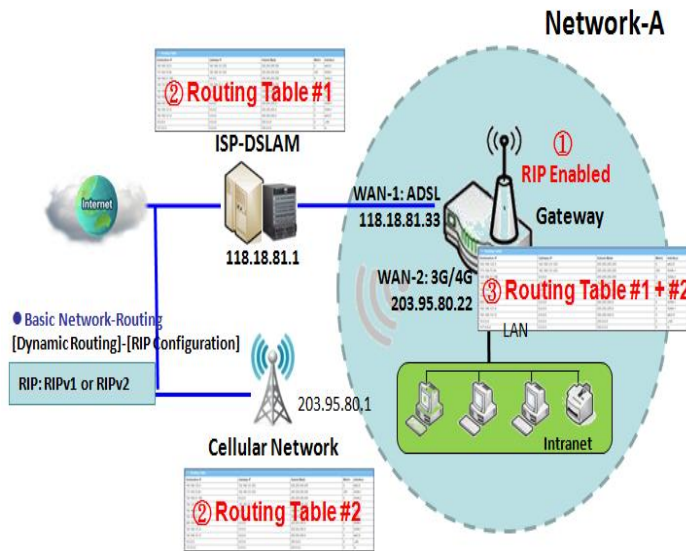
OSPF Configuration				
Item	Setting			
▶ OSPF	☐ Enable			
▶ Router ID				
▶ Authentication	None			
▶ Backbone Subnet				

OSPF Area List				
ID	Area Subnet	Area ID	Enable	Actions
OSPF Area Configuration Item Setting ▶ Area Subnet ▶ Area ID ▶ Area ☐ Enable Save				

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.

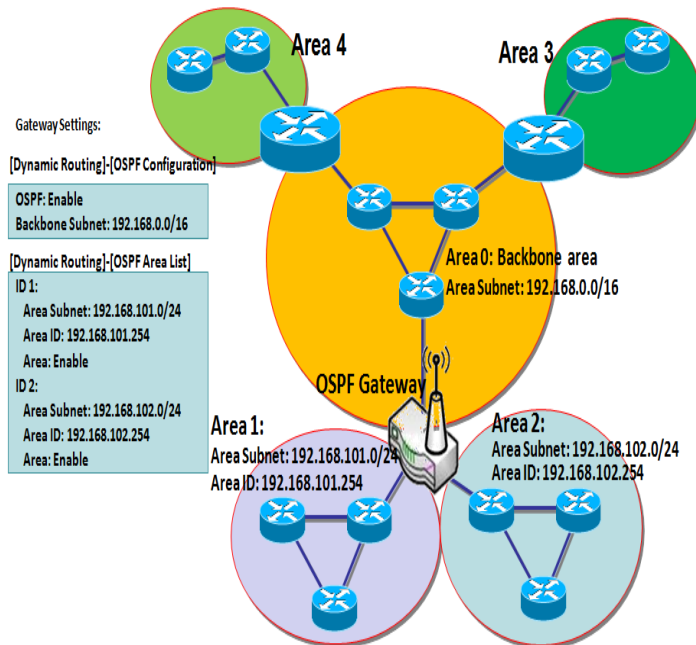
The supported dynamic routing protocols are described as follows.

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



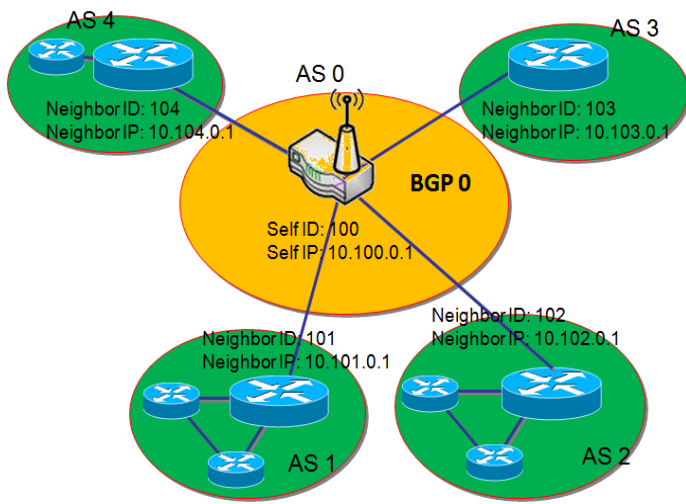
Open Shortest Path First (OSPF) is a routing protocol that uses link state routing algorithm. It is the most widely used interior gateway protocol (IGP) in large enterprise networks. It gathers link state information from available gateways and constructs a topology map of the network. The topology is 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** Tab.

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	Setting
▶ RIP Enable	Disable

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 OSPF and specify OSPF parameters on the gateway.

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

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.

OSPF Area List Add Delete ▲				
ID	Area Subnet	Area ID	Enable	Actions

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

OSPF Area Configuration ▲ ×	
Item	Setting
▶ Area Subnet	
▶ Area ID	
▶ Area	☐ Enable
Save	

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 Configuration
⬆ ⬇

Item	Setting
▶ BGP	☐ Enable
▶ ASN	
▶ Router ID	

BGP Network Configuration		
Item	Value setting	Description
BGP	The box is unchecked by default	Activate BGP.
ASN	1. Numeric String format 2. A must-filled setting	Configures a BGP routing process with an autonomous-system-number. <u>Value Range:</u> 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.

⌵ BGP Network List
Add Delete
⬆

ID	Network Subnet	Enable	Actions

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

⌵ BGP Network Configuration
⬆ ⬇

Item	Setting
▶ Network Subnet	IP : 255.255.255.0 (/24)
▶ Network	☐ Enable

Save

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.

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

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

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

BGP Neighbor Configuration		
Item	Value setting	Description
Neighbor IP	1. IPv4 Format 2. A must-filled setting	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. Numeric String Format 2. A must-filled setting	The Remote autonomous-system-number of the BGP Neighbor. <u>Value Range</u> : 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 > WAN & Uplink > Load Balance.**)

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.

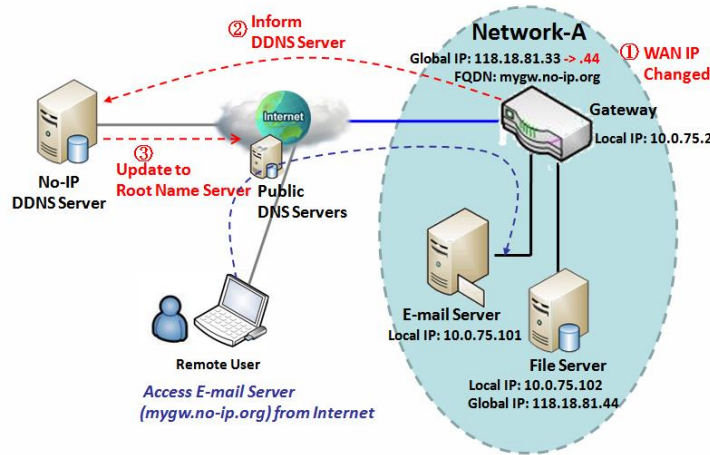
Policy Routing Information ⬆ ✕				
Policy Routing Source	Source IP	Destination IP	Destination Port	WAN Interface
Load Balance	-	-	-	-

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^{4,5} 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, simplifying 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.

4 Wikipedia, "Domain Name System", Jan 2, 2024, http://en.wikipedia.org/wiki/Domain_Name_System

5 Wikipedia, "Dynamic DNS", Nov 29, 2023, http://en.wikipedia.org/wiki/Dynamic_DNS

DNS & DDNS Setting

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

Set up Dynamic DNS

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

DDNS (Dynamic DNS) Configuration		
Item	Value setting	Description
DDNS	The box is unchecked by default	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. <u>Value Range</u> : 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.

Set up DNS Redirect

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

DNS Redirect

Item

Setting

DNS Redirect

☐ Enable

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.

Redirect Rule

Add

Delete

ID	Mapping Rule	Condition	Description	Enable	Action
----	--------------	-----------	-------------	--------	--------

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

Redirect Rule

Save

Item	Setting				
Mapping Rule	<table> <thead> <tr> <th>Domain Name</th> <th>IP</th> </tr> </thead> <tbody> <tr> <td> (* for Any)</td> <td> </td> </tr> </tbody> </table>	Domain Name	IP	(* for Any)	
Domain Name	IP				
(* for Any)					
Condition	Always				
Description					
Enable	☐ Enable				

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. <u>Value Range</u> : 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 disconnected, or unreachable.
Description	1. String format can be any text 2. A must-filled setting	Enter a brief description for this rule. <u>Value Range:</u> 0 ~ 63 characters.
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

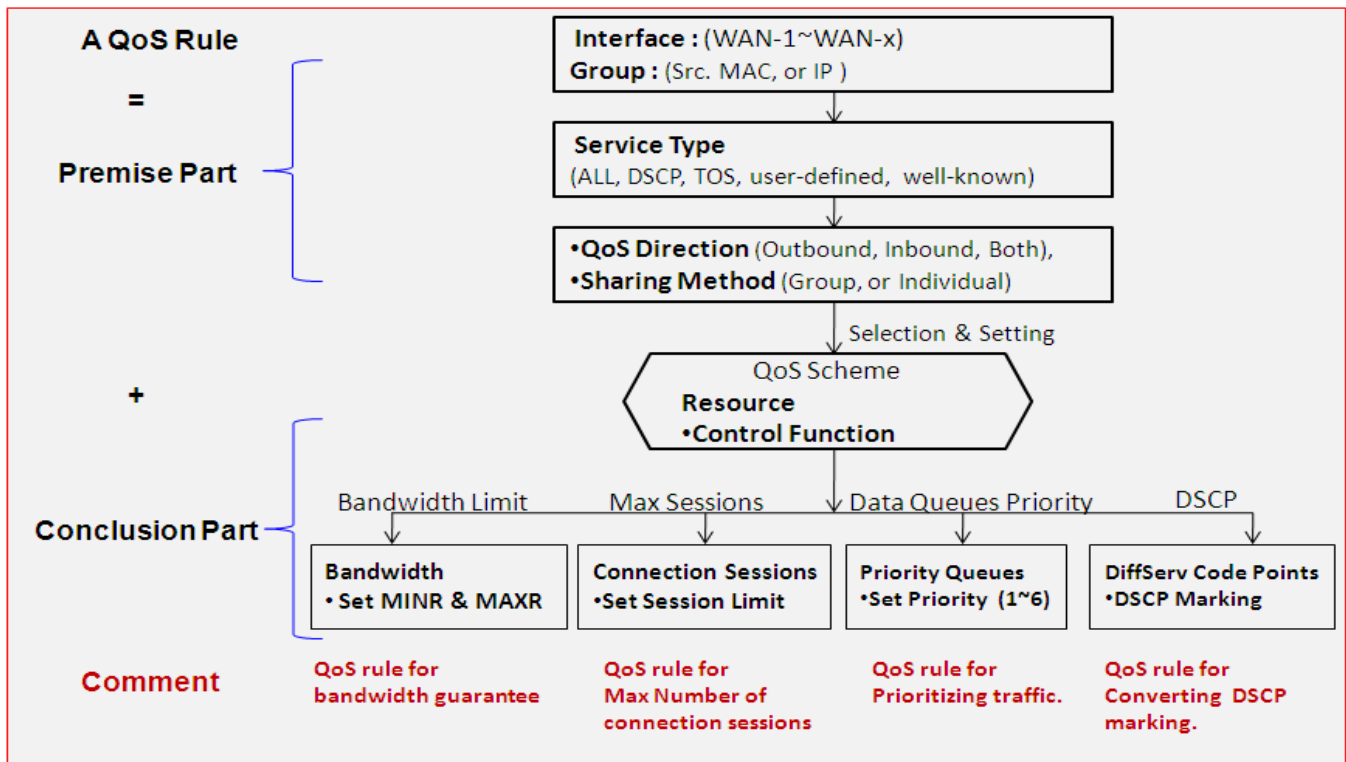
The total amount of data traffic keeps increasing as the bandwidth demand for mobile applications like Game, Chat, VoIP, Video, and web access mounts. New requirements for data transport such as low latency and low data loss emerges to ensure the guaranteed quality of service.

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. The premise part determines the WAN interface, host group, service type in the packets, packet flow direction, and the sharing method. And the conclusion part determines which kind of system resources to enact the rule and the control function for the chosen system resources. 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

QoS Rule Configuration	
Item	Setting
▶ Interface	All WANs ▼
▶ Group	IP ▼ 10.0.75.196 Subnet Mask : 255.255.255.252 (/30) ▼
▶ Service	DSCP ▼ ▶ DiffServ CodePoint IP Precedence 4(CS4) ▼
▶ Queue Outbound	N/A
▶ Queue Inbound	N/A
▶ Time Schedule	(0) Always ▼
▶ Rule Enable	☒ Enable

To convert the code point value (from "IP Precedence 4(CS4)" to "AF Class2(High Drop)") for packets from the specified client hosts (IP 10.0.75.196/255.255.255.252), the "Rule-based QoS" function can be defined as shown in the above configuration.

QoS Configuration Setting

Go to **Basic Network > QoS > Configuration** to access the QoS Configuration 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 Resource Configuration" window lets you configure the total bandwidth or queues of each WAN. The "QoS Rule List" window lists all your defined QoS rules. Finally, the "QoS Rule Configuration" window lets you define how QoS should be applied on the designated traffic.

Enable QoS Function

Configuration	
Item	Setting
▶ QoS Types	Software ☐ Enable
▶ Flexible Bandwidth Management	☐ Enable

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. When FBM is enabled, the system will adjust the bandwidth distribution dynamically by considering the current bandwidth consumption for the optimal system network performance while taking the users' bandwidth subscription profiles into account.
Save	N/A	Save the settings.

Configure System Resource

System Resource Configuration

Item	Setting
Type of System Queue	Bandwidth Queue ▾ 6 (1~6)
WAN Interface	WAN - 1 ▾

WAN Interface Resource

Item	Setting
Bandwidth of Upstream	100 Mbps ▾
Bandwidth of Downstream	100 Mbps ▾
Total Connection Sessions	30000 (1~100000)

System Resource Configuration		
Item	Value Setting	Description
Type of System Queue	1. A 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 (for both Hardware and Software QoS Types) and Priority Queues (for only Software QoS Type). <u>Value Range</u> : 1 ~ 6.
WAN Interface	WAN-1 is selected by default.	Specify the WAN interface configuration related resources in the below WAN Interface Resource section (only required for Software QoS Type)s. ● Bandwidth of Upstream / Downstream Specify total upload / download bandwidth of the selected WAN interface. ● Total Connection Sessions Specify total connection sessions allowed for the selected WAN. <u>Value Range</u> : 1 ~ 10000.
Save	N/A	Save the settings.

Note: For proper implementation of Software-based 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 the available system resources, configure QoS rules to apply on the designated traffic type. The gateway supports a maximum of 128 rule-based QoS rules.

QoS Rule List

Add

Delete

Clear

Restart

Interface	Group	Service	Resource	Control Function	Direction	Sharing Method	Time Schedule	Enable	Actions
-----------	-------	---------	----------	------------------	-----------	----------------	---------------	--------	---------

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

QoS Rule Configuration	
Item	Setting
▶ Interface	All WANs ▼
▶ Group	Src. MAC Address ▼
▶ Service	All ▼
▶ Resource	Bandwidth ▼
▶ Control Function	Set MINR & MAXR ▼ --- Mbps ▼
▶ QoS Direction	Outbound ▼
▶ Time Schedule	(0) Always ▼
▶ Rule Enable	☐ Enable

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: Host groups must be created in advance for the QoS service in the Bound Services field. 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	Activate this QoS rule.

	by default.	
Save	N/A	Save the 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.

Time Schedule List Add Delete ↑ ×		
ID	Rule Name	Actions

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 screen.

Time Schedule Configuration	
Item	Setting
▶ Rule Name	
▶ Rule Policy	Inactivate the Selected Days and Hours Below.

Time Schedule Configuration		
Item	Value Setting	Description
Rule Name	String: any text	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			
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one -- ▾		
2	-- choose one -- ▾		
3	-- choose one -- ▾		
4	-- choose one -- ▾		
5	-- choose one -- ▾		
6	-- choose one -- ▾		
7	-- choose one -- ▾		
8	-- choose one -- ▾		

Time Period Definition		
Item	Value Setting	Description
Week Day	Select from menu	Select everyday or one of weekday
Start Time	Time format (hh :mm)	Start time 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 and Firewall. 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.

Host Group List Add Delete 						
ID	Group Name	Group Type	Member List	Bound Services	Enable	Actions

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

Host Group Configuration	
Item	Setting
▶ Group Name	
▶ Group Type	IP Address-based
▶ Member to Join	Join
▶ Member List	
▶ Bound Services	☐ Firewall ☐ QoS
▶ Group	☐ Enable

Host Group Configuration		
Item	Value setting	Description
Group Name	1. String format can be any text 2. A must-filled setting	Enter a group name for the rule.
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 depending 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 gateway have the permission to access. Go to **Object Definition > External Servers** to access the External Server page.

Create External Server

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

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

External Server Configuration ↑ ×	
Item	Setting
▶ Server Name	
▶ Server Type	Email Server ▼ User Name: Password:
▶ Server IP/FQDN	
▶ Server Port	25
▶ Server	☒ Enable
Save Undo	

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 When selecting Email Server , specify the follwing: Username (String format: any text) Password (String format: any text)
		RADIUS Server 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 (Range: 1-60 mins, Default: 1) Idle Timeout (Range: 1-15 mins, Default: 1)
		Syslog Server
Server IP/FQDN	A must-filled setting	Specify the IP address or FQDN used for the above selected server type.
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 , 514 will be set by default. For RADIUS Server , port 1812 (authentication port) and 1813 (accounting port) will be set by default. <u>Value Range</u> : 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 owner⁶.

In a typical public-key infrastructure (PKI) scheme, the signer is a certificate authority (CA), usually a company such as VeriSign which charges customers for certificates issuance. 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. 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

Root CA Generate ⬆ ✕					
ID	Name	Subject	Issuer	Vaild To	Action

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

⁶ Wikipedia, "Public key certificate", Dec 12, 2023, http://en.wikipedia.org/wiki/Public_key_certificate.

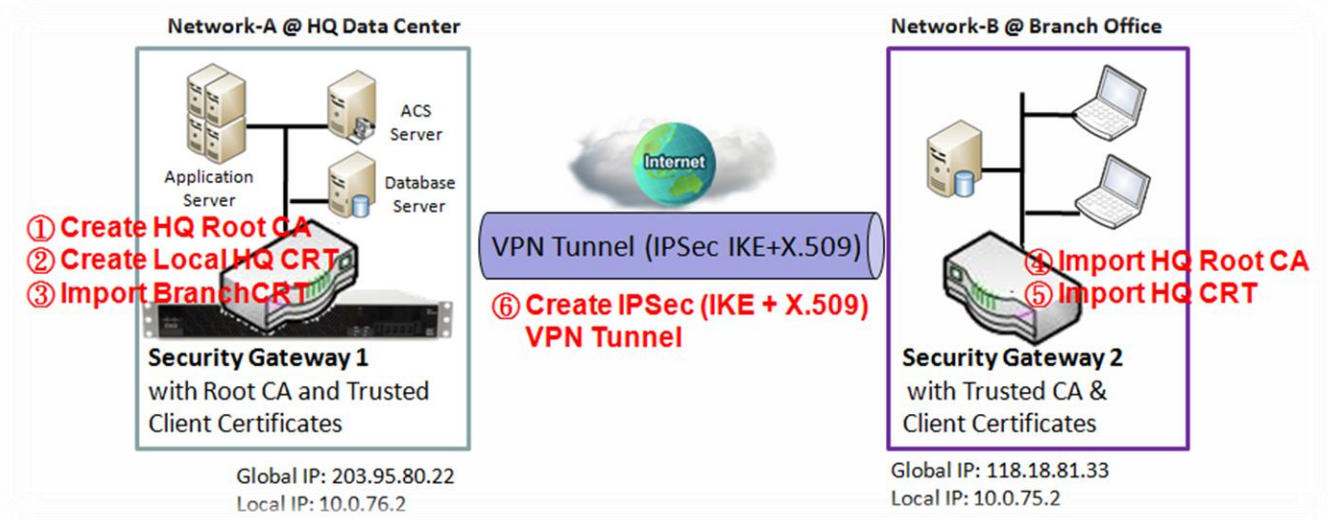
Root CA Certificate Configuration	
Item	Setting
▶ Name	
▶ Key	Key Type : RSA Key Length : 512-bits Digest Algorithm : MD5
▶ Subject Name	Country(C) : State(ST) : Location(L) : Organization(O) : Organization Unit(OU) : Common Name(CN) : E-mail :
▶ Validity Period	20-years

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.

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 certificates 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 also 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: hqcert@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 for generating self-certificates or corresponding CSRs to be signed by other CAs.

Create Local Certificate

Local Certificate List					
Add Import Delete					
ID	Name	Subject	Issuer	Vaild To	Actions

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

Local Certificate Configuration	
Item	Setting
▶ Name	Self-signed : ☐
▶ Key	Key Type : RSA ▼ Key Length : 1024-bits ▼ Digest Algorithm : SHA-1 ▼
▶ Subject Name	Country(C) : State(ST) : Location(L) : Organization(O) : Organization Unit(OU) : Common Name(CN) : E-mail :
▶ Extra Attributes	Challenge Password: Unstructured Name:
Save	

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.
Save	N/A	Save the configuration.

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.

The screenshot shows a web interface for importing certificates. It has two tabs: 'Import' and 'PEM Encoded'. The 'Import' tab is selected and shows a file selection area with a '瀏覽...' (Browse...) button and the text '未選擇檔案。' (No file selected). The 'PEM Encoded' tab is also visible, showing a large text area for pasting PEM encoded text.

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 trusted external CAs. The Trusted Client Certificate List stores trusted client certificates. And the Trusted Client Key List stores trusted client keys.

Trusted Certificate Setting

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

Import Trusted CA Certificate

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

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 Import from a File
Apply
Cancel

瀏覽... 未選擇檔案。

Trusted CA Certificate Import from a PEM
Apply
Cancel

Trusted CA Certificate List		
Item	Value setting	Description
Import from a File	A 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.
---------------	-----	--

Import Trusted Client Certificate

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

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 Import from a File Apply Cancel	
瀏覽... 未選擇檔案。	
Trusted Client Certificate Import from a PEM Apply Cancel	

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

Trusted Client Key List Import Delete		
ID	Name	Actions

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.

The screenshot shows a web interface for importing a Trusted Client Key. It consists of two main panels. The top panel, titled "Trusted Client Key Import from a File", includes a button labeled "瀏覽..." (Browse...) and a message "未選擇檔案。" (No file selected). The bottom panel, titled "Trusted Client Key Import from a PEM", features a large, empty text area for pasting the PEM encoded string. Both panels have "Apply" and "Cancel" buttons.

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

The gateway allows you to apply for a Certificate Signing Request (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 can then download the issued certificate to your local directory.

Issue Certificate Setting

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

Import and Sign Certificate

The screenshot shows a web interface for configuring certificate signing. It consists of two main sections, each with a title bar, a 'Sign' button, and a large input area.

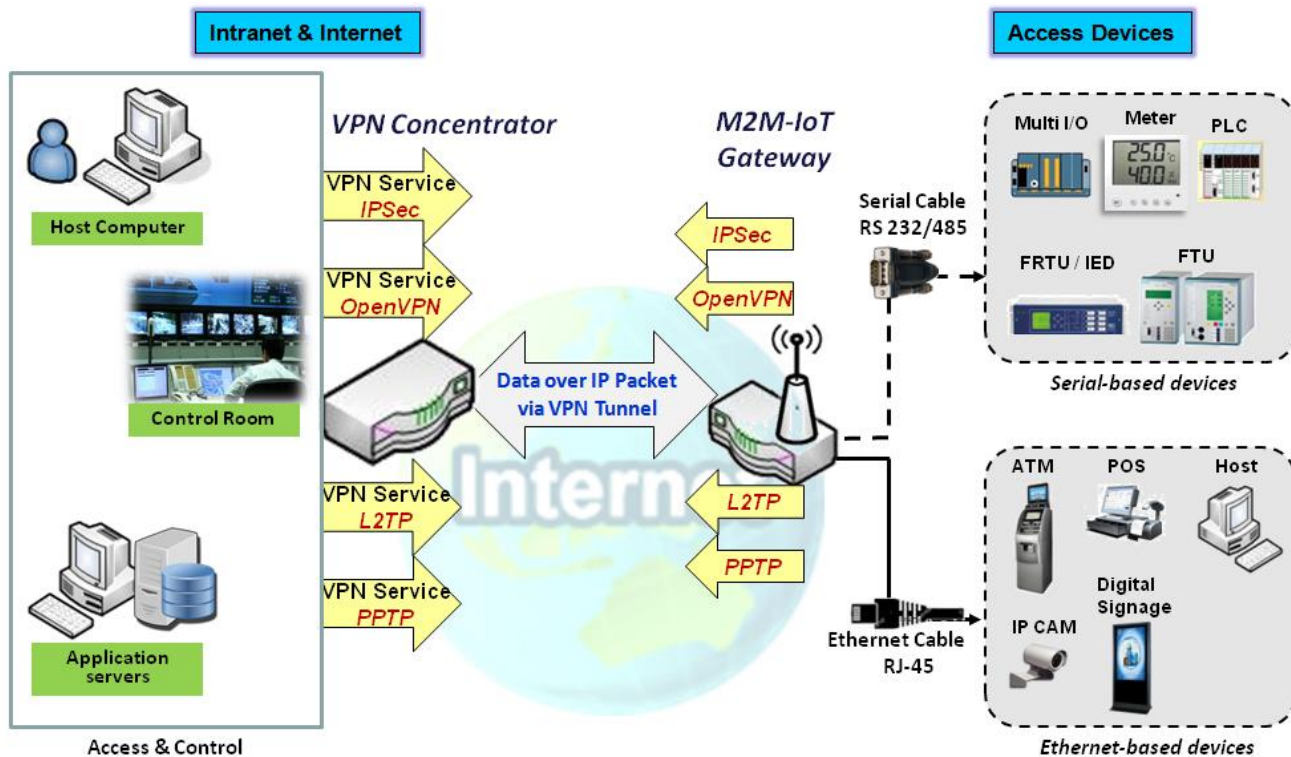
- Section 1:** Title bar: "Certificate Signing Request (CSR) Import from a File". Below the title bar is a "Choose File" button and the text "No file chosen".
- Section 2:** Title bar: "Certificate Signing Request (CSR) Import from a PEM". Below the title bar is a large, empty text area for entering PEM encoded text.

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 PEM encoded text for certificate signing in the field.
Sign	N/A	Sign the imported certificate by root CA.

Chapter 4 Security

4.1 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 tunneling technology supports data confidentiality and security as well as data integrity by employing encapsulation protocols, encryption algorithms, and hashing algorithms.



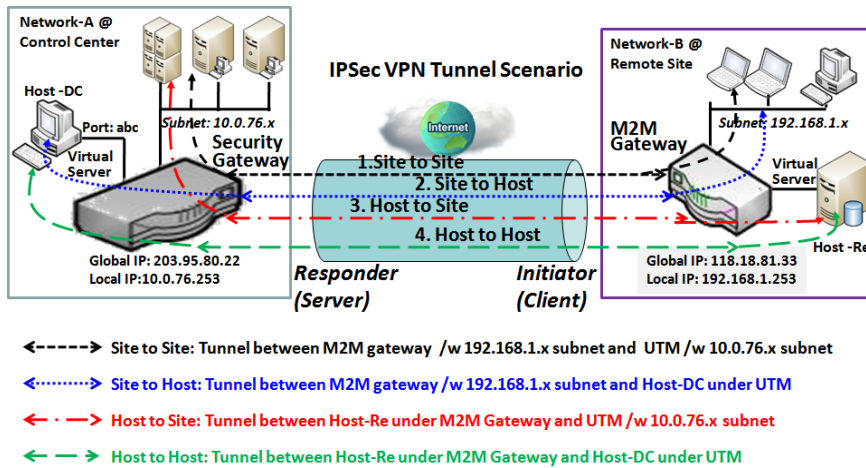
The product series supports different tunneling technologies for building secure tunnels between multiple sites: IPSec, OpenVPN, L2TP (over IPSec), PPTP, and GRE. Advanced functions such as Full Tunnel, Tunnel Failover, Tunnel Load Balance, NetBIOS over IPSec, NAT Traversal, and Dynamic VPN are also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

4.1.1 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 beginning 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	
Item	Setting
IPSec	☐ Enable
Max. Concurrent IPSec Tunnels	16

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.

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

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	
Item	Setting
Tunnel	☐ Enable
Tunnel Name	IPSec #1
Interface	WAN-1 ▼
Tunnel Scenario	Site-to-Site(Tunnel mode) ▼
Tunnel TCP MSS	Auto ▼ 0 (64~1500 Bytes)
ICMP Keep alive	☐ Enable Max. fail times 3 Interval 30 (secs.) Source Addr. Destination Addr.
Encapsulation Protocol	ESP ▼
IKE Version	v1 ▼

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. <u>Value Range:</u> 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.
Tunnel TCP MSS	1. An optional setting 2. Auto is set by default	Select from the size of Tunnel TCP MSS. Select Auto for automatic adjustment among the devices. Select Manual and specify a value for Tunnel TCP MSS. <u>Value Range:</u> 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 number of fail trials, check interval, and source/destination IP address for ICMP transmission. <u>Value Range:</u> 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				
Item	Setting			
▶ Local Subnet List	ID	Subnet IP Address	Subnet Mask	Actions
	1	192.168.66.0	255.255.255.0(24)	Delete
	Add			
▶ Remote Subnet List	ID	Subnet IP Address	Subnet Mask	Actions
	1		255.255.255.0(24)	Delete
	Add			
▶ Remote Gateway	(IP Address/FQDN)			

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: - When Dynamic VPN option in Tunnel Scenario is selected, only one subnet will be available. - When Host-to-Site or Host-to-Host is selected for Tunnel Scenario, Local Subnet will not be available. 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	- A must-filled setting. - Format can be a ipv4 address or FQDN	Specify the remote gateway.

Authentication	
Item	Setting
▶ Key Management	IKE+Pre-shared Key (Min. 8 characters)
▶ Local ID	Type: User Name ID: (Optional)
▶ Remote ID	Type: User Name ID:

Authentication Configuration Window

Item	Value setting	Description
Key Management	- A must-filled setting - 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.

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	
Item	Setting
Tunnel	☐ Enable
Tunnel Name	Dynamic IPSec1
Interface	WAN1
Tunnel Scenario	Tunnel Mode
Encapsulation Protocol	ESP
IKE Version	v1

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. <u>Value Range:</u> 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	
Item	Setting
Local Subnet	192.168.66.0
Local Netmask	255.255.255.0(24)

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	
Item	Setting
▶ Key Management	IKE+Pre-shared Key ▼ (Min. 8 characters)
▶ Local ID	Type: User Name ▼ ID: (Optional)
▶ Remote ID	Type: User Name ▼ ID:

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.

4.1.2 OpenVPN

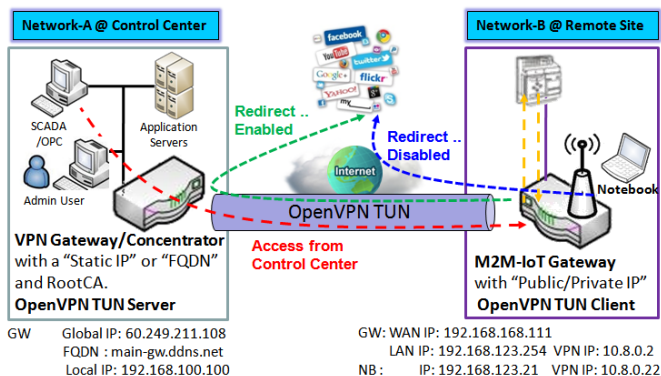
OpenVPN is an application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations. It uses SSL/TLS for secure key exchange. It is capable of traversing network address translators (NATs) and firewalls.

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



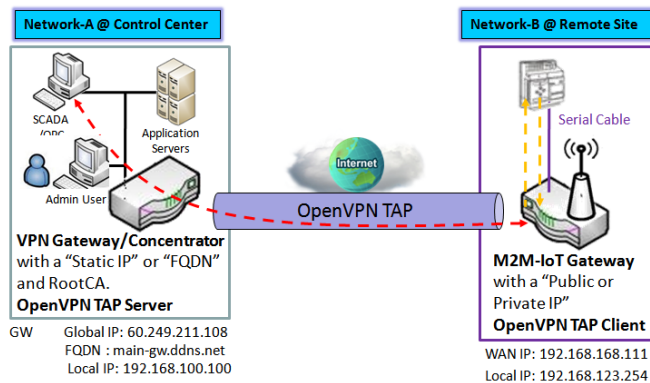
1. M2M-IoT Gateway (as OpenVPN TUN Client) connects to peer VPN Gateway/Concentrator (as OpenVPN TUN Server).
2. M2M-IoT Gateway will be assigned 10.8.0.2 IP Address after OpenVPN TUN Connection established. (10.8.0.x is a virtual subnet)
3. Local networked device will get a virtual IP 10.8.0.x if its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

The term "TUN" mode is 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 a 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 established. **(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.

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

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	Setting
▶ OpenVPN	☒ Enable
▶ Server / Client	Server ▼

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	Setting
▶ OpenVPN	☒ Enable
▶ Server / Client	Server ▼
▶ OpenVPN Configuration file	☐ Enable Export client.ovpn

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	Setting
▶ OpenVPN Server	☐ Enable
▶ Protocol	TCP ▼
▶ Port	4430
▶ Tunnel Scenario	TUN ▼
▶ Authorization Mode	TLS ▼ CA Cert.: amit-IDG761AM-JH.crt ▼ Server Cert.: LocalCert1 ▼
▶ Server Virtual IP	10.8.0.0
▶ DHCP-Proxy Mode	☒ Enable
▶ IP Pool	Starting Address: ~ Ending Address:
▶ Gateway	
▶ Netmask	255.255.255.0(/24) ▼
▶ Redirect Default Gateway	☐ Enable
▶ Encryption Cipher	Blowfish ▼
▶ Hash Algorithm	SHA-1 ▼
▶ LZO Compression	Adaptive ▼
▶ Persist Key	☒ Enable
▶ Persist Tun	☒ Enable
▶ Advanced Configuration	Edit

OpenVPN Server Configuration		
Item	Value setting	Description
OpenVPN Server	The box is unchecked by default.	Activate OpenVPN Server function.
Protocol	1. A must-filled setting 2. By default TCP is selected.	Define the Protocol for the 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 the OpenVPN Server. <u>Value Range:</u> 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. <u>Value Range:</u> 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. <u>Value Range:</u> 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. <u>Value Range:</u> 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. <i>Value Range:</i> 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. 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	Setting
▶ TLS Cipher	None ▼
▶ TLS Auth. Key	 (Optional)
▶ Client to Client	☒ Enable
▶ Duplicate CN	☒ Enable
▶ Tunnel MTU	1500
▶ Tunnel UDP Fragment	0
▶ Tunnel UDP MSS-Fix	☐ Enable
▶ CCD-Dir Default File	
▶ Client Connection Script	
▶ Additional Configuration	

OpenVPN Server Advanced Configuration		
Item	Value setting	Description
TLS Cipher	1. A must-filled setting. 2. TLS-RSA-WITH-AES128-SHA is selected by default	Specify the TLS Cipher : 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 . <u>Value Range:</u> 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 . <u>Value Range:</u> 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 by default.	Activate the Tunnel UDP MSS-Fix Function. Note: Tunnel UDP MSS-Fix will be available only when UDP is chosen for Protocol.
CCD-Dir Default	1. An optional setting.	Specify the CCD-Dir Default File .

File	2. String format: any text	<u>Value Range</u> : 0 ~ 256 characters.
Client Connection Script	1. An optional setting. 2. String format: any text	Specify the Client Connection Script . <u>Value Range</u> : 0 ~ 256 characters.
Additional Configuration	1. An optional setting. 2. String format: any text	Specify the Additional Configuration . <u>Value Range</u> : 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.

Configuration	
Item	Setting
OpenVPN	☒ Enable
Server / Client	Client ▼
OpenVPN Configuration file	☐ Enable Upgrade

OpenVPN Configuration		
Item	Value setting	Description
OpenVPN	The box is unchecked by default	Check the Enable box to activate the OpenVPN function.
Server/Client	Server Configuration is selected by default.	When Server is selected, as the name indicated, server configuration will be displayed below for further setup. When Client is selected, you can specify the client settings in another client configuration window.
OpenVPN Configuration file	1. An Optional setting. 2. The box is unchecked by default.	Click the Enable box to activate the OpenVPN Client configuration via a pre-defined configuration file (a .ovpn file). If you enabled this function, you can't add any OpenVPN clients manually.

OpenVPN Client List														Add	Delete
ID	Client Name	Interface	Protocol	Port	Tunnel Scenario	Remote IP/FQDN	Remote Subnet	Redirect Internet Traffic	NAT	Authorization Mode	Encryption Cipher	Hash Algorithm	Enable	Actions	
OpenVPN Client Configuration															
Item		Setting													
OpenVPN Client Name		OpenVPN Client #1													
Interface		WAN 1 ▼													
Protocol		TCP ▼ Port: 443													
Tunnel Scenario		TUN ▼													
Remote IP/FQDN															
Remote Subnet		☐ Enable 255.255.255.0(/24) ▼													
Redirect Internet Traffic		☐ Enable													
NAT		☒ Enable													
Authorization Mode		TLS ▼ CA Cert.: ▼ Client Cert.: ▼ Client Key.: ▼ Please set the Certificate.													
Encryption Cipher		Blowfish ▼													
Hash Algorithm		SHA-1 ▼													

▶ LZO Compression	Adaptive ▼
▶ Persist Key	☒ Enable
▶ Persist Tun	☒ Enable
▶ Advanced Configuration	Edit
▶ Tunnel	☐ Enable

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. <u>Value Range:</u> 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. <u>Value Range:</u> 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 function and 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. <u>Value Range:</u> 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. <i>Value Range:</i> 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 Client Advanced Configuration	
Item	Setting
▶ TLS Cipher	None ▼
▶ TLS Auth. Key(Optional)	(Optional)
▶ User Name(Optional)	(Optional)
▶ Password(Optional)	(Optional)
▶ Bridge TAP to	VLAN 1 ▼
▶ Firewall Protection	☐ Enable
▶ Client IP Address	Dynamic IP ▼
▶ Tunnel MTU	1500
▶ Tunnel UDP Fragment	1500

▶ Tunnel UDP MSS-Fix	☐ Enable
▶ nsCertType Verification	☐ Enable
▶ TLS Renegotiation Time(seconds)	3600 (seconds)
▶ Connection Retry(seconds)	-1 (seconds)
▶ DNS	Automatically
▶ Additional Configuration	

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: 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 . <u>Value Range:</u> 0 ~ 1500.
Tunnel UDP Fragment	The value is 1500 by default	Specify the value of Tunnel UDP Fragment . <u>Value Range:</u> 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 . <u>Value Range:</u> -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. <u>Value Range:</u> -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. <u>Value Range:</u> 0 ~ 256 characters.

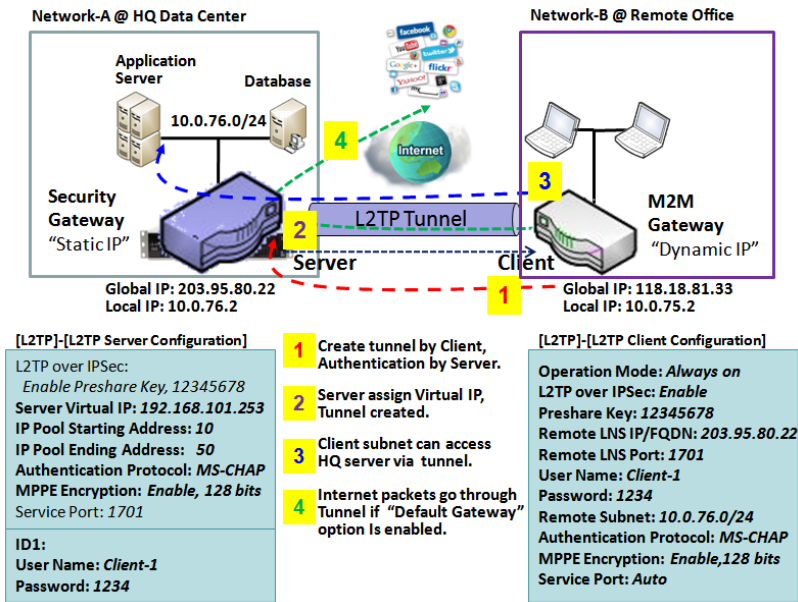
Save	N/A	Save the settings.
Undo	N/A	Cancel the changes and return to the previous page.

4.1.3 L2TP

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or service delivery by ISPs. L2TP doesn'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

Configuration	
Item	Setting
L2TP	☐ Enable
Client/Server	Server ▼

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	Setting
L2TP Server	☐ Enable
Interface	WAN1 ▼
L2TP over IPsec	☐ Enable Preshared Key 1234567890 (Min. 8 characters)
Server Virtual IP	192.168.13.1
IP Pool Starting Address	10
IP Pool Ending Address	17
Authentication Protocol	☒ PAP ☒ CHAP ☐ MS-CHAP ☐ MS-CHAP v2
MPPE Encryption	☐ Enable 40 bits ▼
Service Port	1701

L2TP Server Configuration		
Item	Value setting	Description
L2TP Server	The box is unchecked	Activate the L2TP server.

	by default	
Interface	1. A must-filled setting 2. All WANs is selected by default	Select the interface on which L2TP tunnel is to be established.
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. <u>Value Range</u> : >= 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. <u>Value Range</u> : 1 ~ 65535.
Save	N/A	Save the configuration.
Undo	N/A	Discard the configuration.

L2TP Server Status Refresh				
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

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					Add	Delete		
ID	User Name	Password	Enable	Actions				
User Account Configuration								
User Name		Password		Account				
				☐ Enable				
Save								

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 a L2TP Client

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

L2TP Client Configuration	
Item	Setting
L2TP Client	☐ Enable

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

L2TP Client List & Status								
		Add	Delete	Refresh				
ID	Tunnel Name	Interface	Virtual IP	Remote IP/FQDN	Remote Subnet	Status	Enable	Actions
1	L2TP #1	WAN 1	0.0.0.0	192.168.127.72			☐	Edit ☐ Select

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

L2TP Client Configuration	
Item	Setting
Tunnel Name	L2TP #1
Interface	WAN1
L2TP over IPsec	☐ Enable Preshared Key (Min. 8 characters)
Remote LNS IP/FQDN	
MTU	1500
Remote LNS Port	1701
User Name	
Password	
Tunneling Password (Optional)	
Remote Subnet	
Authentication Protocol	☐ PAP ☐ CHAP ☐ MS-CHAP ☐ MS-CHAP v2
MPPE Encryption	☐ Enable
NAT before Tunneling	☐ Enable
LCP Echo Type	Auto Interval 30 seconds Max. Failure Time 6 times
Service Port	Auto 0
Tunnel	☐ Enable

L2TP Client Configuration		
Item Setting	Value setting	Description
Tunnel Name	A must-filled setting	Enter a name for the tunnel name. <u>Value Range</u> : 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 (refer to Basic Network > WAN & Uplink > Physical Interface).
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 . <u>Value Range</u> : 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. <u>Value Range</u> : 1 ~ 65535.
Username	A must-filled setting	Enter the Username for this L2TP tunnel to be authenticated. <u>Value Range</u> : 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. <u>Value Range</u> : 1 ~ 99999 for Interval Time, 1~999 for Failure Time.

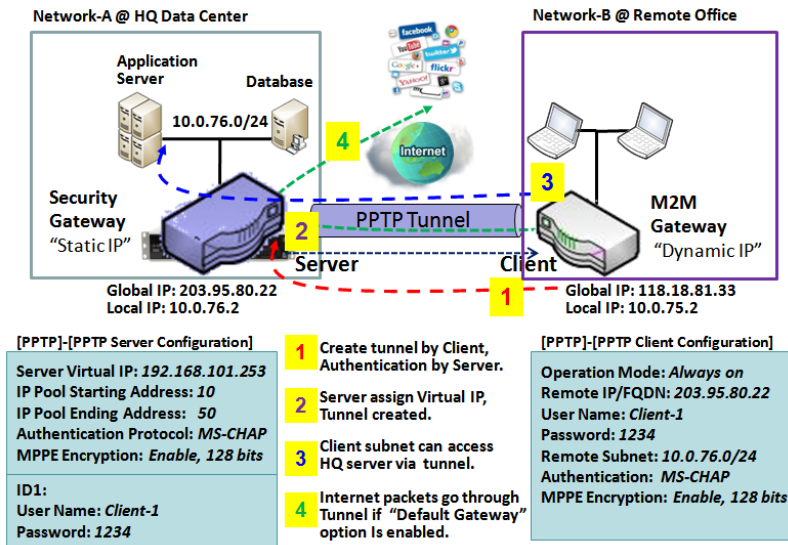
Service Port	A must-filled setting	Specify the Service Port for this L2TP tunnel: Auto, (1701) for Cisco, or User-defined. Auto: automatic configuration of the service port. 1701 (for Cisco): The system uses port 1701 for connecting with CISCO L2TP Server. User-defined: Enter the service port. The default value is 0. <u>Value Range:</u> 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.

4.1.4 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

Configuration	
Item	Setting
PPTP	☐ Enable
Client/Server	Server ▼

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

The gateway supports up to a maximum of 10 PPTP user accounts.

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

PPTP Server Configuration	
Item	Setting
PPTP Server	☐ Enable
Interface	WAN1 ▼
Server Virtual IP	192.168.12.1
IP Pool Starting Address	10
IP Pool Ending Address	17
Authentication Protocol	☐ PAP ☐ CHAP ☒ MS-CHAP ☒ MS-CHAP v2
MPPE Encryption	☒ Enable 40 bits ▼

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 greater than or equal to the start value and less than the start value plus 8 or 254. <u>Value Range</u> : >= 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 Refresh				
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

PPTP Server Status Window		
Item	Value setting	Description
PPTP Server Status	N/A	It displays the 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					Add	Delete		
ID	User Name	Password	Enable	Actions				
User Account Configuration								
User Name		Password			Account			
					☐ Enable			
					Save			

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. <u>Value Range:</u> 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	Setting
▶ PPTP Client	☐ Enable

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

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

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

PPTP Client Configuration	
Item	Setting
▶ Tunnel Name	PPTP #1
▶ Interface	WAN1
▶ Remote IP/FQDN	
▶ MTU	1500
▶ User Name	
▶ Password	
▶ Remote Subnet	
▶ Authentication Protocol	☐ PAP ☐ CHAP ☐ MS-CHAP ☐ MS-CHAP v2
▶ MPPE Encryption	☐ Enable
▶ NAT before Tunneling	☐ Enable
▶ LCP Echo Type	Auto Interval 30 seconds Max. Failure Time 6 times
▶ Tunnel	☐ Enable

PPTP Client Configuration Window		
Item	Value setting	Description
Tunnel Name	A must-filled setting	Enter a name for the tunnel. <u>Value Range:</u> 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 . <u>Value Range:</u> 0 ~ 1500.
Username	A must-filled setting	Enter the Username for this PPTP tunnel for authentication. <u>Value Range:</u> 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 2. An optional setting	Specify whether PPTP 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	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. <u>Value Range:</u> 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.

4.1.5 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 gateway.

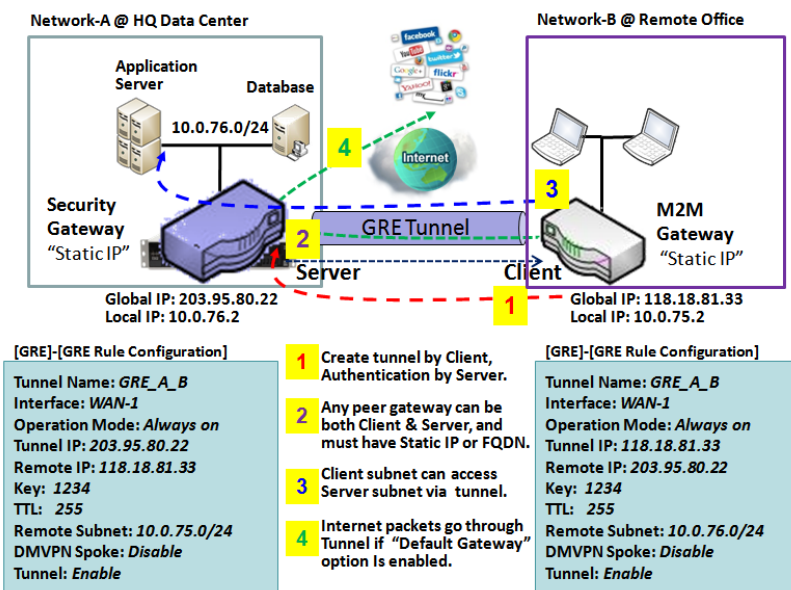
Configuration

Item	Setting
GRE Tunnel	☐ Enable
Max. Concurrent GRE Tunnels	32

GRE Tunnel ListAddDelete

ID	Tunnel Name	Interface	Tunnel IP	Remote IP	MTU	Key	TTL	Remote Subnet	Enable	Actions
----	-------------	-----------	-----------	-----------	-----	-----	-----	---------------	--------	---------

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 client peer, 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** tab.

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

Enable GRE

Configuration	
Item	Setting
GRE Tunnel	☐ Enable
Max. Concurrent GRE Tunnels	32

Enable GRE Window		
Item	Value setting	Description
GRE Tunnel	Unchecked by default	Click the Enable box to enable GRE function.
Max. Concurrent GRE Tunnels	Depends on Product specification.	The specified value will limit the maximum number of simultaneous GRE tunnel connection. The default value can be different for the purchased model.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings.s

Create/Edit GRE tunnel

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

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

GRE Rule Configuration	
Item	Setting
▶ Tunnel Name	GRE #1
▶ Interface	WAN1 ▼
▶ Tunnel IP	IP: MASK: -- select one -- ▼ (Optional)
▶ Remote IP	
▶ MTU	
▶ Key	(Optional)
▶ TTL	
▶ Remote Subnet	
▶ Tunnel	☐ Enable

GRE Rule Configuration Window		
Item	Value setting	Description
Tunnel Name	A must-filled setting	Enter a name for the tunnel. <u>Value Range:</u> 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. <u>Value Range:</u> 0 ~ 1500.
Key	An optional setting	Enter the Key for the GRE connection. <u>Value Range:</u> 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.

4.1.6 EoGRE

Ethernet over GRE (EoGRE) is a tunnel protocol that enables tunneling of layer 2 packets encapsulated via GRE, another tunneling protocol developed by Cisco Systems that encapsulates a wide variety of network layer protocols inside virtual point-to-point links, over an IP network. It can also aggregate WiFi traffic generated from hotspots. This solution enables a gateway to bridge Ethernet traffic from an end host using packet encapsulation inside a GRE tunnel.

Configuration	
Item	Setting
EoGRE Tunnel	☐ Enable
Max. Concurrent EoGRE Tunnels	4

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

EoGRE Setting

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

Enable EoGRE

Configuration	
Item	Setting
EoGRE Tunnel	☐ Enable
Max. Concurrent EoGRE Tunnels	4

Enable GRE Window		
Item	Value setting	Description
EoGRE Tunnel	Unchecked by default	Click the Enable box to enable EoGRE function.
Max. Concurrent EoGRE Tunnels	Depends on Product specification.	The specified value will limit the maximum number of simultaneous EoGRE tunnel connections. The default value can be different for the purchased model.
Save	N/A	Click Save button to save the settings
Undo	N/A	Click Undo button to cancel the settings

Create/Edit EoGRE tunnel

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

Click **Add/Edit** to open EoGRE Rule Configuration

EoGRE Rule Configuration	
Item	Setting
▶ Tunnel Name	EoGRE #1
▶ Interface	WAN1
▶ Tunnel IP	IP: MASK: -- select one -- (Optional)
▶ Remote IP	
▶ MTU	(Optional)
▶ Key	(Optional)
▶ TTL	(Optional)
▶ Port-based VLAN ID Interface	None
▶ Tunnel	☐ Enable

EoGRE Rule Configuration Window		
Item	Value setting	Description
Tunnel Name	A Must fill setting	Enter a tunnel name. Enter a name that is easy for you to identify. Value Range: 1 ~ 8 characters.
Interface	1. A Must fill setting 2. WAN 1 is selected by default	Select the interface on which EoGRE tunnel is to be established. It can be the available WAN interfaces.
Tunnel IP	An Optional setting	Enter the Tunnel IP address and corresponding subnet mask.
Remote IP	A Must fill setting	Enter the Remote IP address of remote EoGRE tunnel gateway. Normally this is the public IP address of the remote EoGRE gateway.
MTU	An Optional setting	MTU refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Value Range: 1 ~ 1500.
Key	An Optional setting	Enter the Key for the EoGRE connection. Value Range: 0 ~ 4294967295.
TTL	An Optional setting	Specify TTL hop-count value for this GRE tunnel. Value Range: 1 ~ 255.
Port-based VLAN ID Interface	1. A Must fill setting 2. None is selected by default	Select a Port-based VLAN ID for aggregating its traffic to the EoGRE tunnel. It can be None , or all available Port –based VLAN IDs. For creating the Port-based VLAN ID, refer to Basic Network > LAN & VLAN > VLAN . If VLAN type is tag-based VLAN, it will be grayed out. You can also aggregate tag-based VLAN group to an EoGRE tunnel with specifying additional TAG ID listing below.
Tunnel	Unchecked by default	Check Enable box to enable this EoGRE tunnel.
Save	N/A	Click Save button to save the settings.
Undo	N/A	Click X button to cancel the settings and back to last page.

Define EoGRE TAG ID Listing

You can define a TAG ID to aggregate VLAN traffic with different tags to form a sub tunnel. Up to 40 tag IDs can be defined for a tunnel.

TAG ID List Add Delete					
ID	TAG ID	MTU	VLAN ID Interface	Enable	Actions

Click Add/Edit to open the TAG ID Configuration screen

TAG ID Configuration	
Item	Setting
▶ TAG ID	
▶ MTU	(Optional)
▶ Tag-based VLAN ID Interface	None ▼
▶ Enable	☐
Save	

TAG ID Configuration Window		
Item	Value setting	Description
TAG ID	A Must fill setting	Enter a Tag ID for a tunnel carrying specified Tag-based VLAN ID. <u>Value Range:</u> 1 ~ 4094.
MTU	An Optional setting	MTU refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. <u>Value Range:</u> 1 ~ 1500, and shouldn't be greater than that of the EoGRE Tunnel.
Tag-based VLAN ID Interface	1. A Must fill setting 2. None is selected by default	Select a Tag-based VLAN ID on which EoGRE tunnel is to be established. It can be None , or all available Tag –based VLAN IDs. If VLAN type is port-based VLAN, it will be grayed out. For creating the VLAN IDs, refer to Basic Network > LAN & VLAN > VLAN .
Enable	Unchecked by default	Check Enable box to enable this TAG rule.
Save	N/A	Save the settings.
Undo	N/A	Cancel the settings and back to last page.

4.1.7 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

Configuration	
Item	Setting
WireGuard	☒ Enable
Operation Mode	Server

Enable PPTP 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	
Item	Setting
WireGuard Server	☐ Enable
Interface	WAN-1
Tunnel IP	IP: MASK: 255.255.255.0(24)
MTU	0
Listen Port	51820
	<button>Generate Keypairs</button>
Keypairs	PrivateKey 4HAlemPgmV+sCczam5a0ZwaguHR/+TXb6Fgsl5pJ628= PublicKey YN+prHmEnDRktFsZr+uNxxUS5+d+MMGJANp+QjmA+JA=
PostUp Script	
PostDown Script	

Peer List						
ID	Peer IP	PublicKey	Remote Subnet	Enable	Profile	Actions
+ + + + + + + + + + + + + + + + + + + +						

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 Subnet 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 Add Delete							↑ ×
ID	Peer IP	PublicKey	Remote Subnet	Enable	Profile	Actions	

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.

WireGuard Client List & Status Add Delete								↑ ×
ID	Tunnel Name	Tunnel IP	Listen Port	Remote IP/FQDN	Server's PublicKey	Remote Subnet	Enable	Actions

Create/Edit WireGuard Client

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

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

WireGuard Client Configuration	
Item	Setting
▶ Tunnel Name	
▶ Tunnel IP	IP: MASK: 255.255.255.0(/24) ▼
▶ MTU	
▶ Listen Port	
▶ Remote IP/FQDN	
▶ Server's PublicKey	
▶ PrivateKey	
▶ Pre-shared Key (Option)	☐ Enable
▶ Keep Alive	☐ Enable
▶ Remote Subnet	
▶ PostUp Script	

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.

4.2 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.

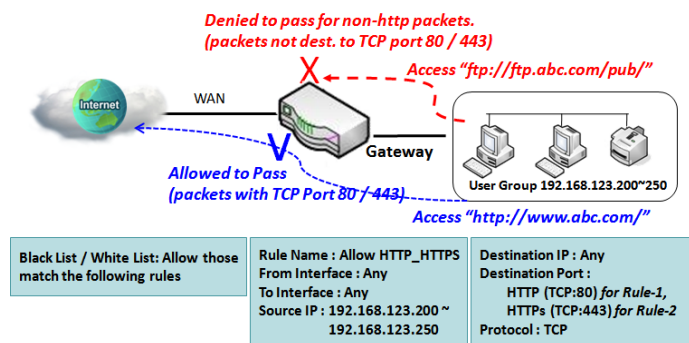
4.2.1 Packet Filter

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.

Configuration												
Item		Setting										
▶ Packet Filters		☒ Enable										
▶ Black List / White List		Deny those match the following rules. ▼										
▶ Log Alert		☐ Log Alert										

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

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 range 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	
Item	Setting
▶ Packet Filters	☐ Enable
▶ Black List / White List	Deny those match the following rules. ▼
▶ Log Alert	☐ Log Alert

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 <i>Deny those match the following rules</i> is selected, packets matching these rules will be blocked. In contrast, for the <i>Allow those match the following rules</i> , 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 create your packet filter rules. It supports a maximum of 20 filter rules.

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

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

Packet Filter Rule Configuration	
Item	Setting
▶ Rule Name	Rule1
▶ From Interface	Any
▶ To Interface	Any
▶ Source IP	Any
▶ Destination IP	Any
▶ Source MAC	Any
▶ Protocol	Any(0)
▶ Source Port	User-defined Service -
▶ Destination Port	User-defined Service -
▶ Time Schedule	(0) Always
▶ Rule	☐ Enable

Packet Filter Rule Configuration		
Item Name	Value setting	Description
Rule Name	1. String format can be any text 2. A must-filled setting	Enter a name for the packet filter rule. <u>Value Range:</u> 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 interface. 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 interface. 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 addresses. 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 address. 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. <u>Value Range:</u> 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 dropdown box 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 dropdown box when Well-known Service is selected, otherwise select User-defined Service and specify a port range. <u>Value Range:</u> 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.

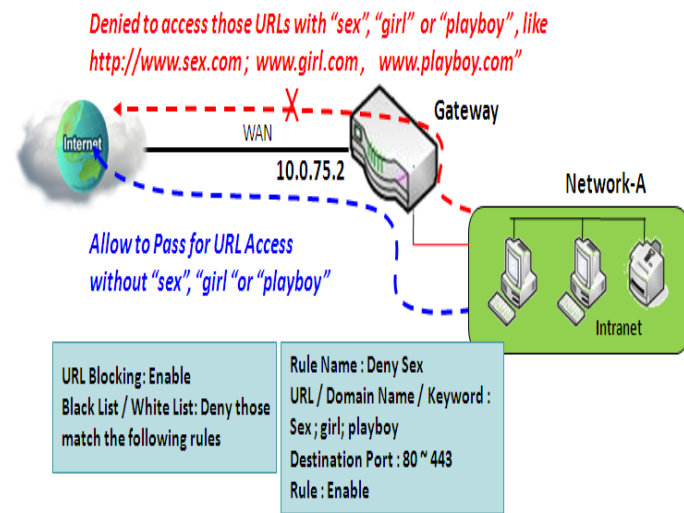
4.2.2 URL Blocking

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

The "Configuration" window lets you activate the URL blocking function. In addition, logging can be enabled to record events of blocked web packets. Refer to **7.3.2 Firewall Status** for instructions on how to view logged alerts.

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

Enable URL Blocking

Configuration	
Item	Setting
▶ URL Blocking	☒ Enable
▶ Black List / White List	Deny those match the following rules. ▼
▶ Log Alert	☐ Enable

Configuration Item	Value setting	Description
URL Blocking	The box is unchecked by default	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 others that don't match the rules 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.

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

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

URL Blocking Rule Configuration

Item	Setting
▶ Rule Name	Rule1
▶ Source IP	Any ▼
▶ Source MAC	Any ▼
▶ URL / Domain Name / Keyword	
▶ Destination Port	Any ▼
▶ Time Schedule Rule	(0) Always ▼
▶ Rule	☐ Enable

URL Blocking Rules Configuration		
Item	Value setting	Description
Rule Name	1. String format can be any text 2. A must-filled setting	Specify an URL Blocking rule name. Enter a name that is easy for you to understand.
Source IP	1. A must-filled setting 2. Any is set by default	This field is to specify the Source IP address . • Select Any to filter packets coming from any IP address. • Select Specific IP Address to filter packets coming from an IP address entered in this field. • Select IP Range to filter packets coming from a specified range of IP addresses entered in this field. • Select IP Address-based Group to filter packets coming from a 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	This field is to specify the Source MAC address . • Select Any to filter packets coming from any MAC addresses. • Select Specific MAC Address to filter packets coming from a MAC address entered in this field. • Select MAC Address-based Group to filter packets coming from a pre-defined group. 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, if a matched rule is found, the packets will be dropped. • In the White List mode, if a matched rule is found, the packets will be accepted while others which 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 a specific Time Schedule to this rule; otherwise leave it as (0) Always . 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 back to last page.

4.2.3 MAC Control

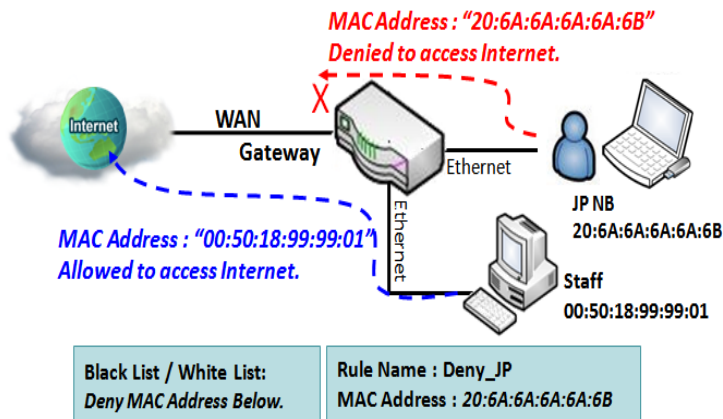
The "MAC Control" function allows you to control the access to the gateway for different users according to a device's MAC address.

Configuration	
Item	Setting
MAC Control	☒ Enable
Black List / White List	Deny MAC Address Below. ▼
Log Alert	☐ Enable
Known MAC from LAN PC List	▼ Copy to

MAC Control Rule List					
ID	Rule Name	MAC Address	Time Schedule Rule	Enable	Actions
MAC Control Rule List Add Delete					

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	
Item	Setting
▶ MAC Control	☐ Enable
▶ Black List / White List	Deny MAC Address Below. ▼
▶ Log Alert	☐ Enable
▶ Known MAC from LAN PC List	▼ Copy to

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.

MAC Control Rule List Add Delete ⬆ ✕					
ID	Rule Name	MAC Address	Time Schedule Rule	Enable	Actions

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

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

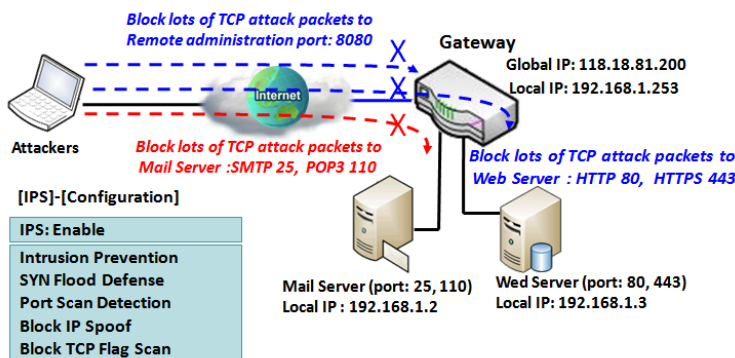
MAC Control Rule Configuration		
Item	Value setting	Description
Rule Name	1. String format can be any text 2. A Must fill setting	Enter a MAC Control rule name.
MAC Address (Use: to Compose)	1. MAC Address string Format with Colon-Hexadecimal notation. 2. A Must fill setting	Specify the Source MAC Address to filter rule, e.g. 00:1B:44:11:3A:B7.
Time Schedule	A Must fill setting	Apply Time Schedule to this rule; otherwise leave it as (0) Always . 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	Cancel the settings.

4.2.4 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.

Configuration	
Item	Setting
▶ IPS	☐ Enable
▶ Log Alert	☐ Enable
Intrusion Prevention	
Item	Setting
▶ SYN Flood Defense	☐ Enable 300 Packets/second (10~10000)
▶ UDP Flood Defense	☐ Enable 300 Packets/second (10~10000)
▶ ICMP Flood Defense	☐ Enable 300 Packets/second (10~10000)
▶ Port Scan Defense	☐ Enable 200 Packets/second (10~10000)

IPS Scenario



As shown in the diagram, the gateway provides email service and web service as well as remote administration through certain ports. So remote 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

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

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

Enable IPS Firewall

Configuration	
Item	Setting
▶ IPS	☐ Enable
▶ Log Alert	☐ Enable

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.

Set up Intrusion Prevention Rules

Enable specific intrusion prevention functions. Ensure that IPS is enabled first.

Intrusion Prevention	
Item	Setting
▶ SYN Flood Defense	☐ Enable 300 Packets/second (10~10000)
▶ UDP Flood Defense	☐ Enable 300 Packets/second (10~10000)
▶ ICMP Flood Defense	☐ Enable 300 Packets/second (10~10000)
▶ Port Scan Defense	☐ Enable 200 Packets/second (10~10000)
▶ Block Land Attack	☐ Enable
▶ Block Ping of Death	☐ Enable
▶ Block IP Spoof	☐ Enable
▶ Block TCP Flag Scan	☐ Enable
▶ Block Smurf	☐ Enable
▶ Block Traceroute	☐ Enable
▶ Block Fraggle Attack	☐ Enable
▶ ARP Spoofing Defense	☐ Enable 300 Packets/second (10~10000)

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, the 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. <u>Value Range:</u> 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. <u>Value Range:</u> 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 addresses. 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. <u>Value Range:</u> 10 ~ 10000.
Save	NA	Save the settings.
Undo	NA	Discard the settings.

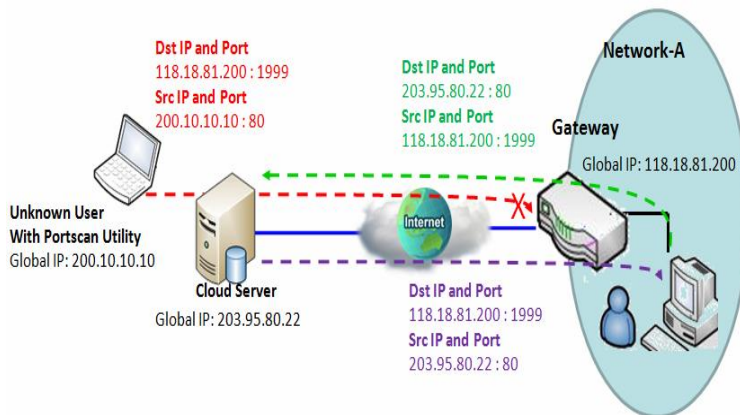
4.2.5 Options

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 coming from the WAN. And finally, “Remote Administrator Hosts” enables you to perform administrative tasks from remote hosts with specified IP address(es).

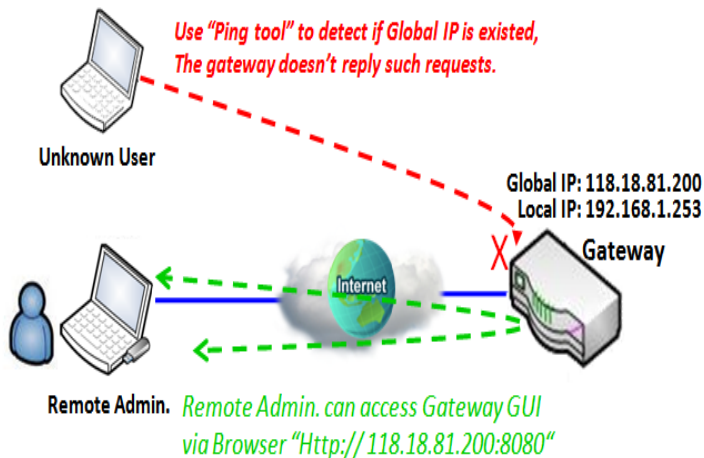
Enable SPI Scenario

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. When an unknown user sends a forged packet to the cloud server through the gateway, the SPI firewall 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** to enable advanced security options of the firewall such as remote access control.

Enable Firewall Options

Firewall Options	
Item	Setting
▶ Stealth Mode	☐ Enable
▶ SPI	☒ Enable
▶ Discard Ping from WAN	☐ Enable

Firewall Options		
Item	Value setting	Description
Stealth Mode	The box is unchecked by default	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							
ID	Interface	Protocol	IP	Subnet Mask	Service Port	Enable	Action
1	All WAN	HTTPS	Any IP	N/A	443	☐	Edit
2	All WAN	HTTPS	Any IP	N/A	443	☐	Edit
3	All WAN	HTTPS	Any IP	N/A	443	☐	Edit
4	All WAN	HTTPS	Any IP	N/A	443	☐	Edit
5	All WAN	HTTPS	Any IP	N/A	443	☐	Edit

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. <u>Value Range</u> : 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.

4.3 Authentication

The Authentication page provides authentication services to clients who request connection access; thus, only authenticated users are granted access to the Internet and controlled resources.

4.3.1 MAC Authentication

A RADIUS server can be used to authorize Internet access with allowed MAC addresses. It checks user information sent via the gateway and permits or blocks connection requests.

Go to Security > Authentication > MAC Authentication.

Enable MAC Authentication

Configuration	
Item	Setting
Mac Authentication	☐ Enable
Radius Server	--- Option --- Add Object
LAN Interface	☐ LAN
Client Connection Idle Time	(20 - 6000 Seconds)

Configuration Item	Value setting	Description
MAC Authentication	The box is unchecked by default.	Enable the MAC Authentication function.
Radius Server	A must-filled setting.	Specify an external RADIUS server for authentication. When the MAC Authentication is enabled, the gateway sends out the connecting client's information to the RADIUS server for authentication.
LAN Interface	A must-filled setting.	Select the network interface(s) to apply the MAC Authentication function. It can be LAN or VLAN(s) (port-based). At least one interface should be selected. Note: DON'T choose the interface with a RADIUS server connected to it.
Client Connection Idle Time	A must-filled setting.	Specify the idle time (in seconds) for a client's connection. If a client doesn't access the network during the specified idle time period, its authentication will be invalidated consequently.
Save	N/A	Save the changes.
Refresh	N/A	Refresh current page.

Create/Edit User List

The User List lists the information of all available users. You can create, edit, delete, or search by keywords to obtain user information.

User List				
Filter by None Add Delete admin Filter				
Previous Next				
ID	Nickname	User Name	Password	Actions

User List		
Item	Value setting	Description
Nickname	N/A	It displays the nickname of a user.
User Name	N/A	It displays the MAC address of a client device..
Password	N/A	It displays the password for a user.
Add	N/A	Add information of a new user.
Delete	N/A	Delete information of a selected user.
Filter	N/A	Enter a keyword to filter the list.
Previous	N/A	Navigation Button of authentication list
Next	N/A	Navigation Button of authentication list

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


User Configuration
Save
✕

Item	Setting
Nickname	
User Name	
Password	

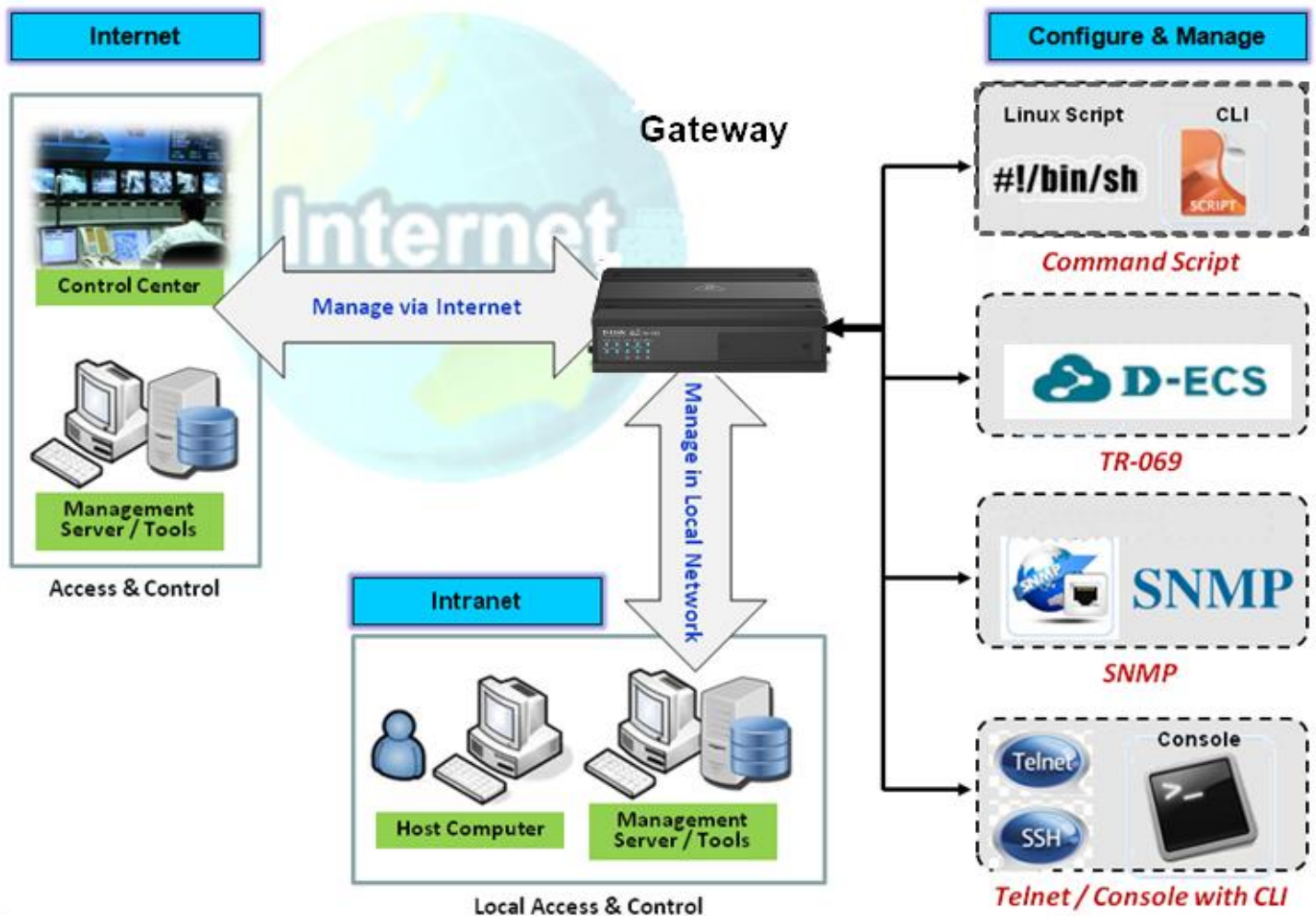
User List		
Item	Value setting	Description
Nickname	1. A must-filled setting. 2. String format can be any text (max. 64 characters).	Enter a nickname for easier identification. <u>Value Range:</u> 1 ~ 64 characters.
User Name	1.A must-filled setting. 2. MAC address format.	Enter the MAC address of the client device. <u>Value Range:</u> 0 ~ 17 characters, MAC format with ':' or '-'.
Password	1. A must-filled setting. 2. String format can be any text (max. 64 characters).	Enter the password for the user.
Save	N/A	Save changes.

Note: A user must be created first in the User List for user authorization.

Chapter 5 Administration

5.1 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 different system management utilities, such as Command Script, SNMP, and Telnet with CLI.



5.1.1 Command Script

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

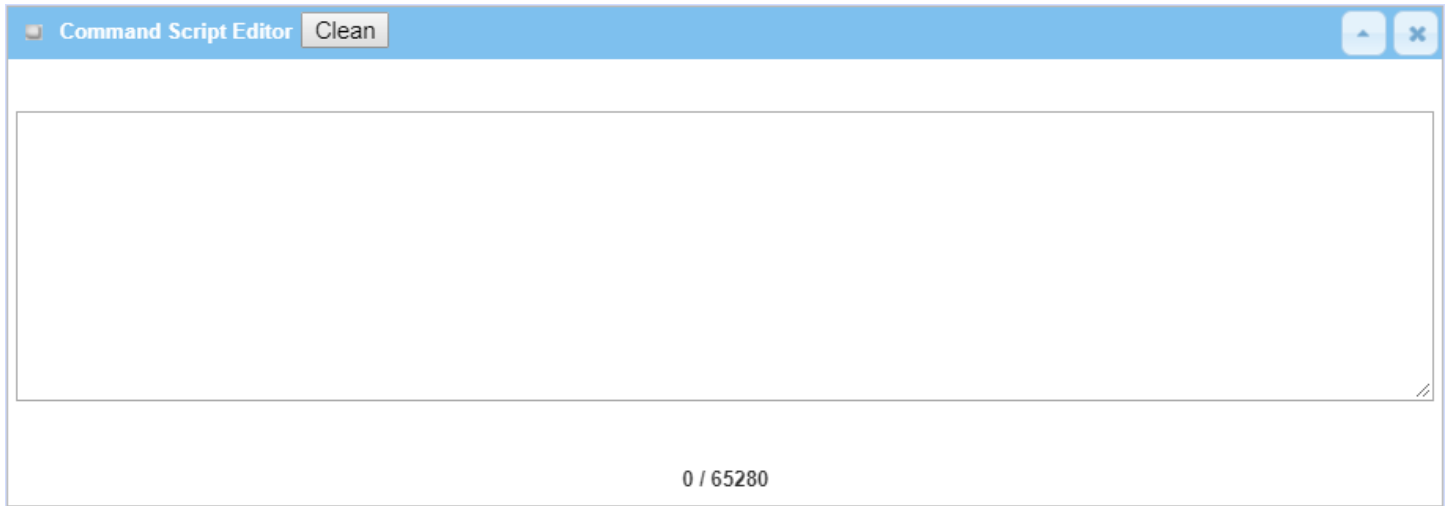
Go to **Administration > Configure & Manage > Command Script > Configuration** to access the Command Script page.

Enable Command Script Configuration

Configuration	
Item	Setting
▶ Command Script	☐ Enable
▶ Backup Script	<button>Via Web UI</button>
▶ Upload Script	<button>Via Web UI</button>
▶ Script Name	
▶ Version	
▶ Description	
▶ Update time	2019-04-08T18:05:31

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. <u>Value Range</u> : 0 ~ 32 characters.
Version	1.An optional setting 2.Any string	Specify the version number for the applied Command script. <u>Value Range</u> : 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	Backup and download configuration.
Save	NA	Save 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	<i>Output file</i>	Duplicate the configuration content from database and store it as a configuration file. (ex: <i>txtConfig clone /tmp/config</i>) 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: <i>txtConfig commit /tmp/config</i>)
enable	NA	Enable plain-text system configuration. (ex: <i>txtConfig enable</i>)
disable	NA	Disable plain-text system configuration. (ex: <i>txtConfig disable</i>)

run_immediately	<i>NA</i>	Apply the configuration content that has been committed in database. (ex: <i>txtConfig run_immediately</i>)
run_immediately	a existing file	Assign a configuration file to apply. (ex: <i>txtConfig run_immediately /tmp/config</i>)

5.1.2 Device Management

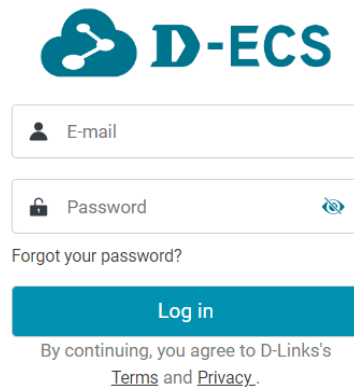
Designed especially for central management of 4G/5G gateway devices, D-ECS is a cloud management platform that offers the utmost in flexibility and availability for device deployment and management. In order for the D-ECS system to communicate with individual devices, device registration must be done 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 **Administration > 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
Self-Certification	Enable self-signed certificates if it is used for a secure website.
Note: The service URL and Server IP STUN Traffic should be modified accordingly depending on the deployment architecture of the D-ECS system.	

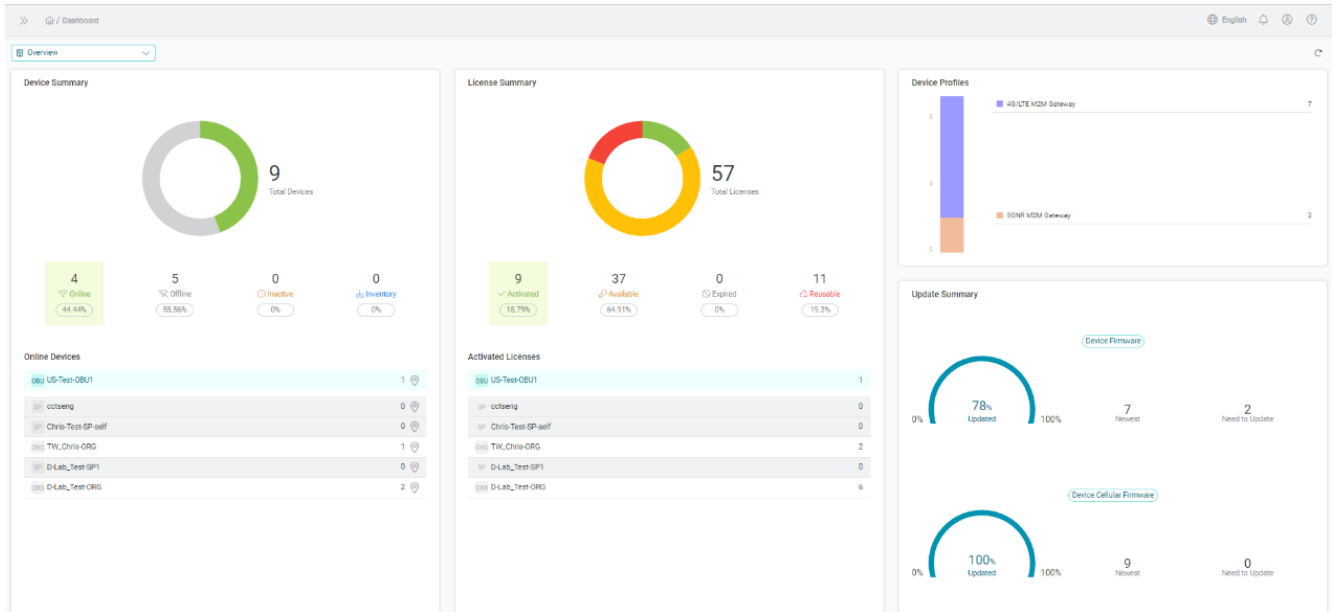
2. Log in to the D-ECS Management Interface by typing the URL in your browser's address field:
<https://portal.decs.dlink.com/login>.



The image shows the D-ECS login interface. At the top is the D-ECS logo, which consists of a blue cloud icon with a white network symbol inside, followed by the text 'D-ECS' in blue. Below the logo are two input fields: 'E-mail' with a person icon and 'Password' with a lock icon and an eye icon for toggling visibility. Below the password field is a link that says 'Forgot your password?'. A blue 'Log in' button is positioned below the links. At the bottom, there is a line of text: 'By continuing, you agree to D-Links's [Terms and Privacy](#).'

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.



5.1.3 RESTful

The Representational State Transfer (REST) interface allows you to securely connect to the gateway to execute remote procedure calls. You can configure this service on the gateway by setting up IP addresses and port numbers for both HTTP and HTTPS access.

Go to **Administration > Configure & Manage > RESTful** to access the configuration page.

Enable RESTful Configuration

Item	Setting
▶ RESTful API	☐ Enable
▶ Interface	WAN-1 ▾
▶ API Access Protocol	http only ▾
▶ API Access Port	6875 (0-65535)
▶ Heartbeat	☐ Enable
▶ URL	limit length = 128
▶ Interval	300 (10-2678400)
▶ Options	☐ CPU ☐ Memory ☐ Data_Usage ☐ Modem_Status ☐ Uptime

Configuration		
Item	Value setting	Description
RESTful API	The box is unchecked by default	Enable or disable the RESTful API.
Interface	N/A	Select either LAN or WAN to apply the RESTful service.
API Access Protocol	N/A	Select the connection protocol: http only or https only.
API Access Port	The default is 6875	TCP port for incoming HTTP connections
Heartbeat	The box is unchecked by default	Enable or disable the heartbeat feature.
HTTPs Certificate Setup		Select the certificate to be used for HTTPs connection
URL	1.An optional setting 2.Any valid file name	Set the addresses on which the server listens for incoming HTTP/HTTPs connections.
Interval	1.An optional setting 2.Any string	Specify the interval for status report frequency. <u>Value Range</u> : 10-2678400 seconds.
Options		Specify the system resource to obtain status on: CPU, Memoryc, Data_Usage, Modem_Status, and Uptime
Save	N/A	Save changes.
Undo	N/A	Discard the changes.

5.1.4 SNMP

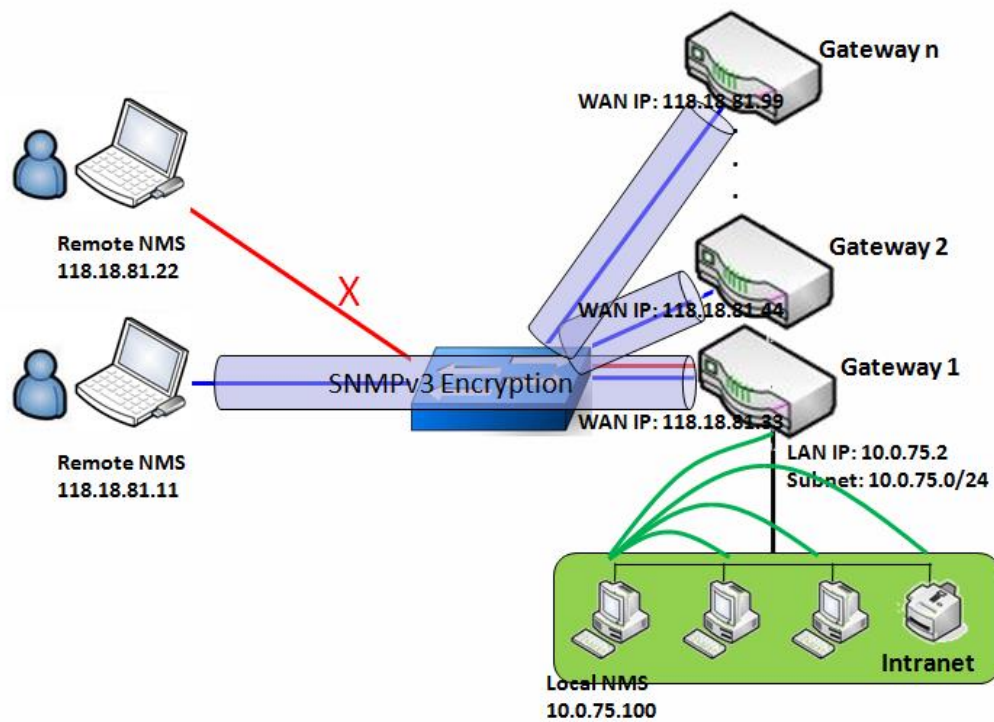
In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give users the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

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

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. The 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

Item	Setting
SNMP Enable	☒ LAN ☐ WAN
WAN Interface	All WANs ▾
Supported Versions	☒ v1 ☒ v2c ☐ v3
SNMP Port	161
Trap Period	10 (1~1440 minutes)
Limited Remote Access IP	Specific IP Address ▾ (IP Address/FQDN) ☐ Enable (IP Address/FQDN) ☐ Enable (IP Address/FQDN) ☐ Enable (IP Address/FQDN) ☐ Enable (IP Address/FQDN) ☐ Enable

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 . <u>Value Range</u> : 1 ~ 65535.
Trap Period	1~1440 minutes	Specify the frequency of trap generation. Note you also need to configure Trap Event Receiver below.
Limited Remote Access 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.

Multiple Community List Add Delete ▲ ✕			
ID	Community	Enable	Actions

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

Multiple Community Rule Configuration	
Item	Setting
Community	Read Only ▼
Enable	☒ Enable

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 (for sending GET and GETNEXT requests) or Read-Write (for sending GET, GETNEXT, and SET requests) 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.

User Privacy List Add Delete ▲ ✕										
ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	OID Filter Prefix	Enable	Actions

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

User Privacy Rule Configuration	
Item	Setting
▶ User Name	
▶ Password	
▶ Authentication	None ▼
▶ Encryption	None ▼
▶ Privacy Mode	noAuthNoPriv ▼
▶ Privacy Key	
▶ Authority	Read ▼
▶ OID Filter Prefix	1
▶ Enable	☒ Enable

User Privacy Rule Configuration		
Item	Value setting	Description
Username	1. A must-filled setting 2. String format: any text	Specify the Username for this version 3 user. <u>Value Range</u> : 1 ~ 32 characters.
Password	1. String format: any text	For Privacy mode of authNoPriv or authPriv , specify the Password for this version 3 user. <u>Value Range</u> : 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 nodes of the given OID. <u>Value Range</u> : 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.

Trap Event Receiver List												Actions
ID	Server IP	Server Port	SNMP Version	Community Name	User Name	Password	Privacy Mode	Authentication	Encryption	Privacy Key	Enable	

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

Trap Event Receiver Rule Configuration	
Item	Setting
▶ Server IP	(IP Address/FQDN)
▶ Server Port	162
▶ SNMP Version	v1
▶ Community Name	
▶ Enable	☒ Enable

Trap Event Receiver Rule Configuration	
Item	Setting
▶ Server IP	(IP Address/FQDN)
▶ Server Port	162
▶ SNMP Version	v3
▶ Community Name	
▶ User Name	
▶ Password	
▶ Privacy Mode	noAuthNoPriv
▶ Authentication	None
▶ Encryption	None
▶ Privacy Key	
▶ Enable	☒ Enable

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 gateway will send traps to the server's 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. <u>Value Range</u> : 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. <u>Value Range</u> : 1 ~ 32 characters.
Username	1. A v3 Must filled setting 2. String format: any text	Specify the Username for version 3. <u>Value Range</u> : 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. <u>Value Range</u> : 8 ~ 64 characters.
Privacy Mode	1. A v3 Must filled setting 2. noAuthNoPriv is selected by default	Select noAuthNoPriv if you do not use any authentication types and encryption methods. For authNoPriv , specify the Authentication and Password. For authPriv , specify the Authentication, Password, Encryption and Privacy Key.
Authentication	1. A v3 Must filled setting 2. None is selected by default	For Privacy Mode of authNoPriv or authPriv , specify the Authentication type: MD5 or SHA-1.
Encryption	1. A v3 Must filled setting 2. None is selected by default	For Privacy Mode of authPriv , specify the Encryption protocol: DES or AES.
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.

Specify settings for the MIB-II System

SNMP MIB-2 System	
Item	Setting
sysContact	
sysLocation	

SNMP MIB-2 System Configuration		
Item	Value setting	Description
sysContact	1. An Optional filled setting 2. String format: any text	Specify the contact information for MIB-2 system. <u>Value Range:</u> 0 ~ 64 characters.
sysLocation	1. An Optional filled setting 2. String format: any text	Specify the location information for MIB-2 system. <u>Value Range:</u> 0 ~ 64 characters.

Edit SNMP Options

If you use a private MIB, you must fill the enterprise name, number and OID.

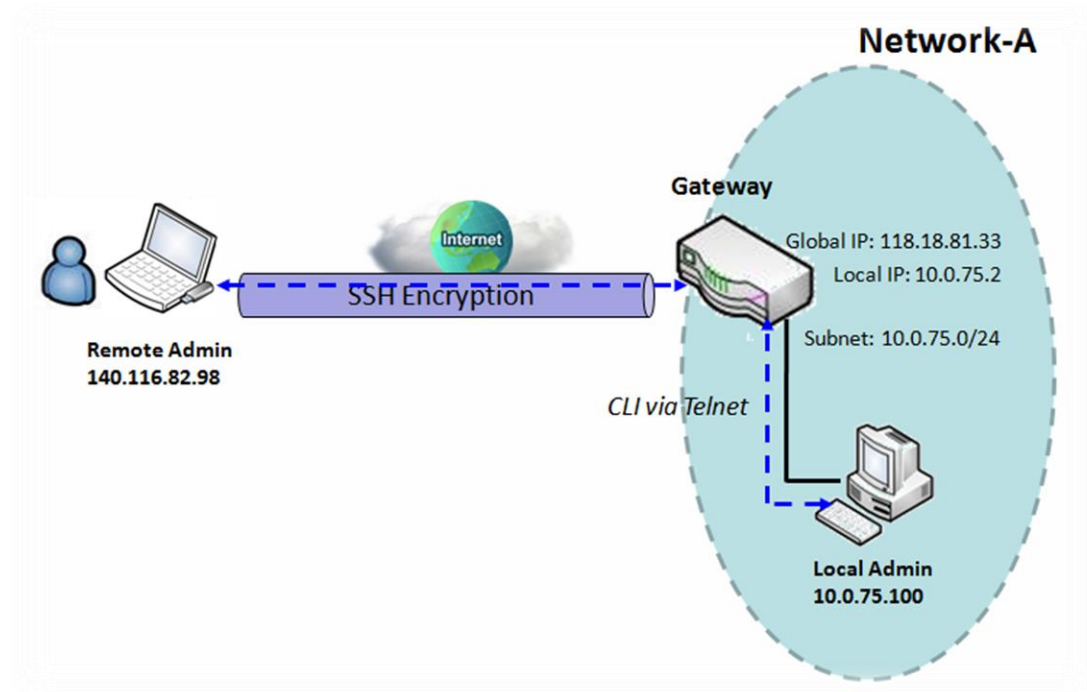
Options	
Item	Setting
Enterprise Name	Dlink
Enterprise Number	171
Enterprise OID	1.3.6.1.4.1. 171.70.4.9

Options		
Item	Value setting	Description
Enterprise Name	1. The default value is Dlink 2. A must-filled setting 3. String format: any text	Specify the Enterprise Name for the particular private MIB. <u>Value Range:</u> 1 ~ 10 characters: A~Z, a~z, 0~9, '-', and '_'.
Enterprise Number	The default value is 171 (Default Enterprise Number) 2. A must-filled setting 3. String format: any number	Specify the Enterprise Number for the particular private MIB. <u>Value Range:</u> 1 ~ 2080768.
Enterprise OID	1. The default value is 1.3.6.1.4.1.171.70.4.9 (Default Enterprise OID) 2. A must-filled setting 3. String format: any legal OID	Specify the Enterprise OID for the particular private MIB where the 1.3.6.1.4.1 represents iso.org.dod.internet.private.enterprise . The value range of the each OID number of the OID string in ASN.1 notation is 1 to 2080768. The maximum length of the enterprise OID is 31. The seventh number must be the enterprise number.
Save	N/A	Save the configuration and apply your changes to SNMP.
Undo	N/A	Cancel the settings.

5.1.5 Telnet & SSH

A command-line interface (CLI), also known as text input and converts commands to appropriate operating system functions. Programs wit 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 h 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).

Parameter Setup Example

Following table lists the parameter configuration as an example for the Gateway in above diagram with "Telnet with CLI" enabling at LAN and WAN interfaces.

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

Configuration Path	[Telnet & 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
Save
Undo

Item	Setting
▶ Telnet	LAN ☒ Enable WAN ☐ Enable (WAN-1 ☒ WAN-4 ☐) Service Port 23
▶ SSH	LAN ☒ Enable WAN ☐ Enable (WAN-1 ☒ WAN-4 ☐) Service Port 22

Configuration		
Item	Value setting	Description
Telnet	1. The LAN Enable box is checked by default.	Activate the Telnet function for the specified LAN or WAN interface. Specify the Service Port for the corresponding service. <u>Value Range:</u> 1 ~65535.
	2. By default Service Port is 23.	
SSH	3. The LAN Enable box is checked by default.	Activate the SSH Telnet function for the specified LAN or WAN interface. Specify the Service Port for the corresponding service. <u>Value Range:</u> 1 ~65535.
	4. By default Service Port is 22.	
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.		

5.2 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.

5.2.1 Password & MMI

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

Set up Host Name

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

Host Name	
Item	Setting
Host Name	

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	
Item	Setting
Username	admin Modify
New Username	
Password	

Password	
Item	Setting
▶ Old Password	
▶ New Password	
▶ New Password Confirmation	

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 Setting for Accessing

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.

Item	Setting
▶ Login	Password-Guessing Attack & MAX: 3 (times)
▶ Login Timeout	☒ Enable 300 (seconds)
▶ GUI Access Protocol	http/https ▼
▶ HTTPs Certificate Setup	☒ default ☐ Select from Certificate List Certificate: TrustedCert0 Key: TrustedKey0
▶ HTTP Compression	☒ gzip ☐ deflate
▶ HTTP Binding	☒ DHCP 1
▶ System Boot Mode	Normal Mode ▼

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 <i>"Already reaching maximum Password-Guessing times, please wait a few seconds!"</i> 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. <u>Value Range:</u> 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

5.2.2 System Information

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

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

System Information	
Item	Setting
▶ Model Name	VHG87BAM_0T001
▶ Device Serial Number	
▶ Kernel Version	2.6.36
▶ FW Version	0000Y90.J31_e32.BETA_04021700
▶ System Time	Thu, 18 Apr 2019 16:18:16 +0800
▶ Device Up-Time	15day 22hr 30min 35sec

System Information		
Item	Value Setting	Description
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.

5.2.3 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 Configuration	
Item	Setting
▶ Synchronization method	Time Server ▼
▶ Time Zone	(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼
▶ Auto-synchronization	Time Server: Available Time Servers (RFC-868): Auto ▼
▶ Daylight Saving Time	☐ Enable
▶ NTP Service	☐ Enable
▶ Synchronize immediately	Active

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 with Manual Setting

System Time Configuration

Item	Setting
Synchronization method	Manual
Time Zone	(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
Daylight Saving Time	☐ Enable
Set Date & Time Manually	2019 / April / 18 (Year/Month/Day) 16 : 24 : 27 (Hour:Minute:Second)
NTP Service	☐ Enable

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 Configuration

Item	Setting
Synchronization method	PC
NTP Service	☐ Enable
Synchronize immediately	Active

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 Configuration

Item	Setting
▶ Synchronization method	Cellular Module ▼
▶ Time Zone	(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼
▶ NTP Service	☐ Enable
▶ Synchronize immediately	Active

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 Configuration	
Item	Setting
▶ Synchronization method	Time Server ▾
▶ Time Zone	(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▾
▶ Auto-synchronization	Time Server: Available Time Servers (RFC-868): Auto ▾
▶ Auto Daylight Saving Time	☒ Enable
▶ NTP Service	☒ Enable
▶ Synchronize immediately	Active

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.
Auto synchronization		Synchronize with a configured time server.
Auto Daylight Saving Time		Enable the Daylight Saving time for time adjustment.
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 will synchronize with the above selected time 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.

5.2.4 System Log

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

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

System Log
View
Email Now

Item	Setting
▶ Web Log Type Category	☒ System ☒ Attacks ☒ Drop ☒ Login message ☐ Debug
▶ Email Alert	☐ Enable Server: --- Option --- ▼ Add Object E-mail Addresses: Subject: Log type Category: ☐ System ☐ Attacks ☐ Drop ☐ Login message ☐ Debug
▶ Syslog	☐ Enable Server: --- Option --- ▼ Add Object Log type Category: ☐ System ☐ Attacks ☐ Drop ☐ Login message ☐ Debug
▶ Log to Storage	☒ Enable Select Device: Internal ▼ Log file name: syslog Split file: ☐ Enable Size: 200 KB ▼ Interval: ☐ Enable 1440 (1 ~ 10080 Minutes) Max Records: 3000 (5~10000) Download log file clear logs Log type Category: ☒ System ☒ Attacks ☒ Drop ☒ Login message ☒ Debug

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 story 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 Previous Next First Last Download Clear	
Time	Log
Apr 1 06:01:36	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb
Apr 1 06:08:31	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb
Apr 1 06:15:30	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb
Apr 1 06:22:06	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb
Apr 1 06:28:42	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb
Apr 1 06:35:42	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb
Apr 1 06:42:20	dnsmasq-dhcp[6016]: Ignoring domain amit.com.tw for DHCP host name NB-msnb

Web Log List Window		
Item	Value Setting	Description
Time column	N/A	It displays event time stamps
Log column	N/A	It displays Log messages

Web Log List 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 logs.
Back	N/A	Return to the previous page.

Web Log Type Category

Web Log Type Category screen allows network administrator to select the type of events to log and be displayed in the Web Log List Window as described in the previous section. Click on the View button to view Log History in the Web Log List window.

▶ Web Log Type Category

☒ System☒ Attacks☒ Drop☒ Login message☐ Debug

Web Log Type Category Setting Window		
Item	Value Setting	Description
System	Checked by default	Check to log system events and to display in the Web Log List window.
Attacks	Checked by default	Check to log attack events and to display in the Web Log List window.
Drop	Checked by default	Check to log packet drop events and to display in the Web Log List window.
Login message	Checked by default	Check to log system login events and to display in the Web Log List window.
Debug	Un-checked by default	Check to log debug events and to display in the Web Log List window.

Email Alert

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

▶ Email Alert	☐ Enable
	Server: --- Option --- ▾ Add Object
	E-mail Addresses:
	Subject:
	Log type Category: ☐ System ☐ Attacks ☐ Drop ☐ Login message ☐ Debug

Email Alert Setting Window

Item	Value Setting	Description
Enable	Un-checked by default	Check 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

☐ Enable
Server: --- Option --- ▼
Add Object

Log type Category:
☐ System
☐ Attacks
☐ Drop
☐ Login message
☐ Debug

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

☒ Enable
Select Device: Internal ▼
Log file name: syslog
Split file: ☐ Enable Size: 200 KB ▼
Interval: ☐ Enable 1440 (1 ~ 10080 Minutes)
Max Records: 3000 (5~10000)
Download log file clear logs
Log type Category:
☒ System
☒ Attacks
☒ Drop
☒ Login message
☒ Debug

Log to Storage Setting Window

Item	Value Setting	Description
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	200 KB is set by default	Enter the file size limit for each split log file. <u>Value Range:</u> 10 ~ 1000.
Interval	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. <u>Value Range:</u> 1 ~ 10080 Minute.
Max Records	3000 is set by default	Enter the maximum number of records to be stored in the log storage. <u>Value Range:</u> 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	Click the Download log file button to download log files to a log.tar file.
Clear Logs	N/A	Click the Clear logs button to delete the log files from the storage.

5.2.5 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	Setting
▶ FW Upgrade	Via Web UI ▼ FW Upgrade
▶ Backup Configuration Settings	Download ▼ Via Web UI
▶ Auto Restore Configuration	☐ Enable Save Conf. Clean Conf. Conf. Info.
▶ Self-defined Logo	Download ▼ Via Web UI Reset
▶ Self-defined CSS	Edit : Download ▼ Via Web UI Reset

FW Backup & Restore		
Item	Value Setting	Description
FW Upgrade	Via Web UI is selected by default	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 configuration stored in the memory 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.

5.2.6 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	
Item	Setting
▶ Reboot	Now ▼ Reboot
▶ Reset to Default	Reset

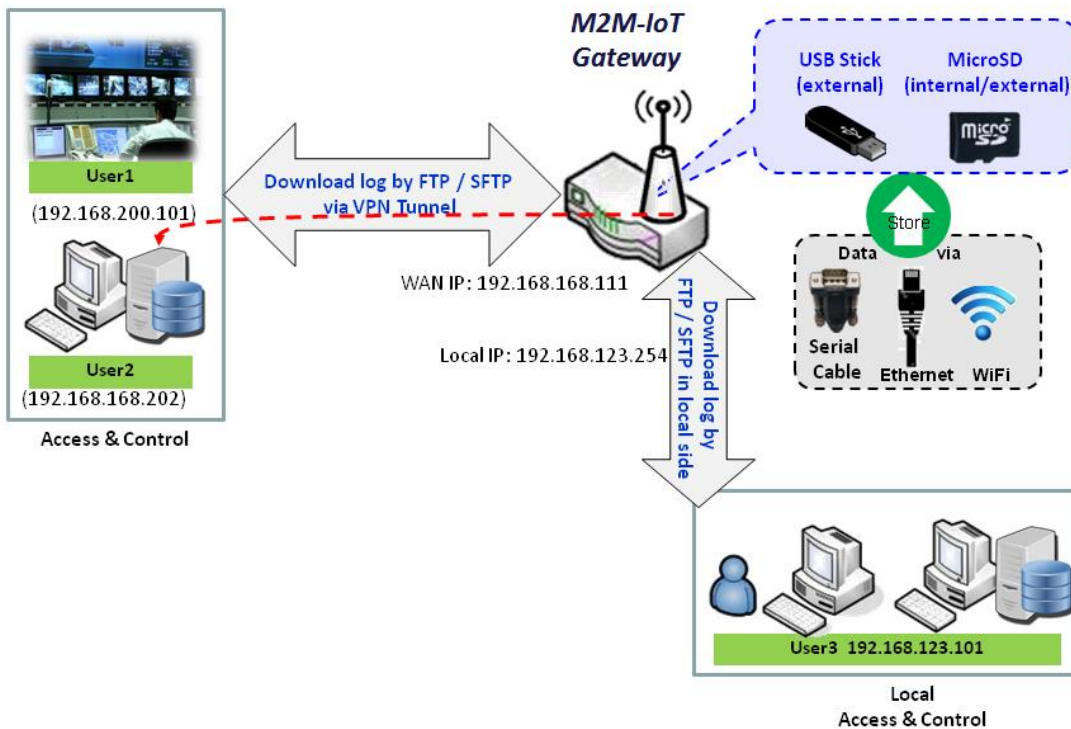
System Operation Window		
Item	Value Setting	Description
Reboot	Now is selected by default	Click the Reboot button to reboot the gateway immediately or schedule a auto reboot. Now: Reboot immediately Time Schedule: Select a pre-defined schedule to reboot the device. To define a schedule, go to Object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

5.3 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 account, 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 log (refer to **Administration > System Operation > System Log**) and GNSS log (refer to **Service > Location Tracking > GNSS**).



5.3.1 Server Configuration

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

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

Enable FTP Server

FTP Server Configuration
Save
⬆
✕

Item	Setting
▶ FTP	☒ Enable
▶ FTP Port	21
▶ Timeout	300 second(s)(60-7200)
▶ Max. Connections per IP	2 ▼
▶ Max. FTP Clients	5 ▼
▶ PASV Mode	☐ Enable
▶ Port Range of PASV Mode	50000 ~ 50031
▶ Auto Report External IP in PASV Mode	☐ Enable
▶ ASCII Transfer Mode	☐ Enable
▶ FTPS(FTP over SSL/TLS)	☐ Enable

Configuration		
Item	Value setting	Description
FTP	The box is unchecked by default.	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. <u>Value Range:</u> 1 ~ 65535.
Timeout	300 seconds is set by default.	Specify the maximum timeout interval for the FTP connection. <u>Value Range:</u> 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 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. <u>Value Range:</u> 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 Mode	Optional setting	Activate the support of ASCII mode data transfers. 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

SFTP Server Configuration
Save

Item	Setting
▶ SFTP	☐ Enable via ☒ LAN via ☒ WAN (WAN-1 ☒ WAN-4 ☐)
▶ SFTP Port	22

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. <u>Value Range</u>: 1 ~ 65535.

5.3.2 User Account

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

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

Create/Edit FTP User Accounts

User Account List Add Delete						
ID	User Name	Password	Directory	Permission	Enable	Actions

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

User Account Configuration Save	
Item	Setting
▶ User Name	admin
▶ Password	
▶ Directory	Browse
▶ Permission	Read/Write ▼
▶ Enable	☒

Configuration		
Item	Value setting	Description
Username	String : non-blank string	Enter the user account for FTP login. <i>Value Range:</i> 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.

5.4 Diagnostic

This gateway offers some common network diagnostic tools for diagnosing the system and troubleshooting causes of connection problems. The Ping and Tracert tests help test the network connectivity.

5.4.1 Diagnostic Tools

Go to Administration > Diagnostic > Diagnostic Tools to access the tools.

Diagnostic Tools

Item	Setting
▶ Ping Test	Host IP: Outer Interface: Auto ▾ LAN Source: Default ▾ Ping
▶ Tracert Test	Host IP: Interface: Auto ▾ UDP ▾ Tracert
▶ Speed Test	Interface: Auto ▾ mode: DL+UL ▾ ☐ SSL Test
▶ Wake on LAN	Wake up

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.

5.4.2 Ethernet Port Setup

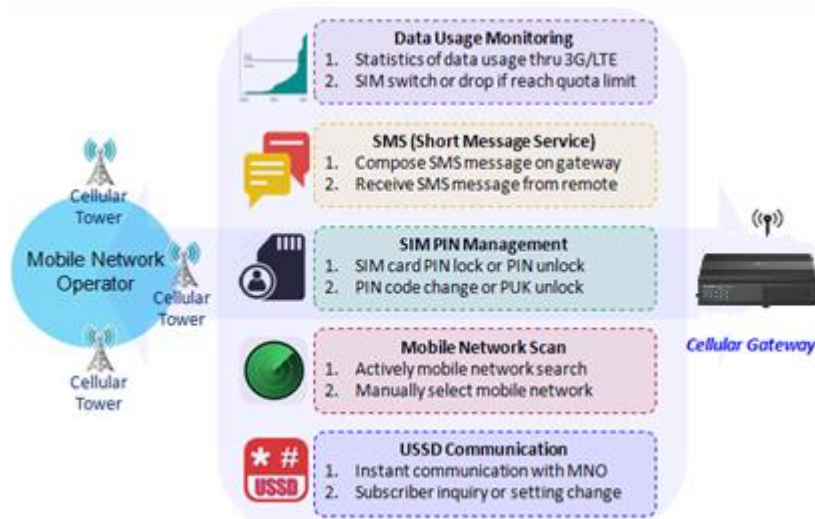
The Ethernet Port Setup function can be used to enable or disable each LAN port of the gateway and adjust flow control of an Ethernet connection. This function helps troubleshoot connectivity and control traffic flow when a connection failure occurs.

Go to Administration > Diagnostic > Ethernet Port Setup to configure the ports.

Ethernet Port Setup		
Item	Value setting	Description
Ethernet Port setup	Enable or disable	Enable or disable the Port Setup function.
Ethernet Port Setup List	Enable or disable	Click Edit to configure the link direction of each port.
Save	N/A	Save the configuration.
Undo	N/A	Discard the changes.

Chapter 6 Service

6.1 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.

6.1.1 Data Usage

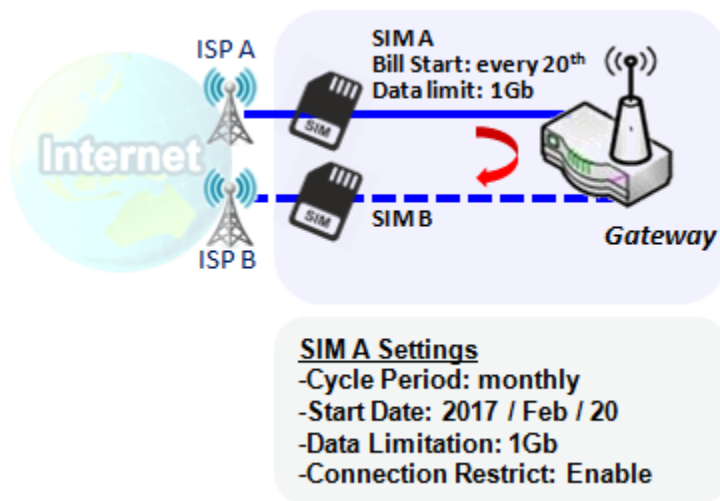
Most cellular data service sets a limit on data usage. If the cellular data usage has been over the data limit, the connection throughput will be reduced or extra charges will incur.

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 Profile List Add Delete								
ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable	Action

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 Data Usage Profile

Cellular Data Usage Profile List Add Delete								
ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable	Action
1	Cellular(5G/LTE) SIM A	Chunghwa	1 Weekly	Wed Jun 12 2024 00:00:00 GMT+0800	1000MB	☒	☒	Edit ☐ Select

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.

3G/4G Data Usage Profile Configuration	
Item	Setting
▶ SIM Select	3G/4G ▾ SIM A ▾
▶ Carrier Name	
▶ Cycle Period	Days ▾
▶ Start Date	2019 ▾ / April ▾ / 1 ▾
▶ Data Limitation	KB ▾
▶ Connection Restrict	☐ Enable
▶ Enable	☒ Enable

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 models 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. <u>Value Range:</u> 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.
---------------	---------------------	----------------------------------

6.1.2 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** tab

You can send SMS text messages or read received SMS messages as you would on a cellular phone.

Set up SMS Configuration

Item	Setting
Physical Interface	3G/4G-1 ▼
SMS	☐ Enable SIM Status: SIM_A
SMS Storage	SIM Card Only ▼
SMS Space	☐ Enable & Keep Available Space (1-10)

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		New SMS	SMS Inbox	SMS Sent Folder		
Item	Setting					
▶ Unread SMS	0					
▶ Received SMS	10					
▶ Sent SMS	0					
▶ Remaining SMS	0					

SMS Summary		
Item	Value setting	Description
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	Setting
▶ Receivers	 (Use '+' for International Format and ';' to Compose Multiple Receivers)
▶ Text Message	Length of Current Input : 0
▶ Result	

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

⬆

ID	From Phone Number	Timestamp	SMS Text Preview	Actions

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 SMS from this screen.

 SMS Sent Folder <button>Delete</button> Close Previous 0 ▼ Next				
ID	Receivers	Timestamp	SMS Text Preview	Actions

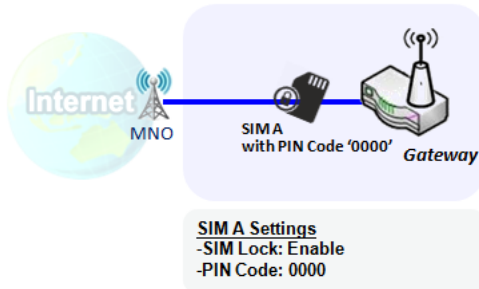
SMS Sent Folder		
Item	Value setting	Description
ID	N/A	The number that identifies the SMS message.
Receivers	N/A	The recipients of the sent message.
Timestamp	N/A	The time that the message is sent.
SMS Text Preview	N/A	Preview the SMS text. Click the Detail button to read a specific message.
Action	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.

6.1.3 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.

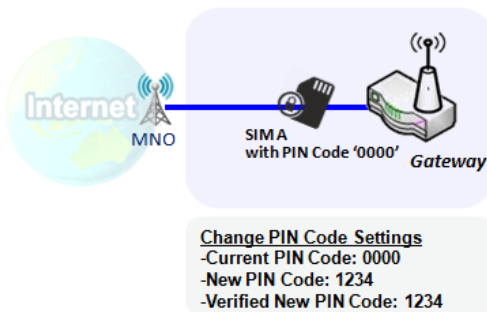
A PIN code on a SIM card has been used widely and the gateway allows you to activate and manage PIN code on a SIM card through the Web UI.

Activate PIN code on SIM Card



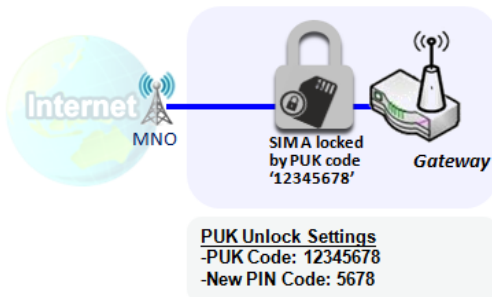
This example shows how to activate PIN code on SIM-A for 3G/4G-1 with the default PIN code “0000”.

Change PIN code on SIM Card



The example 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 will see the remaining times of failure trials. A PUK code will be required to unlock the SIM card.

Select a SIM Card

Configuration

Item	Setting
▶ Physical Interface	3G/4G-1 ▼
▶ SIM Status	SIM-A Ready
▶ SIM Selection	SIM-A ▼ Switch

Configuration Window		
Item	Value setting	Description
Physical Interface	The box is 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	
Item	Setting
▶ PIN Lock	☒ Enable PIN Code: (4~8 digits)
▶ Remaining times	N/A

SIM function Window		
Item Setting	Value setting	Description
PIN lock	Depend on SIM card	Activate 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 unlocking 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	Setting
▶ Current PIN Code	(4~8 digits)
▶ New PIN Code	(4~8 digits)
▶ Verified New PIN Code	(4~8 digits)

Item	Value Setting	Description
Current PIN Code	A must-filled setting	Fill in the current (old) PIN code of the SIM card.
New PIN Code	A must-filled setting	Fill in the new PIN Code you want to change.
Verified New PIN Code	A must-filled setting	Confirm the new PIN Code again.
Apply	N/A	Click the Apply button to change the PIN code with specified new PIN code.
Cancel	N/A	Click the Cancel button to cancel the changes and keep current PIN code.

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

Save

Item

Setting

▶ PUK status	PUK unlock.
▶ Remaining times	N/A
▶ PUK Code	(8 digits)
▶ New PIN Code	(4~8 digits)

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 time, 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 > Connection Setup > Connection with SIM Card** page. Otherwise, it may result in wrong SIM PIN trials with invalid (old) PIN code.

6.1.4 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. 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	Setting
Physical Interface	3G/4G-1 ▼ SIM Status: SIM_A
Network Type	LTE Only ▼
Scan Approach	Auto ▼

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

6.2 Event Handling

The Event Handling allows you to configure pre-defined events, handlers, and corresponding actions with profiles. With this function, you can easily and remotely obtain the status and information on the gateway.

The supported events are categorized into two groups: **Administration** and **System**.

The **Administration events** are events regarding the operation of the gateway, for example, failed login and password changes.

The **System events** are the events that relate to resource consumption such as memory usage.

To start configuring the event handling, you need first enable this function. Then, configure the email servers and remote hosts for sending event notifications on the same Configuration page.

Next, on the Notifying Events page, you have to configure events with event's trigger condition and the corresponding actions (e.g. notification method as pre-configured on the previous Configuration page) for the event. For each event, more than one action can be activated simultaneously.

6.2.1 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		
Item	Setting	
▶ Event Management	☐ Enable	

Configuration Item	Value setting	Description
Event Management	N/A	Enable the event management function to configure event notification servers for corresponding notification method, which can be configured in the Notifying Events page.

Configure Email Servers

Configure emails for sending notifications.

Email Service List				
Add Delete				
ID	Email Server	Email Addresses	Enable	Actions

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 recipient.
Enable	The default is not enabled.	Enable this event handling rule.
Save	N/A	Save the settings.

Create Remote Host Profile

Configure remote hosts for sending notifications when certain events occur. It supports a maximum of 10 profiles.

Remote Host List								
Add Delete								
ID	Host Name	Host IP	Protocol Type	Port Number	Prefix Message	Suffix Message	Enable	Actions

Remote Host Configuration	
Item	Setting
▶ Host Name	
▶ Host IP	
▶ Protocol Type	TCP ▼
▶ Port Number	
▶ Prefix Message	
▶ Suffix Message	
▶ Enable	☐
Save	

Remote Host Configuration		
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	1. String format 2. An Optional filled setting	Enter a message to precede the notification.
Suffix Message	1. String format 2. An Optional 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	NA	Click the Save button to save the configuration

6.2.2 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	Setting
▶ Notifying Events	☒ Enable

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 **6.2.1 Configuration**).

Notifying Event List Add Delete								
ID	Event Name	Event	Trigger Type	Description	Action	Time Schedule	Enable	Actions

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 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 6.2.1 Configuration for the configured event management actions (designated notification servers). 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.

6.3 Location Tracking

Location tracking applications are applications that benefit from Global Navigation Satellite System (GNSS). GNSS is the infrastructure that allows devices to determine their velocity and direction based on the position and time through satellites signals. GNSS includes a variety of satellite systems and Satellite-Based Augmentation Systems (SBAS). SBAS is usually used for improving positioning accuracy. The tables below show 4 major GNSS systems in the world, and SBAS systems in different areas.

Major GNSS System in the world

GNSS System	Owner
GPS	USA
GLONASS	Russia
Galileo	European Union
BeiDou (COMPASS)	China

Satellite-Based Augmentation System (SBAS)

SBAS	Area Coverage
EGNOS	Europe
WAAS	North America
GAGAN	India
MSAS	Japan

Here are the main features of GNSS function on the gateway.



- Retrieve GNSS data from satellites and send to a remote operation center periodically or save the data in local storage.
- Global positioning with multiple GNSS systems, including GPS and optional GLONASS, Galileo, and BeiDou.
- Used with a variety of LBS (Location-Based Service) applications, such as advertisement and emergency call.
- Easy integration with AVL (Automatic Vehicle Location) applications for managing a fleet of service

vehicles.

- Used with other value-added applications, such as asset tracking, electronic toll collection, and intelligent transport system.

6.3.1 GNSS

On the GNSS configuration page, the following functions are available:

- GNSS function activation.
- Customizable prefix and suffix for NMEA 0183 (compatible to 3.0) GPS message type
- GPS data logging in local storage for route record tracking.
- Configurable remote host, time interval, TCP/UDP, and types of GPS data to be sent.

● GPS Message Type

The following table lists all supported types of NMEA 0183 data format. The NMEA 0183 data format was defined and maintained by National Marine Electronics Association (NMEA).

Type	Description	Example
GGA	Fix Information	\$GPGGA,123519,4807.038,N,01131.000,E,1,08,0.9,545.4,M,46.9,M,,*47
GLL	Lat/Lon Data	\$GPGLL,4916.45,N,12311.12,W,225444,A,*1D
GSA	Overall Satellite Data	\$GPGSA,A,3,04,05,,09,12,,,24,,,,,2.5,1.3,2.1*39
GSV	Detailed Satellite Data	\$GPGSV,2,1,08,01,40,083,46,02,17,308,41,12,07,344,39,14,22,228,45*75
RMC	Recommended Minimum Data	\$GPRMC,123519,A,4807.038,N,01131.000,E,022.4,084.4,230394,003.1,W*6A
VTG	Vector Track and Speed Over the Ground	\$GPVTG,054.7,T,034.4,M,005.5,N,010.2,K*48

Note: The availability of GPS message type depends on hardware capability and varies by product models.

● SBAS

SBAS is Satellite-Based Augmentation Systems that is used to improve the accuracy of location data. There are different SBAS systems for different areas in the world.

SBAS	Area Coverage
EGNOS	Europe
WAAS	North America
GAGAN	India
MSAS	Japan

Note: The SBAS feature depends on hardware capability and varies by product models.

● Assisted GPS

Assisted GPS (as known as A-GPS) is used for expedited location fix, especially when satellite signal is weak. After activating this option, the gateway will download almanac data from a A-GPS server through IP network instead of from satellite. You can also choose different data validation intervals. The almanac data will have higher accuracy with a shorter validation period. However, data with a shorter validation period needs to be updated more frequently and thus consume more network bandwidth.

Note: The Assisted GPS feature depends on hardware capability and varies by product models.

- **Data to Storage**

Besides transmitting location data to a remote server, you can also store location data to an internal storage (e.g. microSD card) or an external storage device (e.g. USB drive) in NMEA 0183 raw data format or in GPX file format. The location data will be saved to a new file if the original file size is bigger than the pre-defined file size. You can also browse all saved log files and download them to external devices.

Scenario of location tracking for fleet management

A fleet manager would like to track the location of his trucks in real time. In his operation office, there is a server (IP: 100.100.100.1) which can interpret NMEA RMC data and show a truck's location and display route tracking on the map. The server uses TCP port 888 to receive NMEA RMC data from trucks along with IMEI number added to NMEA RMC data as a prefix for identifying trucks.

Parameter setting example

Basic Settings on each truck:

Configuration Path	[GNSS]-[Configuration]
GNSS	<i>Enable</i>
GNSS Type	<i>GPS</i>
GPS Message Types	<i>RMC</i>
SBAS	<i>Enable</i>
Assisted GPS	<i>Enable, 1</i>
Data to Storage	<i>Disable</i>

Settings for a Remote Server:

Configuration Path	[GNSS]-[Remote Host Configuration]
Host Name	<i>Truck-1</i>
Host IP	<i>100.100.100.1</i>
Protocol Type	<i>TCP</i>
Port Number	<i>888</i>
Interval(s)	<i>15</i>
Prefix Message	<i>123456789012345</i>
Suffix Message	<i>[blank]</i>
Enable Checkbox	<i>[Checked]</i>

GNSS Setting

The GNSS allows you to configure GNSS, log NMEA data to storage, and send data to a remote host. Go to **Service>Location Tracking> GNSS**.

Configure GNSS

Configuration

Item	Setting
GNSS	☒ Enable
GNSS Type	GPS
GNSS Message Types	☐ GGA ☐ GLL ☐ GSA ☐ GSV ☒ RMC ☐ VTG
Data to Storage	☐ Enable Select Device: Internal Interval: 5 (s) Data format: RAW Data file name: RAW_yyyyMMddhhmm Split file: ☒ Enable Type: Size 200 KB RAW_202402220638.log Download log file Delete log file Delete all log file

GNSS Configuration		
Item	Value setting	Description
GNSS Enable	The box is unchecked by default	Activate GNSS functions.
GNSS Type	GPS is selected by default	Select a GNSS Type (GNSS System) that you want to use. Please note this option is hardware dependent.
GNSS Message Types	These box is unchecked by default.	Select one or more GNSS Message Types that you want to use for transmitting and recording GPS data. Only select the type you need, otherwise it will consume unnecessary network bandwidth. Please note this option is hardware dependent.
SBAS	The box is unchecked by default	Check Enable box to activate satellite-based augmentation system (SBAS). Please note this option is hardware dependent.
Assisted GPS	The box is checked by default	Check Enable box to activate Assisted GPS (A-GPS) and specify the update interval in the duration for downloading the Differential Almanac Corrections data from A-GPS server through IP network. Please note this option is hardware dependent.
Data to Storage	The box is unchecked by default	● Enable (The box is unchecked by default) Activate data saving function. ● Select Device (A must-filled setting) Select Internal or External device to store log data. ● Interval (A must-filled setting) Specify the time interval of data generation. By default, 5 second is set. Value Range: 5 ~ 60 seconds. ● Data Format(A must-filled setting) Select data format (RAW or GPX) to store. ● Data file name (A must-filled setting) Define file name to store. ● Split Enable Check Enable box to split large files. ● Split Size& Unit Define file size and unit for splitting each log file. The default is 200 KB and the minimum is 10 KB. ● Download log file Select a log file and Click Download log file to download through Web

		GUI. Delete log file Delete the specified log file. Delete all log file Delete all log files stored in the storage device.
Save	NA	Save the configuration.

Create Remote Host Profile

Configure remote hosts to send NMEA data. The gateway supports a maximum of 10 profiles.

Remote Host List
Add
Delete
▲
×

ID	Host Name	Host IP	Protocol Type	Port Number	Prefix Message	Suffix Message	Enable	Actions
----	-----------	---------	---------------	-------------	----------------	----------------	--------	---------

Remote Host Configuration
×

Item	Setting
▶ Host Name	
▶ Host IP	
▶ Protocol Type	TCP ▼
▶ Port Number	
▶ Prefix Message	
▶ Suffix Message	
▶ Enable	☐

Save

Remote Host Configuration		
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.
Interval(s)	A must-filled setting	Specify the time interval (seconds) between two consecutive NMEA data packets. Value Range: 1 ~255 seconds.
MAC Address Message	Optional	Use MAC address for message delivery.
Prefix Message	1. String format 2. An Optional filled setting	Enter a messaget to proceed the notification.
Suffix Message	1. String format 2. An Optional 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	NA	Save the configuration

6.4 Power Control

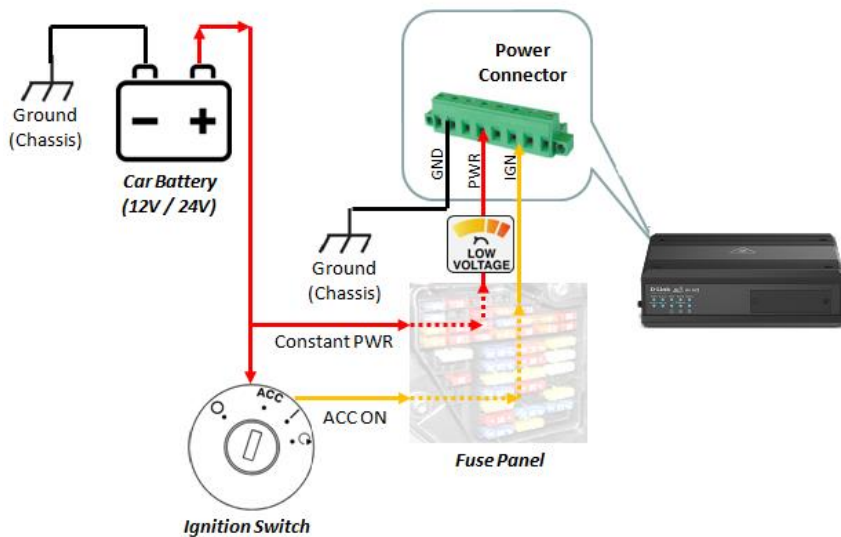
The Power Control supports Ignition Sense function for In-vehicle gateways, or Power Outlet control function for devices supporting external PDU. With power control, you can easily set up the gateway to operate with an external power source such as a vehicle battery or control the device's power ON/OFF with a remote PDU.

6.4.1 Ignition Sense

In most cases, the in-vehicle electronic devices will be shut down when the car's engine stops. And the power supply to almost all in-vehicle devices will be terminated when the car engine stops to prevent in-vehicle devices from draining out battery power.

Designed for in-vehicle applications, the power control features Ignition Sense function that can detect car ignition status and offers the following benefits:

- The gateway continues to operate and powers off according to the delay-off timer control when car engine turns off.
- The gateway will enter standby mode automatically when a pre-set timer is due. When in standby mode, the gateway would stop consuming battery power to prevent draining its power.
- The gateway would enter standby mode automatically if low power voltage is detected.
- The gateway will resume operation when car engine starts.



The following illustrates the delay-off and low-power detection function usage.

**Ignition Sense Settings**

- Ignition Sense: Enable
- Shutdown Timer: 15
- Voltage Sense: Enable
- Shutdown Voltage Threshold: 22

In this example, the surveillance system installed on the bus will transmit video files back to a back-end server when the bus returns to its home station. Even though the driver turns off the engine after he parks the bus, the uplink connection for the surveillance system can still function until all video files are completely uploaded, which takes about **15** minutes. Furthermore, the low voltage detection function can protect battery by turning off the gateway if the detected battery voltage is **22V** (regular voltage is 24V).

Ignition Sense Setting

Go to Service > Power Control > Ignition Sense Tab.

Notes:

1. The availability of the Ignition Sense function depends on product models.
2. The ignition sense feature is disabled by default. Once this feature is enabled, the gateway can only be turned on when the ignition pin is detected (ACC On).

Configuration	
Item	Setting
▶ Ignition Sense	☐ Enable
▶ Shutdown Timer	0 (0~240 minutes)
▶ Voltage Sense	☐ Enable
▶ Shutdown Voltage Threshold	9 (volts) (Range:9V-36V)

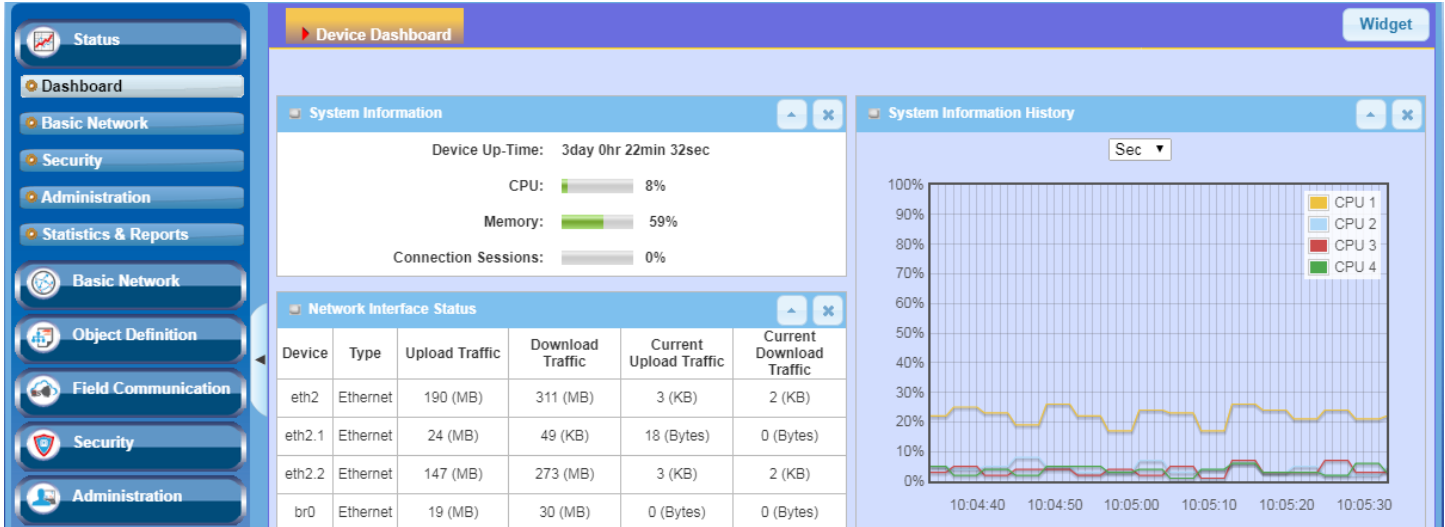
Configuration		
Item	Value setting	Description
Ignition Sense	The box is unchecked by default.	Activate the Ignition Sense function. By default, the function is disabled.
Shutdown Timer	1.Number format : any number between 0 and 240. 2. 0 is set by default.	Enter a shutdown timer (0~240 minutes) to turn off the gateway after the engine stops. '0' means the gateway will never turn off even when the ignition is removed (ACC OFF). <u>Value Range:</u> 0 ~ 240.
Voltage Sense	The box is unchecked by default.	Activate the Voltage Sense function. If the function is enabled, when input voltage reaches the specified threshold value and the ACC (the ignition pin) is detected Off, the gateway will turn off, regardless of the state of the shutdown timer.
Shutdown Voltage Threshold	An optional setting.	Specify a threshold voltage to turn off the gateway when low battery power is detected. <u>Value Range:</u> 9V ~ 36V.
Save	N/A	Save the configuration.
Undo	N/A	Restore the configured back to its previous setting.

Chapter 7 Status

7.1 Dashboard

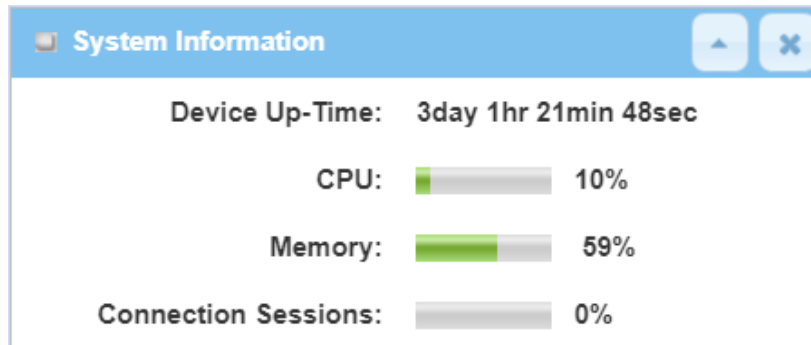
The Device Dashboard window shows the status in graph or tables for a quick overview of the operation status of the gateway. The display will be refreshed very second.

Go to **Status > Dashboard > Device Dashboard** to access the gateway status.



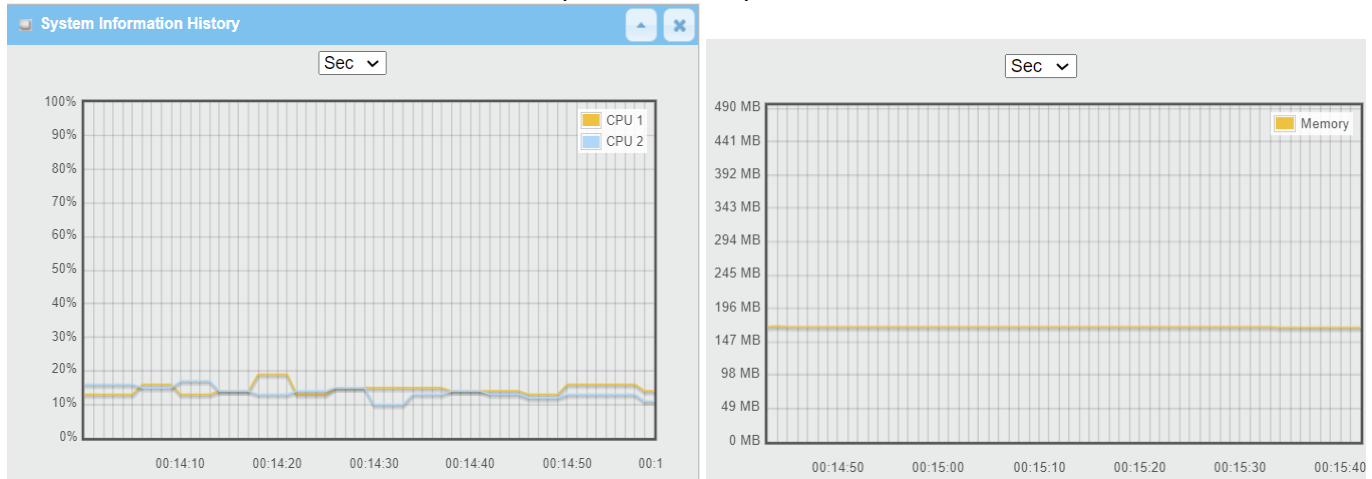
System Information Status

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 on the CPU and memory. You can select the Sec, Min, or Hour menu to show data in the respective time span.



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
rai0	Wireless LAN	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)
br0	Ethernet	31 (MB)	2 (MB)	4 (KB)	677 (Bytes)
eth0.1	Ethernet	32 (MB)	2 (MB)	4 (KB)	677 (Bytes)
apcli0	WiFi	248 (Bytes)	31 (KB)	0 (Bytes)	0 (Bytes)
apcli0	WiFi	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)
ra0	Wireless LAN	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)
eth0	Ethernet	77 (MB)	7 (MB)	4 (KB)	713 (Bytes)

7.2 Basic Network

7.2.1 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	3G/4G	3G/4G	NAT	10.59.152.73	255.255.255.252	10.59.152.74	168.95.1.1, 168.95.192.1	N/A	Connected 0 day 0:26:38	Edit
WAN-2		Disable								Edit

WAN interface IPv4 Network Status		
Item	Value setting	Description
ID	N/A	Displays corresponding WAN interface WAN IDs.
Interface	N/A	Displays the type of WAN physical interface. 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 supported WAN connection methods of 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 Configuration (go to **Basic Network > WAN & Uplink > Connection 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 Configuration (go to **Basic Network > WAN & Uplink > Connection Setup**) and WAN connection status is disconnected.

WAN Interface IPv6 Network Status

WAN interface IPv6 Network Status screen shows status information for IPv6 network.

WAN Interface IPv6 Network Status						
ID	Interface	WAN Type	Link-local IP Address	Global IP Address	Conn. Status	Action
WAN-1	3G/4G	IPv6		/64	Disconnected	Edit

WAN interface IPv6 Network Status		
Item	Value setting	Description
ID	N/A	Displays corresponding WAN interface WAN IDs.
Interface	N/A	Displays the type of WAN physical interface. 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					
IPv4 Address	IPv4 Subnet Mask	IPv6 Link-local Address	IPv6 Global Address	MAC Address	Action
192.168.66.1	255.255.254.0	fe80::250:18ff:fe3a:4a5f	/64	00:50:18:3A:4A:5F	Edit IPv4 Edit IPv6

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).

Cellular Modem Status List					
Interface	Card Information	Link Status	Signal Strength	Network Name	Action
Cellular(5G/LTE)	RM520N-EU	Disconnected	N/A	N/A	Detail

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 WAN Interfaces' total traffic transmitted and received in packets.

Interface Traffic Statistics				
ID	Interface	Received Packets(Mb)	Transmitted Packets(Mb)	Action
WAN-1	3G/4G	217.13	167.09	Reset
WAN-2		-	-	

Interface Traffic Statistics		
Item	Value setting	Description
ID	N/A	Displays corresponding WAN interface'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.

7.2.2 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.

7.2.3 WiFi 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.

WiFi 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	☒	WiFi Uplink	Staff_2.4G	1	b/g/n Mixed	WPA2-PSK(AES)	00:50:18:3A:4A:5F	Edit QR Code
2.4G	VAP-2	☒	WiFi Uplink	default	1	b/g/n Mixed	Open(None)	02:50:18:38:4A:5F	Edit QR Code
2.4G	VAP-3	☐	WiFi Uplink	default	1	b/g/n Mixed	WPA2-PSK(AES)	02:50:18:39:4A:5F	Edit QR Code
2.4G	VAP-4	☐	WiFi Uplink	default	1	b/g/n Mixed	WPA2-PSK(AES)	02:50:18:3A:4A:5F	Edit QR Code
2.4G	VAP-5	☐	WiFi Uplink	default	1	b/g/n Mixed	WPA2-PSK(AES)	02:50:18:3B:4A:5F	Edit QR Code
2.4G	VAP-6	☐	WiFi Uplink	default	1	b/g/n Mixed	WPA2-PSK(AES)	02:50:18:3C:4A:5F	Edit QR Code
2.4G	VAP-7	☐	WiFi Uplink	default	1	b/g/n Mixed	WPA2-PSK(AES)	02:50:18:3D:4A:5F	Edit QR Code

WiFi Virtual AP List		
Item	Value setting	Description
Op. Band	N/A	The WiFi Operation Band (2.4G or 5G) of VAP.
ID	N/A	Displays the ID of VAP.
WiFi Enable	N/A	Displays whether the VAP wireless signal is enabled or disabled.
Op. Mode	N/A	The WiFi Operation Mode of the VAP.
SSID	N/A	Displays the network ID of the VAP.
Channel	N/A	Displays the wireless channel used.
WiFi 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 make a quick access to the WiFi configuration page. (Basic Network > Wi-Fi > Configuration tab) The QR Code button allow you to generate a QR code for quick connection to the VAP by scanning the QR code.

WiFi Uplink Status

The WiFi Uplink Status shows all information of connected WiFi uplink network on each WiFi module..

WiFi Module One Uplink Status							
SSID	BSSID	Channel	Security	RSSI0	RSSI1	Rate	Action
Only_For_Monkey	00:00:00:00:00:00	1	WPA2-PSK(AES)	0	0	0	Edit

WiFi Module One Uplink Status		
Item	Value setting	Description
SSID	N/A	The network ID of VAP.
BSSID	N/A	The BSSID for the connected wireless network.
Channel	N/A	The wireless channel used.
Security	N/A	The authentication and encryption setting for the WiFi uplink connection.
RSSI0, RSSI1	N/A	The Rx sensitivity on each radio path..
Rate	N/A	The link rate for the WiFi uplink connection.
Action	N/A	Click the Edit button to make a quick access to the WiFi uplink configuration page. (Go to Basic Network > WAN & Uplink > Physical Interface tab and click Edit to configure the selected WAN interface.)

WiFi IDS Status

The Wi-Fi IDS Status shows all the wireless intrusion detection system (WIDS) statistics on each Wi-Fi module.

WiFi Module One IDS Status							
Authentication Frame	Association Request Frame	Re-association Request Frame	Probe Request Frame	Disassociation Frame	Deauthentication Frame	EAP Request Frame	Malicious Data Frame
0	0	0	0	0	0	0	0
Reset							

WiFi IDS Status		
Item	Value setting	Description
Authentication Frame	N/A	It displays the receiving Authentication Frame count.
Association Request Frame	N/A	It displays the receiving Association Request Frame count.
Re-association Request Frame	N/A	It displays the receiving Re-association Request Frame count.
Probe Request Frame	N/A	It displays the receiving Probe Request Frame count.
Disassociation Frame	N/A	It displays the receiving Disassociation Frame count.
Deauthentication Frame	N/A	It displays the receiving Deauthentication Frame count.
EAP Request Frame	N/A	It displays the receiving EAP Request Frame count.
Malicious Data Frame	N/A	It displays the number of receiving unauthorized wireless packets.
Action	N/A	Click the Reset button to clear the entire statistic and reset 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.

WiFi Traffic Statistics

The WiFi Traffic Statistic shows all the received and transmitted packets on each WiFi module.

WiFi Module One Traffic Statistics				
Op. Band	ID	Received Packets	Transmitted Packets	Action
2.4G	VAP-1	269	80	Reset
2.4G	VAP-2	26	8	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

WiFi Traffic Statistic		
Item	Value setting	Description
Op. Band	N/A	It displays the WiFi Operation Band (2.4G or 5G) of VAP.
ID	N/A	It displays the VAP ID.
Received Packets	N/A	It displays the number of received packets.
Transmitted Packet	N/A	It 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 entire VAP Traffic Statistic instantly.

7.2.4 DDNS Status

Go to **Status > Basic Network > DDNS** tab to access the DDNS Status information.

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. To configure DDNS, go to **Basic Network > DDNS**.

DDNS Status

DDNS Status List				
Host Name	Provider	Effective IP	Last Update Status	Last Update Time

DDNS Status		
Item	Value Setting	Description
Host Name	N/A	Displays the 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	Refresh the information.

7.3 Security

7.3.1 VPN Status

The VPN Status window 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 Edit ▲ ✕							
ID	Tunnel Name	Tunnel Scenario	Local Subnets	Remote IP/FQDN	Remote Subnets	Conn. Time	Status

IPSec Tunnel Status		
Item	Value setting	Description
Tunnel Name	N/A	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 Client Status Edit Detail ▲ ✕							
ID	OpenVPN Client Name	Interface	Remote IP/FQDN	Remote Subnet	Virtual IP	Conn. Time	Conn. Status

OpenVPN Server Status		
Item	Value setting	Description
User Name	N//	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

L2TP Client Status

Edit

ID	L2TP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Conn. Time	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 L2TP Server/Client Status shows the connection status of the established L2TP tunnels. To configure L2TP, go to **Security > VPN** and select the **L2TP** tab.

L2TP Server Status Edit							↑ ×
ID	User Name	Remote IP	Remote Virtual IP	Remote Call ID	Conn. Time	Status	

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 Edit								↑ ×
ID	L2TP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Conn. Time	Status	

L2TP Client Status		
Item	Value setting	Description
Client Name	N/A	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

Edit

ID	User Name	Remote IP	Remote Virtual IP	Conn. Time	Status
----	-----------	-----------	-------------------	------------	--------

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

Edit

ID	PPTP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Conn. Time	Status
----	------------------	-----------	------------	----------------	-------------------------------	------------	--------

PPTP Client Status

Item	Value setting	Description
Client Name	N/A	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).

7.3.2 Firewall Status

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

Click the icon [+] to display log history. Click the Edit button to display the configuration page.

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

Packet Filter Status

Packet Filters Edit			
Activated Filter Rule	Detected Contents	IP	Time

Packet Filter Status		
Item	Value setting	Description
Activated Filter Rule	N/A	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 Edit			
Activated Blocking Rule	Blocked URL	IP	Time

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

Edit

Activated Control Rule	Blocked MAC Addresses	IP	Time
------------------------	-----------------------	----	------

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 packets 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 Edit ▲ ✕		
Detected Intrusion	IP	Time
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

Options Edit			
Stealth Mode	SPI	Discard Ping from WAN	Remote Administrator Management
Disable	Disable	Disable	IP: 192.168.121.54, User Name: admin, Time: Apr 1 11:14:54

Firewall Options Status		
Item	Value setting	Description
Stealth Mode	N/A	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**).

7.4 Administration

7.4.1 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 Linking Status						
User Name	IP Address	Port	Community	Auth. Mode	Privacy Mode	SNMP Version

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		
Trap Level	Time	Trap Event

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

7.4.2 Log Storage Status

The **Log Storage Status** screen shows the information of device storage, such as the file system and data speed.

Go to **Status > Administration > Log Storage** to access the Log Storage page.

Log Storage Status

Storage Information  					
Device Select	Device Description	Usage	File System	Speed	Status

7.4.3 GNSS Status

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

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

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

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

7.5 Statistics & Report

7.5.1 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 (2 entries) Previous Next First Last Export (.xml) Export (.csv) Refresh							
User Name	Protocol	Internal IP & Port	MAC	NAT-host IP & Port	External IP & Port	Duration Time	State
	TCP	192.168.123.173:51464			192.168.123.254:80	2020/10/29 03:57~	
	UDP	192.168.123.173:68			192.168.123.254:67	2020/10/29 03:57~	

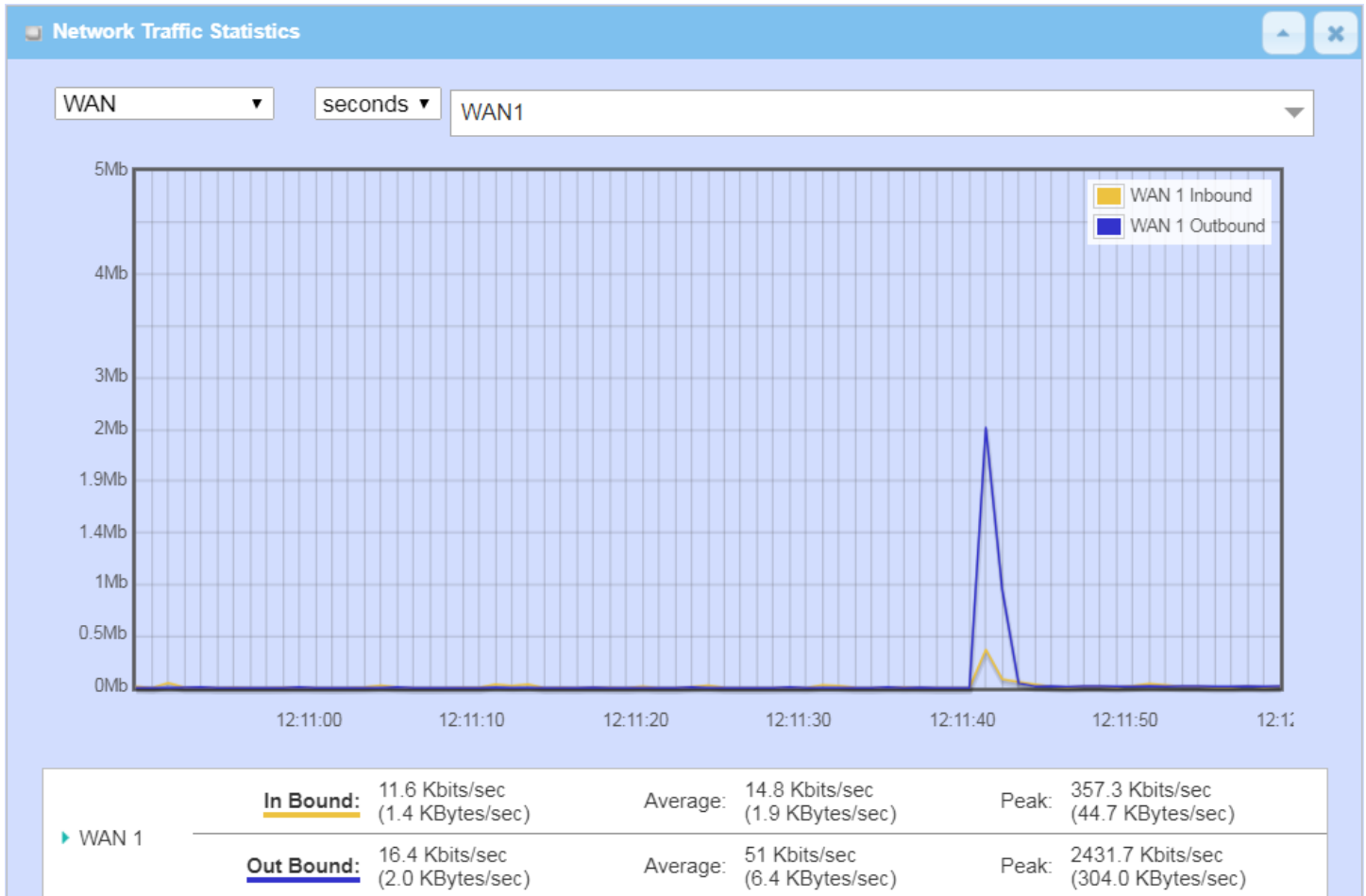
Connection Session List		
Item	Value setting	Description
Previous	N/A	Click Previous to view the previous page of the connection history.
Next	N/A	Click Next to view the next page of the connection history.
First	N/A	Click First to view the first page of the connection history.
Last	N/A	Click Last to 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.

7.5.2 Network Traffic

The 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 (seconds, minutes, or hours).



7.5.3 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.

Device Manager Login Statistics					
Previous Next First Last Export (.xml) Export (.csv) Refresh					
User Name	Protocol Type	IP Address	Info	Duration Time	
admin	HTTP	192.168.0.160	Admin	2023/05/07 04:08~	
admin	HTTP	192.168.0.160	Admin	2023/05/07 06:17~	
admin	HTTP	192.168.0.160	Admin	2023/05/07 06:49~	
admin	HTTP	192.168.0.160	Admin	2023/05/05 07:43~	
admin	HTTP	192.168.0.160	Admin	2023/05/05 07:52~	
admin	HTTP	192.168.0.160	Admin	2023/05/05 09:01~	
admin	HTTP	192.168.0.160	Admin	2023/05/05 11:18~	
admin	HTTP	192.168.0.160	Admin	2023/05/05 11:42~	
admin	HTTP	192.168.0.160	Admin	2023/05/05 13:47~	
admin	HTTP	192.168.0.160	Admin	2023/05/05 14:21~	

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.

7.5.4 Cellular Usage

The Cellular Usage screen shows statistics of cellular data usage. The cellular data usage can be presented by hour or by day.

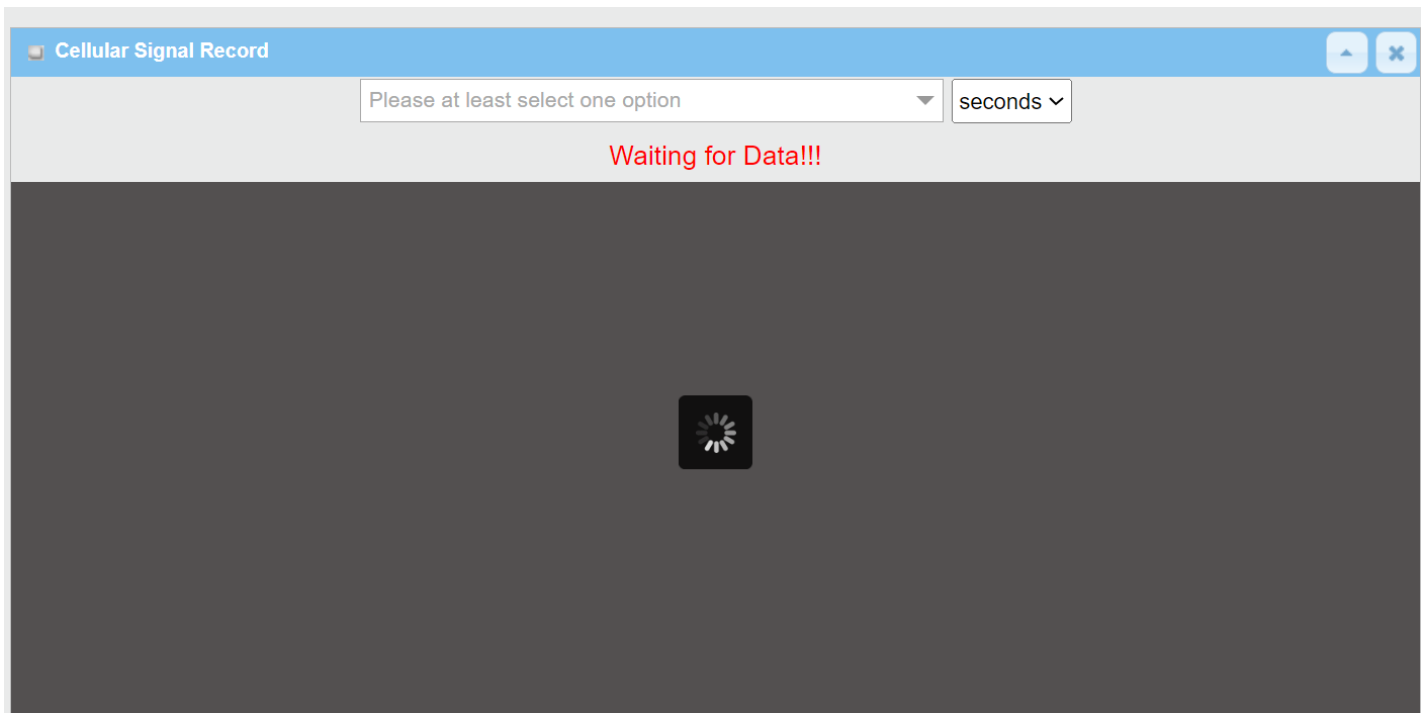
Go to Status > Statistics & Reports > Cellular Usage to access the Cellular Usage page.



7.5.5 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.



Appendix A GPL WRITTEN OFFER

This product incorporates open source software components covered by the terms of third party copyright notices and license agreements contained below.

GPSTBabel

Version 1.4.4

Copyright (C) 2002-2005 Robert Lipe<robertlipe@usa.net>

GPL License: <https://www.gpsbabel.org/>

Curl

Version 7.19.6

Copyright (c) 1996-2009, Daniel Stenberg, <daniel@haxx.se>.

MIT/X derivate License: <https://curl.haxx.se/>

OpenSSL

Version 1.0.2m

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

GPL License: <https://www.openssl.org/>

brctl - ethernet bridge administration

Stephen Hemminger <shemminger@osdl.org>

Lennert Buytenhek <buytenh@gnu.org>

version 1.1

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

tc - show / manipulate traffic control settings

Stephen Hemminger<shemminger@osdl.org>

Alexey Kuznetsov<kuznet@ms2.inr.ac.ru>

version iproute2-ss050330

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

dhcp-fwd — starts the DHCP forwarding agent

Enrico Scholz <enrico.scholz@informatik.tu-chemnitz.de>

version 0.7

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

lftp - Sophisticated file transfer program

Alexander V. Lukyanov <lav@yars.free.net>

version:4.5.x

Copyright (c) 1996-2014 by Alexander V. Lukyanov (lav@yars.free.net)

dnsmasq - A lightweight DHCP and caching DNS server.

Simon Kelley <simon@thekelleys.org.uk>

version:2.72

dnsmasq is Copyright (c) 2000-2014 Simon Kelley

socat - Multipurpose relay

Version: 2.0.0-b8

GPLv2

<http://www.dest-unreach.org/socat/>

LibModbus

Version: 3.0.3

LGPL v2

<http://libmodbus.org/news/>

LibIEC60870

GPLv2

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

<https://sourceforge.net/projects/mrts/>

Openswan

Version: v2.6.38 GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

<https://www.openswan.org/>

Opennhp

Version: v0.14.1

OpenNHRP is an NHRP implementation for Linux. It has most of the RFC2332 and Cisco IOS extensions.

Project homepage: <http://sourceforge.net/projects/opennhp>

Git repository: <git://opennhp.git.sourceforge.net/gitroot/opennhp>

LICENSE

OpenNHRP is licensed under the MIT License. See MIT-LICENSE.txt for additional details.

OpenNHRP embeds libev. libev is dual licensed with 2-clause BSD and GPLv2+ licenses. See libev/LICENSE for additional details.

OpenNHRP links to c-ares. c-ares is licensed under the MIT License.

<https://sourceforge.net/projects/opennhp/>

IPSec-tools

Version: v0.8

No GPL be written

<http://ipsec-tools.sourceforge.net/>

PPTP

Version: pptp-1.7.1

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
<http://pptpclient.sourceforge.net/>

PPTPServ

Version: 1.3.4

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed. <http://poptop.sourceforge.net/>

L2TP

Version: 0.4

Copying All software included in this package is Copyright 2002 Roaring
Penguin Software Inc. You may distribute it under the terms of the
GNU General Public License (the "GPL"), Version 2, or (at your option)
any later version.
<http://www.roaringpenguin.com/>

L2TPServ

Version: v 1.3.1 GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
<http://www.xelerance.com/software/xl2tpd/>

Mpstat: from sysstat, system performance tools for Linux

Version: 10.1.6

Copyright: (C) 1999-2013 by Sebastien Godard (sysstat <at> orange.fr)

SSHD: dropbear, a SSH2 server

Version: 0.53.1

Copyright: (c) 2002-2008 Matt Johnston

Libncurses: The ncurses (new curses) library is a free software emulation of curses in System V Release 4.0 (SVr4), and more.

Version: 5.9

Copyright: (c) 1998,2000,2004,2005,2006,2008,2011,2015 Free Software Foundation, Inc., 51 Franklin Street, Boston, MA 02110-1301, USA

MiniUPnP: The miniUPnP daemon is an UPnP IGD (internet gateway device) which provide NAT traversal services to any UPnP enabled client on the network.

Version: 1.7

Copyright: (c) 2006-2011, Thomas BERNARD

CoovaChilli is an open-source software access controller for captive portal (UAM) and 802.1X access provisioning.

Version: 1.3.0

Copyright: (C) 2007-2012 David Bird (Coova Technologies) <support@coova.com>

Krb5: Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.

Version: 1.11.3

Copyright: (C) 1985-2013 by the Massachusetts Institute of Technology and its contributors

OpenLDAP: a suite of the Lightweight Directory Access Protocol (v3) servers, clients, utilities, and development tools.

Version: 2.4

Copyright: 1998-2014 The OpenLDAP Foundation

Samba3311: the free SMB and CIFS client and server for UNIX and other operating systems

Version: 3.3.11

Copyright: (C) 2007 Free Software Foundation, Inc. <<http://fsf.org/>>

NTPClient: an NTP (RFC-1305, RFC-4330) client for unix-alike computers

Version: 2007_365

Copyright: 1997, 1999, 2000, 2003, 2006, 2007 Larry Doolittle

exFAT: FUSE-based exFAT implementation

Version: 0.9.8

Copyright: (C) 2010-2012 Andrew Nayenko

NTFS_3G: The NTFS-3G driver is an open source, freely available read/write NTFS driver for Linux, FreeBSD, Mac OS X, NetBSD, Solaris and Haiku.

Version: 2009.4.4

Copyright: (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

mysql-5_1_72: a release of MySQL, a dual-license SQL database server

Version: 5.1.72

Copyright: (c) 2000, 2013, Oracle and/or its affiliates

FreeRadius: a high performance and highly configurable RADIUS server

Version: 2.1.12

Copyright: (C) 1999-2011 The FreeRADIUS server project and contributors

Linux IPv6 Router Advertisement Daemon – radvd

Version: V 1.15

Copyright (c) 1996,1997 by Lars Fenneberg<lf@elemental.net>

BSD License: <http://www.litech.org/radvd/>

WIDE-DHCPv6

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) clients, servers, and relay agents.

Version: 20080615

Copyright (C) 1998-2004 WIDE Project.

BSD License: <https://sourceforge.net/projects/wide-dhcpv6/>

Python version 2.7.12

This Python distribution contains no GNU General Public Licensed (GPLed) code so it may be used in proprietary projects just like prior Python distributions. There are interfaces to some GNU code but these are entirely optional

OpenPAM Radula

This software was developed for the FreeBSD Project by ThinkSec AS and Network Associates Laboratories, the Security Research Division of Network Associates, Inc. under DARPA/SPAWAR contract N66001-01-C-8035 ("CBOSS"), as part of the DARPA CHATS research program.

ISC DHCP Version 4.3.5

Copyright (c) 2004-2016 by Internet Systems Consortium, Inc. ("ISC")