M2M LTE Gateway with serial Port

M2M L28

User Manual

M2M LTE Gateway with serial port

Chapter 1 Introduction

1.1 Introduction

Congratulations on your purchase of this outstanding product: M2M Cellular Gateway. For M2M (Machine-to-Machine) applications, AirLive M2M Cellular Gateway is absolutely the right choice. With built-in world-class 3G/4G module, you just need to insert SIM card from local mobile carrier to get to Internet. The redundant SIM design provides a more reliable WAN connection for critical applications. By VPN tunneling technology, remote sites easily become a part of Intranet, and all data are transmitted in a secure (256-bit AES encryption) link. To meet a variety of M2M application requirements, AirLive M2M Cellular Gateway products are based on modular design.

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

Main Features:

- Provide various and configurable WAN connection.
- Support dual SIMs for the redundant wireless WAN connection.
- Provide Ethernet ports for comprehensive LAN connection and LAN-1 port can be configured to be another WAN interface.
- Feature with VPN and NAT firewall to have powerful security.
- Support the robust remote or local management to monitor network.
- Designed by solid and easy-to-mount metal body for business and IOT environment to work with a variety M2M (Machine-to-Machine) applications.

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

1.2 Contents List

1.2.1 Package Contents

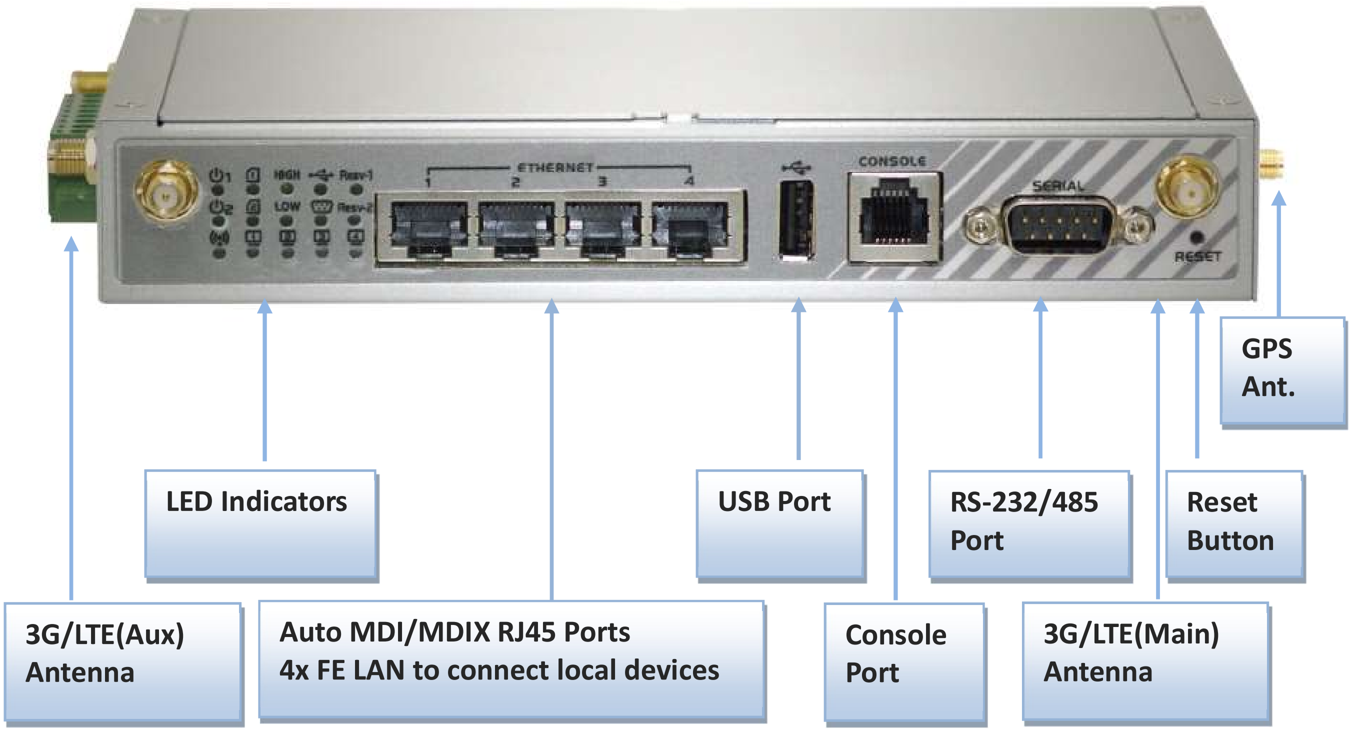
#Standard Package

Items	Description	Contents	Quantity
1	M2M L28 **M2M Cellular Gateway**		1pcs
2	**Cellular Antenna**		2pcs
3	**WiFi Antenna**		2pcs
4	**Power Adapter** **(DC 12V/2A)** (*[1])		1pcs
5	**RJ45 Cable**		1pcs
6	**Console Cable**		1pcs
7	**CD** **(Manual)**		1pcs
8	**Mounting Bracket**		2pcs
9	**DIN-Rail Bracket**		1pcs

[1] The maximum power consumption of M2M L28 1 is 15.5W.

1.3 Hardware Configuration

➢ Front View



※ **Reset Button**

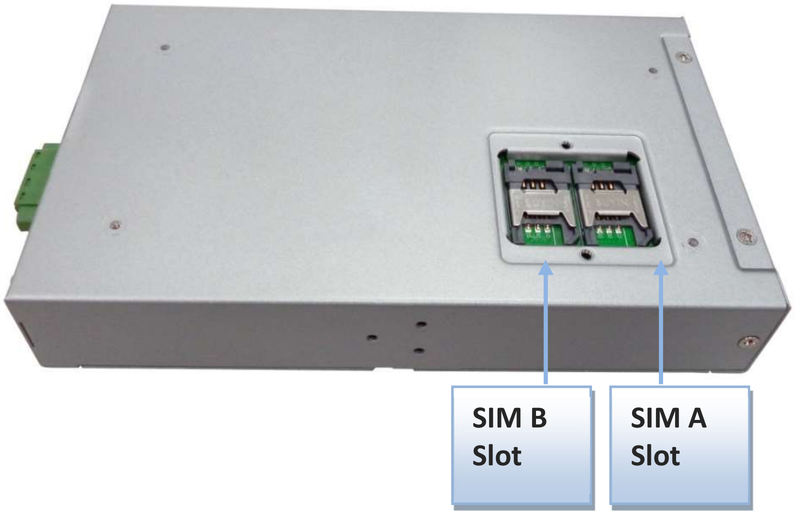
The RESET button provides user with a quick and easy way to resort the default setting. Press the RESET button continuously for 6 seconds, and then release it. The device will restore to factory default settings.

※ **GPS Antenna**

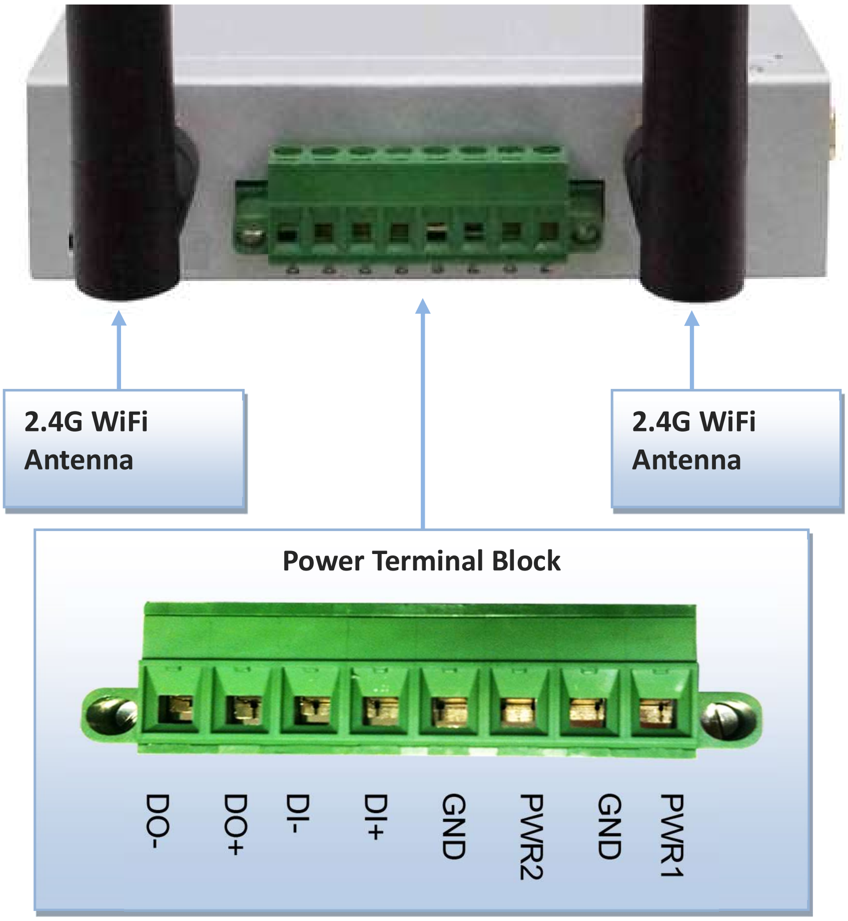
The GPS Antenna is an optional accessory, not included in the standard package. If you intend to use the provided GNSS function, please purchase additional passive-type GPS antenna and install it to the corresponding SMA connector in advance.

M2M LTE Gateway with serial port

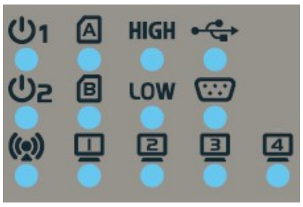
- Bottom View



- Left View



1.4 LED Indication



LED Icon	Indication	LED Color	Description
⏻1	Power Source 1	Green	**Steady ON:** Device is powered on by power source 1
⏻2	Power Source 2 (*[2])	Green	**Steady ON:** Device is powered on by power source 2
((•))	WLAN (WiFi)	Green	**Steady ON:** Wireless radio is enabled **Flash:** Data packets are transferred **OFF:** Wireless radio is disabled
A	SIM A	Green	**Steady ON:** SIM card A is used
B	SIM B	Green	**Steady ON:** SIM card B is used
1 ~ 4	LAN 1 ~ LAN 4	Green	**Steady ON:** Ethernet connection of LAN is established **Flash:** Data packets are transferred
HIGH	High 3G/LTE Signal	Green	**Steady ON:** The signal strength of 3G/LTE is strong
LOW	Low 3G/LTE Signal	Green	**Steady ON:** The signal strength of 3G/LTE is weak
	USB	Green	**Steady ON:** If USB device is attached
	Serial Port	Green	**Steady ON:** If serial device is attached

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

1.5 Installation & Maintenance Notice

1.5.1 SYSTEM REQUIREMENTS

Network Requirements	• An Ethernet RJ45 cable or DSL modem • 3G/4G cellular service subscription • IEEE 802.11n or 802.11b/ g wireless clients • 10/100 Ethernet adapter on PC
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 6.0 or higher • Chrome 2.0 or higher • Firefox 3.0 or higher • Safari 3.0 or higher

1.5.2 WARNING

Attention

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

1.5.3 HOT SURFACE CAUTION

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

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

1.6 Hardware Installation

This chapter describes how to install and configure the hardware

1.6.1 Mount the Unit

The M2M series products can be mounted on a wall, horizontal plane, or DIN Rail in a cabinet with the mounting accessories (brackets or DIN-rail kit). The mounting accessories are not screwed on the product when out of factory. Please screw the wall-mount kits or DIN-rail bracket on the product first.

1.6.2 Insert the SIM Card

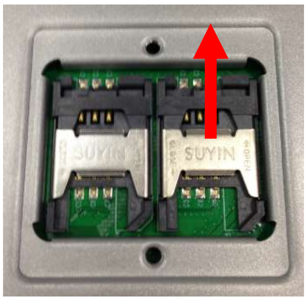
WARNING: BEFORE INSERTING OR CHANGING THE SIM CARD, PLEASE MAKE SURE THAT POWER OF THE DEVICE IS SWITCHED OFF.

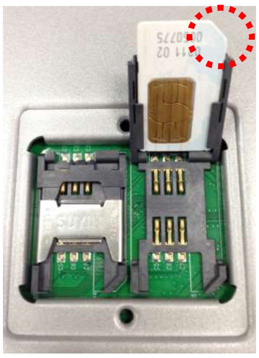
The SIM card slots are located at the bottom side of M2M housing. You need to unscrew and remove the outer SIM card cover before installing or removing the SIM card. Please follow the instructions to insert a SIM card. After SIM card is well placed, screw back the outer SIM card cover.

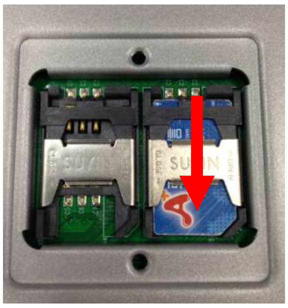
Step 1:
Follow red arrow to unlock SIM socket

Step 2:
Lift up SIM holder, and insert SIM card

Step 3:
Put back SIM holder, and follow red arrow to lock SIM socket

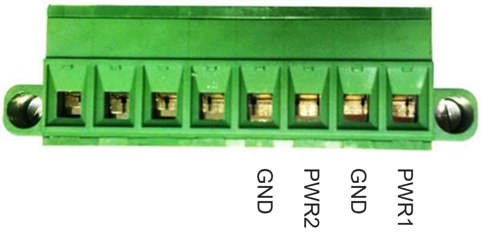




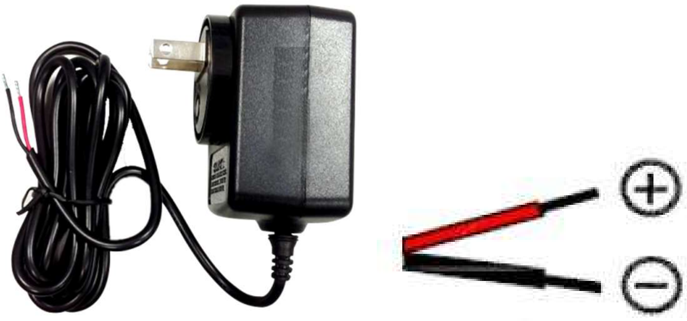


1.6.3 Connecting Power

The M2M L28 can be powered by connecting a power source to the terminal block . **It supports dual 9 to 48VDC power inputs**. Following picture is the power terminal block pin assignments. Please check carefully and connect to the right power requirements and polarity.



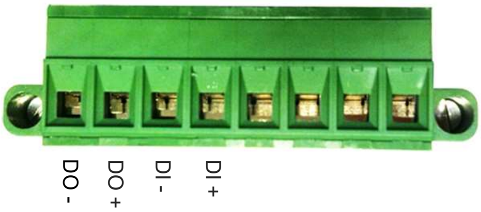
There are a DC converter and a DC12V/2A power adapter[3] in the package for you to easily connect DC power adapter to this terminal block.



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

1.6.4 Connecting DI/DO Devices

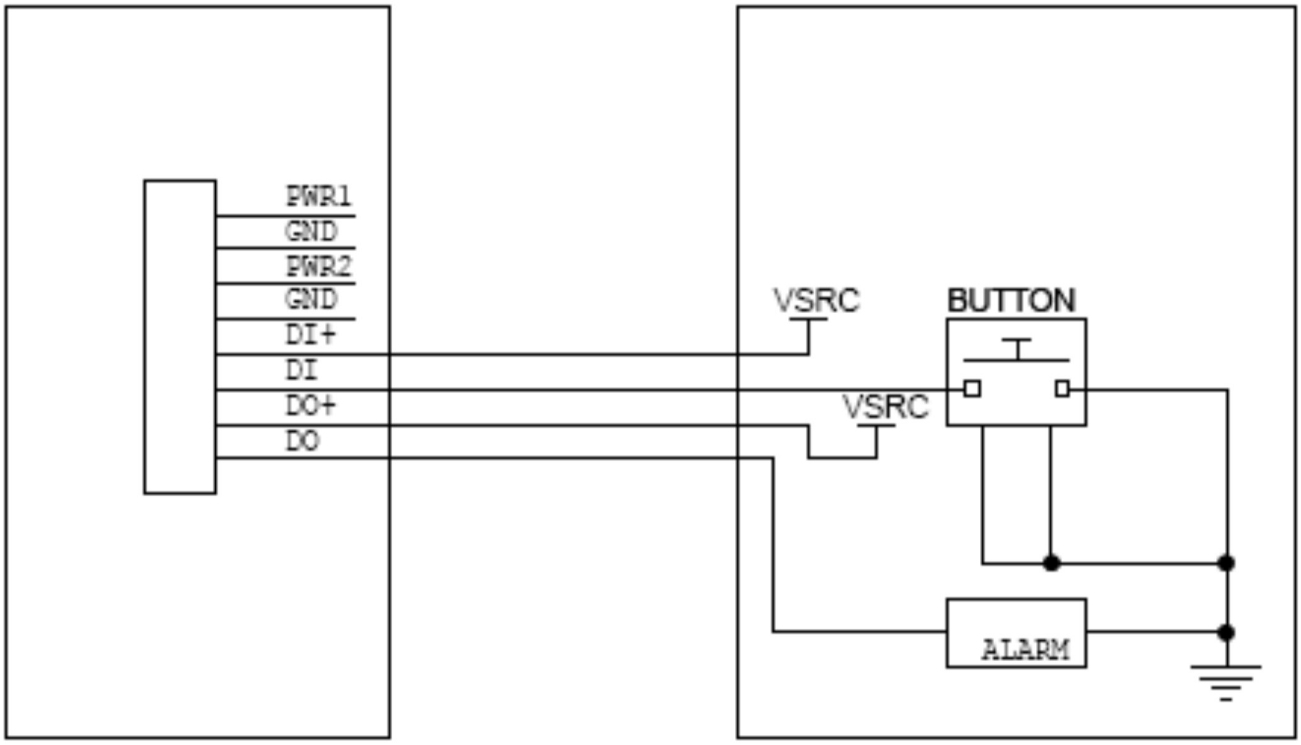
There are a DI and a DO ports together with power terminal block. Please refer to following specification to connect DI and DO devices.



[3] The maximum power consumption of M2M L28 is 15.5W.

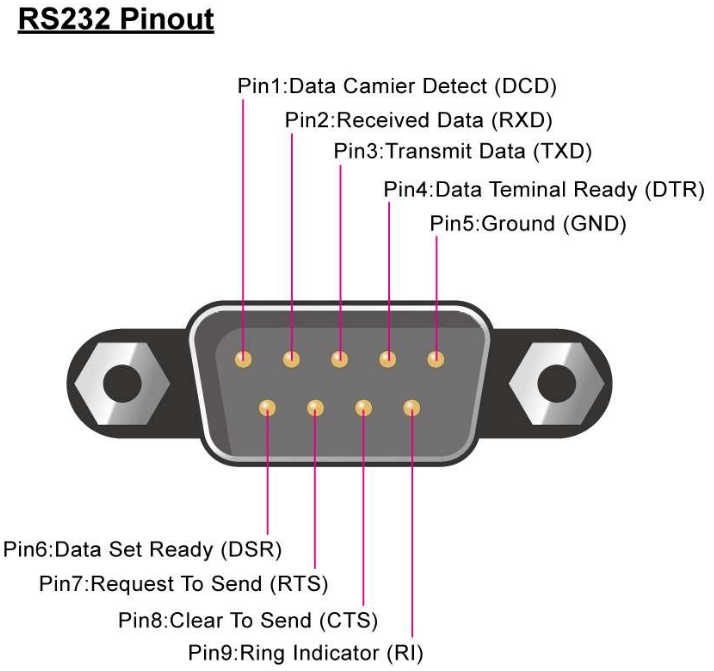
Mode	Specification	
Digital Input	Trigger Voltage (high)	Logic level 1: 5V~30V
	Normal Voltage (low)	Logic level 0: 0V~2.0V
Digital Output	Voltage (Relay Mode)	Depends on external device maximum voltage is 30V
	Maximum Current	1A

Example of Connection Diagram



1.6.5 Connecting Serial Devices

The M2M provides one standard serial port DB-9 male connector. Connect the serial device to the unit DB-9 male port with the right pin assignments of RS-232/485 are shown as below.



	Pin1	Pin2	Pin3	Pin4	Pin5	Pin6	Pin7	Pin8	Pin9
RS-232	DCD	RXD	TXD	DTR	GND	DSR	RTS	CTS	RI
RS-485			DATA+	DATA-	GND				

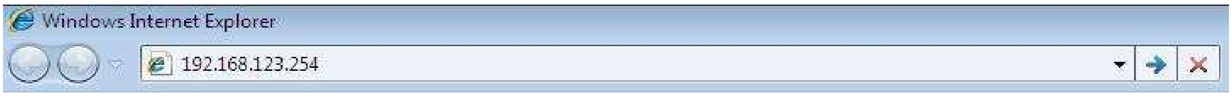
1.6.6 Connecting to the Network or a Host

The M2M series provides four RJ45 ports to connect 10/100Mbps Ethernet. It can auto detect the transmission speed on the network and configure itself automatically. Connect the Ethernet cable to the RJ45 ports of the device. Plug one end of an Ethernet cable into your computer’s network port and the other end into one of M2M series for LAN ports on the front panel. If you need to configure or troubleshoot the device, you may need to connect the M2M series directly to the host PC. In this way, you can also use the RJ45 Ethernet cable to connect the M2M series to the host PC’s Ethernet port.

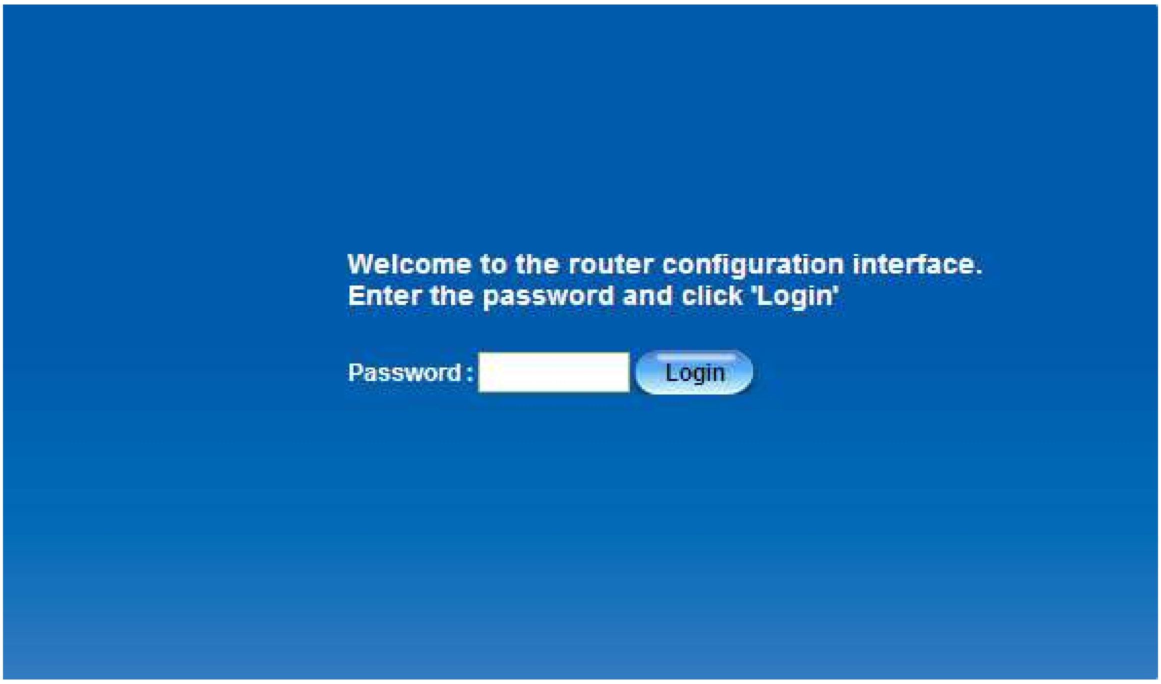
1.6.5 Setup by Configuring WEB UI

You can browse web UI to configure the device.

Type in the IP Address (**http://192.168.123.254**) [4]



When you see the login page, enter the password **'admin'** [5] and then click **'Login'** button.

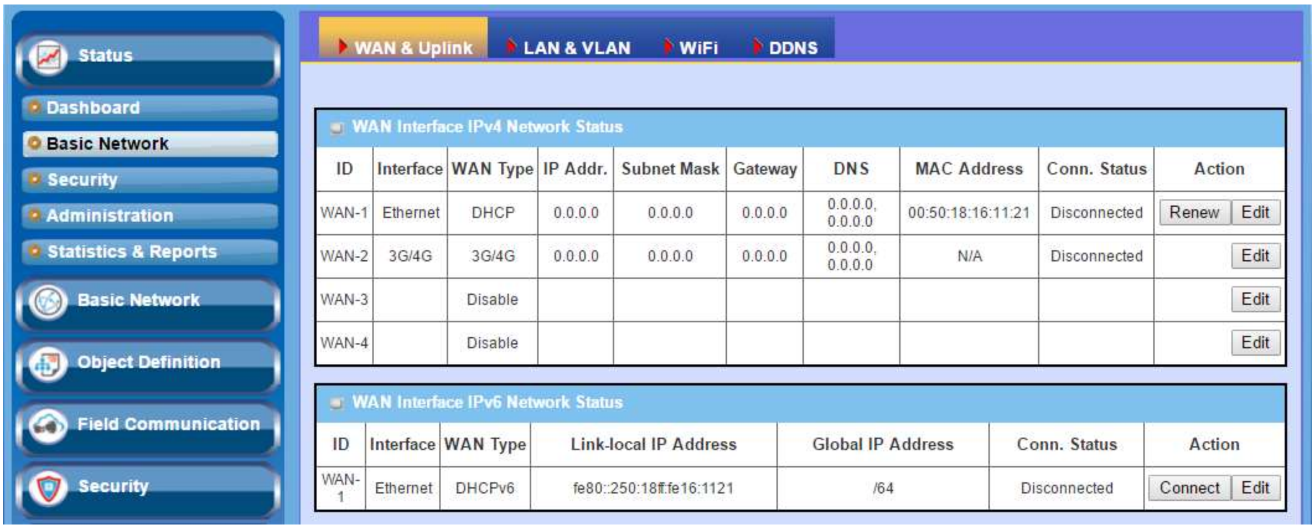

Welcome to the router configuration interface.
Enter the password and click 'Login'

[4] The default LAN IP address of this gateway is 192.168.123.254. If you change it, you need to type the new IP address

[5] It's strongly recommending you to change this login password from default value

Chapter 2 Status

2.3 Basic Network



WAN Interface IPv4 Network Status

ID	Interface	WAN Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Action
WAN-1	Ethernet	DHCP	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	00:50:18:16:11:21	Disconnected	Renew Edit
WAN-2	3G/4G	3G/4G	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	N/A	Disconnected	Edit
WAN-3		Disable							Edit
WAN-4		Disable							Edit

WAN Interface IPv6 Network Status

ID	Interface	WAN Type	Link-local IP Address	Global IP Address	Conn. Status	Action
WAN-1	Ethernet	DHCPv6	fe80::250:18ff:fe16:1121	/64	Disconnected	Connect Edit

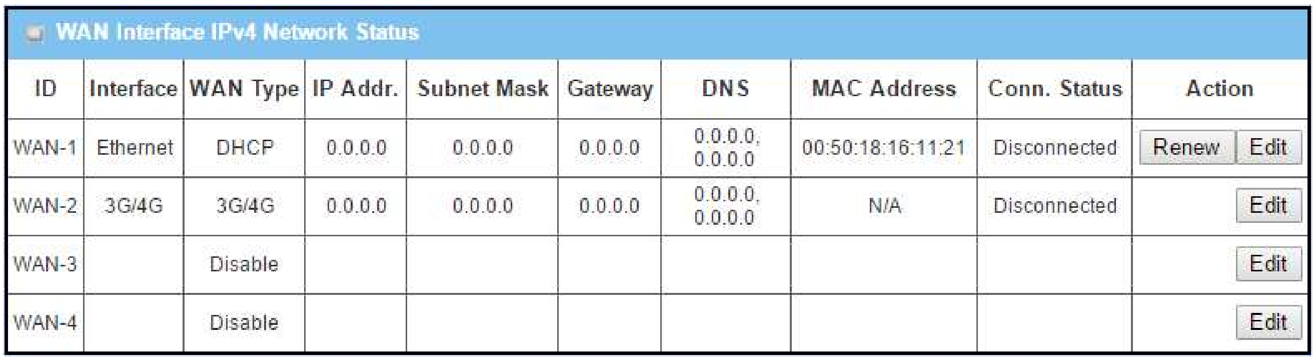
2.3.1 WAN & Uplink Status

The **WAN & Uplink Status** window shows the current status for different network type, including network configuration, connecting information, modem status and traffic statistics.

From the menu on the left, select **Status > Basic Network > WAN & Uplink Status**

WAN interface IPv4 Network Status

WAN interface IPv4 Network Status screen shows status information for IPv4 network.



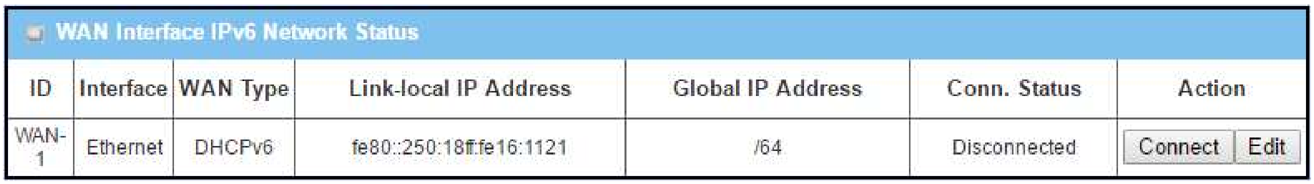
WAN Interface IPv4 Network Status

ID	Interface	WAN Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Action
WAN-1	Ethernet	DHCP	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	00:50:18:16:11:21	Disconnected	Renew Edit
WAN-2	3G/4G	3G/4G	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	N/A	Disconnected	Edit
WAN-3		Disable							Edit
WAN-4		Disable							Edit

WAN interface IPv4 Network Status		
Item	Value setting	Description
ID	N/A	It displays corresponding WAN interface WAN IDs.
Interface	N/A	It displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, 3G/4G, USB 3G/4G.
WAN Type	N/A	It displays the method which public IP address is obtained from your ISP. Depending on the model purchased, it can be Static IP, Dynamic IP, PPPoE, PPTP, L2TP, 3G/4G.
IP Addr.	N/A	It displays the public IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left un-configured.
Subnet Mask	N/A	It displays the Subnet Mask for public IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left un-configured.
Gateway	N/A	It displays the Gateway IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left un-configured.
DNS	N/A	It displays the IP address of DNS server obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left un-configured.
MAC Address	N/A	It displays the MAC Address for your ISP to allow you for Internet access. Note: Not all ISP may require this field.
Conn. Status	N/A	It displays the connection status of the device to your ISP. Status are Connected or disconnected.
Action	N/A	This area provides functional buttons. **Renew** button allows user to force the device to request an IP address from the DHCP server. Note: **Renew** button is available when DHCP WAN Type is used and WAN connection is disconnected. **Release** button allows user to force the device to clear its IP address setting to disconnect from DHCP server. Note: **Release** button is available when DHCP WAN Type is used and WAN connection is connected. **Connect** button allows user to manually connect the device to the Internet. Note: Connect button is available when Connection Control in WAN Type setting is set to Connect Manually (Refer to **Edit** button in **Basic Network > WAN & Uplink > Internet Setup**) and WAN connection status is disconnected. **Disconnect** button allows user to manually disconnect the device from the Internet. Note: **Connect** button is available when Connection Control in WAN Type setting is set to Connect Manually (Refer to **Edit** button in **Basic Network > WAN & Uplink > Internet Setup**) and WAN connection status is connected.

WAN interface IPv6 Network Status

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



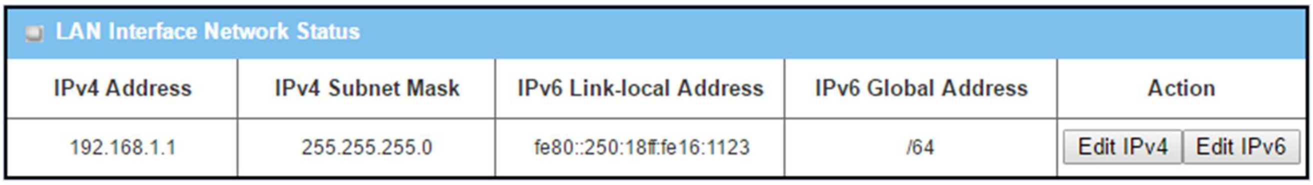
WAN Interface IPv6 Network Status

ID	Interface	WAN Type	Link-local IP Address	Global IP Address	Conn. Status	Action
WAN-1	Ethernet	DHCPv6	fe80::250:18ff:fe16:1121	/64	Disconnected	Connect Edit

WAN interface IPv6 Network Status		
Item	**Value setting**	**Description**
ID	N/A	It displays corresponding WAN interface WAN IDs.
Interface	N/A	It displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, 3G/4G, USB 3G/4G.
WAN Type	N/A	It displays the method which public IP address is obtained from your ISP. WAN type setting can be changed from **Basic Network > IPv6 > Configuration**.
Link-local IP Address	N/A	It displays the LAN IPv6 Link-Local address.
Global IP Address	N/A	It displays the IPv6 global IP address assigned by your ISP for your Internet connection.
Conn. Status	N/A	It displays the connection status. The status can be connected, disconnected and connecting.
Action	N/A	This area provides functional buttons. **Edit Button** when pressed, web-based utility will take you to the IPv6 configuration page. (**Basic Network > IPv6 > Configuration**.)

LAN Interface Network Status

LAN Interface Network Status screen shows IPv4 and IPv6 information of LAN network.



LAN Interface Network Status

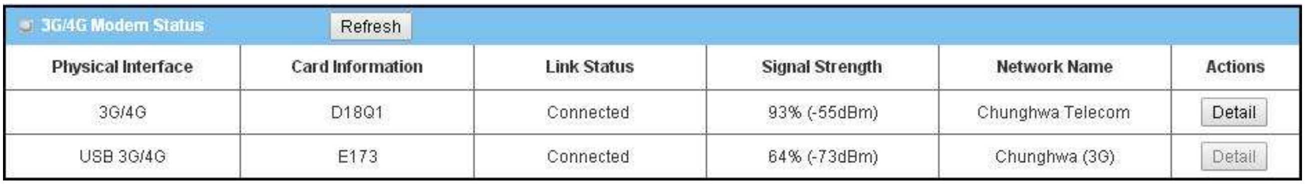
IPv4 Address	IPv4 Subnet Mask	IPv6 Link-local Address	IPv6 Global Address	Action
192.168.1.1	255.255.255.0	fe80::250:18ff:fe16:1123	/64	Edit IPv4 Edit IPv6

LAN Interface Network Status		
Item	**Value setting**	**Description**
IPv4 Address	N/A	It displays the current IPv4 IP Address of the gateway This is also the IP Address user use to access Router’s Web-based Utility.
IPv4 Subnet Mask	N/A	It displays the current mask of the subnet.
IPv6 Link-local	N/A	It displays the current LAN IPv6 Link-Local address.

Address		This is also the IPv6 IP Address user use to access Router's Web-based Utility.
IPv6 Global Address	N/A	It displays the current IPv6 global IP address assigned by your ISP for your Internet connection.
Action	N/A	This area provides functional buttons. **Edit IPv4 Button** when press, web-based utility will take you to the Ethernet LAN configuration page. (**Basic Network > LAN & VLAN > Ethernet LAN** tab). **Edit IPv6 Button** when press, web-based utility will take you to the IPv6 configuration page. (**Basic Network > IPv6 > Configuration**.)

3G/4G Modem Status

3G/4G Modem Status screen shows status information for 3G/4G WAN network.

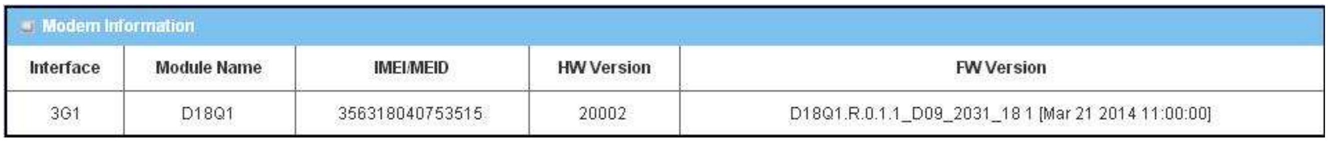


Physical Interface	Card Information	Link Status	Signal Strength	Network Name	Actions
3G/4G	D18Q1	Connected	93% (-55dBm)	Chunghwa Telecom	Detail
USB 3G/4G	E173	Connected	64% (-73dBm)	Chunghwa (3G)	Detail

3G/4G Modem Status		
Item	**Value setting**	**Description**
Physical Interface	N/A	It displays the type of WAN physical interface. Depending on the model you purchased, it can be 3G/4G and USB 3G/4G. Note: Some device model may support two 3G/4G modules. Their physical interface name will be **3G/4G-1** and **3G/4G-2**.
Card Information	N/A	It displays the vendor's 3G/4G modem model name.
Link Status	N/A	It displays the 3G/4G connection status. The status can be Connecting, Connected, Disconnecting, and Disconnected.
Signal Strength	N/A	It displays the 3G/4G wireless signal level.
Network Name	N/A	It displays the name of the service network carrier.
Refresh	N/A	Click the **Refresh** button to renew the information.
Action	N/A	This area provides functional buttons. **Detail Button** when press, windows of detail information will appear. They are the Modem Information, SIM Status, and Service Information. Refer to next page for more. Note: Currently USB 3G/4G doesn't support this feature.

When the **Detail** button is pressed, 3G/4G modem information windows such as Modem Information, SIM Status, and Service Information will appear. These windows are explained below.

Modem Information (Detail Button)

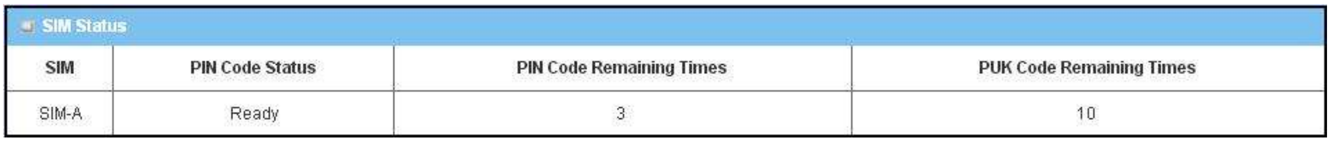


Modem Information

Interface	Module Name	IMEI/MEID	HW Version	FW Version
3G1	D18Q1	356318040753515	20002	D18Q1.R.0.1.1_D09_2031_18 1 [Mar 21 2014 11:00:00]

Modem Information (after Detail button)		
Item	**Value setting**	**Description**
Interface	N/A	It displays the type of WAN physical interface.
Module Name	N/A	It displays the vendor's 3G/4G modem model name.
IMEI/MEID	N/A	It displays the device IMEI code of the module.
HW Version	N/A	It displays the hardware version of the 3G/4G module.
FW Version	N/A	It displays the firmware version of the 3G/4G module.

SIM Status



SIM Status

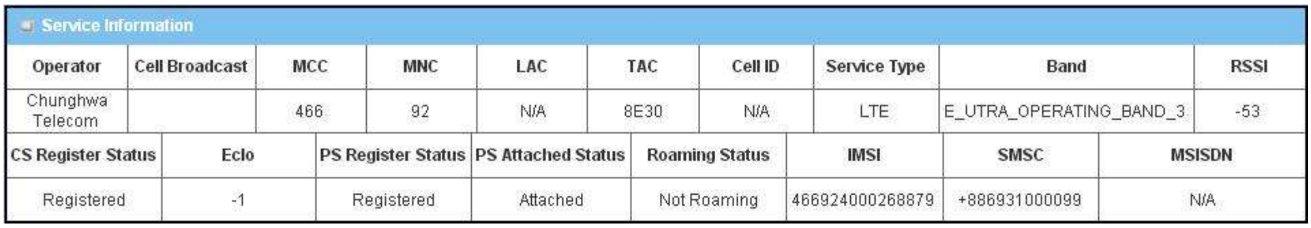
SIM	PIN Code Status	PIN Code Remaining Times	PUK Code Remaining Times
SIM-A	Ready	3	10

SIM Status (after Detail button)		
Item	**Value setting**	**Description**
SIM	N/A	It displays the operating SIM card. The display can be SIM-A or SIM-B. Note: Some device just supports one SIM slot and only SIM-A is available.
PIN Code Status	N/A	It displays the status of whether the SIM is required to be unlocked and absent of SIM card. The display can be Ready, SIM card not inserted, incorrect PIN code, PIN is required, Blocked. **Ready*** the PIN code is entered correctly and the SIM is unlocked. **SIM card not insert*** the SIM card is not detected. Check if SIM card is inserted properly. **PIN code incorrect*** the PIN code entered is incorrect. **PIN is required*** the PIN code is required to unlock the SIM card. **Blocked*** the SIM card is locked and need PUK code to unlock. It is probably due to the device had exceeded the allowed number of times to unlock. Refer to **PIN Code Remaining Times**
PIN Code Remaining	N/A	This displays the remaining time of the counter that you are allowed to try to unlock SIM card with the PIN code*. Once the number of unlocking tries has

Times		been exhausted the counter will display zero then the SIM card is locked. You are not allowed to unlock with the PIN code and would need to enter the PUK code to unlock instead. Note: You will need to enquire the telecom carrier for the PUK code to unlock or further technical services.
PUK Code Remaining Times	N/A	This displays the remaining time of the counter that you are allowed to try to unlock SIM card with the PUK code*. Once the number of unlocking tries has been exhausted the counter will display zero then the SIM card is locked. Note: When the counter has reached zero, you will need to enquire the telecom carrier for further technical services.

*To enter or re-enter PIN code, please go to Basic Network > WAN & Uplink > Internet Setup > Connection with SIM-A Card.

Service Information



Service Information

Operator	Cell Broadcast	MCC	MNC	LAC	TAC	Cell ID	Service Type	Band	RSSI
Chunghwa Telecom		466	92	N/A	8E30	N/A	LTE	E_UTRA_OPERATING_BAND_3	-53

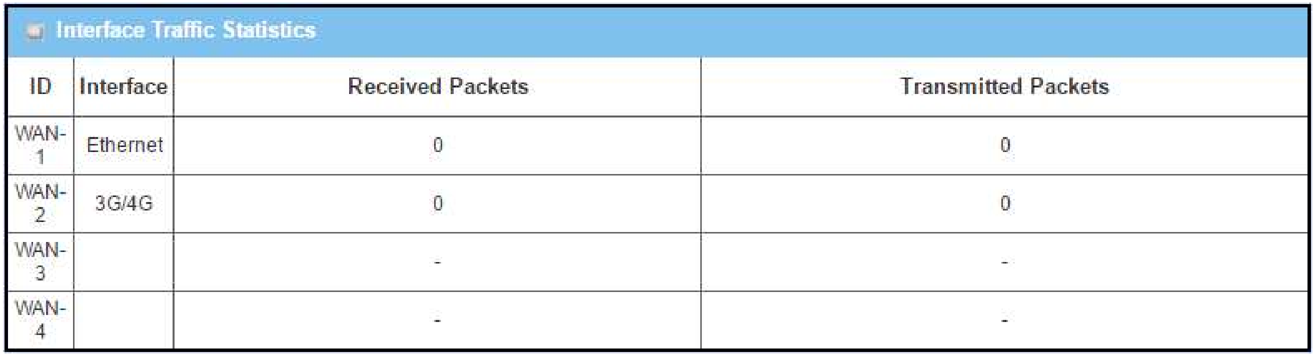
CS Register Status	Eclo	PS Register Status	PS Attached Status	Roaming Status	IMSI	SMSC	MSISDN
Registered	-1	Registered	Attached	Not Roaming	466924000268879	+886931000099	N/A

Service Information (after Detail button)		
Item	**Value setting**	**Description**
Operator	N/A	It displays the name of the carrier.
Cell Broadcast	N/A	It displays the cell messaging information. This is only available in GSM network and that your carrier provides this information.
MCC	N/A	It displays the MCC (Mobile Country Code) information that obtains from the current registered network.
MNC	N/A	It displays the MNC (Mobile Network Code) information that obtains from the current registered network.
LAC	N/A	It displays the LAC (Location Area Code) information in hexadecimal format, only available in GSM/UMTS networks.
TAC	N/A	It displays the TAC (Tracking Area Code) information in hexadecimal format, only available in LTE network.
Cell ID	N/A	It displays the Cell ID (CID) information in hexadecimal format.
Service Type	N/A	It displays the service type of the network that currently registered. It can be GSM, WCDMA or LTE.
Band	N/A	It displays the band currently used.
RSSI	N/A	It displays the RSSI (Received Signal Strength Indicator) in unit dBm of the signal.

CS Register Status	N/A	It displays the Circuit Switched (CS) registration status to the circuit domain service. The status can be Registered or Unregistered.
EcIo	N/A	It displays the Ec/Io information, the ratio of the signal to the interference. Note: the value is taken logarithmically and usually is negative.
PS Register Status	N/A	It displays the registration status to the packet domain service. The possible value will be Registered or Unregistered.
PS Attached Status	N/A	It shows the PS attached status. It can be Attached or Detached.
Roaming Status	N/A	It displays the registration status to the network, at roaming or at home network. It can be Roaming or Not Roaming.
IMSI	N/A	It displays the IMSI (International Mobile Subscriber Identity) information, which usually is composed of 15 digits.
SMSC	N/A	It displays the SMSC (Short Message Service Center) information, which is necessary for SMS service.
MSISDN	N/A	It displays the MSISDN (Mobile Station International Subscriber Directory Number) information. The information is available if the SIM card supports it.

Interface Traffic Statistics

Interface Traffic Statistics screen displays the Interface's total transmitted packets.



Interface Traffic Statistics

ID	Interface	Received Packets	Transmitted Packets
WAN-1	Ethernet	0	0
WAN-2	3G/4G	0	0
WAN-3		-	-
WAN-4		-	-

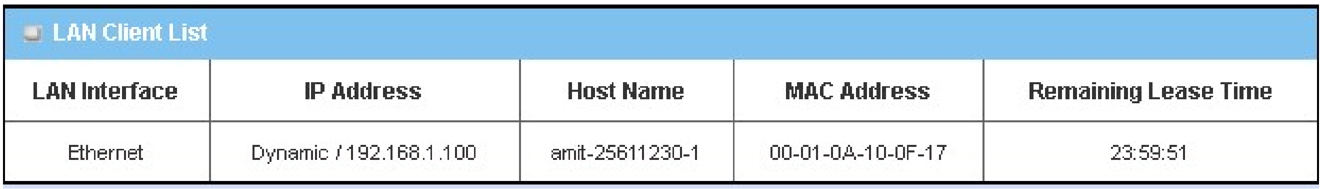
Interface Traffic Statistics		
Item	**Value setting**	**Description**
ID	N/A	It displays corresponding WAN interface WAN IDs.
Interface	N/A	It displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, 3G/4G, USB 3G/4G.
Received Packets	N/A	It displays the downstream packets. It is reset when the device is rebooted.
Transmitted Packets	N/A	It displays the upstream packets. It is reset when the device is rebooted.

2.3.3 LAN & VLAN Status

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

Client List

The **Client List** shows you the LAN Interface, IP address, Host Name, MAC Address, and Remaining Lease Time of each device that is connected to this router.



LAN Client List

LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time
Ethernet	Dynamic / 192.168.1.100	amit-25611230-1	00-01-0A-10-0F-17	23:59:51

LAN Client List

Item	Value setting	Description
LAN Interface	N/A	Client record of LAN Interface. String Format.
IP Address	N/A	Client record of IP Address Type and the IP Address. Type is String Format and the IP Address is IPv4 Format.
Host Name	N/A	Client record of Host Name. String Format.
MAC Address	N/A	Client record of MAC Address. MAC Address Format.
Remaining Lease Time	N/A	Client record of Remaining Lease Time. Time Format.

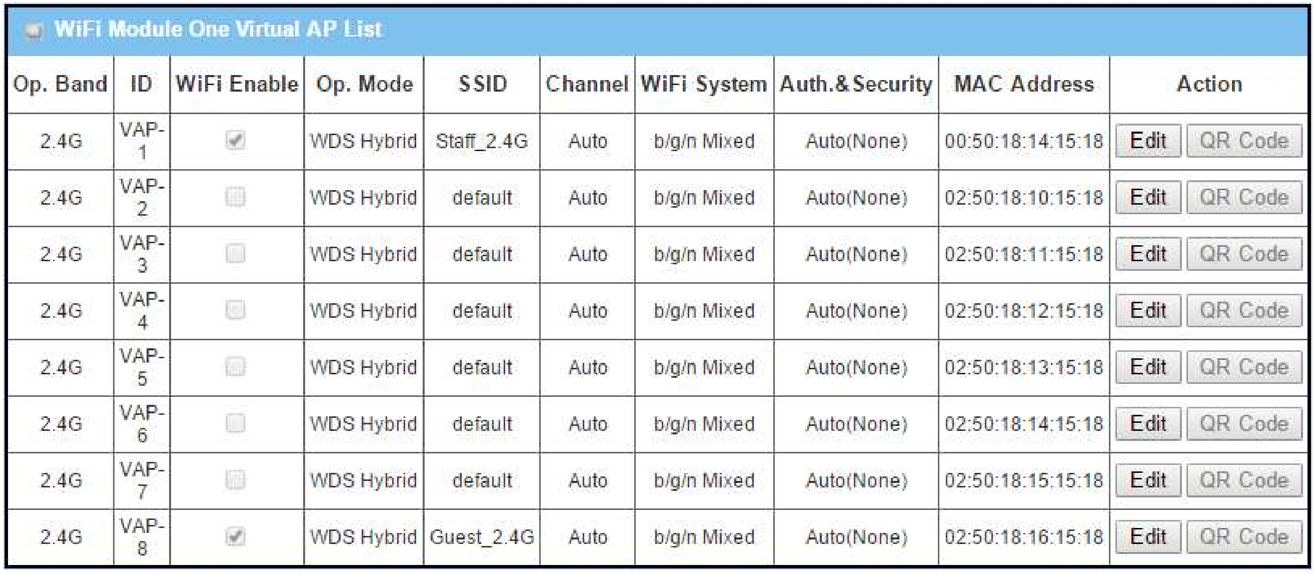
2.3.5 WiFi Status

The **WiFi Status** window shows the overall statistics of WiFi VAP entries.

Go to **Status > Basic Network > WiFi** tab.

WiFi Virtual AP List

The WiFi Virtual AP List shows all of the virtual AP information. The **Edit** button allows for quick configuration changes.



WiFi Module One Virtual AP List

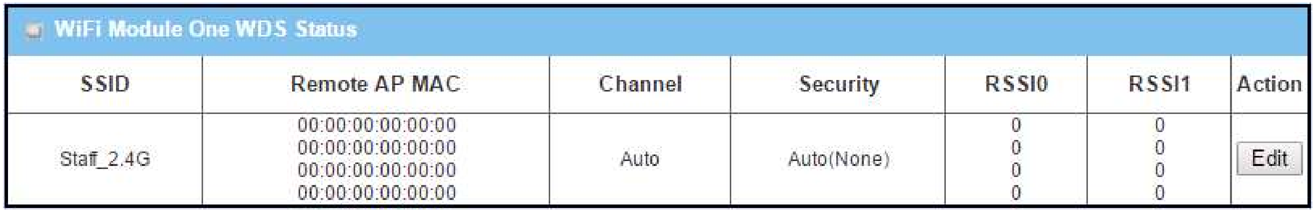
Op. Band	ID	WiFi Enable	Op. Mode	SSID	Channel	WiFi System	Auth.&Security	MAC Address	Action
2.4G	VAP-1	☑	WDS Hybrid	Staff_2.4G	Auto	b/g/n Mixed	Auto(None)	00:50:18:14:15:18	Edit QR Code
2.4G	VAP-2	□	WDS Hybrid	default	Auto	b/g/n Mixed	Auto(None)	02:50:18:10:15:18	Edit QR Code
2.4G	VAP-3	□	WDS Hybrid	default	Auto	b/g/n Mixed	Auto(None)	02:50:18:11:15:18	Edit QR Code
2.4G	VAP-4	□	WDS Hybrid	default	Auto	b/g/n Mixed	Auto(None)	02:50:18:12:15:18	Edit QR Code
2.4G	VAP-5	□	WDS Hybrid	default	Auto	b/g/n Mixed	Auto(None)	02:50:18:13:15:18	Edit QR Code
2.4G	VAP-6	□	WDS Hybrid	default	Auto	b/g/n Mixed	Auto(None)	02:50:18:14:15:18	Edit QR Code
2.4G	VAP-7	□	WDS Hybrid	default	Auto	b/g/n Mixed	Auto(None)	02:50:18:15:15:18	Edit QR Code
2.4G	VAP-8	☑	WDS Hybrid	Guest_2.4G	Auto	b/g/n Mixed	Auto(None)	02:50:18:16:15:18	Edit QR Code

WiFi Virtual AP List		
Item	**Value setting**	**Description**
Op. Band	N/A	It displays the Wi-Fi Operation Band (2.4G or 5G) of VAP.
ID	N/A	It displays the ID of VAP.
WiFi Enable	N/A	It displays whether the VAP wireless signal is enabled or disabled.
Op. Mode	N/A	The Wi-Fi Operation Mode of VAP. Depends of device model, modes are AP Router, WDS Only and WDS Hybrid, Universal Repeater and Client.
SSID	N/A	It displays the network ID of VAP.
Channel	N/A	It displays the wireless channel used.
WiFi System	N/A	The WiFi System of VAP.
Auth. & Security	N/A	It displays the authentication and encryption type used.
MAC Address	N/A	It displays MAC Address of VAP.
Action	N/A	Click the **Edit** button to make a quick access to the WiFi configuration page. (**Basic Network > WiFi > Configuration** tab)

		The **QR Code** button allow you to generate QR code for quick connect to the VAP by scanning the QR code.

WiFi WDS Status

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



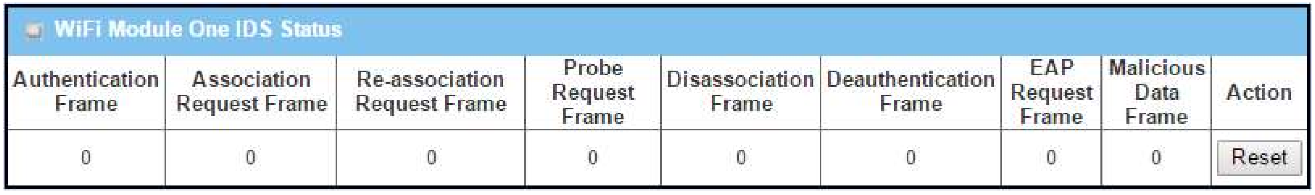
WiFi Module One WDS Status

SSID	Remote AP MAC	Channel	Security	RSSI0	RSSI1	Action
Staff_2.4G	00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00	Auto	Auto(None)	0 0 0 0	0 0 0 0	Edit

WiFi IDS Status Item	Value setting	Description
SSID	N/A	It displays the network ID of VAP.
Remote AP MAC	N/A	It displays the the Remote AP MAC list for the WDS peers.
Channel	N/A	It displays the wireless channel used.
Security	N/A	It displays the authentication and encryption setting for the WDS connection.
RSSI0, RSSI1	N/A	It displays the Rx sensitivity on each radio path..
Action	N/A	Click the **Edit** button to make a quick access to the WiFi configuration page. (**Basic Network > WiFi > Configuration** tab)

WiFi IDS Status

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



WiFi Module One IDS Status

Authentication Frame	Association Request Frame	Re-association Request Frame	Probe Request Frame	Disassociation Frame	Deauthentication Frame	EAP Request Frame	Malicious Data Frame	Action
0	0	0	0	0	0	0	0	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.

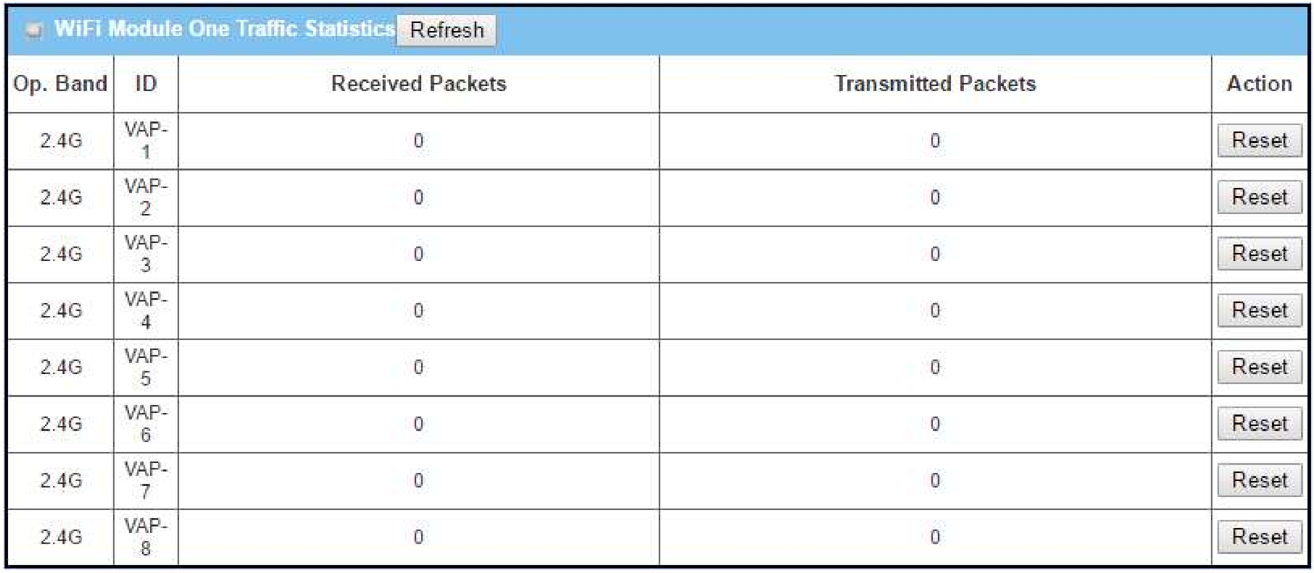
Ensure WIDS function is enabled

Go to Basic Network > WiFi > Advanced Configuration tab

Note that the WIDS of **2.4G** or **5G** should be configured **separately**.

WiFi Traffic Statistic

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



WiFi Module One Traffic Statistics Refresh

Op. Band	ID	Received Packets	Transmitted Packets	Action
2.4G	VAP-1	0	0	Reset
2.4G	VAP-2	0	0	Reset
2.4G	VAP-3	0	0	Reset
2.4G	VAP-4	0	0	Reset
2.4G	VAP-5	0	0	Reset
2.4G	VAP-6	0	0	Reset
2.4G	VAP-7	0	0	Reset
2.4G	VAP-8	0	0	Reset

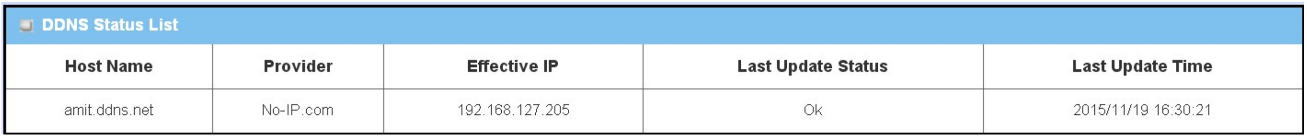
WiFi Traffic Statistic		
Item	Value setting	Description
Op. Band	N/A	It displays the Wi-Fi Operation Band (2.4G or 5G) of VAP.
ID	N/A	It displays the VAP ID.
Received Packets	N/A	It displays the number of reveived packets.
Transmitted Packet	N/A	It displays the number of transmitted packets.
Action	N/A	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.

2.3.7 DDNS Status

The **DDNS Status** window shows the current DDNS service in use, the last update status, and the last update time to the DDNS service server.

Go to **Status > Basic Network > DDNS.**

DDNS Status

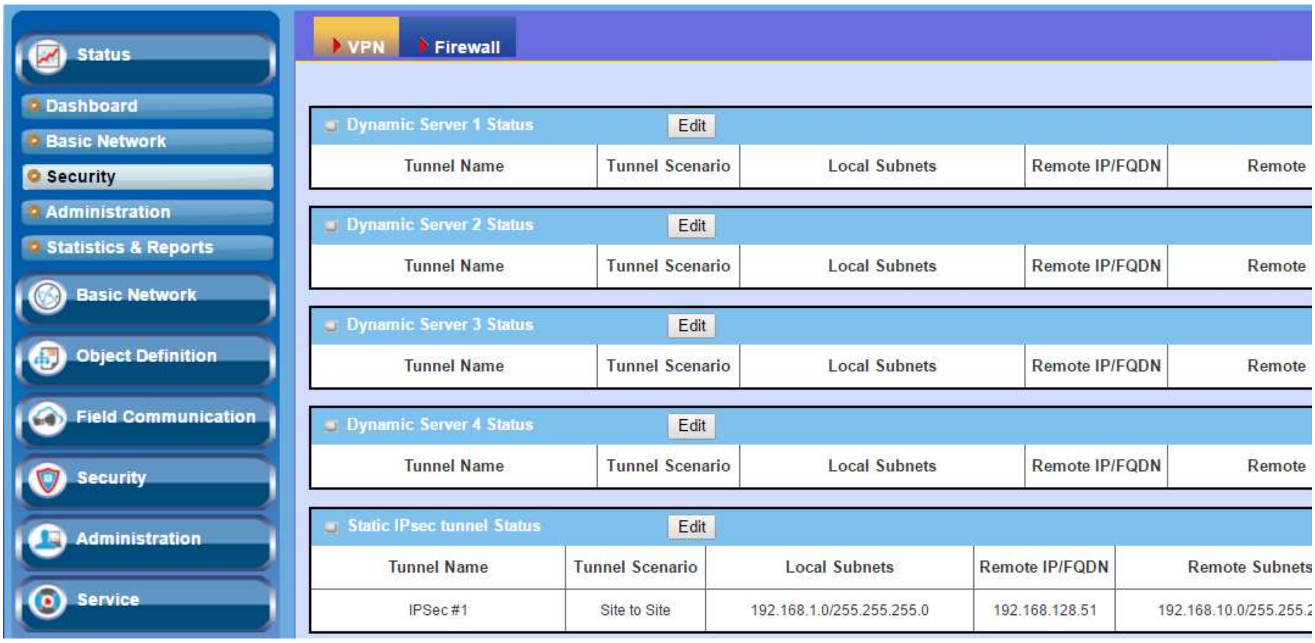


DDNS Status List

Host Name	Provider	Effective IP	Last Update Status	Last Update Time
amit.ddns.net	No-IP.com	192.168.127.205	Ok	2015/11/19 16:30:21

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

2.5 Security



Dynamic Server 1 Status

Tunnel Name	Tunnel Scenario	Local Subnets	Remote IP/FQDN	Remote

Dynamic Server 2 Status

Tunnel Name	Tunnel Scenario	Local Subnets	Remote IP/FQDN	Remote

Dynamic Server 3 Status

Tunnel Name	Tunnel Scenario	Local Subnets	Remote IP/FQDN	Remote

Dynamic Server 4 Status

Tunnel Name	Tunnel Scenario	Local Subnets	Remote IP/FQDN	Remote

Static IPsec tunnel Status

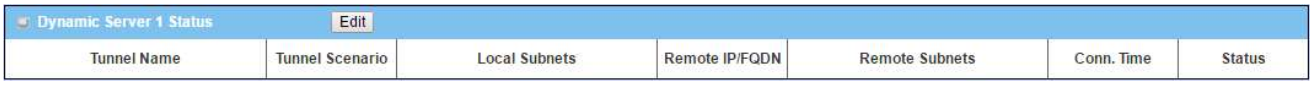
Tunnel Name	Tunnel Scenario	Local Subnets	Remote IP/FQDN	Remote Subnets
IPSec #1	Site to Site	192.168.1.0/255.255.255.0	192.168.128.51	192.168.10.0/255.255.2

2.5.1 VPN Status

The **VPN Status** widow shows the overall VPN tunnel status.
From the menu on the left, select **Status > Security > VPN Status**.

Dynamic VPN Server Status

Dynamic VPN Server Status windows show the configuration for establishing Dynamic VPN connection and current connection status.



Dynamic Server 1 Status

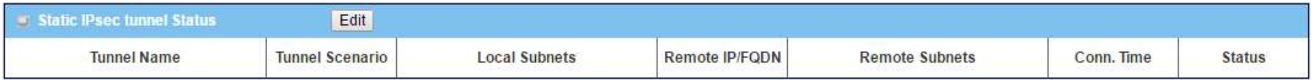
Tunnel Name	Tunnel Scenario	Local Subnets	Remote IP/FQDN	Remote Subnets	Conn. Time	Status

Dynamic Server Status		
Item	**Value setting**	**Description**
Tunnel Name	N/A	It displays the tunnel name you have entered to identify.
Tunnel Scenario	N/A	It displays the Dynamic VPN as the tunnel scenario.
Local Subnets	N/A	It displays the Local Subnets specified.
Remote IP/FQDN	N/A	It displays the Remote IP/FQDN specified.
Remote Subnets	N/A	It displays the Remote Subnets specified.
Conn. Time	N/A	It displays the connection time for the Dynamic VPN connection.

Status	N/A	It displays the Status of the Dynamic VPN connection. The status displays are Connected, Disconnected, Wait for traffic, and Connecting.
Edit Button	N/A	Click on **Edit** Button to change Dynamic VPN setting, web-based utility will take you to the IPSec configuration page. (**Security > VPN > IPSec** tab)

Static IPSec Status

Static IPSec Status shows the configuration for establishing IPSec tunnel and current connection status.



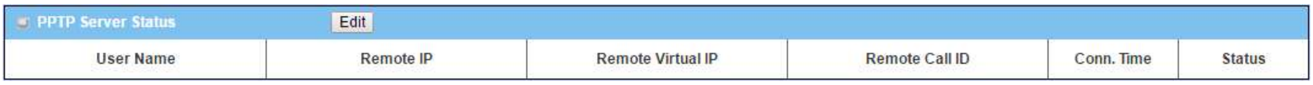
Static IPsec tunnel Status Edit

Tunnel Name	Tunnel Scenario	Local Subnets	Remote IP/FQDN	Remote Subnets	Conn. Time	Status

Static IPSec Status		
Item	**Value setting**	**Description**
Tunnel Name	N/A	It displays the tunnel name you have entered to identify.
Tunnel Scenario	N/A	It displays the Tunnel Scenario specified.
Local Subnets	N/A	It displays the Local Subnets specified.
Remote IP/FQDN	N/A	It displays the Remote IP/FQDN specified.
Remote Subnets	N/A	It displays the Remote Subnets specified.
Conn. Time	N/A	It displays the connection time for the IPSec tunnel.
Status	N/A	It displays the Status of the VPN connection. The status displays are Connected, Disconnected, Wait for traffic, and Connecting.
Edit Button	N/A	Click on Edit Button to change IPSec setting, web-based utility will take you to the IPSec configuration page. (**Security > VPN > IPSec** tab)

PPTP Server/Client Status

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

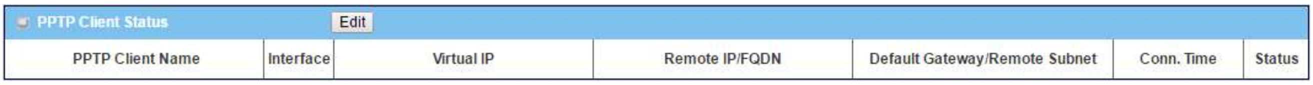


PPTP Server Status Edit

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

PPTP Server Status		
Item	**Value setting**	**Description**
User Name	N/A	It displays the login name of the user used for the connection.
Remote IP	N/A	It displays the public IP address (the WAN IP address) of the connected PPTP client.
Remote Virtual IP	N/A	It displays the IP address assigned to the connected PPTP client.
Remote Call ID	N/A	It displays the PPTP client Call ID.
Conn. Time	N/A	It displays the connection time for the PPTP tunnel.

Status	N/A	It displays the Status of each of the PPTP client connection. The status displays Connected, Disconnect, and Connecting.
Edit Button	N/A	Click on **Edit** Button to change PPTP server setting, web-based utility will take you to the PPTP server configuration page. (**Security > VPN > PPTP** tab)

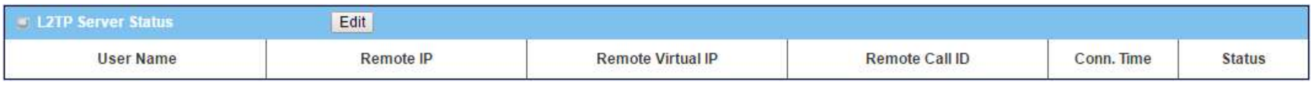


PPTP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Conn. Time	Status

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

L2TP Server/Client Status

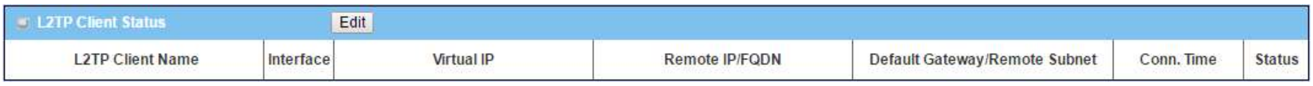
LT2TP Server/Client Status shows the configuration for establishing LT2TP tunnel and current connection status.



L2TP Server Status

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

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



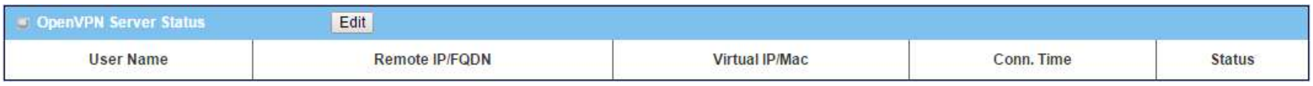
L2TP Client Status

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

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

OpenVPN Server Status

According to OpenVPN configuration, the **OpenVPN Server/Client Status** shows the status and statistics for the OpenVPN connection from the server side or client side.

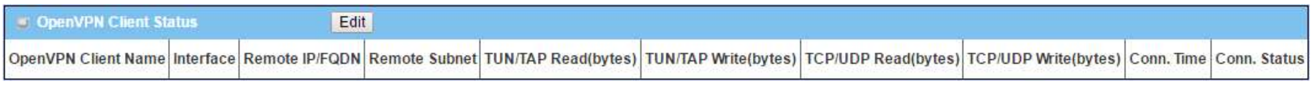


OpenVPN Server Status Edit

User Name	Remote IP/FQDN	Virtual IP/Mac	Conn. Time	Status

OpenVPN Server Status		
Item	**Value setting**	**Description**
User Name	N/A	It displays the Client name you have entered for identification.
Remote IP/FQDN	N/A	It displays the public IP address (the WAN IP address) of the connected OpenVPN Client
Virtual IP/MAC	N/A	It displays the virtual IP/MAC address assigned to the connected OpenVPN client.
Conn. Time	N/A	It displays the connection time for the corresponding OpenVPN tunnel.
Status	N/A	It displays the connection status of the corresponding OpenVPN tunnel. The status can be Connected, or Disconnected.

OpenVPN Server Status



OpenVPN Client Status Edit

OpenVPN Client Name	Interface	Remote IP/FQDN	Remote Subnet	TUN/TAP Read(bytes)	TUN/TAP Write(bytes)	TCP/UDP Read(bytes)	TCP/UDP Write(bytes)	Conn. Time	Conn. Status

OpenVPN Client Status		
Item	**Value setting**	**Description**
OpenVPN Client Name	N/A	It displays the Client name you have entered for identification.
Interface	N/A	It displays the WAN interface specified for the OpenVPN client connection.
Remote IP/FQDN	N/A	It displays the peer OpenVPN Server's Public IP address (the WAN IP address) or FQDN.
Remote Subnet	N/A	It displays the Remote Subnet specified.
TUN/TAP Read(bytes)	N/A	It displays the TUN/TAP Read Bytes of OpenVPN Client.
TUN/TAP Write(bytes)	N/A	It displays the TUN/TAP Write Bytes of OpenVPN Client.
TCP/UDP Read(bytes)	N/A	It displays the TCP/UDP Read Bytes of OpenVPN Client.
TCP/UDP Write(bytes)	N/A	It displays the TCP/UDP Write Bytes of OpenVPN Client. Connection
Conn. Time	N/A	It displays the connection time for the corresponding OpenVPN tunnel.
Conn. Status	N/A	It displays the connection status of the corresponding OpenVPN tunnel. The status can be Connected, or Disconnected.

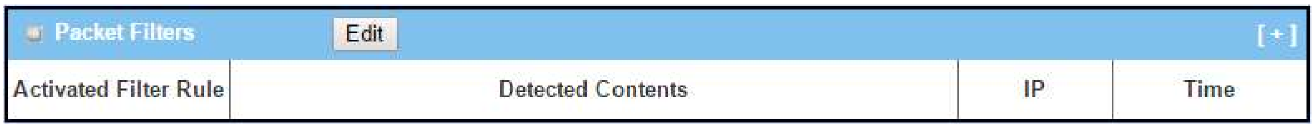
2.5.3 Firewall Status

From the menu on the left, select **Status > Security > Firewall Status** Tab.

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

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

Packet Filter Status



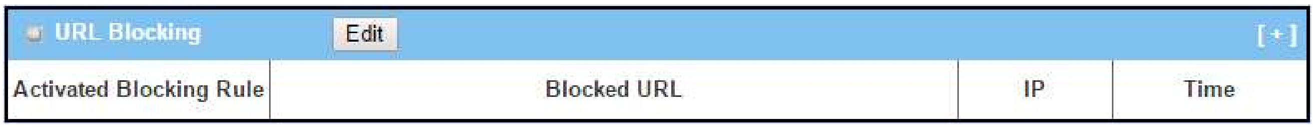
Packet Filters Edit [+]

Activated Filter Rule	Detected Contents	IP	Time

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

Note: Ensure Packet Filter Log Alert is enabled.
*Refer to **Security > Firewall > Packet Filter** tab. Check Log Alert and save the setting.*

URL Blocking Status



URL Blocking Edit [+]

Activated Blocking Rule	Blocked URL	IP	Time

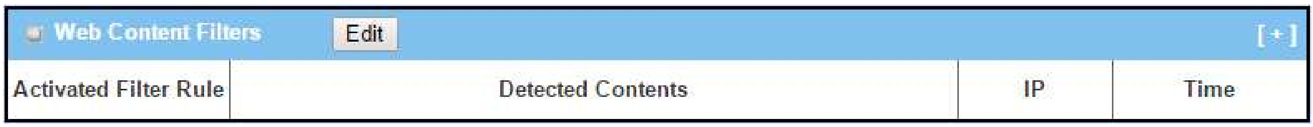
URL Blocking Status		
Item	**Value setting**	**Description**
Activated Blocking Rule	N/A	This is the URL Blocking Rule name.

Blocked URL	N/A	This is the logged packet information.
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure URL Blocking Log Alert is enabled.

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

Web Content Filter Status



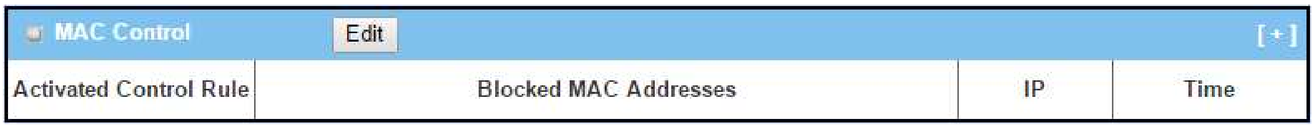
Activated Filter Rule	Detected Contents	IP	Time

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

Note: Ensure Web Content Filter Log Alert is enabled.

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

MAC Control Status



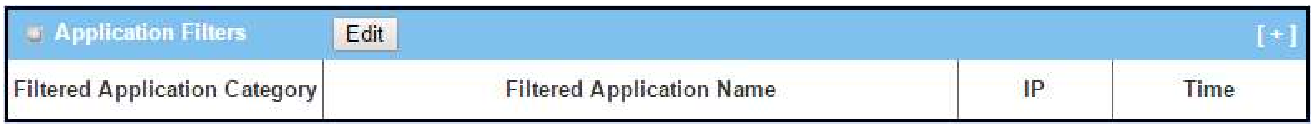
Activated Control Rule	Blocked MAC Addresses	IP	Time

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

Note: Ensure MAC Control Log Alert is enabled.

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

Application Filters Status

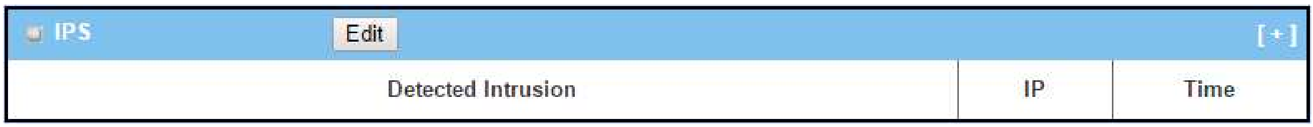


Filtered Application Category	Filtered Application Name	IP	Time

Application Filters Status		
Item	**Value setting**	**Description**
Filtered Application Category	N/A	The name of the Application Category being blocked.
Filtered Application Name	N/A	The name of the Application being blocked.
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure Application Filter Log Alert is enabled.
*Refer to **Security > Firewall > Application Filter** tab. Check Log Alert and save the setting.*

IPS Status

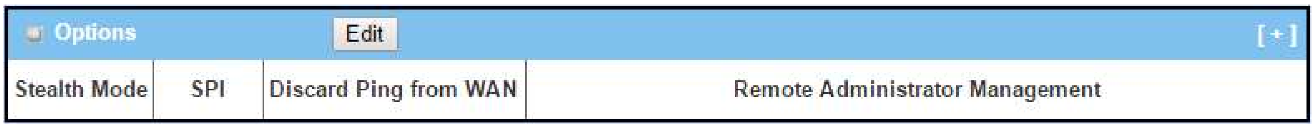


Detected Intrusion	IP	Time

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

Note: Ensure IPS Log Alert is enabled.
Refer to ***Security > Firewall > IPS*** *tab. Check Log Alert and save the setting.*

Firewall Options Status

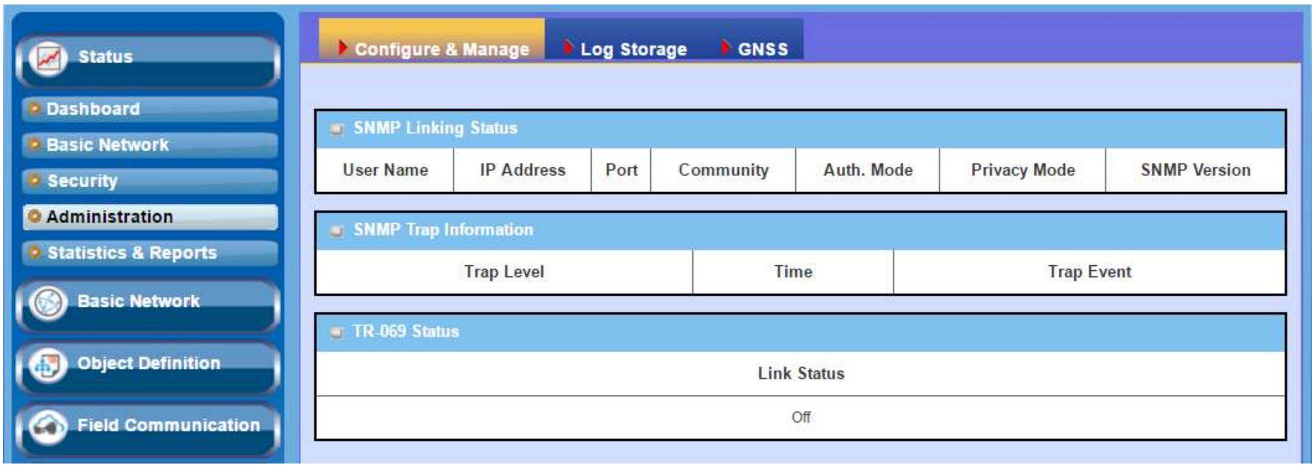


Stealth Mode	SPI	Discard Ping from WAN	Remote Administrator Management

Firewall Options Status		
Item	**Value setting**	**Description**
Stealth Mode	N/A	Enable or Disable setting status of Stealth Mode on Firewall Options. String Format: Disable or Enable
SPI	N/A	Enable or Disable setting status of SPI on Firewall Options. String Format : Disable or Enable
Discard Ping from WAN	N/A	Enable or Disable setting status of Discard Ping from WAN on Firewall Options. String Format: Disable or Enable
Remote Administrator Management	N/A	Enable or Disable setting status of Remote Administrator. If Remote Administrator is enabled, it shows the currently logged in administrator’s source IP address and login user name and the login time. Format: IP : "Source IP", User Name: "Login User Name", Time: "Date time" Example: IP: 192.168.127.39, User Name: admin, Time: Mar 3 01:34:13

Note: Ensure Firewall Options Log Alert is enabled.
Refer to ***Security > Firewall > Options*** *tab. Check Log Alert and save the setting.*

2.7 Administration



SNMP Linking Status

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

SNMP Trap Information

Trap Level	Time	Trap Event

TR-069 Status

Link Status
Off

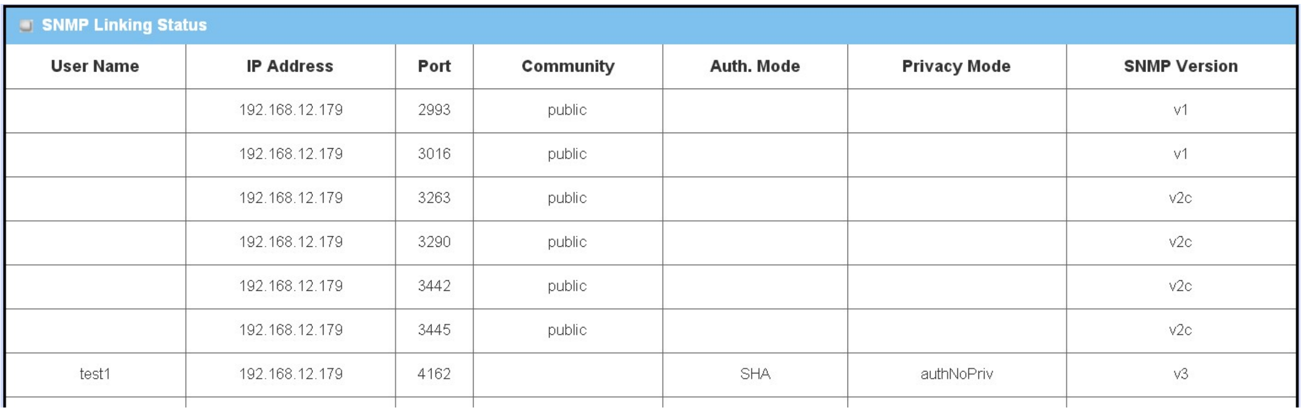
2.7.1 Configure & Manage Status

The **Configure & Manage Status** window shows the status for managing remote network devices. The type of management available in your device is depended on the device model purchased. The commonly used ones are the SNMP, TR-069, and UPnP.

From the menu on the left, select **Status > Administration > Configure & Manage** tab.

SNMP Linking Status

SNMP Link Status screen shows the status of current active SNMP connections.



SNMP Linking Status

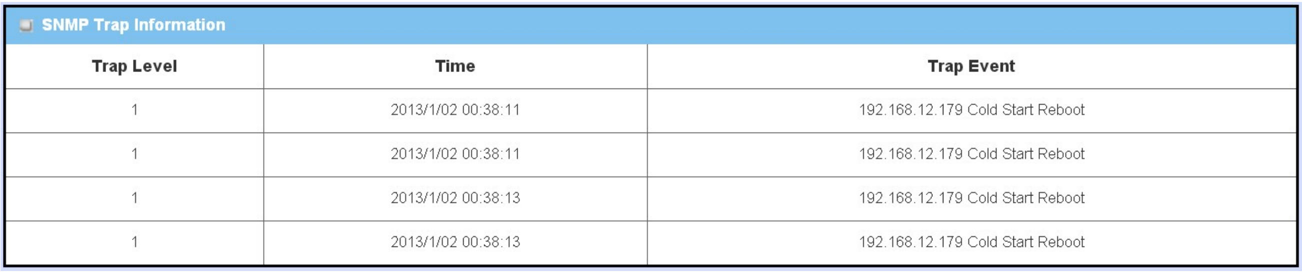
User Name	IP Address	Port	Community	Auth. Mode	Privacy Mode	SNMP Version
	192.168.12.179	2993	public			v1
	192.168.12.179	3016	public			v1
	192.168.12.179	3263	public			v2c
	192.168.12.179	3290	public			v2c
	192.168.12.179	3442	public			v2c
	192.168.12.179	3445	public			v2c
test1	192.168.12.179	4162		SHA	authNoPriv	v3

SNMP Link Status		
Item	Value setting	Description

User Name	N/A	It displays the user name for authentication. This is only available for SNMP version 3.
IP Address	N/A	It displays the IP address of SNMP manager.
Port	N/A	It displays the port number used to maintain connection with the SNMP manager.
Community	N/A	It displays the community for SNMP version 1 or version 2c only.
Auth. Mode	N/A	It displays the authentication method for SNMP version 3 only.
Privacy Mode	N/A	It displays the privacy mode for version 3 only.
SNMP Version	N/A	It displays the SNMP Version employed.

SNMP Trap Information

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



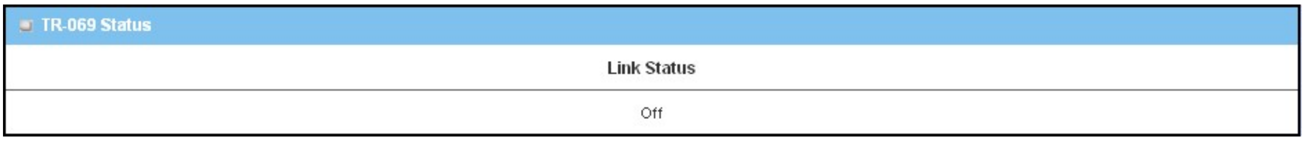
SNMP Trap Information

Trap Level	Time	Trap Event
1	2013/1/02 00:38:11	192.168.12.179 Cold Start Reboot
1	2013/1/02 00:38:11	192.168.12.179 Cold Start Reboot
1	2013/1/02 00:38:13	192.168.12.179 Cold Start Reboot
1	2013/1/02 00:38:13	192.168.12.179 Cold Start Reboot

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

TR-069 Status

TR-069 Status screen shows the current connection status with the TR-068 server.



TR-069 Status

Link Status
Off

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

2.7.3 Log Storage Status

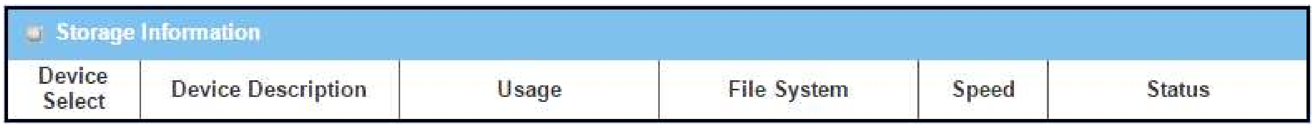
The **Log Storage Status** window shows the status for selected device storage.

From the menu on the left, select **Status > Administration > Log Storage** tab.

Log Storage Status

Log Storage Status screen shows the status of current the selected device storage. The status includes Device Select, Device Description, Usage, File System, Speed, and status

.



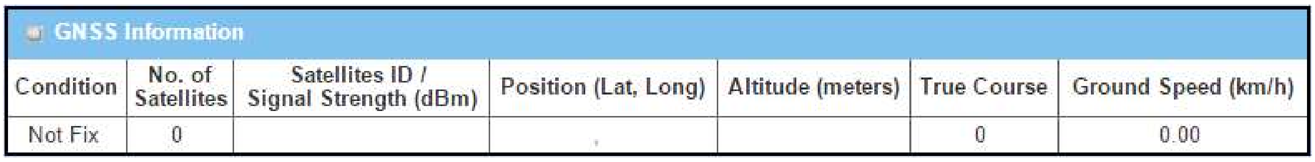
Storage Information

Device Select	Device Description	Usage	File System	Speed	Status

2.7.5 GNSS Information

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

From the menu on the left, select **Status > Administtration > GNSS** tab.

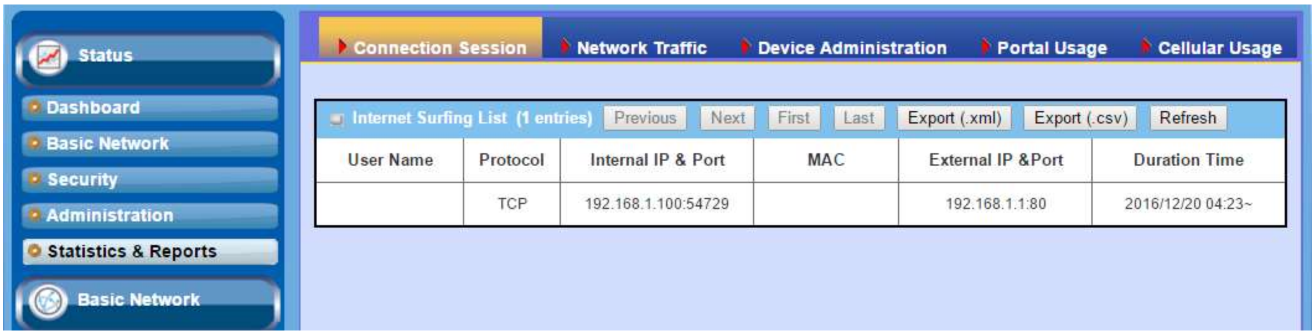


GNSS Information

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

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

2.9 Statistics & Report

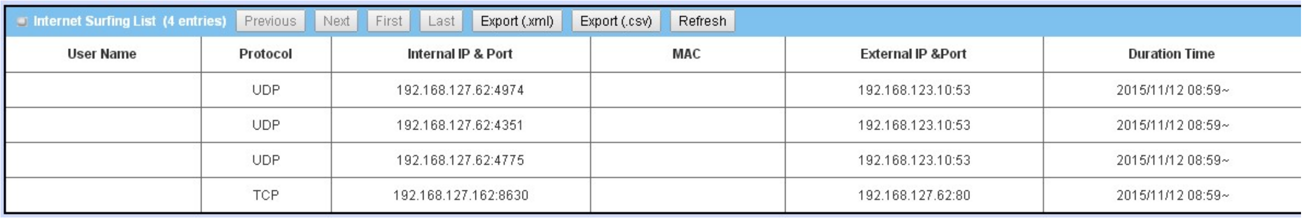


User Name	Protocol	Internal IP & Port	MAC	External IP &Port	Duration Time
	TCP	192.168.1.100:54729		192.168.1.1:80	2016/12/20 04:23~

2.9.1 Connection Session

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

Internet Surfing Statistic shows the connection tracks on this router.



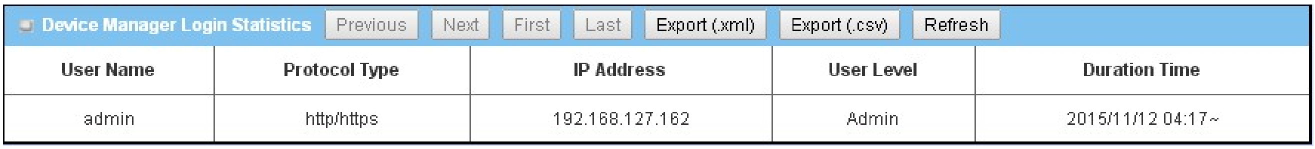
User Name	Protocol	Internal IP & Port	MAC	External IP &Port	Duration Time
	UDP	192.168.127.62:4974		192.168.123.10:53	2015/11/12 08:59~
	UDP	192.168.127.62:4351		192.168.123.10:53	2015/11/12 08:59~
	UDP	192.168.127.62:4775		192.168.123.10:53	2015/11/12 08:59~
	TCP	192.168.127.162:8630		192.168.127.62:80	2015/11/12 08:59~

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

2.9.5 Device Administration

Go to **Status > Statistics & Reports > Device Administration** tab.

Device Administration shows the login information.



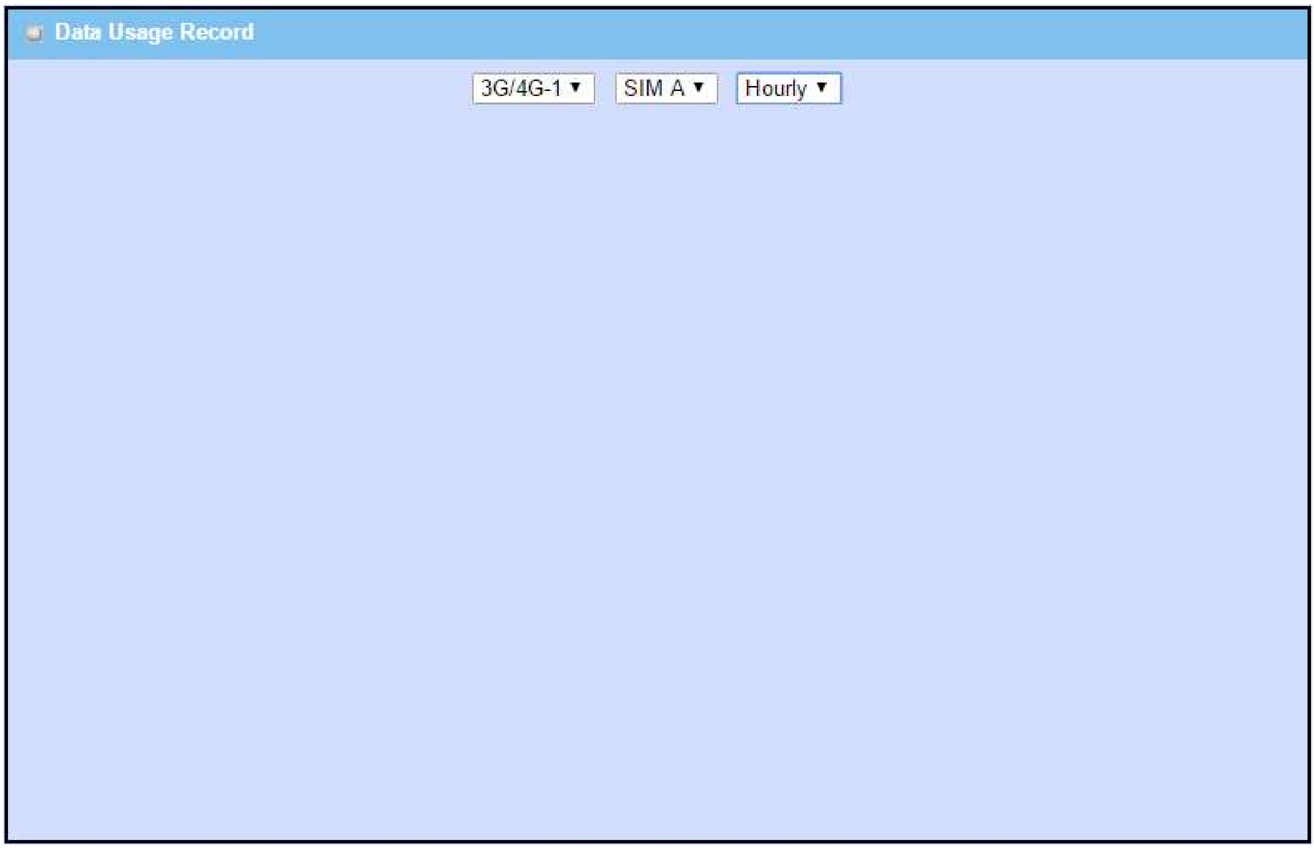
User Name	Protocol Type	IP Address	User Level	Duration Time
admin	http/https	192.168.127.162	Admin	2015/11/12 04:17~

Device Manager Login Statistic Item	Value setting	Description
Previous	N/A	Click the **Previous** button; you will see the previous page of login statistics.
Next	N/A	Click the **Next** button; you will see the next page of login statistics
First	N/A	Click the **First** button; you will see the first page of login statistics
Last	N/A	Click the **Last** button; you will see the last page of login statistics
Export (.xml)	N/A	Click the **Export (.xml)** button to export the login statistics to xml file.
Export (.csv)	N/A	Click the **Export (.csv)** button to export the login statistics to csv file.
Refresh	N/A	Click the **Refresh** button to refresh the login statistics

2.9.9 Cellular Usage

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

Cellular Usage screen shows data usage statistics for the selected cellular interface. The cellular data usage can be accumulated per hour or per day.



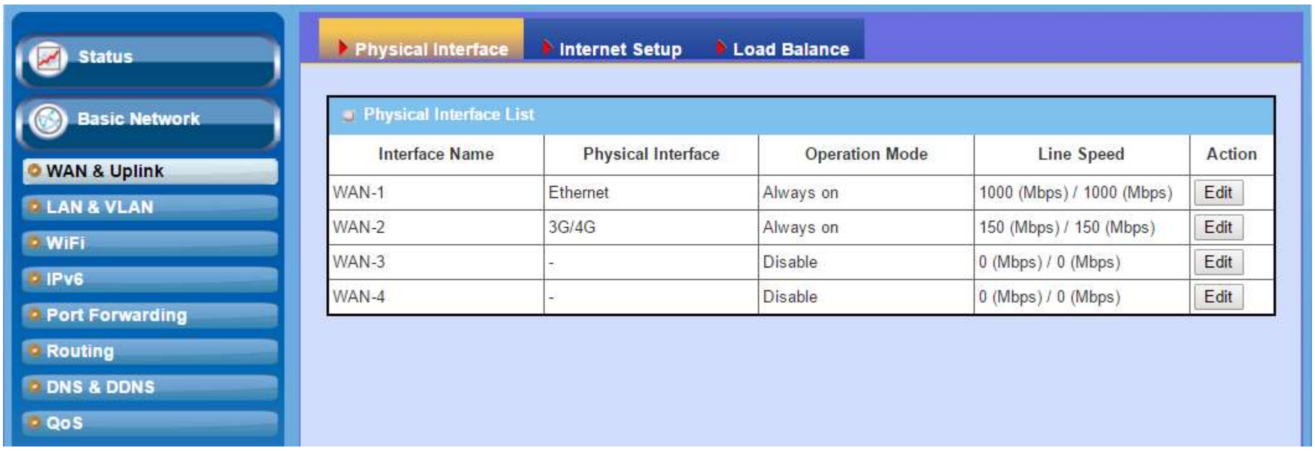
Chapter 3 Basic Network

3.1 WAN & Uplink

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

So, the WAN Connection lets you specify the WAN Physical Interface, WAN Internet Setup and WAN Load Balance for Intranet to access Internet. For each WAN interface, you must specify its physical interface first and then its Internet setup to connect to ISP. If the gateway has multiple WAN interfaces, you also can assign physical interface to participate in the Load Balance function.

In Physical Interface, you can choose “Ethernet”, “3G/4G”, “USB 3G/4G” or “ADSL” based on the supported interfaces of the gateway. In Internet Setup, you can choose adequate WAN type for different kind of WAN interface. When the gateway has multiple WAN interfaces, load balance function operates between these interfaces to maximize the WAN bandwidth utilization.



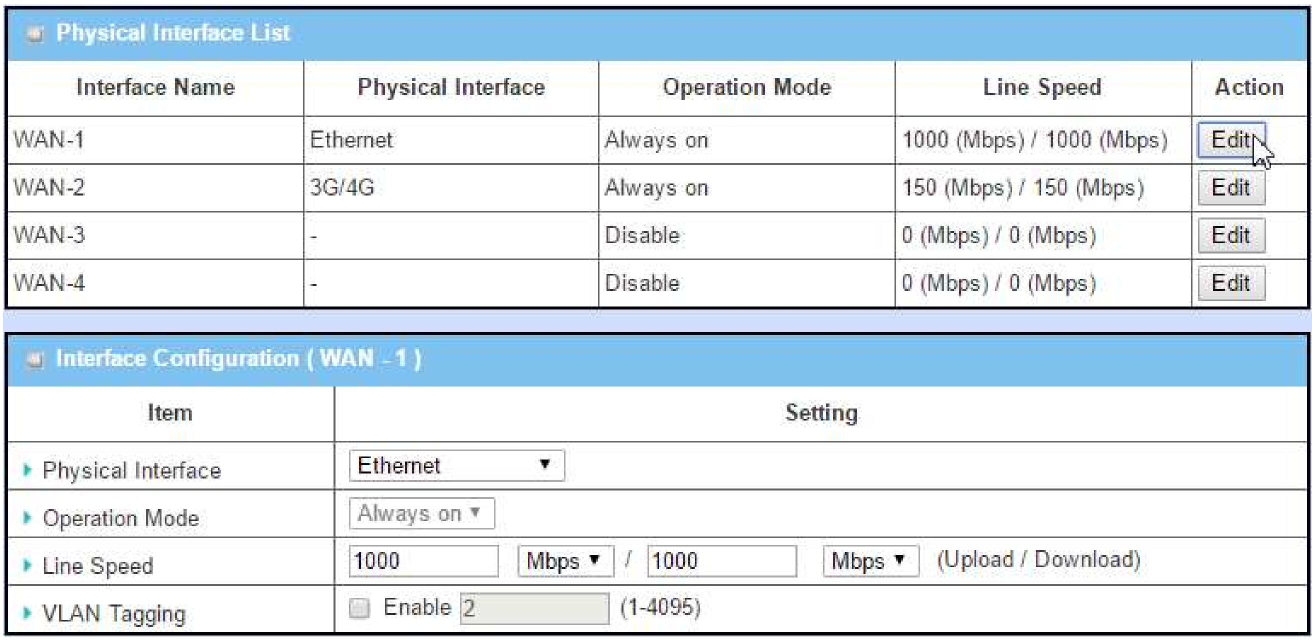
Physical Interface List

Interface Name	Physical Interface	Operation Mode	Line Speed	Action
WAN-1	Ethernet	Always on	1000 (Mbps) / 1000 (Mbps)	Edit
WAN-2	3G/4G	Always on	150 (Mbps) / 150 (Mbps)	Edit
WAN-3	-	Disable	0 (Mbps) / 0 (Mbps)	Edit
WAN-4	-	Disable	0 (Mbps) / 0 (Mbps)	Edit

3.1.1 Physical Interface

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

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



Physical Interface List

Interface Name	Physical Interface	Operation Mode	Line Speed	Action
WAN-1	Ethernet	Always on	1000 (Mbps) / 1000 (Mbps)	Edit
WAN-2	3G/4G	Always on	150 (Mbps) / 150 (Mbps)	Edit
WAN-3	-	Disable	0 (Mbps) / 0 (Mbps)	Edit
WAN-4	-	Disable	0 (Mbps) / 0 (Mbps)	Edit

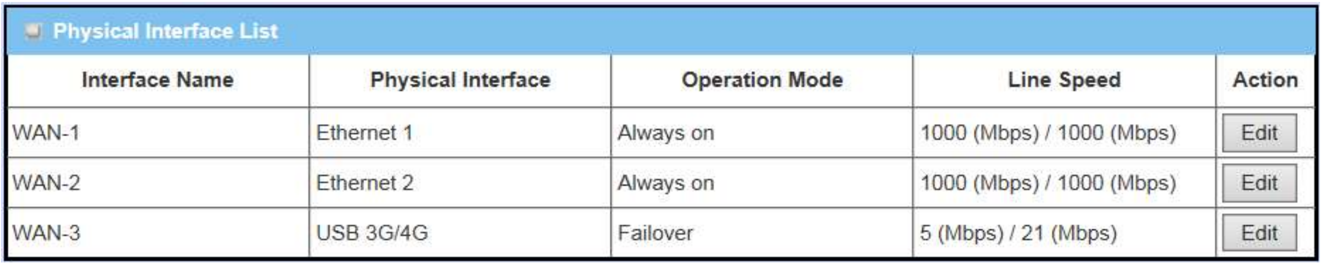
Interface Configuration (WAN - 1)

Item	Setting
Physical Interface	Ethernet ▼
Operation Mode	Always on ▼
Line Speed	1000 Mbps ▼ / 1000 Mbps ▼ (Upload / Download)
VLAN Tagging	□ Enable 2 (1-4095)

Physical Interface List

The Physical Interface List shows all WAN interfaces of the gateway device, including their name, what kinds of physical interface, their operation mode and line speed. There is one "Edit" button for each WAN interface, which can let you configure the interface. Please see "Interface Configuration" section beneath. Following are some "Physical Interface List" window examples for different gateway products.

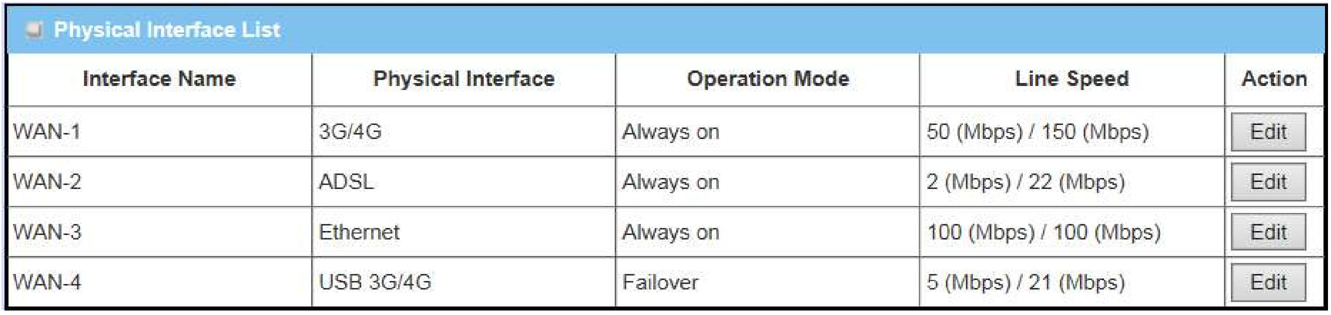
An example of a SDE852AM-00001 device



Physical Interface List

Interface Name	Physical Interface	Operation Mode	Line Speed	Action
WAN-1	Ethernet 1	Always on	1000 (Mbps) / 1000 (Mbps)	Edit
WAN-2	Ethernet 2	Always on	1000 (Mbps) / 1000 (Mbps)	Edit
WAN-3	USB 3G/4G	Failover	5 (Mbps) / 21 (Mbps)	Edit

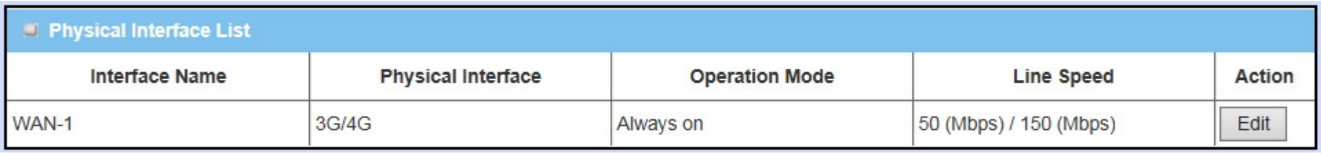
An example of an IOG761AM-0TDA1 device



Physical Interface List

Interface Name	Physical Interface	Operation Mode	Line Speed	Action
WAN-1	3G/4G	Always on	50 (Mbps) / 150 (Mbps)	Edit
WAN-2	ADSL	Always on	2 (Mbps) / 22 (Mbps)	Edit
WAN-3	Ethernet	Always on	100 (Mbps) / 100 (Mbps)	Edit
WAN-4	USB 3G/4G	Failover	5 (Mbps) / 21 (Mbps)	Edit

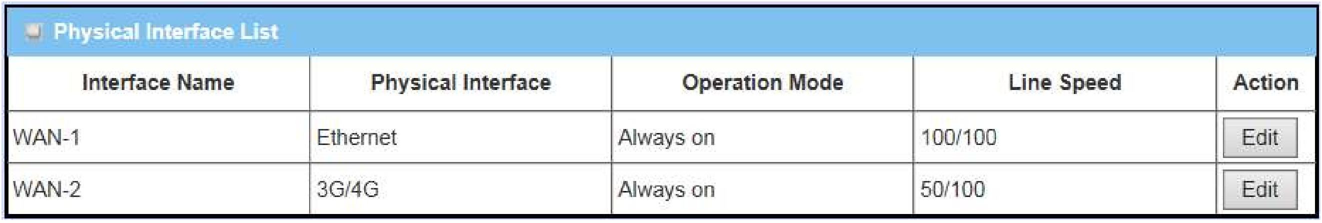
An example of an ODG761AM-0T1 device



Physical Interface List

Interface Name	Physical Interface	Operation Mode	Line Speed	Action
WAN-1	3G/4G	Always on	50 (Mbps) / 150 (Mbps)	Edit

An example of a BDG761AM-0T1 device



Physical Interface List

Interface Name	Physical Interface	Operation Mode	Line Speed	Action
WAN-1	Ethernet	Always on	100/100	Edit
WAN-2	3G/4G	Always on	50/100	Edit

The contents of "Physical Interface List" in above example windows are just some examples. They vary from model to model. It depends on the model you purchased.

- **Interface Name**

  The logic name of WAN interfaces is identified by “WAN-1”, “WAN-2”, …, and so on.

- **Physical Interface**

  This device is equipped with some kinds of WAN interfaces to support different WAN types of connections. You can configure one by one to get proper internet connection setup. Refer to the product specification for the available WAN interfaces for the model you purchased.

- **Operation Mode**

There are three option items “Always-on”, “Failover”, and “Disable” for the operation mode setting. It decides whether the corresponding WAN interface functions as the main access, as a failover access connection or disable the interface.

- **Line Speed**

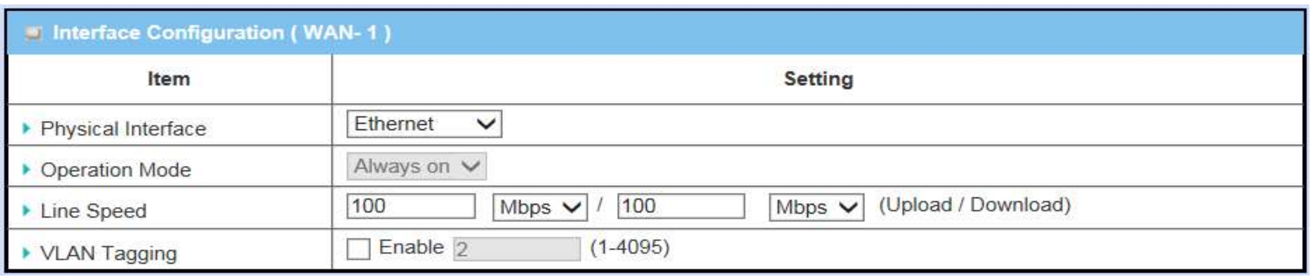
Specify the correct line speed (bandwidth) of uploading and downloading for each WAN interface allow the device to operate its QoS and WAN Load Balance functions normally. It is necessary to configure the parameters if you want to use QoS and WAN Load Balance functions on the gateway device.

- **VLAN Tagging**

Sometimes, your ISP required a VLAN tag to be inserted into the WAN packets from Gateway for specific services. You must specify it in the WAN physical interface. Please note that only Ethernet and ADSL physical interfaces support the feature.

Interface Configuration

The configuration of a WAN interface includes the settings of interface type, operation mode, line speed of upload and download, and VLAN tagging. The WAN interface name at the end of window caption indicates which interface that you are configuring.



Interface Configuration (WAN- 1)

Item	Setting
Physical Interface	Ethernet
Operation Mode	Always on
Line Speed	100 Mbps / 100 Mbps (Upload / Download)
VLAN Tagging	□ Enable 2 (1-4095)

The content in above diagram is an example for Ethernet WAN interface.

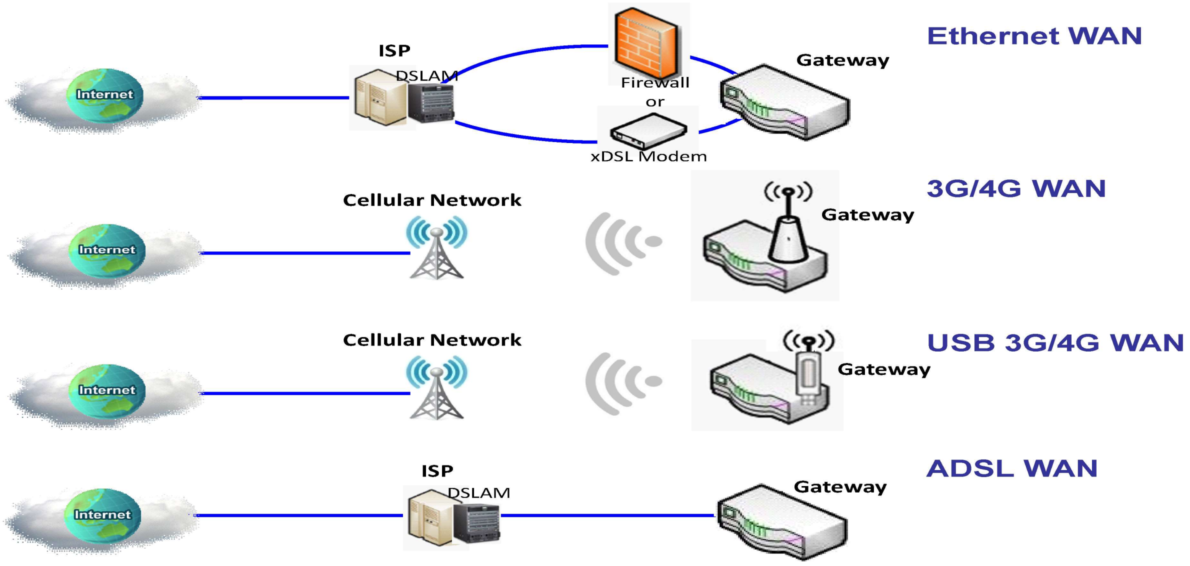
- **Physical Interface**

This device is equipped with some kinds of WAN interfaces to support different WAN types of connections. You can configure one by one to get proper internet connection setup. Refer to the product specification for the available WAN interfaces for the model you purchased.

Following are some physical interface configuration examples and their illustration diagrams. Please be noted that USB 3G/4G can be used only as a failover interface. The primary connection is WAN-1 and its operation mode must be "Always on". So, the physical interface of WAN-1 will not be "USB 3G/4G".

M2M LTE Gateway with serial port

Configuration Path	[Physical Interface]-[Interface Configuration (WAN-n)], n=1, 2, ...			
Physical Interface	*Ethernet*	*3G/4G*	*USB 3G/4G*	*ADSL*
Operation Mode	*Always on*	*Always on*	*Failover*	*Always on*
Line Speed	*100Mbps / 100Mbps*	*50Mbps / 150Mbps*	*5Mbps / 21Mbps*	*2Mbps / 22Mbps*



Ethernet WAN: The gateway has one or more RJ45 WAN ports that can be configured to be WAN connections. For each Ethernet WAN port, please plug in RJ45 cable from your external DSL modem to the port and follow UI setting to setup. If the gateway is setup behind a firewall device, plug in RJ45 cable from one Ethernet port of firewall device instead.

3G/4G WAN: The gateway has one or more built-in 3G/4G[6] modems that can be configured to be WAN connections. For each built-in modem, there are 1 or 2 SIM cards to be inserted into the modem, please insert the SIM card and follow UI setting to setup.

Caution

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

[5] The specification of embedded module depends on respective model.

USB 3G/4G WAN: The gateway has one USB port that might support 3G/4G USB modem[7] for a WAN connection. Please plug 3G/4G USB dongle and follow UI setting to setup.

ADSL WAN: The gateway has one ADSL modem built-in that can be configured to be a WAN connection, please plug in RJ11 cable (normally the landline phone cable) in DSL port and follow UI setting to setup.

- **Operation Mode**

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

Always on: Set this WAN interface to be active all the time. Only the interfaces with "Always on" operation mode can share their bandwidth for load balance function. That means when two or more Internet connections are established simultaneously at "Always on" mode, outgoing data will be transferred through these WAN connections base on load balance policies. This mode is especially suitable for high bandwidth requirement, such as video stream transmission.

Failover: A failover interface is a backup connection to the primary. That means only when its primary WAN connection is broken, the backup connection will be started up to substitute the primary connection. In addition, there is a "Seamless" option for Failover operation mode. When seamless option is activated by checking on the "Seamless" box in configuration window, both the primary connection and the failover connection are started up after system rebooting. But only the primary connection executes the data transfer, while the failover one just keeps alive of connection line. As soon as the primary connection is broken, the system will switch, meaning failover, the routing path to the failover connection to save the dial up time of failover connection since it has been alive.

Disable: Set this WAN interface to be inactive.

➢ **Failover Scenario without Seamless**:

As an example, you can set the operation mode of WAN-2 interface to be a backup WAN connection. WAN-1 interface serves as the primary connection of WAN-2 and its operation mode is "Always on". But the "Seamless" box is unchecked. That means WAN-2 failover from WAN-1 and it won’t be activated until primary WAN connection (WAN-1) has failed. When the primary interface is recovered back with a connection, primary interface will take over data transfer again. Following 4 tables list the parameter configuration for these two WAN interfaces.

6 Please check the product specification for the WAN & Uplink. Only specific model supports USB 3G/4G WAN function. Besides, please refer to compatibility list to check which 3G or 4G dongles are supported.

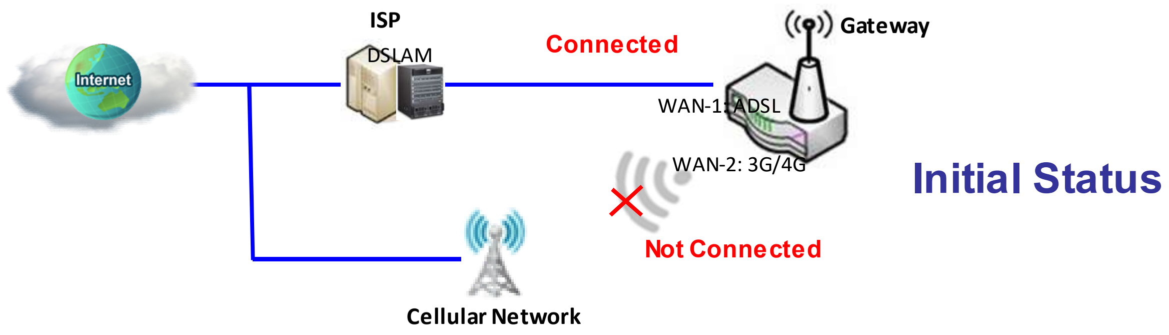
Configuration Path	[Physical Interface]-[Interface Configuration (WAN-n)], n=1, 2	
Interface Name	WAN-1	WAN-2
Physical Interface	*ADSL*	*USB 3G/4G*
Operation Mode	*Always on*	*Failover WAN-1 □Seamless*
Line Speed	*2Mbps / 22Mbps*	*5Mbps / 21Mbps*

Configuration Path	[Internet Setup]-[Internet Connection Configuration (WAN-n)], n=1, 2	
Interface Name	WAN-1	WAN-2
WAN Type	*Ethernet over ATM with NAT*	*3G/4G*

Configuration Path	[Internet Setup]-[Ethernet over ATM with NAT WAN Type Configuration]
Interface Name	WAN-1
Connection Control	*Auto-reconnect (Always on)*
Data Encryption	*LLC*
VPI Number	*0*
VCI Number	*33*
Schedule Type	*UBR*

Configuration Path	[Internet Setup]-[3G/4G WAN Type Configuration]
Interface Name	WAN-2
Dial-up Profile	*Auto-detection*
Connection Control	*Auto-reconnect (Always on)*

So, the initial status of two WAN connections is shown in following diagram.



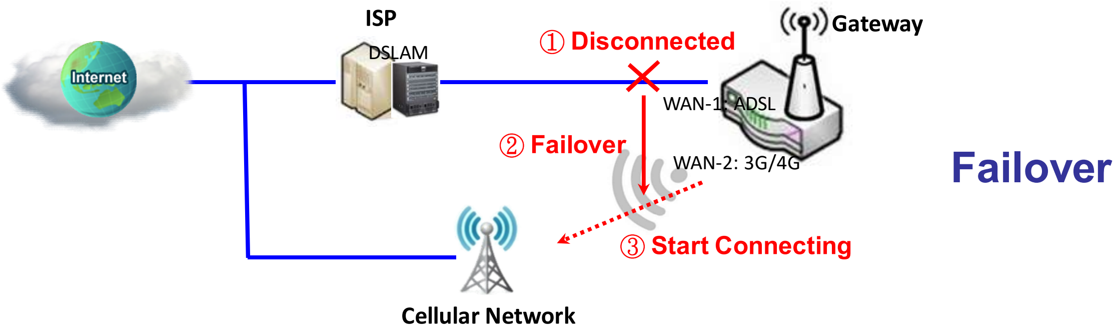
Next, Failover and Failback processes are shown in following diagram. Their steps are:

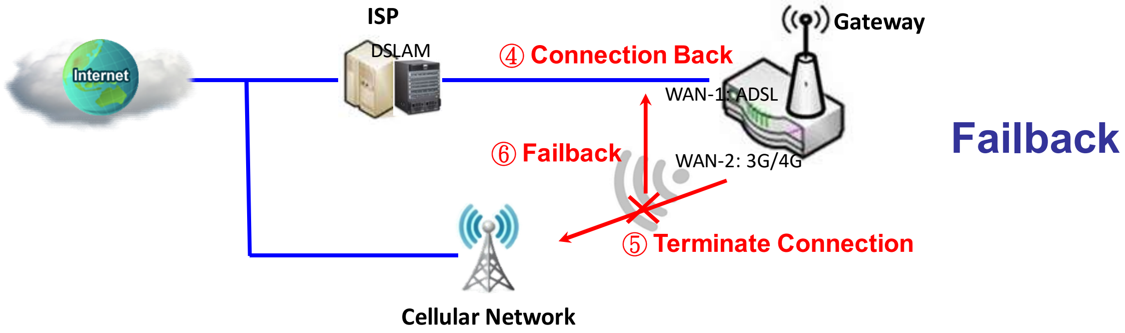
<u>S 1:</u> When system discovers the primary WAN connection is failed.
<u>S 2:</u> System starts the failover process.
<u>S 3:</u> System tries to create the WAN connection by using Failover WAN interface, and use it for incoming data transmitting mission.
<u>S 4:</u> System keeps trying to recover the failed primary WAN connection. Once it is recovered,

system starts the failback process.

S 5: When failback process starts, system terminates the current WAN connection via Failover WAN interface.

S 6: System changes the data routing path back to the primary WAN interface as same state as at the beginning of system normal operation.





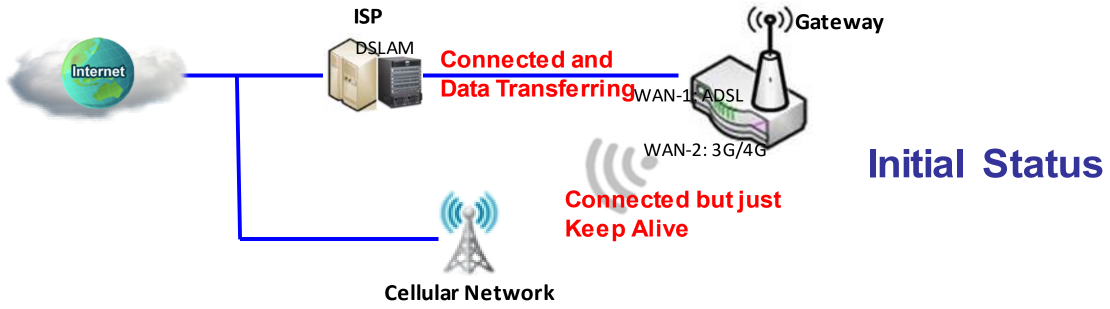
➢ **Seamless Failover Scenario:**

As another example, all parameter configuration for WAN-1 and WAN-2 is same as above example except the "Seamless" box is checked as bellow (in red color).

Configuration Path	[Physical Interface]-[Interface Configuration (WAN-n)], n=1, 2	
Interface Name	WAN-1	WAN-2
Physical Interface	*ADSL*	*USB 3G/4G*
Operation Mode	*Always on*	*Failover WAN-1 ■Seamless*
Line Speed	*2Mbps / 22Mbps*	*5Mbps / 21Mbps*

When the “Seamless” enable checkbox is activated, it can allow the Failover interface to be connected continuously after system booting up. The Failover interface just keeps connecting but without data transfer. The purpose is to aim at the shortening of switch time during failover process. So, when primary connection is disconnected, failover interface will take over the data transfer mission instantly by only changing routing path to failover interface. The dialing-up time of failover connection is saved since it has been connected beforehand.

So, the initial status of two WAN connections for Seamless Failover is shown in following diagram.



Next, Failover and Failback processes are shown in following diagram. Their steps are:

S 1: When system discovers the primary WAN connection is failed.

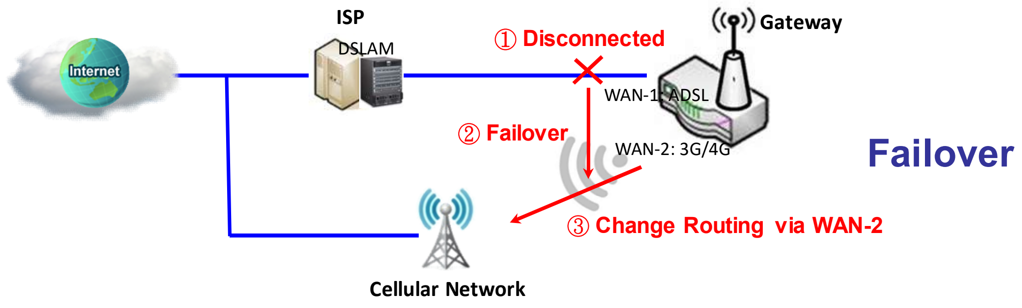
S 2: System starts the failover process.

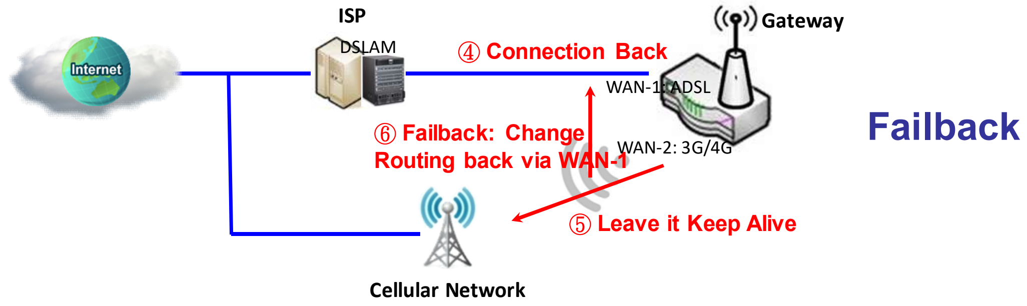
S 3: System changes the data routing path to the failover WAN interface for further data transmitting. It is faster than the one in the normal mode of failover since routing change is simpler than dialing up a new WAN connection.

S 4: System keeps trying to recover the failed primary WAN connection. Once it is recovered, system starts the failback process.

S 5: When failback process starts, system will leave alive the current WAN connection via Failover WAN interface, but no more data transmitting.

S 6: System changes the data routing path back to the primary WAN interface as same state as at the beginning of system normal operation.





- **Dual SIM Failover Scenario:**

If your purchased product has one or more embedded 3G/LTE module, and they have dual SIMs to be used as connection profiles to connect to mobile system for each 3G/LTE module. But please be noted, only one SIM card is used for a 3G/LTE module. Failover and Seamless Failover scenarios mentioned above are interacted between multiple interfaces. One embedded 3G/LTE module creates only one WAN interface, even it has dual SIMs. A special failover mechanism between using both SIM cards to connect to mobile system is presented here. It is called as Dual SIM Failover.

In this Dual SIM Failover, there are four kinds of SIM card usage scenarios, including "SIM-A First", "SIM-B First“, and “SIM-A Only and “SIM-B Only”. By default, “SIM-A First” scenario is used to connect to mobile system for data transfer. So in the case when “SIM-A Only” or “SIM-B Only” is used, the specified SIM slot card is the only one to be used for negotiation parameters between gateway device and mobile base station. However, 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, gateway system will switch to use the other SIM card for an alternate automatically and will not switch back to use original SIM card except current SIM connection is also broken. That is, SIM-A and SIM-B are used iteratively, but either one will keep being used for data transfer when current connection is still alive.

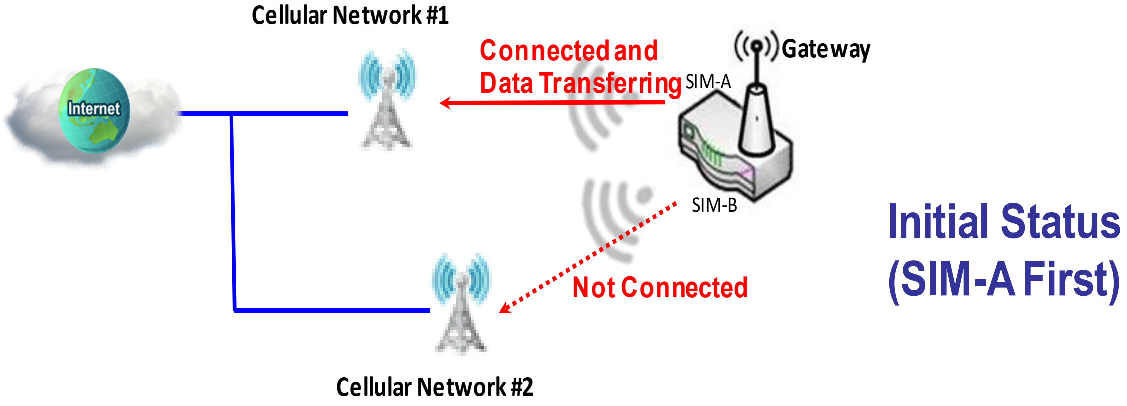
Following 3 tables list the parameter configuration for the Dual SIM failover scenario. Other settings that don't show out in the tables, please leave them as default values.

Configuration Path	[Physical Interface]-[Interface Configuration (WAN-1)]
Interface Name	WAN-1
Physical Interface	***3G/4G***
Operation Mode	***Always on***
Line Speed	***50Mbps / 150Mbps***

Configuration Path	[Internet Setup]-[Internet Connection Configuration (WAN-1)]
Interface Name	WAN-1
WAN Type	***3G/4G***

Configuration Path	[Internet Setup]-[3G/4G WAN Type Configuration]
Interface Name	WAN-1
Preferred SIM Card	***SIM-A First***

So, the initial status of two WAN connections using different SIM card is shown in the following diagram.



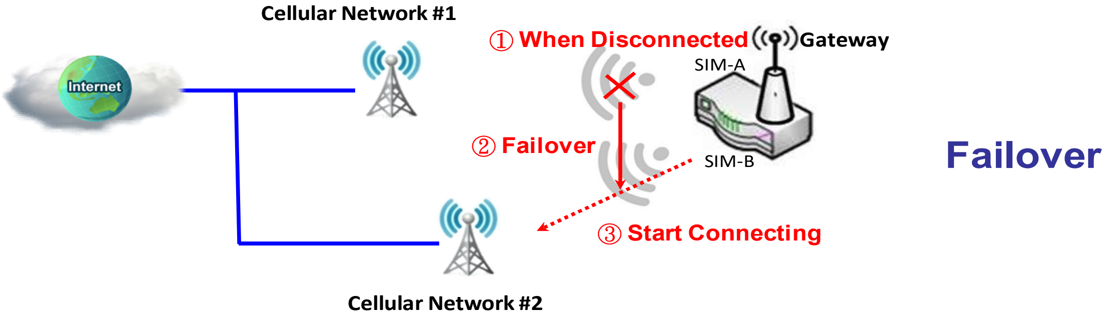
Next, Dual SIM Failover process with SIM-A First scenario is shown in the following diagram. The steps are:

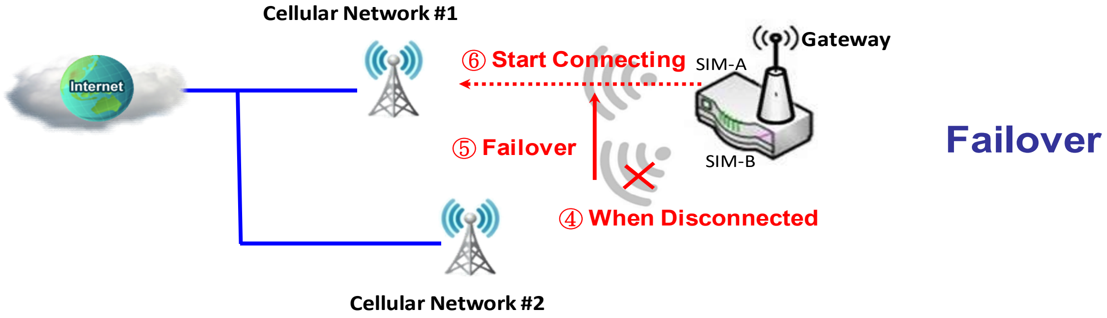
Pre-state: System tries to connect to mobile system for an Internet connection by using connection profile in SIM-A (for SIM-A First scenario) after system rebooting. If the connection is successful, data transfer from Intranet to Internet will be executed in this WAN connection. Call the connection as SIM-A connection. But if SIM-A connection failed, system will try to connect to mobile system by using connection profile in SIM-B. If it is successful, call it as SIM-B connection. In this way, use SIM-A and SIM-B alternately for a successful WAN connection. At last, assume it is SIM-m connection here for a successful connection, m can be 'A' or 'B'.

S 1: When system discovers the SIM-m connection is failed, system starts the failover process.

S 2: System tries to create another WAN connection by using connection profile in SIM-n, and use it for incoming data transmitting mission, where n can be 'A' or 'B'.

S 3: System keeps executing data transfer via SIM-n connection until the connection failed. Once the SIM-n connection failed, system starts the failover process again and goes back to S2 step.





- **Line Speed**

To declare correct line speed of uploading and downloading for each WAN interface can let the device operate its QoS and WAN Load Balance functions normally.

If you don't know accurate line speed of your subscribed Internet service, following are some suggestions:

- High Speed Ethernet WAN: Upload 100Mbps, Download 100Mbps;
- Gigabit Ethernet WAN: Upload 1000Mbps, Download 1000Mbps;
- CAT4 Built-in LTE Module: Upload 50Mbps, Download 150Mbps;
- CAT3 LTE USB Dongle: Upload 50Mbps, Download 100Mbps;
- 3G USB Dongle: Upload 5Mbps, Download 21Mbps;
- ADSL2+: Upload 2Mbps, Download 22Mbps.

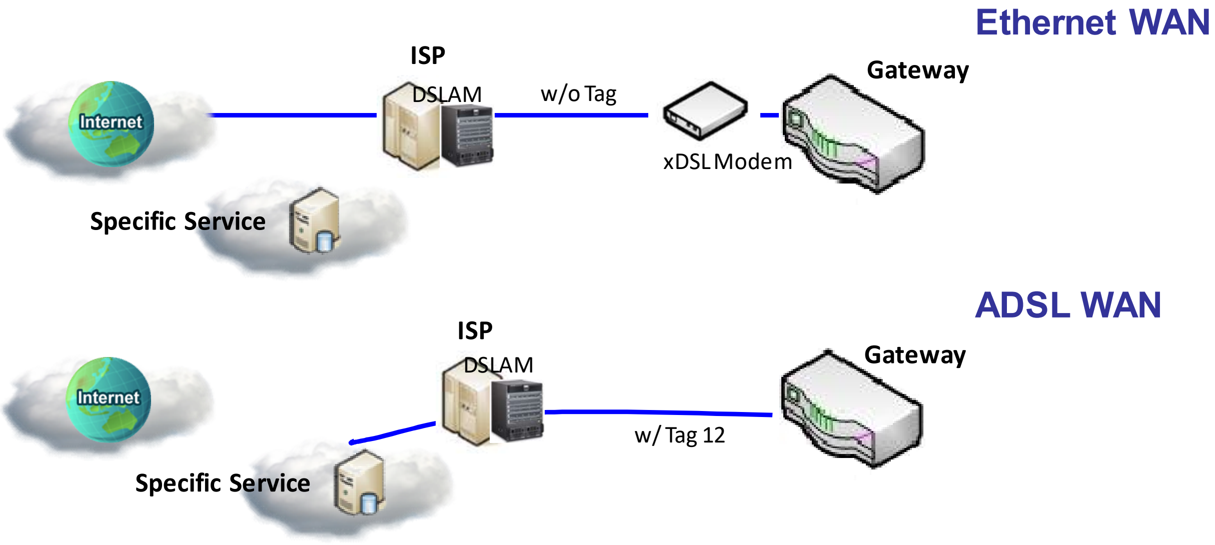
- **VLAN Tagging**

Sometimes, your ISP required a VLAN tag to be inserted into the WAN packets from Gateway for specific services. Ensure to specify it in the WAN physical interface. Please be noted that only Ethernet and ADSL physical interfaces support the feature.

As an example (just for an example, your device may not have an ADSL WAN), you can setup WAN-

1 without VLAN Tagging by using Ethernet WAN interface for your Intranet to access the Internet. In addition, you also can setup WAN-2 with VLAN Tagging (Tag ID 12) using ADSL WAN interface for your Intranet to access specific service in ISP. Following table list the physical interface configuration for these two WAN interfaces, and their scenarios are shown in the following diagram.

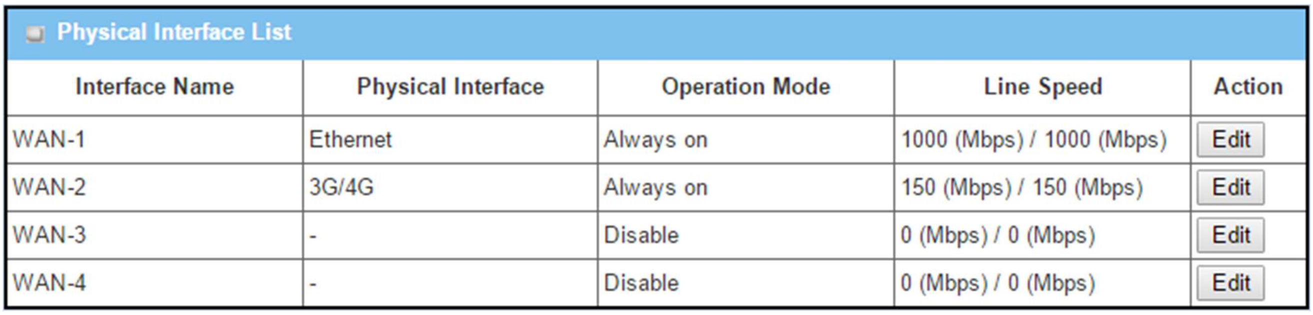
Configuration Path	[Physical Interface]-[Interface Configuration (WAN-n)], n=1, 2	
Interface Name	WAN-1	WAN-2
Physical Interface	***Ethernet***	***ADSL***
Operation Mode	***Always on***	***Always on***
Line Speed	***100Mbps / 100Mbps***	***2Mbps / 22Mbps***
VLAN Tagging	***□Enable***	***■Enable 12***



P.s. 3G/4G or USB 3G/4G can't carry any VLAN tag in communication packets

Physical Interface Setting

The Physical Interface allows user to setup the physical WAN interface and to adjust WAN’s behavior. Note: Numbers of available WAN Interfaces can be different for the purchased gateway.



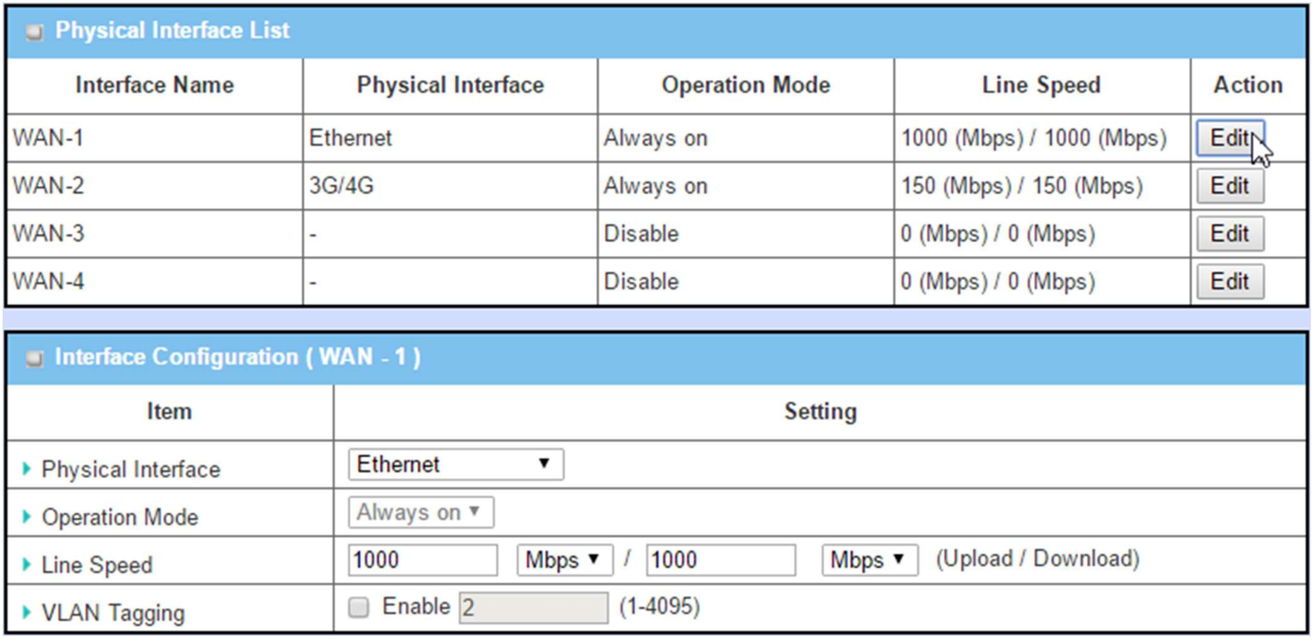
Physical Interface List

Interface Name	Physical Interface	Operation Mode	Line Speed	Action
WAN-1	Ethernet	Always on	1000 (Mbps) / 1000 (Mbps)	Edit
WAN-2	3G/4G	Always on	150 (Mbps) / 150 (Mbps)	Edit
WAN-3	-	Disable	0 (Mbps) / 0 (Mbps)	Edit
WAN-4	-	Disable	0 (Mbps) / 0 (Mbps)	Edit

Go to Basic Network>WAN > Physical Interface tab.

Configure Physical Interface Setting

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



Physical Interface List

Interface Name	Physical Interface	Operation Mode	Line Speed	Action
WAN-1	Ethernet	Always on	1000 (Mbps) / 1000 (Mbps)	Edit
WAN-2	3G/4G	Always on	150 (Mbps) / 150 (Mbps)	Edit
WAN-3	-	Disable	0 (Mbps) / 0 (Mbps)	Edit
WAN-4	-	Disable	0 (Mbps) / 0 (Mbps)	Edit

Interface Configuration (WAN - 1)

Item	Setting
Physical Interface	Ethernet ▾
Operation Mode	Always on ▾
Line Speed	1000 Mbps ▾ / 1000 Mbps ▾ (Upload / Download)
VLAN Tagging	□ Enable 2 (1-4095)

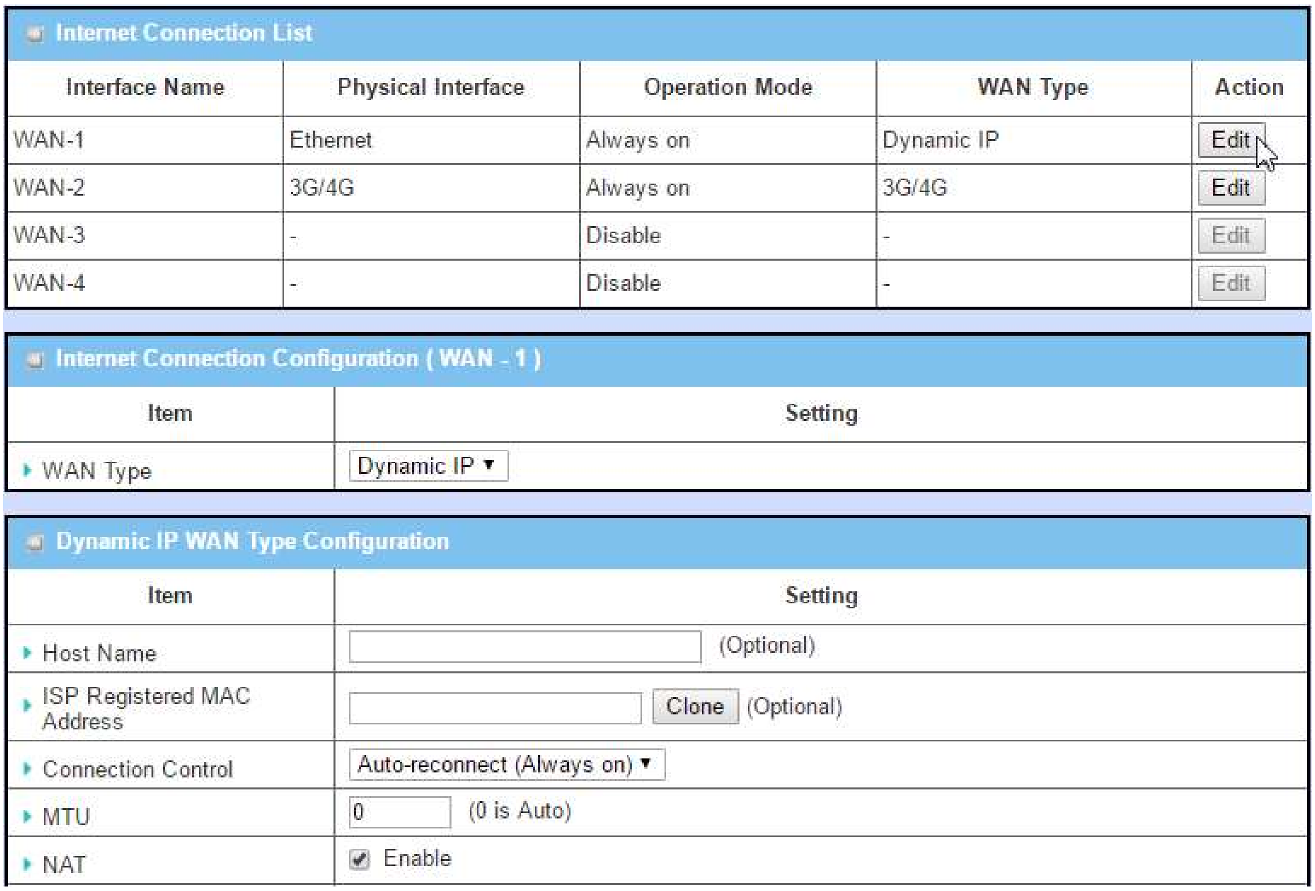
Interface Configuration		
Item	Value setting	Description
Physical Interface	1. A Must fill setting 2. WAN-1 is the primary interface and is factory set to Always on.	Select Ethernet or 3G/4G for WAN-2. In this example WAN-2 is been edited. Depending on the router model, **Disable** and **Failover** options will be available only to multiple WAN gateway. WAN-2 and WAN-3 interfaces are only available to multiple WAN gateway.
Operation Mode	A Must fill setting	Define the operation mode of the interface. Select **Always on** to make this WAN always active. Select **Disable** to disable this WAN interface. Select **Failover** to make this WAN a Failover WAN when the primary or the secondary WAN link failed. Then select the primary or the existed secondary WAN interface to switch Failover from. To failover seamlessly, check **Seamless** box. This failover WAN will keep connected to the network (i.e. 3G/4G network) but no traffic will be transmitted through it until failover happens. If **Seamless** box is unchecked, failover WAN will begin to initiate a connection request to the network (i.e. the nearest 3G/4G base station) when failover occurs. During failover period, users may notice a period of connection time. (Note: for WAN-1, only **Always on** option is available.)
Line Speed	A Must fill setting	Define the upload and download bandwidth for the WAN. The actual bandwidth will also be affected if the **Priority** is specified in Load Balance Strategy. Refer to **Basic Network > WAN & Uplink > Load Balance** tab if your device supports Load Balance function.
VLAN Tagging	Optional setting	Check **Enable** box to enter tag value provided by your ISP. Otherwise uncheck the box.

3.1.3 Internet Setup

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

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

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



Internet Connection List

Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet	Always on	Dynamic IP	Edit
WAN-2	3G/4G	Always on	3G/4G	Edit
WAN-3	-	Disable	-	Edit
WAN-4	-	Disable	-	Edit

Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	Dynamic IP ▾

Dynamic IP WAN Type Configuration

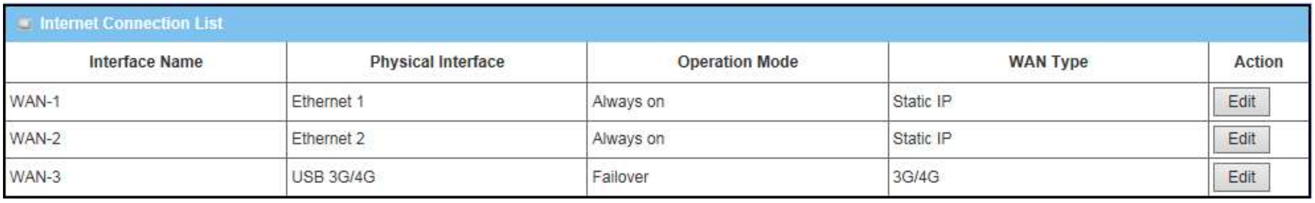
Item	Setting
Host Name	(Optional)
ISP Registered MAC Address	Clone (Optional)
Connection Control	Auto-reconnect (Always on) ▾
MTU	0 (0 is Auto)
NAT	☑ Enable

The contents, as shown in above screenshot, may vary depending on the model you purchased.

Internet Connection List

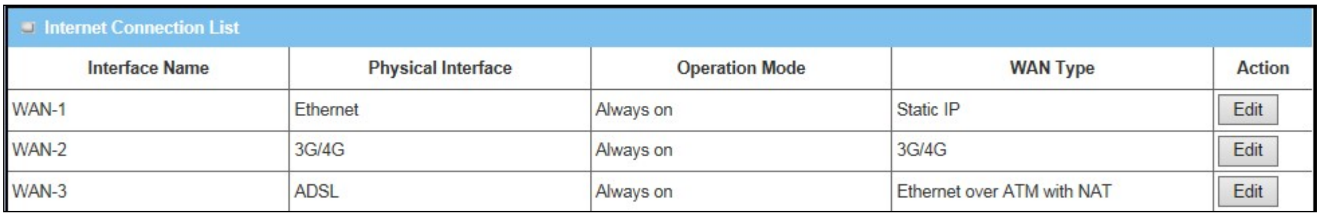
The Internet Connection List shows the WAN connection profiles of all WAN interfaces in the gateway device, including interface name, the kinds of physical interface, their operation mode and WAN connection type. There is one "Edit" button for each WAN interface to let you configure its Internet connection. Please see "Internet Connection Configuration" section beneath. Following are some "Internet Connection List" window examples for different gateway products.

SDE852AM-00001 example



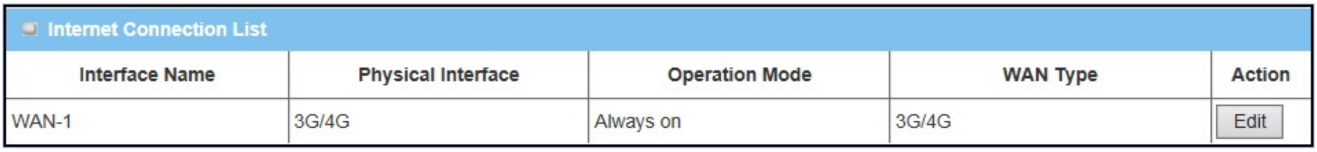
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet 1	Always on	Static IP	Edit
WAN-2	Ethernet 2	Always on	Static IP	Edit
WAN-3	USB 3G/4G	Failover	3G/4G	Edit

IOG761AM-0TDA1 example



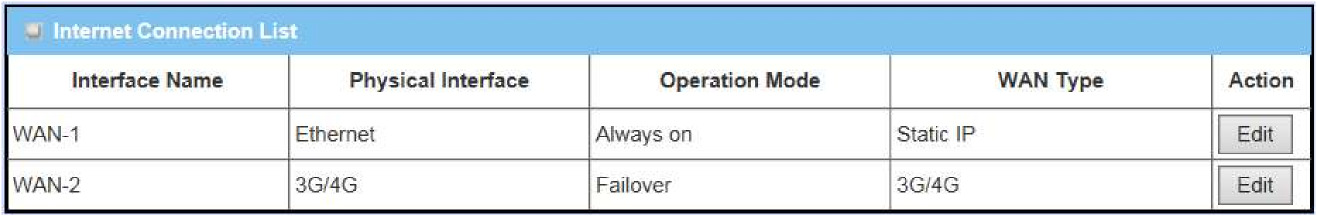
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet	Always on	Static IP	Edit
WAN-2	3G/4G	Always on	3G/4G	Edit
WAN-3	ADSL	Always on	Ethernet over ATM with NAT	Edit

ODG761AM-0T1 example



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

BDG761AM-0T1 example



Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet	Always on	Static IP	Edit
WAN-2	3G/4G	Failover	3G/4G	Edit

The contents of "Physical Interface List", as shown in above screenshot, may vary depending on the model you purchased.

- **Interface Name**
  The logic name of WAN interfaces is identified by “WAN-1”, “WAN-2”, …, and so on.

- **Physical Interface**

  This device is equipped with some kinds of WAN Interfaces. Please refer to **[Basic Network]-[WAN & Uplink]-[Physical Interface]** section.

- **Operation Mode**

  It is "Always on", "Failover" or "Disable". Please refer to **[Basic Network]-[WAN & Uplink]-[Physical Interface]** section.

- **WAN Type**

  The supported WAN types for each WAN interface depend on the kind of interface. Following are all kinds of physical interfaces and their supported WAN types.

  ✧ Ethernet interface: A fixed line ISP that provides xDSL or cable modem for you to setup the WAN connection.

  - Static IP Address WAN type: Select this option if ISP provides a fixed IP address to you. You will need to enter in the IP address, subnet mask, and gateway address, provided to you by your ISP.
  - Dynamic IP Address WAN type: You may choose this WAN type if you connects a cable modem or a fiber (VDSL modem) for Internet connection. The assigned IP address for the WAN interface by a DHCP server may be different every time.
  - PPP over Ethernet WAN type: As known as PPPoE. This WAN type is widely used for ADSL connection.
  - PPTP WAN type: This WAN type is more popular in Russia.
  - L2TP WAN type: This WAN type is more popular in Israel.

  ✧ 3G/4G or USB 3G/4G interface[8]: The ISP is a mobile operator that can provide LTE, HSPA+, HSPA, WCDMA, EDGE, GPRS data services.

  - 3G/4G WAN type: If you have subscribed 3G/4G data services from a mobile operator. You can setup a 3G/4G WAN connection by using the gateway device. This gateway can support LTE/3G/2G data connection based on mobile system specifications that mobile

[7] Please check the product specification for the supporting of 3G/4G capability in WAN & Uplink section.

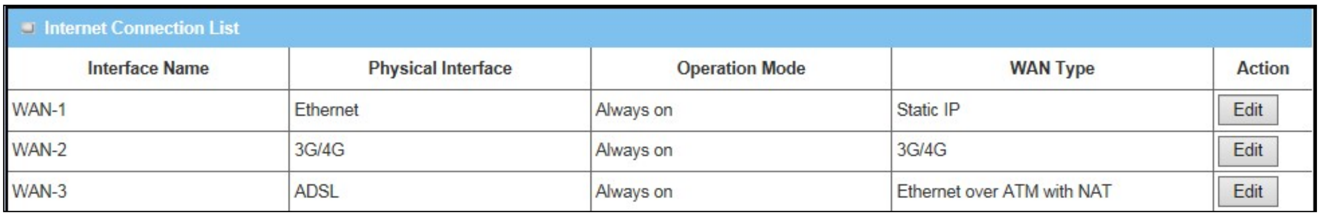
operator provides. In addition, if your 3G data plan is not with a flat rate, it’s recommended to set Connection Control mode to Connect-on-Demand or Manually.

- ✧ ADSL interface: Asymmetric digital subscriber line (ADSL) is a type of digital subscriber line (DSL) technology, a data communications technology that enables faster data transmission over copper telephone lines than a conventional voiceband modem can provide. Use a RJ11 cable to connect the ADSL port of gateway device to the DSLAM at ISP, and connect further to a conventional Internet Protocol network.
  - ■ Ethernet over ATM with NAT WAN type: The option is intended to be used in implementations which use ATM networks to carry multiprotocol traffic among hosts, routers and bridges which are ATM end systems.
  - ■ IP over ATM WAN type: Select this option if ISP provides VPI/VCI, VC-based/LLC-based multiplexing, IP address, subnet mask, gateway address and DNS to you to setup an ADSL Internet connection.
  - ■ PPPoE (ADSL) WAN type: Select this option if your ISP requires you to use a PPPoE connection for accessing Internet. This option is typically used for DSL services.
  - ■ PPP over ATM WAN type: The Point-to-Point Protocol over ATM (PPPoA) is a network protocol for encapsulating PPP frames in AAL5. It is used mainly with DSL carrier.
  - ■ RFC 1483 Bridged WAN type: RFC1483 Bridged is for carrying connectionless network interconnected traffic over an ATM network. Bridging performs higher-layer protocol multiplexing implicitly by ATM virtual circuits.

Internet Connection Configuration

To setup the Internet connection profile for each physical WAN interface, you must specify its WAN Type for the interface and then define related parameters for the WAN type. So the gateway will connect to ISP that you subscribe to, and ISP further links the connection to the Internet.

WAN Type varies from interface to interface. Based on physical interface, the supported WAN Types and related settings are shown as below. In the example bellow, the IOG761AM-0TDA1 is used to show the Internet connection configurations as it includes most kinds of physical interfaces.



Internet Connection List

Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet	Always on	Static IP	Edit
WAN-2	3G/4G	Always on	3G/4G	Edit
WAN-3	ADSL	Always on	Ethernet over ATM with NAT	Edit

- **Ethernet interface:** there are Static IP, Dynamic IP, PPPoE, PPTP and L2TP WAN types.
    - Static IP Address WAN Type: Settings include WAN IP Address, WAN Subnet Mask, WAN Gateway, Primary DNS, Secondary DNS, MTU, NAT, Network Monitoring, IGMP and WAN IP Alias.
    - Dynamic IP Address WAN Type: Settings include Host Name, ISP registered MAC Address, Connection Control, Maximum Idle Time, MTU, NAT, Network Monitoring, IGMP and WAN IP Alias.
    - PPPoE WAN Type: Settings include IPv6 Dual Stack, PPPoE Account & Password, Primary DNS / Secondary DNS, Connection Control, Maximum Idle Time, Service Name / Assigned IP Address, MTU, NAT, Network Monitoring, IGMP and WAN IP Alias.
    - PPTP WAN Type: Settings include IP Mode, Server IP / Name, PPTP Account & Password, Connection ID, Connection Control, Maximum Idle Time, Service Name / Assigned IP Address, MTU, MPPE, NAT, Network Monitoring, IGMP and WAN IP Alias.
    - L2TP WAN Type: Settings include IP Mode, Server IP / Name, L2TP Account & Password, Connection Control, Maximum Idle Time, MTU, MPPE, NAT, Network Monitoring, IGMP and WAN IP Alias.
- **3G/4G or USB 3G/4G interface:** there is only 3G/4G WAN type.
    - 3G/4G WAN Type: Settings include Dial-up Profile, APN, PIN Code, Dialed Number, Account & Password, Authentication, Primary DNS, Secondary DNS, Connection Control, Maximum Idle Time, Time Schedule, MTU, NAT, Network Monitoring and IGMP.
- **ADSL interface:** there are Ethernet over ATM with NAT, IP over ATM, PPPoE (ADSL), PPP over ATM and RFC 1483 Bridged WAN types.
    - Ethernet over ATM with NAT and IP over ATM WAN Types: Settings include IP Mode, Host Name, ISP Registered MAC Address, Connection Control, MTU, NAT, Data Encapsulation, VPI Number, VCI Number, Schedule Type, Network Monitoring, IGMP and WAN IP Alias.
    - PPPoE (ADSL) and PPP over ATM WAN Types: Settings include PPPoE Account & Password, Primary DNS, Secondary DNS, Connection Control, Service Name, Assigned IP Address, MTU,

NAT, Data Encapsulation, VPI Number, VCI Number, Schedule Type, Network Monitoring, IGMP and WAN IP Alias.

- RFC 1483 Bridged WAN type: Settings include Data Encapsulation, VPI Number, VCI Number, Schedule Type, Network Monitoring, IGMP and WAN IP Alias.

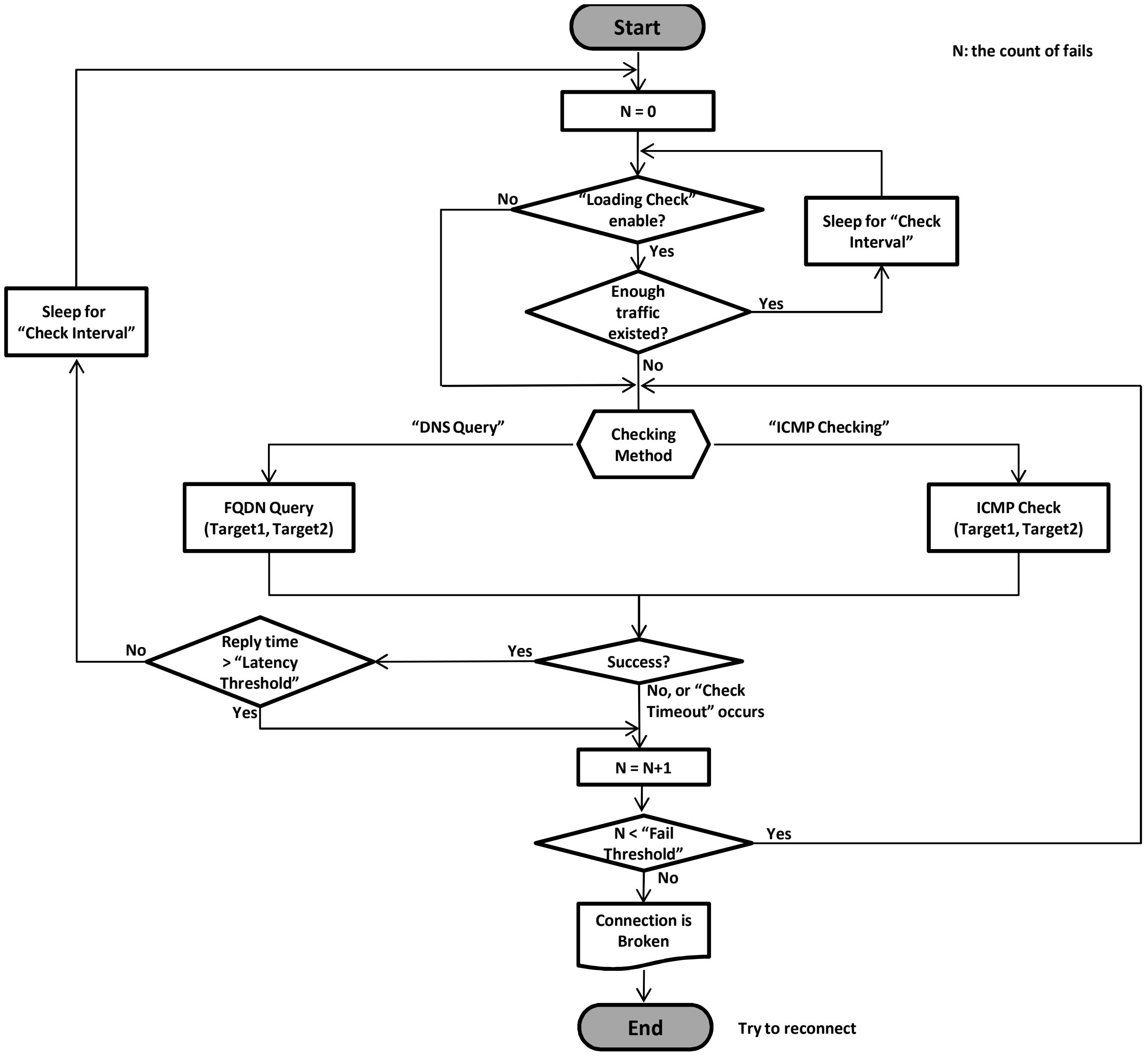
There are some common and important configuration parameters common to all WAN Type as listed below.

- **Network Monitoring**

The gateway supports failover function and the function must depend on the correct decision when a connection is down. Some parameters are used in the decision process.

- **DNS Query / ICMP Checking**: either one is used to check alive for a WAN connection.
- **Loading Checking:** The response time of replied keep-alive packets may increase when WAN bandwidth is fully occupied. To avoid keep-alive feature work abnormally, enable this option will stop sending keep-alive packets when there are continuous incoming and outgoing data packets passing through WAN connection.
- **Check Interval:** Indicate how often to send keep-alive packet.
- **Check Timeout:** Set allowance of time period to receive response of keep-alive packet. If this gateway doesn’t receive response within this time period, this gateway will acknowledge this keep alive is failed.
- **Latency Threshold:** Set acceptance of response time. This gateway will record this keep-alive check is failed if the response time of replied packet is longer than this setting.
- **Fail Threshold:** Times of failed checking. This WAN connection will be recognized as broken if the times of continuous failed keep-alive checking equals to this value.
- **Target1/Target2:** Set host that is used for keep alive checking. It can be DNS1, DNS2, default Gateway, or other host that you need to input IP address manually.

The decision flow chart of keep-alive checking for a WAN connection is shown as below.



- **Connection Control**

There are three ways for connection control, "Auto-reconnect (Always on)", "Dial-on-demand" and "Manually".

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

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

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

Please be noted, if the WAN interface serves as the primary one for another WAN interface in Failover role, the Connection Control parameter will not be available to you to configure as the system must set it to "Auto-reconnect (Always on)".

➢ **Auto-reconnect / Dial-on-demand / Manually Scenario**:

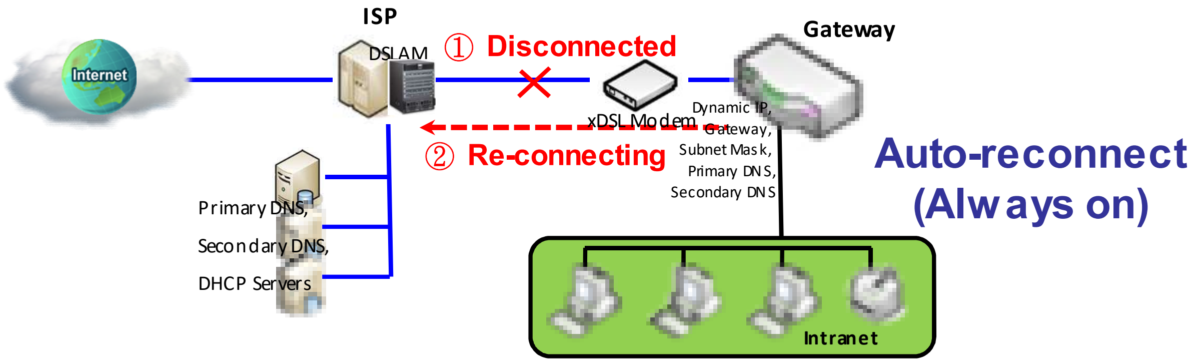
As an example, WAN-1, WAN-2 and WAN-3 are all Ethernet interfaces with "Always on" operation mode. Their WAN Type is set to "Dynamic IP" but with different Connection Control approaches. WAN-1 uses "Auto-reconnect (Always on)", WAN-2 uses "Dial-on-demand" and WAN-3 uses "Manually". Following 3 tables list the parameter configuration for these three WAN interfaces.

Configuration Path	[Physical Interface]-[Interface Configuration (WAN-n)] , n=1,2,3		
Interface Name	WAN-1	WAN-2	WAN-3
Physical Interface	***Ethernet***	***Ethernet***	***Ethernet***
Operation Mode	***Always on***	***Always on***	***Always on***
Line Speed	***100Mbps / 100Mbps***	***100Mbps / 100Mbps***	***100Mbps / 100Mbps***

Configuration Path	[Internet Setup]-[Internet Connection Configuration (WAN-n)], n=1, 2, 3		
Interface Name	WAN-1	WAN-2	WAN-3
WAN Type	***Dynamic IP***	***Dynamic IP***	***Dynamic IP***

Configuration Path	[Internet Setup]-[Dynamic IP WAN Type Configuration]		
Interface Name	WAN-1	WAN-2	WAN-3
Connection Control	***Auto-reconnect (Always on)***	***Dial-on-demand***	***Manually***

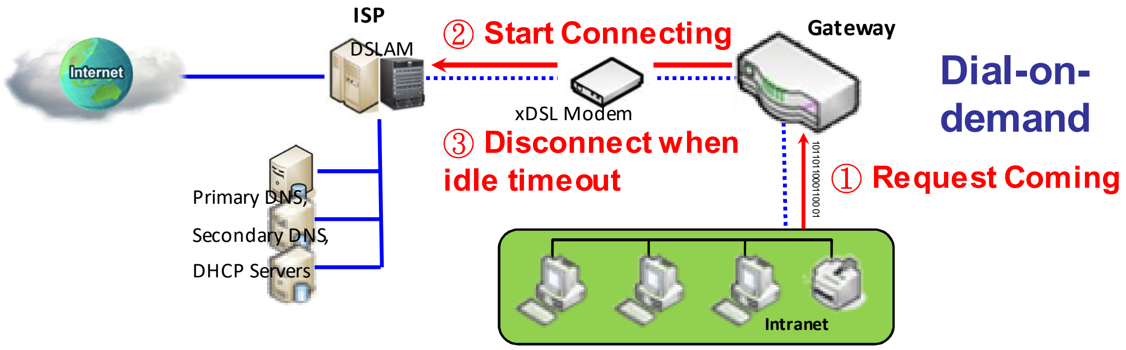
System keeps alive the WAN connection whose connection control is "Auto-reconnect (Always on)". After system booting up, the connection will be alive and once the connection is down, system will re-connect it. The scenario is shown in following diagram.



Its steps are:

Pre-state: After system booting up, system tries to let the WAN connection be alive.
S 1: When system discovers the WAN connection is failed.
S 2: System starts to re-connect the WAN connection till connect successfully as same as Pre-state.

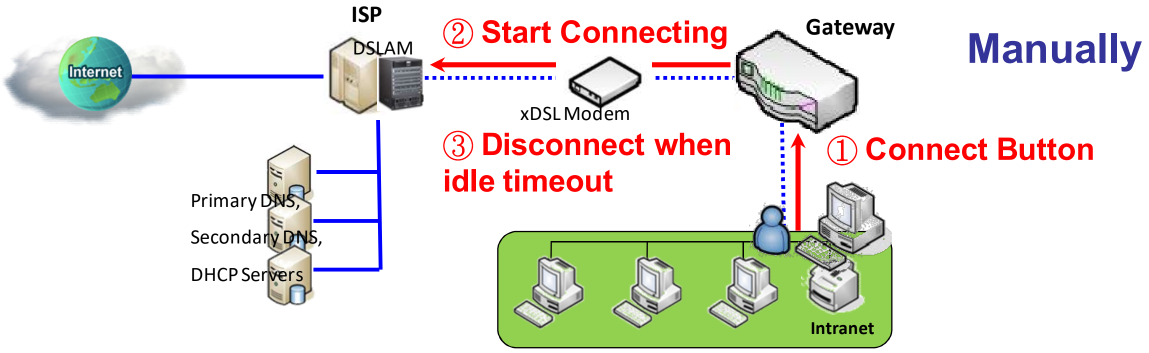
In the "Dial-on-demand" scenario, system will not make the WAN connection until gateway receives an Internet accessing request from Intranet. And then the connection will keep alive only when there still is data transfer. If there is no data transfer for a period that is longer than the Maximum Idle Time, system will disconnect it and let the WAN connection go back to its initial state – disconnected. The scenario is shown in following diagram.



Its steps are:

Pre-state: After system booting up, the WAN connection is disconnected.
S 1: When an Internet accessing request is fed into the gateway from the Intranet.
S 2: System starts to make the WAN connection till connect successfully. Keep the connection alive only when there still is data transfer to the Internet.
S 3: If the WAN connection timeout, system will disconnect it and let it go back to Pre-state.

At last, for "Manually" scenario, system will not make the WAN connection until administrator click on the "Connect" button on the "Network Status" configuration window. Please refer to **[System]-[Network Status]** section. And then the connection will keep alive only when there still is data transfer. If there is no data transfer for a period that is longer than the Maximum Idle Time, system will disconnect it and let the WAN connection go back to its initial state –disconnected. The scenario is shown in following diagram.



Its steps are:

Pre-state: After system booting up, the WAN connection is disconnected.

S 1: When administrator click on the "Connect" button on the "Network Status" configuration window.

S 2: System starts to make the WAN connection till connect successfully. Keep the connection alive only when there still is data transfer to the Internet.

S 3: If the WAN connection timeout, system will disconnect it and return to its Pre-state.

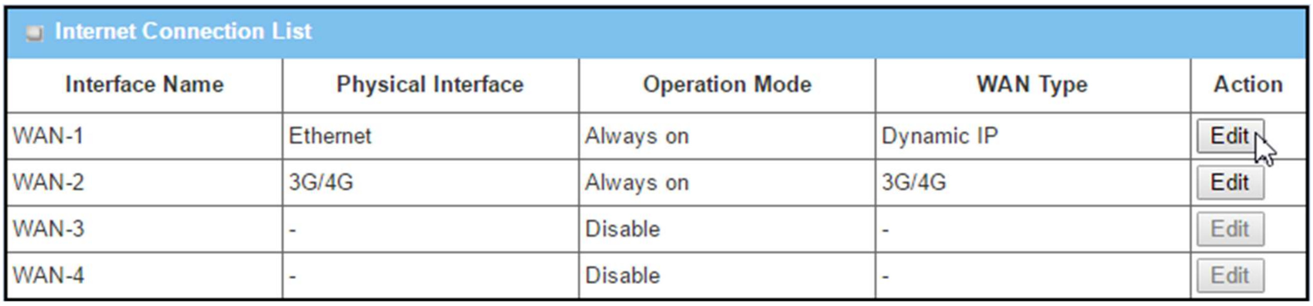
Internet Setup Setting

Internet Setup allows user to setup WAN connection of the gateway. Depending on the model of the device, there are Ethernet, ADSL, 3G/4G WAN connection interfaces. This section shows the type of WAN and the numbers of WAN interfaces are supported by your device.

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

Go to Basic Network>WAN > Internet Setup tab

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



Internet Connection List

Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet	Always on	Dynamic IP	Edit
WAN-2	3G/4G	Always on	3G/4G	Edit
WAN-3	-	Disable	-	Edit
WAN-4	-	Disable	-	Edit

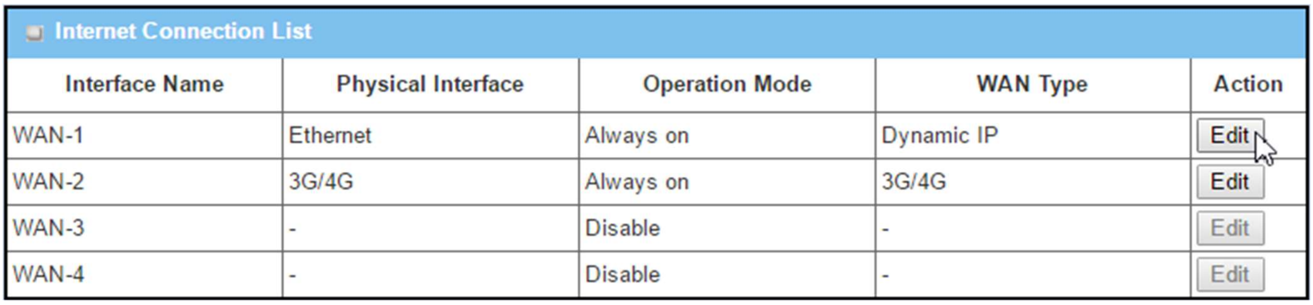
Internet Connection List		
Item	**Value setting**	**Description**
Interface Name	N/A	Shows the name of WAN interface.
Physical Interface	N/A	Physical Interfaces (i.e. Ethernet, 3G, 4G) shows the type of interface configured to map with **Interface Name** (WAN-1, WAN-2, WAN-3, and etc.).
Operation Mode	N/A	**Operation Mode** shows the current setting of Connection Control mode of WAN interface to keep WAN connection. ● **Auto-reconnect (Always on)** ● **Connect-on-demand** ● **Connect Manually**
WAN Type	N/A	**WAN Type** shows the type of connection method to your SERVICE PROVIDER. Depending on the device model, the following WAN connection types are supported. • **Ethernet:** Static IP | Dynamic IP |PPPoE | PPTP | L2TP • **ADSL:** Ethernet over ATM with NAT | IP over ATM | PPPoE (ADSL) | PPP over ATM • **3G/4G**

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

Internet Setup – Ethernet WAN

If the device connects to Internet through Ethernet WAN port, this section will help you to complete Ethernet WAN connection setup.

Go to Basic Network > WAN & Uplink > Internet Setup tab.

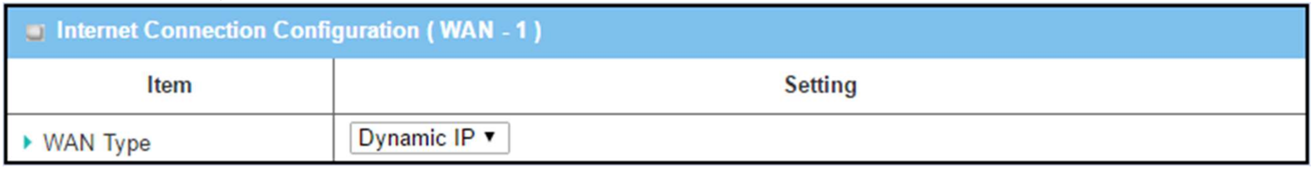


Internet Connection List

Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet	Always on	Dynamic IP	Edit
WAN-2	3G/4G	Always on	3G/4G	Edit
WAN-3	-	Disable	-	Edit
WAN-4	-	Disable	-	Edit

Configure Ethernet WAN Setting

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

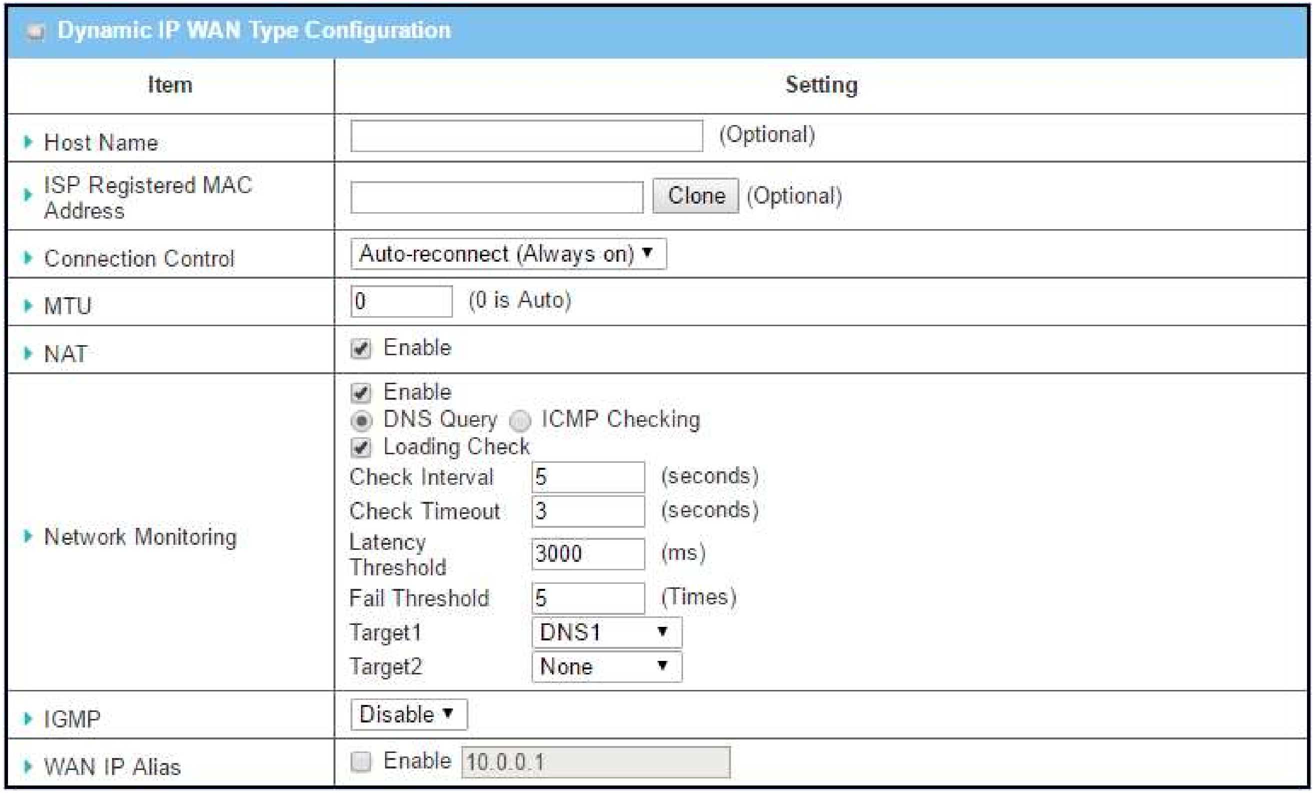


Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	Dynamic IP ▾

Internet Connection Configuration		
Item	**Value setting**	**Description**
WAN Type	1. A Must filled setting 2. Dynamic IP is set by default	From the dropdown box, select Internet connection method for Ethernet WAN Connection. Detail settings are described in the next few pages. • **Dynamic IP** • **Static IP** • **PPPoE** • **PPTP** • **L2TP**

Dynamic IP (Ethernet WAN)



Dynamic IP WAN Type Configuration

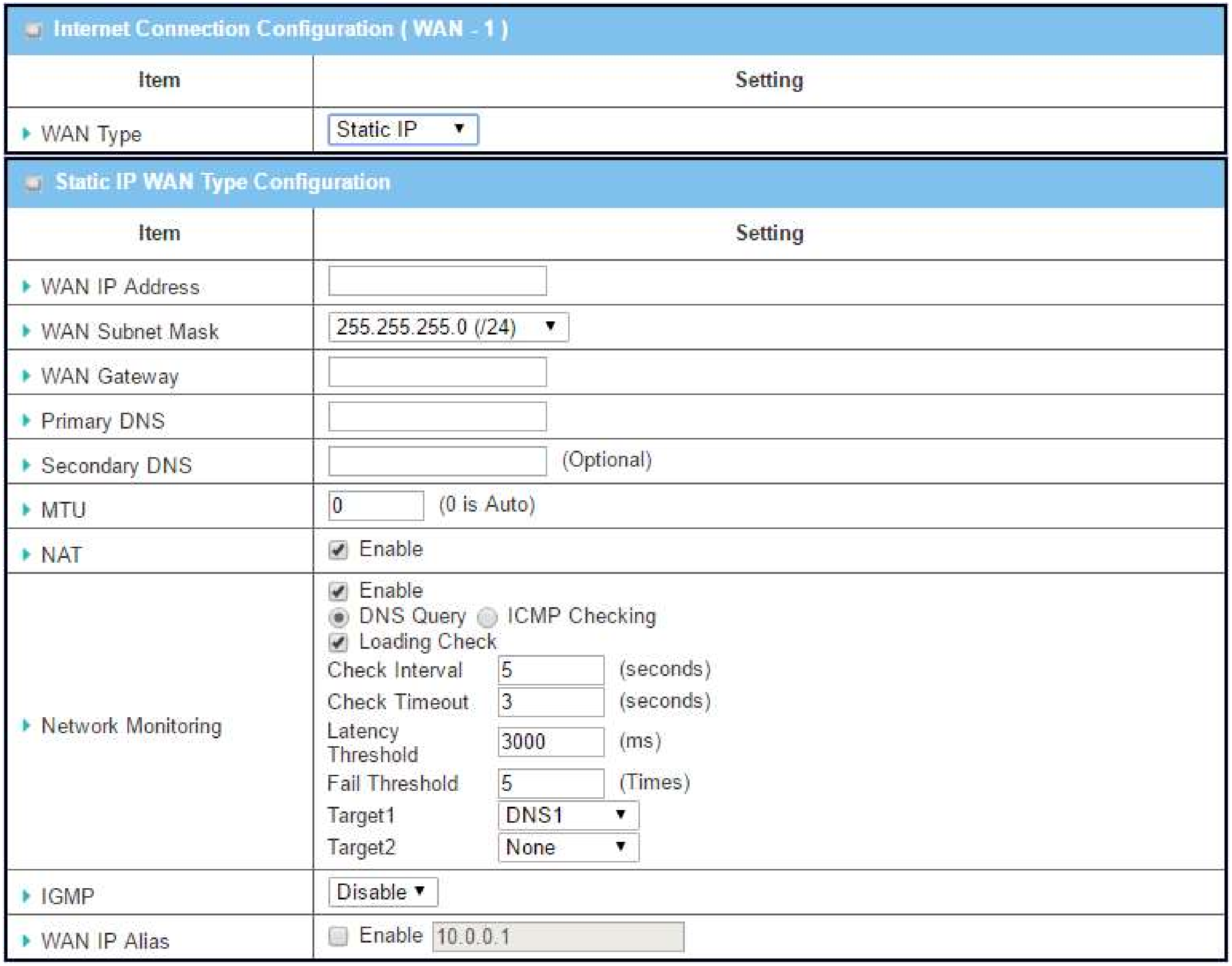
Item	Setting
Host Name	(Optional)
ISP Registered MAC Address	Clone (Optional)
Connection Control	Auto-reconnect (Always on)
MTU	0 (0 is Auto)
NAT	☑ Enable
Network Monitoring	☑ Enable ● DNS Query ○ ICMP Checking ☑ Loading Check Check Interval 5 (seconds) Check Timeout 3 (seconds) Latency Threshold 3000 (ms) Fail Threshold 5 (Times) Target1 DNS1 Target2 None
IGMP	Disable
WAN IP Alias	□ Enable 10.0.0.1

Dynamic IP WAN Type Configuration		
Item	**Value setting**	**Description**
Host Name	An optional setting	Enter the host name provided by your Service Provider.
ISP Registered MAC Address	An optional setting	Enter the MAC address that you have registered with your service provider. Or Click the **Clone** button to clone your PC's MAC to this field. Usually this is the PC's MAC address assigned to allow you to connect to Internet.
Connection Control	A Must filled setting	There are three connection modes. • **Auto-reconnect (Always on)** enables the router to always keep the Internet connection on. • **Connect-on-demand** enables the router to automatically re-establish Internet connection as soon as user attempts to access the Internet. Internet connection will be disconnected when it has been inactive for a specified idle time. • **Connect Manually** allows user to connect to Internet manually**.** Internet connection will be inactive after it has been inactive for specified idle time.
MTU	1. A Must filled setting 2. **Auto** (value zero) is set by default	**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.

	3. Manual set range 1200~1500	
NAT	1. An optional setting 2. NAT is enabled by default	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
Network Monitoring	1. An optional setting 2. Enabled by default	When the Network Monitoring feature is enabled, the gateway will use DNS Query or ICMP to periodically check Internet connection – connected or disconnected. ● Choose either **DNS Query** or **ICMP Checking** to detect WAN link. With **DNS Query,** the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. With **ICMP Checking,** the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2. ● **Loading Check** Enable Loading Check allows the router to ignore unreturned DNS Queries or ICMP requests when WAN bandwidth is fully occupied. This is to prevent false link-down status. ● **Check Interval** defines the transmitting interval between two DNS Query or ICMP checking packets. ● **Check Timeout** defines the timeout of each DNS query/ICMP. ● **Latency Threshold** defines the tolerance threshold of responding time. ● **Fail Threshold** specifies the detected disconnection before the router recognize the WAN link down status. Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged. ● **Target1** (**DNS1** set by default**)** specifies the first target of sending DNS query/ICMP request. ■ **DNS1**: set the primary DNS to be the target. ■ **DNS2**: set the secondary DNS to be the target. ■ **Gateway**: set the Current gateway to be the target. ■ **Other Host**: enter an IP address to be the target. ● **Target2** (**None** set by default**)** specifies the second target of sending DNS query/ICMP request. ■ **None**: to disable **Target2.** ■ **DNS1**: set the primary DNS to be the target. ■ **DNS2**: set the secondary DNS to be the target. ■ **Gateway**: set the Current gateway to be the target. ■ **Other Host**: enter an IP address to be the target.
IGMP	1. A Must filled setting 2. Disable is set by default	Enable IGMP (Internet Group Management Protocol) would enable the router to listen to IGMP packets to discover which interfaces are connected to which device. The router uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.
WAN IP Alias	1. An optional setting 2. Box is unchecked by	Enable **WAN IP Alias** then enter the IP address provided by your service provider.

	default	**WAN IP Alias** is used by the device router and is treated as a second set of WAN IP to provide dual WAN IP address to your LAN network.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

Static IP (Ethernet WAN)



Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	Static IP ▾

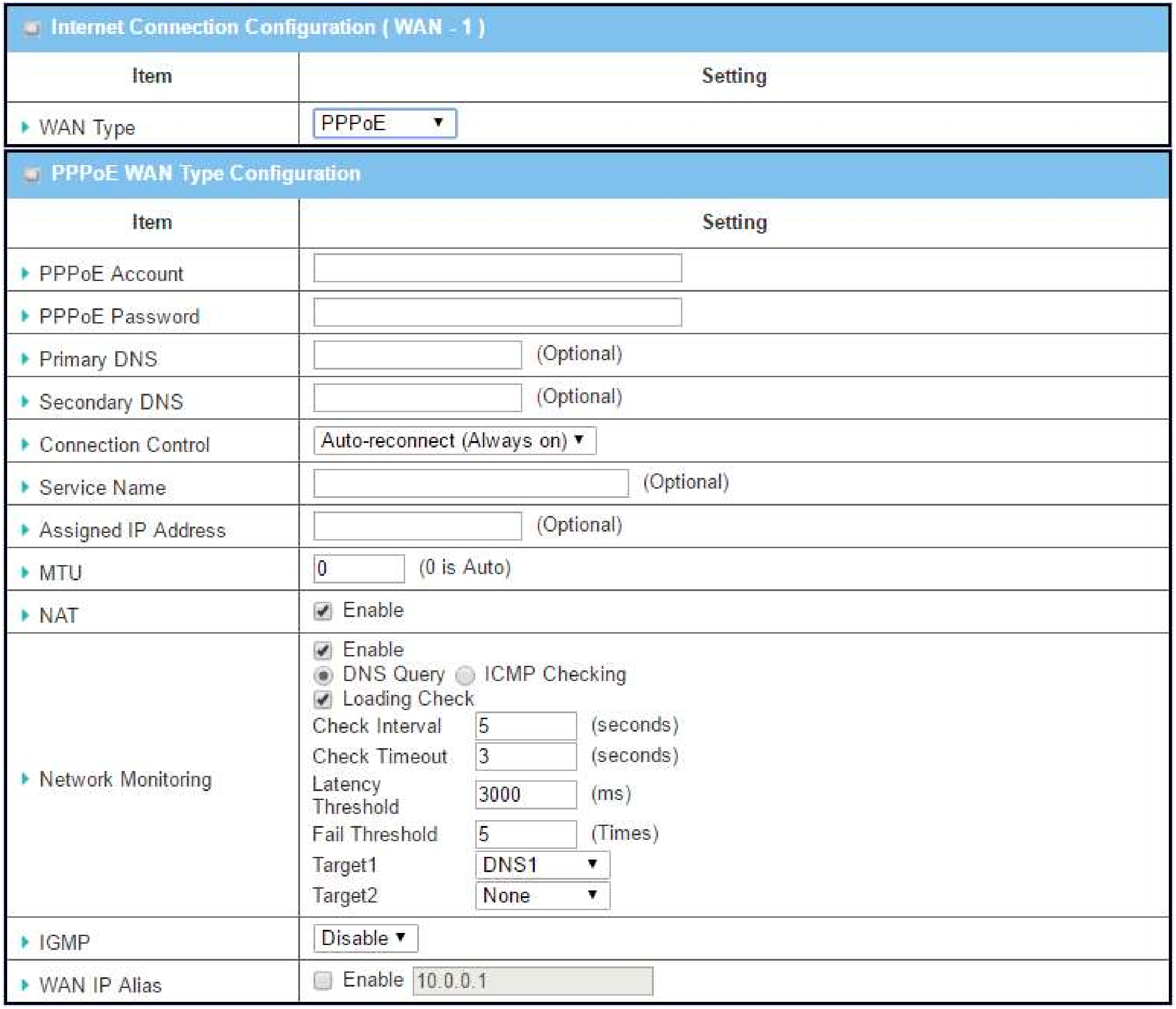
Static IP WAN Type Configuration

Item	Setting
WAN IP Address	
WAN Subnet Mask	255.255.255.0 (/24) ▾
WAN Gateway	
Primary DNS	
Secondary DNS	(Optional)
MTU	0 (0 is Auto)
NAT	☑ Enable
Network Monitoring	☑ Enable ● DNS Query ○ ICMP Checking ☑ Loading Check Check Interval 5 (seconds) Check Timeout 3 (seconds) Latency Threshold 3000 (ms) Fail Threshold 5 (Times) Target1 DNS1 ▾ Target2 None ▾
IGMP	Disable ▾
WAN IP Alias	□ Enable 10.0.0.1

Static IP WAN Type Configuration		
Item	**Value setting**	**Description**
WAN IP Address	A Must filled setting	Enter the WAN IP address given by your Service Provider
WAN Subnet Mask	A Must filled setting	Enter the WAN subnet mask given by your Service Provider
WAN Gateway	A Must filled setting	Enter the WAN gateway IP address given by your Service Provider
Primary DNS	A Must filled setting	Enter the primary WAN DNS IP address given by your Service Provider
Secondary DNS	An optional setting	Enter the secondary WAN DNS IP address given by your Service Provider
MTU	1. A Must filled setting	**MTU** refers to Maximum Transmission Unit. It specifies the largest

	2. Auto (value zero) is set by default	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. Box is checked by default	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable.
Network Monitoring	1. An optional setting 2. Box is checked by default	When the Network Monitoring feature is enabled, the router will use DNS Query or ICMP to periodically check Internet connection – connected or disconnected. For the configuration details, please refer to the description stated in Dynamic Ethernet WAN section.
IGMP	1. A Must filled setting 2. Disable is set by default	Enable IGMP (Internet Group Management Protocol) would enable the router to listen to IGMP packets to discover which interfaces are connected to which device. The router uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.
WAN IP Alias	1. An optional setting 2. Box is unchecked by default	Enable **WAN IP Alias** then enter the IP address provided by your Service Provider. **WAN IP Alias** is used by the device router and is treated as a second set of WAN IP to provide dual WAN IP address to your LAN network.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

PPPoE (Ethernet WAN)



Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	PPPoE ▼

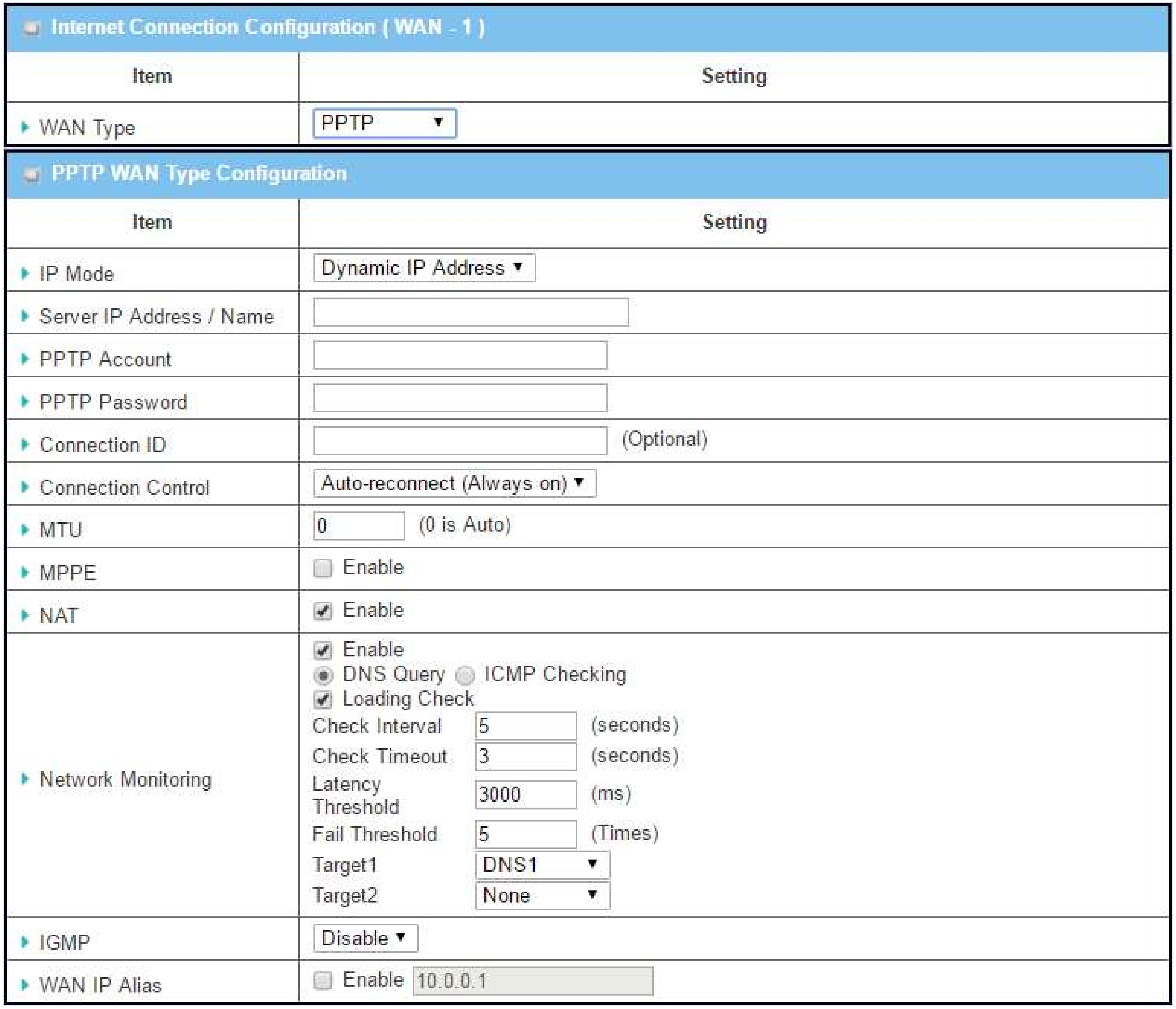
PPPoE WAN Type Configuration

Item	Setting
PPPoE Account	
PPPoE Password	
Primary DNS	(Optional)
Secondary DNS	(Optional)
Connection Control	Auto-reconnect (Always on) ▼
Service Name	(Optional)
Assigned IP Address	(Optional)
MTU	0 (0 is Auto)
NAT	☑ Enable
Network Monitoring	☑ Enable ● DNS Query ○ ICMP Checking ☑ Loading Check Check Interval 5 (seconds) Check Timeout 3 (seconds) Latency Threshold 3000 (ms) Fail Threshold 5 (Times) Target1 DNS1 ▼ Target2 None ▼
IGMP	Disable ▼
WAN IP Alias	□ Enable 10.0.0.1

PPPoE WAN Type Configuration		
Item	**Value setting**	**Description**
PPPoE Account	A Must filled setting	Enter the PPPoE User Name provided by your Service Provider.
PPPoE Password	A Must filled setting	Enter the PPPoE password provided by your Service Provider.
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.
Connection Control	1. A Must filled setting 2. Auto-reconnect is set by default 3. Default idle time is 600s	There are three connection modes. • **Auto-reconnect (Always on)** enables the router to always keep the Internet connection on. • **Connect-on-demand** enables the router to automatically re-establish Internet connection as soon as user attempts to access the Internet. Internet connection will be

		disconnected when it has been inactive for a specified idle time. - **Connect Manually** allows user to connect to Internet manually**.** Internet connection will be inactive after it has been inactive for specified idle time.
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 Service Provider.
MTU	1. A Must filled setting 2. Auto (value zero) is set by default	**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. Box is checked by default	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable.
Network Monitoring	1. An optional setting 2. Box is checked by default	When the Network Monitoring feature is enabled, the router will use DNS Query or ICMP to periodically check Internet connection – connected or disconnected. For the configuration details, please refer to the description stated in Dynamic Ethernet WAN section.
IGMP	1. A Must filled setting 2. Disable is set by default	Enable IGMP (Internet Group Management Protocol) would enable the router to listen to IGMP packets to discover which interfaces are connected to which device. The router uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.
WAN IP Alias	1. An optional setting 2. Box is unchecked by default	Enable **WAN IP Alias** then enter the IP address provided by your Service Provider. **WAN IP Alias** is used by the device router and is treated as a second set of WAN IP to provide dual WAN IP address to your LAN network.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

PPTP (Ethernet WAN)



Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	PPTP ▾

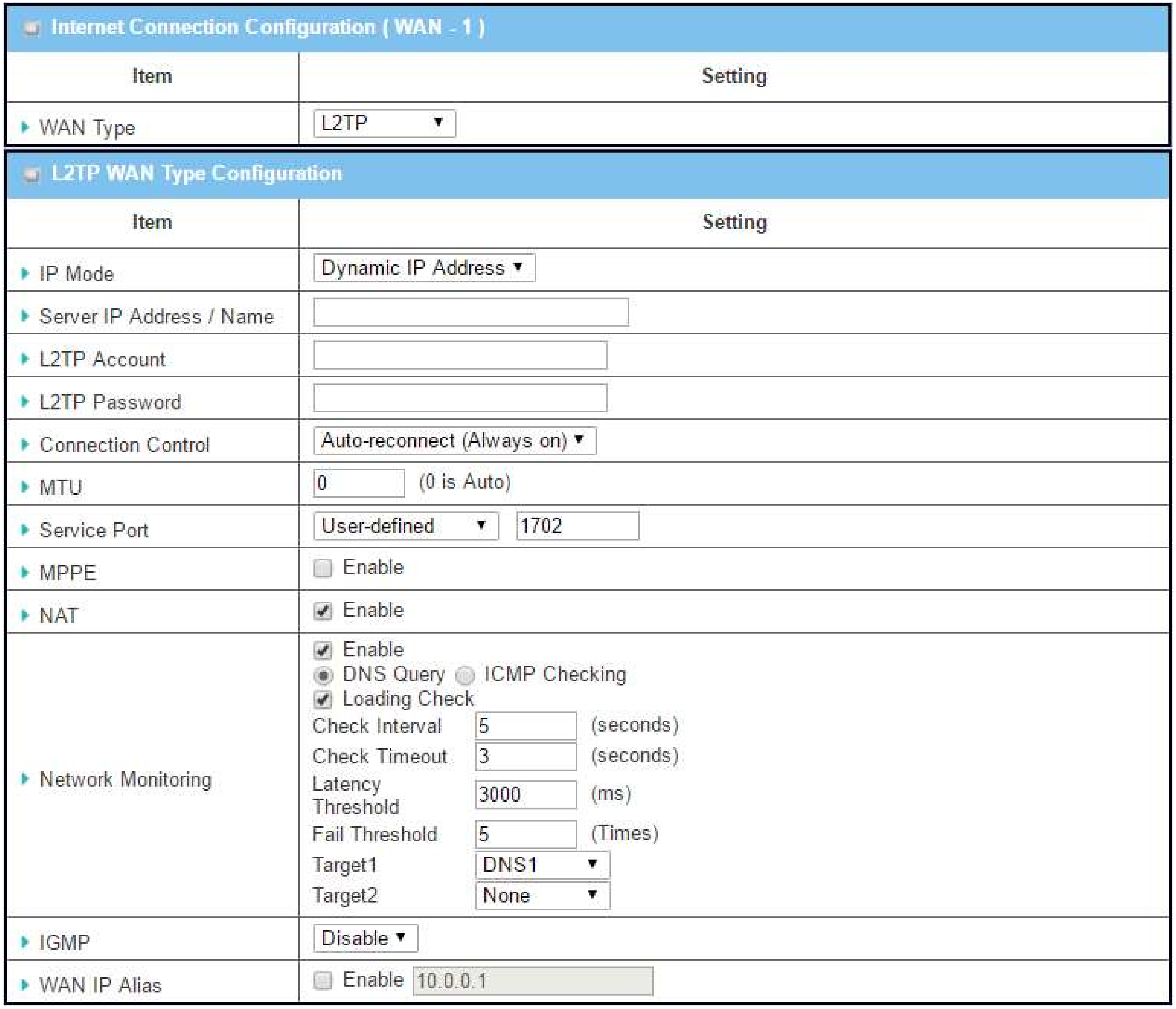
PPTP WAN Type Configuration

Item	Setting
IP Mode	Dynamic IP Address ▾
Server IP Address / Name	
PPTP Account	
PPTP Password	
Connection ID	(Optional)
Connection Control	Auto-reconnect (Always on) ▾
MTU	0 (0 is Auto)
MPPE	□ Enable
NAT	☑ Enable
Network Monitoring	☑ Enable ● DNS Query ○ ICMP Checking ☑ Loading Check Check Interval 5 (seconds) Check Timeout 3 (seconds) Latency Threshold 3000 (ms) Fail Threshold 5 (Times) Target1 DNS1 ▾ Target2 None ▾
IGMP	Disable ▾
WAN IP Alias	□ Enable 10.0.0.1

PPTP WAN Type Configuration		
Item	**Value setting**	**Description**
IP Mode	A Must filled setting	Select either Static or Dynamic IP address for PPTP Internet connection. ● When **Static IP Address** is selected, you will need to enter the **WAN IP Address**, **WAN Subnet Mask,** and **WAN Gateway**. ■ **WAN IP Address** (A Must filled setting)**:** Enter the WAN IP address given by your Service Provider. ■ **WAN Subnet Mask** (A Must filled setting)**:** Enter the WAN subnet mask given by your Service Provider. ■ **WAN Gateway** (A Must filled setting)**:** Enter the WAN gateway IP address given by your Service Provider. ● When **Dynamic IP** is selected, there are no above settings

		required.
Server IP Address/Name	A Must filled setting	Enter the PPTP server name or IP Address.
PPTP Account	A Must filled setting	Enter the PPTP username provided by your Service Provider.
PPTP Password	A Must filled setting	Enter the PPTP connection password provided by your Service Provider.
Connection ID	An optional setting	Enter a name to identify the PPTP connection.
Connection Control	A Must filled setting	There are three connection modes. • **Auto-reconnect (Always on)** enables the router to always keep the Internet connection on. • **Connect-on-demand** enables the router to automatically re-establish Internet connection as soon as user attempts to access the Internet. Internet connection will be disconnected when it has been inactive for a specified idle time. • **Connect Manually** allows user to connect to Internet manually**.** Internet connection will be inactive after it has been inactive for specified idle time.
MTU	1. A Must filled setting 2. Auto (value zero) is set by default	**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.
MPPE	An optional setting	Select **Enable** to enable MPPE **(**Microsoft Point-to-Point Encryption) security for PPTP connection.
NAT	1. An optional setting 2. Box is checked by default	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
Network Monitoring	1. An optional setting 2. Box is checked by default	When the Network Monitoring feature is enabled, the router will use DNS Query or ICMP to periodically check Internet connection – connected or disconnected. For the configuration details, please refer to the description stated in Dynamic Ethernet WAN section.
IGMP	1. A Must filled setting 2. Disable is set by default	Enable IGMP (Internet Group Management Protocol) would enable the router to listen to IGMP packets to discover which interfaces are connected to which device. The router uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.
WAN IP Alias	1. An optional setting 2. Box is unchecked by default	Enable **WAN IP Alias** then enter the IP address provided by your Service Provider. **WAN IP Alias** is used by the device router and is treated as a second set of WAN IP to provide dual WAN IP address to your LAN network.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

L2TP (Ethernet WAN)



Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	L2TP ▼

L2TP WAN Type Configuration

Item	Setting
IP Mode	Dynamic IP Address ▼
Server IP Address / Name	
L2TP Account	
L2TP Password	
Connection Control	Auto-reconnect (Always on) ▼
MTU	0 (0 is Auto)
Service Port	User-defined ▼ 1702
MPPE	□ Enable
NAT	☑ Enable
Network Monitoring	☑ Enable ● DNS Query ○ ICMP Checking ☑ Loading Check Check Interval 5 (seconds) Check Timeout 3 (seconds) Latency Threshold 3000 (ms) Fail Threshold 5 (Times) Target1 DNS1 ▼ Target2 None ▼
IGMP	Disable ▼
WAN IP Alias	□ Enable 10.0.0.1

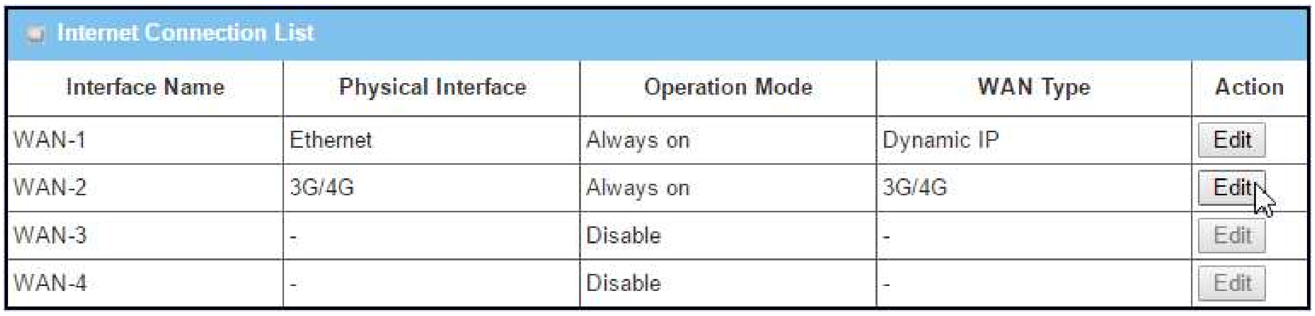
L2TP WAN Type Configuration		
Item	**Value setting**	**Description**
IP Mode	A Must filled setting	Select either Static or Dynamic IP address for L2TP Internet connection. ● When **Static IP Address** is selected, you will need to enter the **WAN IP Address**, **WAN Subnet Mask,** and **WAN Gateway**. ■ **WAN IP Address** (A Must filled setting)**:** Enter the WAN IP address given by your Service Provider. ■ **WAN Subnet Mask** (A Must filled setting)**:** Enter the WAN subnet mask given by your Service Provider. ■ **WAN Gateway** (A Must filled setting)**:** Enter the WAN gateway IP address given by your Service Provider. ● When **Dynamic IP** is selected, there are no above settings

		required.
Server IP Address/Name	A Must filled setting	Enter the L2TP server name or IP Address.
L2TP Account	A Must filled setting	Enter the L2TP username provided by your Service Provider.
L2TP Password	A Must filled setting	Enter the L2TP connection password provided by your Service Provider.
Connection Control	A Must filled setting	There are three connection modes. • **Auto-reconnect (Always on)** enables the router to always keep the Internet connection on. • **Connect-on-demand** enables the router to automatically re-establish Internet connection as soon as user attempts to access the Internet. Internet connection will be disconnected when it has been inactive for a specified idle time. • **Connect Manually** allows user to connect to Internet manually**.** Internet connection will be inactive after it has been inactive for specified idle time.
MTU	1. A Must filled setting 2. Auto (value zero) is set by default	**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.
Service Port	A Must filled setting	Enter the service port that the Internet service. There are three options can be selected : ● **Auto:** Port will be automatically assigned. ● **1701 (For Cisco)**: Set service port to port 1701 to connect to CISCO server. ● **User-defined**: enter a service port provided by your Service Provider.
MPPE	An optional setting	Select **Enable** to enable MPPE **(**Microsoft Point-to-Point Encryption) security for PPTP connection.
NAT	1. An optional setting 2. Box is checked by default	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
Network Monitoring	1. An optional setting 2. Box is checked by default	When the Network Monitoring feature is enabled, the router will use DNS Query or ICMP to periodically check Internet connection – connected or disconnected. For the configuration details, please refer to the description stated in Dynamic Ethernet WAN section.
IGMP	1. A Must filled setting 2. Disable is set by default	Enable IGMP (Internet Group Management Protocol) would enable the router to listen to IGMP packets to discover which interfaces are connected to which device. The router uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.
WAN IP Alias	1. An optional setting 2. Box is unchecked by default	Enable **WAN IP Alias** then enter the IP address provided by your Service Provider. **WAN IP Alias** is used by the device router and is treated as a second set of WAN IP to provide dual WAN IP address to your LAN network.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

Internet Setup – 3G/4G WAN

If the device connects to Internet through 3G/4G network, this section will help you to complete 3G/4G connection setup.

Go to Basic Network > WAN & Uplink > Internet Setup tab.

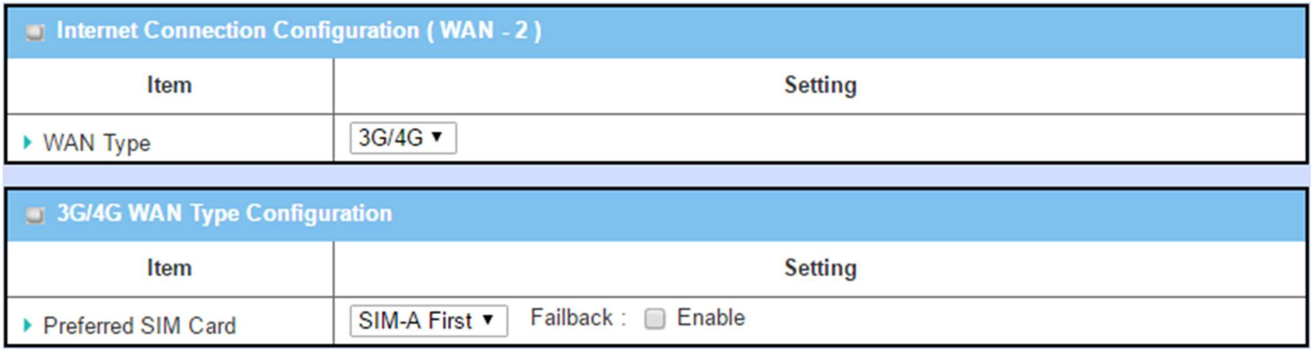


Internet Connection List

Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet	Always on	Dynamic IP	Edit
WAN-2	3G/4G	Always on	3G/4G	Edit
WAN-3	-	Disable	-	Edit
WAN-4	-	Disable	-	Edit

Configure 3G/4G WAN Setting

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



Internet Connection Configuration (WAN - 2)

Item	Setting
WAN Type	3G/4G ▾

3G/4G WAN Type Configuration

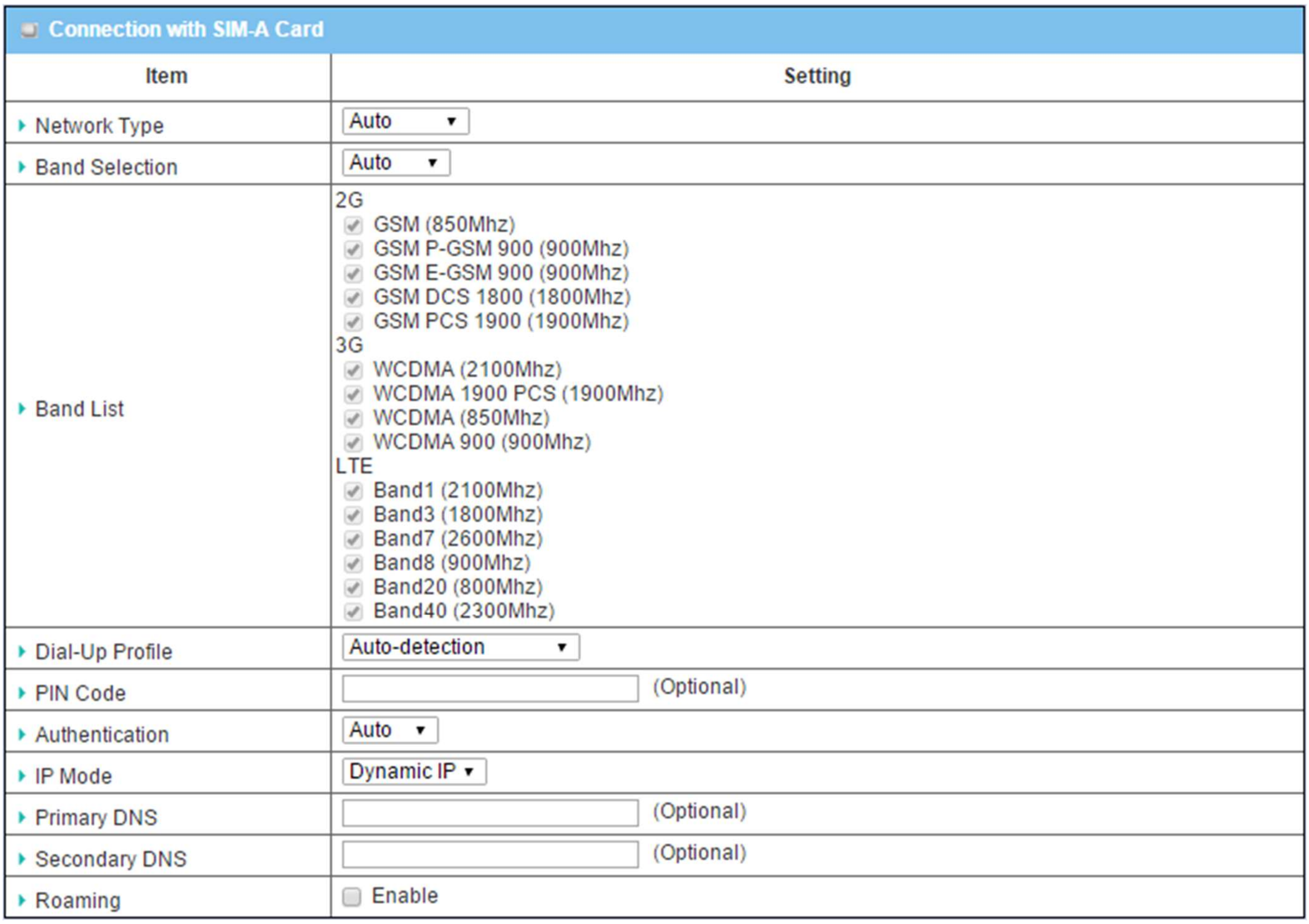
Item	Setting
Preferred SIM Card	SIM-A First ▾ Failback : □ Enable

3G/4G Connection Configuration Item	Value setting	Description
WAN Type	3. A Must filled setting 4. 3G/4G is set by default	From the dropdown box, select Internet connection method for 3G/4G WAN Connection. Only **3G/4G** is available.
Preferred SIM Card	1. A Must filled setting 2. By default **SIM-A First** is selected 3. **Failback** is unchecked by default	Choose which SIM card you want to use for the connection. When **SIM-A First** or **SIM-B First** is selected, it means the connection is built first by using SIM A/SIM B. And if the connection is failed, it will change to the other SIM card and try to dial again, until the connection is up. When **SIM-A only** or **SIM-B only** is selected, it will try to dial up only

	using the SIM card you selected. When **Failback** is checked, it means if the connection is dialed-up not using the main SIM you selected, it will failback to the main SIM and try to establish the connection periodically. **Note_1**: In some AirLive's products, only **SIM-A** can be chose. **Note_2**: **Failback** is available only when **SIM-A First** or **SIM-B First** is selected.

Configure SIM-A / SIM-B Card

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



Connection with SIM-A Card

Item	Setting
Network Type	Auto ▼
Band Selection	Auto ▼
Band List	2G ☑ GSM (850Mhz) ☑ GSM P-GSM 900 (900Mhz) ☑ GSM E-GSM 900 (900Mhz) ☑ GSM DCS 1800 (1800Mhz) ☑ GSM PCS 1900 (1900Mhz) 3G ☑ WCDMA (2100Mhz) ☑ WCDMA 1900 PCS (1900Mhz) ☑ WCDMA (850Mhz) ☑ WCDMA 900 (900Mhz) LTE ☑ Band1 (2100Mhz) ☑ Band3 (1800Mhz) ☑ Band7 (2600Mhz) ☑ Band8 (900Mhz) ☑ Band20 (800Mhz) ☑ Band40 (2300Mhz)
Dial-Up Profile	Auto-detection ▼
PIN Code	(Optional)
Authentication	Auto ▼
IP Mode	Dynamic IP ▼
Primary DNS	(Optional)
Secondary DNS	(Optional)
Roaming	□ Enable

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

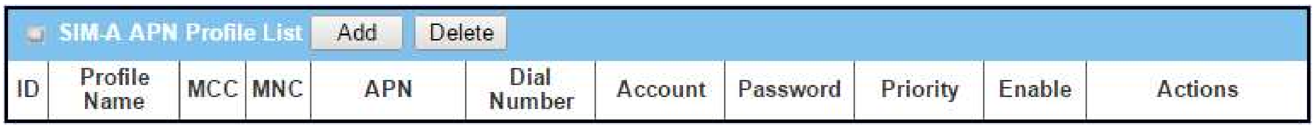
Note_2: Both **Connection with SIM-A Card** and **Connection with SIM-B Card** will pop up only when the **SIM-A First** or **SIM-B First** is selected, otherwise it only pops out one of them.

3G/4G Connection Configuration		
Item	**Value setting**	**Description**
Network Type	1. A Must filled setting 2. By default **Auto** is selected	Select **Auto** to register a network automatically, regardless of the network type. Select **2G Only** to register the 2G network only. Select **2G Prefer** to register the 2G network first if it is available. Select **3G only** to register the 3G network only. Select **3G Prefer** to register the 3G network first if it is available. Select **LTE only** to register the LTE network only. **Note_1**: Options may be different due to the specification of the module.
Band Selection	1. A Must filled setting 2. By default **Auto** is selected	Select **Auto** to register a network automatically, regardless of the band. Select **Manual** to choose specific bands you want to appoint to. **Note_1**: **USB 3G/4G** doesn't support this function.
Band List	1. A Must filled setting 2. The box is all checked by default	When **Band Selection > Auto** is selected, all bands are enabled and can't be unchecked. When **Band Selection > Manual** is selected, at least one band needs to be checked in each network type. **Note_1**: **USB 3G/4G** doesn't support this function.
Dial-Up Profile	1. A Must filled setting 2. By default **Auto-Detection** is selected	Select **Auto-Detection** to automatically bring out all configurations needed while dialing-up, by comparing the IMSI of the SIM card to the record listed in the manufacture's database. Select **Manual-configuration** to set **APN** (Access Point Name), **Dial Number**, **Account**, and **Password** to what your carrier provides. Select **APN Profile List** to set more than one profile to dial up in turn, until the connection is established. It will pop up a new filed, please go to **Basic Network > WAN & Uplink > Internet Setup > SIM-A APN Profile List** for details.
PIN code	String format : interger	Enter the PIN (Personal Identification Number) code if it needs to unlock your SIM card.
Authentication	1. A Must filled setting 2. By default **Auto** is selected	Select **PAP** (Password Authentication Protocol) and use such protocol to be authenticated with the carrier's server. Select **CHAP** (Challenge Handshake Authentication Protocol) and use such protocol to be authenticated with the carrier's server. When **Auto** is selected, it means it will authenticate with the server either **PAP** or **CHAP**.
IP Mode	1. A Must filled setting 2. By default **Dynamic IP** is selected	When **Dynamic IP** is selected, it means it will get all IP configurations from the carrier's server and set to the device directly. If you have specific application provided by the carrier, and want to set IP configurations on your own, you can switch to **Static IP** mode and fill in all parameters that required, such as IP address, subnet mask and gateway. **Note_1**: **IP Subnet Mask** is a must filled setting, make sure you have the right configuration. Otherwise, the connection may get issues.

Primary DNS	String format : IP address (IPv4 type)	Enter the IP address to change the primary DNS (Domain Name Server) setting. If it is not filled-in, the server address is given by the carrier while dialing-up.
Secondary DNS	String format : IP address (IPv4 type)	Enter the IP address to change the secondary DNS (Domain Name Server) setting. If it is not filled-in, the server address is given by the carrier while dialing-up.
Roaming	The box is unchecked by default	Check the box to establish the connection even the registration status is roaming, not in home network. **Note_1**: It may cost additional charges if the connection is under roaming.

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

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

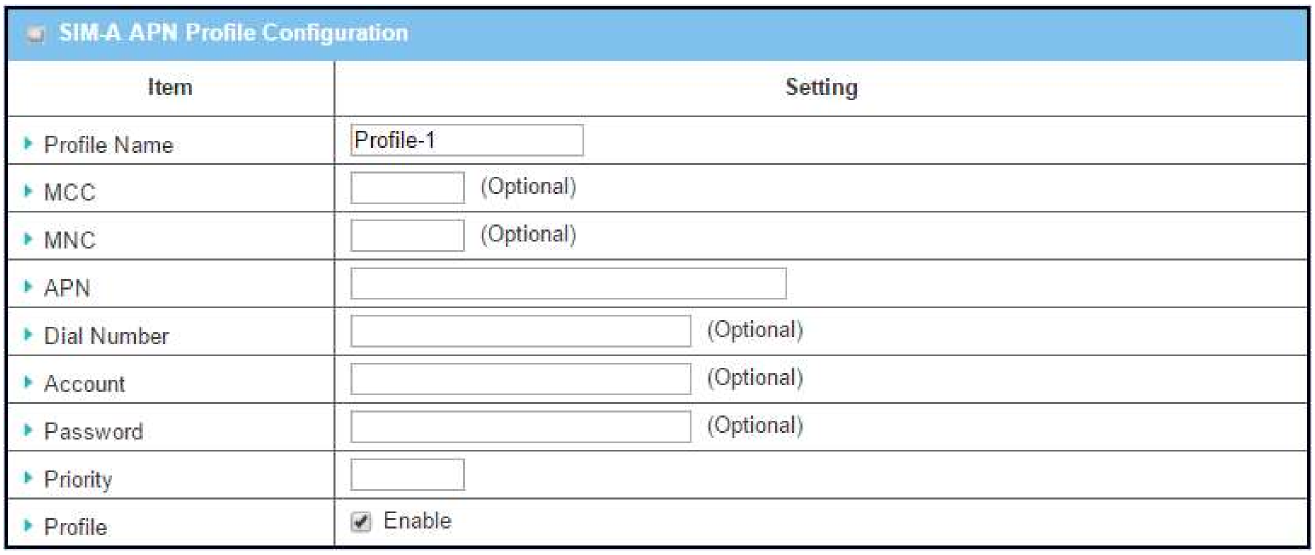


SIM-A APN Profile List Add Delete

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

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

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



SIM-A APN Profile Configuration

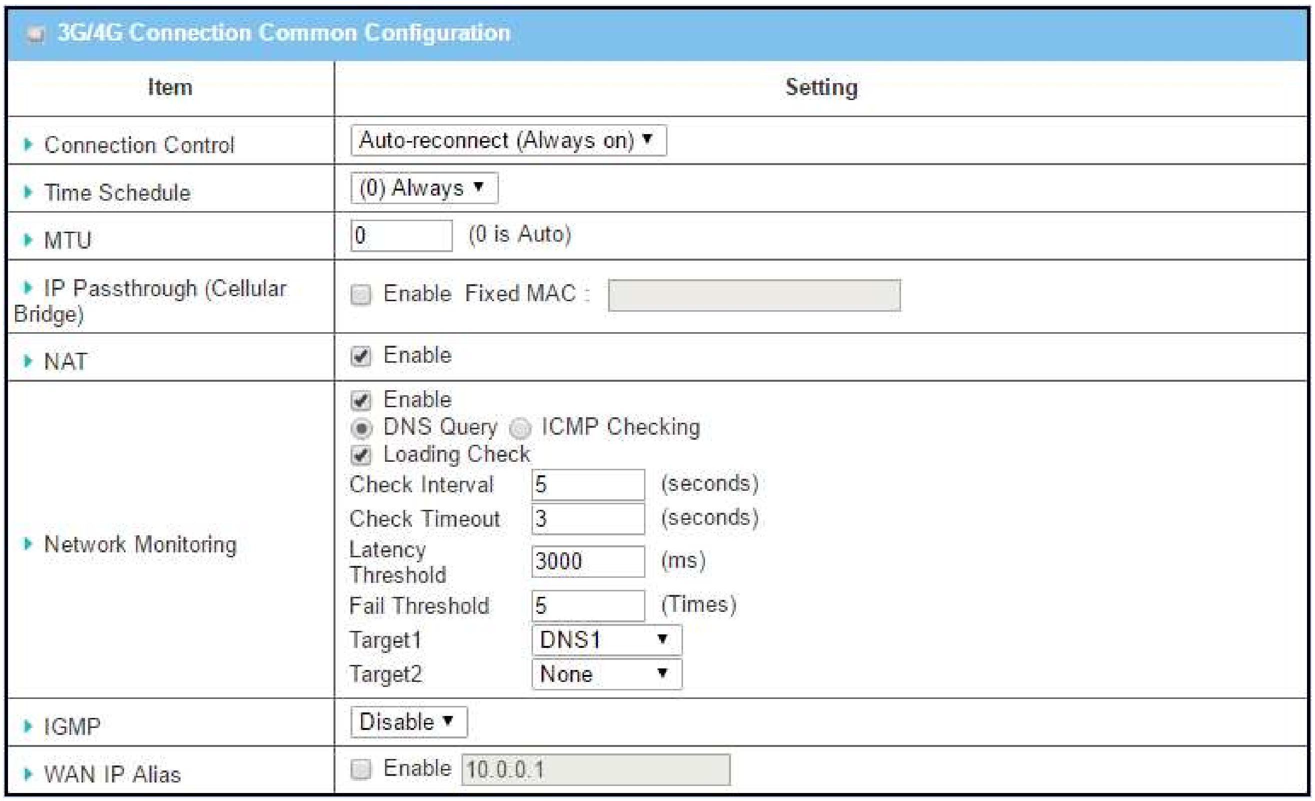
Item	Setting
Profile Name	Profile-1
MCC	(Optional)
MNC	(Optional)
APN	
Dial Number	(Optional)
Account	(Optional)
Password	(Optional)
Priority	
Profile	☑ Enable

3G/4G Connection Configuration		
Item	**Value setting**	**Description**
Profile Name	1. By default **Profile-x** is listed 2. String format : any	Enter the profile name you want to describe for this profile.

	text	
MCC	String format : integer	Enter the **MCC** (Mobile Country Code) you want to use for this profile. **Note_1**: the **MCC** should be related to the **MNC**, this filed can't be invalid value if **MNC** is filled-in.
MNC	String format : integer	Enter the **MNC** (Mobile Network Code) you want to use for this profile. **Note_1**: the **MNC** should be related to the **MCC**, this filed can't be invalid value if **MCC** is filled-in.
APN	String format : any text	Enter the **APN** you want to use to establish the connection.
Dial Number	String format : integer, asterisk and number sign	Enter the **Dial Number** you want to use to establish the connection.
Account	String format : any text	Enter the **Account** you want to use for the authentication.
Password	String format : any text	Enter the **Password** you want to use for the authentication.
Priority	1. A Must filled setting 2. String format : integer	Enter the value for the dialing-up order. The valid value is from 1 to 16. It will start to dial up with the profile that assigned with the smallest number.
Profile	The box is checked by default	Check the box to enable this profile. Uncheck the box to disable this profile in dialing-up action.

Setup 3G/4G Connection Common Configuration

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



3G/4G Connection Common Configuration

Item	Setting
Connection Control	Auto-reconnect (Always on) ▾
Time Schedule	(0) Always ▾
MTU	0 (0 is Auto)
IP Passthrough (Cellular Bridge)	□ Enable Fixed MAC :
NAT	☑ Enable
Network Monitoring	☑ Enable ● DNS Query ○ ICMP Checking ☑ Loading Check Check Interval 5 (seconds) Check Timeout 3 (seconds) Latency Threshold 3000 (ms) Fail Threshold 5 (Times) Target1 DNS1 ▾ Target2 None ▾
IGMP	Disable ▾
WAN IP Alias	□ Enable 10.0.0.1

3G/4G Connection Configuration Item	Value setting	Description
Connection Control	By default **Auto-reconnect (Always on)** is selected	When **Auto-reconnect (Always on)** is selected, it means it will keep the connection on all the time. When **Connect-on-demand** is selected, it means the connection will be established only when detecting data traffic. When **Connect Manually** is selected, it means you need to click the **Connect** button to dial up the connection manually. Please go to Status > Network Status for details. **Note_1**: This field is available only when **Basic Network > WAN > Physical Interface > Operation Mode** is selected to **Always on**.
Time Schedule	1. A Must filled setting 2. By default **(0) Always** is selected	When **(0) Always** is selected, it means this WAN is under operation all the time. Once you have set other schedule rules, there will be other options to select. Please go to **System > Scheduling** for details.
MTU	1. A Must filled setting 2. By default **0** is filled-in 3. String format : integer	Enter the **MTU** (Maximum Transmission Unit) you want to set the configuration.
IP Pass-through (Cellular Bridge)	1. The box is unchecked by default 2. String format for **Fixed MAC**:	When **Enable** box is checked, it means the device will directly assign the WAN IP to the first connected local LAN client. However, when an optional **Fixed MAC** is filled-in a non-zero value, it means only the client with this MAC address can get the WAN IP

	MAC address, e.g. 00:50:18:aa:bb:cc	address. **Note_1**: This field is only available when 3G/4G-n is set to **WAN-1**. **Note_2**: When the **IP Pass-through** is enabled, it will disable other WAN (exclude 3G/4G WAN) if they are set. But if there are other 3G/4G WANs, the **IP Pass-through** will be enabled automatically when the one in WAN1 is checked. **Note_3**: When the **IP Pass-through** is on, **NAT** and **WAN IP Alias** will be unavailable until the function is disabled again.
NAT	The box is checked by default	Uncheck the box to disable **NAT** (Network Address Translation) function.
Network Monitoring	1. An optional setting 2. Enabled by default	When the Network Monitoring feature is enabled, the gateway will use DNS Query or ICMP to periodically check Internet connection – connected or disconnected. ● Choose either **DNS Query** or **ICMP Checking** to detect WAN link. With **DNS Query,** the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. With **ICMP Checking,** the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2. ● **Loading Check** Enable Loading Check allows the router to ignore unreturned DNS Queries or ICMP requests when WAN bandwidth is fully occupied. This is to prevent false link-down status. ● **Check Interval** defines the transmitting interval between two DNS Query or ICMP checking packets. ● **Check Timeout** defines the timeout of each DNS query/ICMP. ● **Latency Threshold** defines the tolerance threshold of responding time. ● **Fail Threshold** specifies the detected disconnection before the router recognize the WAN link down status. Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged. ● **Target1** (**DNS1** set by default**)** specifies the first target of sending DNS query/ICMP request. ■ **DNS1**: set the primary DNS to be the target. ■ **DNS2**: set the secondary DNS to be the target. ■ **Gateway**: set the Current gateway to be the target. ■ **Other Host**: enter an IP address to be the target. ● **Target2** (**None** set by default**)** specifies the second target of sending DNS query/ICMP request. ■ **None**: to disable **Target2.** ■ **DNS1**: set the primary DNS to be the target. ■ **DNS2**: set the secondary DNS to be the target. ■ **Gateway**: set the Current gateway to be the target. **Other Host**: enter an IP address to be the target.
IGMP	By default **Disable** is selected	Select **Auto** to enable **IGMP** (Internet Group Management Protocol) function. Check the **Enable** box to enable **IGMP Proxy**.

WAN IP Alias	1. The box is unchecked by default 2. String format: IP address (IPv4 type)	Check the box to enable **WAN IP Alias**, and fill in the IP address you want to assign.

3.1.5 Load Balance

When there are more than one WAN interfaces, and when the bandwidth of one WAN connection is not enough for the traffic loads from the Intranet to the Internet, the gateway device needs the WAN load balance function to enlarge the total WAN bandwidth.

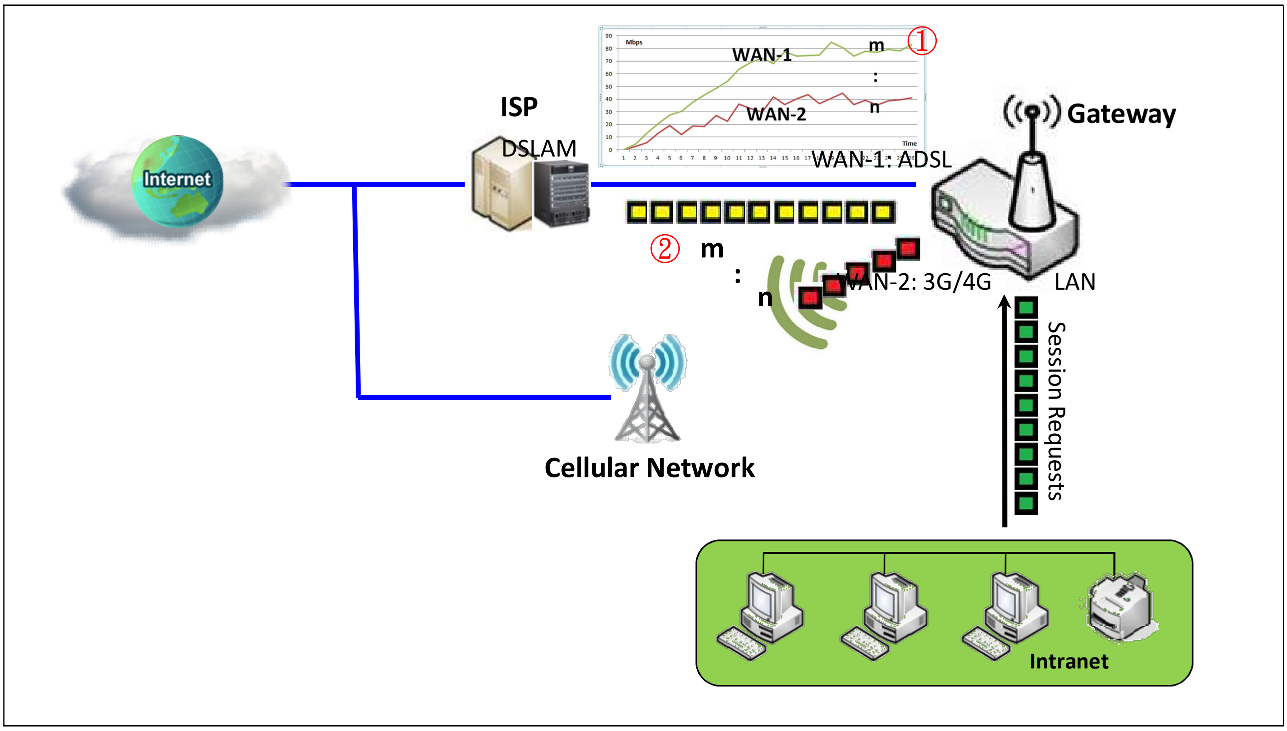
The multi-WAN "Load Balance" function provides three optional strategies: By Smart Weight, By Specific Weight, and By User Policy. Administrator can choose strategy based on his immediate need and environment consideration.

When you choose "By Smart Weight" strategy, system will operate load balance function automatically based on the embedded Smart Weight algorithm. However, when you choose "By Specific Weight" strategy, you can define the ratio of transferred sessions between all WAN interfaces for data transfer. At last, when you choose "By User Policy" strategy, you can define or select one user policy for routing dedicated packet flow via one WAN interface.

By Smart Weight Load Balance Strategy

For "By Smart Weight" load balance strategy, the gateway will operate the function automatically without additional parameters, except the available bandwidth (Line Speed) of each WAN interface, which is configured in **[Basic Network]-[WAN & Uplink]-[Physical Interface]** section. The gateway decides further routing ratio of connection flow to all WAN interfaces based on current traffic flow loads (in bytes) on all WAN interfaces. Administrator may take it as a fast approach to maximize the bandwidth utilization of multiple WAN interfaces in gateway.

That is, the gateway will take the line speed settings of all WAN interfaces specified in "Physical Interface" configuration page, as the default ratio among WAN interfaces for data transfer. Based on the ratio of packet bytes via these WAN interfaces in past period (maybe 5 minutes), system decides how many sessions will be transferred via each WAN interface for current period of traffic loadings as shown in the following illustration diagram.



Following 2 tables list the parameter configuration for the above example diagram of load balance function. The ratio m:n in this example is 22:11.

Configuration Path	[Physical Interface]-[Interface Configuration (WAN-n)] , n=1,2	
Interface Name	WAN-1	WAN-2
Physical Interface	***ADSL***	***3G/4G***
Operation Mode	***Always on***	***Always on***
Line Speed	***2Mbps / 22Mbps***	***1Mbps / 11Mbps***

Configuration Path	[Load Balance]-[Configuration]
Load Balance	■ ***Enable***
Load Balance Strategy	***By Smart Weight***

The steps of the Smart Weight algorithm are:

Pre-state: System takes the line speed settings of all WAN interfaces as the initial ratio between all WAN interfaces for load balance.

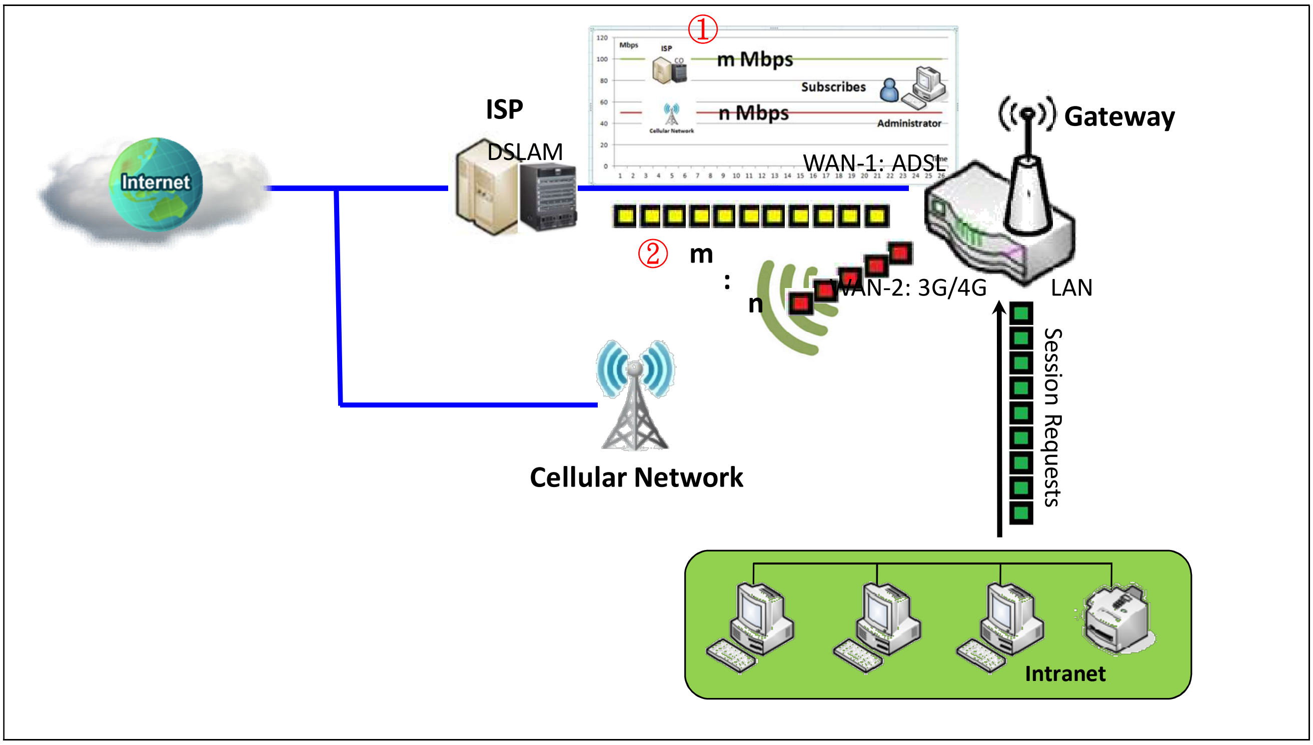
S 1: Count the transferred packet bytes for all WAN interfaces in current time period, for example 5 minutes. At the end of time period, the new transferring ratio for each WAN interface will be changed to the ratio for the counted transferred data among all interfaces for next time period.

S 2: Based on the new ratio that is obtained at S1, system decides how many sessions will be transferred via each WAN interface for another time period. Loop S1 and S2 steps forever until administrator changes the load balance strategy.

By Specific Weight Load Balance Strategy

However, when you choose "By Specific Weight" load balance strategy, there is a list of two parameter pairs that is used for the load balance strategy: WAN Interface & Weight (%). The line speed of each WAN interface serves as its default weight whose value is the ratio of its line speed to total line speed of all WAN interfaces. Certainly, administrator also can fine tune the weight list based on the default one. The gateway's traffic control process will operate routing adequately based on the dedicated weights on all WAN interfaces.

Following is another example diagram to illustrate the scenario. At the beginning, gateway has two WAN interfaces and their download line speed are 22Mbps (m Mbps) for WAN-1 interface and 11Mbps (n Mbps) for WAN-2. That comes from administrator subscribes ADSL ISP for a 22 Mbps WAN connection and 3G/4G ISP for another 11 Mbps WAN connection. Administrator fills these values in the line speed field for each WAN interface. Please refer to section **[Basic Network]-[WAN & Uplink]-[Physical Interface]**. So, the default routing ratio for these both interfaces is 2:1 (=22:11) in load balance function as shown in following illustration diagram. The value of m is 22 and n is 11.



Following 3 tables list the parameter configuration for the above example diagram of load balance function. The ration m:n in this example is 22:11.

Configuration Path	[Physical Interface]-[Interface Configuration (WAN-n)] , n=1,2

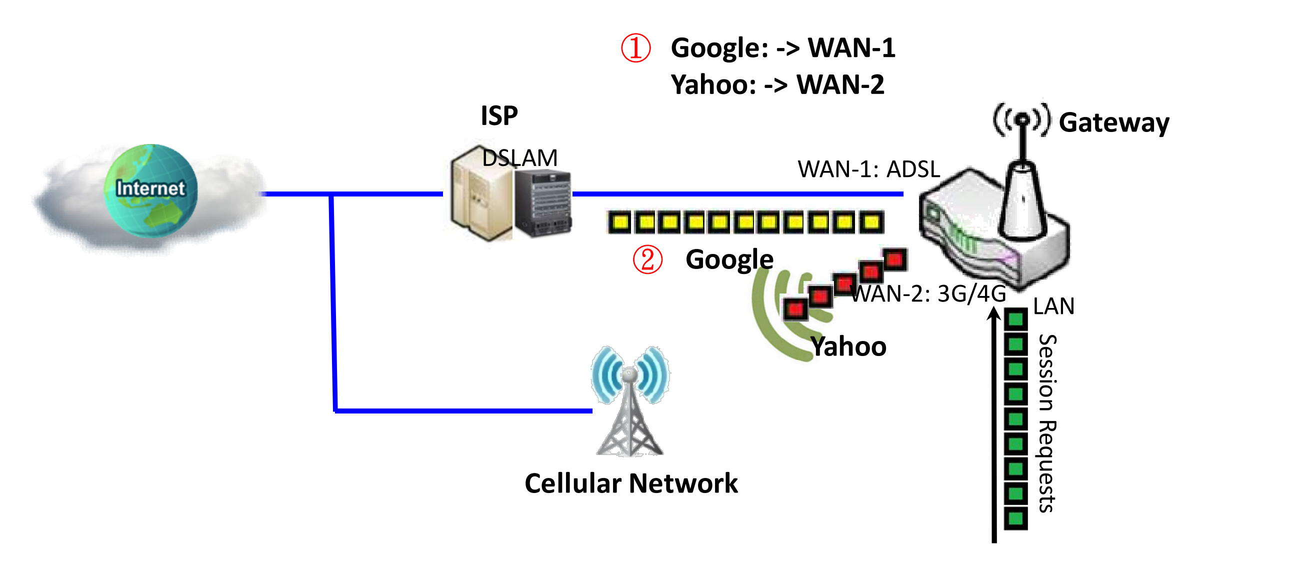
Interface Name	WAN-1	WAN-2
Physical Interface	***ADSL***	***3G/4G***
Operation Mode	***Always on***	***Always on***
Line Speed	***2Mbps / 22Mbps***	***1Mbps / 11Mbps***

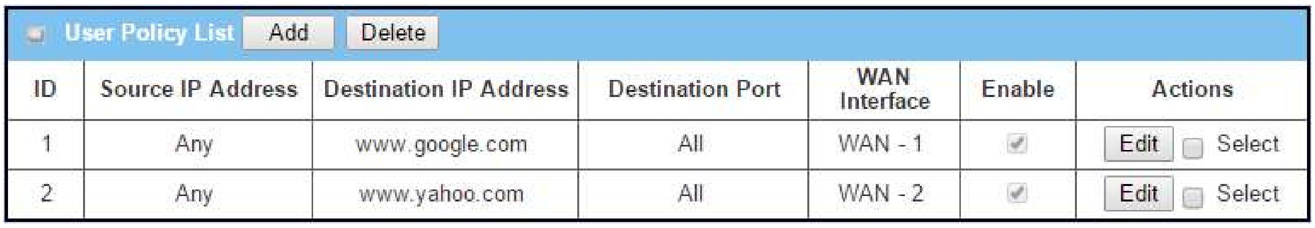
Configuration Path	[Load Balance]-[Configuration]
Load Balance	■ ***Enable***
Load Balance Strategy	***By Priority***

Configuration Path	[Load Balance]-[Priority Definition]	
WAN ID	**WAN-1**	**WAN-2**
Priority (%)	***67%***	***33%***

By User Policy Load Balance Strategy

Finally, when you choose "By User Policy" load balance strategy, there are two more configuration windows: "User Policy List" and "User Policy Configuration". "User Policy List" shows all your defined user policy entries, and the "User Policy Configuration" window will let you configure one user policy for routing dedicated packet flow via one WAN interface. They are shown in following diagrams.





ID	Source IP Address	Destination IP Address	Destination Port	WAN Interface	Enable	Actions
1	Any	www.google.com	All	WAN - 1	✓	Edit □ Select
2	Any	www.yahoo.com	All	WAN - 2	✓	Edit □ Select

Above example shows that administrator hopes the packet flow whose destination is "www.google.com", "www.yahoo.com" will be transferred via WAN-1, and WAN-2 respectively. For other un-specified packet flows will be routed by default via different WAN interfaces by "Smart Weight" load balance strategy.

To meet the load balance requirement as in the above example diagram, administrator need configure the device based on following configuration table contents.

Configuration Path	[Physical Interface]-[Interface Configuration (WAN-n)] , n=1,2	
Interface Name	WAN-1	WAN-2
Physical Interface	***ADSL***	***3G/4G***
Operation Mode	***Always on***	***Always on***
Line Speed	***2Mbps / 22Mbps***	***1Mbps / 11Mbps***

Configuration Path	[Load Balance]-[Configuration]
Load Balance	■ ***Enable***
Load Balance Strategy	***By User Policy***

Configuration Path	[Load Balance]-[User Policy Configuration]	
ID	**1**	**2**
Source IP Address	***Any***	***Any***
Destination IP Address	***Domain Name www.google.com***	***Domain Name www.yahoo.com***
Destination Port	***All***	***All***
Protocol	***Both***	***Both***
WAN Interface	***WAN-1***	***WAN-2***
Policy	■ ***Enable***	■ ***Enable***

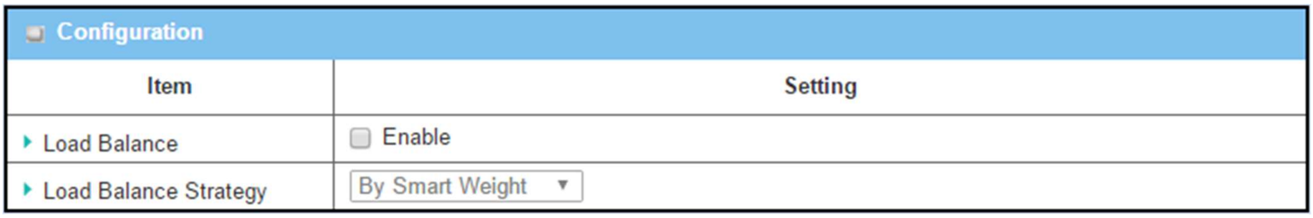
Load Balance Setting

The **Load Balance** function is used to manage balance bandwidth usage among multiple WAN connections.

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

The "Configuration" window is to enable the load balance function and specify the strategy. When you choose "By Smart Weight" strategy, system will operate load balance function automatically based on the embedded Smart Weight algorithm. However, when you choose "By Specific Weight" strategy, the further "Weight Definition" configuration window will let you define the ratio of transferred sessions between all WAN interfaces for data transfer. At last, when you choose "By User Policy" strategy, the further "User Policy List" shows all defined user policy entries, and the "User Policy Configuration" window will let you create and define one user policy for routing dedicated packet flow via one WAN interface.

Enable/Select Load Balance Strategy

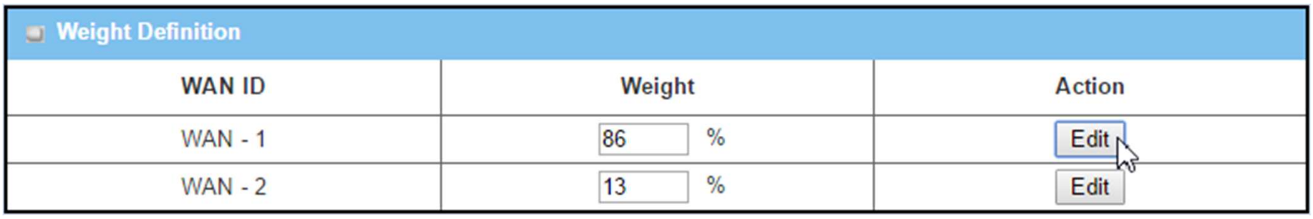


Configuration

Item	Setting
Load Balance	□ Enable
Load Balance Strategy	By Smart 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.	There are three load balance strategies:. **By Smart Weight**: System will operate load balance function automatically based on the embedded Smart Weight algorithm. **By Specific Weight**: System will adjust the ratio of transferred sessions among all WANs based on the specified weights for each WAN. **By User Policy**: System will route traffics through available WAN interface based on user defined rules.
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore what you just configured back to the previous setting.

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



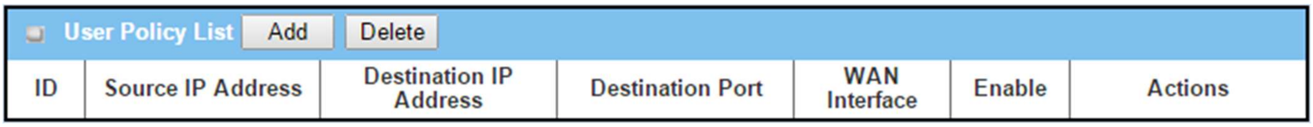
Weight Definition

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

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 the weight ratio for each WAN interface. Initially, the bandwidth ratio of each WAN is set by default. Note: The sum of all weights can't be greater than 100%.
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore what you just configured back to the previous setting.

When **By User Policy** is selected, a **User Policy List** screen will appear. With properly configured your policy rules, system will route traffics through available WAN interface based on user defined rules

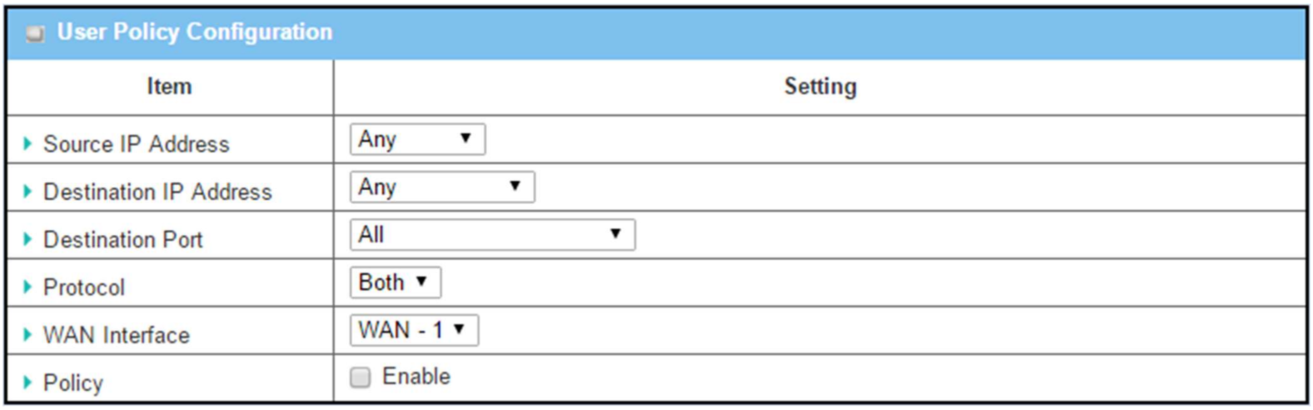
Create User Policy



User Policy List Add Delete

ID	Source IP Address	Destination IP Address	Destination Port	WAN Interface	Enable	Actions

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



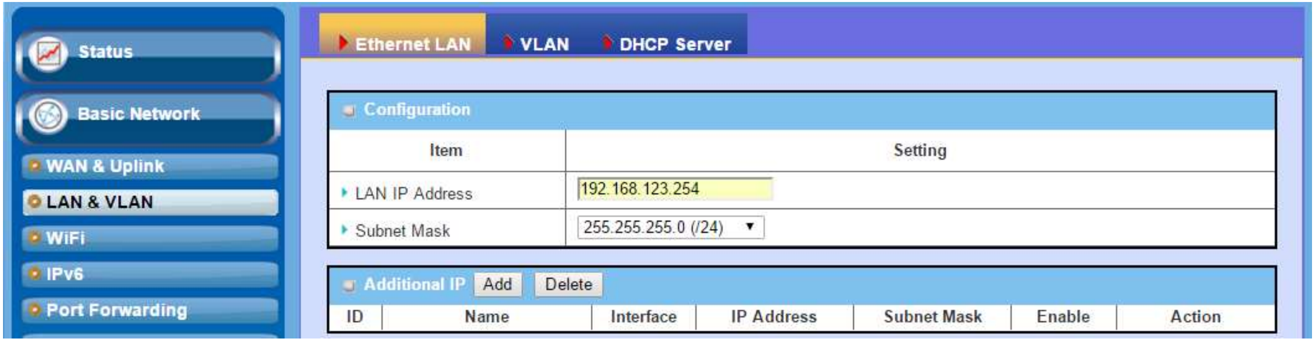
User Policy Configuration

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 can be selected : **Any**: No specific Source IP is provided. The traffic may come from any source **Subnet**: Specify the Subnet for the traffics come from the subnet. Input format is : xxx.xxx.xxx.xxx/xx e.g. 192.168.123.0/24. **IP Range**: Specify the IP Range for the traffics come from the IPs **Single IP**: Specify a unique IP Address for the traffics come from the IP. Input format is : xxx.xxx.xxx.xxx e.g. 192.168.123.101.
Destination IP Address	1. A Must filled setting 2. **Any** is selected by default.	There are five options can be selected : **Any**: No specific destination IP is provided. The traffic may come to any destination. **Subnet**: Specify the Subnet for the traffics come to the subnet. Input format is : xxx.xxx.xxx.xxx/xx e.g. 192.168.123.0/24. **IP Range**: Specify the IP Range for the traffics come to the IPs **Single IP**: Specify a unique IP Address for the traffics come to the IP. Input format is : xxx.xxx.xxx.xxx e.g. 192.168.123.101. **Domain Name**: Specify the domain name for the traffics come to the domain
Destination Port	1. A Must filled setting 2. **All** is selected by default.	There are four options can be selected : **All**: No specific destination port is provided. **Port Range**: Specify the Destination Port Range for the traffics **Single Port**: Specify a unique destination Port for the traffics **Well-known Applications**: Select the service port of well-known application defined in dropdown list.
Protocol	1. A Must filled setting 2. **Both** is selected by default.	There are three options can be selected. They are **Both**, **TCP**, and **UDP**.
WAN Interface	1. A Must filled setting 2. **WAN-1** is selected by default.	User can select the interface that traffic should go. 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	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore what you just configured back to the previous setting.

3.3 LAN & VLAN

This section provides a brief description of LAN and VLAN. It also explains how to create and modify virtual LANs which are more commonly known as VLANs.



Configuration

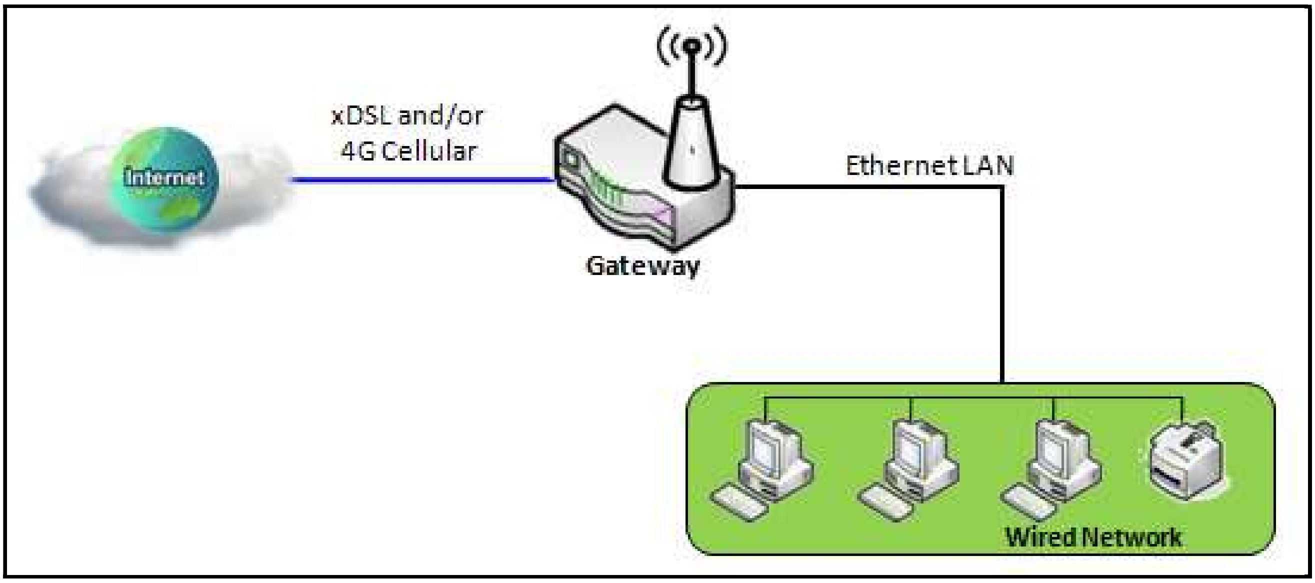
Item	Setting
LAN IP Address	192.168.123.254
Subnet Mask	255.255.255.0 (/24)

Additional IP

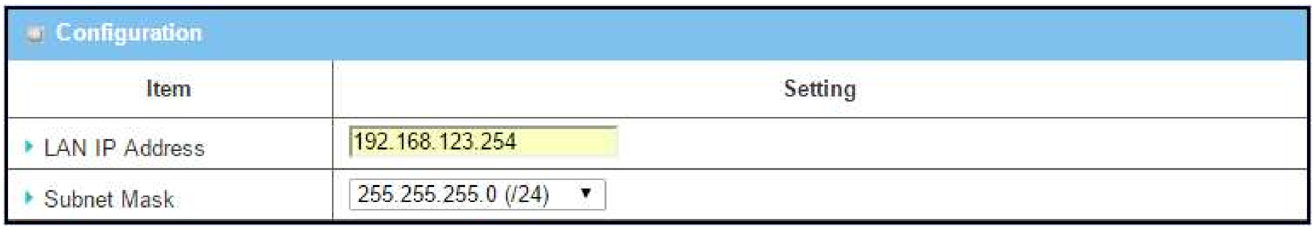
ID	Name	Interface	IP Address	Subnet Mask	Enable	Action

3.3.1 Ethernet LAN

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



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

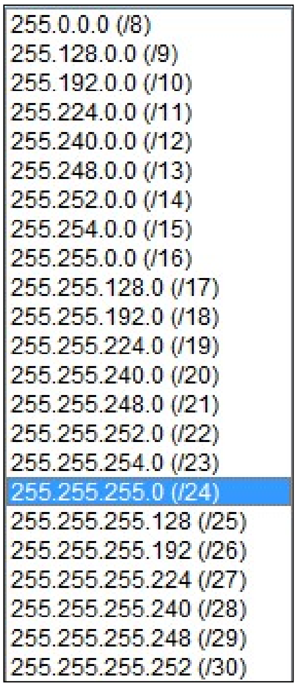


Configuration

Item	Setting
LAN IP Address	192.168.123.254
Subnet Mask	255.255.255.0 (/24) ▼

LAN IP Address: The local IP address of this device. The computer on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary. It's also the IP address of web UI. If you change it, you need to type new IP address in the browser to see web UI.

Subnet Mask: Input your Subnet mask. Subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0 (/24), and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway, so there are maximum 253 clients allowed in LAN network. Hereafter are the available options for subnet mask.



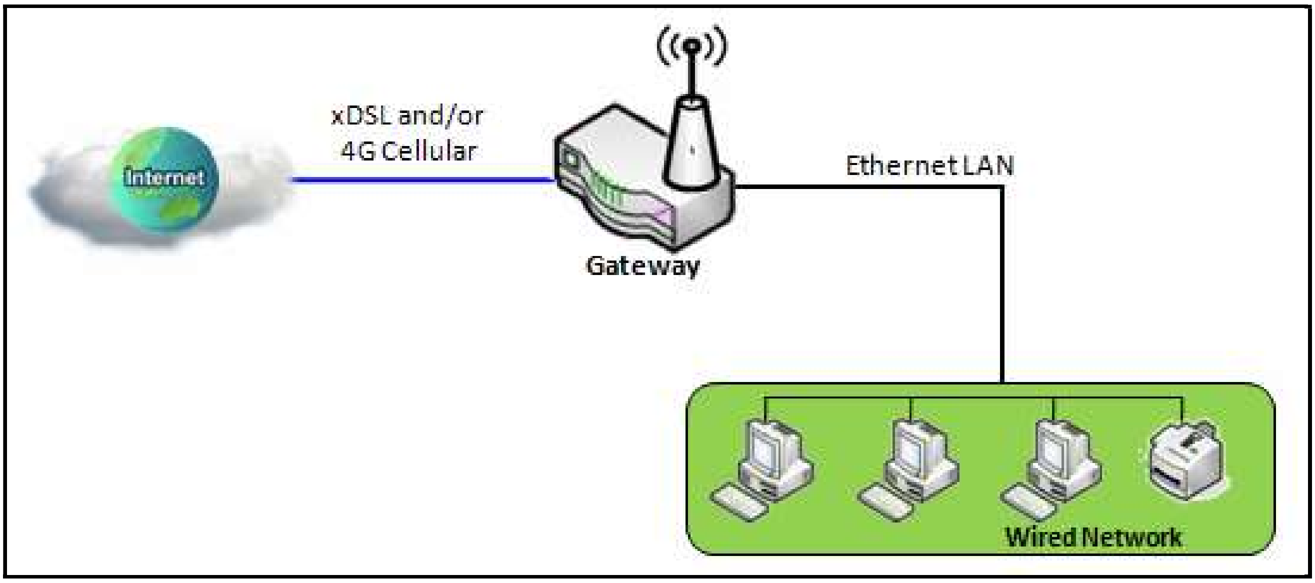
255.0.0.0 (/8)
255.128.0.0 (/9)
255.192.0.0 (/10)
255.224.0.0 (/11)
255.240.0.0 (/12)
255.248.0.0 (/13)
255.252.0.0 (/14)
255.254.0.0 (/15)
255.255.0.0 (/16)
255.255.128.0 (/17)
255.255.192.0 (/18)
255.255.224.0 (/19)
255.255.240.0 (/20)
255.255.248.0 (/21)
255.255.252.0 (/22)
255.255.254.0 (/23)
255.255.255.0 (/24)
255.255.255.128 (/25)
255.255.255.192 (/26)
255.255.255.224 (/27)
255.255.255.240 (/28)
255.255.255.248 (/29)
255.255.255.252 (/30)

3.3.3 VLAN

This section provides a brief description of LAN and VLAN (Virtual LAN). It also explains how to create and modify virtual LANs which are more commonly known as VLANs.

➢ Ethernet LAN

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



➢ VLAN

The VLAN is a logical network under a certain switch or router device to group lots of client hosts with a specific VLAN ID. This device supports both Port-based VLAN and Tag-based VLAN. In Port-based VLAN, all client hosts belong to the same group by transferring data via some physical ports that are tagged with same VLAN ID in the device. The ports of a VLAN form an independent traffic domain in which the traffic generated by the nodes remains within the VLAN. However, in Tag-based VLAN, all packets with same VLAN ID will be treated as the same group of them and own same access property and QoS property. It is especially useful when individuals of a VLAN group are located at different floor location.

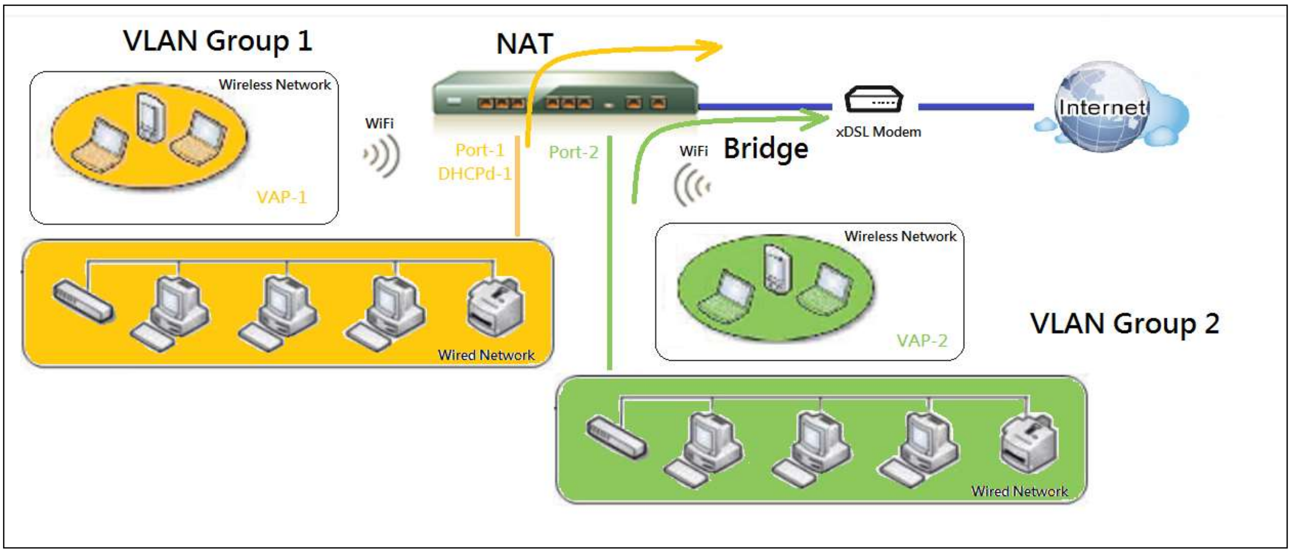
The VLAN function allows you to divide local network into different “virtual LANs”. In some cases, ISP may need router to support “VLAN tag” for certain kinds of services (e.g. IPTV) to work properly. In some cases, SMB departments are separated and located at any floor of building. All client hosts in the same department should own common access property and QoS property. You can select either one operation mode, port-based VLAN or tag-based VLAN, and then configure according to your network configuration.

Please be noted, for some gateway with only one physical Ethernet LAN port, only very limited configuration are available if you enable the Port-based VLAN.

There are some common VLAN scenarios for the device as follows:

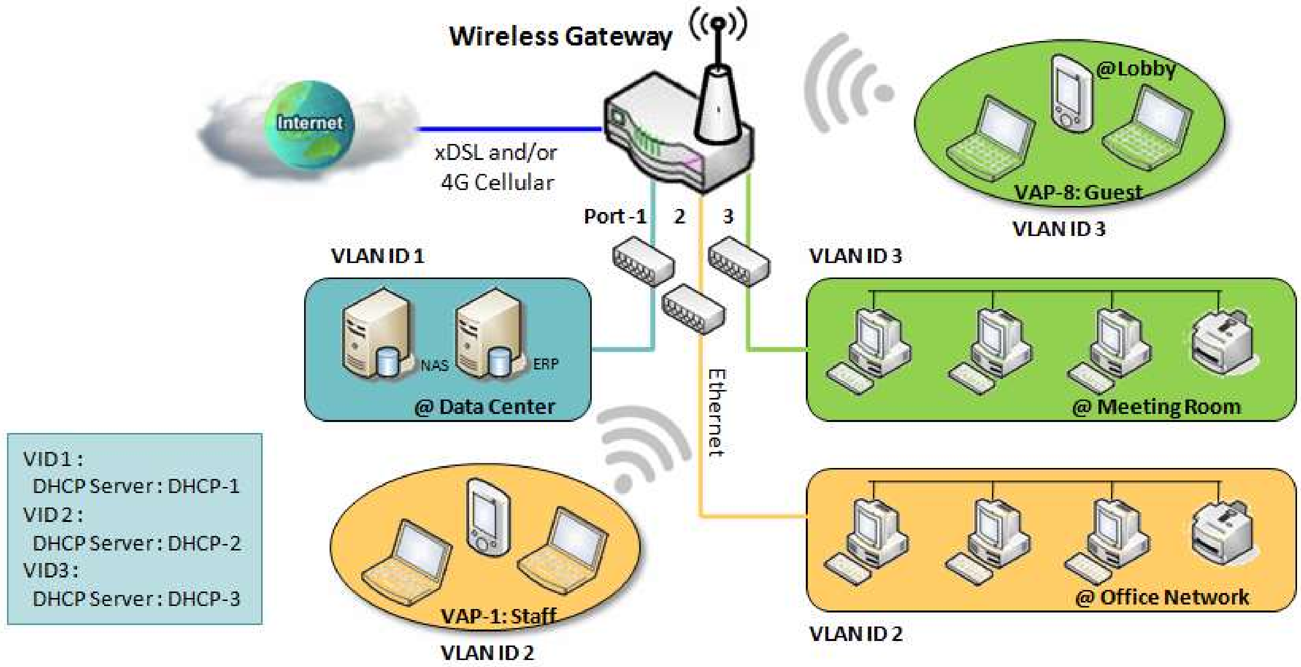
➢ Port-based VLAN

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



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

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

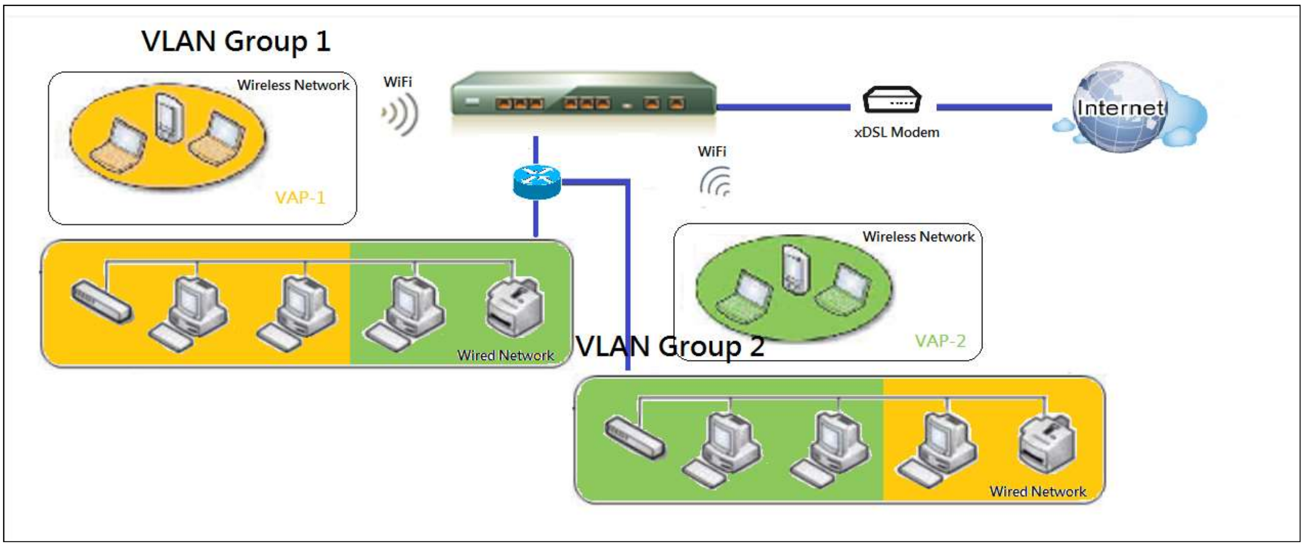


Above is the general case for 3 Ethernet LAN ports in the gateway. But if the device just has one Ethernet LAN port, there will be only one VLAN group for the device. Under such situation, it still supports both the NAT and Bridge mode for the Port-based VLAN configuration.

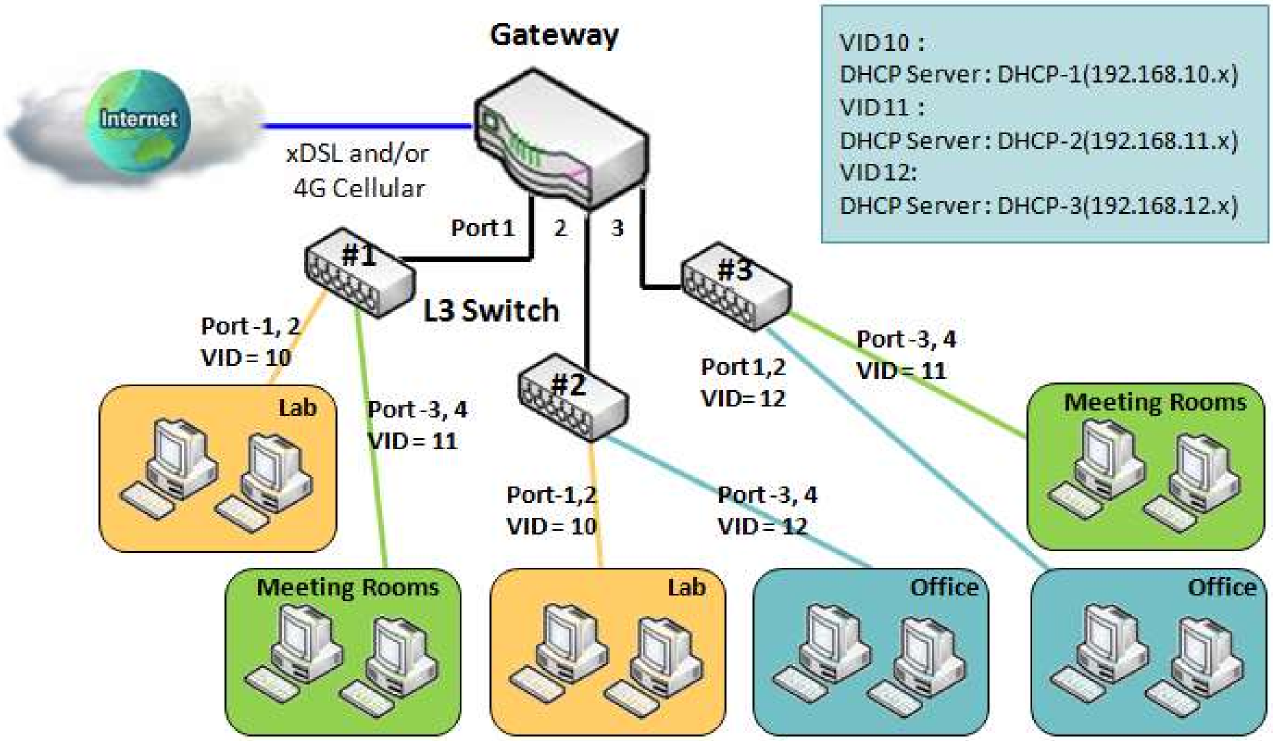
➢ Tag-based VLAN

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

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



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

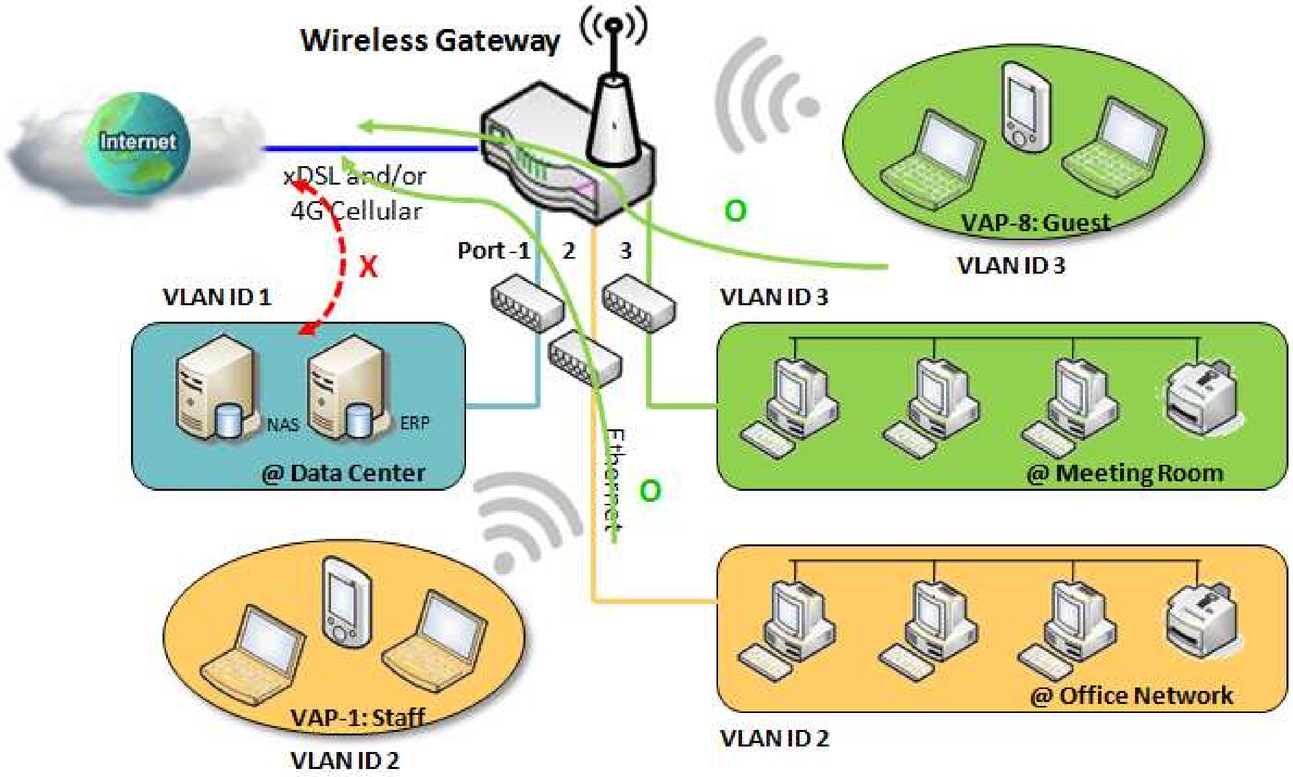


➢ VLAN Groups Access Control

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

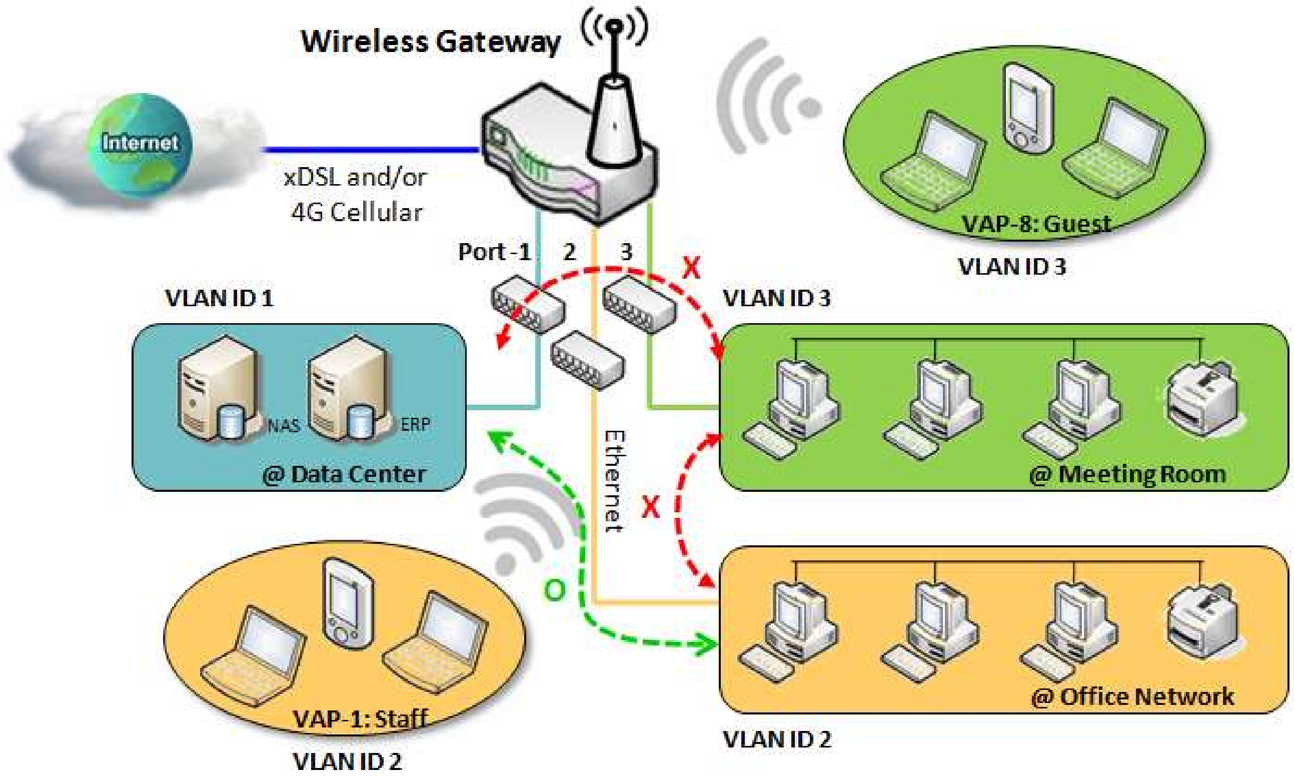
VLAN Group Internet Access

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



Inter VLAN Group Routing:

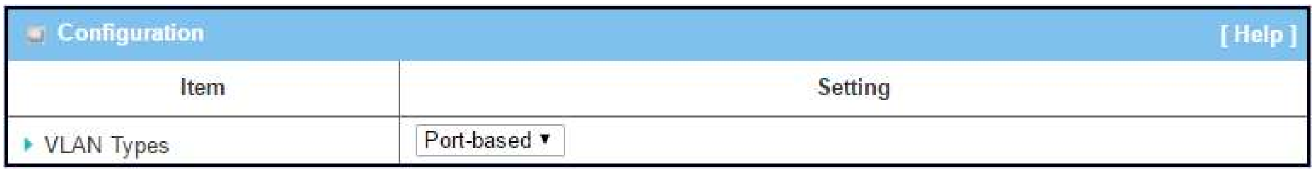
In Port-based tagging, administrator can specify member hosts of one VLAN group to be able to communicate with the ones of another VLAN group or not. This is a communication pair, and one VLAN group can join many communication pairs. But communication pair doesn't have the transitive property. That is,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



VLAN Setting

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

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

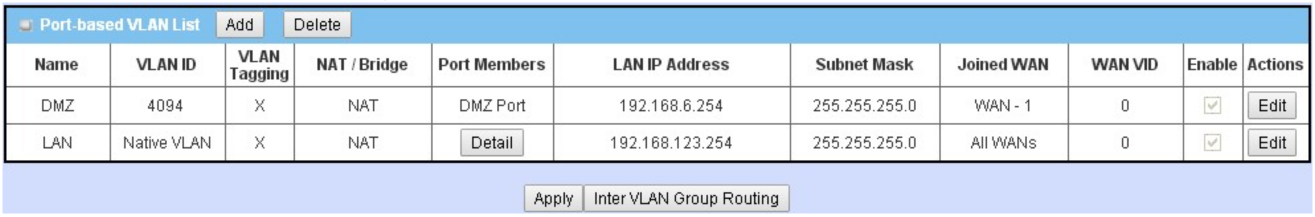


Item	Setting
VLAN Types	Port-based ▾

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

Port-based VLAN – Create/Edit VLAN Rules

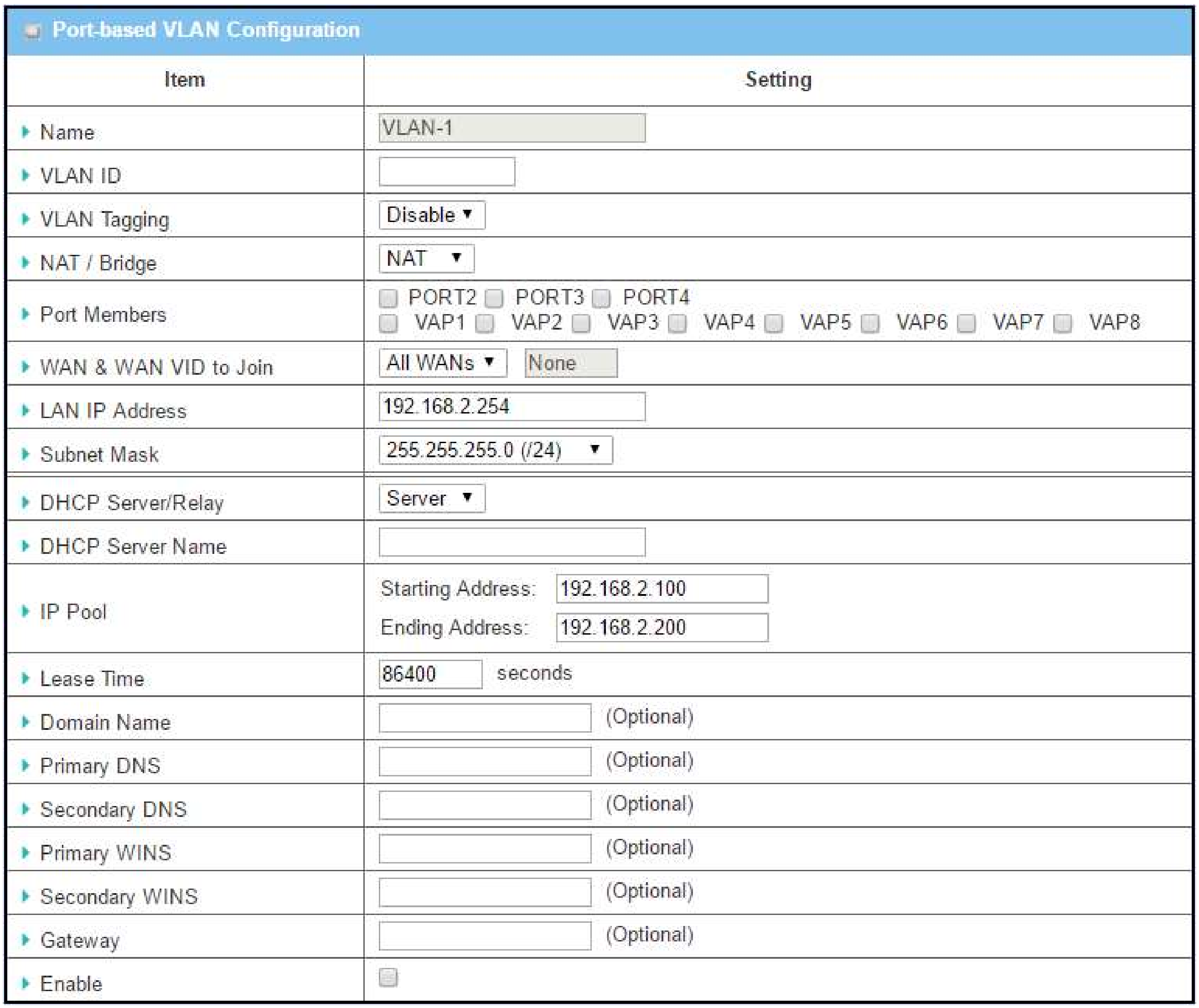
The port-based VLAN allows you to custom each LAN port. There is a default rule shows the configuration of all LAN ports. Also, if your device has a DMZ port, you will see DMZ configuration, too. The maxima rule numbers is based on LAN port numbers.



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

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

Port-based VLAN – Configuration



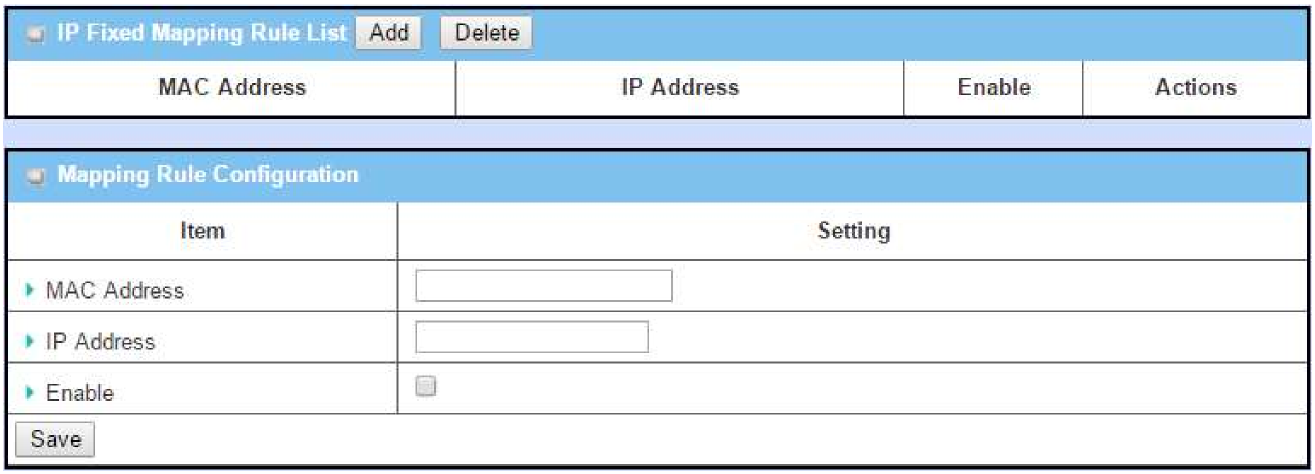
Port-based VLAN Configuration

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

Port-based VLAN Configuration		
Item	**Value setting**	**Description**
Name	1. A Must filled setting 2. String format: already have default texts	Define the **Name** of this rule. It has a default text and can not be modified.
VLAN ID	A Must filled setting	Define the VLAN ID number, range is 1~4094.
VLAN Tagging	**Disable** is selected by default.	The rule is activated according to **VLAN ID** and **Port Members** configuration when **Enable** is selected. The rule is activated according **Port Members** configuration when

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

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



IP Fixed Mapping Rule List Add Delete

MAC Address	IP Address	Enable	Actions

Mapping Rule Configuration

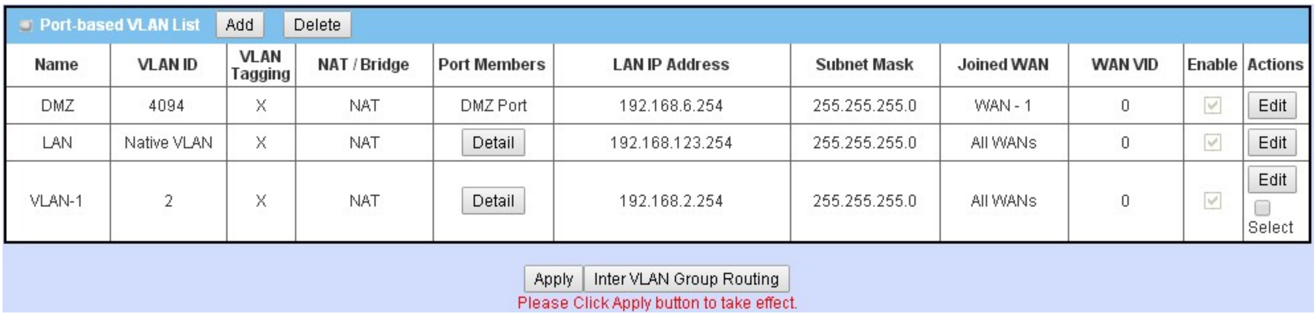
Item	Setting
MAC Address	
IP Address	
Enable	☐

Save

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

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

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



Port-based VLAN List Add Delete

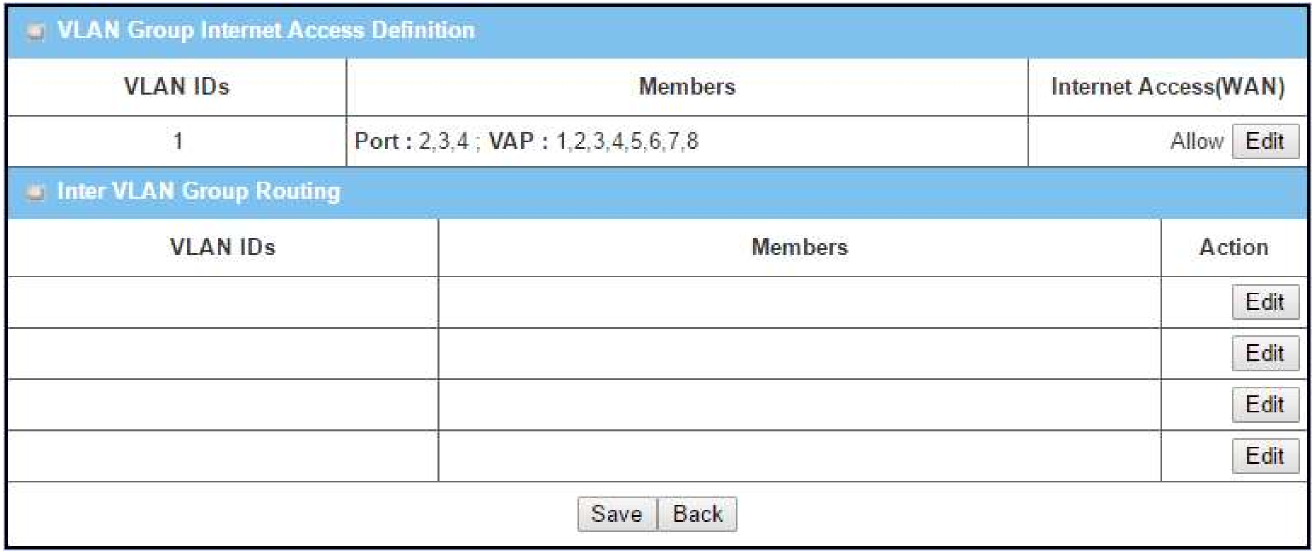
Name	VLAN ID	VLAN Tagging	NAT / Bridge	Port Members	LAN IP Address	Subnet Mask	Joined WAN	WAN VID	Enable	Actions
DMZ	4094	X	NAT	DMZ Port	192.168.6.254	255.255.255.0	WAN - 1	0	☑	Edit
LAN	Native VLAN	X	NAT	Detail	192.168.123.254	255.255.255.0	All WANs	0	☑	Edit
VLAN-1	2	X	NAT	Detail	192.168.2.254	255.255.255.0	All WANs	0	☑	Edit ☐ Select

Apply Inter VLAN Group Routing

Please Click Apply button to take effect.

Port-based VLAN – Inter VLAN Group Routing

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



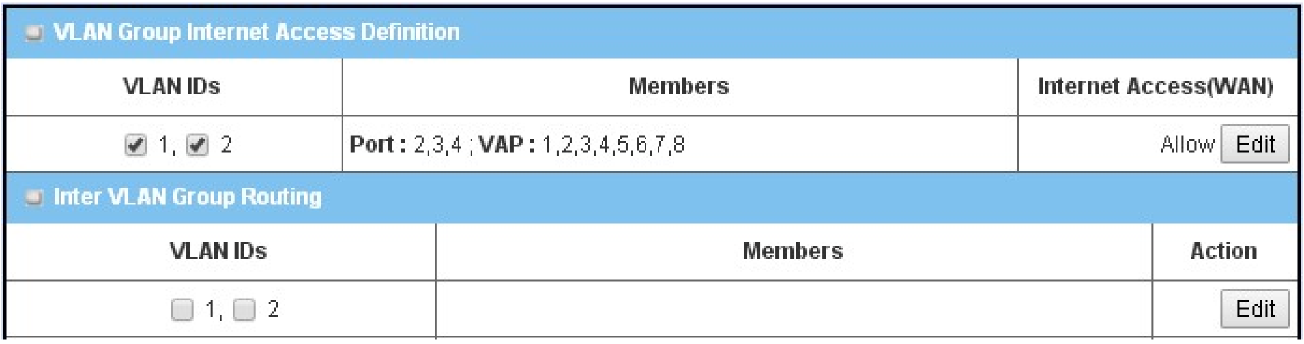
VLAN Group Internet Access Definition

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

Inter VLAN Group Routing

VLAN IDs	Members	Action
		Edit
		Edit
		Edit
		Edit

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



VLAN Group Internet Access Definition

VLAN IDs	Members	Internet Access(WAN)
☑ 1, ☑ 2	Port : 2,3,4 ; VAP : 1,2,3,4,5,6,7,8	Allow Edit

Inter VLAN Group Routing

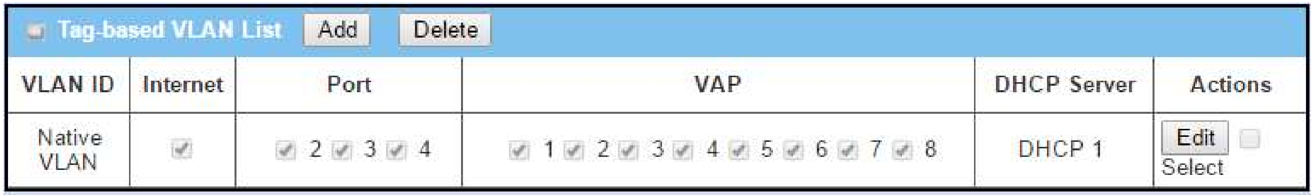
VLAN IDs	Members	Action
☐ 1, ☐ 2		Edit

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

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

Tag-based VLAN – Create/Edit VLAN Rules

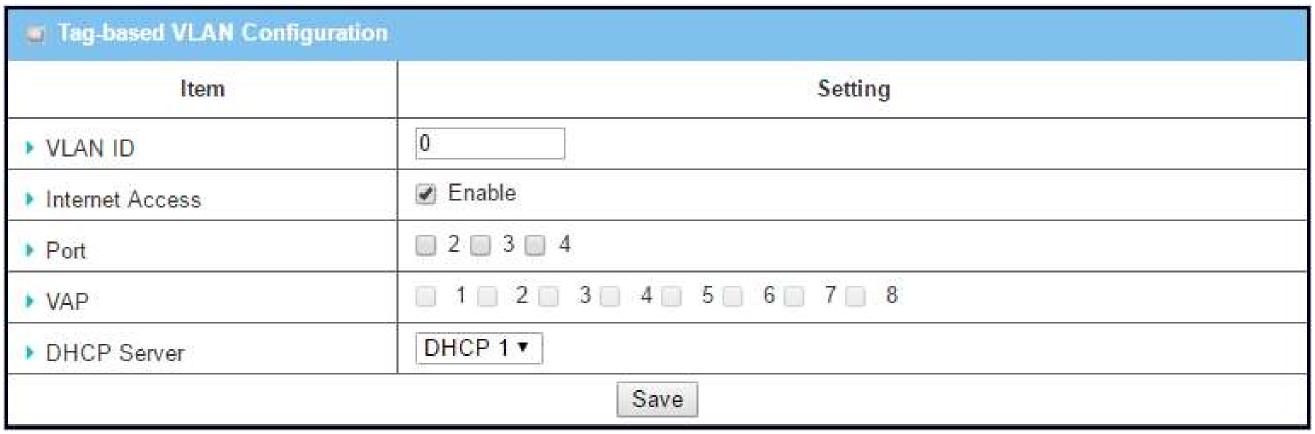
The **Tag-based VLAN** allows you to customize each LAN port according to VLAN ID. There is a default rule shows the configuration of all LAN ports and all VAPs. Also, if your device has a DMZ port, you will see DMZ configuration, too. The router supports up to a maximum of 128 tag-based VLAN rule sets.



Tag-based VLAN List Add Delete

VLAN ID	Internet	Port	VAP	DHCP Server	Actions
Native VLAN	☑	☑ 2 ☑ 3 ☑ 4	☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8	DHCP 1	Edit □ Select

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



Tag-based VLAN Configuration

Item	Setting
VLAN ID	0
Internet Access	☑ Enable
Port	□ 2 □ 3 □ 4
VAP	□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8
DHCP Server	DHCP 1 ▾

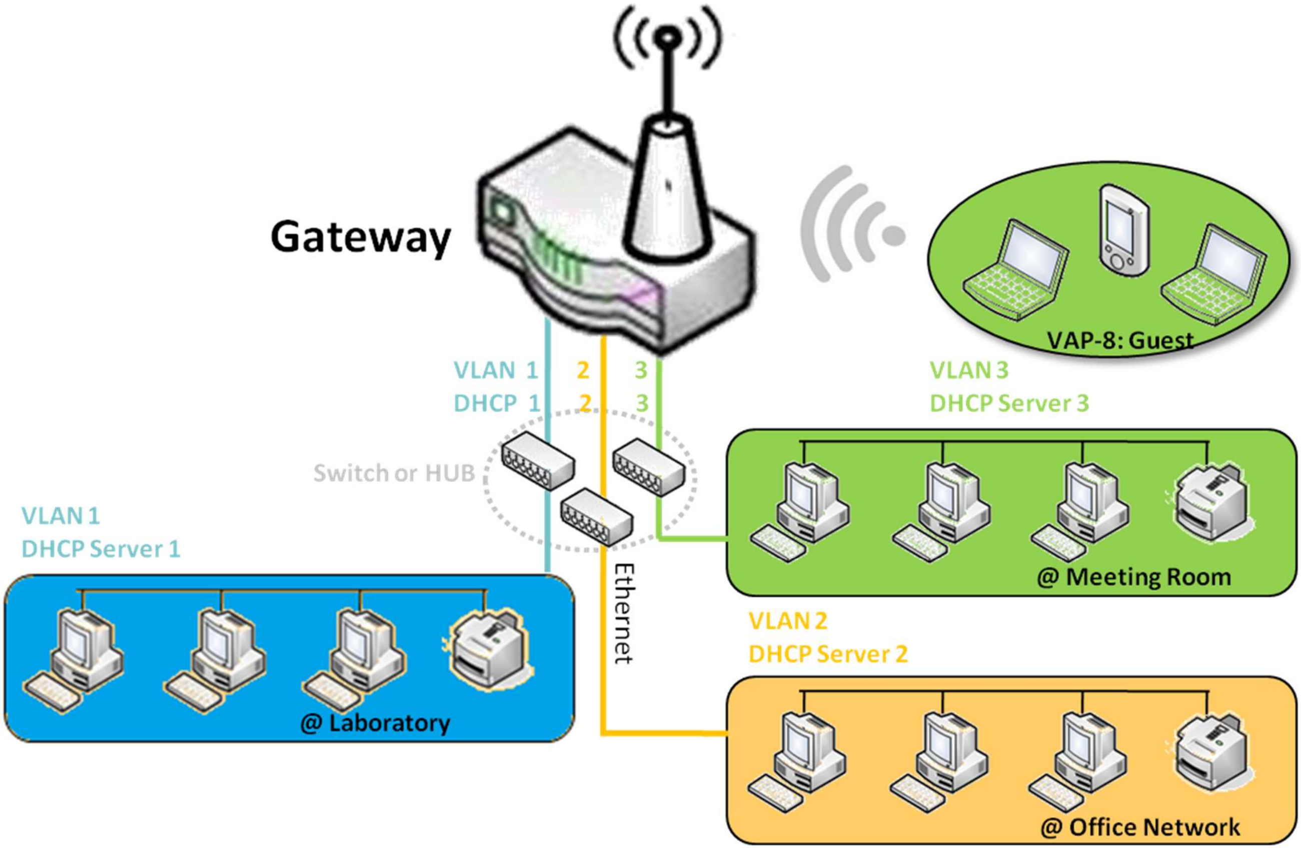
Save

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

3.3.7 DHCP Server

➢ DHCP Server

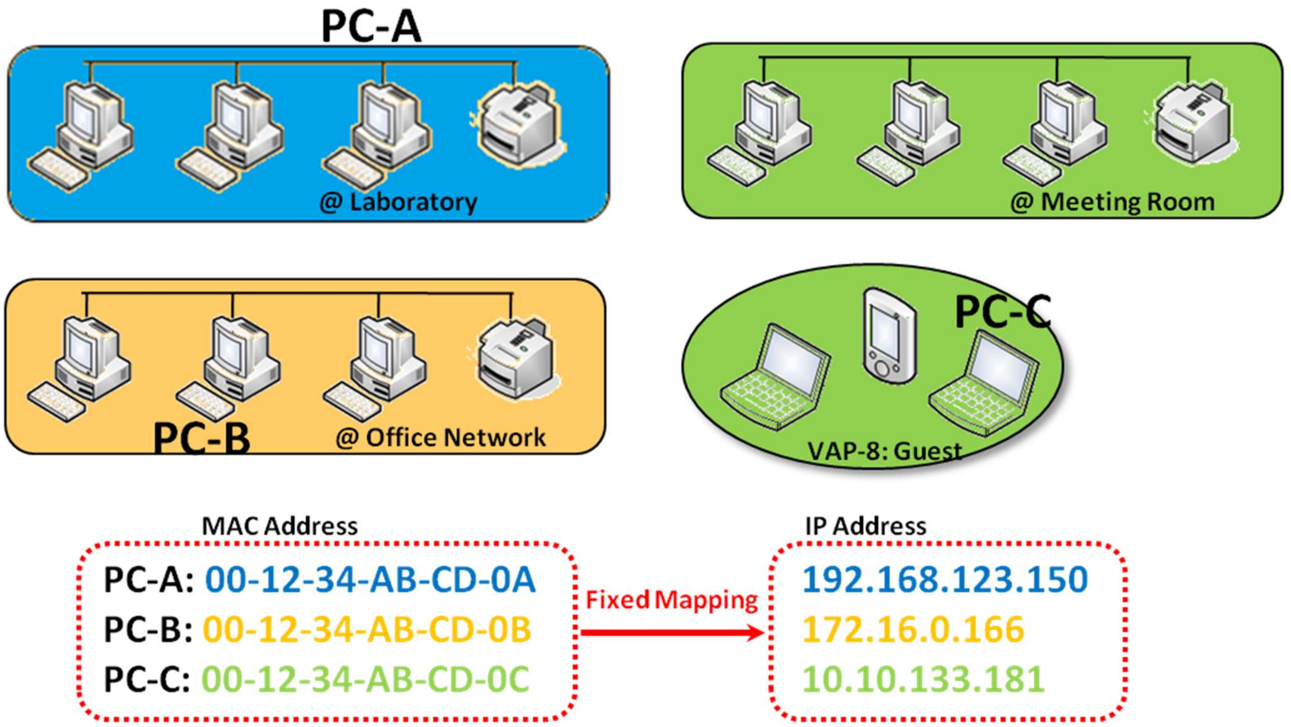
The gateway supports up to 4 DHCP servers to fulfill the DHCP requests from different VLAN groups (please refer to VLAN section for getting more usage details). And there is one default setting for whose LAN IP Address is the same one of gateway LAN interface, with its default Subnet Mask setting as "255.255.255.0", and its default IP Pool ranges is from ".100" to ".200" as shown at the DHCP Server List page on gateway's WEB UI.



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

➢ Fixed Mapping

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



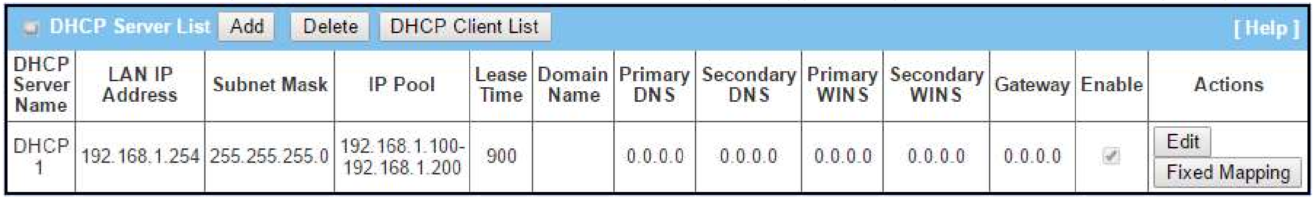
DHCP Server Setting

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

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

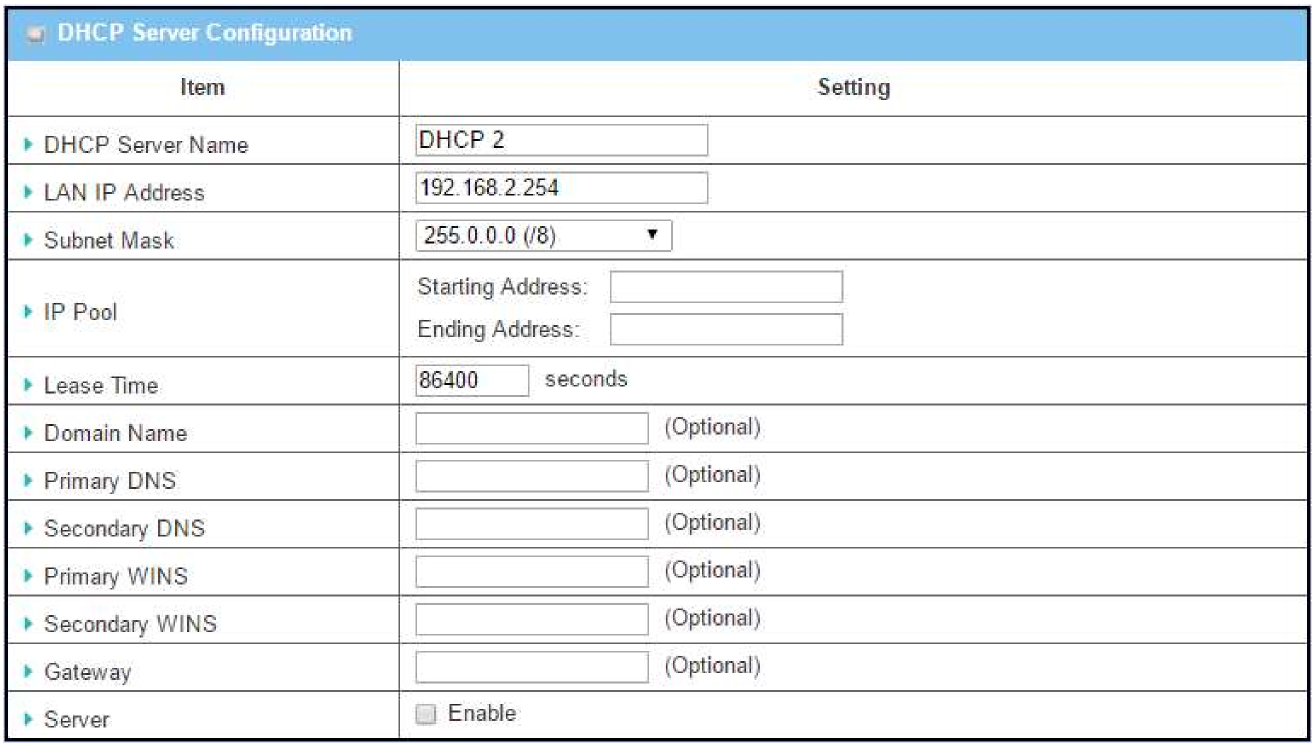
Create/Edit DHCP Server Policy

The router allows you to custom your DHCP Server Policy. It supports up to a maximum of 4 policy sets.



DHCP Server Name	LAN IP Address	Subnet Mask	IP Pool	Lease Time	Domain Name	Primary DNS	Secondary DNS	Primary WINS	Secondary WINS	Gateway	Enable	Actions
DHCP 1	192.168.1.254	255.255.255.0	192.168.1.100- 192.168.1.200	900		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	☑	Edit Fixed Mapping

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

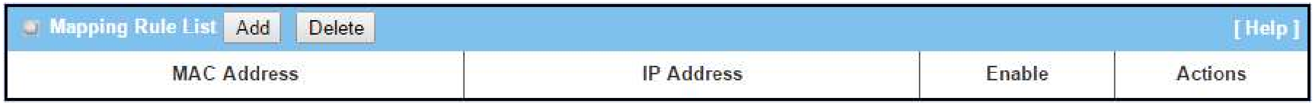


Item	Setting
DHCP Server Name	DHCP 2
LAN IP Address	192.168.2.254
Subnet Mask	255.0.0.0 (/8) ▼
IP Pool	Starting Address: Ending Address:
Lease Time	86400 seconds
Domain Name	(Optional)
Primary DNS	(Optional)
Secondary DNS	(Optional)
Primary WINS	(Optional)
Secondary WINS	(Optional)
Gateway	(Optional)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

DHCP Server Configuration		
Item	**Value setting**	**Description**
DHCP Server Name	1. String format can be any text 2. A Must filled setting	Enter a DHCP Server name. Enter a name that is easy for you to understand.
LAN IP Address	1. IPv4 format. 2. A Must filled setting	The LAN IP Address of this DHCP Server.
Subnet Mask	255.0.0.0 (/8) is set by default	The Subnet Mask of this DHCP Server.
IP Pool	1. IPv4 format. 2. A Must filled setting	The IP Pool of this DHCP Server. It composed of Starting Address entered in this field and Ending Address entered in this field.
Lease Time	1. Numberic string format. 2. A Must filled setting	The Lease Time of this DHCP Server.
Domain Name	String format can be any text	The Domain Name of this DHCP Server.
Primary DNS	IPv4 format	The Primary DNS of this DHCP Server.
Secondary DNS	IPv4 format	The Secondary DNS of this DHCP Server.
Primary WINS	IPv4 format	The Primary WINS of this DHCP Server.
Secondary WINS	IPv4 format	The Secondary WINS of this DHCP Server.
Gateway	IPv4 format	The Gateway of this DHCP Server.
Server	The box is unchecked by default.	Click **Enable** box to activate this DHCP Server.
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore what you just configured back to the previous setting. Please note that the restored setting may not be the factory default setting but a retrieve of what was saved in the memory.
Back	NA	When the **Back** button is clicked the screen will return to the DHCP Server Configuration page.

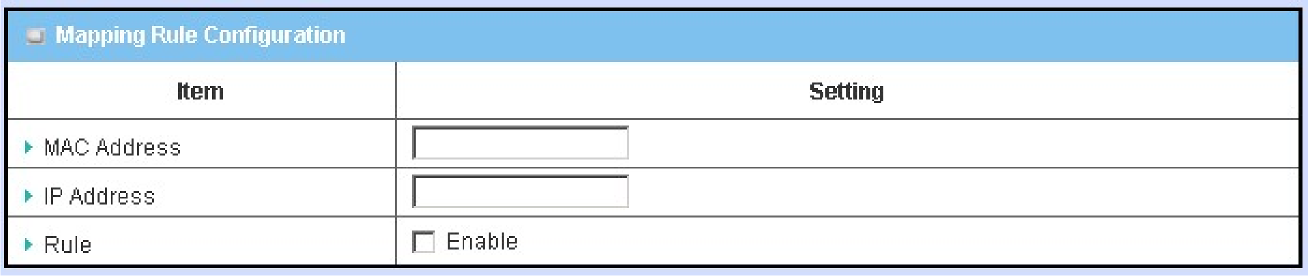
Create/Edit Mapping Rule List on DHCP Server

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



MAC Address	IP Address	Enable	Actions

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



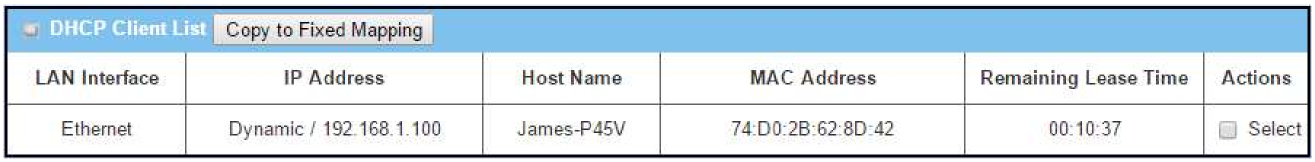
Mapping Rule Configuration

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	The MAC Address of this mapping rule.
IP Address	1. IPv4 format. 2. A Must filled setting	The IP Address of this mapping rule.
Enabling the Rule	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting. Please note that the restored setting may not be the factory default setting but a retrieve of what was saved in the memory.
Back	N/A	When the **Back** button is clicked the screen will return to the **DHCP Server Configuration** page.

View/Copy DHCP Client List

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



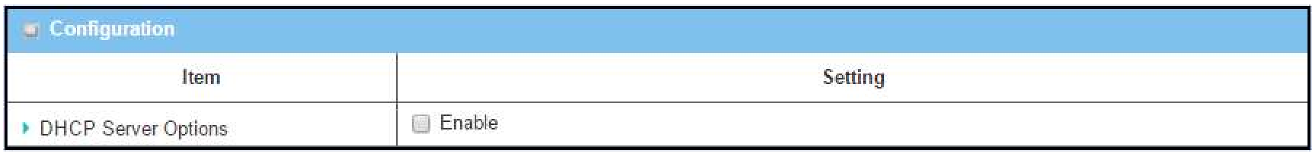
LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time	Actions
Ethernet	Dynamic / 192.168.1.100	James-P45V	74:D0:2B:62:8D:42	00:10:37	□ Select

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

Enable/Disable DHCP Server Options

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

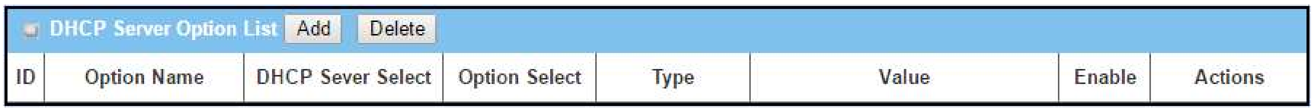
Option	Meaning	RFC
66	TFTP server name	[RFC 2132]
72	Default World Wide Web Server	[RFC 2132]
114	URL	[RFC 3679]



Item	Setting
DHCP Server Options	□ Enable

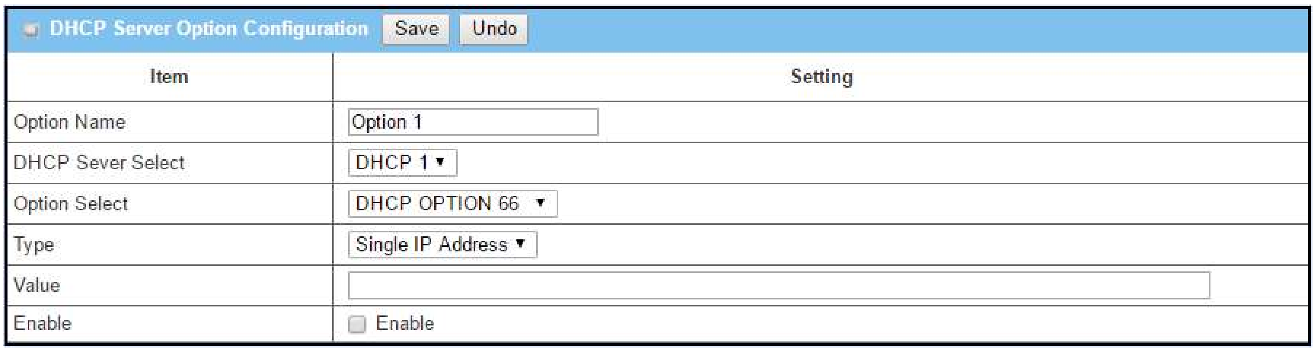
Create/Edit DHCP Server Options

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



ID	Option Name	DHCP Sever Select	Option Select	Type	Value	Enable	Actions

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



DHCP Server Option Configuration

Item	Setting
Option Name	Option 1
DHCP Sever Select	DHCP 1 ▾
Option Select	DHCP OPTION 66 ▾
Type	Single IP Address ▾
Value	
Enable	□ Enable

<table>
<tr><th colspan="5">DHCP Server Option Configuration</th></tr>
<tr><th>Item</th><th>Value setting</th><th colspan="3">Description</th></tr>
<tr><td><b>Option Name</b></td><td>1. String format can be any text
2. A Must filled setting</td><td colspan="3">Enter a DHCP Server Option name. Enter a name that is easy for you to understand.</td></tr>
<tr><td><b>DHCP Server Select</b></td><td>Dropdown list of all available DHCP servers.</td><td colspan="3">Choose the DHCP server this option should apply to.</td></tr>
<tr><td><b>Option Select</b></td><td>Dropdown list
66 - tftp
72 – www
114 - url</td><td colspan="3">Choose the specific option you want to set.</td></tr>
<tr><td rowspan="5"><b>Type</b></td><td rowspan="5">Dropdown list of DHCP server option value’s type</td><td colspan="3">Each different options has different value types.</td></tr>
<tr><td rowspan="2">66</td><td colspan="2">Single IP Address</td></tr>
<tr><td colspan="2">Single FQDN</td></tr>
<tr><td>72</td><td colspan="2">IP Addresses List, separated by “,”</td></tr>
<tr><td>114</td><td colspan="2">Single URL</td></tr>
<tr><td rowspan="5"><b>Value</b></td><td rowspan="5">1. IPv4 format
2. FQDN format
3. IP list
4. URL format
5. A Must filled setting</td><td colspan="3">Should conform to Type :</td></tr>
<tr><td></td><td>Type</td><td>Value</td></tr>
<tr><td rowspan="2">66</td><td>Single IP Address</td><td>IPv4 format</td></tr>
<tr><td>Single FQDN</td><td>FQDN format</td></tr>
<tr><td>72</td><td>IP Addresses List, separated by “,”</td><td>IPv4 format, separated by “,”</td></tr>
</table>

		114	Single URL	URL format
Enable	The box is unchecked by default.	Click **Enable** box to activate this setting.		
Save	*NA*	Click the **Save** button to save the setting.		
Undo	*NA*	When the **Undo** button is clicked the screen will return back with nothing changed.		

3.5 WiFi

The device may provide WiFi interface for mobile devices or BYOD devices to connect for Internet accessing. The WiFi system in the device complies with 802.11ac/11n/11g/11b standard in 2.4GHz single band or 2.4G/5GHz concurrent dual bands of operation. There are several wireless operation modes provided by this device. They are: "**AP Router Mode**", "**WDS Only Mode**", and "**WDS Hybrid Mode**". You can choose the expected mode from the wireless operation mode list.

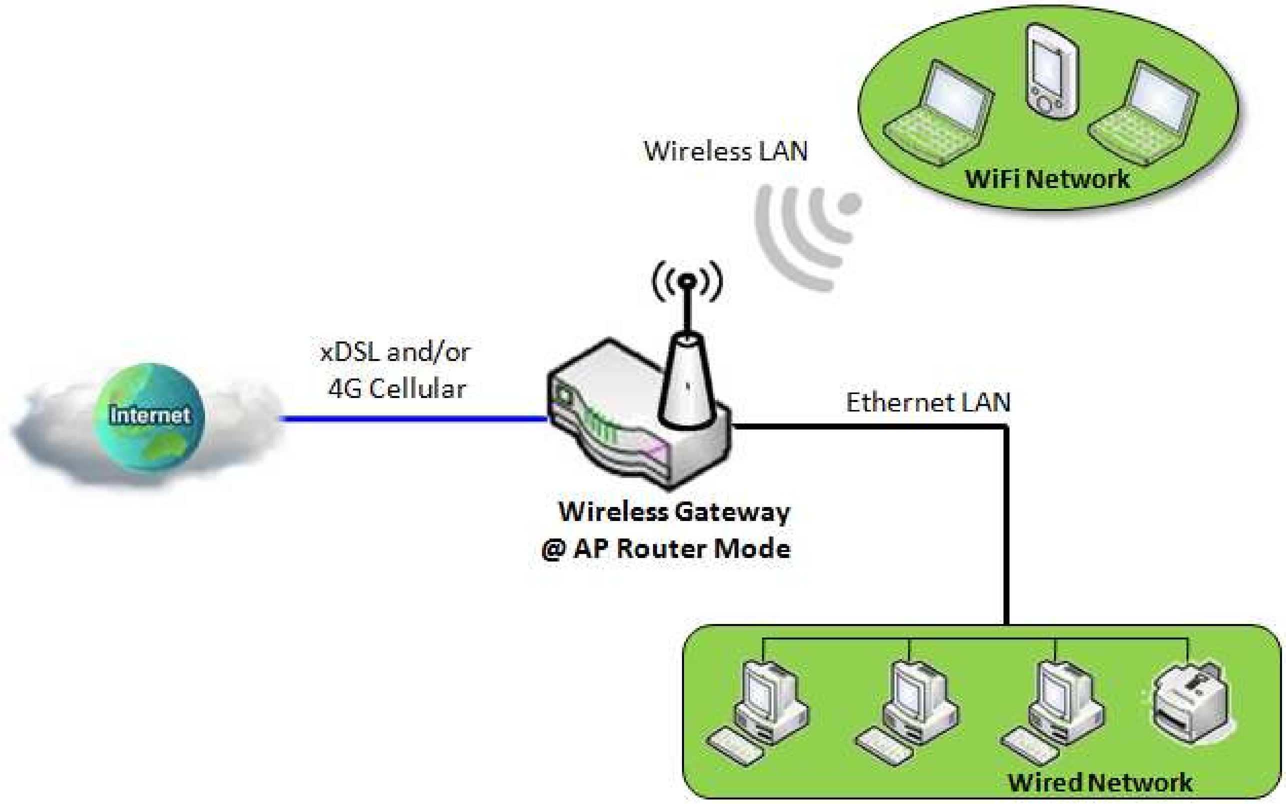
There are some sub-sections for you to configure the WiFi function. In the first WiFi Configuration section, you have to finish almost all the settings for using the WiFi function, including the operation mode, optional VAP settings, Channel, WiFi System, Authentication & Encryption key, and Station / VAP isolation settings. In Wireless Client List section, it provides a quick solution for you to know the information of connected wireless clients. And the Advanced Configuration section provides more parameters for advanced user to fine tune the connectivity performance for the WiFi function.

Hereunder is the scenarios for each wireless operation mode, you can get how it works, and what is the difference among them. To connect your wireless devices with the wireless gateway, make sure your application scenario for WiFi network and choose the most adequate operation mode.

➢ AP Router Mode

This mode allows you to get your wired and wireless devices connected to form the Intranet of the wireless gateway, and the Intranet will link to the Internet with NAT mechanism of the gateway. So, this gateway is working as a WiFi AP, but also a WiFi hotspot for Internet accessing service. It means local WiFi clients can associate to it, and go to Internet. With its NAT mechanism, all of wireless clients don't need to get public IP addresses from ISP.

Following diagram illustrates the wireless gateway that is running at AP Router operation mode.

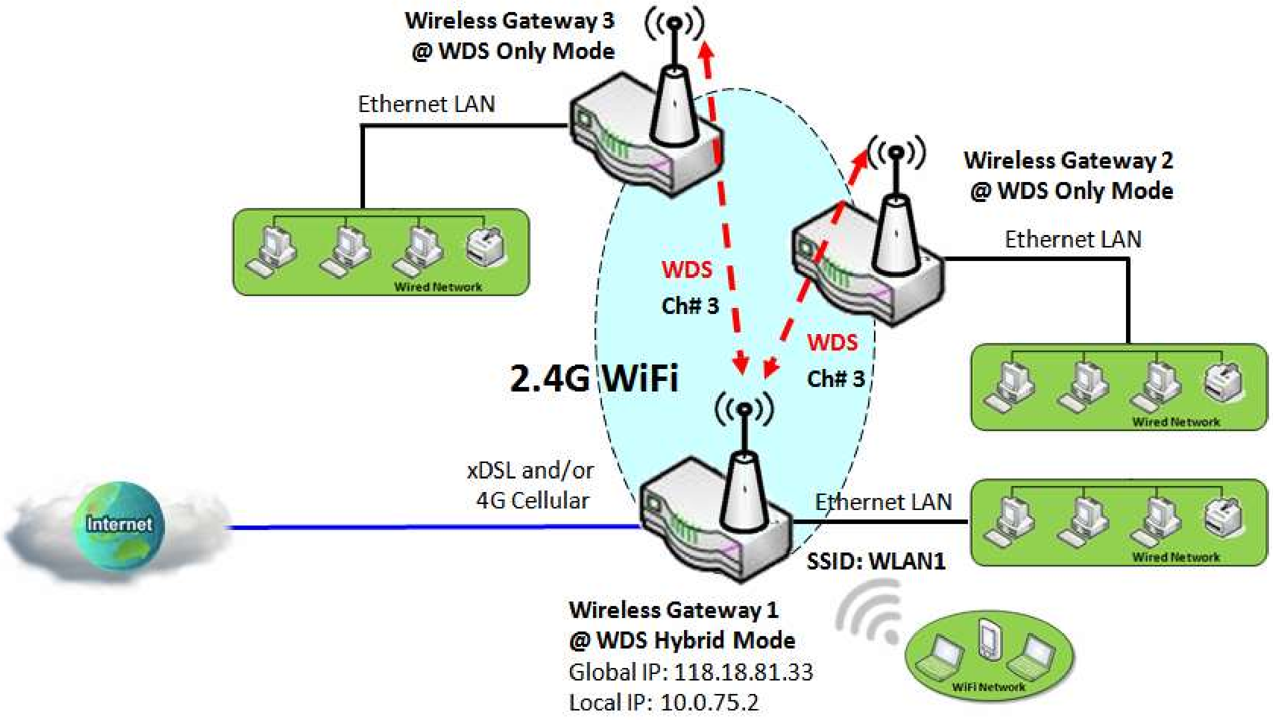


➢ WDS Only Mode & WDS Hybrid Mode

WDS (Wireless Distributed System) Only mode drives a wireless gateway to be a WiFi repeater for its wired Intranet. But WDS Hybrid mode drives it act as an access point for its WiFi Intranet and a WiFi repeater for its wired and WiFi Intranets at the same time. Users can thus use the features to build up a large wireless network in a large space like airports, hotels and schools …etc.

While acting as a wireless bridge, multiple wireless gateways running at "WDS Only" or "WDS Hybrid" mode link together so that they can communicate with each other through wireless interface (with WDS). Thus all client hosts in their wired Intranets or WiFi Intranets can also communicate each other in the scenario.

Following diagram illustrates that there are two remote wireless gateways running at "WDS Only" operation mode. They both use channel 3 to link to the local Wireless Gateway 1 through WDS approach, but the local gateway is running at "WDS Hybrid" mode and has an Internet connection. And their wired Intranets can thus access the Internet through the Wireless Gateway 1 since these three wireless gateways have been linked together by WDS. Please be noted that the gateways running at "WDS Only" mode will disable any DHCP server by default, so the client hosts under the gateways will request their IP address from the Wireless Gateway 1 that has at least one DHCP server working. Besides, the Wireless Gateway 1 also execute the NAT mechanism for Internet accessing. That is, the gateway at "WDS Only" mode provides WiFi bridge to other gateways without embedded DHCP server and NAT. However, the gateway at "WDS Hybrid" mode joins in a WDS link network, provides DHCP servers for IP assigning and executes NAT function for Internet accessing.

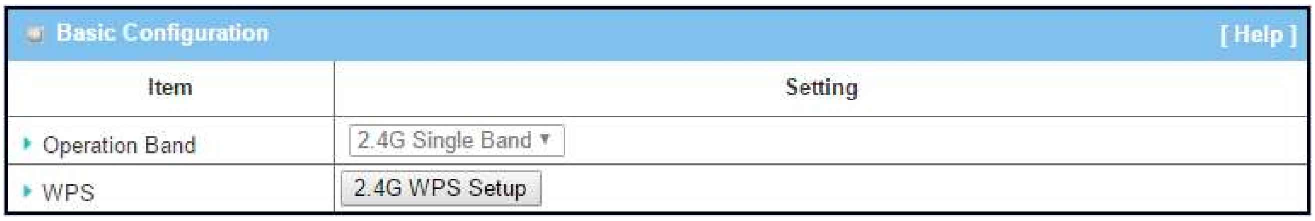


3.5.1 WiFi Configuration

The Wi-Fi configuration allows user to configure 2.4G or 5G Wi-Fi setting, such as SSID or pre-shared key.

Go to **Basic Network > WiFi > WiFi Module One** Tab. If the gateway is equipped with two WiFi module, there will be another **WiFi Module Two**. You can do the similar configurations on both WiFi modules.

Basic Configuration

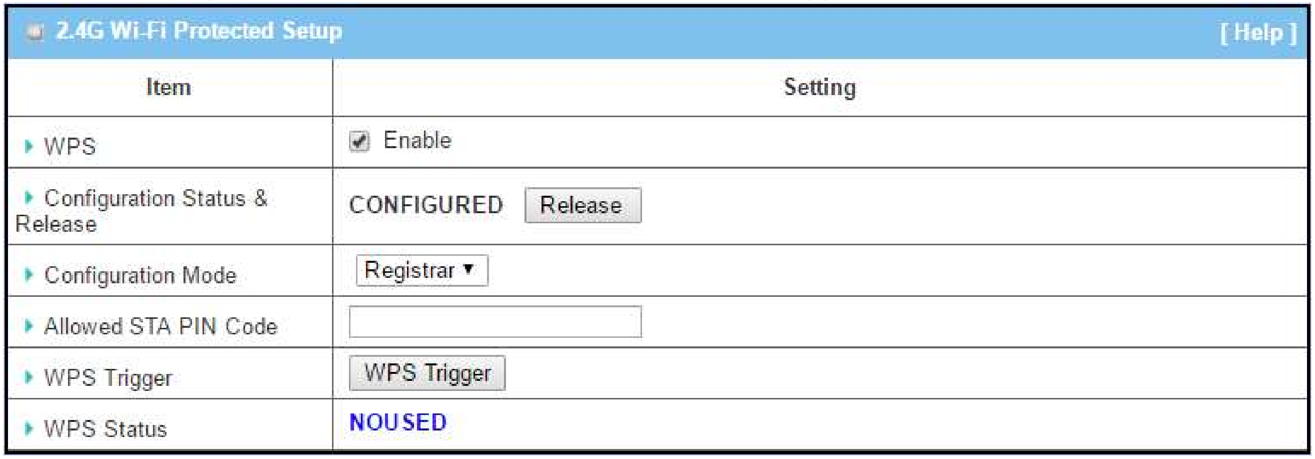


Basic Configuration [Help]

Item	Setting
Operation Band	2.4G Single Band ▾
WPS	2.4G WPS Setup

Basic Configuration		
Item	**Value setting**	**Description**
Operation Band	A Must filled setting	Specify the intended operation band for the WiFi module. Basically, this setting is fixed and cannot be changed once the module is integrated into the gaye product. However, there are some module with selectable band for user to choose according to his network environment. Under such situation, you can specify which operation band is suitable for the application.
WPS	N/A	Press 2.4G or 5G button will lead user to **Wi-Fi Protected Setup** page. Refer to the next sub-section **Wi-Fi Protected Setup** for more details.

When **WPS Setup** button is clicked, a screen similar to this will appear



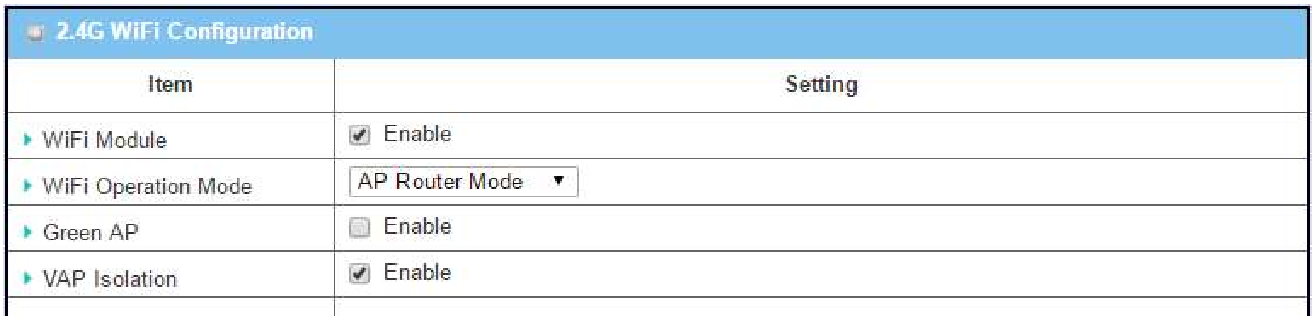
2.4G Wi-Fi Protected Setup [Help]

Item	Setting
WPS	☑ Enable
Configuration Status & Release	CONFIGURED Release
Configuration Mode	Registrar ▾
Allowed STA PIN Code	
WPS Trigger	WPS Trigger
WPS Status	NOUSED

Wi-Fi Protected Setup

Item	Value setting	Description
WPS	The box is checked by default.	Check the **Enable** box to activate WPS function.
Configuration Status	N/A	The configuration status of AP is displayed here. Press **Set/Release** button to change the configuration status. ● **UNCONFIGURED** It means the AP settings is not configured by WPS. The status will change to **CONFIGURED** after WPS. ● **CONFIGURED** It means the AP settings has been configured by WPS.
Configuration Mode	A Must filled setting	Select WPS configuration mode from **Registrar** or **Enrollee**. When **Registrar** is selected It means the AP will play a role of **Registrar** in WPS process. ● **Allowed STA PIN Code** Enter the PIN code which client given. ● Press **Save** button to save the current configuration. ● **WPS Trigger** Start WPS action. (Make sure **Save** configuration before **Triggering WPS**.) • Press **Save** button to save the current configuration. When **Enrollee** is selected It means the AP will play a role of **Enrollee** in WPS process. ● AP PIN Code & New Generate The **AP PIN Code** provides **external Registrar** to enter. **New Generate** button will generate a new PIN code. ● Press **Save** button to save the current configuration.
WPS Status	N/A	It shows the current WPS status of progress. ● **NOUSED** **:** WPS function is disabled. ● **IDLE** **:** WPS function is ready. ● **STARTPROCESS** **:** WPS function is starting and processing now. ● **CONFIGURED** **:** WPS finished process successfully. ● **PROCESSFAIL** **:** WPS process failed.
Undo	N/A	Press the **Undo** button to restore configuration to previous setting before saving. Note that some settings would not take effect from **Undo** button, such as **New Generate** or **Set/Release**.
Back	N/A	Press the **Back** button to return to the **Wi-Fi Configuration** page.

Configure WiFi Setting



2.4G WiFi Configuration

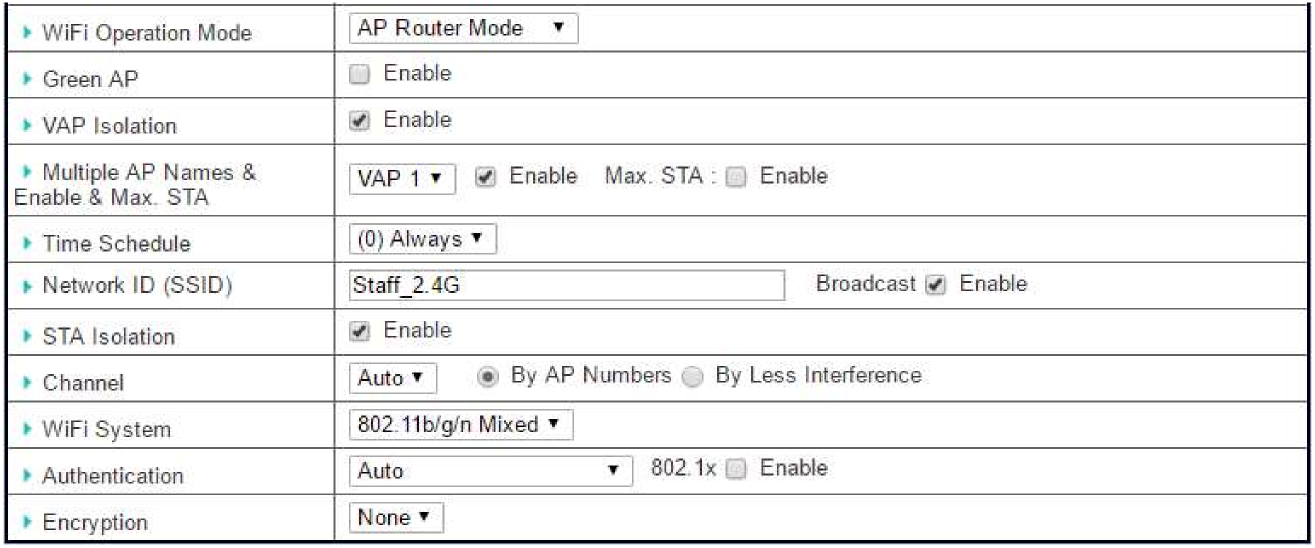
Item	Setting
WiFi Module	☑ Enable
WiFi Operation Mode	AP Router Mode ▼
Green AP	□ Enable
VAP Isolation	☑ Enable

Configuring Wi-Fi Settings		
Item	**Value setting**	**Description**
WiFi Module	The box is checked by default	Check the **Enable** box to activate Wi-Fi function.
WiFi Operation Mode		Specify the **WiFi Operation Mode** accroding to your application. Go to the following table for **AP Router Mode**, **WDS Only Mode**, **WDS Hybrid Mode**, **Universal Repeater Mode**, **AP Only Mode**, and **CLient Mode** settings. The available operation modes are depend on the product specification.

In the following, the specific configuration description for each WiFi operation mode is given.

AP Router Mode

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



WiFi Operation Mode	AP Router Mode ▼
Green AP	□ Enable
VAP Isolation	☑ Enable
Multiple AP Names & Enable & Max. STA	VAP 1 ▼ ☑ Enable Max. STA : □ Enable
Time Schedule	(0) Always ▼
Network ID (SSID)	Staff_2.4G Broadcast ☑ Enable
STA Isolation	☑ Enable
Channel	Auto ▼ ● By AP Numbers ○ By Less Interference
WiFi System	802.11b/g/n Mixed ▼
Authentication	Auto ▼ 802.1x □ Enable
Encryption	None ▼

AP Router Mode		
Item	**Value setting**	**Description**

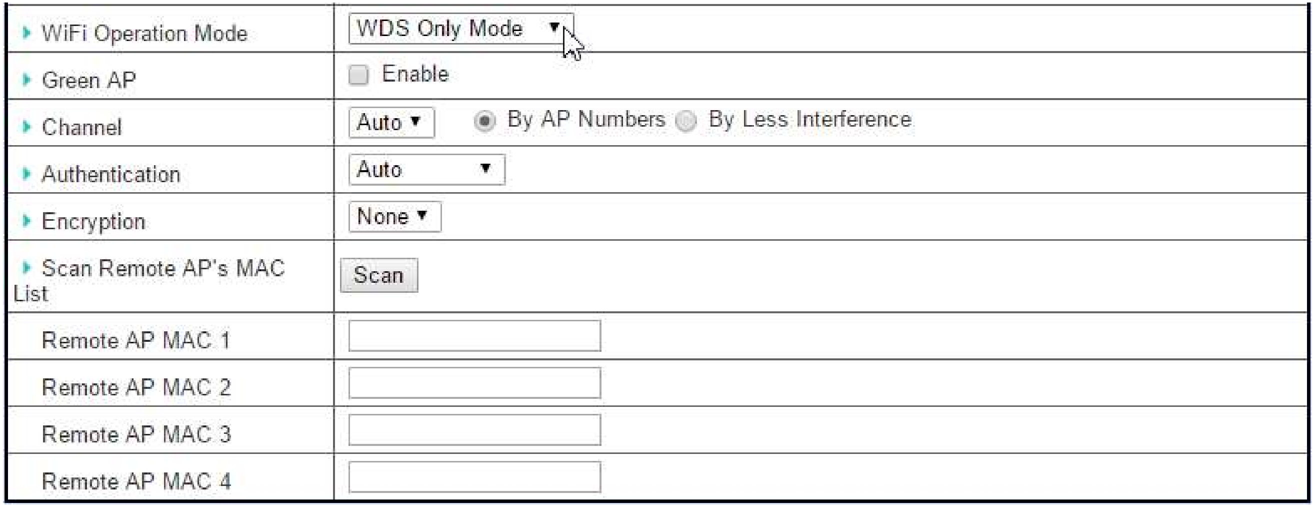
Green AP	The box is unchecked by default.	Check the **Enable** box to activate **Green AP** function.
VAP Isolation	The box is checked by default.	Check the **Enable** box to activate this function. By default, the box is checked, it means that stations which associated to different VAPs cannot communicate with each other.
Multiple AP Names	1. A Must filled setting 2. VAP1 and VAP8 are activated by default.	● **Multiple AP Names (VAP)** It means **multiple SSID** feature and the device support up to 8 **virtual SSIDs.** Select one of VAP to configure its setting at a time. ● **Enable** Check the **enable** box to activate the selected VAP. ● **Max. STA** Limit the maximum number of client station. Check this box and enter a limitation. The box is unchecked (unlimited) by default.
Time Schedule	A Must filled setting	Apply a specific **Time Schedule** to this rule, otherwise leave it as **(0) Always**. If the dropdown list is empty ensure **Time Schedule** is pre-configured. Refer to **Object Definition** > **Scheduling > Configuration** tab.
Network ID (SSID)	1. String format : Any text 2. The box is checked by default.	Enter the SSID for the VAP, and decide whether to broadcast the SSID or not. The **SSID** is used for identifying from another AP, and client stations will associate with AP according to SSID. If the broadcast SSID option is enabled, it means the SSID will be broadcasted, and the stations can associate with this device by scanning SSID.
STA Isolation	The box is checked by default.	Check the **Enable** box to activate this function. By default, the box is checked, it means that stations which associated to the same VAP cannot communicate with each other.
Channel	1. A Must filled setting. 2. **Auto** is selected be default.	Select a radio channel for the VAP. Each channel is corresponding to different radio band. 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 AP numbers (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 WiFi System. The dropdown list of **Wi-Fi system** is based on **IEEE 802.11** standard. ● **2.4G Wi-Fi** can select b, g and n only or mixed with each other. ● **5G Wi-Fi** can select a, n and ac only or mixed with each other.
Authentication	1. A Must filled setting 2. **Auto** is selected be default.	For security, there are several authentication methods supported. Client stations should provide the key when associate with this device. When **Open** is selected The check box named **802.1x** shows up next to the dropdown list. ● **802.1x** (The box is unchecked by default) When **802.1x** is enabled, it means the client stations will be authenticated by RADIUS server. **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 The preshared WEP key should be set for authenticating.
		When **Auto** is selected The device will select **Open** or **Shared** by requesting of client automatically. The check box named **802.1x** shows up next to the dropdown list. ● **802.1x** (The box is unchecked by default) When **802.1x** is enabled, it means the client stations will be authenticated by RADIUS server. **RADIUS Server IP** (The default IP is 0.0.0.0) **RADIUS Server Port** (The default value is 1812) **RADIUS Shared Key**
		When **WPA** or **WPA2** is selected They are implementation of IEEE 802.11i. **WPA** only had implemented part of IEEE 802.11i, but owns the better **compatibility**. **WPA2** had fully implemented 802.11i standard, and owns the highest **security**. ● **RADIUS Server** The client stations will be authenticated by RADIUS server. **RADIUS Server IP** (The default IP is 0.0.0.0) **RADIUS Server Port** (The default value is 1812) **RADIUS Shared Key**
		When **WPA** / **WPA2** is selected It owns the same setting as **WPA** or **WPA2**. The client stations can associate with this device via **WPA** or **WPA2**.
		When **WPA-PSK** or **WPA2-PSK** is selected It owns the same encryption system as WPA or WPA2. The authentication uses pre-shared key instead of RADIUS server.
		When **WPA-PSK** / **WPA2-PSK** is selected It owns the same setting as **WPA-PSK** or **WPA2-PSK**. The client stations can associate with this device via **WPA-PSK** or **WPA2-PSK**.
Encryption	1. A Must filled setting. 2. **None** is selected be default.	Select a suitable encryption method and enter the required key(s). The available method in the dropdown list depends on the Authentication you selected. **None** It means that the device is open system without encrypting. **WEP** Up to 4 WEP keys can be set, and you have to select one as current key. The key type can 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 ASCII table. **TKIP** TKIP was proposed instead of WEP without upgrading hardware. Enter a Preshared Key for it. The length of key is from 8 to 63 characters. **AES** The newest encryption system in WiFi, it also designed for the fast 802.11n high bitrates schemes. Enter a Preshared Key for it. The length of key is from 8 to 63 characters. You are recommended to use **AES** encryption instead of any others for

		security. **TKIP / AES** **TKIP / AES** mixed mode. It means that the client stations can associate with this device via **TKIP** or **AES**. Enter a Preshared Key for it. The length of key is from 8 to 63 characters.
Save	N/A	Click the **Save** button to save the current configuration.
Undo	N/A	Click the **Undo** button to restore configuration to previous setting before saving.
Apply	N/A	Click the **Apply** button to apply the saved configuration.

WDS Only Mode

For the WDS Only mode, the device only bridges the connected wired clients to another WDS-enabled Wi-Fi device which the device associated with. That is, it also means the no wireless clients stat can connect to this device while WDS Only Mode is selected.



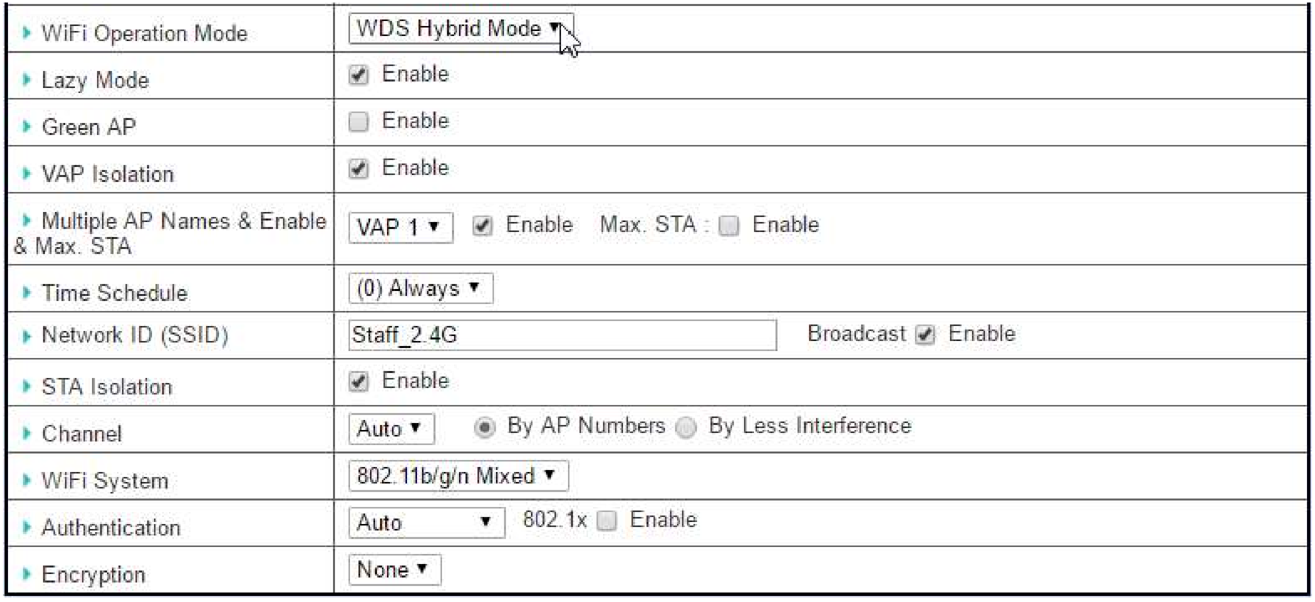
WiFi Operation Mode	WDS Only Mode ▾
Green AP	□ Enable
Channel	Auto ▾ ● By AP Numbers ○ By Less Interference
Authentication	Auto ▾
Encryption	None ▾
Scan Remote AP's MAC List	Scan
Remote AP MAC 1	
Remote AP MAC 2	
Remote AP MAC 3	
Remote AP MAC 4	

WDS Only Mode		
Item	Value setting	Description
Green AP	The box is unchecked by default.	Check the **Enable** box to activate **Green AP** function.
Channel	1. A Must filled setting. 2. **Auto** is selected be default.	Select a radio channel for the VAP. Each channel is corresponding to different radio band. 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 AP numbers (The less, the better). ● **By Less Interference** The channel will be selected according to interference. (The lower, the better).
Authentication	1. A Must filled setting 2. **Auto** is selected be default.	For security, there are several authentication methods supported. Client stations should provide the key when associate with this device.
		When **Open** is selected The check box named **802.1x** shows up next to the dropdown list. ● **802.1x** (The box is unchecked by default) When **802.1x** is enabled, it means the client stations will be authenticated by RADIUS server. **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 The preshared WEP key should be set for authenticating.

		When **Auto** is selected The device will select **Open** or **Shared** by requesting of client automatically. The check box named **802.1x** shows up next to the dropdown list. ● **802.1x** (The box is unchecked by default) When **802.1x** is enabled, it means the client stations will be authenticated by RADIUS server. **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** is selected It owns the same encryption system as WPA. The authentication uses pre-shared key instead of RADIUS server.
		When **WPA2-PSK** is selected It owns the same encryption system as WPA2. The authentication uses pre-shared key instead of RADIUS server.
Encryption	1. A Must filled setting. 2. **None** is selected be default.	Select a suitable encryption method and enter the required key(s). The available method in the dropdown list depends on the Authentication you selected. **None** It means that the device is open system without encrypting. **WEP** Up to 4 WEP keys can be set, and you have to select one as current key. The key type can 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 ASCII table. **TKIP** TKIP was proposed instead of WEP without upgrading hardware. Enter a Preshared Key for it. The length of key is from 8 to 63 characters. **AES** The newest encryption system in WiFi, it also designed for the fast 802.11n high bitrates schemes. Enter a Preshared Key for it. The length of key is from 8 to 63 characters. You are recommended to use **AES** encryption instead of any others for security.
Scan Remote AP's MAC List	N/A	Press the **Scan** button to scan the spatial AP information, and then select one from the AP list, the MAC of selected AP will be auto filled in the following Remote AP MAC table.
Remote AP MAC 1~4	A Must filled setting	Enter the remote AP's MAC manually, or via auto-scan approach, The device will bridge the traffic to the remote AP when associated successfully.
Save	N/A	Click the **Save** button to save the current configuration.
Undo	N/A	Click the **Undo** button to restore configuration to previous setting before saving.
Apply	N/A	Click the **Apply** button to apply the saved configuration.

WDS Hybrid Mode

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



WiFi Operation Mode	WDS Hybrid Mode ▾
Lazy Mode	☑ Enable
Green AP	□ Enable
VAP Isolation	☑ Enable
Multiple AP Names & Enable & Max. STA	VAP 1 ▾ ☑ Enable Max. STA : □ Enable
Time Schedule	(0) Always ▾
Network ID (SSID)	Staff_2.4G Broadcast ☑ Enable
STA Isolation	☑ Enable
Channel	Auto ▾ ● By AP Numbers ○ By Less Interference
WiFi System	802.11b/g/n Mixed ▾
Authentication	Auto ▾ 802.1x □ Enable
Encryption	None ▾

WDS Hybrid Mode		
Item	**Value setting**	**Description**
Lazy Mode	The box is checked by default.	Check the **Enable** box to activate this function. With the function been enabled, the device can auto-learn WDS peers without manually entering other AP's MAC address. But at least one of the APs has to fill remote AP MAC addresses.
Green AP	The box is unchecked by default.	Check the **Enable** box to activate **Green AP** function.
VAP Isolation	The box is checked by default.	Check the **Enable** box to activate this function. By default, the box is checked, it means that stations which associated to different VAPs cannot communicate with each other.
Multiple AP Names	1. A Must filled setting 2. VAP1 and VAP8 are activated by default.	● **Multiple AP Names (VAP)** It means **multiple SSID** feature and the device support up to 8 **virtual SSIDs.** Select one of VAP to configure its setting at a time. ● **Enable** Check the **enable** box to activate the selected VAP. ● **Max. STA** Limit the maximum number of client station. Check this box and enter a limitation. The box is unchecked (unlimited) by default.
Time Schedule	A Must filled setting	Apply a specific **Time Schedule** to this rule, otherwise leave it as **(0) Always**. If the dropdown list is empty ensure **Time Schedule** is pre-configured. Refer to **Object Definition** > **Scheduling > Configuration** tab.
Network ID (SSID)	1. String format : Any text	Enter the SSID for the VAP, and decide whether to broadcast the SSID or not.

	2. The box is checked by default.	The **SSID** is used for identifying from another AP, and client stations will associate with AP according to SSID. If the broadcast SSID option is enabled, it means the SSID will be broadcasted, and the stations can associate with this device by scanning SSID.
STA Isolation	The box is checked by default.	Check the **Enable** box to activate this function. By default, the box is checked, it means that stations which associated to the same VAP cannot communicate with each other.
Channel	1. A Must filled setting. 2. **Auto** is selected be default.	Select a radio channel for the VAP. Each channel is corresponding to different radio band. 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 AP numbers (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 WiFi System. The dropdown list of **Wi-Fi system** is based on **IEEE 802.11** standard. ● **2.4G Wi-Fi** can select b, g and n only or mixed with each other. ● **5G Wi-Fi** can select a, n and ac only or mixed with each other.
Authentication	1. A Must filled setting 2. **Auto** is selected be default.	For security, there are several authentication methods supported. Client stations should provide the key when associate with this device.
		When **Open** is selected The check box named **802.1x** shows up next to the dropdown list. ● **802.1x** (The box is unchecked by default) When **802.1x** is enabled, it means the client stations will be authenticated by RADIUS server. **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 The preshared WEP key should be set for authenticating.
		When **Auto** is selected The device will select **Open** or **Shared** by requesting of client automatically. The check box named **802.1x** shows up next to the dropdown list. ● **802.1x** (The box is unchecked by default) When **802.1x** is enabled, it means the client stations will be authenticated by RADIUS server. **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** is selected It owns the same encryption system as WPA. The authentication uses pre-shared key instead of RADIUS server.
		When **WPA2-PSK** is selected It owns the same encryption system as WPA2. The authentication uses pre-shared key instead of RADIUS server.
Encryption	1. A Must filled setting.	Select a suitable encryption method and enter the required key(s).

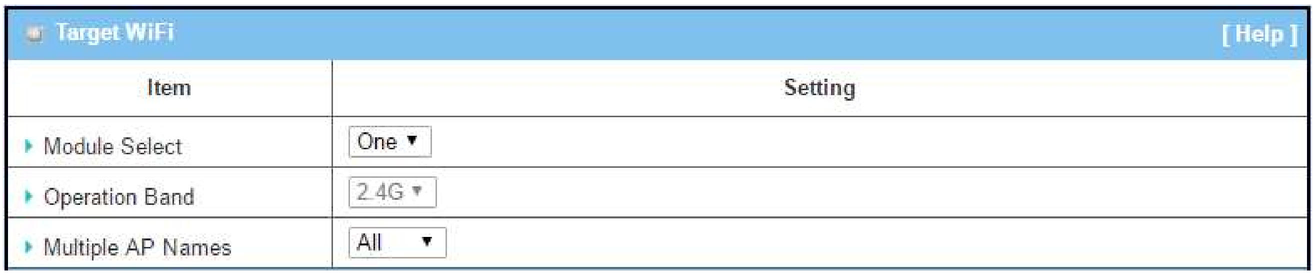
	2. **None** is selected be default.	The available method in the dropdown list depends on the Authentication you selected. **None** It means that the device is open system without encrypting. **WEP** Up to 4 WEP keys can be set, and you have to select one as current key. The key type can set to **HEX** 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 ASCII table. **TKIP** TKIP was proposed instead of WEP without upgrading hardware. Enter a Preshared Key for it. The length of key is from 8 to 63 characters. **AES** The newest encryption system in WiFi, it also designed for the fast 802.11n high bitrates schemes. Enter a Preshared Key for it. The length of key is from 8 to 63 characters. You are recommended to use **AES** encryption instead of any others for security.
Save	N/A	Click the **Save** button to save the current configuration.
Undo	N/A	Click the **Undo** button to restore configuration to previous setting before saving.
Apply	N/A	Click the **Apply** button to apply the saved configuration.

3.5.3 Wireless Client List

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

Go to **Basic Network > WiFi > Wireless Client List** Tab.

Select Target WiFi



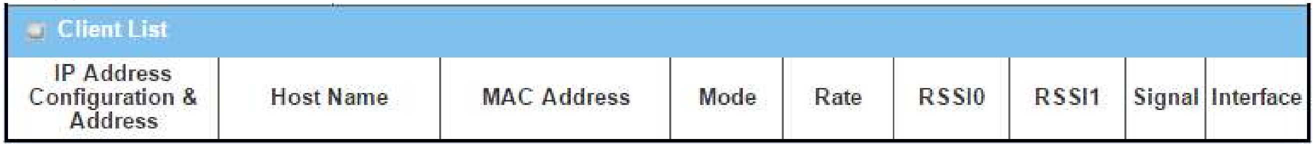
Target WiFi [Help]

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 WiFi module to check the information of connected clients. For those single WiFi module products, this option is hidden.
Operation Band	A Must filled setting.	Specify the intended operation band for the WiFi module. Basically, this setting is fixed and cannot be changed once the module is integrated into the gaye product. However, there are some module with selectable band for user to choose according to his network environment. Under such situation, you can specify which operation band is suitable for the application.
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. By default, All VAP is selected.

Show Client List

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



Client List

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

Target Configuration		
Item	**Value setting**	**Description**
IP Address Configuration & Address	N/A	It shows the Client's IP address and the deriving method. **Dynamic** means the IP address is derived from a DHCP server. **Static** means the IP address is a fixed one that is self-filled by client.

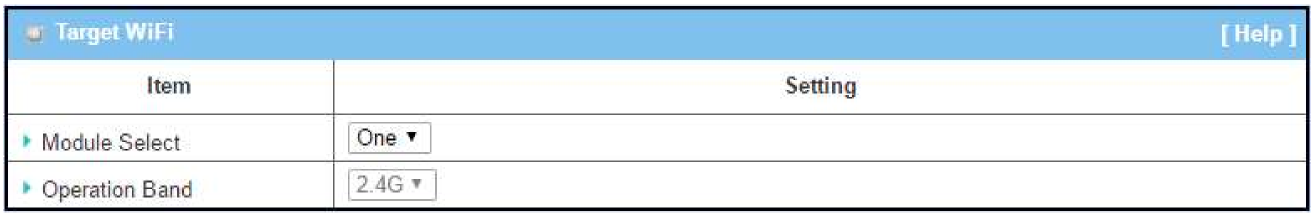
Host Name	N/A	It shows the host name of client.
MAC Address	N/A	It shows the MAC address of client.
Mode	N/A	It shows what kind of **Wi-Fi system** the client used to associate with this device.
Rate	N/A	It shows the **data rate** between client and this device.
RSSI0, RSSI1	N/A	It shows the RX sensitivity (RSSI) value for each radio path.
Signal	N/A	The **signal strength** between client and this device.
Interface	N/A	It shows the VAP ID that the client associated with.
Refresh	N/A	Click the **Refresh** button to update the Client List immediately.

3.5.7 Advanced Configuration

This device provides advanced wireless configuration for professional user to optimize the wireless performance under the specific installation environment. Please note that if you are not familiar with the WiFi technology, just leave the advanced configuration with its default values, or the connectivity and performance may get worse with improper settings.

Go to **Basic Network > WiFi > Advanced Configuration** Tab.

Select Target WiFi

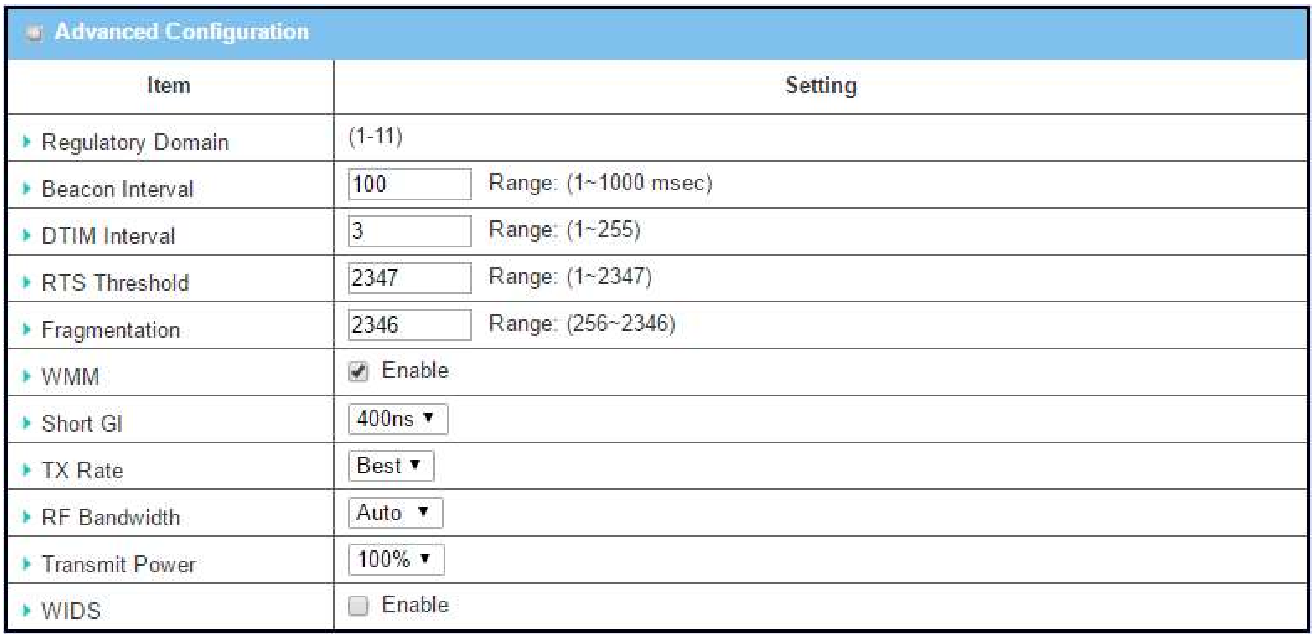


Target WiFi [Help]

Item	Setting
Module Select	One ▼
Operation Band	2.4G ▼

Target Configuration		
Item	**Value setting**	**Description**
Module Select	A Must filled setting.	Select the WiFi module to check the information of connected clients. For those single WiFi module products, this option is hidden.
Operation Band	A Must filled setting.	Specify the intended operation band for the WiFi module. Basically, this setting is fixed and cannot be changed once the module is integrated into the gaye product. However, there are some module with selectable band for user to choose according to his network environment. Under such situation, you can specify which operation band is suitable for the application.

Setup Advacned 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 the **Regulatory Domain**.
Beacon Interval	100	It shows the time interval between each beacon packet broadcasted. The beacon packet contains **SSID**, **Channel ID** and **Security setting**.
DTIM Interval	3	A **DTIM (Delivery Traffic Indication Message)** is a countdown informing clients of the next window for listening to broadcast message. When the device has buffered broadcast message for associated client, it sends the next DTIM with a DTIM value.
RTS Threshold	2347	**RTS (Request to send) Threshold** means when the packet size is over the setting value, then active **RTS** technique. RTS/CTS is a **collision avoidance** technique. It means RTS **never** activated when the threshold is set to **2347**.
Fragmentation	2346	Wireless frames can be divided into smaller units (fragments) to **improve performance** in the presence of RF interference at the limits of RF coverage.
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 lower **Short GI** could **increase** not only the **transition rate** but also **error rate**.
TX Rate	By default **Best** is selected	It means the **data transition rate**. When **Best** is selected, the device will choice a proper **data rat**e according to **signal strength**.
RF Bandwidth	By default **Auto** is selected	The setting of RF bandwidth limits the maximum data rate.
Transmit Power	By default **100%** is	Normally the wireless transmitter operates at 100% power. By setting

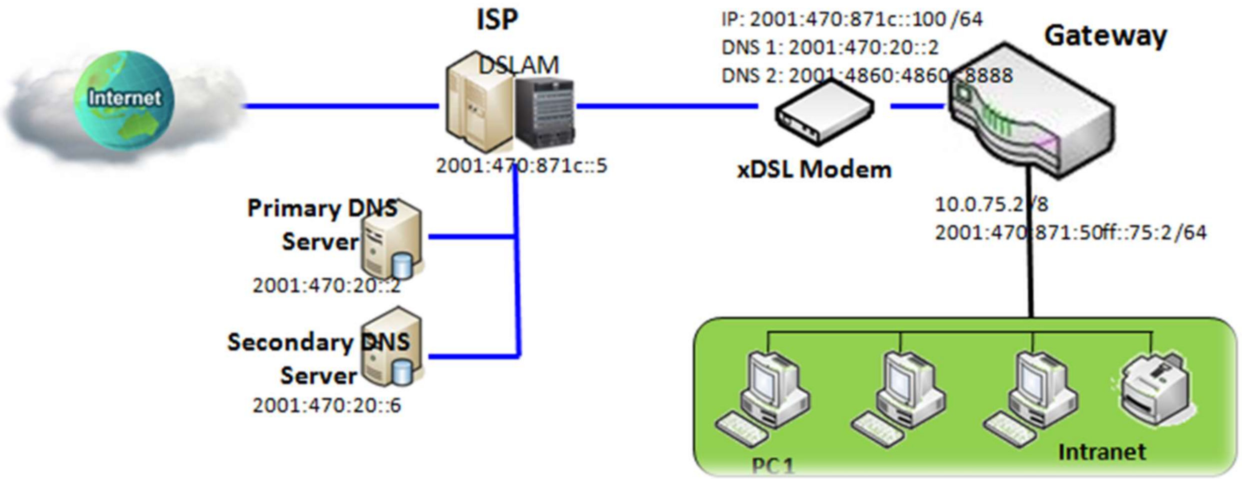
	selected	the **transmit power** to control the Wi-Fi **coverage**.
5G Band Steering	The box is unchecked by default	When the client station associate with 2.4G Wi-Fi, the device will send the client to 5G Wi-Fi automatically if the client is available on accessing this 5G Wi-Fi band. This option is only available on the module that supports 5GHz band.
WIDS	The box is unchecked by default	The WIDS (Wireless Intrusion Detection System) will analyze all the packet and make a statistic table in Wi-Fi status. Go to **Status** > **Basic Network** > **WiFi** tab for detailed WIDS status.
Save	N/A	Click the **Save** button to save the current configuration.
Undo	N/A	Click the **Undo** button to restore configuration to previous setting before saving.

3.7 IPv6

The growth of the Internet has created a need for more addresses than are possible with IPv4. **IPv6** (**Internet Protocol version 6**) is a version of the Internet Protocol (IP) intended to succeed IPv4, which is the protocol currently used to direct almost all Internet traffic. IPv6 also implements additional features not present in IPv4. It simplifies aspects of address assignment (stateless address auto-configuration), network renumbering and router announcements when changing Internet connectivity providers. This gateway supports various types of IPv6 connection (Static IPv6 / DHCPv6 / PPPoEv6 / 6to4 / 6in4). **Please contact your ISP the type of IPv6 is supported before you proceed with IPv6 setup.**

Static IPv6

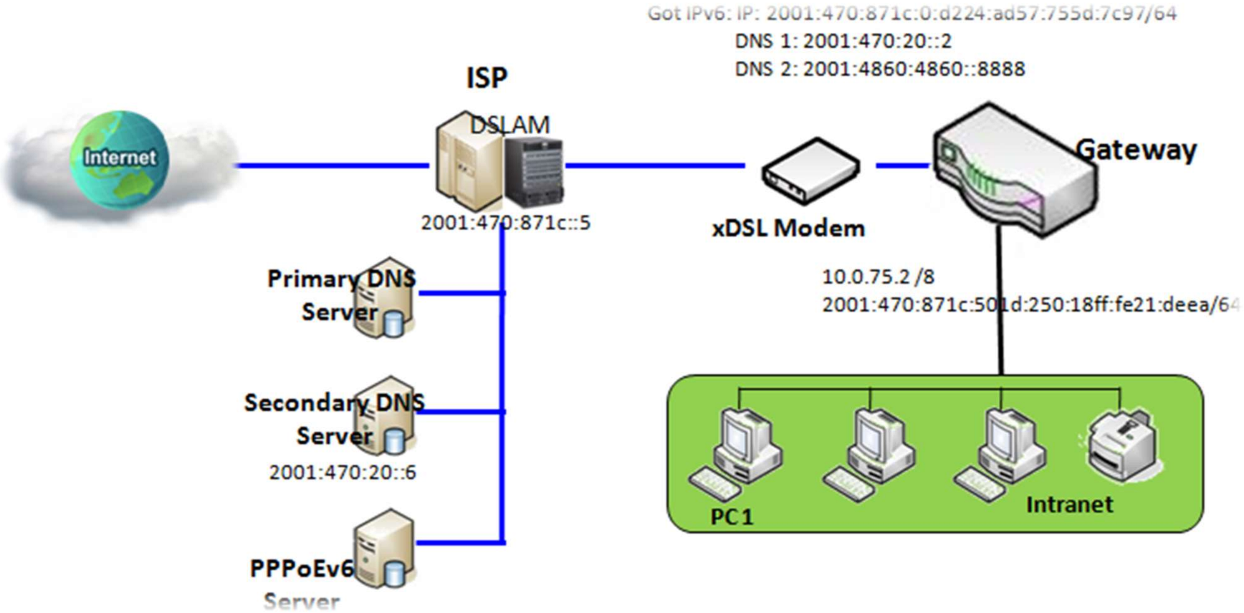
Static IPv6 does the same function as static IPv4. The static IPv6 provides manual setting of IPv6 address, IPv6 default gateway address, and IPv6 DNS.



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

DHCPv6

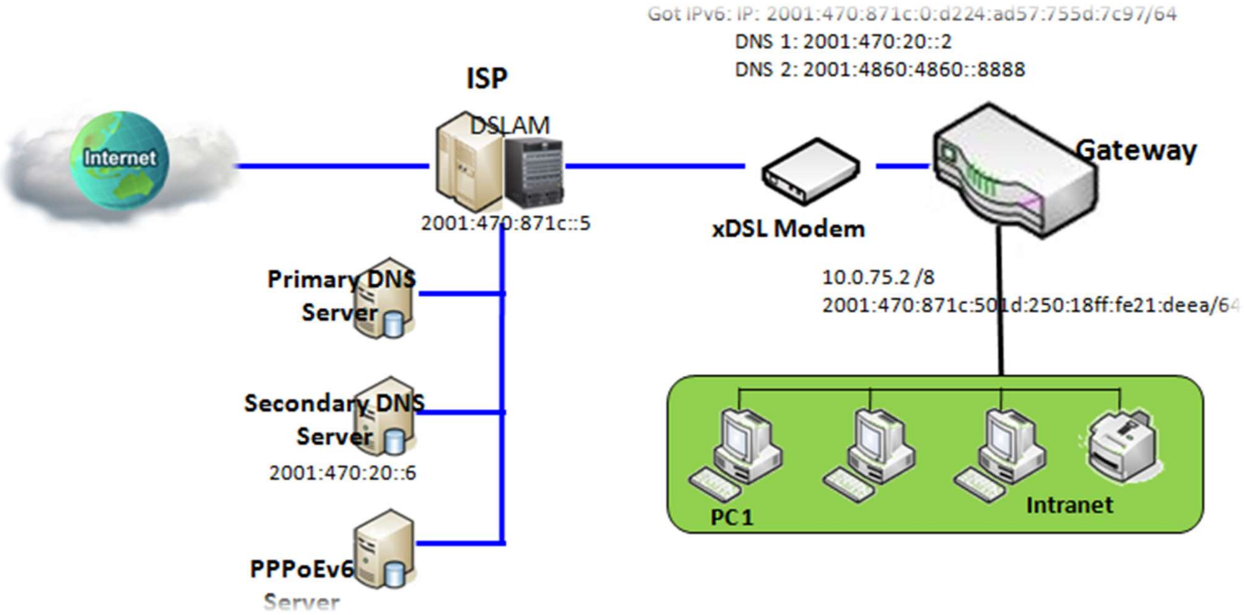
DHCP in IPv6 does the same function as DHCP in IPv4. The DHCP server sends IP address, DNS server addresses and other possible data to the DHCP client to configure automatically. The server also sends a lease time of the address and time to re-contact the server for IPv6 address renewal. The client has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



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

PPPoEv6

PPPoEv6 in IPv6 does the same function as PPPoE in IPv4. The PPPoEv6 server provides configuration parameters based on PPPoEv6 client request. When PPPoEv6 server gets client request and successfully authenticates it, the server sends IP address, DNS server addresses and other required parameters to automatically configure the client.

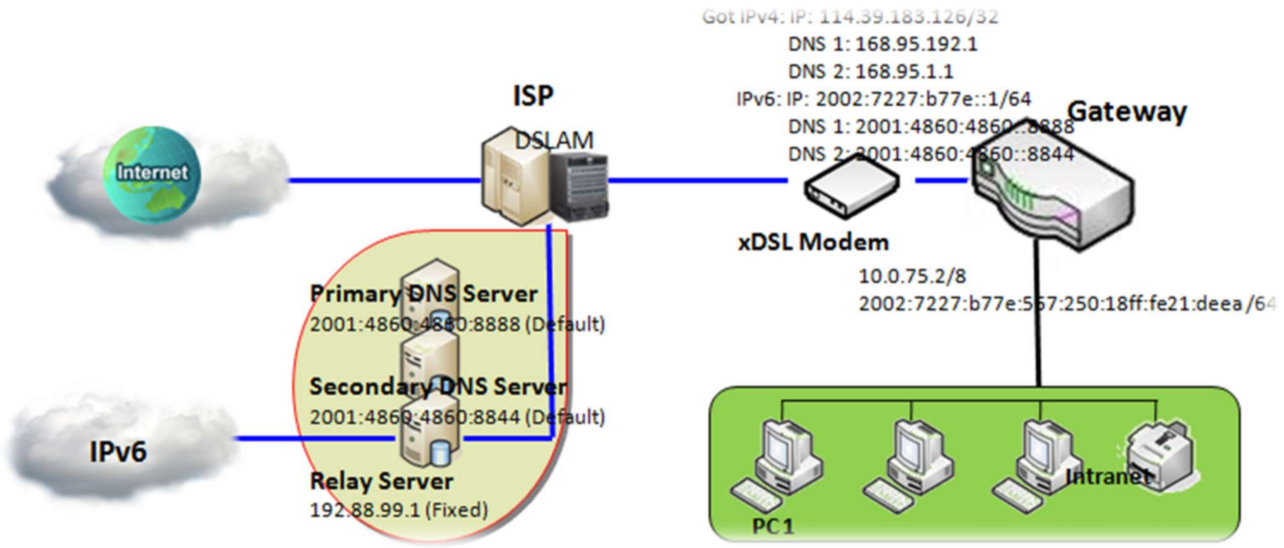


The diagram above depicts the IPv6 addressing through PPPoE, PPPoEv6 server (DSLAM) on the ISP side provides IPv6 configuration upon receiving PPPoEv6 client request. When PPPoEv6 server gets client request and successfully authenticates it, the server sends IP address, DNS server addresses and other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

6to4

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

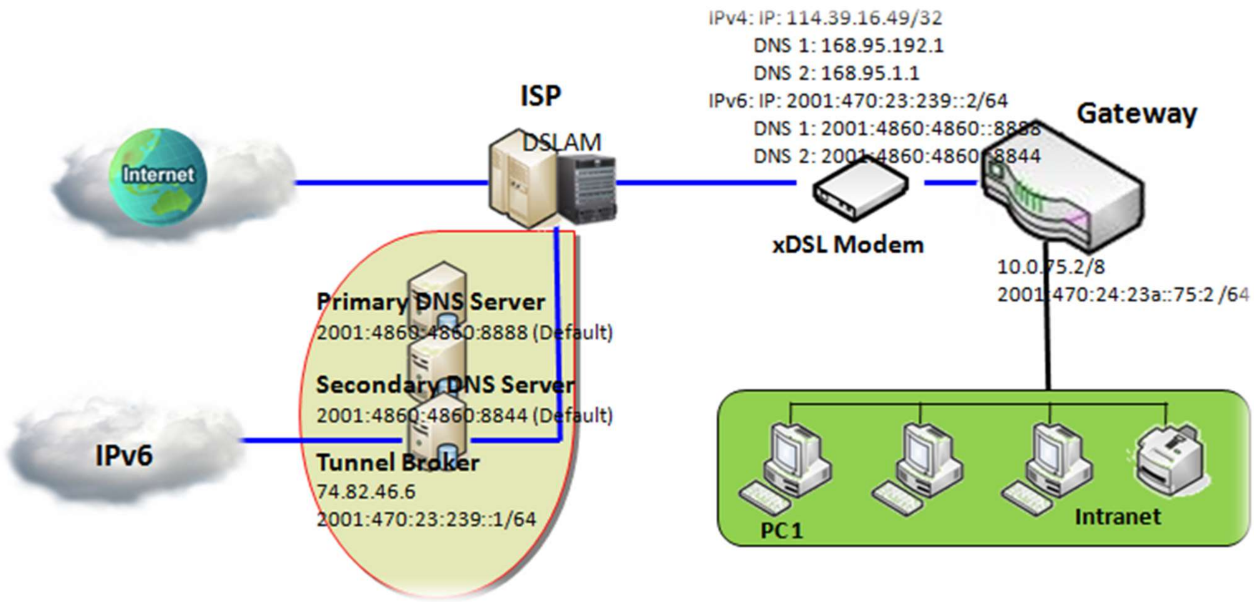
6to4 may be used by an individual host, or by a local IPv6 network. When used by a host, it must have a global IPv4 address connected, and the host is responsible for encapsulation of outgoing IPv6 packets and decapsulation of incoming 6to4 packets. If the host is configured to forward packets for other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


Got IPv4: IP: 114.39.183.126/32
DNS 1: 168.95.192.1
DNS 2: 168.95.1.1
IPv6: IP: 2002:7227:b77e::1/64
DNS 1: 2001:4860:4860::8888
DNS 2: 2001:4860:4860::8844
ISP
DSLAM
Gateway
Internet
xDSL Modem
10.0.75.2/8
2002:7227:b77e:567:250:18ff:fe21:deea/64
Primary DNS Server
2001:4860:4860:8888 (Default)
Secondary DNS Server
2001:4860:4860:8844 (Default)
IPv6
Relay Server
192.88.99.1 (Fixed)
Intranet
PC 1

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

6in4

6in4 is an Internet transition mechanism for Internet IPv4 to IPv6 migration. 6in4 uses tunneling to encapsulate IPv6 traffic over explicitly-configured IPv4 links. As defined in RFC 4213, the 6in4 traffic is sent over the IPv4 Internet inside IPv4 packets whose IP headers have the IP protocol number set to 41. This protocol number is specifically designated for IPv6 encapsulation.

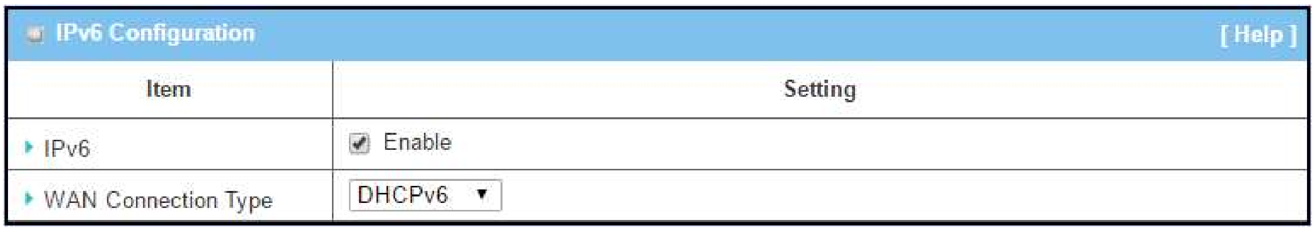

IPv4: IP: 114.39.16.49/32
DNS 1: 168.95.192.1
DNS 2: 168.95.1.1
IPv6: IP: 2001:470:23:239::2/64
DNS 1: 2001:4860:4860::8888
DNS 2: 2001:4860:4860::8844
ISP
DSLAM
Gateway
Internet
xDSL Modem
10.0.75.2/8
2001:470:24:23a::75:2 /64
Primary DNS Server
2001:4860:4860:8888 (Default)
Secondary DNS Server
2001:4860:4860:8844 (Default)
IPv6
Tunnel Broker
74.82.46.6
2001:470:23:239::1/64
PC 1
Intranet

In above diagram, the 6in4 usually needs to register to a 6in4 tunnel service, known as Tunnel Broker, in order to use. It also need end point global IPv4 address as 114.39.16.49 to complete 6in4 setting.

3.7.1 IPv6 Configuration

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

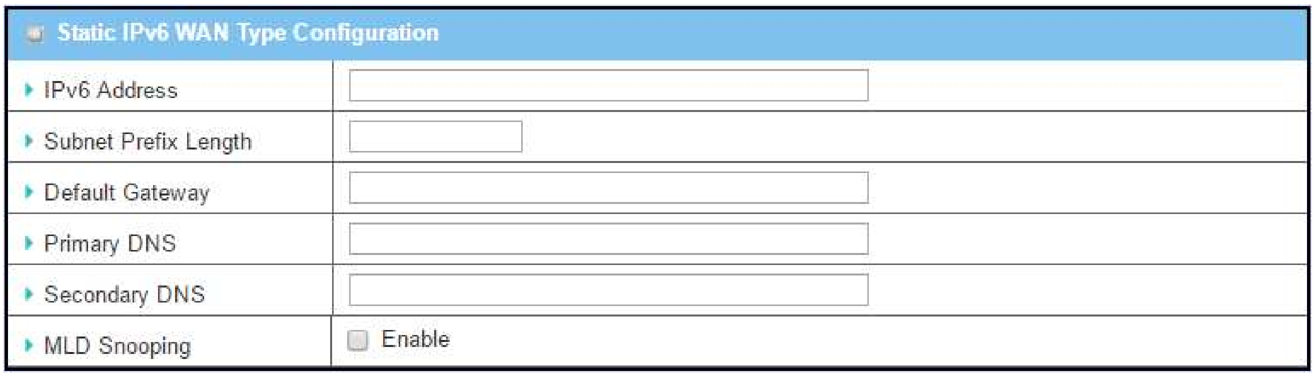
Go to **Basic Network > IPv6 > Configuration** Tab.



Item	Setting
IPv6	☑ Enable
WAN Connection Type	DHCPv6 ▼

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

Static IPv6 WAN Type Configuration

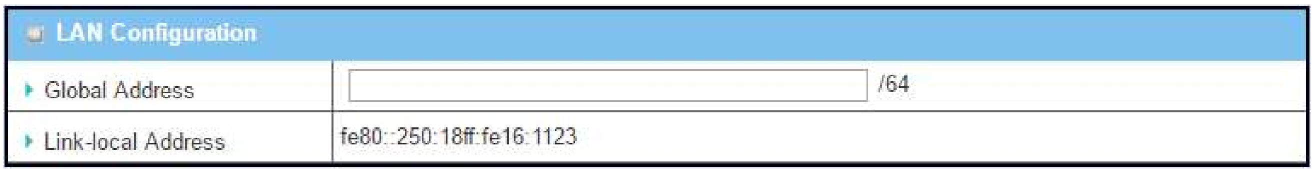


Static IPv6 WAN Type Configuration

IPv6 Address	
Subnet Prefix Length	
Default Gateway	
Primary DNS	
Secondary DNS	
MLD Snooping	□ Enable

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

LAN Configuration



LAN Configuration

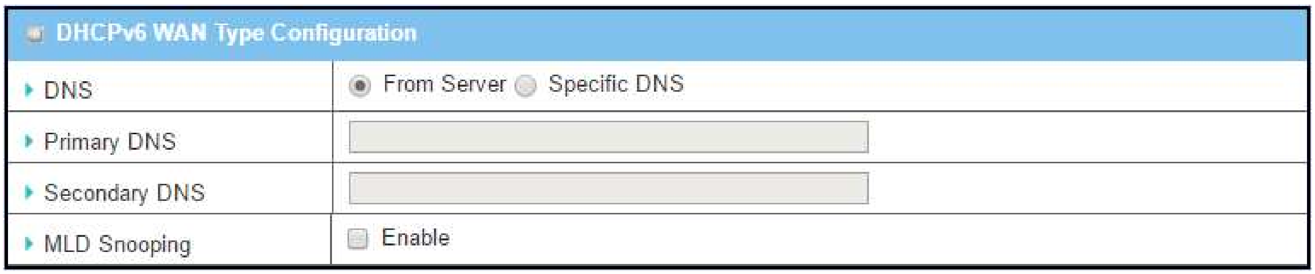
Global Address	/64
Link-local Address	fe80::250:18ff:fe16:1123

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

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

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

DHCPv6 WAN Type Configuration

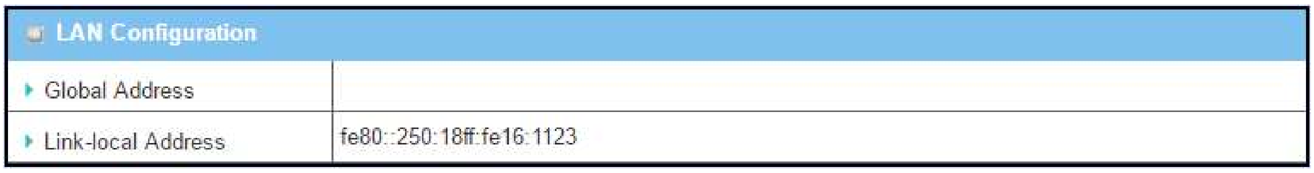


DHCPv6 WAN Type Configuration

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 the [Specific DNS] option to active Primary DNS and Secondary DNS. Then fill the DNS information.
Primary DNS	Can not modified by default	Enter the WAN **primary DNS Server**.
Secondary DNS	Can not modified by default	Enter the WAN **secondary DNS Server**.
MLD	The box is unchecked by default	Enable/Disable the MLD Snooping function

LAN Configuration



LAN Configuration

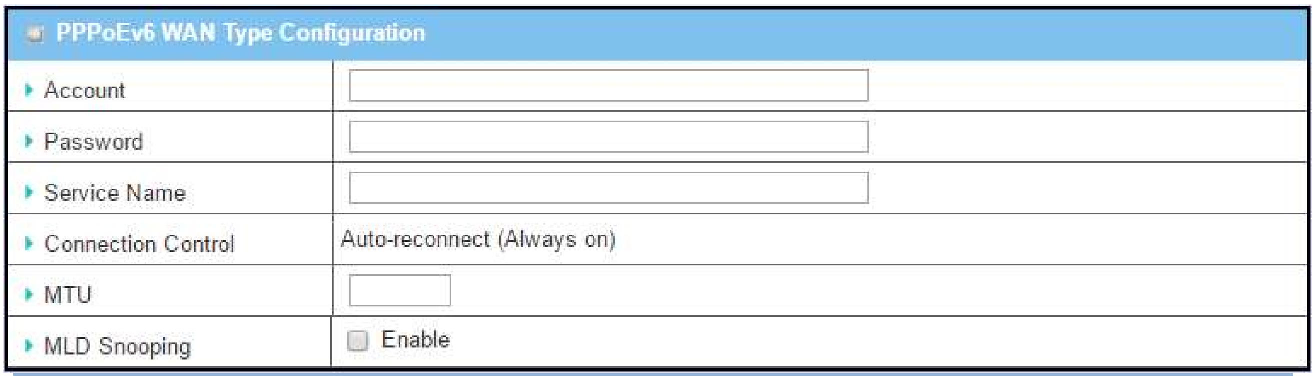
Global Address	
Link-local Address	fe80::250:18ff:fe16:1123

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

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

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

PPPoEv6 WAN Type Configuration

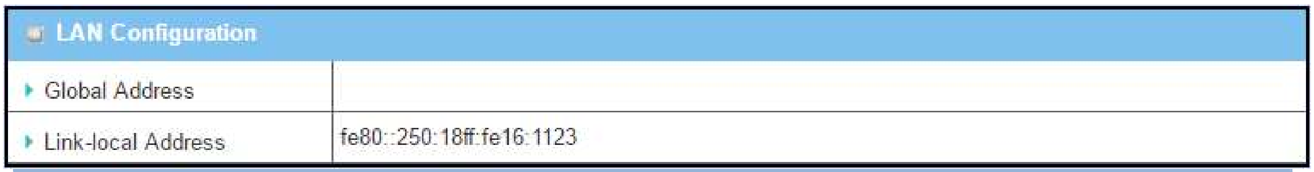


PPPoEv6 WAN Type Configuration

Account	
Password	
Service Name	
Connection Control	Auto-reconnect (Always on)
MTU	
MLD Snooping	□ Enable

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

LAN Configuration



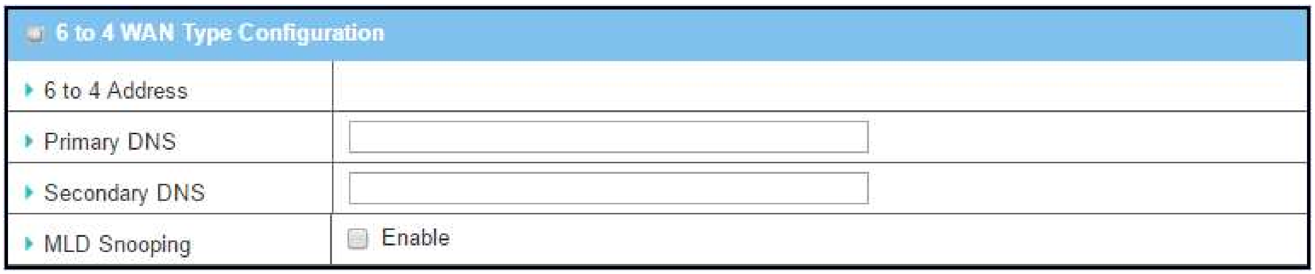
LAN Configuration

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

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

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

6to4 WAN Type Configuration

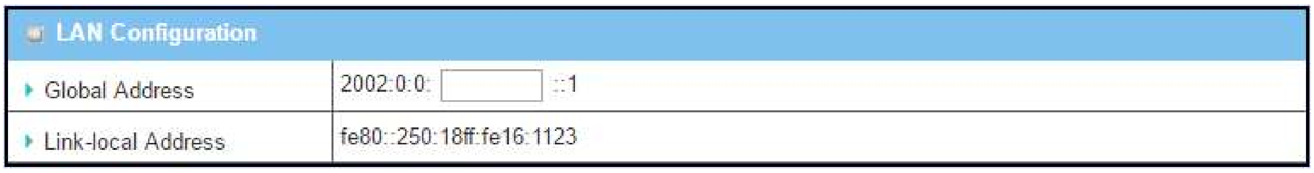


6 to 4 WAN Type Configuration

6 to 4 Address	
Primary DNS	
Secondary DNS	
MLD Snooping	□ Enable

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

LAN Configuration



LAN Configuration

Global Address	2002:0:0: ::1
Link-local Address	fe80::250:18ff:fe16:1123

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

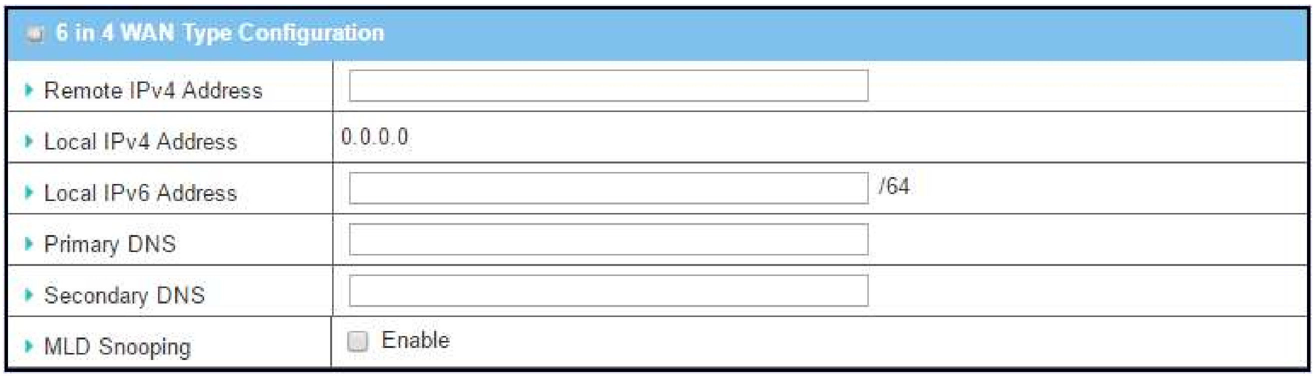
Then go to **Address Auto-configuration (summary)** for setting LAN environment.

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

6in4 WAN Type Configuration

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

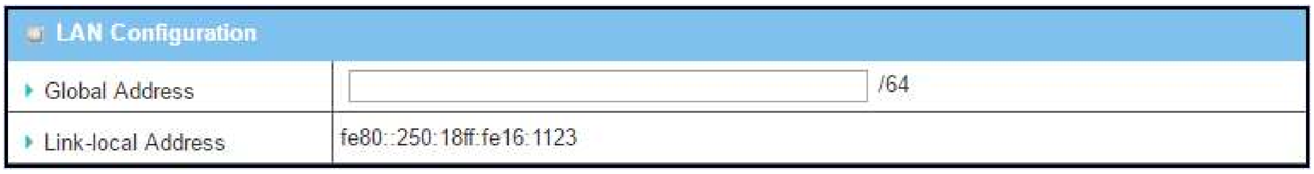
Then enter the **Local IPv4 address** of router into **Client IPv4 Address** field in IPv6 tunnel broker setting page.



6 in 4 WAN Type Configuration	
Remote IPv4 Address	
Local IPv4 Address	0.0.0.0
Local IPv6 Address	/64
Primary DNS	
Secondary DNS	
MLD Snooping	□ Enable

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

LAN Configuration



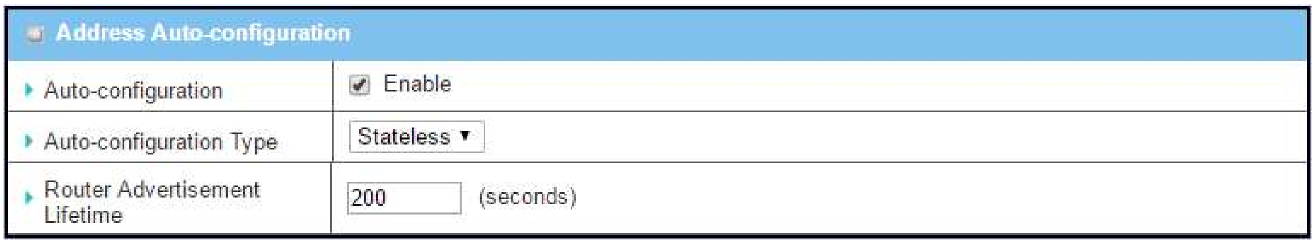
LAN Configuration	
Global Address	/64
Link-local Address	fe80::250:18ff:fe16:1123

LAN Configuration		
Item	**Value setting**	**Description**
Global Address	A Must filled setting	Filled **Routed /64** gotten from tunnel broker in this field.

Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

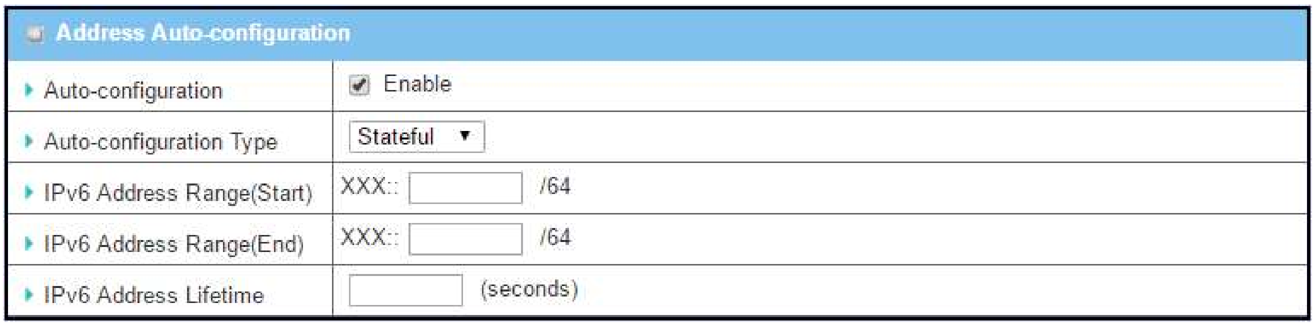
Then go to **Address Auto-configuration (summary)** for setting LAN environment.
If above setting is configured, click the **save button** to save the configuration and click **reboot button** to reboot the router.

Address Auto-configuration



Address Auto-configuration

Auto-configuration	☑ Enable
Auto-configuration Type	Stateless ▾
Router Advertisement Lifetime	200 (seconds)



Address Auto-configuration

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

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

	IPv6 Address Range (End) (A Must filled setting): Enter the end IPv6 Address for the DHCPv6 range for your local computers. 0200 is setted by default. **IPv6 Address Lifetime** (A Must filled setting) : Enter the DHCPv6 lifetime for your local computers. 36000 is setted by default.

3.9 Port Forwarding

Network address translation (NAT) is a methodology of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device. The technique was originally used for ease of rerouting traffic in IP networks without renumbering every host. It has become a popular and essential tool in conserving global address space allocations in face of IPv4 address exhaustion. The product you purchased embeds and activates the NAT function. You also can disable the NAT function in **[Basic Network]-[WAN & Uplink]-[Internet Setup]-[WAN Type Configuration]** page.

In addition to native NAT function, you can also configure further NAT related functions in the Port Forwarding page. They are NAT Loopback, Virtual Server, Virtual Computer, IP Translation, Special AP & ALG, DMZ and Pass Through, etc..

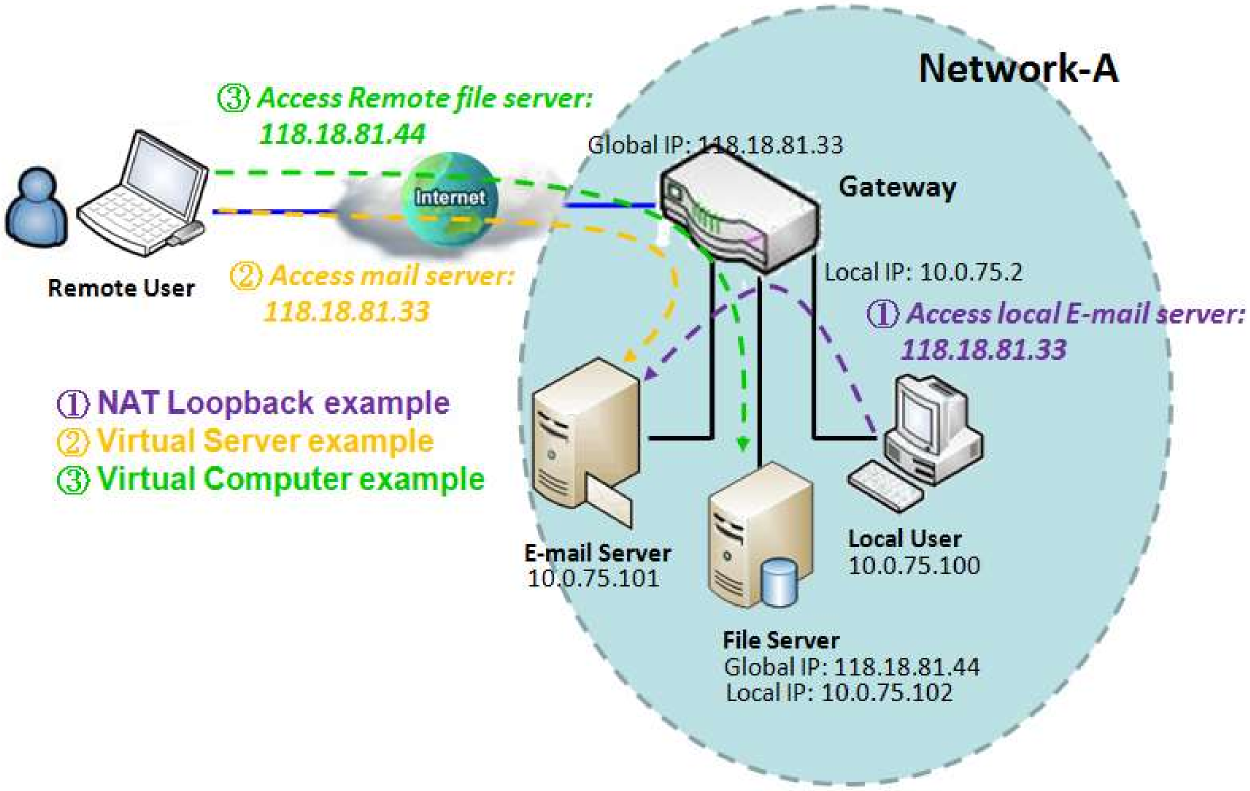
Normally, with global IP address or FQDN of WAN interface in the gateway, employees who travel outside the office can access various servers behind the office gateway. You can set up those servers by using "Virtual Server" feature of the gateway (refer to next section) to forward all server accessing requests to local LAN servers for traveling employees for remote access. But most often, employees are to reconfigure their PC to access to those servers from inside the LAN network each time after their trip. NAT Loopback can be enabled to overcome.

With "Virtual Server" feature, traveling employees may thus access office servers using the FQDN or IP address of WAN interface in the gateway, and the accessing request packets will be delivered to the WAN interface of gateway after NAT translation. Gateway forwards the inbound request packets to the local LAN servers and LAN servers make a reply to these request packets by connection tracking back. But if the NAT Loopback feature in the gateway is enabled, these packets will not flow to the WAN interface, but only loopback to the local LAN servers. And LAN servers make a reply.

3.9.1 Configuration

NAT Loopback

This feature allows you to access the WAN global IP address from your inside NAT local network. It is useful when you run a server inside your network. For example, if you set a mail server at LAN side, your local devices can access this mail server through gateway's global IP address when enable NAT loopback feature. On either side are you in accessing the email server, at the LAN side or at the WAN side, you don't need to change the IP address of the mail server, as shown in scenario ① of following diagram.



Scenario Application Timing

Without the need of reconfigure their PC each time, the employee from inside or outside the office can access enterprise servers. So network administrator must activate the "NAT Loopback" feature to do that.

Scenario Description

Local user can access mail server by FQDN or global IP when NAT loop back is enable.

Global user can access mail server only when mail server is set as virtual server of the gateway.

Parameter Setup Example

Following 2 tables list the parameter configuration as an example for above diagram of gateway with "NAT Loopback" feature activated.

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

Configuration Path	[Configuration]-[NAT Loopback]

NAT Loopback	■ ***Enable***

Configuration Path	[Virtual Server & Virtual Computer]-[Virtual Server List]	
ID	1	2
Public Port	***25 (SMTP)***	***110 (POP3)***
Server IP	***10.0.75.101***	***10.0.75.101***
Private Port	***25 (SMTP)***	***110 (POP3)***
Rule	■ ***Enable***	■ ***Enable***

Scenario Operation Procedure

In above diagram, the Gateway is the gateway of Network-A, and the subnet of its Intranet is 10.0.75.0/24. The gateway has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN interface. It serves as a NAT router.

Activate the NAT Loopback feature on the Gateway.

Define the E-mail virtual server to be located at a server with IP address 10.0.75.101 in the Intranet of Network-A, including SMTP service port 25 and POP3 service port 110.

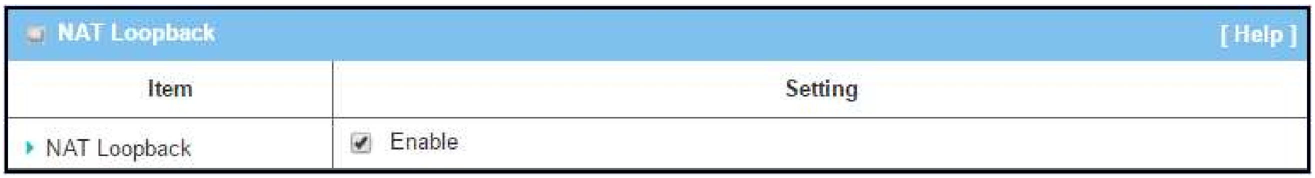
So, the local user at host with IP address 10.0.75.100 can access the E-mail server by using the global IP 118.18.81.33. But in reality the E-mail request packets from the local host will not reach the WAN interface, but just loop back to the E-mail server in the Intranet.

Configuration Setting

Go to Basic Network > Port Forwarding > Configuration tab.

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

Enable NAT Loopback



NAT Loopback [Help]

Item	Setting
NAT Loopback	☑ Enable

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

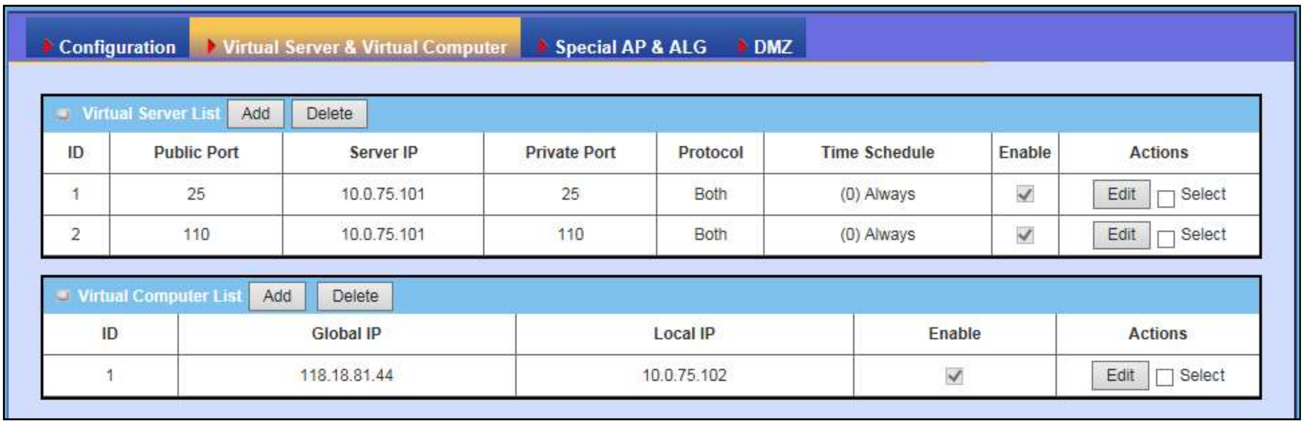
3.9.3 Virtual Server & Virtual Computer

Virtual server is another name for port forwarding used by some routers. In computer networking, port forwarding or port mapping is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall. This technique is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the gateway (external network), by remapping the destination IP address and port number of the communication to an internal host.

Port forwarding allows remote computers (a computers on the Internet) to connect to a specific computer or service within a private local-area network (LAN). So you can deploy some servers in your Intranet with the firewall protection by your gateway. This device’s NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this device gateway are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

However, a virtual computer is a host in the Intranet whose IP address is global and is visible to the outside world. Since it is in the Intranet, it is protected by the firewall gateway when it acts like a node in the Internet.

In "Virtual Server & Virtual Computer" page, there are two list windows for all virtual servers and virtual computer. "Virtual Server List" window lists the public port used in the Internet, server IP at LAN side, private port used in the Intranet, used protocol for the service on the server and the integrated time schedule rule for all virtual servers. There is an "Add" button for you to add and create new virtual server, and the "Edit" button to modify the existed virtual server settings. On "Virtual Computer List" window, the mapping of the global IP address and the local IP address for all virtual computers are listed. There is also an "Add" button for you to add and create new virtual computer, and the "Edit" button to modify the existed virtual computer.

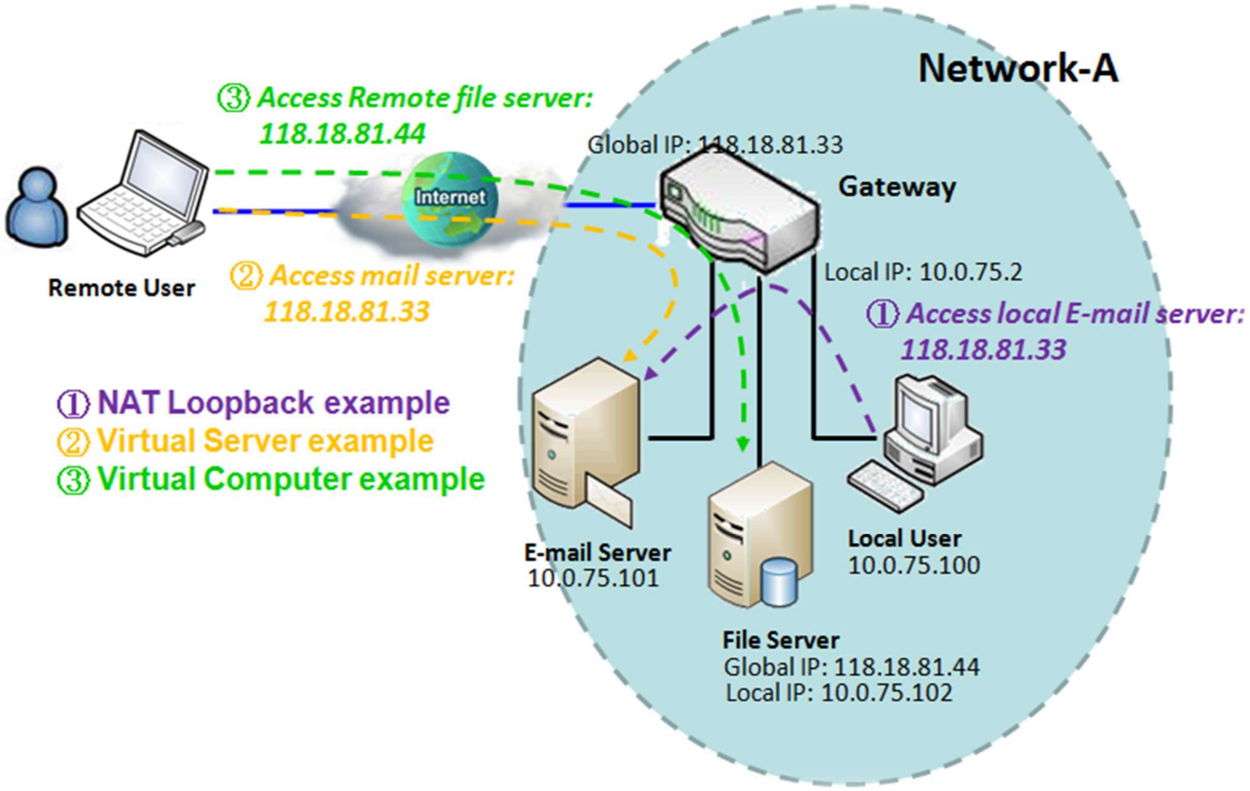


ID	Public Port	Server IP	Private Port	Protocol	Time Schedule	Enable	Actions
1	25	10.0.75.101	25	Both	(0) Always	✓	Edit □ Select
2	110	10.0.75.101	110	Both	(0) Always	✓	Edit □ Select

ID	Global IP	Local IP	Enable	Actions
1	118.18.81.44	10.0.75.102	✓	Edit □ Select

Virtual Server

"Virtual Server" feature allows you to define some servers with the global IP address or FQDN of the gateway as if they are servers existed in the Internet. But in fact, these servers are located in the Intranet and are physically behind the gateway. The gateway serves the service requests by port forwarding the requests to the LAN servers and transfers the replies from LAN servers to the requester on the WAN side. For example, if you set an E-mail server on the LAN side with IP address 10.0.75.101, a remote user can access the gateway for E-mail service if you defined a virtual E-mail server for the gateway by using the real E-mail server on the LAN side, as shown in scenario ② in following diagram**.**



Scenario Application Timing

Set up some application servers in the Intranet of deployed network for services and are protected by the gateway firewall. In a way that the gateway appears to be the physical server to the remote users, while the real server is, in reality, operating and providing service at the LAN side behind the gateway.

Scenario Description

The gateway serves as an E-mail server for remote users E-mail services from the gateway.

The gateway executes port forwarding transferring the E-mail service requests to the LAN servers and sends the replies from LAN servers to the requester.

The E-mail server at LAN side is the server for E-mail service.

Parameter Setup Example

Following table list the parameter configuration as an example for scenario ② in above diagram. Please be noted that the E-mail service includes SMTP and POP3 service ports.

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

Configuration Path	[Virtual Server & Virtual Computer]-[Virtual Server List]	
ID	***1***	***2***
Public Port	***25 (SMTP)***	***110 (POP3)***
Server IP	***10.0.75.101***	***10.0.75.101***
Private Port	***25 (SMTP)***	***110 (POP3)***
Rule	■ ***Enable***	■ ***Enable***

Scenario Operation Procedure

In above diagram, the Gateway is the gateway of Network-A and the subnet of its Intranet is 10.0.75.0/24. The gateway has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN interface. It serves as a NAT router.

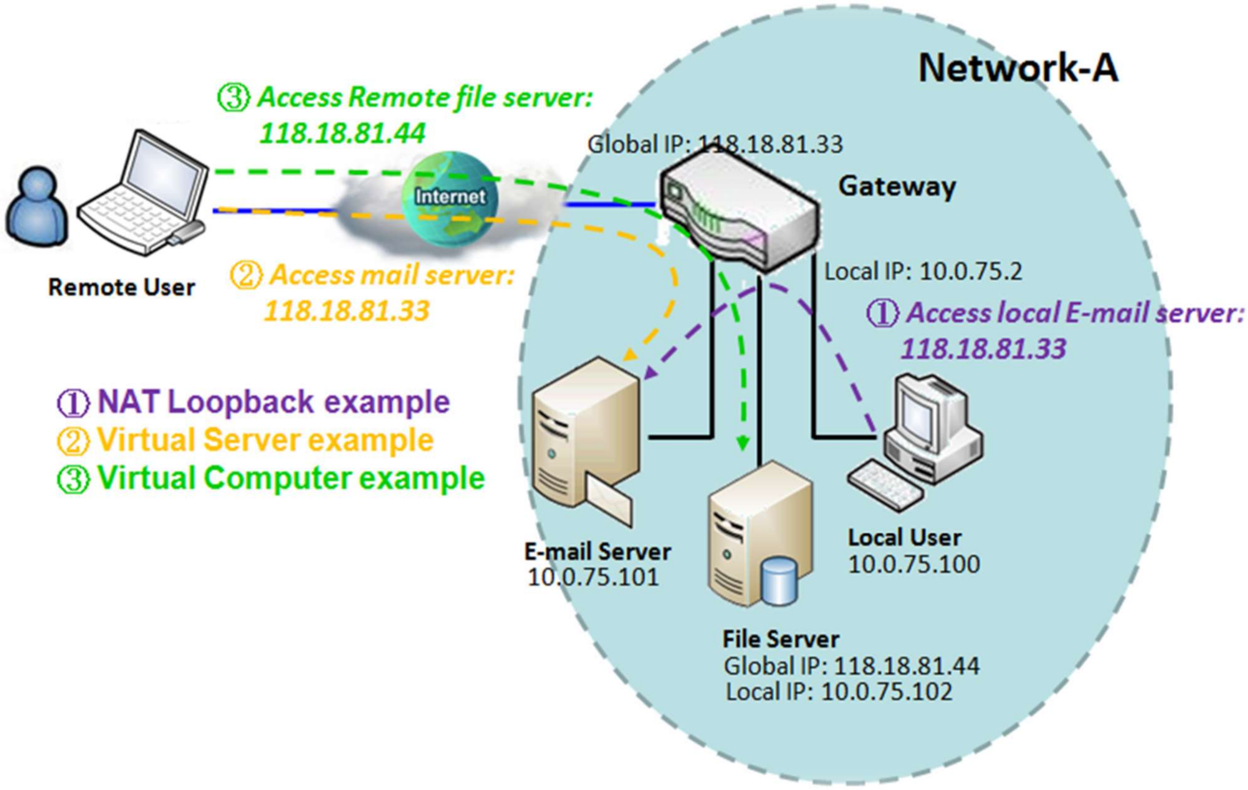
Define the E-mail virtual server to be located at a server with IP address 10.0.75.101 in the Intranet of Network-A, including SMTP service port 25 and POP3 service port 110.

So, the remote user can access the E-mail server in the gateway that has the global IP 118.18.81.33 at its WAN side. But the real E-mail server is located at LAN side and the gateway is the port forwarder for E-mail service.

A virtual server rule can be integrated with a schedule rule. That means, the virtual server rule can be activated only at the pre-defined time schedule.

Virtual Computer

"Virtual Computer" feature allows you to assign LAN hosts to global IP addresses, so that they can be visible to outside world. While so, they are also protected by the gateway firewall as same as they are protected when being client hosts in the Intranet. For example, if you set an FTP file server at LAN side with local IP address 10.0.75.102 and global IP address 118.18.82.44, a remote user can access the file server while it is hidden behind the NAT gateway. That is because the gateway takes care of all accessing to the IP address 118.18.82.44, including to forward the access requests to the file server and to send the replies from the server to outside world, as shown in scenario ③ of following diagram.



Scenario Application Timing

To setup some hosts in the Intranet of deployed networking to be visible to outside world but also be protected by the NAT gateway firewall, use the "Virtual Computer" feature in the gateway to implement the application scenario.

Scenario Description

A LAN host is assigned with a global IP address to be visible to outside world. The host has an embedded FTP file server and is protected by the gateway firewall.

The gateway acts as the media between the LAN host and outside world to allow remote access.

Parameter Setup Example

Following table list the parameter configuration as an example for scenario ③ in above diagram.

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

Configuration Path	[Virtual Server & Virtual Computer]-[Virtual Computer List]
ID	***1***
Global IP	***118.18.81.44***
Local IP	***10.0.75.102***
Rule	■ ***Enable***

Scenario Operation Procedure

In above diagram, the Gateway is the gateway of Network-A and the subnet of its Intranet is 10.0.75.0/24. The gateway has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN interface. It serves as a NAT router.

A LAN host with private IP address 10.0.75.102 has an embedded FTP file server in it. The host is expected to be visible to the outside world with global IP address 118.18.81.44, but also be protected by the gateway firewall.

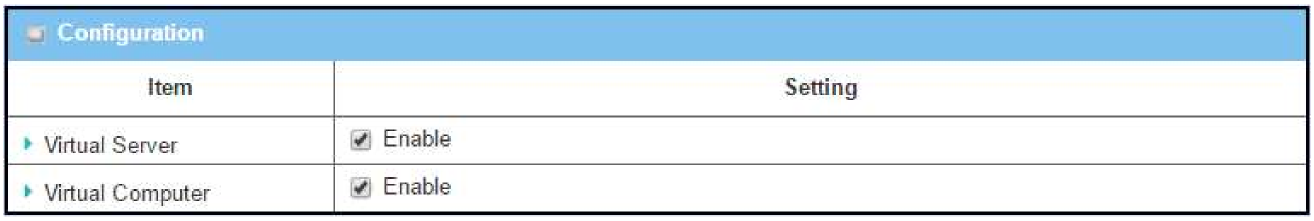
Configure a virtual computer in the gateway for the mapping between the global IP address 118.18.81.44 and the local IP address 10.0.75.102. The gateway will take care of all accessing to the FTP file server by server's global IP address, and it acts as a media between the LAN host and the outside world by using its "Virtual Computer" feature.

So remote users can request for file services from the FTP file server, even it is existed in a LAN host.

Virtual Server & Virtual Computer Setting

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

Enable Virtual Server and Virtual Computer

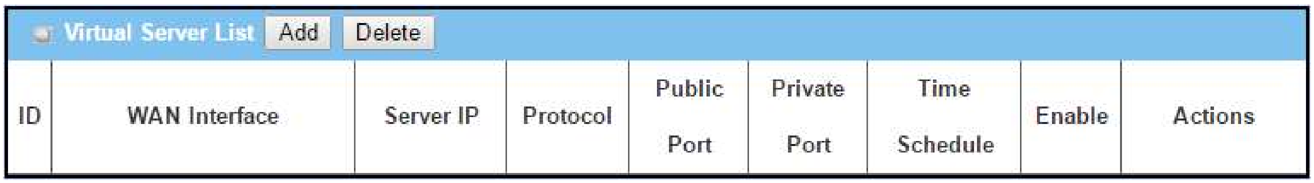


Configuration	
Item	Setting
Virtual Server	☑ Enable
Virtual Computer	☑ Enable

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

Create/Edit Virtual Server

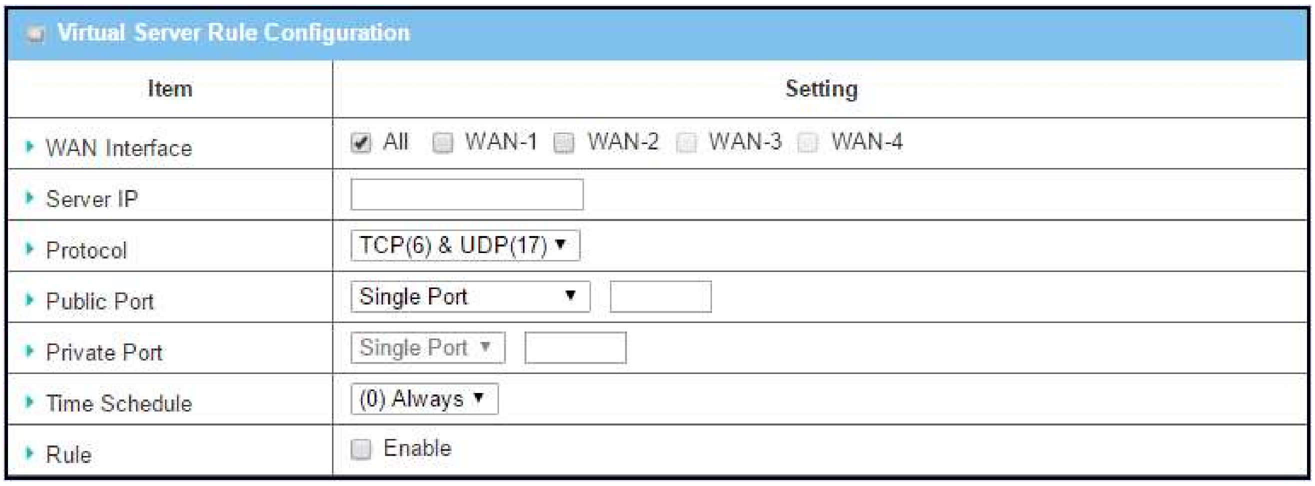
The router allows you to custom your Virtual Server rules. The router supports up to a maximum of 20 rule-based Virtual Server sets.



Virtual Server List Add Delete

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

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



Virtual Server Rule Configuration	
Item	Setting
WAN Interface	☑ All □ WAN-1 □ WAN-2 □ WAN-3 □ WAN-4
Server IP	
Protocol	TCP(6) & UDP(17) ▾
Public Port	Single Port ▾
Private Port	Single Port ▾
Time Schedule	(0) Always ▾
Rule	□ Enable

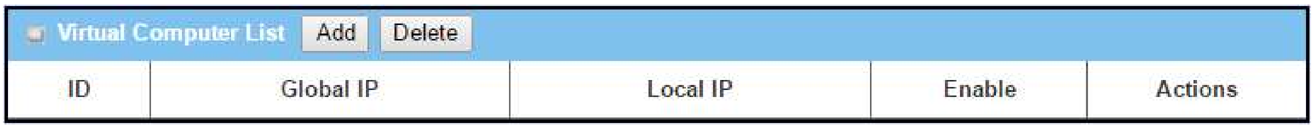
Virtual Server Rule Configuration Item	Value setting	Description
WAN Interface	1. A Must filled setting 2. Default is **ALL**.	Define the selected interface to be the packet-entering interface of the router. If the packets to be filtered are coming from **WAN-x** then select **WAN-x** for this field.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

		Public Port is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number. **Public Port** is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **Object Definition)** Then check **Enable** box to enable this rule. When **"TCP & UDP"** is selected It means the option "Protocol" of packet filter rule is TCP and UDP. **Public Port** selected a predefined port from **Well-known Service**, and **Private Port** is the same with **Public Port** number. **Public Port** is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number. **Public Port** is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **Object Definition)** Then check **Enable** box to enable this rule. When **"GRE"** is selected It means the option "Protocol" of packet filter rule is GRE. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **Object Definition)** Then check **Enable** box to enable this rule.
		When **"ESP"** is selected It means the option "Protocol" of packet filter rule is ESP. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **Object Definition)** Then check **Enable** box to enable this rule. Click the **Save** button to save the settings. When **"SCTP"** is selected It means the option "Protocol" of packet filter rule is SCTP. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **Object Definition)** Then check **Enable** box to enable this rule. When **"User-defined"** is selected It means the option "Protocol" of packet filter rule is User-defined. For **Protocol Number**, enter a port number. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **Object Definition)** Then check **Enable** box to enable this rule.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click **Undo** to cancel the settings.

Back	N/A	When the **Back** button is clicked the screen will return to the Packet Filters Configuration page.

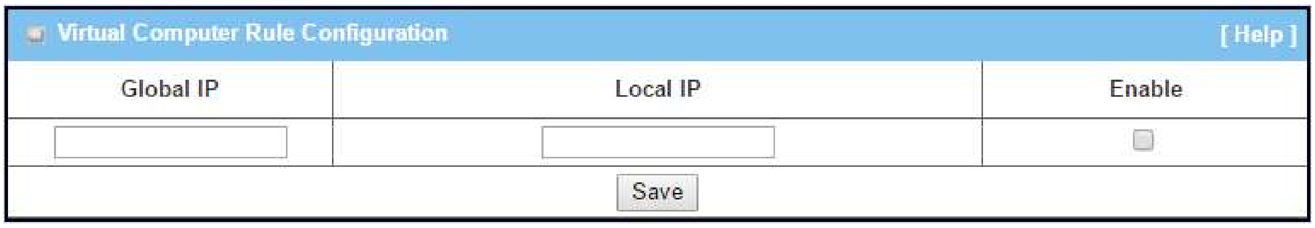
Create/Edit Virtual Computer

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



ID	Global IP	Local IP	Enable	Actions

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



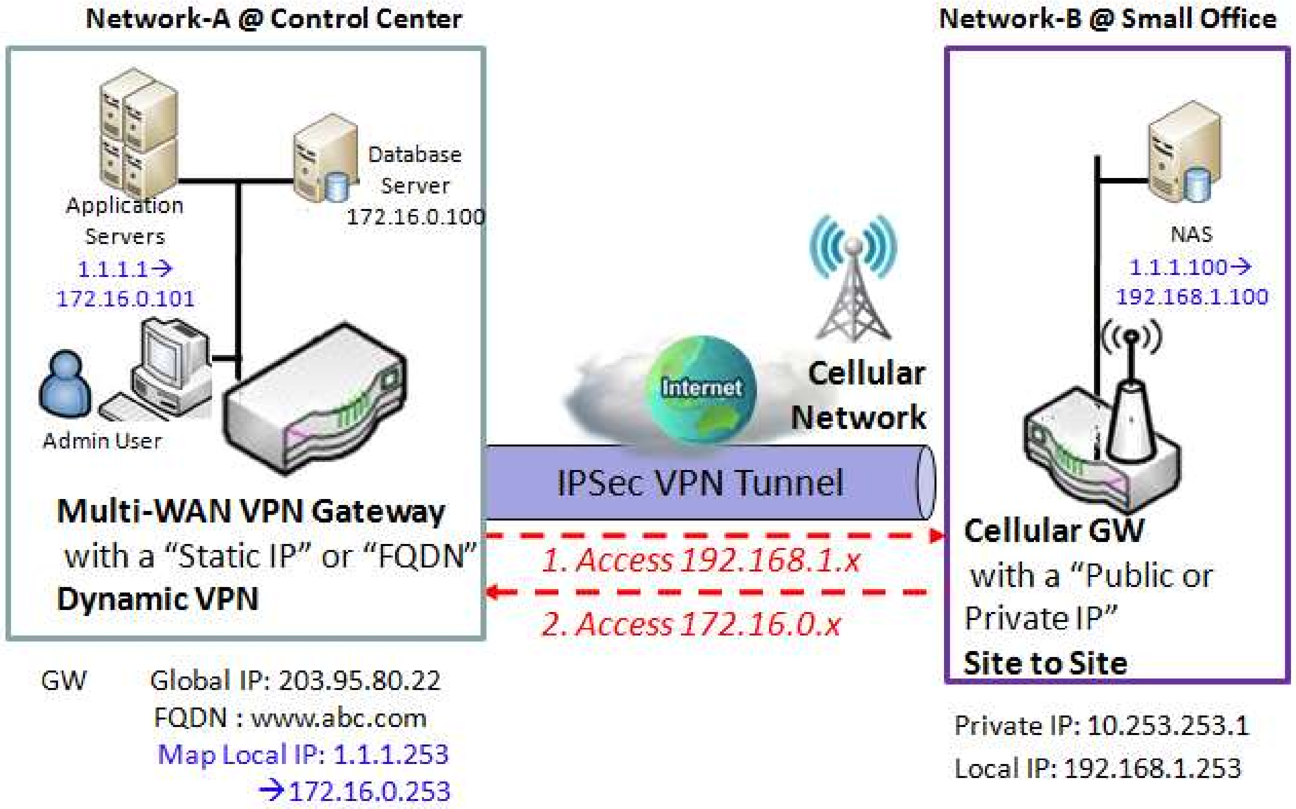
Global IP	Local IP	Enable
		□

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

3.9.5 IP Translation

IP Translation is slimier to One-to-One NAT. it is a feature where you can configure the gateway with multiple IP addresses issued by your Internet Service Provider (ISP) and map them to individual intranet devices with specific IP addresses. That is, configuring the IP Translation feature creates a one-to-one mapping between a public IP address and a private IP address of a local host. In addition, admin users also map a private IP address range to a public IP address range of equal instances.

This feature offers another way to make systems behind a firewall and configured with private IP addresses appear to have public IP addresses.



1. Admin user can access Application server via IP Address 1.1.1.1 instead of 172.16.0.101
2. Admin user also can access NAS which mapped IP Address 1.1.1.100 instead of 192.168.1.100 via Remote VPN Tunnel

Scenario Application Timing

Sometimes, the admin users want to manage IP Address of servers easily or easy to memorize in the Intranet, IP Translation can help local servers to map valid public IP Address in closed or Intranet Network.

Scenario Description

Admin user setups IP Address 1.1.1.1 to substitute for 172.16.0.101 of application server on intranet network.

Admin user setups IP Address 1.1.1.100 to substitute for 192.168.1.100 of NAS Device in remote intranet network..

Users in Control Center can access application server via 1.1.1.1 or NAS device via 1.1.1.100.

Parameter Setup Example

Following table lists the parameter configuration as an example for the gateway in above diagram.

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

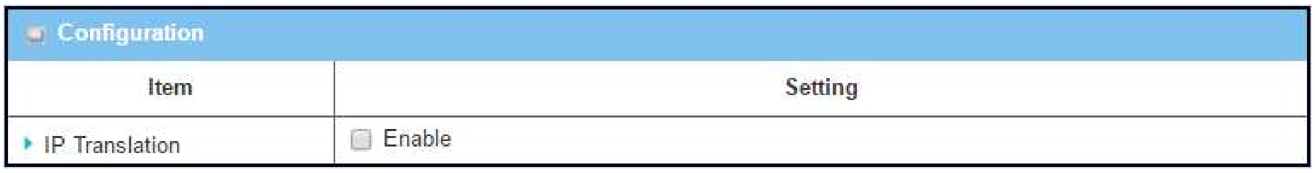
Configuration Path	[Configuration]-[IP Translation]
IP Translation	Enable ■

Configuration Path	[IP Translation]-[IP Translation List]	
ID	1	2
Mapping IP address	1.1.1.1 →172.16.0.101	1.1.1.100 → 192.168.1.100
Description	Application Server	Remote NAS
Rule	■ Enable	■ Enable

IP Translation Setting

Go to **Basic Network > Port Forwarding > IP Translation** tab.

Enable IP Translation



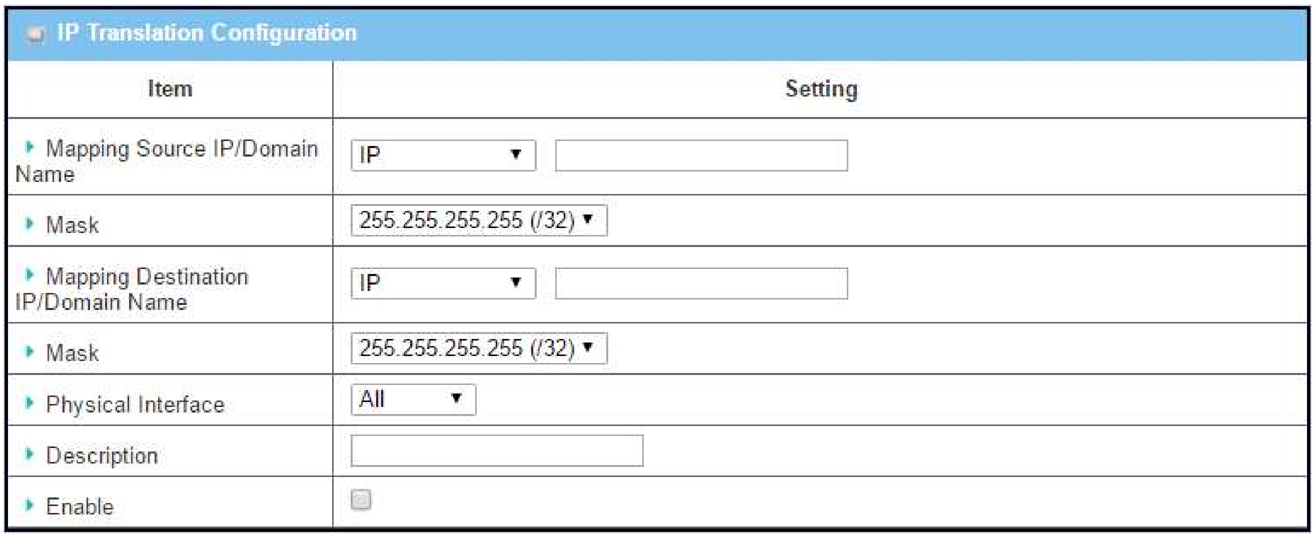
Configuration

Item	Setting
IP Translation	□ Enable

Configuration Item	Value setting	Description
IP Translation	The box is unchecked by default	Check the **Enable** box to activate the IP translation function
Save	N/A	Click the **Save** button to save the settings.

Create/Edit IP Translation Rule

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



IP Translation Configuration

Item	Setting
Mapping Source IP/Domain Name	IP ▾
Mask	255.255.255.255 (/32) ▾
Mapping Destination IP/Domain Name	IP ▾
Mask	255.255.255.255 (/32) ▾
Physical Interface	All ▾
Description	
Enable	□

IP Translation Configuration Item	Value setting	Description
Mapping Source IP/Domain Name	1. A Must filled setting 2.**IP** is selected by default.	Specify the original **IP** / **Domain Name** to be translated.
Mask	1. A Must filled setting 2.**255.255.255.255(/32)** is selected by default.	Enter the required subnet mask if **Source IP** is specified above. It can be a single IP with 255.255.255.255 (/32) subnet mask, or an IP group limited with proper subnet setting.

Mapping Destination IP/Domain Name	1. A Must filled setting 2.**IP** is selected by default.	Specify the expected target **IP** / **Domain Name** that will be used to replace the original one.
Mask	1. A Must filled setting 2.**255.255.255.255(/32)** is selected by default.	Enter the required subnet mask if **Destination IP** is specified above. It can be a single IP with 255.255.255.255 (/32) subnet mask, or an IP group limited with proper subnet setting.
Physical Interface	1. A Must filled setting 2.**All** is selected by default.	Specify the interface to apply the translation rule. The enabled WAN Interface will be available in the dropdown list. By default, **All** is selected, and the translation rule will be applied to the traffics passing through all WAN interfaces.
Description	An optional setting.	Specify a brief description or rule name for this IP Translation rule.
Enable	The box is unchecked by default	Check the **Enable** box to activate the translation rule.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the settings

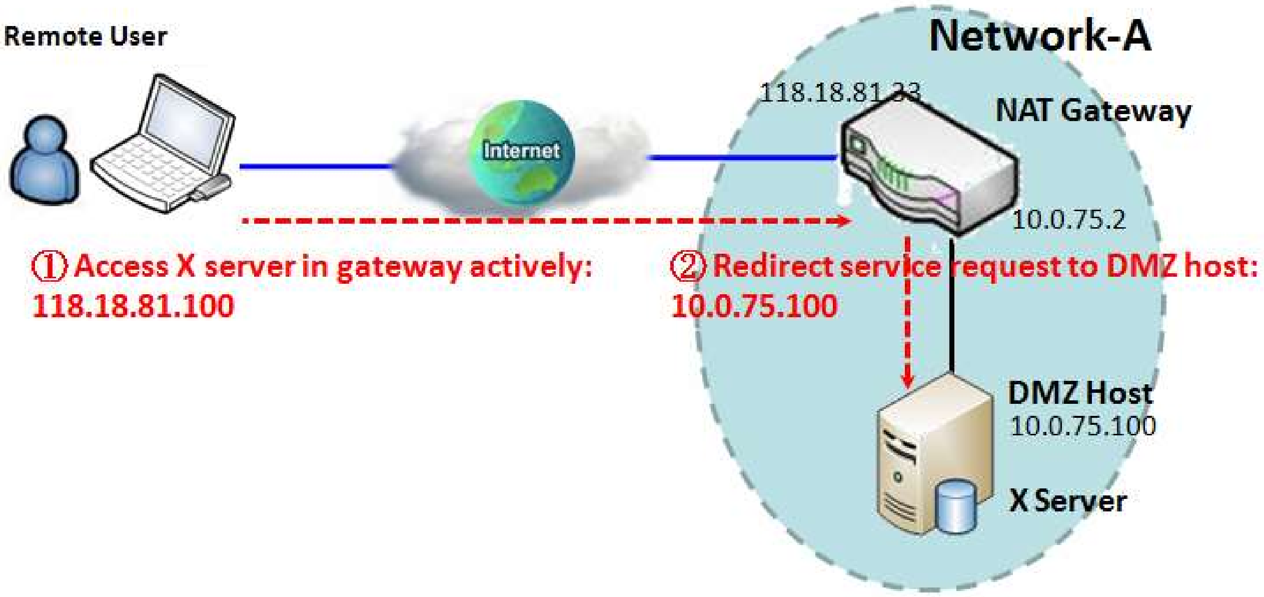
3.9.9 DMZ & Pass Through

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

In "DMZ" page, there is only one configuration window for "DMZ" feature. The window lets you activate the DMZ function and specify the IP address in the Intranet to be DMZ host so that the host under DMZ function can run applications freely that would, otherwise, blocked by NAT mechanism of the gateway with DMZ feature disabled. That is, the incoming packets issued by an active application in the Internet are usually blocked outside of the NAT gateway. But the DMZ host can receive those packets and make replies. That is, it is reactive to outside world. In the meantime, it is also protected by the gateway firewall.

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

DMZ Scenario



Scenario Application Timing

When the administrator of the gateway wants to set up some service daemons in a host that is in the Intranet to allow remote users request for services from the host actively, even the host is behind a NAT gateway. But remote users think the gateway provides those services, so users use the global IP of the gateway to request their services. Apply the DMZ feature in the NAT gateway to meet the application scenario. In addition, please also be noted that the client host is still protected by the gateway firewall.

Scenario Description

The DMZ host is behind a NAT gateway and receives all normal and active packets from the Internet.

Remote user can access the DMZ host by using the IP address of the gateway, and the gateway will skip the NAT checking on the DMZ host.

DMZ host is still protected by the gateway firewall.

Parameter Setup Example

Following table lists the parameter configuration as an example for the gateway in above diagram with DMZ enabling.

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

Configuration Path	[DMZ]-[Configuration]
DMZ	IP Address of DMZ Host: ***10.0.75.100*** ■ ***Enable***

Scenario Operation Procedure

In above diagram, the NAT Gateway is the gateway of Network-A and the subnet of its Intranet is 10.0.75.0/24. The gateway has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN interface. It serves as a NAT router.

Configure a host in the Intranet to be the DMZ Host and activate the rule, whose IP address is 10.0.75.100.

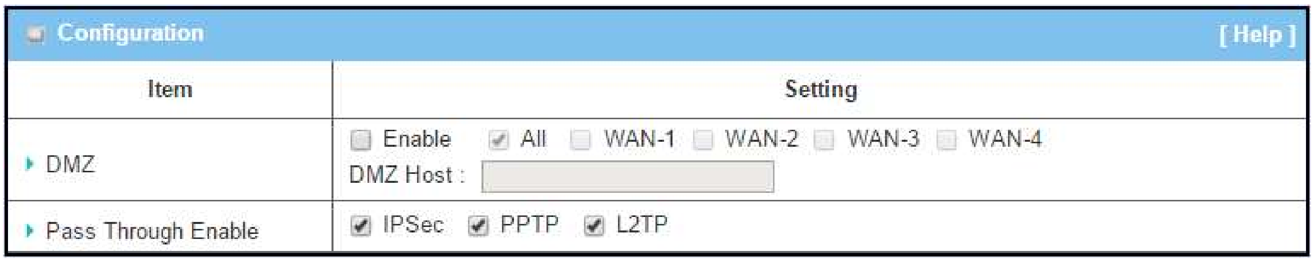
Assume there is an X server installed in the DMZ host. Then, the remote user can request services from the X server in the DMZ host by skipping the NAT checking by the gateway.

DMZ & Pass Through Setting

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

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

Enable DMZ and Pass Through



Configuration [Help]

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**.	Check the **Enable** box to activate this SDMZ function Define the selected interface to be the packet-entering interface of the router. If the packets to be filtered are coming from **WAN-x** then select **WAN-x** for this field. Select **ALL** for packets coming into the router from any interfaces. It can be selected **WAN-x** box when **WAN-x** enabled. This field of **DMZ Host** is to specify the IP address of Host LAN IP.
Pass Through Enable	The boxes are checked by default	Check the box to enable the pass through function for the IPSec, PPTP, and L2TP. With the pass through function enabled, the VPN hosts behind the gateway still can connect to remote VPN servers.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click **Undo** to cancel the settings

3.b Routing

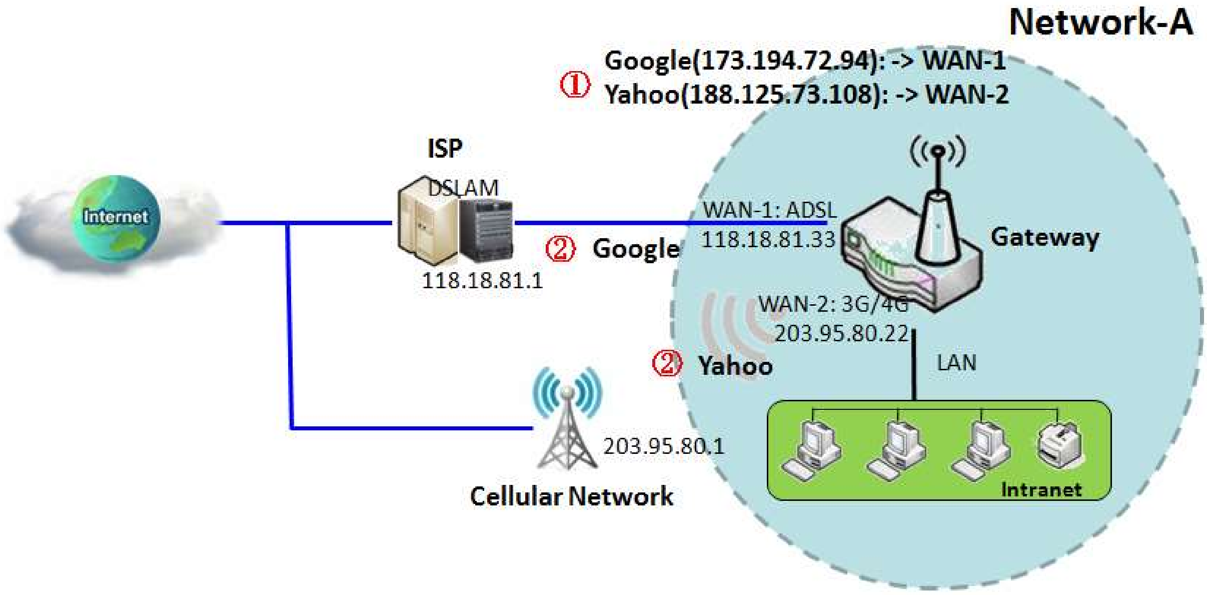
If you have more than one router and subnet, you will need to enable routing function to allow packets to find proper routing path and allow different subnets to communicate with each other. Routing is the process of selecting best paths in a network. It is performed for many kinds of networks, like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

The routing tables record your pre-defined routing paths for some specific destination subnets. It is static routing. However, if the contents of routing tables record the obtained routing paths from neighbor routers by using some protocols, such as RIP, OSPF and BGP. It is dynamic routing. These both routing approaches will be illustrated one after one.

3.b.1 Static Routing

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

Static Routing Scenario



Scenario Application Timing

When the administrator of the gateway wants to specify what kinds of packets to be transferred via which one gateway interface and which peer gateway to their destination. It can be carried out by the "Static Routing" feature.

Scenario Description

Dedicated packet flows from the Intranet will be routed to their destination via the pre-defined peer gateway and corresponding gateway interface that are defined in the system routing table by manual.

Parameter Setup Example

Following tables list the parameter configuration as an example for the gateway in above diagram with "Static Routing" enabling.

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

Configuration Path	[Static Routing]-[Configuration]
Static Routing	■ ***Enable***

Configuration Path	[Static Routing]-[Static Routing Rule List]	
ID	1	2
Destination IP	***173.194.72.94***	***188.125.73.108***
Subnet Mask	***255.255.255.255***	***255.255.255.255***
Gateway	***118.18.81.1***	***203.95.80.1***
Metric	***255***	***255***
Rule	■ ***Enable***	■ ***Enable***

Scenario Operation Procedure

In above diagram, the Gateway is the gateway of Network-A and the subnet of its Intranet is 10.0.75.0/24. The gateway has the IP address of 10.0.75.2 for LAN interface, 118.18.81.33 for WAN-1 interface and 203.95.80.22 for WAN-2 interface. It serves as a NAT router.

Configure two static routing rules for the gateway. The first one is to define the packets from the Intranet to the Google web site (173.194.72.94) will be routed via the WAN-1 interface and the ADSL ISP's gateway. The second one is to define the packets to the Yahoo web site (188.125.73.108) will be routed via the WAN-2 interface and the Cellular Network ISP's gateway.

System will route the packets from the Intranet to Google site and Yahoo site based on above settings.

Static Routing Setting

In "Static Routing" page, there are three configuration windows for static routing feature. They are the "Configuration" window, "Static Routing Rule List" window and "Static Routing Rule Configuration" window.

The "Configuration" window lets you activate the global static routing feature only. Even you have defined many static routing rules for the gateway, if you want to disable them temporarily, just uncheck the Enable box to disable it.

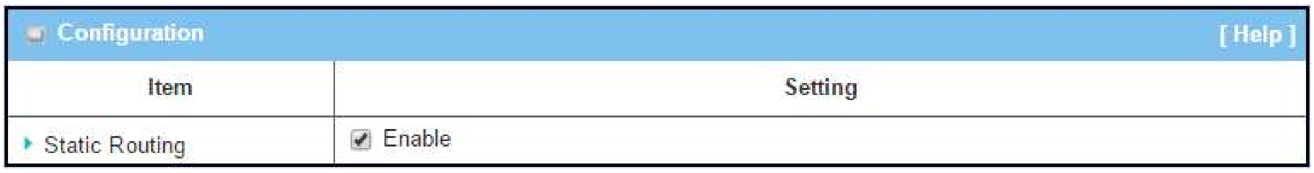
The "Static Routing Rule List" window lists all your defined static routing rule entries. Using "Add" or "Edit" button to add and create one new static routing rule or to modify an existed one.

When "Add" or "Edit" button is applied the "Static Routing Rule Configuration" window will appear to let you define a static routing rule. The parameters include the destination IP address and subnet mask of dedicated host/server or subnet, the IP address of peer gateway, the metric and the rule activation.

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

Enable Static Routing

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

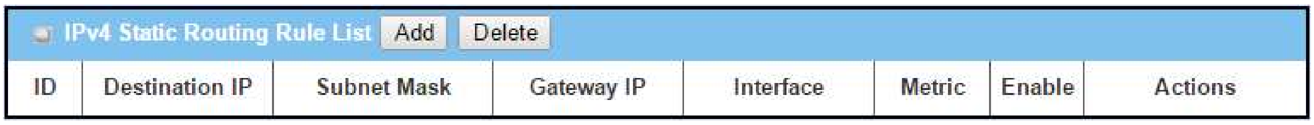


Item	Setting
Static Routing	☑ Enable

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

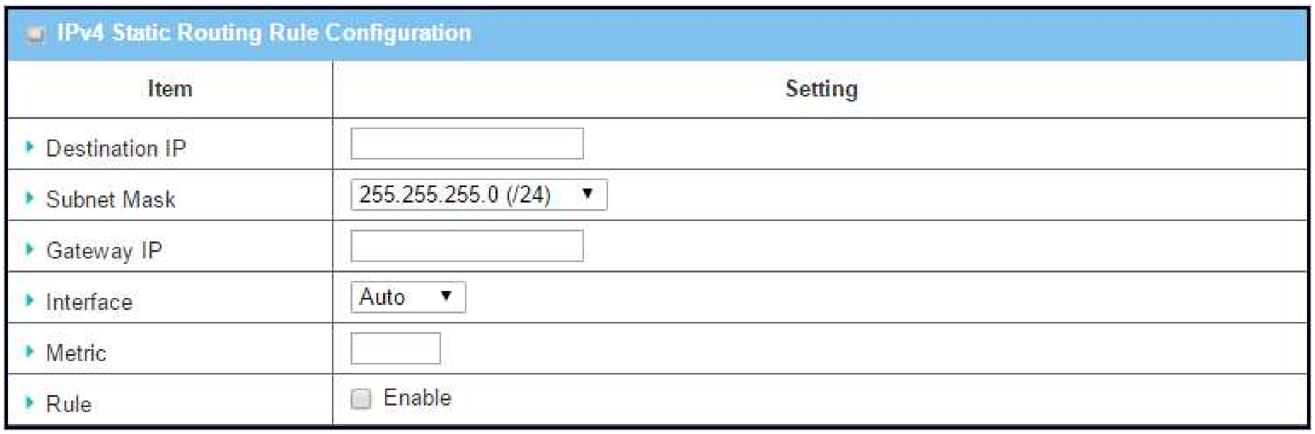
Create/Edit Static Routing Rules

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



ID	Destination IP	Subnet Mask	Gateway IP	Interface	Metric	Enable	Actions

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



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	The Destination IP of this static routing rule.
Subnet Mask	255.255.255.0 (/24) is set by default	The Subnet Mask of this static routing rule.
Gateway IP	1. IPv4 Format 2. A Must filled setting	The Gateway IP of this static routing rule.
Interface	Auto is set by default	The Interface of this static routing rule.
Metric	1. Numberic String Format 2. A Must filled setting	The Metric of this static routing rule.
Rule	The box is unchecked by	Click **Enable** box to activate this rule.

	default.	
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore what you just configured back to the previous setting. Please note that the restored setting may not be the factory default setting but a retrieve of what was saved in the memory.
Back	NA	When the **Back** button is clicked the screen will return to the Static Routing Configuration page.

3.b.3 Dynamic Routing

Dynamic Routing, also called adaptive routing, describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in network conditions. The adaptation is intended to allow as many routes as possible to remain valid (that is, have destinations that can be reached) in response to the change.

This gateway supports dynamic routing protocols, including RIPv1/RIPv2 (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol), for you to establish routing table automatically. The feature of dynamic routing will be very useful when there are lots of subnets in your network. Generally speaking, RIP is suitable for small network. OSPF is more suitable for medium network. BGP is more used for big network infrastructure.

The supported dynamic routing protocols are described as follows.

RIP Scenario

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

OSPF Scenario

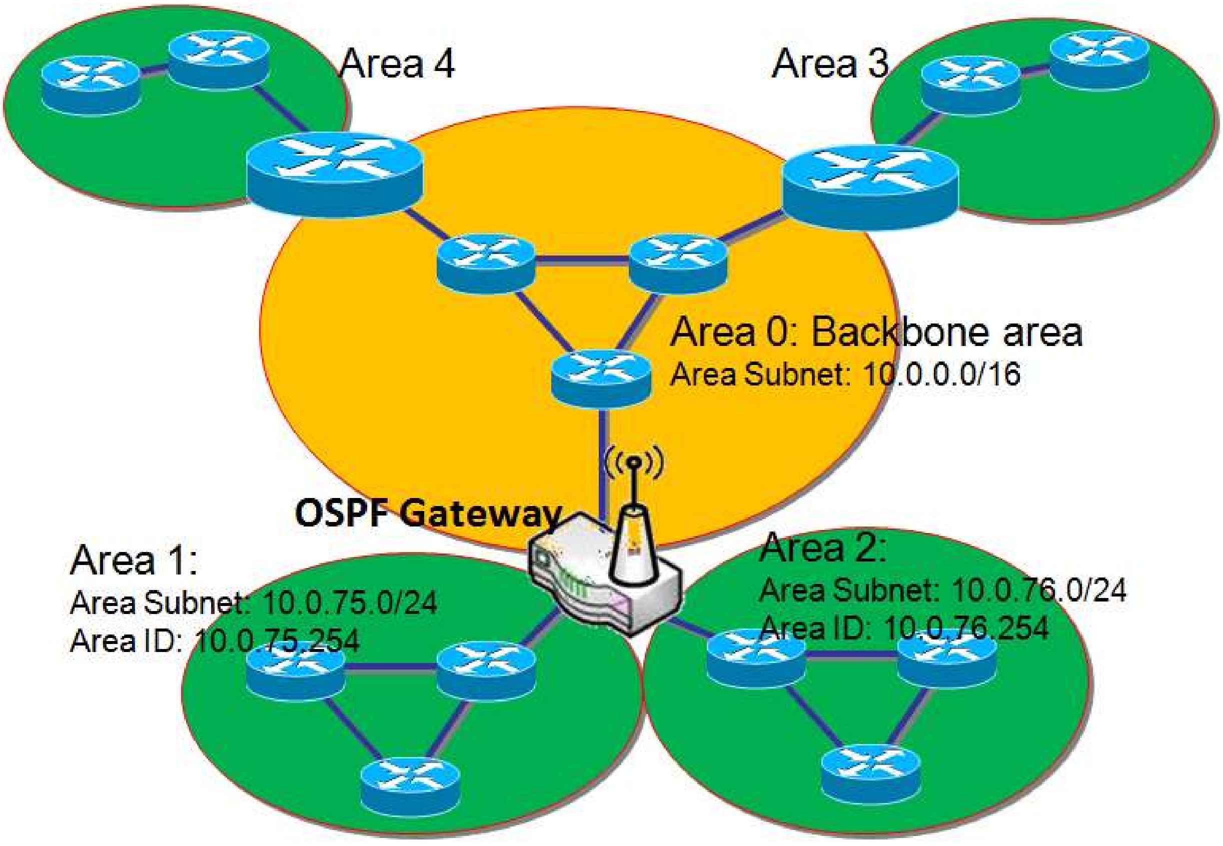
Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). OSPF is perhaps the most widely used interior gateway protocol (IGP) in large enterprise networks. IS-IS, another link-state dynamic routing protocol, is more common in large service provider networks. The most widely used exterior gateway protocol is the Border Gateway Protocol (BGP), the principal routing protocol between autonomous systems on the Internet.

OSPF is an interior gateway protocol (IGP) for routing Internet Protocol (IP) packets solely within a single routing domain, such as an autonomous system. It gathers link state information from available routers and constructs a topology map of the network. The topology is presented as a routing table to the Internet Layer which routes datagrams based solely on the destination IP address found in IP packets.

OSPF detects changes in the topology, such as link failures, and converges on a new loop-free routing structure within seconds. It computes the shortest path tree for each route using a method based on Dijkstra's algorithm, a shortest path first algorithm.

The OSPF routing policies for constructing a route table are governed by link cost factors (external metrics) associated with each routing interface. Cost factors may be the distance of a router (round-trip time), data throughput of a link, or link availability and reliability, expressed as simple unit-less numbers. This provides a dynamic process of traffic load balancing between routes of equal cost.

An OSPF network may be structured, or subdivided, into routing areas to simplify administration and optimize traffic and resource utilization. Areas are identified by 32-bit numbers, expressed either simply in decimal, or often in octet-based dot-decimal notation, familiar from IPv4 address notation.



Scenario Application Timing

When the administrator of the gateway wants to deploy one OSPF gateway in a large enterprise and expects the gateway to learn its routing table by using OSPF protocol from the enterprise backbone. The OSPF gateway will forward its routing information to other routers that are under the gateway and not linked to the enterprise backbone.

Scenario Description

The OSPF gateway gathers routing information from the backbone gateways in area 0 by using OSPF dynamic routing protocol.

The OSPF gateway will forward its routing information to other routers that are under the gateway and not linked to the enterprise backbone.

Parameter Setup Example

Following tables list the parameter configuration as an example for the OSPF gateway in above diagram.

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

Configuration Path	[Dynamic Routing]-[OSPF Configuration]
OSPF	■ ***Enable***
Backbone Subnet	**10.0.0.0/16**

Configuration Path	[Dynamic Routing]-[OSPF Area List]	
ID	1	2
Area Subnet	***10.0.75.0/24***	***10.0.76.0/24***
Area ID	***10.0.75.254***	***10.0.76.254***
Area	■ ***Enable***	■ ***Enable***

Scenario Operation Procedure

In above diagram, the OSPF Gateway is one gateway of the enterprise backbone (area code is 0.0.0.0 and area subnet is 10.0.0.0/16) and it links with other OSPF gateways in the backbone. It dominates two areas of subnets: area 1 with area code is 10.0.75.254 and area subnet is 10.0.75.0/24, and area 2 with area code is 10.0.76.254 and area subnet is 10.0.76.0/24.

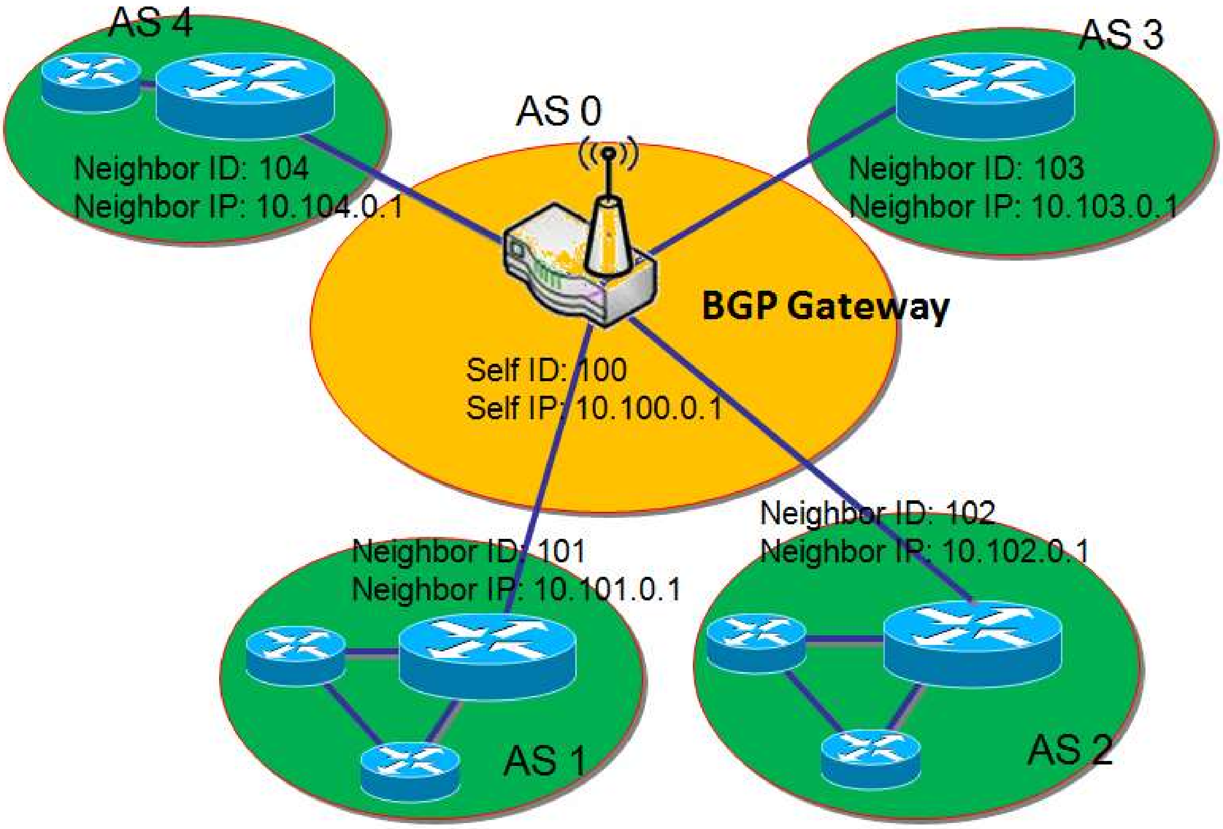
By operating with OSPF protocol, the OSPF gateway can gather the routing information from other OSPF gateways in the enterprise backbone. And then it forwards the routing information to the routers in its dominated areas.

Finally, the routers in the dominated areas of the OSPF Gateway know the shortest routing path for each destination IP address of outgoing packets.

BGP Scenario

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet. The protocol is often classified as a path vector protocol but is sometimes also classed as a distance-vector routing protocol. The Border Gateway Protocol makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator, and is involved in making core routing decisions.

BGP may be used for routing within an AS. In this application it is referred to as Interior Border Gateway Protocol, Internal BGP, or iBGP. In contrast, the Internet application of the protocol may be referred to as Exterior Border Gateway Protocol, External BGP, or eBGP.



Scenario Application Timing

Most Internet service providers (ISPs) must use BGP to establish routing between one another (especially if they are multi-homed). Very large private IP networks use BGP internally. An example would be the joining of a number of large OSPF (Open Shortest Path First) networks where OSPF by itself would not scale to size. Another reason to use BGP is multi-homing a network for better redundancy, either to multiple access points of a single ISP or to multiple ISPs.

Scenario Description

The BGP gateway dominates an autonomous system (AS) of networking and links with some other border gateways for exchanging routing information.

The BGP gateway will distribute the collected routing information in its dominated AS. Then all routers in the AS know how to route packets to other AS.

Parameter Setup Example

Following tables list the parameter configuration as an example for the BGP gateway in above diagram.

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

Configuration Path	[Dynamic Routing]-[BGP Configuration]
BGP	■ ***Enable***
Self ID	**100**

Configuration Path	[Dynamic Routing]-[BGP Neighbor List]			
ID	1	2	3	4
Neighbor IP	***10.101.0.1***	***10.102.0.1***	***10.103.0.1***	***10.104.0.1***
Neighbor ID	***101***	***102***	***103***	***104***
Neighbor	■ ***Enable***	■ ***Enable***	■ ***Enable***	■ ***Enable***

Scenario Operation Procedure

In above diagram, the BGP Gateway is one gateway of its dominated AS (self IP is 10.100.0.1 and self ID is 100) and it links with other BGP gateways in the Internet. The scenario is like the networking in one ISP to be linked with the ones in other ISPs.

By operating with BGP protocol, the BGP gateway can gather the routing information from other BGP gateways in the Internet. And then it forwards the routing information to the routers in its dominated AS.

Finally, the routers in the dominated AS of the BGP Gateway know how to route packets to other AS.

Dynamic Routing Setting

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

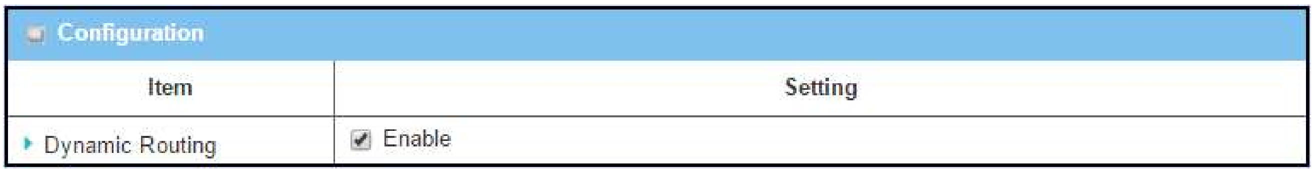
In the "Dynamic Routing" page, there are seven configuration windows for dynamic routing feature. They are the "RIP Configuration" window, "OSPF Configuration" window, "OSPF Area List", "OSPF Area Configuration", "BGP Configuration", "BGP Neighbor List" and "BGP Neighbor Configuration" window. RIP, OSPF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

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

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

Enable Dynamic Routing

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



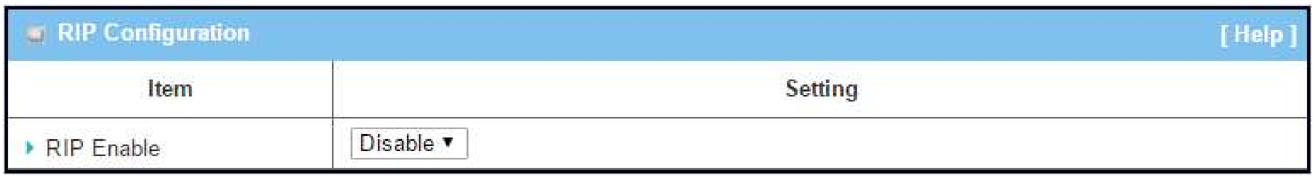
Configuration

Item	Setting
Dynamic Routing	☑ Enable

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

Enable RIP

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



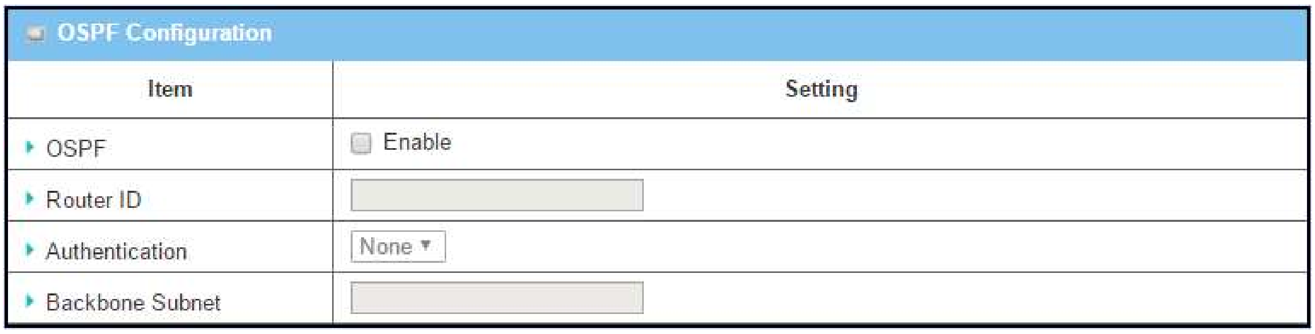
RIP Configuration [Help]

Item	Setting
RIP Enable	Disable ▾

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

Enable OSPF

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



OSPF Configuration

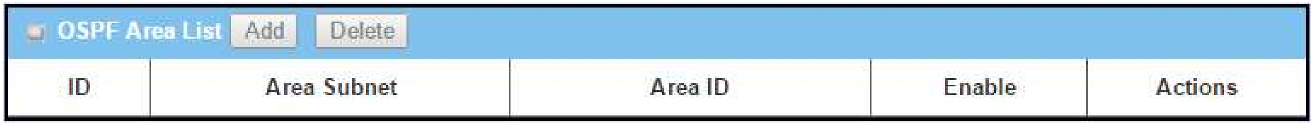
Item	Setting
OSPF	□ Enable
Router ID	
Authentication	None ▾
Backbone Subnet	

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

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

Create/Edit OSPF Area Rules

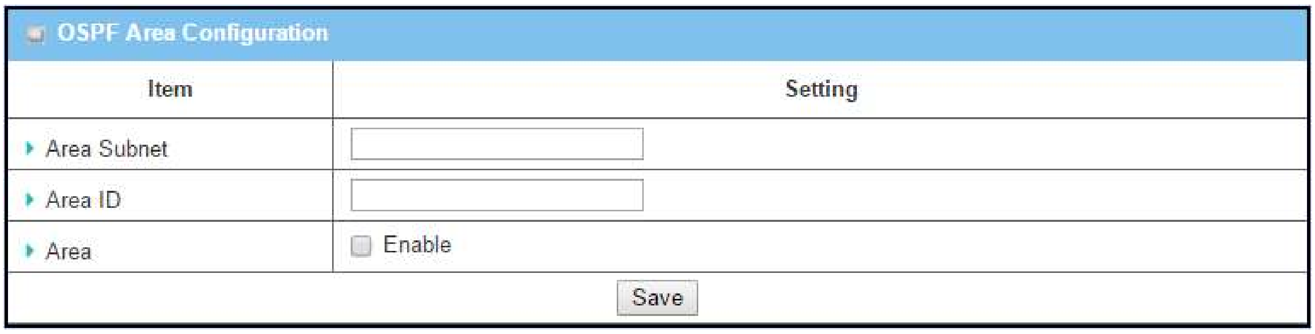
The router allows you to custom your OSPF Area List rules. It supports up to a maximum of 32 rule sets.



OSPF Area List Add Delete

ID	Area Subnet	Area ID	Enable	Actions

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



OSPF Area Configuration

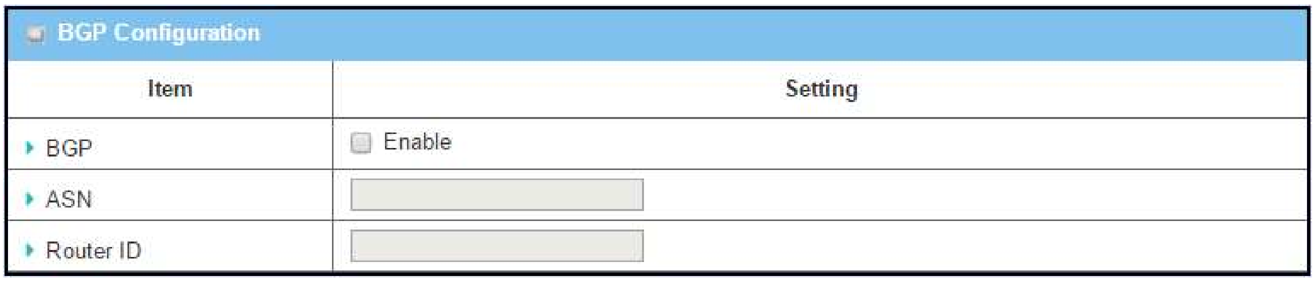
Item	Setting
Area Subnet	
Area ID	
Area	□ Enable

Save

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

Enable BGP

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



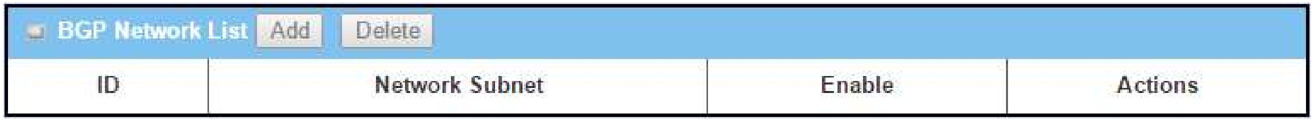
BGP Configuration

Item	Setting
BGP	□ Enable
ASN	
Router ID	

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

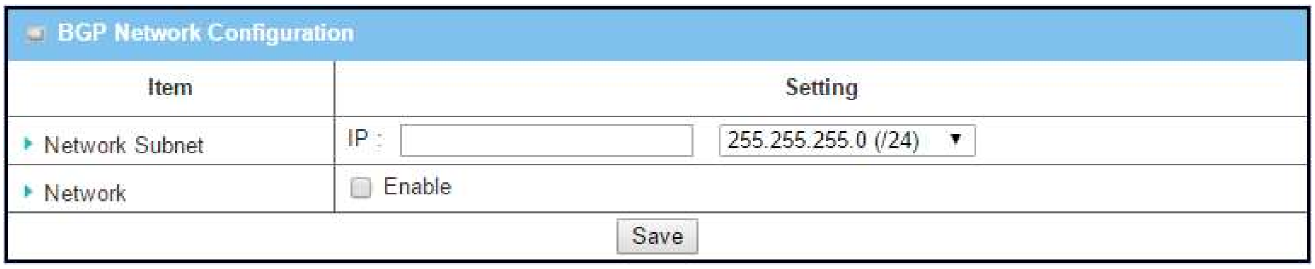
Create/Edit BGP Network Rules

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



ID	Network Subnet	Enable	Actions

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



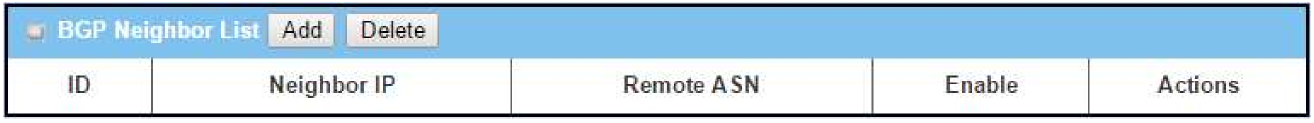
BGP Network Configuration

Item	Setting
Network Subnet	IP : 255.255.255.0 (/24) ▼
Network	□ Enable

Item	Value setting	Description
Network Subnet	1. IPv4 Format 2. A Must filled setting	The Network Subnet of this router on BGP Network List. It composes of entered the IP address in this field and the selected subnet mask.
Network	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration

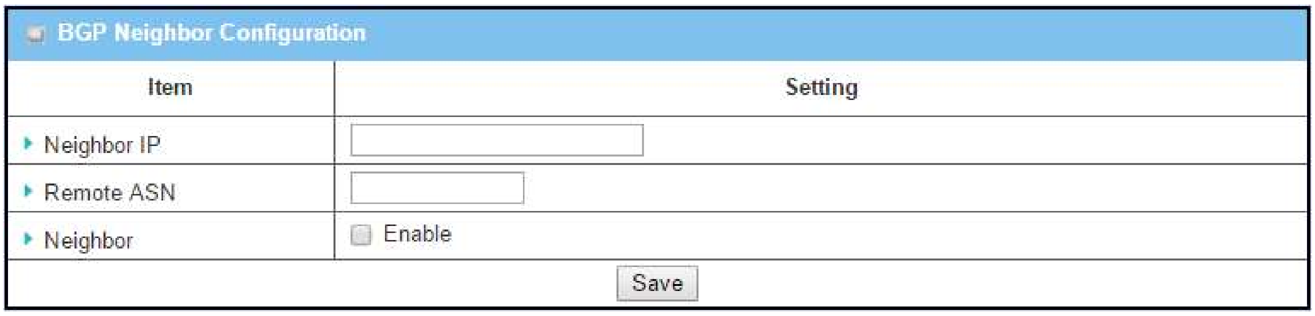
Create/Edit BGP Neighbor Rules

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



ID	Neighbor IP	Remote ASN	Enable	Actions

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



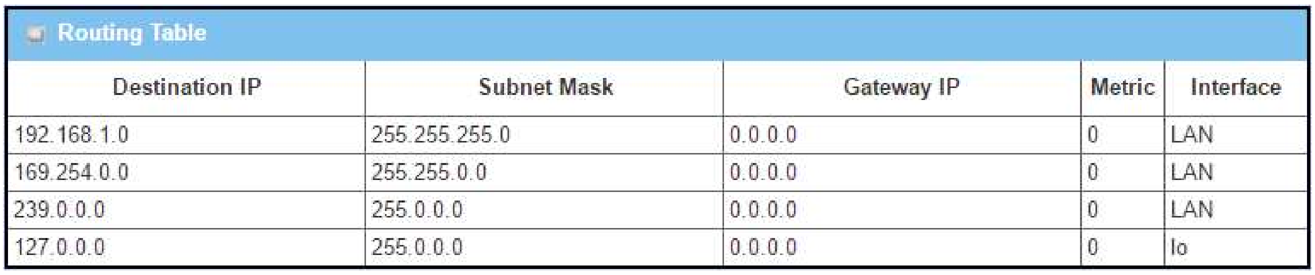
Item	Setting
Neighbor IP	
Remote ASN	
Neighbor	□ Enable

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

3.b.5 Routing Information

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

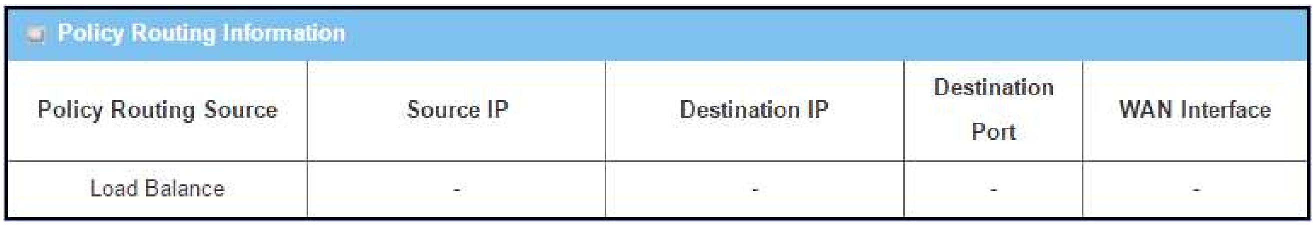
Go to **Basic Network > Routing > Routing Information** Tab.



Routing Table

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

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



Policy Routing Information

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

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

3.d DNS & DDNS

How does user access your server if your WAN IP address changes all the time? One way is to register a new domain name, and maintain your own DNS server. Another simpler way is to apply a domain name to a third-party DDNS service provider. The service can be free or charged. If you want to understand the basic concepts of DNS and Dynamic DNS, you can refer to Wikipedia website[9,10].

3.d.1 DNS & DDNS Configuration

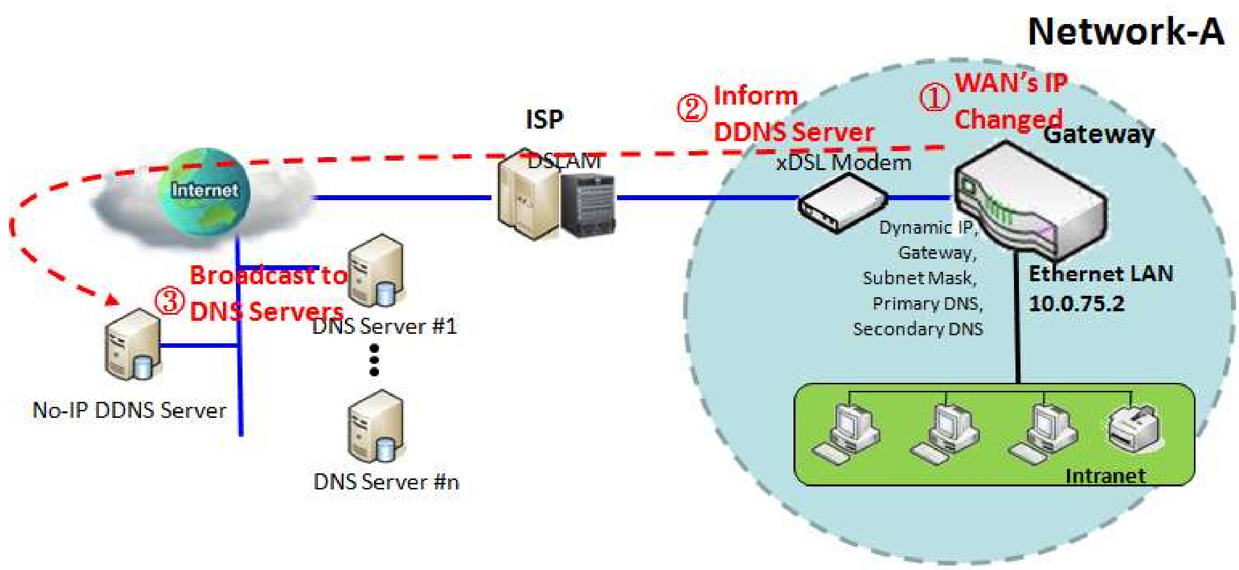
To host your server on a changing IP address, you have to use dynamic domain name service (DDNS). Therefore, anyone wishing to reach your host only needs to know the domain name. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service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

In short, the Dynamic DNS service allows the gateway to alias a public dynamic IP address to a static domain name, allowing the gateway to be more easily accessed from various locations on the Internet. The user has to register a domain name to a third-party DDNS service provider to use DDNS function.

Once the IP address of a WAN interface in the gateway has changed, the dynamic DNS agent in the gateway will inform the DDNS server with the new IP address. The server automatically re-maps your domain name with the changed IP address. So, other hosts in the Internet world will be able to link to your gateway by using your domain name regardless of the changing global IP address.

Dynamic DNS Scenario

[9] http://en.wikipedia.org/wiki/Domain_Name_System
[10] http://en.wikipedia.org/wiki/Dynamic_DNS



Scenario Application Timing

When the IP address of the Gateway is often changed by ISP, and other hosts in the Internet want to link to the gateway device by using its corresponding domain name, the gateway must provide the dynamic DNS function to carry out the requirement.

Scenario Description

Apply one account to the DDNS provider for DDNS service before DDNS function in the gateway can work.

The gateway asks the DDNS server to re-map the domain name and WAN's IP address of the gateway once the IP address has been changed.

Parameter Setup Example

Following table lists the parameter configuration as an example for the gateway in above diagram with "Dynamic DNS" enabling.

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

Configuration Path	[Dynamic DNS]-[Dynamic DNS]
DDNS	■ ***Enable***
Provider	**No-IP.com**
Host Name	**JP-NB**
Username / E-mail	**Chinghuihsieh**

Password / Key	**ddnspassword**

Scenario Operation Procedure

In above diagram, the Gateway is the gateway of Network-A and the subnet of its Intranet is 10.0.75.0/24. The gateway has the IP address of 10.0.75.2 for LAN interface and gets a dynamic IP 118.18.81.33 for WAN-1 interface. It serves as a NAT router.

Configure the required parameters for DDNS function by referring to above setup example. When the gateway has booted up and has gotten a dynamic IP address for the WAN interface, the DDNS agent in the gateway tries to request the DDNS server with the mapping between the domain name and the obtained WAN IP address of the gateway.

The DDNS server broadcasts the mapping to other DNS servers for DNS hosting service in the Internet world. So, other hosts in the Internet can link to the gateway by using the domain name.

Once the gateway has dynamically changed its WAN IP address from ISP, the DDNS agent tries again to request the DDNS server with the re-mapping between the domain name and the new WAN IP address of the gateway.

The DDNS server broadcasts again the new mapping to other DNS servers for DNS hosting service in the Internet world.

Finally, other hosts in the Internet can still link to the gateway by using the domain name, even the WAN IP address of the gateway has changed.

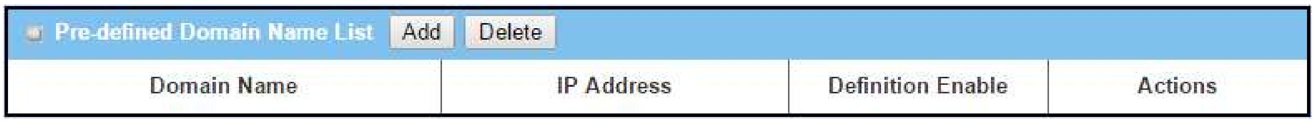
DNS & DDNS Setting

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

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

Create/Edit Pre-defined Domain Name List

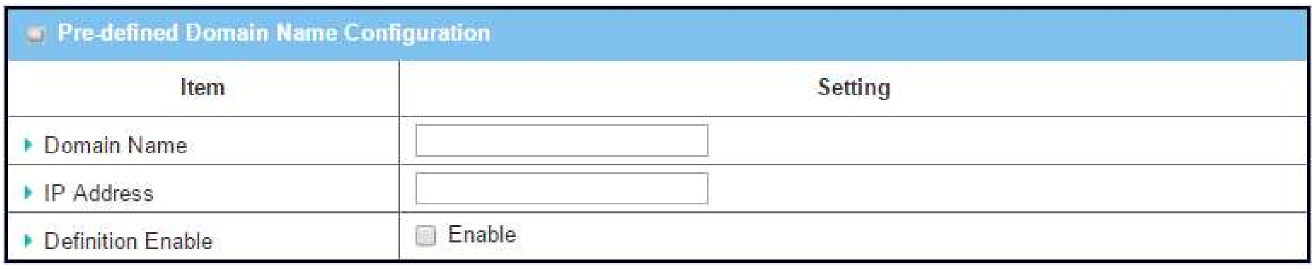
The router allows you to custom your pre-defined domain name list. It supports up to a maximum of 128 sets.



Pre-defined Domain Name List Add Delete

Domain Name	IP Address	Definition Enable	Actions

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



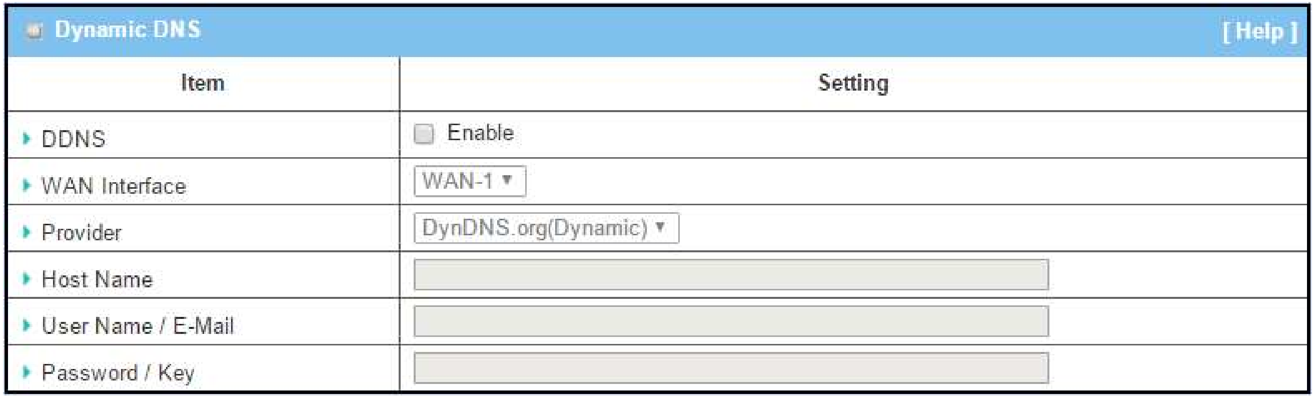
Pre-defined Domain Name Configuration

Item	Setting
Domain Name	
IP Address	
Definition Enable	□ Enable

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

Setup Dynamic DNS

The router allows you to custom your Dynamic DNS settings.



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

DDNS (Dynamic DNS) Configuration		
Item	**Value setting**	**Description**
DDNS	The box is unchecked by default	Check the **Enable** box to activate this function.
WAN Interface	WAN 1 is set by default	Select the WAN Interface IP Address of the router.
Provider	DynDNS.org (Dynamic) is set by default	Your DDNS provider of Dynamic DNS.
Host Name	1. String format can be any text 2. A Must filled setting	Your registered host name of Dynamic DNS.
User Name / E-Mail	1. String format can be any text 2. A Must filled setting	Your User name or E-mail addresss of Dynamic DNS.
Password / Key	1. String format can be any text 2. A Must filled setting	Your Password or Key of Dynamic DNS.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

3.f QoS

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

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

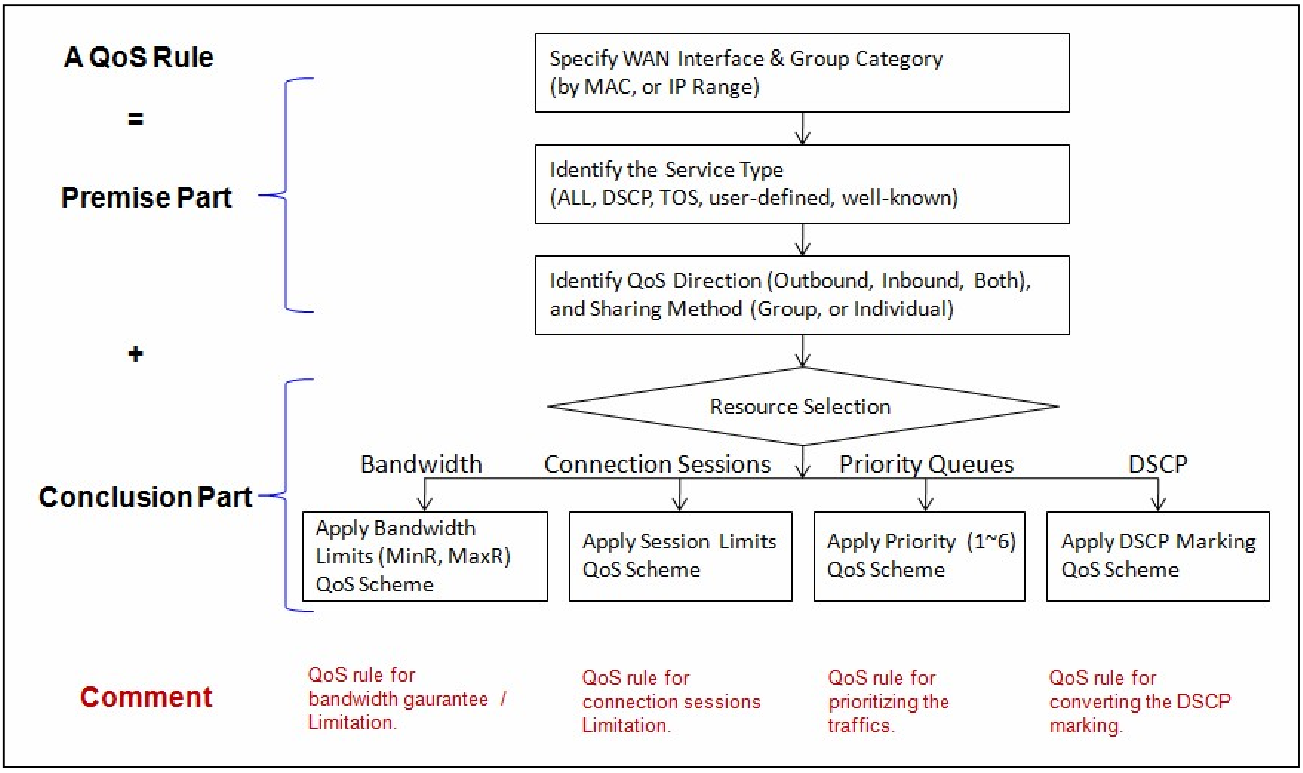
To utilize your network throughput completely, administrator must define bandwidth control rules carefully to balance the utilization of network bandwidth for all users to access. It is indeed required that an access gateway satisfies the requirements of latency-critical applications, minimum access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

3.f.1 QoS Configuration

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

QoS Rule Configuration

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


A QoS Rule
=
Premise Part
+
Conclusion Part
Comment
Specify WAN Interface & Group Category
(by MAC, or IP Range)
Identify the Service Type
(ALL, DSCP, TOS, user-defined, well-known)
Identify QoS Direction (Outbound, Inbound, Both),
and Sharing Method (Group, or Individual)
Resource Selection
Bandwidth
Connection Sessions
Priority Queues
DSCP
Apply Bandwidth Limits (MinR, MaxR) QoS Scheme
Apply Session Limits QoS Scheme
Apply Priority (1~6) QoS Scheme
Apply DSCP Marking QoS Scheme
QoS rule for bandwidth gaurantee / Limitation.
QoS rule for connection sessions Limitation.
QoS rule for prioritizing the traffics.
QoS rule for converting the DSCP marking.

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

The Rule-based QoS has following features.

Multiple Group Categories

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

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

Differentiated Services

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

Differentiated services can be based on 802.1p, DSCP, TOS, VLAN ID, User-defined Services and Well-known Services.

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

Available Control Functions

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

For bandwidth resource, control functions include guaranteeing bandwidth and limiting bandwidth. For priority queue resource, control function is setting priority. For DSCP resource, control function is DSCP marking. The last resource is Connection Sessions; the related control function is limiting connection sessions.

Individual / Group Control

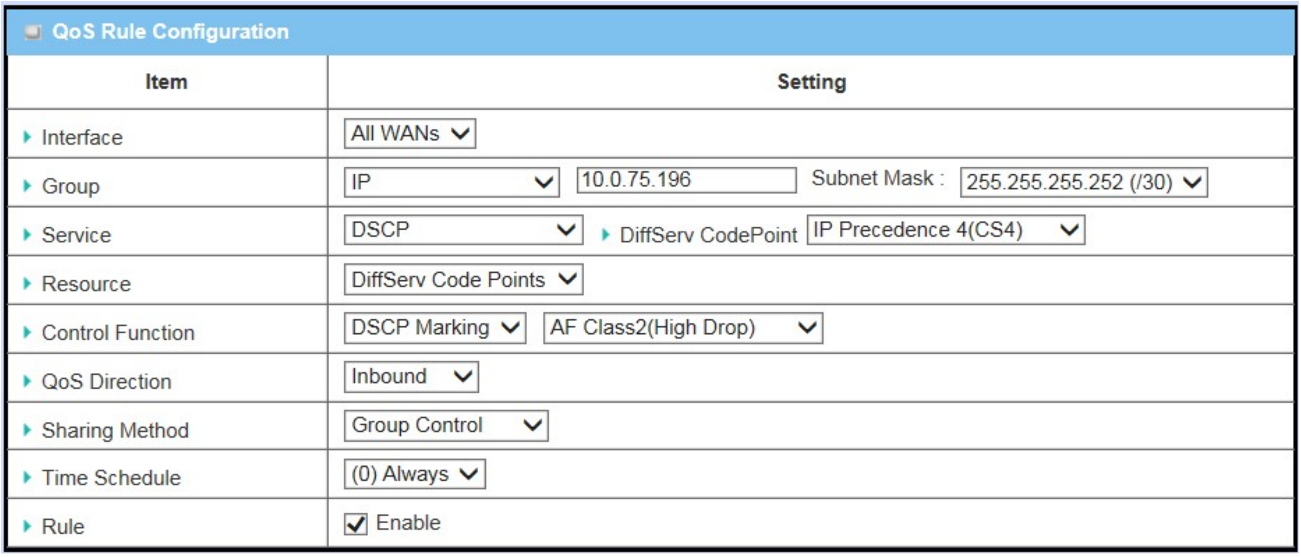
One QoS rule can be applied to individual member or whole group in the target group. This feature depends on model.

Outbound / Inbound Control

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

Two QoS rule examples are listed as below.

➢ "DSCP" Type of QoS Rule Example



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)
Resource	DiffServ Code Points
Control Function	DSCP Marking AF Class2(High Drop)
QoS Direction	Inbound
Sharing Method	Group Control
Time Schedule	(0) Always
Rule	☑ Enable

Scenario Application Timing

When the administrator of the gateway wants to convert the code point value, "IP Precedence 4(CS4)", in the packets from some client hosts (IP 10.0.75.196~199) to the code value, "AF Class2(High Drop)", he can use the "Rule-based QoS" function to carry out this rule by defining an QoS rule as shown in above diagram.

Scenario Description

Convert the code point value from "IP Precedence 4(CS4)" to "AF Class2(High Drop)" for incoming packets from some client hosts in the Intranet.

Parameter Setup Example

Following tables list the parameter configuration as an example for the gateway in above diagram with "Rule-based QoS" enabling.

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

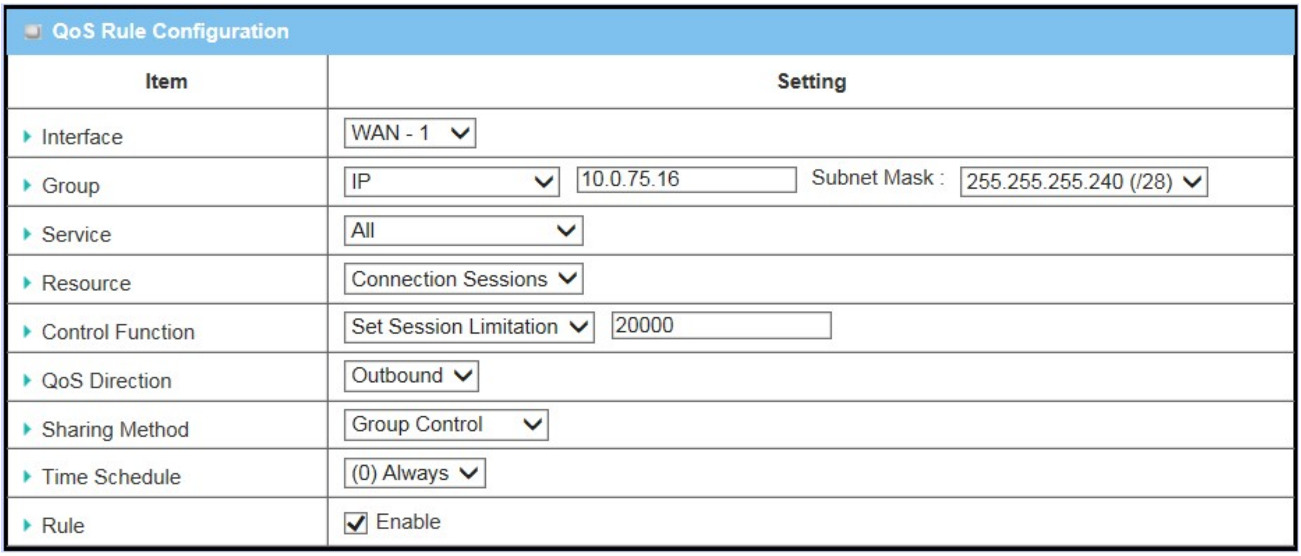
Configuration Path	[Rule-based QoS]-[Configuration]
Rule-based QoS	■ *Enable*
Flexible Bandwidth Management	■ *Enable*

Configuration Path	[Rule-based QoS]-[QoS Rule Configuration]
Interface	*All WANs*
Group	***IP 10.0.75.196*** Subnet Mask: ***255.255.255.252 (/30)***
Service	***DSCP*** DiffServ Code Point ***IP Precedence 4(CS4)***
Resource	***DiffServ Code Points***
Control Function	***DSCP Marking AF Class2(High Drop)***
QoS Direction	***Inbound***
Sharing Method	***Group Control***
Time Schedule	***(0) Always***
Rule	■ ***Enable***

Scenario Operation Procedure

This rule means IP packets from all WAN interfaces to LAN IP address 10.0.75.196 ~ 10.0.75.199 which have DiffServ code points with “IP Precedence 4(CS4)” value will be modified by “DSCP Marking” control function with “AF Class 2(High Drop)” value at any time.

➢ "Connection Sessions" Type of QoS Rule Example



QoS Rule Configuration

Item	Setting
Interface	WAN - 1
Group	IP 10.0.75.16 Subnet Mask : 255.255.255.240 (/28)
Service	All
Resource	Connection Sessions
Control Function	Set Session Limitation 20000
QoS Direction	Outbound
Sharing Method	Group Control
Time Schedule	(0) Always
Rule	☑ Enable

Scenario Application Timing

When the administrator of the gateway wants to limit the connection sessions from some client hosts (IP 10.0.75.16~31) to 20000 sessions totally for accessing the Internet, he can use the "Rule-based QoS" function to carry out it by defining an QoS rule as shown in above diagram.

Scenario Description

Specify the maximum connection sessions from some client hosts (IP 10.0.75.16~31) for accessing the Internet.

Parameter Setup Example

Following tables list the parameter configuration as an example for the gateway in above diagram with "Rule-based QoS" enabling.

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

Configuration Path	[Rule-based QoS]-[Configuration]
Rule-based QoS	■ ***Enable***
Flexible Bandwidth Management	■ ***Enable***

Configuration Path	[Rule-based QoS]-[QoS Rule Configuration]
Interface	***WAN-1***
Group	***IP 10.0.75.16*** Subnet Mask: ***255.255.255.240 (/28)***
Service	***All***
Resource	***Connection Sessions***
Control Function	***Set Session Limitation 20000***
QoS Direction	***Outbound***
Sharing Method	***Group Control***

Time Schedule	***(0) Always***
Rule	■ ***Enable***

Scenario Operation Procedure

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

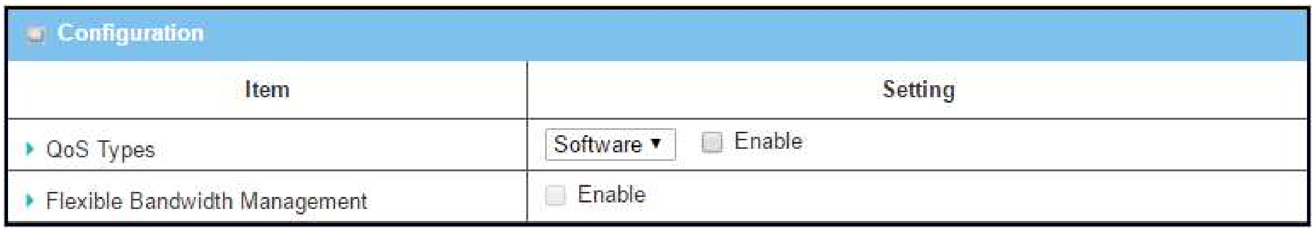
QoS Configuration Setting

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

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

Go to Basic Network > QoS > Configuration tab.

Enable QoS Function



Configuration

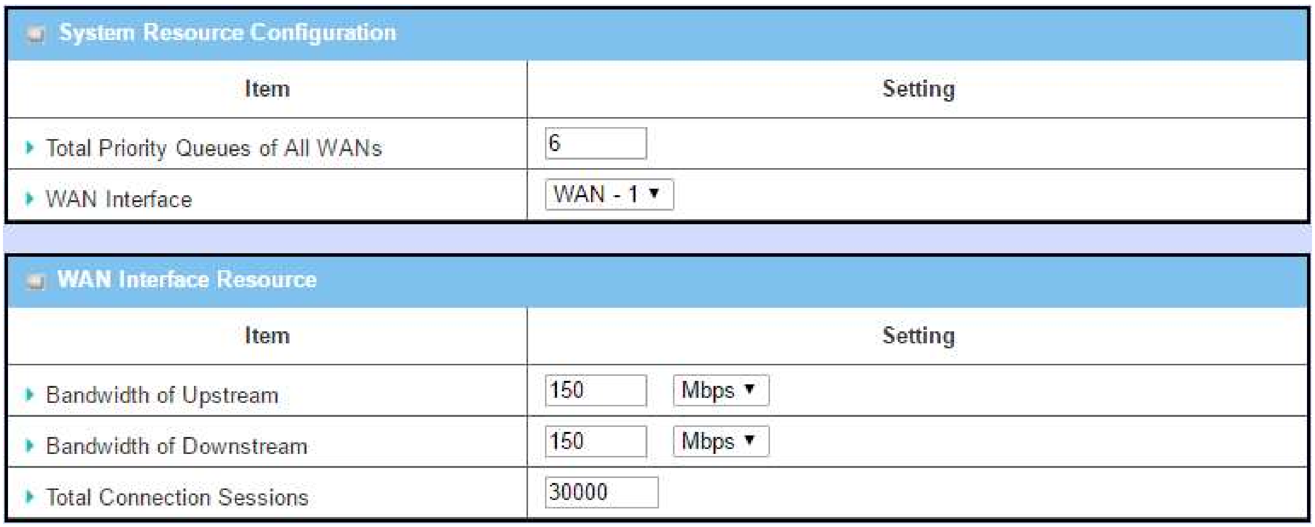
Item	Setting
QoS Types	Software ▾ □ Enable
Flexible Bandwidth Management	□ Enable

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, and then click **Enable** box to activate the QoS function. The default QoS type is set to **Software** QoS. For some models, there is another option for **Hardware** QoS.
Flexible Bandwidth Management	The box is unchecked by default	Click **Enable** box to activate the Flexible Bandwidth Management function.
Save	N/A	Click the **Save** button to save the settings.

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

Ensure QoS and Bandwidth are enabled and saved to further configure the detailed QoS settings.

Setup System Resource



System Resource Configuration

Item	Setting
Total Priority Queues of All WANs	6
WAN Interface	WAN - 1 ▾

WAN Interface Resource

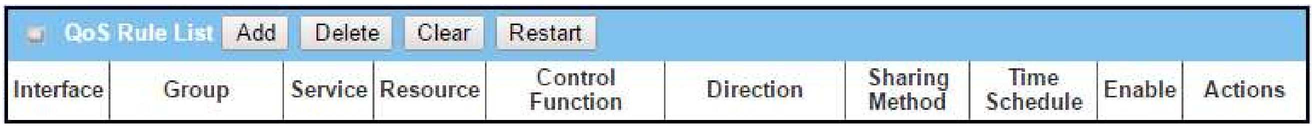
Item	Setting
Bandwidth of Upstream	150 Mbps ▾
Bandwidth of Downstream	150 Mbps ▾
Total Connection Sessions	30000

System Resource Configuration		
Item	**Value Setting**	**Description**
Total Priority Queues of All WANs	1. A Must filled setting. 2. **6** is set by default.	Define the total priority queues that are available for the QoS settings that required to specifying **Priority Queues** of **Resource.** It is also related to default banwidth of WANs.
WAN Interface	**WAN-1** is selected by default.	Select the WAN interface and then the following **WAN Interface Resource** screen will show the related resources for configuration. ● **Bandwidth of Upstream** Specify total upload bandwidth of the selected WAN. ● **Bandwidth of Downstream** Specify total download bandwidth of the selected WAN. ● **Total Connection Sessions** Specify total connection sessions of the selected WAN.
Save	N/A	Click the **Save** button to save the settings.

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

Create/Edit QoS Rules

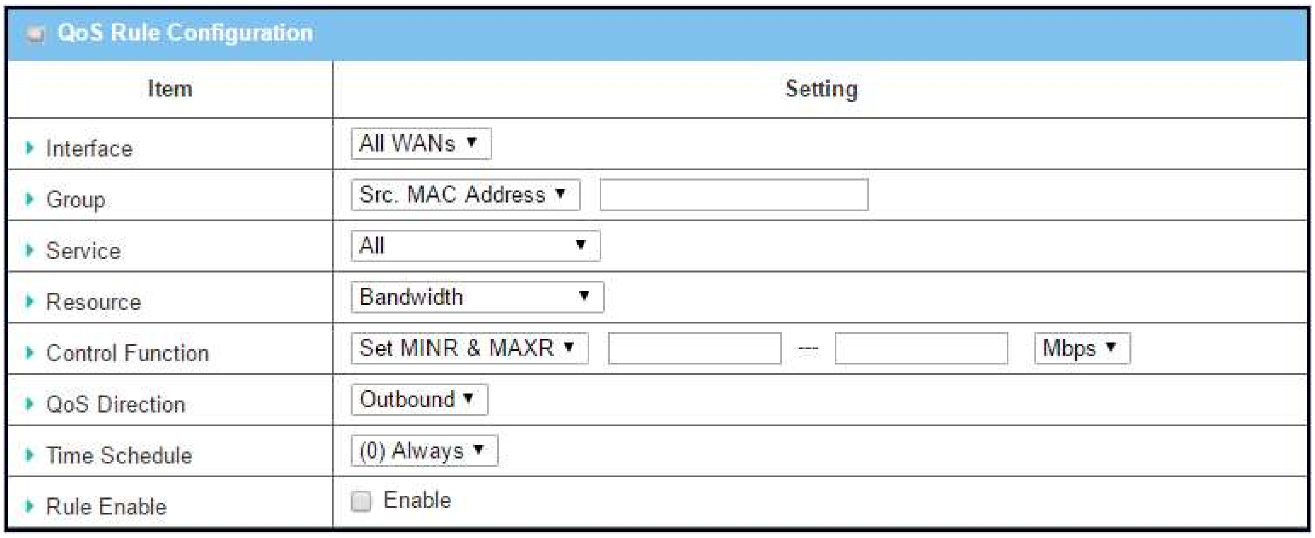
After enabled the QoS function and configured the system resources, you have to further specify some QoS rules for provide better service on the interested traffics. The gateway supports up to a maximum of 128 rule-based QoS rule sets.



QoS Rule List Add Delete Clear Restart

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

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



QoS Rule Configuration

Item	Setting
Interface	All WANs ▾
Group	Src. MAC Address ▾
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. It can be **Src. MAC Address**, **IP**, or **Host Name.** Select **Src. MAC Address** to prioritize packets based on MAC. Configure **Service** in the next line then go to **Resource_1**. Select **IP** to prioritize packets based on IP address and Subnet Mask. Configure **Service** in the next line, then go to **Resource_2**. Select **Host Name** to prioritize packets based on a group of a pre-configured group of host from the dropdown list. If the dropdown list is empty, ensure if any group is pre-configured. Configure **Service** in the next line, then go to **Resource_3.**

		Note: The required host groups must be created in advance and corresponding **QoS** checkbox in the **Multiple Bound Services** field is checked before the **Host Group** option become available. Refer to **Object Definition > Grouping > Host Grouping.**
Service	1. A Must filled setting. 2. **All** is selected by default.	Specify the service type of traffics that have to be applied with the QoS rule. It can be **All**, **DSCP**, **TOS**, **User-defined Service**, or **Well-known Service**. Select **All** for all packets. Select **DSCP** for DSCP type packets only. Select **TOS** for TOS type packets only. You have to select a service type (**Minimize-Cost**, **Maximize-Reliability**, **Maximize-Throughput**, or **Minimize-Delay**) from the dropdown list as well. Select **User-defined Service** for user-defined packets only. You have to define the port range and protocol as well. Select **Well-known Service** for specific application packets only. You have to select the required service from the dropdown list as well.
Resource, and **Control Function**	A Must filled setting	Specify the Resource Type and corresponding Control function for the QoS rule. The available Resource options are **Bandwidth**, **Connection Sessions**, **Priority Queues**, and **DiffServ Codepoints**. **Bandwidth**: Select **Bandwidth** as the resource type for the QoS Rule, and you have to assign the min rate, max rate and rate unit as the bandwidth settings in the **Control Function** / **Set MINR & MAXR** field. **Connection Sessions**: Select **Connection Sessions** as the resource type for the QoS Rule, and you have to assign 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 you have to 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 you have to 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. It can be **Outbound**, **Inbound**, or **Both**. **Outbound**: Select **Outbound** to prioritize the traffics going to the Internet via the specified interface. Under such situation, the hosts specified in the Group field is a source group. **Inbound**: Select **Inbound** to prioritize the traffics coming from the Internet via the specified interface. Under such situation, the hosts

		specified in the Group field is a destination group. **Both**: Select **both** to prioritize the traffics passing through the specified interface, both Inbound and Outbound are considered. Under such situation, the hosts specified in the Group field can be a source or destination group.
Sharing Method	1. A Must filled setting. 2. **Group Control** is selected by default.	Specify the preferred sharing method for how to apply the QoS rule on the selected group. It can be **Individual Control** or **Group Control**. **Individual Control**: If **Individual Control** is selected, each host in the group will have his own QoS service resource as specified in the rule. **Group Control**: If **Group Control** is selected, all the group hosts share the same QoS service resource.
Time Schedule	1. A Must filled setting. 2. **(0) Always** is selected by default.	Apply **Time Schedule** to this rule, otherwise leave it as (0) **Always.** (refer to **Object Definition > Scheduling > Configuration** settings)
Rule Enable	The box is unchecked by default.	Click **Enable** box to activate this QoS rule.
Save	N/A	Click the **Save** button to save the settings.

3.h Redundancy

In engineering, redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system, usually in the form of a backup or fail-safe. In an IP networking, the access gateway is the critical part of the networking system. Redundant gateway plays the backup one of the master gateway and it will take over the data transmitting job once it finds the master gateway failed.

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

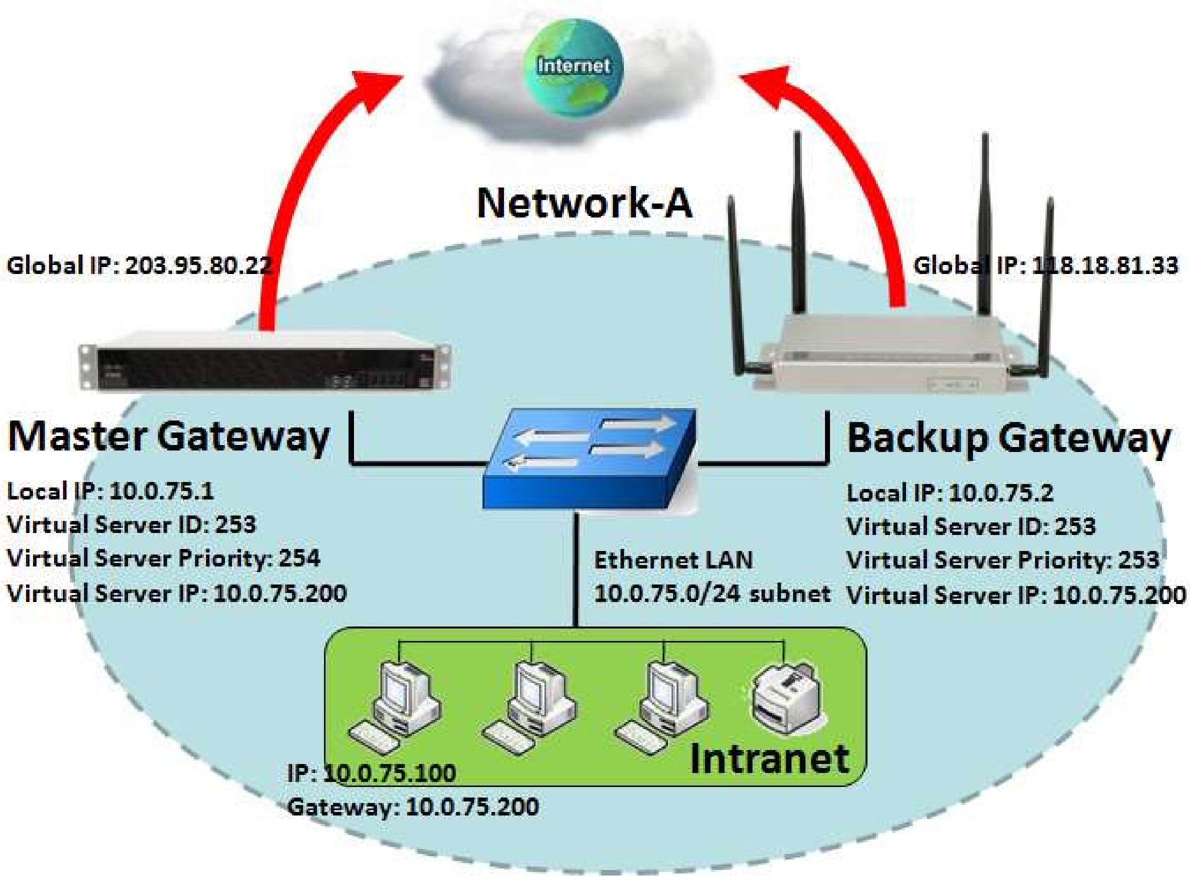
3.h.1 VRRP

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

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

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

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



Scenario Application Timing

When the enterprise gateway needs a reliable connection to the Internet, administrator can setup a group of VRRP redundant gateways as the enterprise entry gateway. Each member gateway connects to different ISP for a redundant connection to the Internet. So, the enterprise gateway is reliable even the master connection is failed.

Scenario Description

When the master gateway is disabled of its Internet connection, the backup gateway whose priority is the highest among the ones with alive Internet connection will take over the data communication duty and serves as the master.

Once the backup gateway is recovered from terminated Internet connection and its priority is higher than the one of the master gateway, the data communication duty will return to it.

Parameter Setup Example

Following tables list the parameter configuration as a group example for the gateways in above diagram with "VRRP" enabling.

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

- Master Gateway

Configuration Path	[Ethernet LAN]-[Configuration] ([Basic Network]-[LAN&VLAN])
LAN IP Address	*10.0.75.1*
Subnet Mask	*255.255.255.0 (/24)*

Configuration Path	[VRRP]-[Configuration]
VRRP	■ *Enable*
Virtual Server ID	*253*
Priority of Virtual Server	*254*
Virtual Server IP Address	*10.0.75.200*

- Backup Gateway

Configuration Path	[Ethernet LAN]-[Configuration] ([Basic Network]-[LAN&VLAN])
LAN IP Address	*10.0.75.2*
Subnet Mask	*255.255.255.0 (/24)*

Configuration Path	[VRRP]-[Configuration]
VRRP	■ *Enable*
Virtual Server ID	*253*
Priority of Virtual Server	*253*
Virtual Server IP Address	*10.0.75.200*

Scenario Operation Procedure

In above diagram, the Master Gateway and the Backup Gateway are the redundant gateway group of Network-A and the subnet of its Intranet is 10.0.75.0/24. The master gateway has the IP address of 10.0.75.1 for LAN interface, 203.95.80.22 for WAN-1 interface. However, the backup gateway has the IP address of 10.0.75.2 for LAN interface, 118.18.81.33 for WAN-1 interface. They both serve as NAT routers.

Specify the ID of VRRP virtual server to be "253" and its IP address to be "10.0.75.200". The priority of the master gateway is 254 and it is larger than the one (253) of the backup gateway.

At first stage, all data from the Intranet go through the master gateway that has the highest priority.

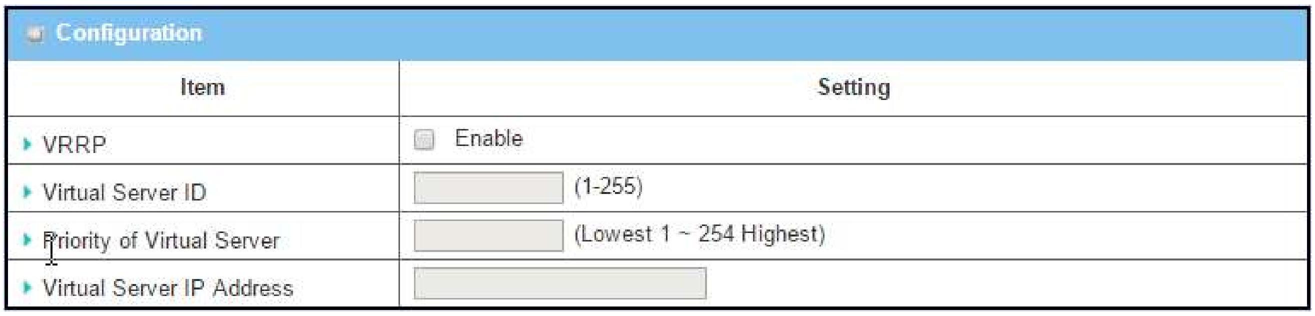
Once the master Internet connection is broken, the backup gateway will take over the data transmitting job and serve as the master gateway.

When a gateway with higher priority than current master gateway recovers from its broken Internet connection, it will be in charge of the data transmitting again.

VRRP Setting

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

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

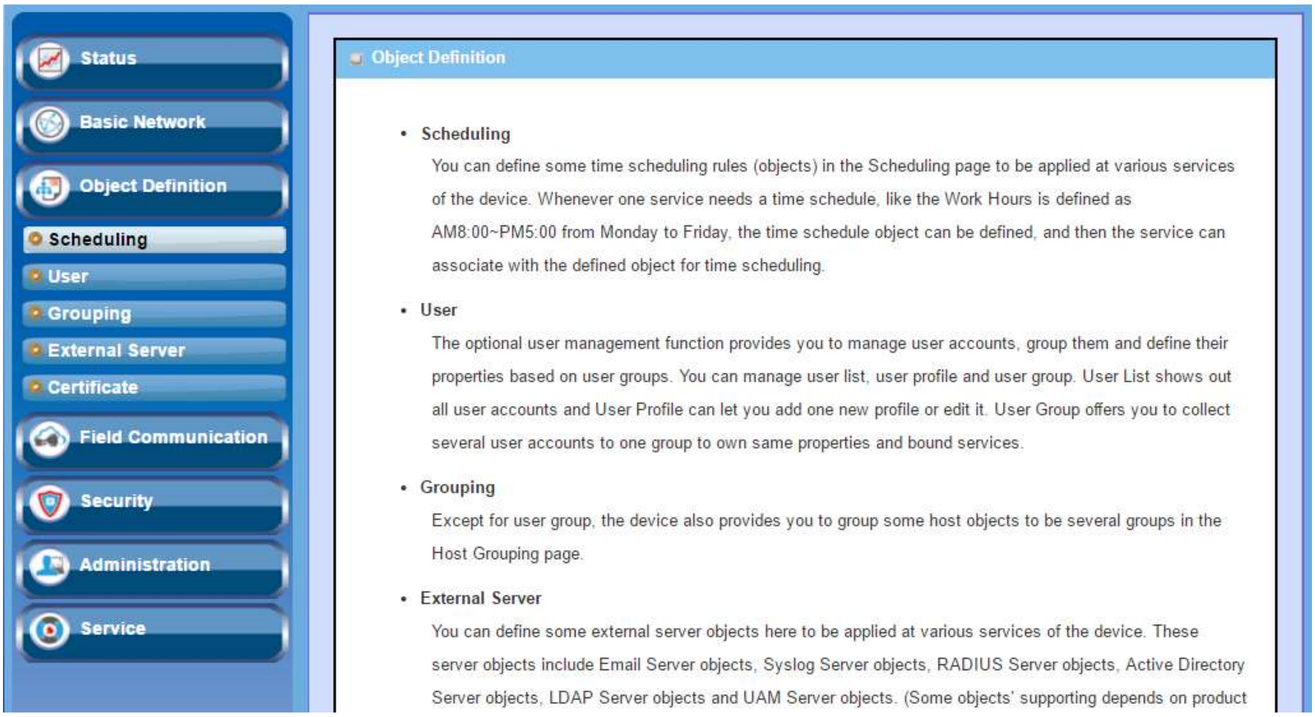


Configuration

Item	Setting
VRRP	□ Enable
Virtual Server ID	(1-255)
Priority of Virtual Server	(Lowest 1 ~ 254 Highest)
Virtual Server IP Address	

VRRP Item	Value setting	Description
VRRP	The box is unchecked by default.	Check the **Enable** box to activate this VRRP function.
Virtual Server ID	1. Numberic String Format 2. A Must filled setting	Specify the Virtual Server ID on VRRP of the gateway. The value range is from 1 to 255.
Priority of Virtual Server	1. Numberic String Format 2. A Must filled setting	Specify the Priority of Virtual Server on VRRP of the gateway. The value range is from 1 to 254.
Virtual Server IP Address	1. IPv4 Format 2. A Must filled setting	Specify the Virtual Server IP Address on VRRP of the gateway.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.

Chapter 5 Object Definition



Object Definition

- Scheduling

  You can define some time scheduling rules (objects) in the Scheduling page to be applied at various services of the device. Whenever one service needs a time schedule, like the Work Hours is defined as AM8:00~PM5:00 from Monday to Friday, the time schedule object can be defined, and then the service can associate with the defined object for time scheduling.

- User

  The optional user management function provides you to manage user accounts, group them and define their properties based on user groups. You can manage user list, user profile and user group. User List shows out all user accounts and User Profile can let you add one new profile or edit it. User Group offers you to collect several user accounts to one group to own same properties and bound services.

- Grouping

  Except for user group, the device also provides you to group some host objects to be several groups in the Host Grouping page.

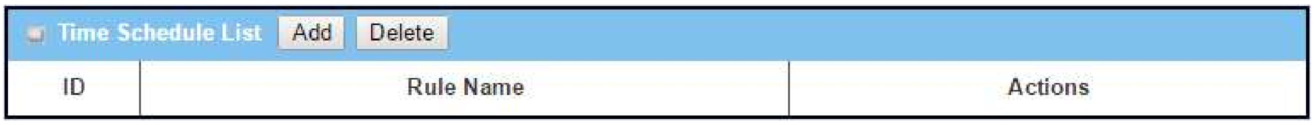
- External Server

  You can define some external server objects here to be applied at various services of the device. These server objects include Email Server objects, Syslog Server objects, RADIUS Server objects, Active Directory Server objects, LDAP Server objects and UAM Server objects. (Some objects' supporting depends on product

5.1 Scheduling

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

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

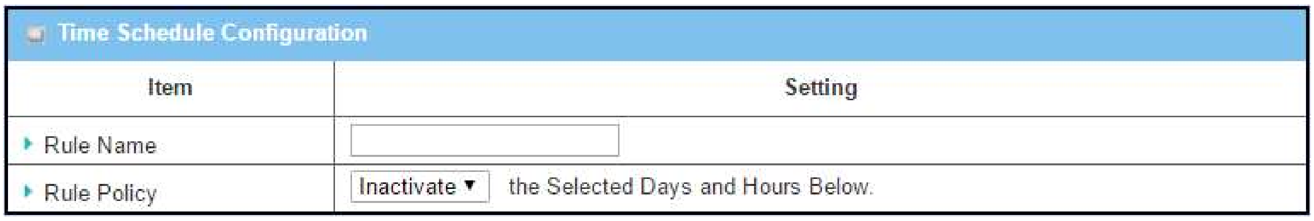


Time Schedule List

ID	Rule Name	Actions

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

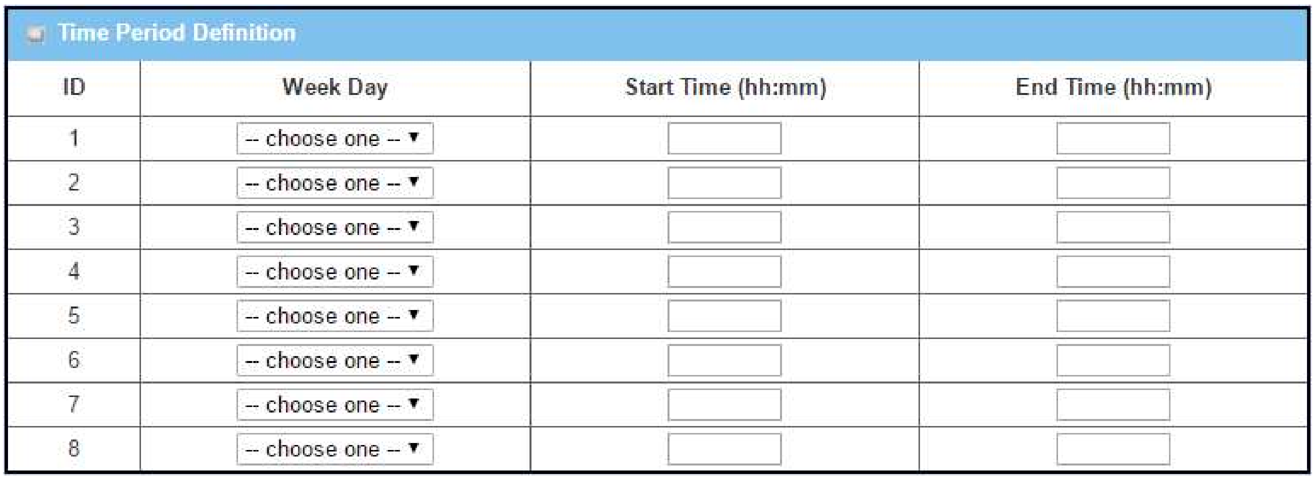
When Add button is applied, Time Schedule Configuration and Time Period Definition screen will appear.



Time Schedule Configuration

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

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



Time Period Definition

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

Time Period Definition		
Item	**Value Setting**	**Description**
Week Day	Select from menu	Select everyday or one of weekday
Start Time	Time format (hh :mm)	Start time in selected weekday
End Time	Time format (hh :mm)	End time in selected weekday

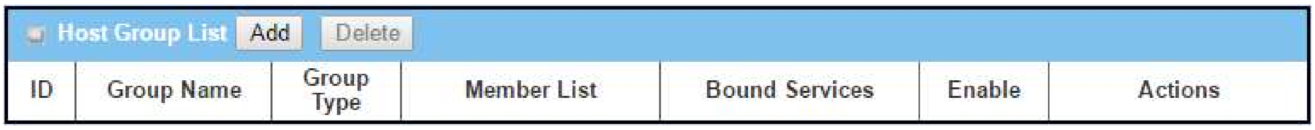
5.5 Grouping

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

5.5.1 Host Grouping

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

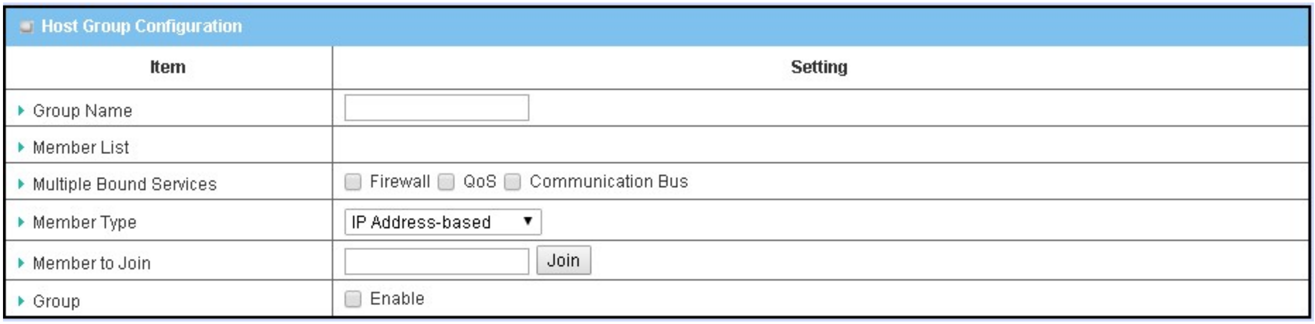
The Host Grouping function allows user to make host group for some services, such as QoS, Firewall, and Communication Bus. The supported service types could be different for the purchased product.



Host Group List Add Delete

ID	Group Name	Group Type	Member List	Bound Services	Enable	Actions

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



Host Group Configuration

Item	Setting
Group Name	
Member List	
Multiple Bound Services	□ Firewall □ QoS □ Communication Bus
Member Type	IP Address-based ▾
Member to Join	Join
Group	□ Enable

Host Group Configuration		
Item	**Value setting**	**Description**
Group Name	1. String format can be any text 2. A Must filled setting	Enter a group name for the rule.It is a name that is easy for you to understand.
Member List	NA	This field will indicate the hosts (members) contained in the group.
Multiple Bound Services	The boxes are unchecked by default	Binding the services that the host group can be applied. If you enable the **Firewall**, the produced group can be used in firewall service. Same as by enable **Qos** and **Communication Bus**.

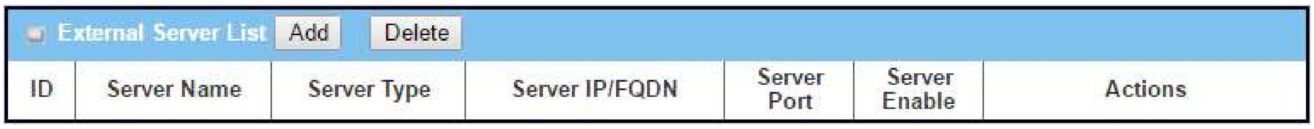
		Note: The supported service type can be different for the purchased product.
Member Type	1. **IP Address-based** is selected by default. 2. A Must filled setting	Select the member type for the host group. It can be **IP Address-based**, **MAC Address-based**, or **Host Namve-based**. When **IP Address-based** is selected, only IP address can be added in **Member to Join.** When **MAC Address-based** is selected, only MAC address can be added in **Member to Join.** When **Host Name-based** is selected, only host name can be added in **Member to Join.**
Member to Join	N/A	Add the members to the group in this field. You can enter the member information as specified in the Member Type above, and press the **Join** button to add. Only one member can be add at a time, so you have to add the members to the group one by one.
Group	The box is unchecked by default	Check the **Enable** checkbox to activate the host group rule. So that the group can be bound to selected service(s) for further configuration.

5.7 External Server

The External Server setting allows user to add external server.

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

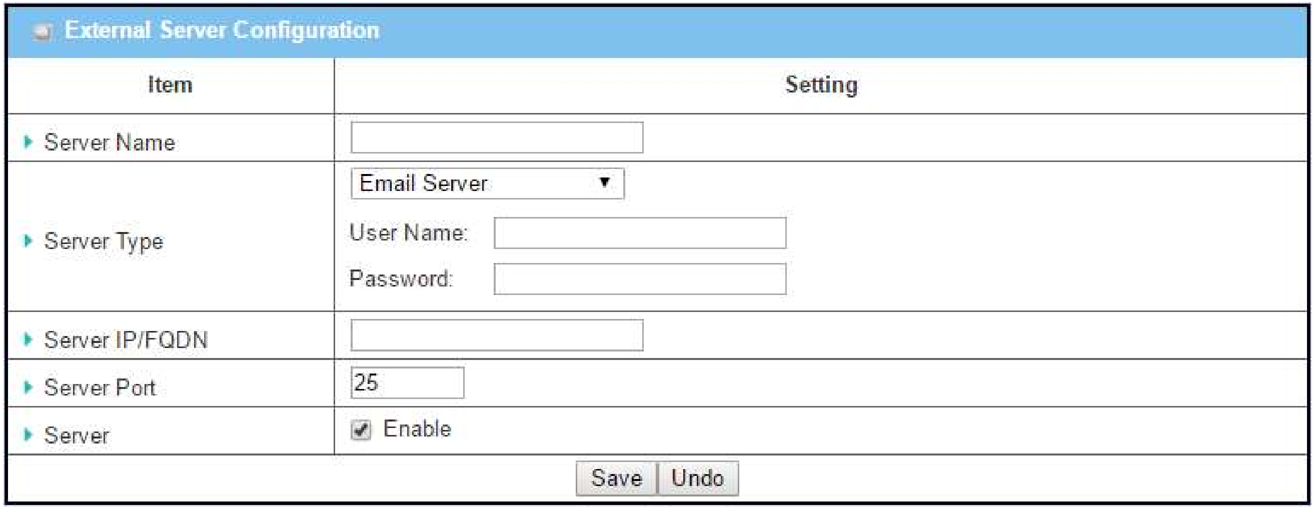
Create external server



External Server List Add Delete

ID	Server Name	Server Type	Server IP/FQDN	Server Port	Server Enable	Actions

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



External Server Configuration

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 server name. Enter a name that is easy for you to understand..
Server IP/FQDN	A Must filled setting	This field is to specify the external server IP.
Server Port	A Must filled setting	This field is to specify the external server port.
Server Type	A Must filled setting	Specify the Server Type of the external server, and enter the required settings for the accessing the server.
		Email Server (A Must filled setting) : When **Email Server** is selected, **User Name**, and **Password** are also required. **User Name** (String format: any text) **Password** (String format: any text)
		RADIUS Server (A Must filled setting) : When **RADIUS Server** is selected, the following settings are also required. **Accounting Port** (A Must filled setting) Primary : **Shared Key** (String format: any text) Authentication Protocol (By default CHAP is selected) Session Timeout (By default **1**) The values must be between 1 and 60. Idle Timeout: (By default 1) The values must be between 1 and 26. Secondary : **Shared Key** (String format: any text) Authentication Protocol (By default CHAP is selected) Session Timeout (By default **1**) The values must be between 1 and 60. Idle Timeout: (By default 1) The values must be between 1 and 26.
		Active Directory Server (A Must filled setting) : When **Active Directory Server** is selected, **Domain** setting is also required. **Domain** (String format: any text)
		LDAP Server (A Must filled setting) : When **LDAP Server** is selected, the following settings are also required. **Base DN** (String format: any text) **Identity** (String format: any text) **Password** (String format: any text)
		UAM Server (A Must filled setting) :

		When **UAM Server** is selected, the following settings are also required. **Login URL** (String format: any text) **Shared Secret** (String format: any text) **N/AS/Gateway ID** (String format: any text) **Location ID** (String format: any text) **Location Name** (String format: any text)
		TACACS+ Server (A Must filled setting) : When **TACACS+ Server** is selected, the following settings are also required. **Shared Key** (String format: any text) **Session Timeout** (String format: any number) The values must be between 1 and 60.
		SCEP Server (A Must filled setting) : When **SCEP Server** is selected, the following settings are also required. **Path** (String format: any text, By default **cgi-bin** is filled) **Application** (String format: any text, By default **pkiclient.exe** is filled)
Server IP/FQDN	A Must filled setting	Specify the IP address or FQDN used for the external server.
Server Port	A Must filled setting	Specify the Port used for the external server. If you selected a certain server type, the default server port number will be set. For **Email Server** 25 will be set by default; For **Syslog Server**, port 514 will be set by default; For **RADIUS Server**, port 1812 will be set by default; For **Active Directory Server**, port 389 will be set by default; For **LDAP Server**, port 389 will be set by default; For **UAM Server**, port 80 will be set by default; For **TACACS+ Server**, port 49 will be set by default; For **SCEP Server**, port 80 will be set by default;
Server	The box is checked by default	Click **Enable to** activate this External Server.
Save	N/A	Click the **Save button** to save the settings
Undo	N/A	Click the **Undo** button to cancel the settings
Refresh	N/A	Click the **Refresh** button to refresh the external server list.

5.9 Certificate

In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are genuine. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner[11].

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

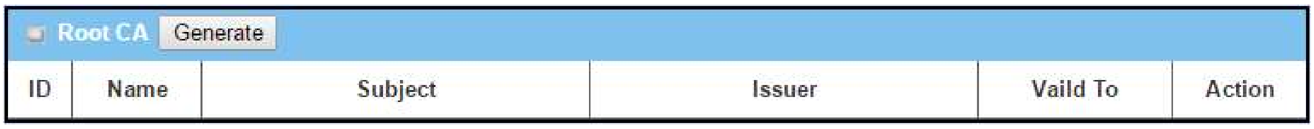
Certificates are an important component of Transport Layer Security (TLS, sometimes called by its older name SSL), where they prevent an attacker from impersonating a secure website or other server. They are also used in other important applications, such as email encryption and code signing. Here, it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

5.9.1 Configuration

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

Go to Object Definition > Certificate > Configuration tab.

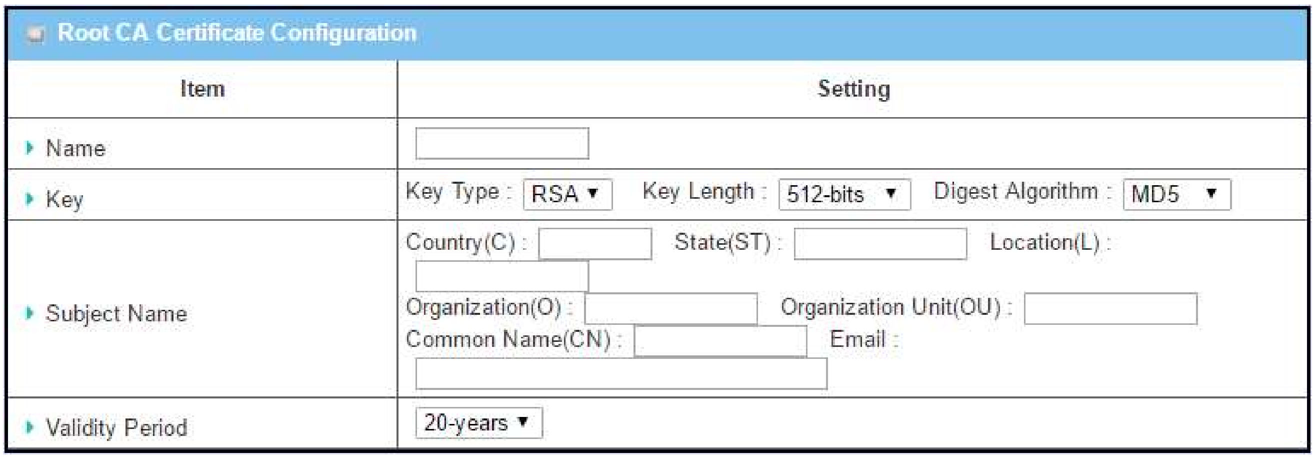
Create root CA



ID	Name	Subject	Issuer	Vaild To	Action

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

[11] http://en.wikipedia.org/wiki/Public_key_certificate.



Root CA Certificate Configuration

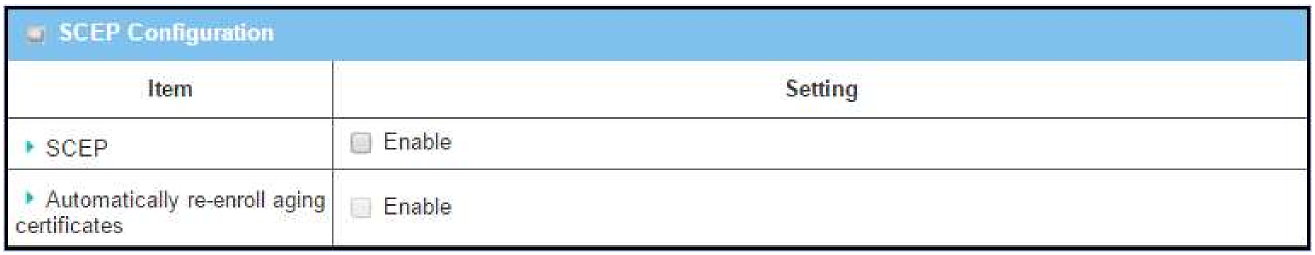
Item	Setting
Name	
Key	Key Type : RSA ▾ Key Length : 512-bits ▾ Digest Algorithm : MD5 ▾

Subject Name	Country(C) : State(ST) : Location(L) :
	Organization(O) : Organization Unit(OU) :
	Common Name(CN) : Email :

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

Setup SCEP



SCEP Configuration

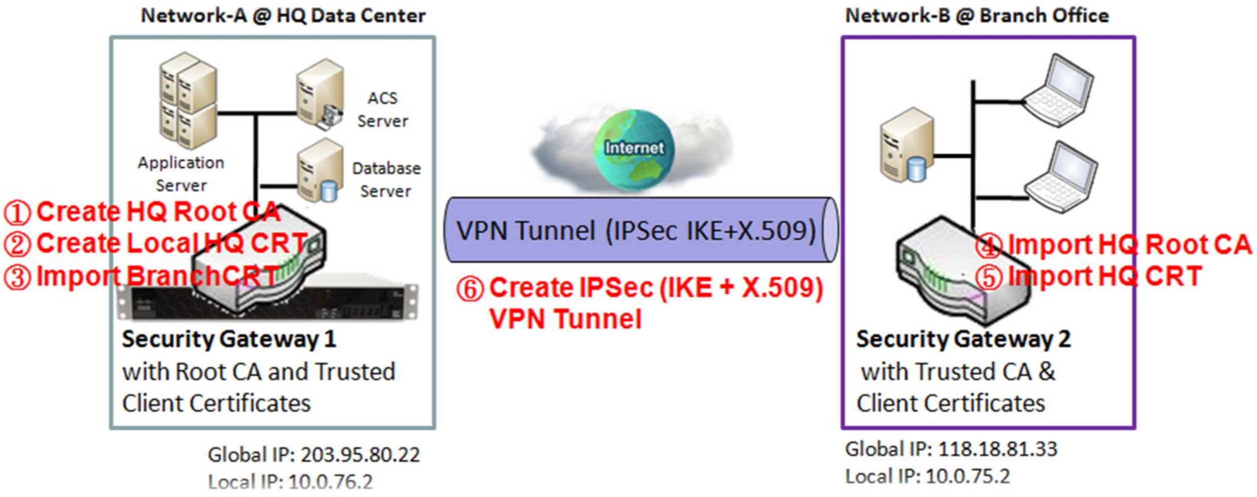
Item	Setting
SCEP	□ Enable
Automatically re-enroll aging certificates	□ Enable

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

5.9.3 My Certificate

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

Self-signed Certificate Usage Scenario



Scenario Application Timing

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

Scenario Description

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

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

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

Parameter Setup Example

For Network-A at HQ

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

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

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

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): AirLive ***HQ*** Organization Unit(OU): ***HQRD*** Common Name(CN): ***HQCRT*** E-mail: ***hqcrt@* AirLive.com**

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	***User Name Network-A***
Remote ID	***User Name Network-B***

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

For Network-B at Branch Office

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

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

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

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	***User Name Network-B***
Remote ID	***User Name Network-A***

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

Scenario Operation Procedure

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

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

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

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

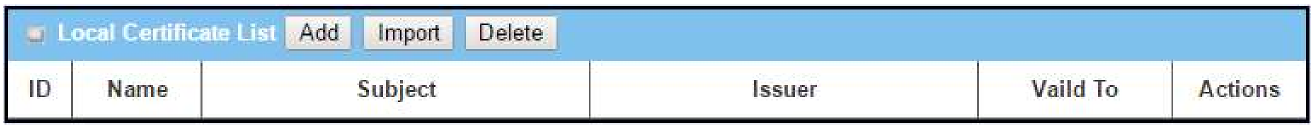
Finally, the client hosts in two subnets of 10.0.75.0/24 and 10.0.76.0/24 can communicate with each other.

My Certificate Setting

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

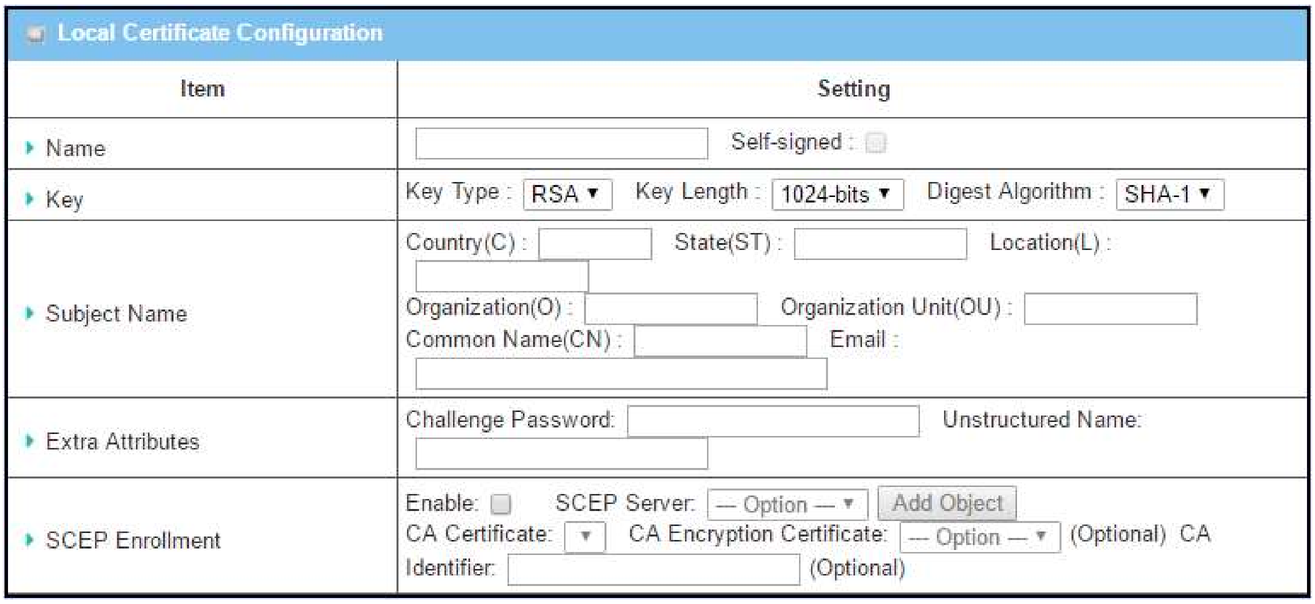
Go to Object Definition > Certificate > My Certificate tab.

Create local certificate



ID	Name	Subject	Issuer	Vaild To	Actions

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



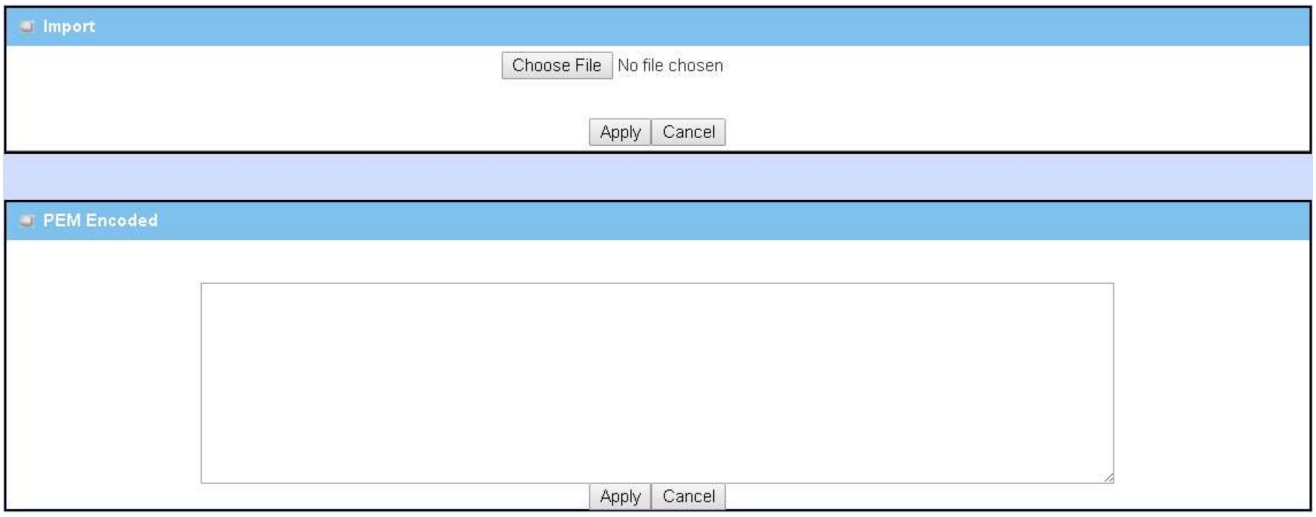
Item	Setting
Name	Self-signed : □
Key	Key Type : RSA ▾ Key Length : 1024-bits ▾ Digest Algorithm : SHA-1 ▾

Subject Name	Country(C) : State(ST) : Location(L) :
	Organization(O) : Organization Unit(OU) :
	Common Name(CN) : Email :

Extra Attributes	Challenge Password: Unstructured Name:
SCEP Enrollment	Enable: □ SCEP Server: -- Option -- ▾ Add Object CA Certificate: ▾ CA Encryption Certificate: -- Option -- ▾ (Optional) CA Identifier: (Optional)

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

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

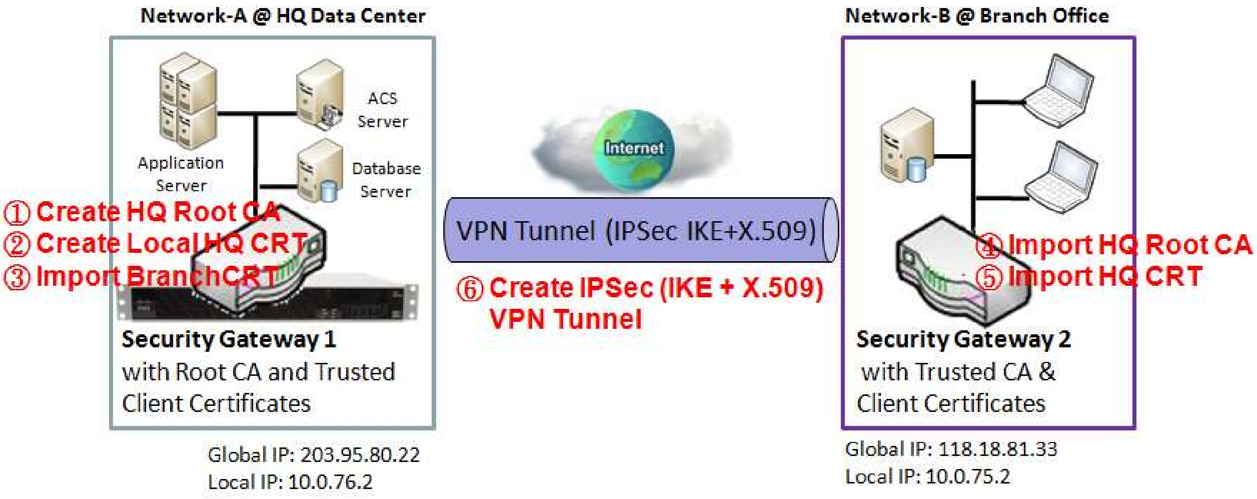


Import Item	Value setting	Description
Import	A Must filled setting	Select a certificate file from user's computer, and click the **Apply** button to import the specified certificate file to the gateway.
PEM Encoded	1. String format can be any text 2. A Must filled setting	This is an alternative approach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

5.9.5 Trusted Certificate

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

Self-signed Certificate Usage Scenario



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

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

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

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

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

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

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

For Network-A at HQ

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

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

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

For Network-B at Branch Office

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

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

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

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

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

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

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

WAN-1 interface. They both serve as the NAT security gateways.

In Gateway 2 import the certificates of the root CA and HQCRT that were generated and signed by Gateway 1 into the "Trusted CA Certificate List" and "Trusted Client Certificate List" of Gateway 2.

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

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

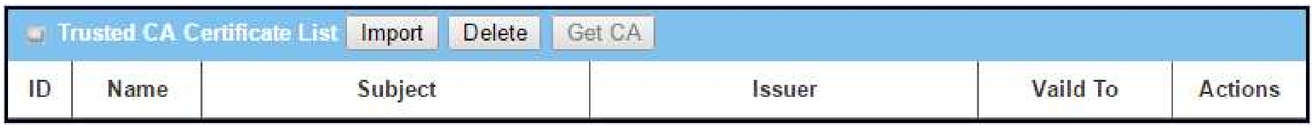
Finally, the client hosts in two subnets of 10.0.75.0/24 and 10.0.76.0/24 can communicate with each other.

Trusted Certificate Setting

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

Go to Object Definition > Certificate > Trusted Certificate tab.

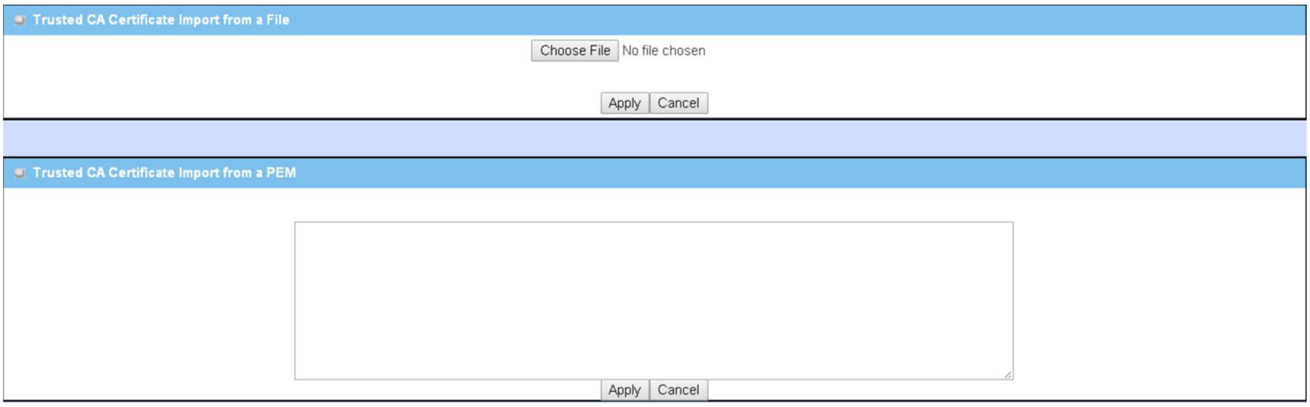
Import Trusted CA Certificate



Trusted CA Certificate List Import Delete Get CA

ID	Name	Subject	Issuer	Vaild To	Actions

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



Trusted CA Certificate Import from a File

Choose File No file chosen

Apply Cancel

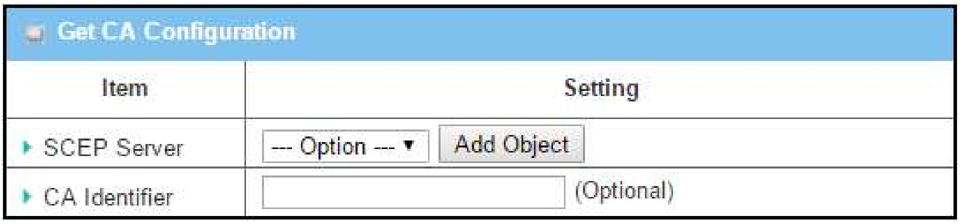
Trusted CA Certificate Import from a PEM

Apply Cancel

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

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

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

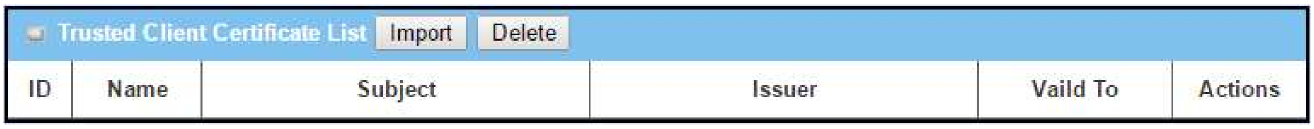


Get CA Configuration

Item	Setting
SCEP Server	--- Option --- ▾ Add Object
CA Identifier	(Optional)

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

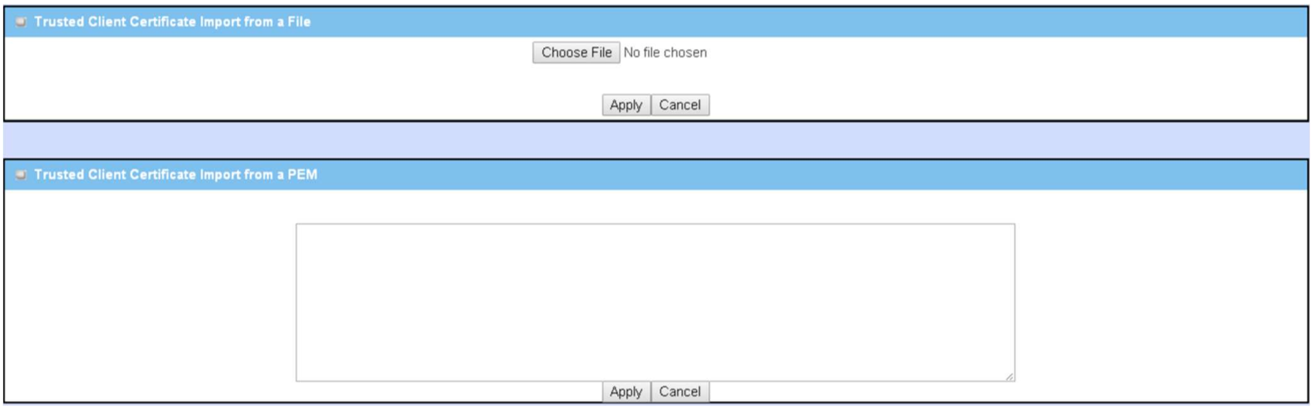
Import Trusted Client Certificate



Trusted Client Certificate List Import Delete

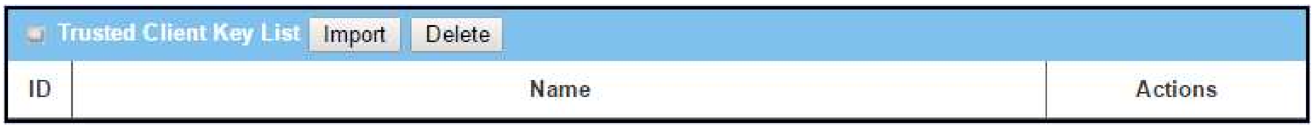
ID	Name	Subject	Issuer	Vaild To	Actions

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

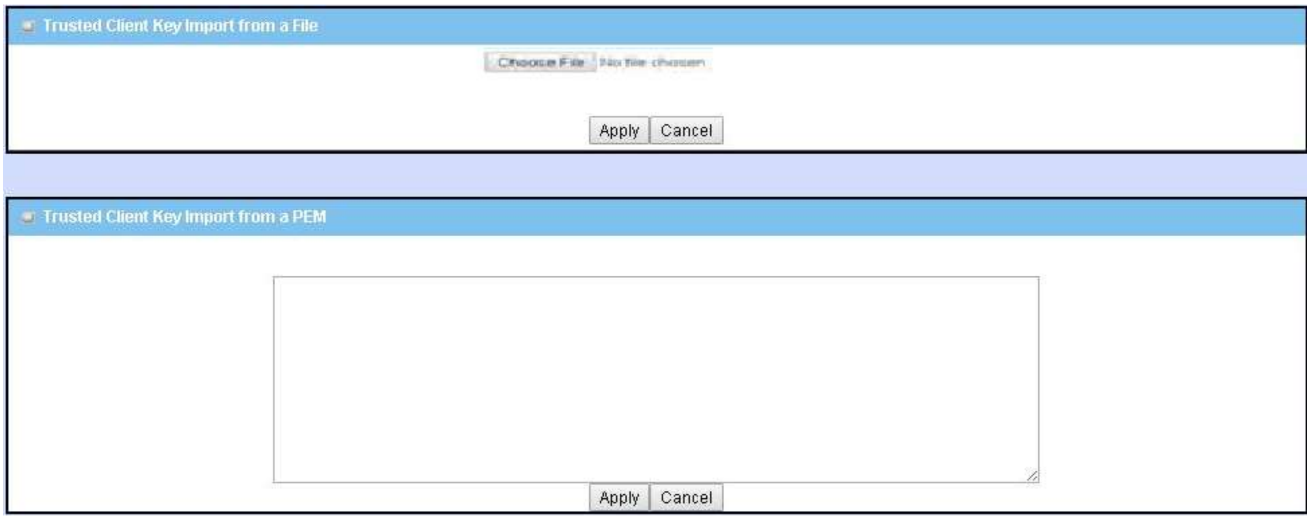

Trusted Client Certificate Import from a File
Choose File
No file chosen
Apply
Cancel
Trusted Client Certificate Import from a PEM
Apply
Cancel

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

Import Trusted Client Key



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


Trusted Client Key Import from a File
Choose File
No file chosen
Apply
Cancel
Trusted Client Key Import from a PEM
Apply
Cancel

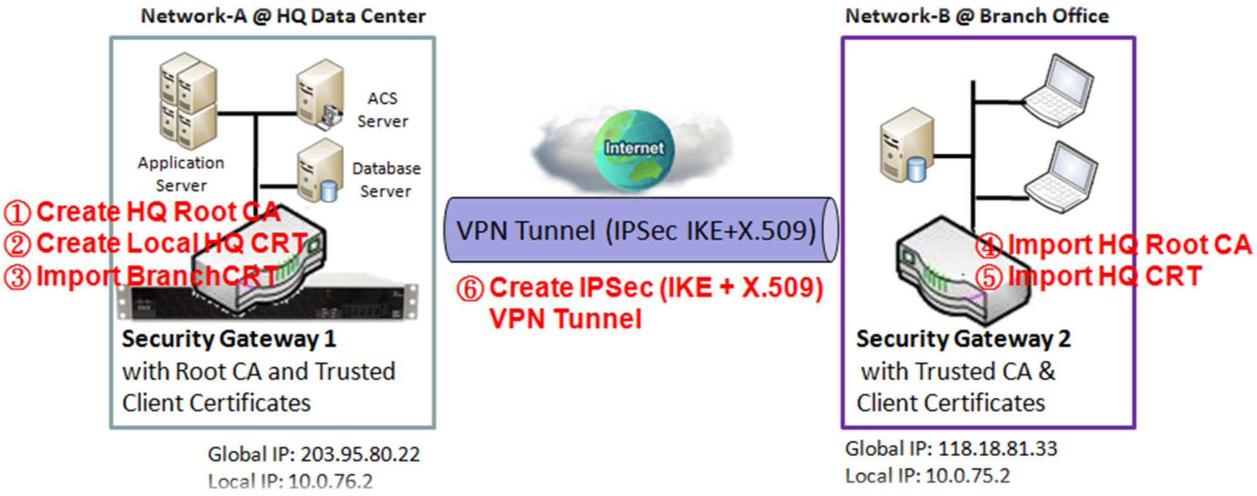
Trusted Client Key List		
Item	**Value setting**	**Description**
Import from a File	A Must filled setting	Select a certificate key file from user's computer, and click the **Apply** button to import the specified key file to the gateway.
Import from a PEM	1. String format can be any text 2. A Must filled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

5.9.7 Issue Certificate

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

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

Self-signed Certificate Usage Scenario



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

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

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

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

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

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

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

For Network-A at HQ

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

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

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

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

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

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

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

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

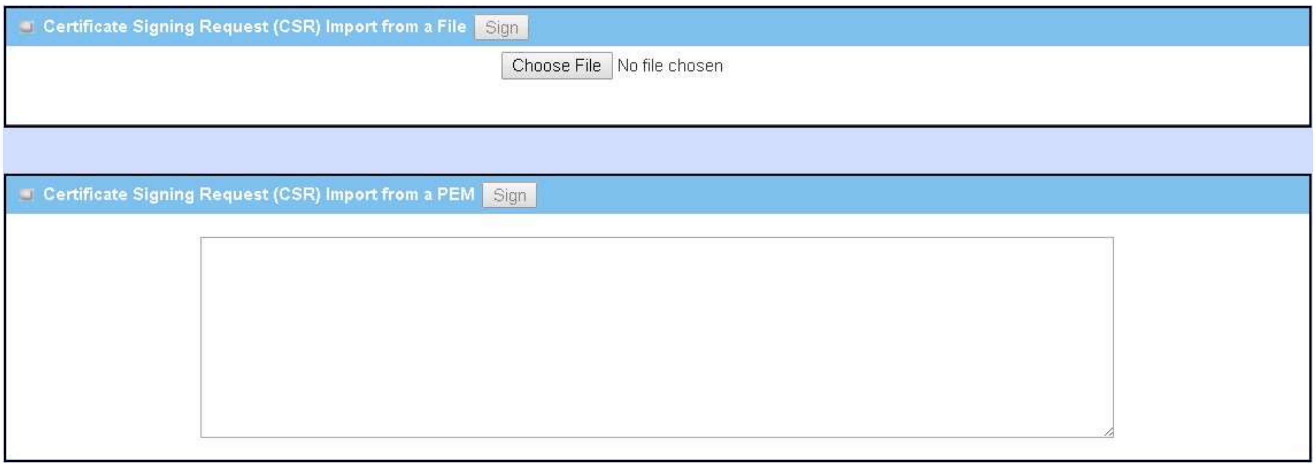
Finally, the client hosts in two subnets of 10.0.75.0/24 and 10.0.76.0/24 can communicate with each other.

Issue Certificate Setting

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

Go to Object Definition > Certificate > Issue Certificate tab.

Import and Issue Certificate


Certificate Signing Request (CSR) Import from a File
Sign
Choose File
No file chosen
Certificate Signing Request (CSR) Import from a PEM
Sign

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

Chapter 7 Field Communication

7.1 Bus & Protocol

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

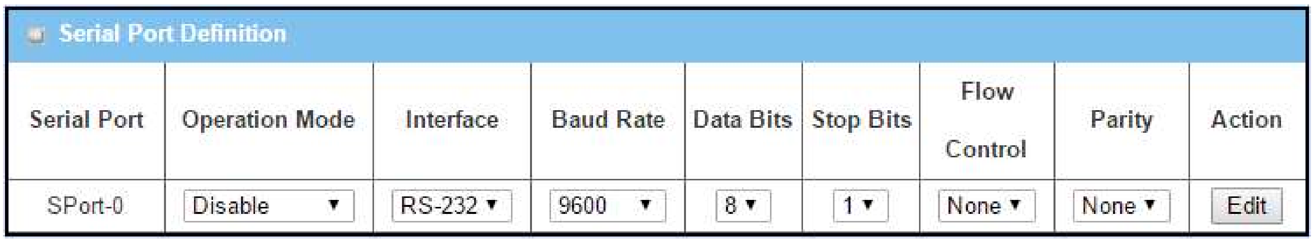
7.1.1 Port Configuration

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

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

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

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



Serial Port Definition

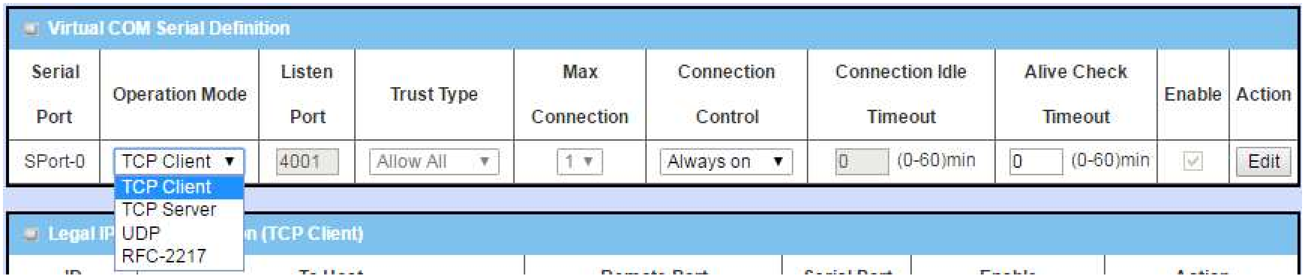
Serial Port	Operation Mode	Interface	Baud Rate	Data Bits	Stop Bits	Flow Control	Parity	Action
SPort-0	Disable ▼	RS-232 ▼	9600 ▼	8 ▼	1 ▼	None ▼	None ▼	Edit

Port Configuration Window		
Item	**Value setting**	**Description**
Serial Port	*N/A*	It displays the serial port ID of the serial port.

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

7.1.3 Virtual COM

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



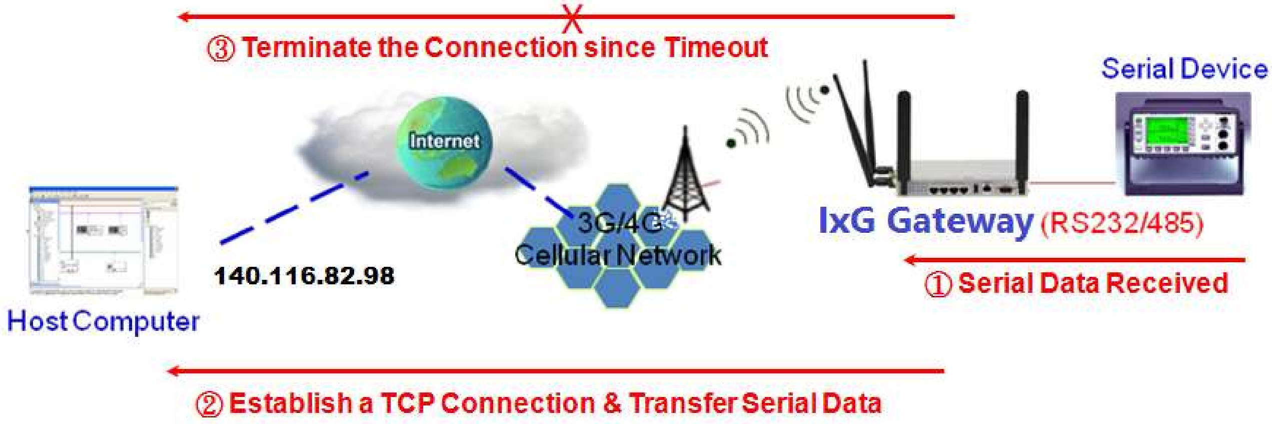
Virtual COM Serial Definition

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

Legal IP n (TCP Client)

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

TCP Client Mode in On-demand Control Scenario



Scenario Application Timing

When the administrator expects the gateway to actively establish a TCP connection to a pre-defined host computer when serial data arrives, the operation mode for the "Virtual COM" function is required to be "TCP Client" and the connection control is required to be "On-demand". Besides, after the data has been transferred, the TCP connection can be automatically disconnected from the host computer by using the TCP alive check timeout or idle timeout settings.

Scenario Description

M2M LTE Gateway with serial port

When the connection control of virtual COM is "On-demand", and once the ~~IOG~~ gateway receives data from the connected serial device, it will establish a TCP connection to transfer the received serial data to the remote host.

After the data has been transferred, the gateway automatically disconnects the established TCP session from the host computer by using the TCP alive check timeout or idle timeout settings.

Finally, the host computer can process the collected serial data and make further decisions.

Parameter Setup Example

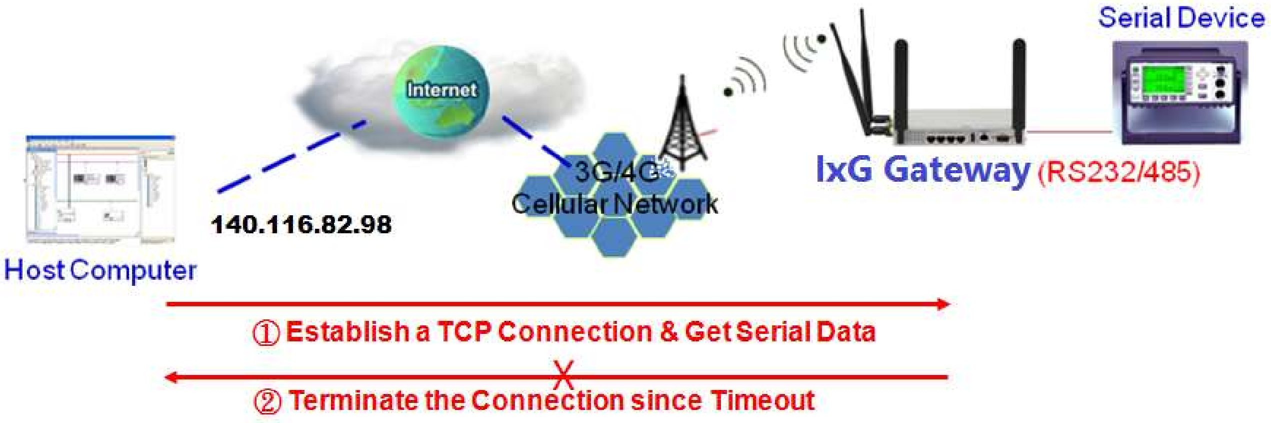
Following tables list the parameter configuration as an example for "TCP Client" mode in "Virtual COM" function, as shown in above diagram.

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

Configuration Path	[Virtual COM]-[Virtual COM Serial Definition]
Operation Mode	***TCP Client***
Connection Control	***On-demand***
Connection Idle Timeout	***1*** (0-60) min
Alive Check Timeout	***1*** (0-60) min

Configuration Path	[Virtual COM]-[Legal IP/FQDN Definition (TCP Client)]
ID	1
To Host	***140.116.82.98***
Remote Port	***4001***
Serial Port	***SPort-0***
Definition	■ ***Enable***

TCP Server Mode



Scenario Application Timing

When the administrator expects the gateway to wait passively for the serial data requests from the host computer, and the host computer will establish a TCP connection to get data from the serial device, the operation mode for the "Virtual COM" function is required to be "TCP Server". In this mode, the gateway provides a unique "IP: Port" address on a TCP/IP network. It supports up to 4 simultaneous connections, so that multiple hosts can collect data from the same serial device at the same time.

Scenario Description

When the Internet Host Computer wants to get the serial data via the gateway, it will try to establish a TCP connection to the gateway if the connection is off.

After the data has been transferred, the TCP connection will be automatically disconnected from the host computer by using the TCP alive check timeout or idle timeout settings.

Finally, the host computer can process the collected serial data and make further decisions.

Parameter Setup Example

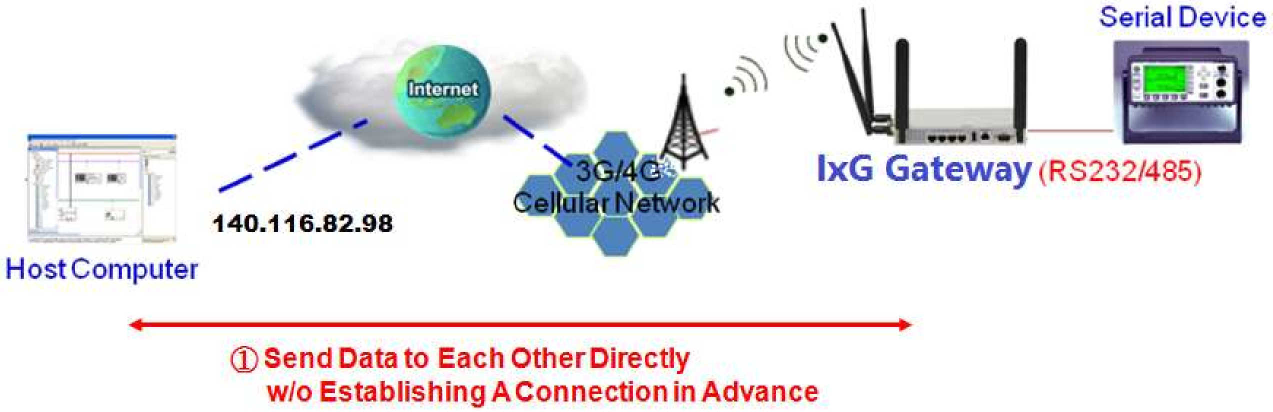
Following tables list the parameter configuration as an example for the "TCP Server" mode in "Virtual COM" function, as shown in above diagram.

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

Configuration Path	[Virtual COM]-[Virtual COM Serial Definition]
Operation Mode	***TCP Server***
Listen Port	***4001***
Trust Type	***Specific IPs***
Max Connection	***4***
Connection Idle Timeout	***1*** (0-60) min
Alive Check Timeout	***1*** (0-60) min

Configuration Path	[Virtual COM]-[Trusted IP Definition]
ID	1
Host	***140.116.82.98***
Serial Port	■ ***Sport-0***
Definition	■ ***Enable***

UDP Mode



Scenario Application Timing

If both the Internet Host Computer and the remote serial device are expected to initiate a data transfer when it require to do that, the operation mode for the "Virtual COM" function in the gateway is required to be "UDP". In this mode, the UDP data can be transferred between the gateway and multiple host computers from either peer, making this mode ideal for message display applications. It supports up to 4 legal host computers to connect to the serial device via the gateway.

Scenario Description

A remote Internet host computer whose IP address is 140.116.82.98 has a management system in it to collect the serial data from or send data to the serial device via the gateway.

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

Parameter Setup Example

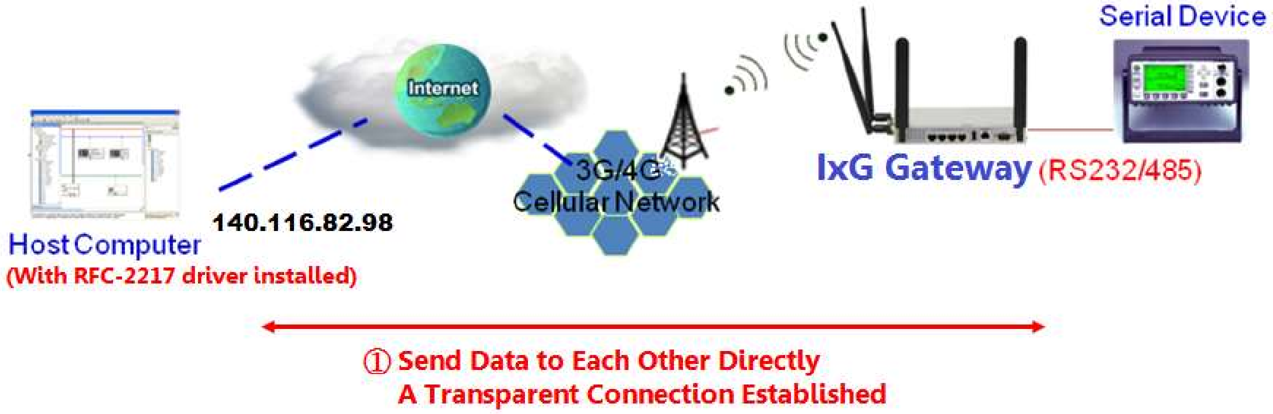
Following tables list the parameter configuration as an example for the "UDP" mode in "Virtual COM" function, as shown in above diagram.

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

Configuration Path	[Virtual COM]-[Virtual COM Serial Definition]
Operation Mode	*UDP*
Listen Port	*4001*

Configuration Path	[Virtual COM]-[Legal IP Definition (UDP)]
ID	1
Host	*140.116.82.98*
Remote Port	*4001*
Serial Port	*Sport-0*
Definition	■ *Enable*

RFC-2217 Mode


Serial Device
Internet
3G/4G
Cellular Network
IxG Gateway (RS232/485)
140.116.82.98
Host Computer
(With RFC-2217 driver installed)
① Send Data to Each Other Directly
A Transparent Connection Established

Scenario Application Timing

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

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

Scenario Description

A remote Internet host computer whose IP address is 140.116.82.98 has a RFC-2217 Virtual COM driver installed in it, and also has some legacy serial application software in it to collect the serial data from or send data to the serial device via the gateway.

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

M2M LTE Gateway with serial port

Parameter Setup Example

Following tables list the parameter configuration as an example for the “RFC-2217" mode in "Virtual COM" function, as shown in above diagram.

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

Configuration Path	[Virtual COM]-[Virtual COM Serial Definition]
Operation Mode	***RFC-2217***
Listen Port	***4001***
Trust Type	***Specific IPs***

Configuration Path	[Virtual COM]-[Trusted IP Definition (RFC-2217)]
ID	1
Host	***140.116.82.98***
Serial Port	***Sport-0***
Enable	■ ***Enable***

Virtual COM Setting

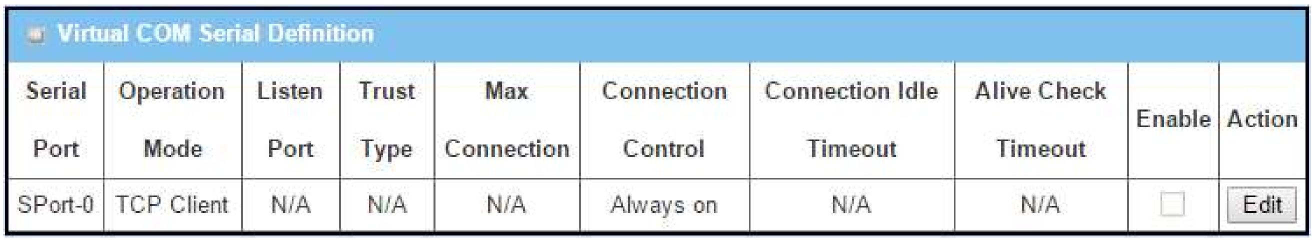
Virtual COM setting screen enables user to connect a Virtual COM port based device to the Internet. It allows user to access serial data remotely. There are TCP Client, TCP Server, UDP, and RFC2217 modes for remote accessing the connected serial device.

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

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

Enable TCP Client Mode

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

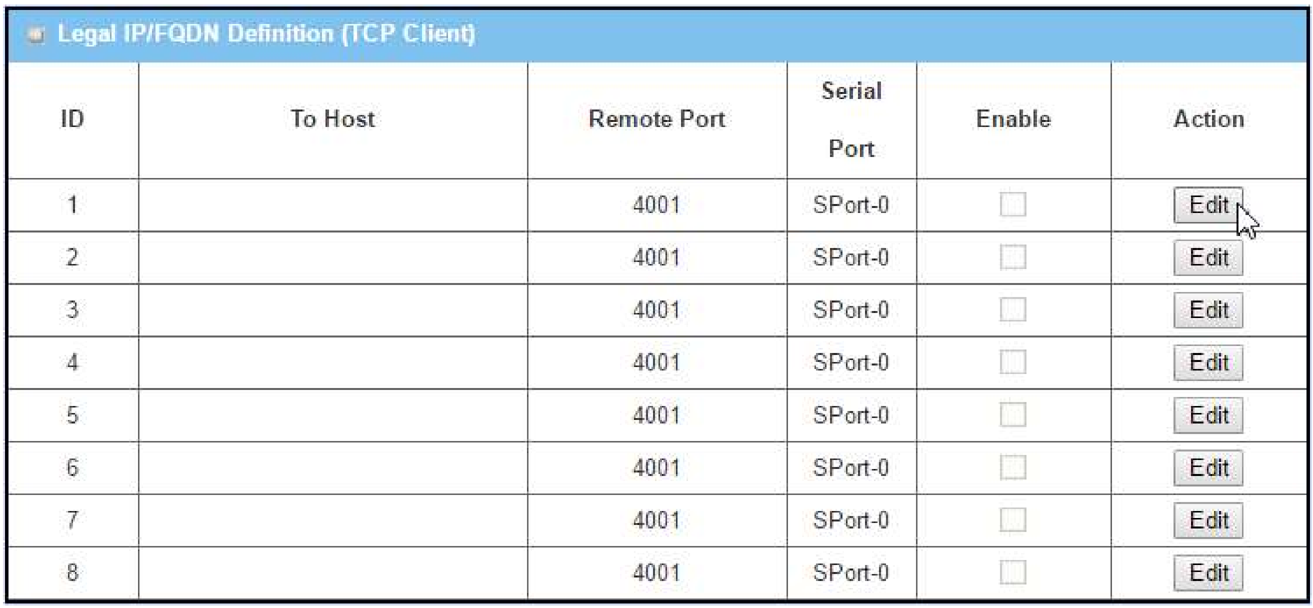


Virtual COM Serial Definition

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

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

Specify Remote TCP Server



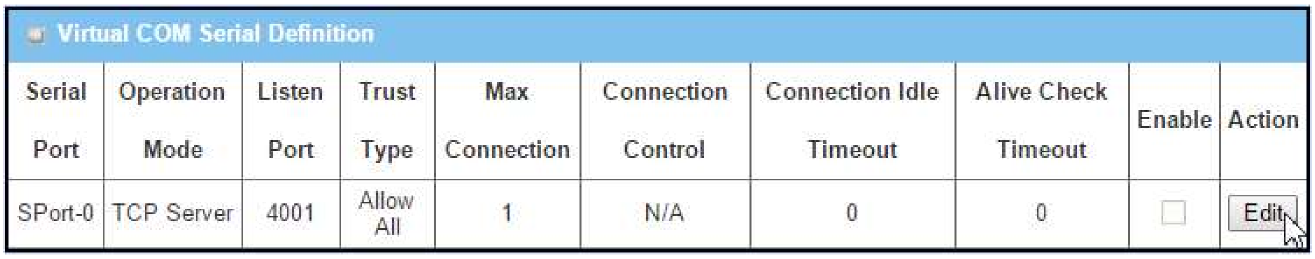
■ Legal IP/FQDN Definition (TCP Client)

ID	To Host	Remote Port	Serial Port	Enable	Action
1		4001	SPort-0	□	Edit
2		4001	SPort-0	□	Edit
3		4001	SPort-0	□	Edit
4		4001	SPort-0	□	Edit
5		4001	SPort-0	□	Edit
6		4001	SPort-0	□	Edit
7		4001	SPort-0	□	Edit
8		4001	SPort-0	□	Edit

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

Enable TCP Server Mode

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

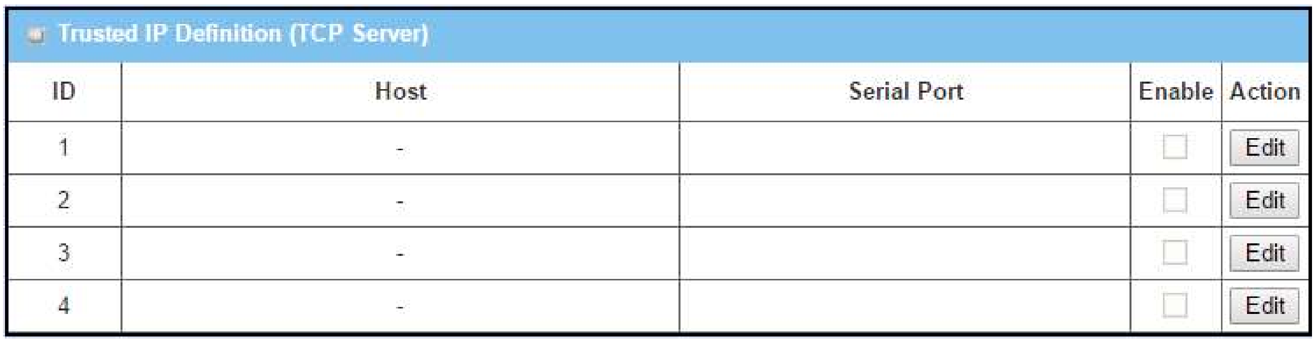


Virtual COM Serial Definition

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

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

Specify TCP Clients for TCP Server Access



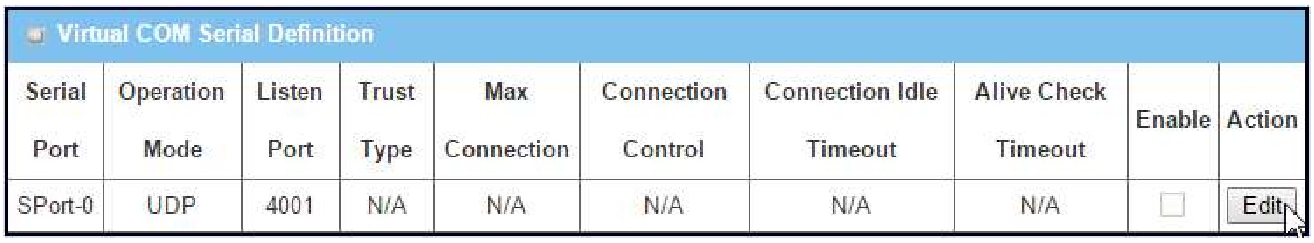
Trusted IP Definition (TCP Server)

ID	Host	Serial Port	Enable	Action
1	-		□	Edit
2	-		□	Edit
3	-		□	Edit
4	-		□	Edit

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

Enable UDP Mode

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

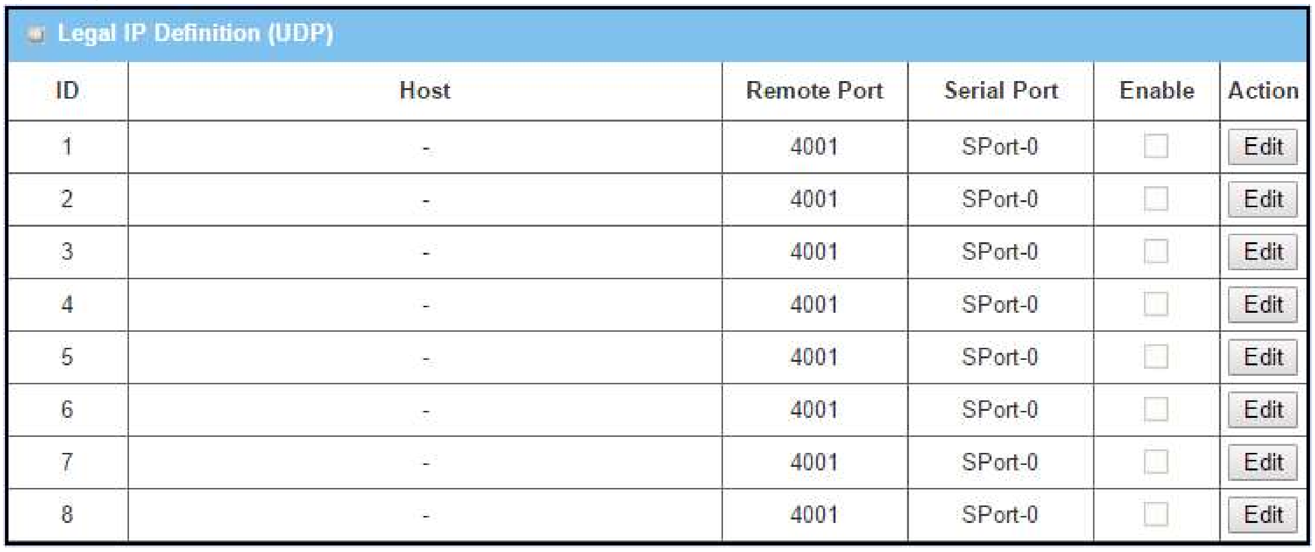


Virtual COM Serial Definition

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

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

Specify Remote UDP



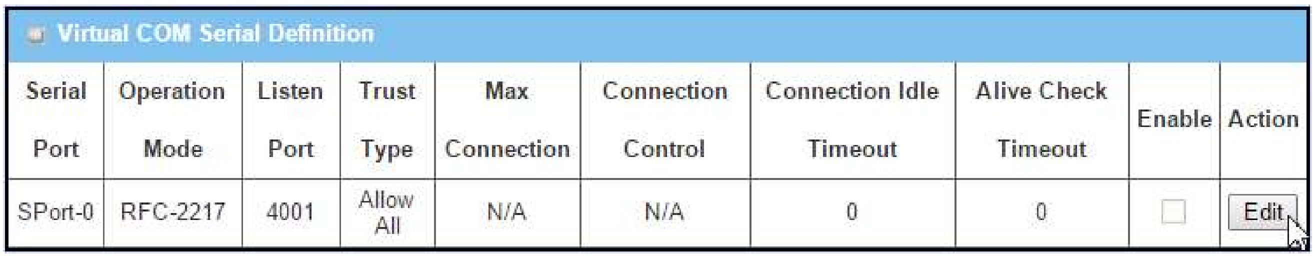
Legal IP Definition (UDP)

ID	Host	Remote Port	Serial Port	Enable	Action
1	-	4001	SPort-0	□	Edit
2	-	4001	SPort-0	□	Edit
3	-	4001	SPort-0	□	Edit
4	-	4001	SPort-0	□	Edit
5	-	4001	SPort-0	□	Edit
6	-	4001	SPort-0	□	Edit
7	-	4001	SPort-0	□	Edit
8	-	4001	SPort-0	□	Edit

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

Enable RFC-2217 Mode

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

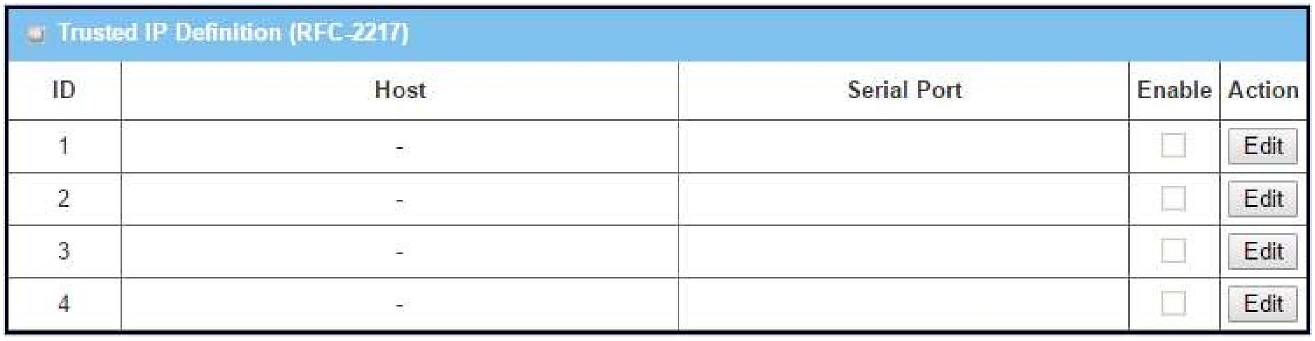


Virtual COM Serial Definition

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

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

Specify Remote Host for Access

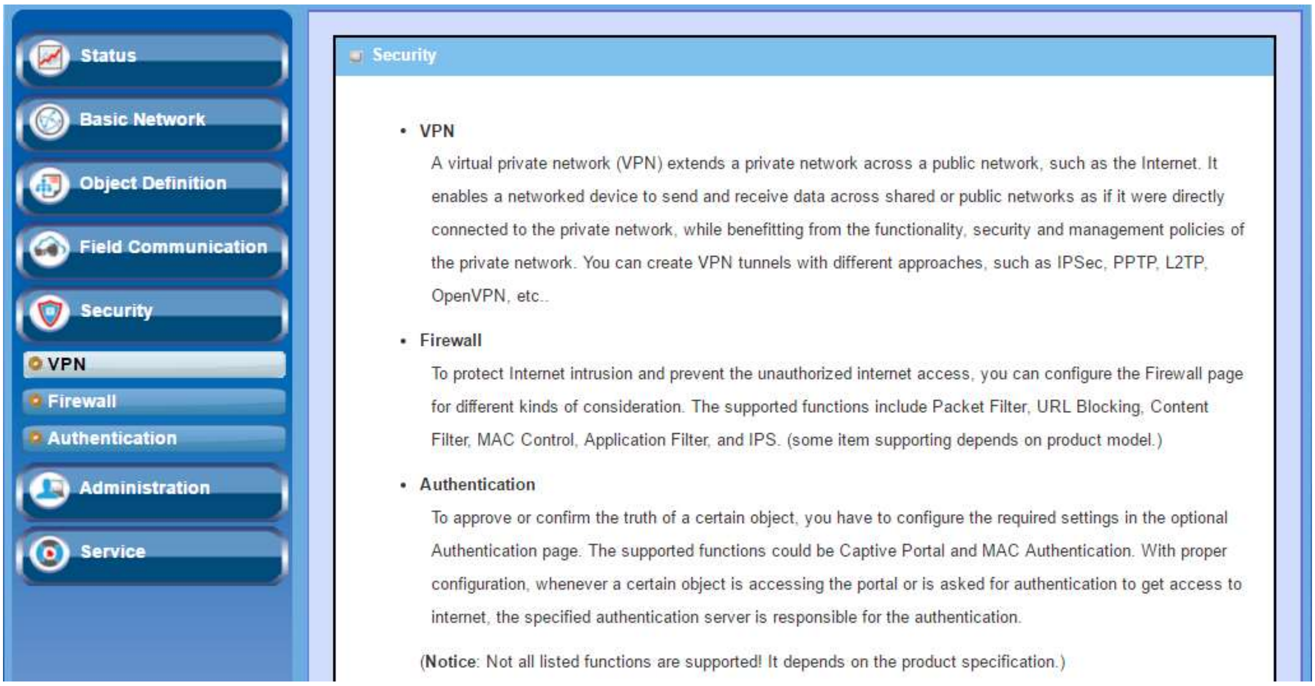


Trusted IP Definition (RFC-2217)

ID	Host	Serial Port	Enable	Action
1	-		□	Edit
2	-		□	Edit
3	-		□	Edit
4	-		□	Edit

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

Chapter 9 Security



- VPN

  A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a networked device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network. You can create VPN tunnels with different approaches, such as IPSec, PPTP, L2TP, OpenVPN, etc..

- Firewall

  To protect Internet intrusion and prevent the unauthorized internet access, you can configure the Firewall page for different kinds of consideration. The supported functions include Packet Filter, URL Blocking, Content Filter, MAC Control, Application Filter, and IPS. (some item supporting depends on product model.)

- Authentication

  To approve or confirm the truth of a certain object, you have to configure the required settings in the optional Authentication page. The supported functions could be Captive Portal and MAC Authentication. With proper configuration, whenever a certain object is accessing the portal or is asked for authentication to get access to internet, the specified authentication server is responsible for the authentication.

(**Notice**: Not all listed functions are supported! It depends on the product specification.)

9.1 VPN

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The tunnel technology supports data confidentiality, data origin authentication and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

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

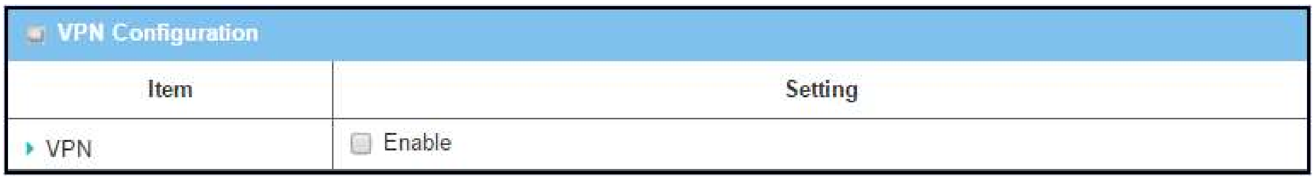
9.1.1 Configuration

The VPN configuration allows user to enable or disable all the VPN functions of the gateway device. The VPN enables check box must be checked to enable to allow IPSec, PPTP, L2TP and GRE to function.

Go to **Security > VPN > Configuration** tab

VPN Configuration

Enable VPN check box will activate all VPN related functions.



VPN Configuration

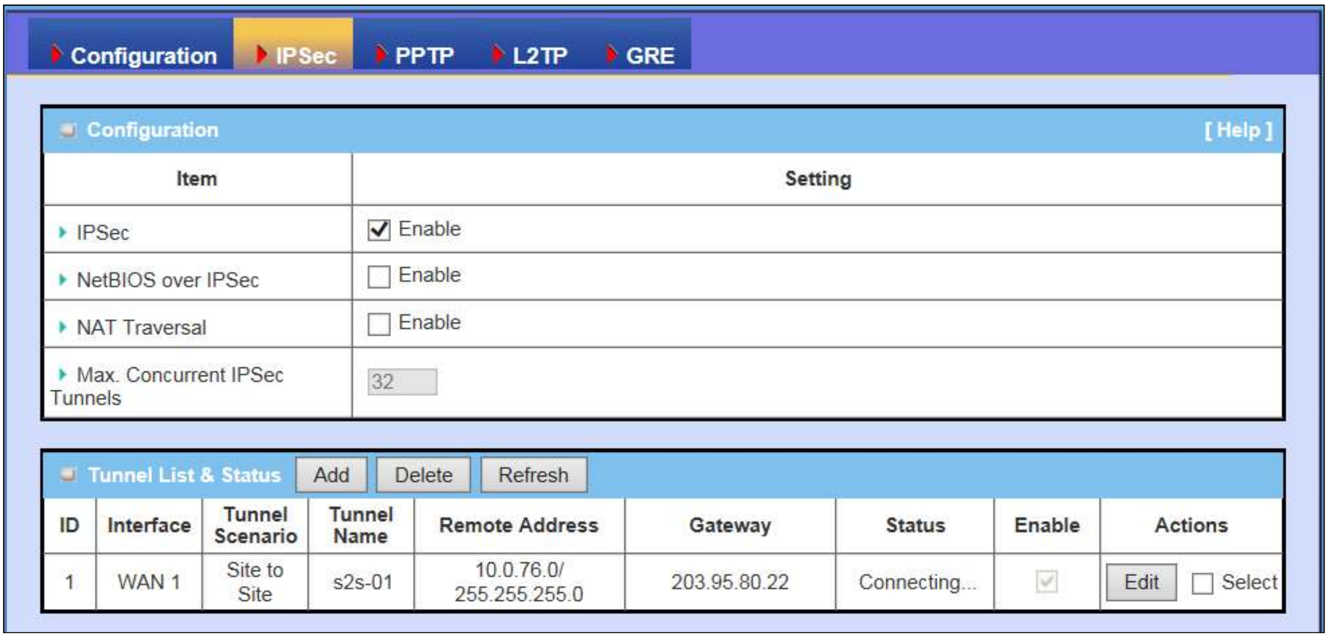
Item	Setting
VPN	□ Enable

VPN Configuration		
Item	**Value setting**	**Description**
VPN	The box is unchecked by default	Check the **Enable** box to enable all VPN functions
Save	N/A	Click the **Save** button to save the settings

9.1.3 IPSec

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

An IPSec VPN tunnel is established between IPSec client and server. Sometimes, we call the IPSec VPN client as the initiator and the IPSec VPN server as the responder. There are two phases to negotiate between the initiator and responder during tunnel establishment, IKE phase and IPSec phase. At IKE phase, IKE authenticates IPSec peers and negotiates IKE SAs (Security Association) to set up a secure channel for negotiating IPSec SAs in phase 2. At IPSec phase, IKE negotiates IPSec SA parameters and sets up matching IPSec SAs in the peers. After these both phases, data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.



Configuration [Help]

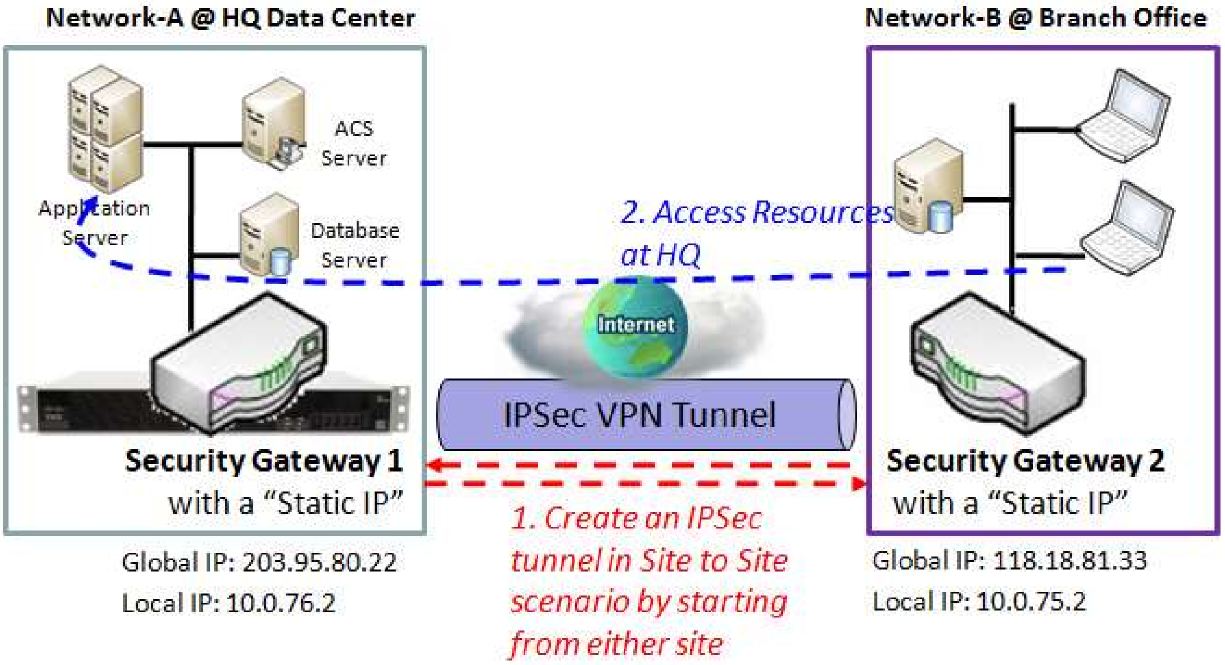
Item	Setting
IPSec	☑ Enable
NetBIOS over IPSec	□ Enable
NAT Traversal	□ Enable
Max. Concurrent IPSec Tunnels	32

Tunnel List & Status Add Delete Refresh

ID	Interface	Tunnel Scenario	Tunnel Name	Remote Address	Gateway	Status	Enable	Actions
1	WAN 1	Site to Site	s2s-01	10.0.76.0/ 255.255.255.0	203.95.80.22	Connecting...	☑	Edit □ Select

Before going to setup the VPN connections, you may need to decide the scenario type for the tunneling. The scenario can be "Site to Site", "Site to Host", "Host to Site", "Host to Host", or "Dynamic VPN". There are three commonly used IPSec VPN connection scenarios as follows.

Site to Site Tunnel Scenario


Network-A @ HQ Data Center
Network-B @ Branch Office
Application Server
ACS Server
Database Server
2. Access Resources at HQ
Internet
IPSec VPN Tunnel
Security Gateway 1 with a "Static IP"
Security Gateway 2 with a "Static IP"
1. Create an IPSec tunnel in Site to Site scenario by starting from either site
Global IP: 203.95.80.22
Local IP: 10.0.76.2
Global IP: 118.18.81.33
Local IP: 10.0.75.2

Scenario Application Timing

The security gateway can be located at branch office or mobile office. When the client hosts behind the security gateway want to make a secure communication with the ones behind another security gateway in headquarters or another branch office, both security gateways need to establish a VPN tunnel first. Both Intranets of security gateways have their own subnet and the "Site to Site" tunnel scenario is used. "Site" means a subnet of client hosts.

Scenario Description

Both Initiator and Responder of IPSec tunnel must have a "Static IP" or a "FQDN" for "Site to Site" scenario.

Any peer gateway can be worked as an Initiator or a Responder of the IPSec VPN tunnel.

Two phases (IKE and IPSec) to negotiate for establishing an IPSec VPN tunnel with pre-shared key and optional X-Auth account / password.

Parameter Setup Example

For Network-A at HQ

Following 5 tables list the parameter configuration for above example diagram of IPSec VPN tunnel in Network-A.

Use default value for those parameters that are not mentioned in these 5 tables.

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+Pre-shared Key 12345678***
Local ID	***User Name Network-A***
Remote ID	***User Name Network-B***

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

For Network-B at Branch Office

Following 5 tables list the parameter configuration for above example diagram of IPSec VPN tunnel in Network-B.

Use default value for those parameters that are not mentioned in these 5 tables.

Please also note that the authentication parameters of both peers must match each other to successfully establishing authentication process, and it is just for an example here.

Besides, Negotiation Mode and X-Auth in "IKE Phase" configuration window should be also matched in both peers.

And there is at least one proposal entity in IKE Proposal Definition and at least one proposal entity in IPSec Proposal Definition is same for both peers. Use the default ones in the setup example and they are not shown in followings.

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

Configuration Path	[IPSec]-[Tunnel Configuration]
Tunnel	■ ***Enable***
Tunnel Name	***s2s-201***
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+Pre-shared Key 12345678***
Local ID	***User Name Network-B***
Remote ID	***User Name Network-A***

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

Scenario Operation Procedure

In above diagram, Network-A is in the headquarters, and the subnet of its Intranet is 10.0.76.0/24. The security gateway for Network-A has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN interface.

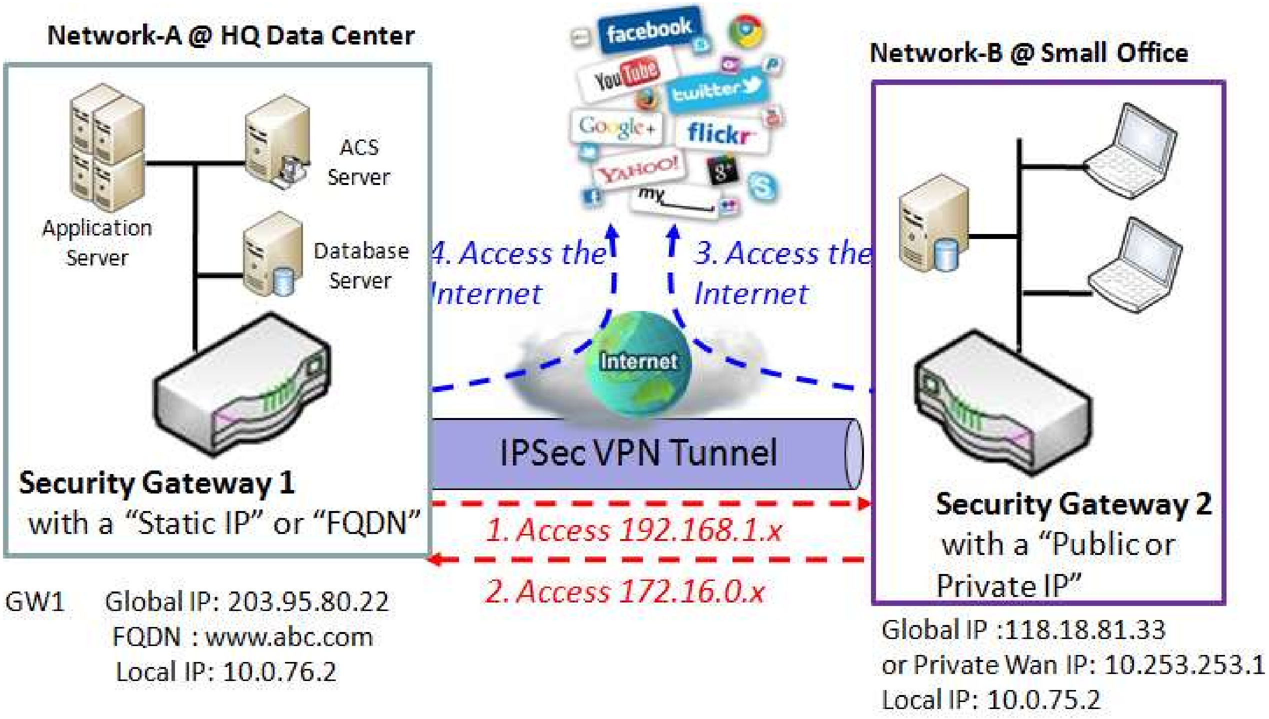
However, Network-B is in the branch office and the subnet of its Intranet is 10.0.75.0/24. The security gateway for Network-B has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN interface.

Establish an IPSec VPN tunnel with "Site to Site" scenario by starting from either site. So both Intranets of 10.0.75.0/24 and 10.0.76.0/24 can securely communicate each other.

Finally, the client hosts in the Intranet of Network-B at branch office can access the server or database resources in the Intranet of Network-A at HQ in a secured link.

Dynamic VPN Tunnel Scenario

Business Security Gateway can ignore IP information of clients when using Dynamic VPN, so it is suitable for users to build VPN tunnels with Business Security Gateway from a remote mobile site. Remote peer is a site will be indicated in the negotiation packets, including what remote subnet is. It must be noted that the remote peer has to initiate the tunnel establishing process first in this application scenario.



Scenario Application Timing

If the security gateway in headquarters wants to allow any traveling employees to securely access the enterprise operation systems to access office resources from outside, the Dynamic VPN connection can be setup up to meet the requirement. These mobile employees are carrying with their notebooks or security supporting gateways outsides, and use these devices to connect to the Internet and try to access the enterprise resources at headquarters. But the IP address that the devices get is dynamic, not fixed. When the security gateway of headquarters need to check the IP address of a remote device during establishing a secure VPN tunnel for data communication, mobile devices will fail since they have not fixed IP address. So, to activate the "Dynamic VPN" function on the headquarters gateway is a fast approach for the secure data communication between mobile devices and the headquarters gateway. You can follow the deployment steps as below.

Scenario Description

Dynamic VPN is suitable for the Initiator being a mobile site or a mobile device with a dynamic IP, only the Responder has a “Static IP” or a “FQDN”.

Two phases (IKE and IPSec) to negotiate for establishing an IPSec VPN tunnel with pre-shared key and optional X-Auth account / password.

Parameter Setup Example

For Network-A at HQ

Following 5 tables list the parameter configuration for above example diagram of IPSec VPN tunnel in Network-A.

Use default value for those parameters that are not mentioned in these 5 tables.

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

Configuration Path	[IPSec]-[Tunnel Configuration]
Tunnel	■ *Enable*
Tunnel Name	*dvpn-101*
Interface	*WAN 1*
Tunnel Scenario	*Dynamic VPN*
Operation Mode	*Always on*

Configuration Path	[IPSec]-[Local & Remote Configuration]
Local Subnet	*10.0.76.0*
Local Netmask	*255.255.255.0*

Configuration Path	[IPSec]-[Authentication]
Key Management	*IKE+Pre-shared Key 12345678*
Local ID	*User Name Network-B*

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

For Network-B at Mobile Office

Following 5 tables list the parameter configuration for above example diagram of IPSec VPN tunnel in Network-B.

Use default value for those parameters that are not mentioned in these 5 tables.

Please also note that the authentication parameters of both peers must match each other to complete the authentication process successfully, and it is just for an example here.

In addition, Negotiation Mode and X-Auth in "IKE Phase" configuration window should be also matched on both peers.

And there is at least one proposal entity in IKE Proposal Definition and at least one proposal entity in IPSec Proposal Definition are the same for both peers. Use the default ones in the setup example and they are not shown in followings.

Configuration Path	[IPSec]-[Configuration]
IPSec	■ *Enable*
Configuration Path	[IPSec]-[Tunnel Configuration]
Tunnel	■ *Enable*
Tunnel Name	*dvpn-201*
Interface	*WAN 1*
Tunnel Scenario	*Site to Site*
Operation Mode	*Always on*
Keep alive	■ *Enable* *Ping FQDN → www.abc.com , Interval 120 sec*

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 or www.abc.com* *PS : Some advanced users will use Dynamic DDS function to update Global IP address which is not fixed .We suggest enabling "Keep alive" item.*

Configuration Path	[IPSec]-[Authentication]
Key Management	*IKE+Pre-shared Key 12345678*
Local ID	*User Name Network-B*

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

Scenario Operation Procedure

In above diagram, Network-A is in the headquarters, and the subnet of its Intranet is 10.0.76.0/24. The security gateway for Network-A has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 (or FQDN:www.abc.com) for WAN interface.

However, Network-B is in the mobile office and the subnet of its Intranet is 10.0.75.0/24. The security gateway for Network-B has a dynamic IP address of 118.18.81.33 for WAN interface or private IP address of 10.253.253.1 in Cellular Network

Establish an IPSec VPN tunnel with "Dynamic VPN" scenario by starting from the mobile site. So both Intranets of 10.0.75.0/24 and 10.0.76.0/24 can securely communicate each other.

Finally, the client hosts in the Intranet of Network-B at mobile office can access the server or database resources in the Intranet of Network-A at HQ with a secured link.

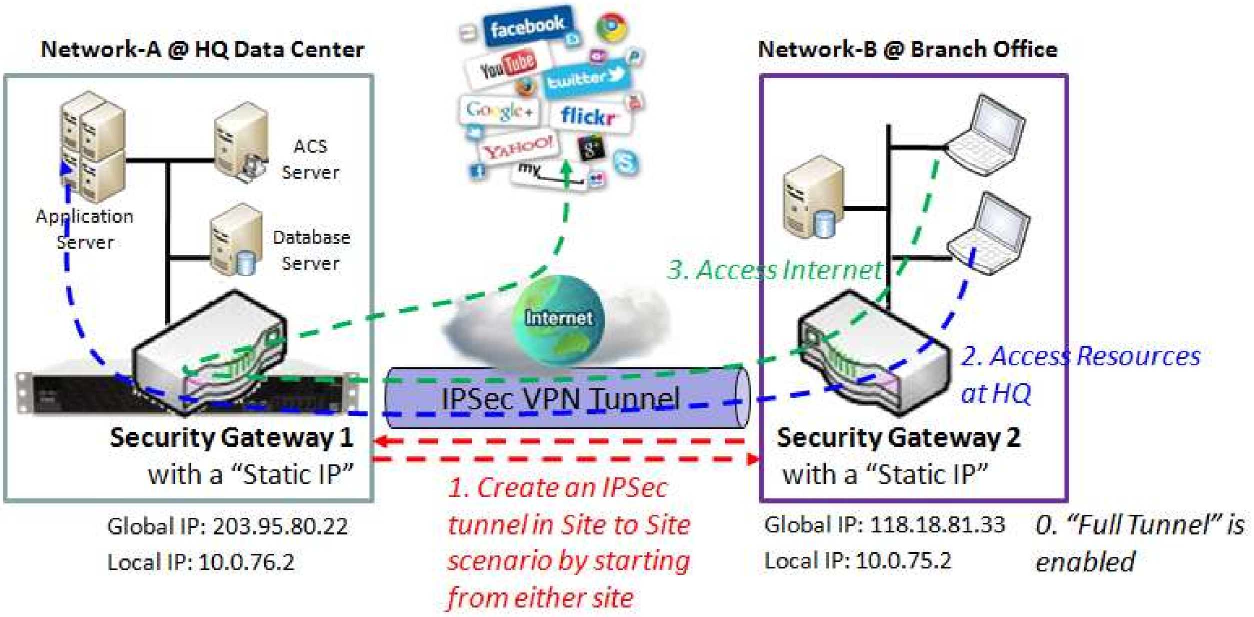
That means, the security gateway in headquarters supports "Dynamic VPN" function and then you, as a mobile user, can access its Intranet resources from remote side with a secured link; even your device is not on a fixed IP address.

"Full Tunnel"-enabled Site to Site Tunnel Scenario

In "Site to Site" tunnel scenario, the client hosts of remote site can securely access the enterprise resources in the Intranet of headquarters gateway via an established VPN tunnel, as described above. But the regular Internet accessing at remote site still go through the WAN interface of remote gateway, not the VPN tunnel. If you want all packets to be transferred from the Network-B at branch office via this VPN tunnel, including the enterprise resource accessing and the Internet accessing, you can refer to following scenario example.

When Full Tunnel function of remote Business Security Gateway is enabled, all data traffic from remote clients behind remote Business Security Gateway will go over the VPN tunnel. That is, if a user is operating at a PC that is in the Intranet of remote Business Security Gateway, all application packets and private data packets from the PC will be transmitted securely in the VPN tunnel to access the resources behind HQ Business Security Gateway, including surfing the Internet. As a result, every time the user surfs the web for shopping or searching data on Internet, checking personal emails, or accessing HQ servers, all are done on a secured connection through HQ Business Security Gateway.

Following diagram illustrates this application scenario. It is the same as the one for the "Site to Site" scenario with "Full Tunnel" disabled. But the "Full Tunnel" parameter in this scenario is enabled now. When the "Site to Site" IPSec VPN tunnel has been established by either peer, all client hosts in Network-B at branch office can access the resources in HQ and the Internet by using the tunnel in a secure link since the "Full Tunnel" function is activated in Network-B site.



Scenario Application Timing

The security gateway can be located at branch office or mobile office. When the client hosts behind the security gateway want to make a secure communication with the ones behind another security gateway in headquarters or another branch office, both security gateways need establish a VPN tunnel first. Both Intranets of security gateways have their own subnet and the "Site to Site" tunnel scenario is used. "Site" means a subnet of client hosts. Moreover, since the "Full Tunnel" feature is enabled at branch office site, all packet flows will go through the established VPN tunnel between both sites, including the HQ resource accessing and regular Internet accessing.

Scenario Description

Both Initiator and Responder of IPSec tunnel must have a "Static IP" or a "FQDN" for "Site to Site" scenario.

Any peer gateway can be worked as an Initiator or a Responder of the IPSec VPN tunnel.

Two phases (IKE and IPSec) to negotiate for establishing an IPSec VPN tunnel with pre-shared key and optional X-Auth account / password.

"Full Tunnel" feature to be enabled drives all packet flows from local site will be transferred via the established VPN tunnel.

Parameter Setup Example

For Network-A at HQ

Following 5 tables list the parameter configuration for above example diagram of IPSec VPN tunnel in Network-A.

Use default value for those parameters that are not mentioned in these 5 tables.

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+Pre-shared Key 12345678***
Local ID	***User Name Network-A***
Remote ID	***User Name Network-B***

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

For Network-B at Branch Office

Following 5 tables list the parameter configuration for above example diagram of IPSec VPN tunnel in Network-B.

Use default value for those parameters that are not mentioned in these 5 tables. Please be noted that the special parameter configuration in red color.

Please also note that the authentication parameters of both peers must match each other to complete the authentication process successfully, and it is just for an example here.

In addition, Negotiation Mode and X-Auth in "IKE Phase" configuration window should be also matched in both peers.

And there is at least one proposal entity in IKE Proposal Definition and at least one proposal entity in IPSec Proposal Definition is same for both peers. Use the default ones in the setup example and they are not shown in followings.

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

Configuration Path	[IPSec]-[Tunnel Configuration]
Tunnel	■ ***Enable***
Tunnel Name	***s2s-201***
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	■ ***Enable***
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+Pre-shared Key 12345678***
Local ID	***User Name Network-B***
Remote ID	***User Name Network-A***

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

Scenario Operation Procedure

In above diagram, Network-A is in the headquarters, and the subnet of its Intranet is 10.0.76.0/24. The security gateway for Network-A has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN interface.

However, Network-B is in the branch office and the subnet of its Intranet is 10.0.75.0/24. The security gateway for Network-B has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN interface.

Establish an IPSec VPN tunnel with "Site to Site" scenario by starting from either site. So both Intranets of 10.0.75.0/24 and 10.0.76.0/24 can securely communicate each other.

Finally, all packet flows from the client hosts in the Intranet of Network-B at branch office will go through the established VPN tunnel.

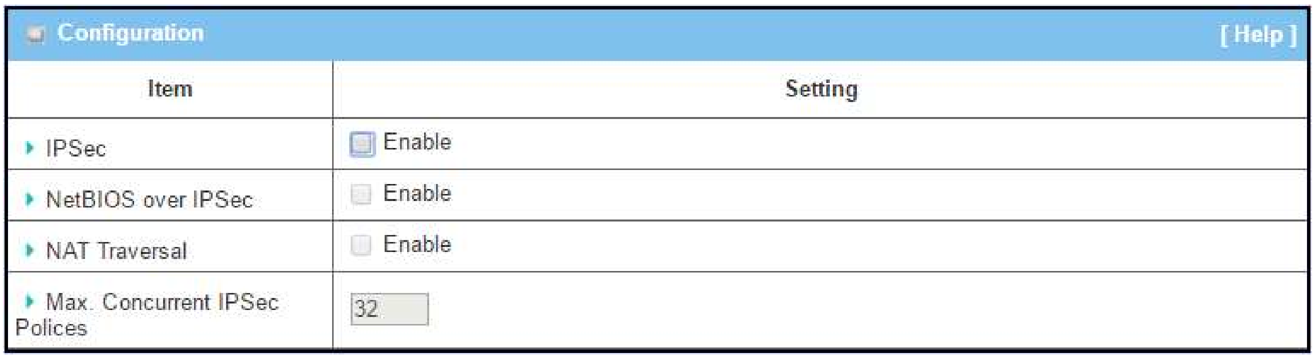
That means, the security gateway in branch office supports "Full Tunnel" feature and the client hosts behind it can access not only the server or database resources in the Intranet of Network-A at HQ, but also the Internet in a secured connection. The HQ gateway controls and secures the IP networking request flows from the branch office.

IPSec Setting

The IPSec Setting allows user to create and configure IPSec tunnels. Before you proceed ensure that the VPN is enabled and saved. To enable VPN, go to **Security > VPN > Configuration** tab.

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

Enable IPSec



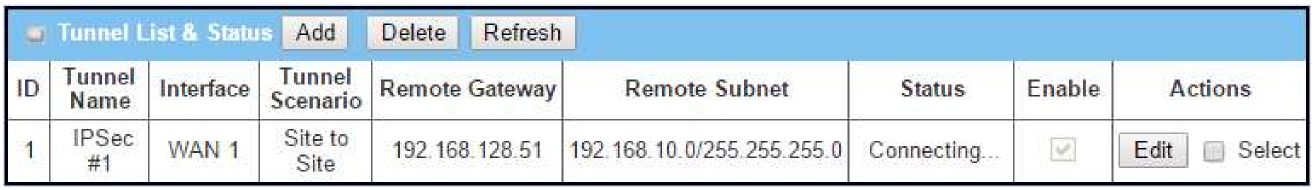
Configuration [Help]

Item	Setting
IPSec	□ Enable
NetBIOS over IPSec	□ Enable
NAT Traversal	□ Enable
Max. Concurrent IPSec Polices	32

Enable IPSec Window		
Item	**Value setting**	**Description**
IPsec	Unchecked by default	Click the **Enable** box to enable IPSec function.
NetBIOS over IPSec	Unchecked by default	Click the **Enable** box to enable NetBIOS over IPSec function.
NAT Traversal	Unchecked by default	Click the **Enable** box to enable NAT Traversal function.
Max. Concurrent IPSec Tunnels	32 is set by default	The specified value will limit the maximum number of simultaneous IPSec tunnel connection. The default value can be different for the purchased model.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Create/Edit IPSec tunnel

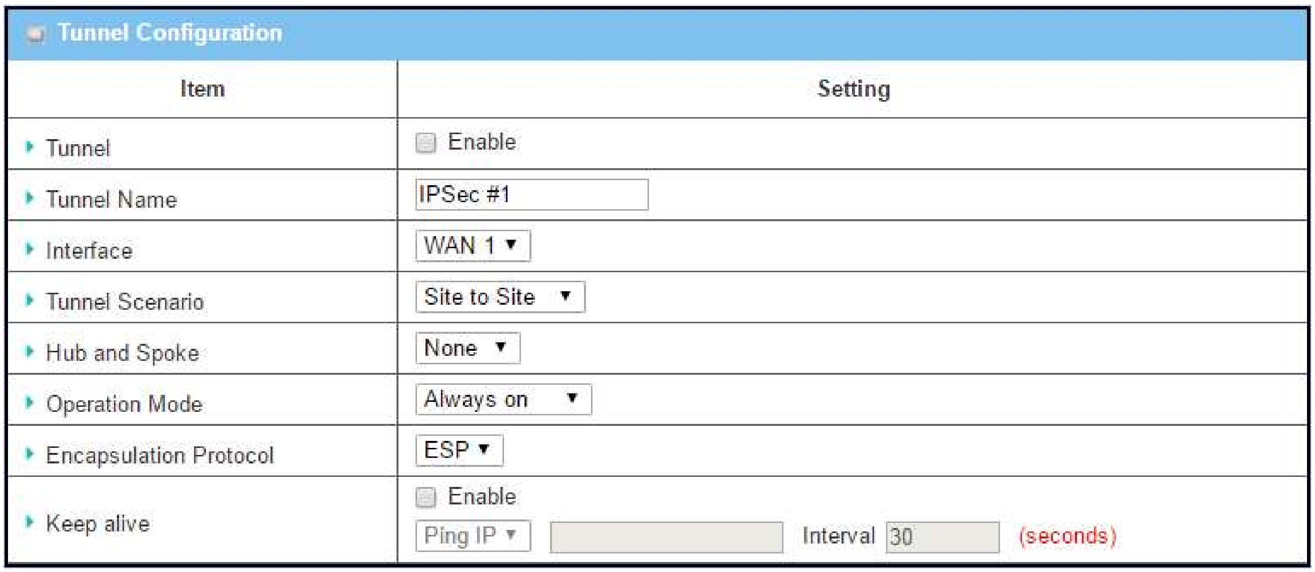
Ensure that the IPSec enable box is checked to enable before further configuring the IPSec tunnel settings.



Tunnel List & Status Add Delete Refresh

ID	Tunnel Name	Interface	Tunnel Scenario	Remote Gateway	Remote Subnet	Status	Enable	Actions
1	IPSec #1	WAN 1	Site to Site	192.168.128.51	192.168.10.0/255.255.255.0	Connecting...	☑	Edit □ Select

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

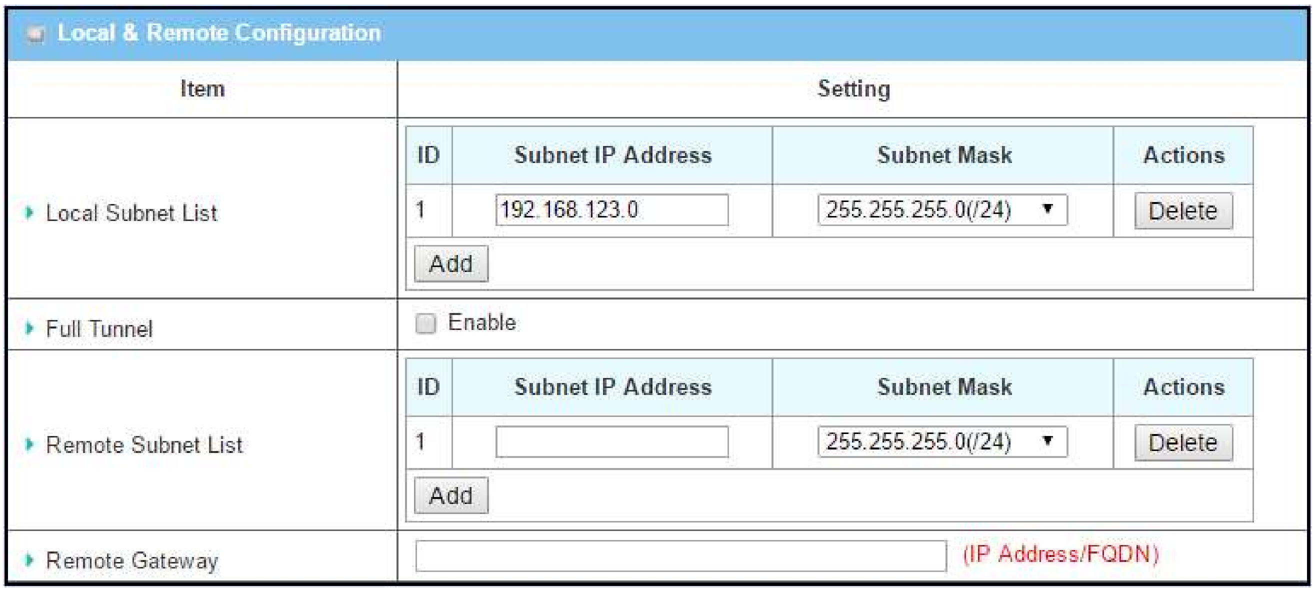


Tunnel Configuration

Item	Setting
Tunnel	□ Enable
Tunnel Name	IPSec #1
Interface	WAN 1 ▾
Tunnel Scenario	Site to Site ▾
Hub and Spoke	None ▾
Operation Mode	Always on ▾
Encapsulation Protocol	ESP ▾
Keep alive	□ Enable Ping IP ▾ Interval 30 (seconds)

Tunnel Configuration Window		
Item	**Value setting**	**Description**
Tunnel	Unchecked by default	Check the **Enable** box to activate the IPSec tunnel
Tunnel Name	1. A Must fill setting 2. String format can be any text	Enter a tunnel name. Enter a name that is easy for you to identify.
Interface	1. A Must fill setting 2. WAN 1 is selected by default	Select WAN interface on which IPSec tunnel is to be established.
Tunnel Scenario	1. A Must fill setting 2. Site to site is selected by default	Select an IPSec tunneling scenario from the dropdown box for your application. Select **Site-to-Site**, **Site-to-Host**, **Host-to-Site**, or **Host-to-Host**. With **Site-to-Site** or **Site-to-Host** or **Host-to-Site**, IPSec operates in tunnel mode. The difference among them is the number of subnets. With **Host-to-Host**, IPSec operates in transport mode.

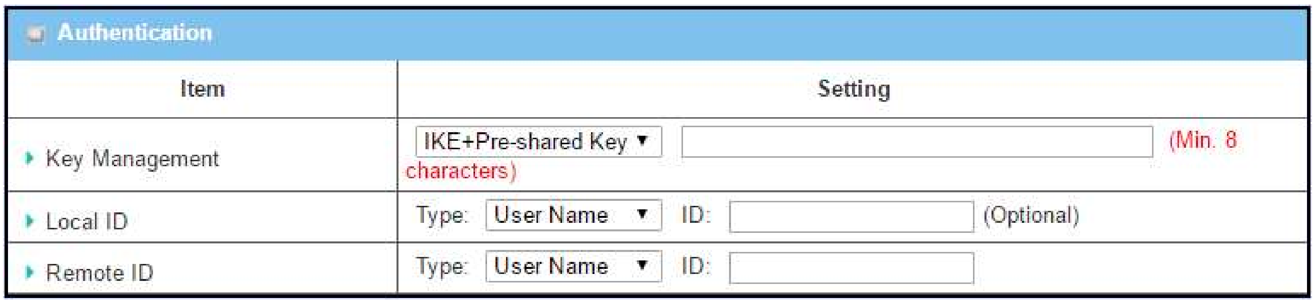
Hub and Spoke	1. An optional setting 2. None is set by default	Select from the dropdown box to setup your gateway for Hub-and-Spoke IPSec VPN Deployments. Select **None** if your deployments will not support Hub or Spoke encryption. Select **Hub** for a Hub role in the IPSec design. Select **Spoke** for a Spoke role in the IPSec design. Note: Hub and Spoke are available only for Site-to-Site VPN tunneling specified in Tunnel Scenario. It is not available for Dynamic VPN tunneling application.
Operation Mode	1. A Must fill setting 2. Alway on is selected by default	There are three available operation modes. Always On, Failover, Load Balance. **Failover/ Always** Define whether the IPSec tunnel is a failover tunnel function or an Always on tunnel. Note: If this IPSec is a failover tunneling, you will need to select a primary IPSec tunnel from which to failover to. **Load Balance** Define whether the IPSec tunnel connection will take part in load balance function of the gateway. You will not need to select with WAN interface as the system will automatically utilize the available WAN interfaces to balance traffic loads. For more details on WAN Load Balance, refer to Load Balance Usage in this manual. On gateway's web-based utility, go to Basic Network > WAN > Load Balance tab. Note: Failover and Load Balance functions are not available for Dynamic VPN specified in Tunnel Scenario.
Encapsulation Protocol	1. A Must fill setting 2. ESP is selected by default	Select the Encapsulation Protocol from the dropdown box for this IPSec tunnel. Available encapsulations are ESP and AH.
Keep alive	1. Unchecked by default 2. 30s is set by default	Check the **Enable** box to enable Keep alive function. Select Ping IP to keep live and enter the IP address to ping. Enter the ping time interval in seconds. Note: Keep alive option is not available for Dynamic VPN specified in Tunnel Scenario.



Local & Remote Configuration

Item	Setting
Local Subnet List	ID: 1; Subnet IP Address: 192.168.123.0; Subnet Mask: 255.255.255.0(/24); Actions: Delete Add
Full Tunnel	□ Enable
Remote Subnet List	ID: 1; Subnet IP Address: ; Subnet Mask: 255.255.255.0(/24); Actions: Delete Add
Remote Gateway	(IP Address/FQDN)

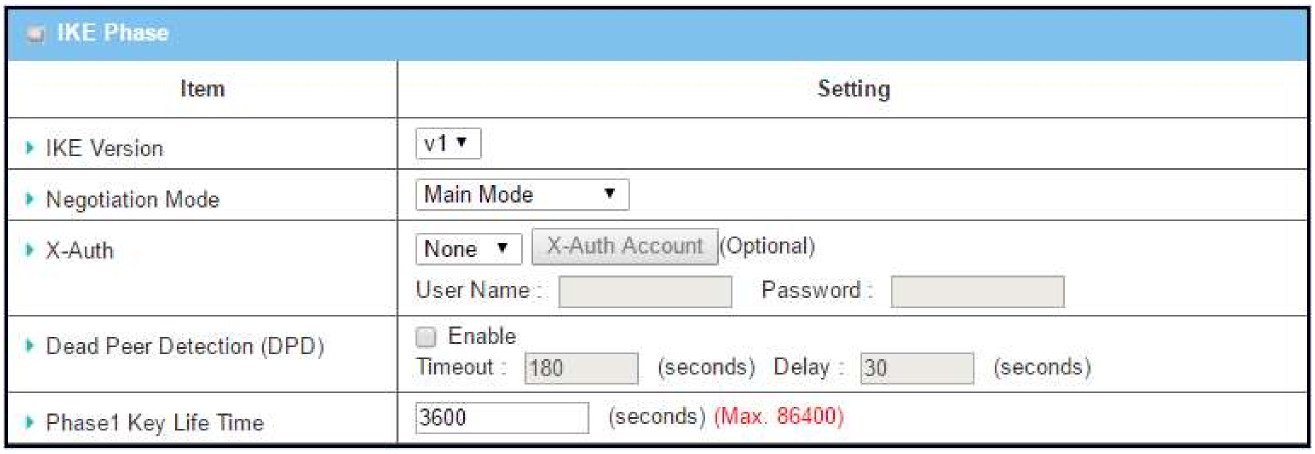
Local & Remote Configuration Window		
Item	**Value setting**	**Description**
Local Subnet List	A Must fill setting	Specify the Local Subnet IP address and Subnet Mask. Click the Add or Delete button to add or delete a Local Subnet. Note_1: When Dynamic VPN option in Tunnel Scenario is selected, there will be only one subnet available. Note_2: When Host-to-Site or Host-to-Host option in Tunnel Scenario is selected, Local Subnet will not be available. Note_3: When Hub and Spoke option in Hub and Spoke is selected, there will be only one subnet available.
Full Tunnel	Unchecked by default	Click Enable box to enable Full Tunnel. Note: Full tunnel is available only for Site-to-Site specified in Tunnel Scenario.
Remote Subnet List	A Must fill setting	Specify the Remote Subnet IP address and Subnet Mask. Click the Add or Delete button to add or delete Remote Subnet setting.
Remote Gateway	1. A Must fill setting. 2. Format can be a ipv4 address or FQDN	Specify the Remote Gateway.



Authentication

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

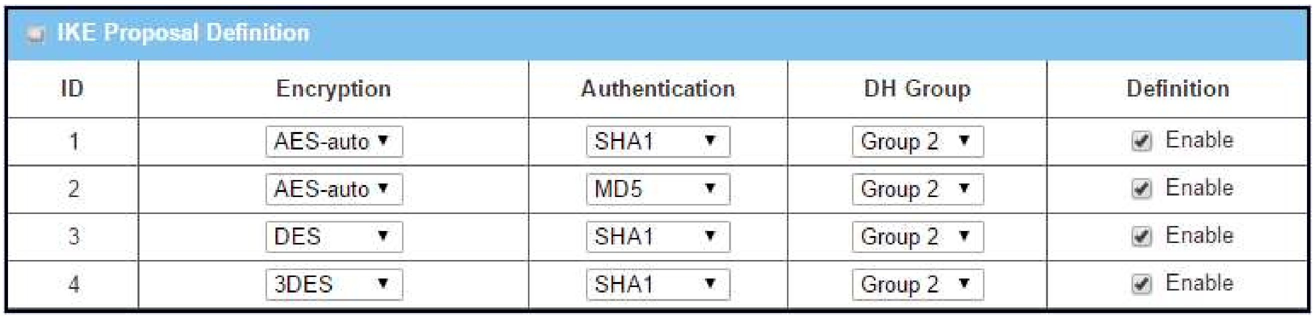
Authentication Configuration Window		
Item	**Value setting**	**Description**
Key Management	1. A Must fill setting 2. Pre-shared Key 8 to 32 characters.	Select Key Management from the dropdown box for this IPSec tunnel. **IKE+Pre-shared Key**: user needs to set a key (Min. 8 characters). **IKE+X.509**: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



IKE Phase

Item	Setting
IKE Version	v1 ▾
Negotiation Mode	Main Mode ▾
X-Auth	None ▾ X-Auth Account (Optional) User Name : Password :
Dead Peer Detection (DPD)	□ Enable Timeout : 180 (seconds) Delay : 30 (seconds)
Phase1 Key Life Time	3600 (seconds) (Max. 86400)

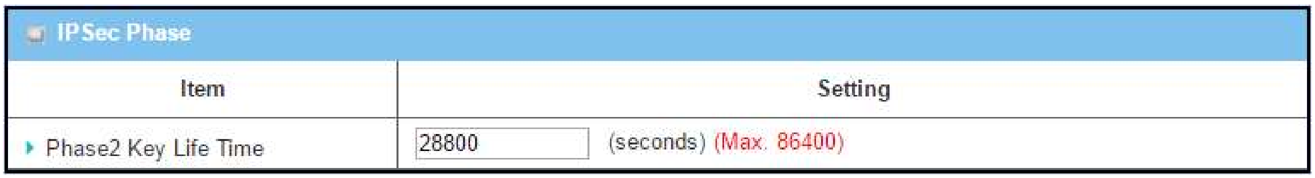
IKE Phase Window Item	 Value setting	 Description
IKE Version	1. A must fill setting 2. v1 is selected by default	Specify the IKE version for this IPSec tunnel. Select v1 or v2 Note: IKE versions will not be available when Dynamic VPN option in Tunnel Scenario is selected, or AH option in Encapsulation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



IKE Proposal Definition

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

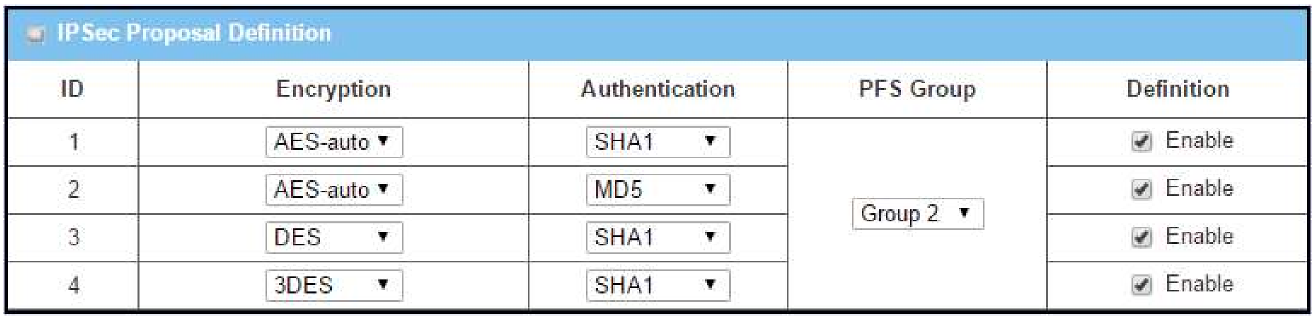
IKE Proposal Definition Window		
Item	**Value setting**	**Description**
IKE Proposal Definition	A Must fill setting	Specify the Phase 1 Encryption method. AES-auto/AES128/AES192/AES256/DES/3DES Specify the Authentication method. None/MD5/SHA1/SHA2-256/SHA2-512 Specify the DH Group None/Group1/ Group2/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



IPSec Phase

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

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



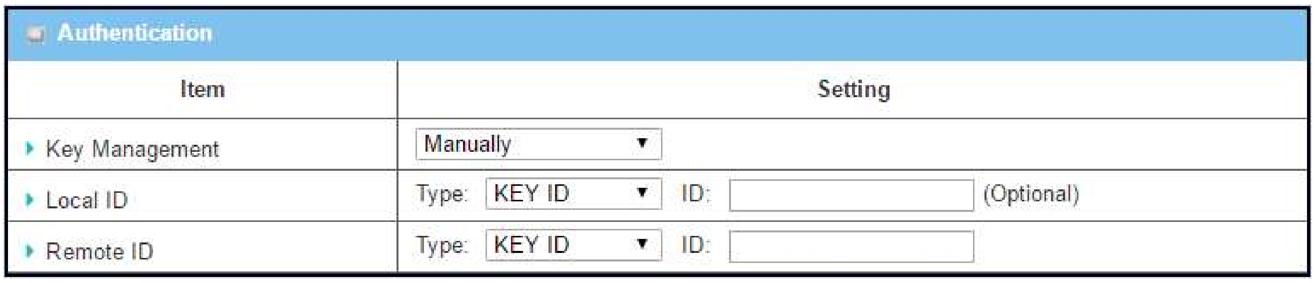
IPSec Proposal Definition

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

IPSec Proposal Definition Window		
Item	**Value setting**	**Description**
IPSec Proposal Definition	A Must fill setting	Specify the Encryption method None/AES-auto/AES128/AES192/AES256/DES/3DES Specify Authentication method None/MD5/SHA1/SHA2-256/SHA2-512 Specify the PFS Group None/Group1/ Group2/ Group5/ Group14/ Group15/ Group16/ Group17/ Group18/ Click Enable to enable this setting
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** button to cancel the settings
Back	N/A	Click **Back** button to return to the previous page.

Manual Key Management

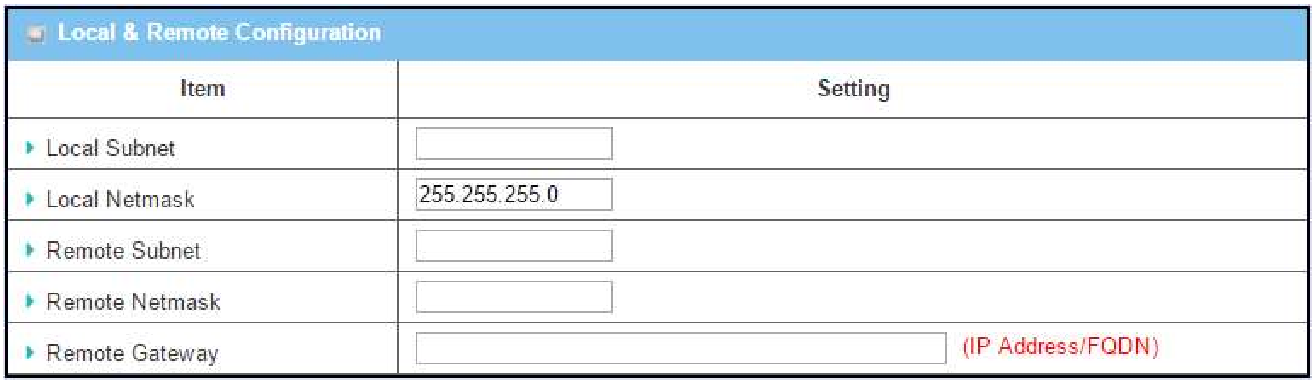
When the Manually option is selected for Key Management as described in Authentication Configuration Window, a series of configuration windows for Manual IPSec Tunnel configuration will appear. The configuration windows are the Local & Remote Configuration, the Authentication, and the Manual Proposal.



Authentication

Item	Setting
Key Management	Manually ▾
Local ID	Type: KEY ID ▾ ID: (Optional)
Remote ID	Type: KEY ID ▾ ID:

Authentication Configuration Window		
Item	**Value setting**	**Description**
Key Management	A Must fill setting	Select Key Management from the dropdown box for this IPSec tunnel. In this section **Manually** is the option selected. For **IKE+Pre-shared Key** and **IKE+X.509** option, please refer to the table in previous 5 pages where key management is described.
Local ID	An optional setting	Specify the **Local ID** for this IPSec tunnel to authenticate. Select the **Key ID** for Local ID and enter the Key ID (English alphabet or number).
Remote ID	An optional setting	Specify the **Remote ID** for this IPSec tunnel to authenticate. Select **Key ID** for Remote ID and enter the Key ID (English alphabet or number).

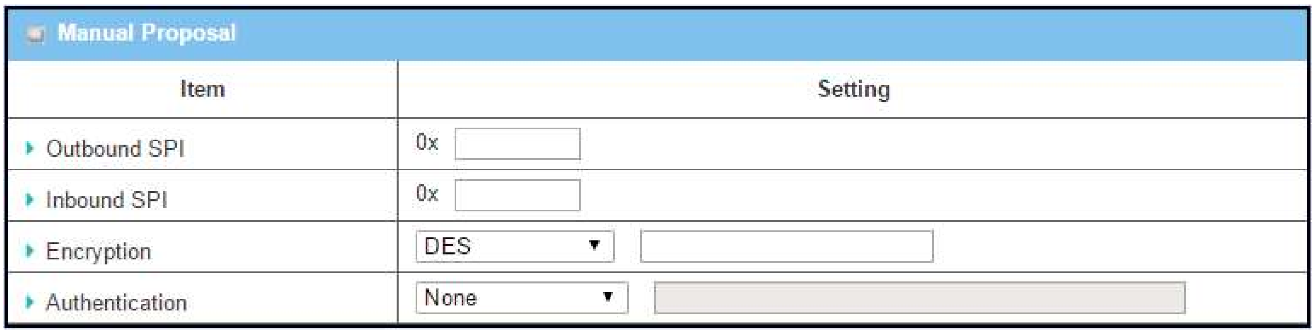


Local & Remote Configuration

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

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

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



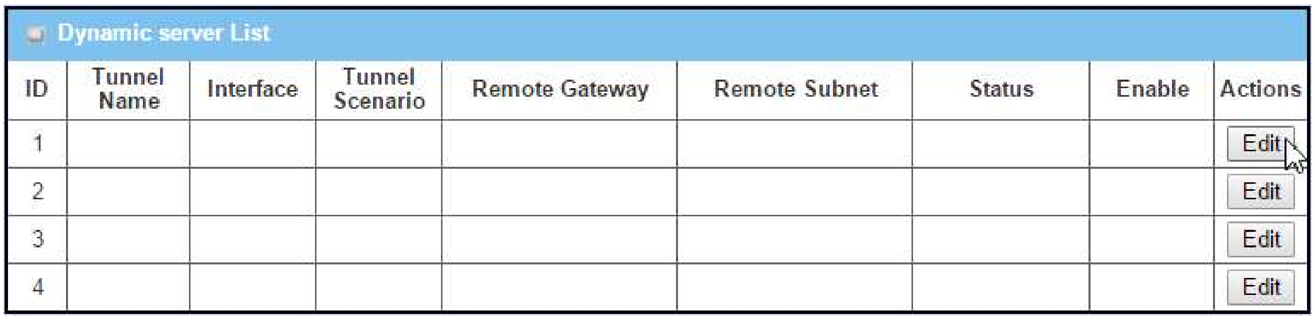
Manual Proposal

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

Manual Proposal Window		
Item	**Value setting**	**Description**
Outbound SPI	Hexadecimal format	Specify the Outbound SPI for this IPSec tunnel.
Inbound SPI	Hexadecimal format	Specify the Inbound SPI for this IPSec tunnel.
Encryption	1. A Must fill setting 2. Hexadecimal format	Specify the Encryption Method and Encryption key Available encryption methods are DES/3DES/AES128/AES192/AES256 The key length for DES is 16, 3DES is 48, AES128 is 32, AES192 is 48, AES256 is 64.

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

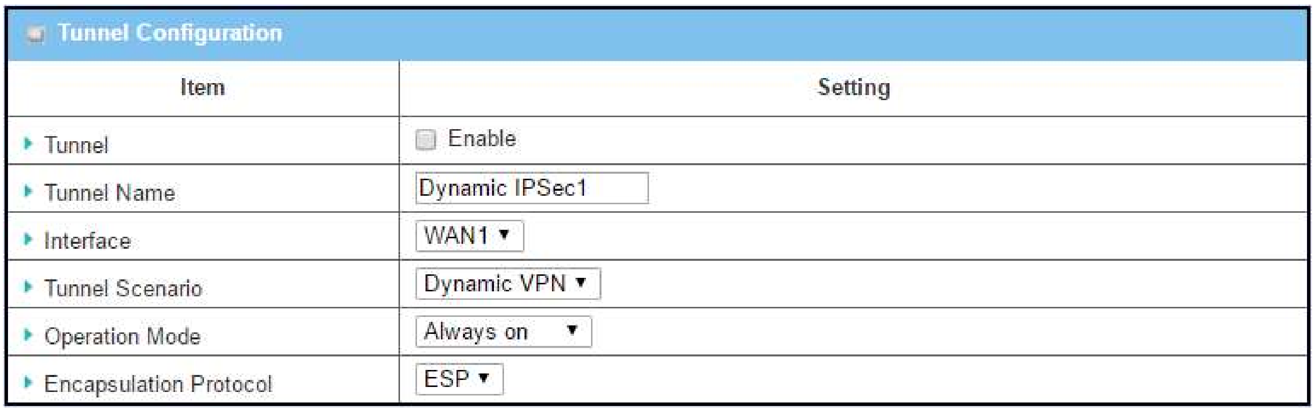
Create/Edit Dynamic VPN Server List



Dynamic server List

ID	Tunnel Name	Interface	Tunnel Scenario	Remote Gateway	Remote Subnet	Status	Enable	Actions
1								Edit
2								Edit
3								Edit
4								Edit

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

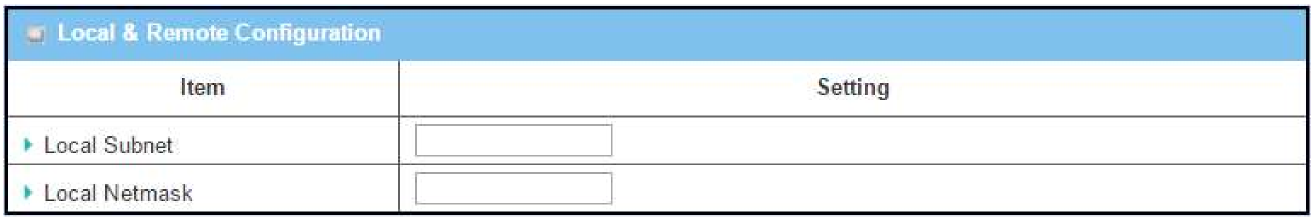


Tunnel Configuration

Item	Setting
Tunnel	□ Enable
Tunnel Name	Dynamic IPSec1
Interface	WAN1 ▾
Tunnel Scenario	Dynamic VPN ▾
Operation Mode	Always on ▾
Encapsulation Protocol	ESP ▾

Tunnel Configuration Window

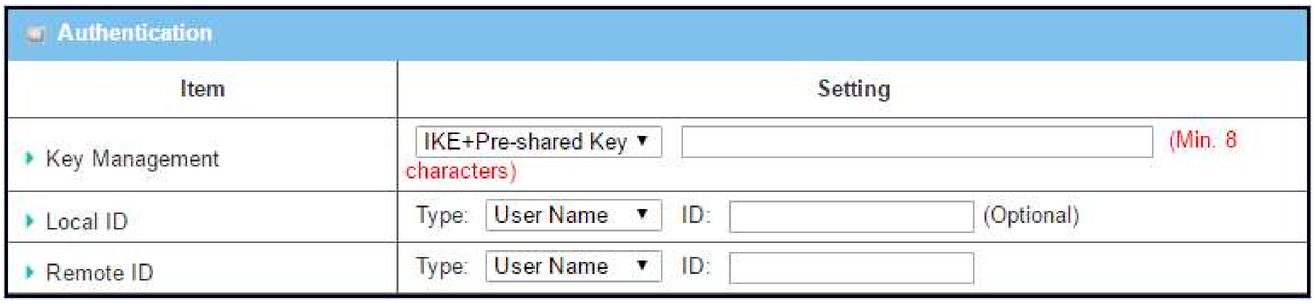
Item	Value setting	Description
Tunnel	Unchecked by default	Check the **Enable** box to activate the Dynamic IPSec VPN tunnel
Tunnel Name	1. A Must fill setting 2. String format can be any text	Enter a tunnel name. Enter a name that is easy for you to identify.
Interface	1. A Must fill setting 2. WAN 1 is selected by default	Select WAN interface on which IPSec tunnel is to be established.
Tunnel Scenario	1. A Must fill setting 2. Dynamic VPN is selected by default	The IPSec tunneling scenario is fixed to Dynamic VPN.
Operation Mode	1. A Must fill setting 2. Alway on is selected by default	The available operation mode is Always On. Failover and Load Balance options are not available for the Dynamic IPSec scenario.
Encapsulation Protocol	1. A Must fill setting 2. ESP is selected by default	Select the Encapsulation Protocol from the dropdown box for this IPSec tunnel. Available encapsulations are ESP and AH.



Local & Remote Configuration

Item	Setting
Local Subnet	
Local Netmask	

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



Authentication

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 fill setting 2. Pre-shared Key 8 to 32 characters.	Select Key Management from the dropdown box for this IPSec tunnel. **IKE+Pre-shared Key**: user needs to set a key (Min. 8 characters).
Local ID	An optional setting	Specify the Local ID for this IPSec tunnel to authenticate. Select User Name for Local ID and enter the username. The username may include but can't be all numbers. Select FQDN for Local ID and enter the FQDN. Select User@FQDN for Local ID and enter the User@FQDN. Select Key ID for Local ID and enter the Key ID (English alphabet or number).
Remote ID	An optional setting	Specify the Remote ID for this IPSec tunnel to authenticate. Selected User Name for Remote ID and enter the username. The username may include but can't be all numbers. Select FQDN for Local ID and enter the FQDN. Select User@FQDN for Remote ID and enter the User@FQDN. Select Key ID for Remote ID and enter the Key ID (English alphabet or number).. Note: Remote ID will be not available when Dynamic VPN option in Tunnel Scenario is selected.

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

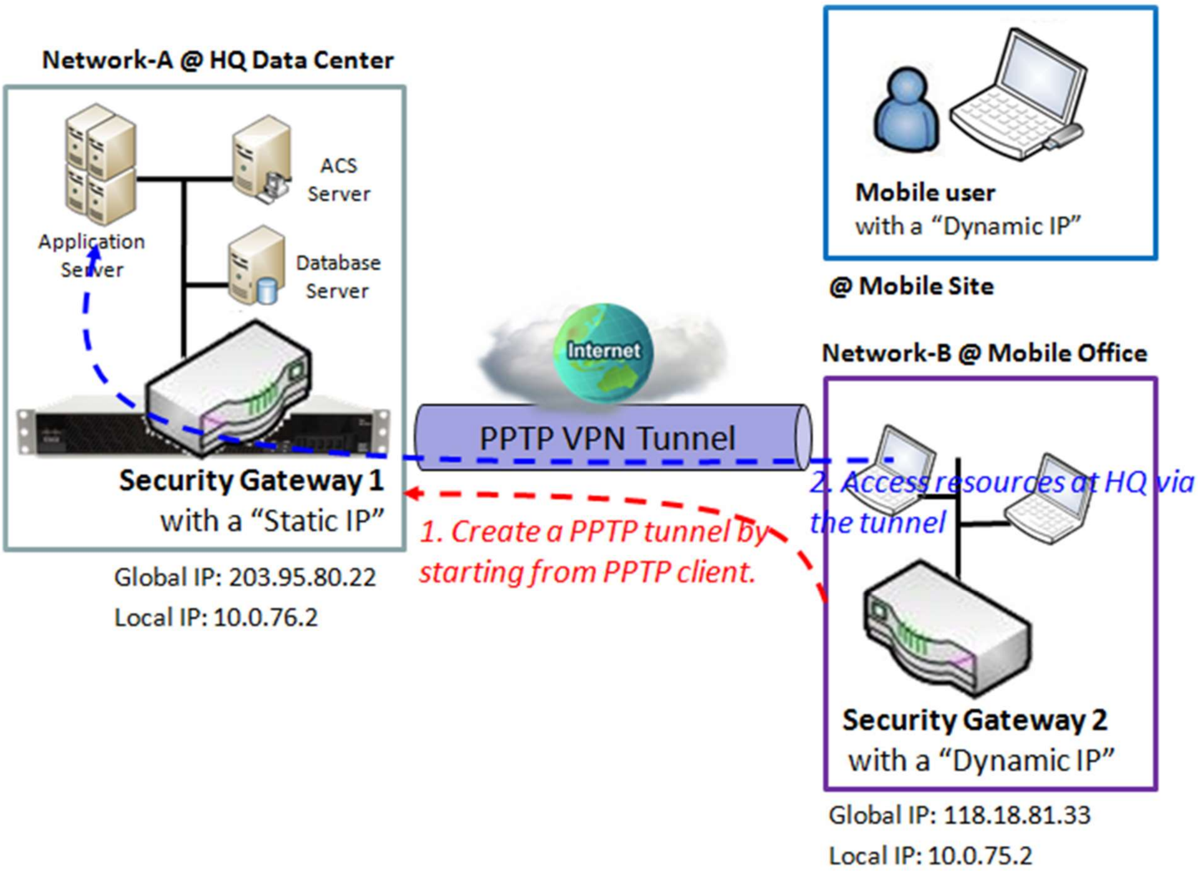
9.1.5 PPTP

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. The PPTP specification does not describe encryption or authentication features and relies on the Point-to-Point Protocol being tunneled to implement security functionality. However, the most common PPTP implementation shipping with the Microsoft Windows product families implements various levels of authentication and encryption natively as standard features of the Windows PPTP stack. The intended use of this protocol is to provide security levels and remote access levels comparable with typical VPN products.

The security gateway can play either "PPTP Server" role or "PPTP Client" role for a PPTP VPN tunnel, or both at the same time for different tunnels. Deploy a security gateway for local office and establish a virtual private network with the remote gateway of another office by using PPTP tunneling. So, all client hosts behind local security gateway can make data communication with others behind remote gateway.

Or when you are a mobile user with a notebook or carrying along a security gateway and you want to access the servers and database in company headquarters (HQ). In addition, the security gateway in HQ supports the PPTP VPN server function. So you can dial in the HQ gateway and access the HQ resources by establishing a PPTP VPN tunnel. It is a virtual private network between your device and HQ gateway for your resource accessing.

PPTP VPN Server Scenario



Scenario Application Timing

The Scenario diagram illustrates the security gateway 1 at headquarter playing the PPTP VPN server role. The PPTP tunnel is established by starting from PPTP client, the Security Gateway 2 in Network-B or the mobile device, like notebook. All client hosts behind the Security Gateway 2 or the mobile device can access the resources in the Intranet of Network-A at headquarters via this established PPTP tunnel. Usually, these hosts at PPTP client peer access the Internet directly via the WAN interface of Security Gateway 2. Only the packets whose destination is in the dedicated subnet to Network-A will be transferred via the PPTP tunnel.

Scenario Description

PPTP Tunneling is a Client and Server based tunneling technology.

The PPTP Server must have a Static IP or a FQDN and maintain a Client list (account / password). The Client may be a mobile user or mobile site and requesting the PPTP tunnel connection with its account / password.

PPTP protocol is used for establishing a PPTP VPN tunnel.

Parameter Setup Example

For Network-A at HQ, following 3 tables list the parameter configuration for above example diagram of PPTP VPN server in Network-A.

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

Configuration Path	[PPTP]-[Configuration]
PPTP	■ ***Enable***
Client/Server	**Server**

Configuration Path	[PPTP]-[PPTP Server Configuration]
PPTP Server	■ ***Enable***
Server Virtual IP	***192.168.101.253***
IP Pool Starting Address	***10*** **(that means 192.168.101.10)**
IP Pool Ending Address	***50*** **(that means 192.168.101.50)**
Authentication Protocol	***MS-CHAP***
MPPE Encryption	■ ***Enable 128 bits***

Configuration Path	[PPTP]-[User Account Configuration]	
ID	**1**	**2**
User Name	***User-1***	***User-2***
Password	***1234***	***4321***
Account	■ ***Enable***	■ ***Enable***

Scenario Operation Procedure

In above diagram, Network-A is in the headquarters, and the subnet of its Intranet is 10.0.76.0/24. The security gateway for Network-A has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN interface. It serves as a PPTP server.

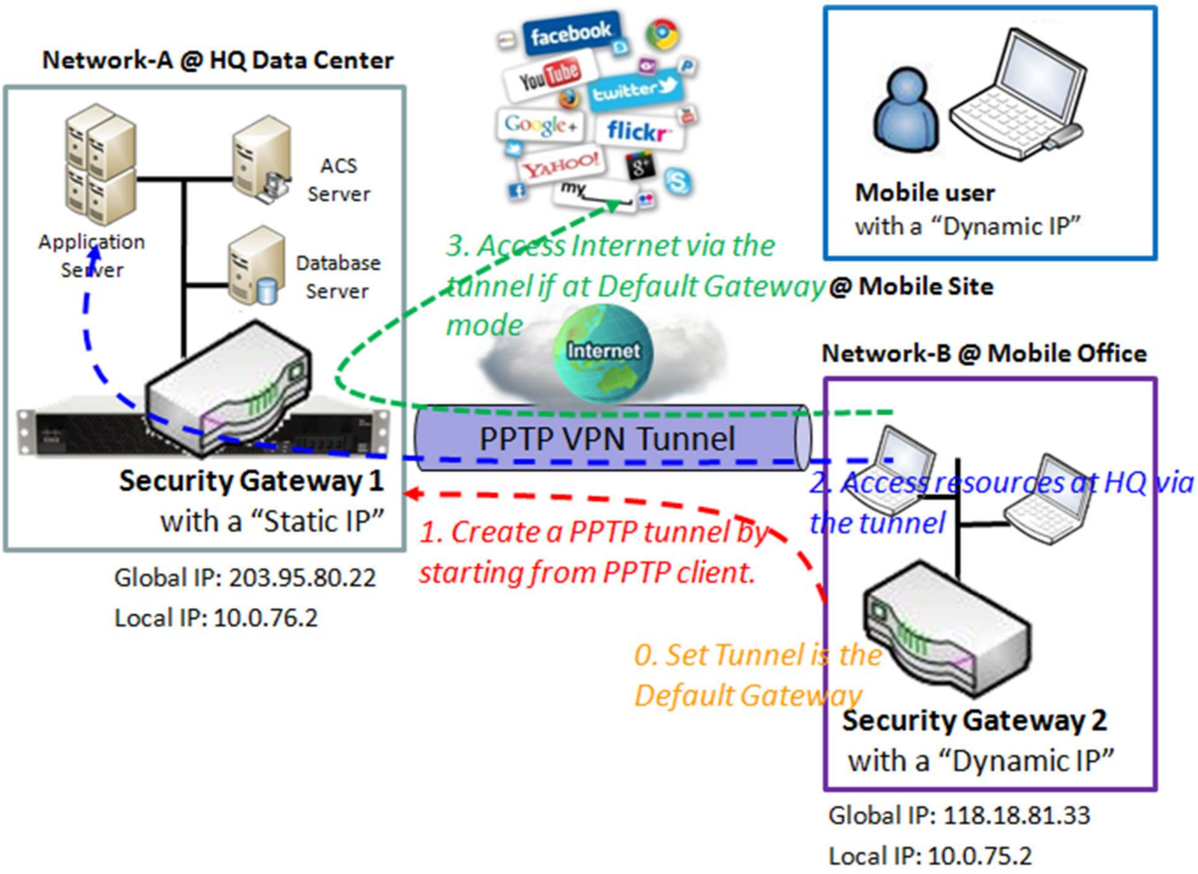
However, Network-B is in the mobile office and the subnet of its Intranet is 10.0.75.0/24. The security gateway for Network-B has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN interface. It serves as a PPTP client.

PPTP server provides two user accounts, User-1 and User-2, for PPTP clients dialing in.

Establish a PPTP VPN tunnel by starting from the PPTP client site. So both Intranets of 10.0.75.0/24 and 10.0.76.0/24 can securely communicate each other.

Finally, the client hosts in the Intranet of Network-B at mobile office can access the server or database resources in the Intranet of Network-A at HQ in a secured link.

PPTP VPN Client Scenario



Scenario Application Timing

Above diagram illustrates the Security Gateway 2 or the mobile device playing the PPTP VPN client role. The PPTP tunnel is established by the PPTP client making the tunnel connection request initiation and the Security Gateway 1 in Network-A of headquarters serves as the PPTP VPN server responding to the request. Once the tunnel has been established, all client hosts behind the Security Gateway 2 or the mobile device can access the resources in the Intranet of Network-A at headquarters via this established PPTP tunnel. Usually, these hosts at PPTP client peer access the Internet directly via the WAN interface of Security Gateway 2. Only the packets whose destination is in the dedicated subnet to Network-A will be transferred via the PPTP tunnel. But if PPTP client peer is configured to all packets are delivered via the PPTP tunnel, as shown in the diagram by configuring the PPTP tunnel is the default gateway at PPTP client peer, the Internet accessing packets will be also sent to the Security Gateway 1 in Network-A and be re-transferred to the Internet. That means the Internet accessing of PPTP Client peer is also controlled by the Security Gateway 1, the PPTP VPN server.

Scenario Description

PPTP Tunneling is a Client and Server based tunneling technology.

The PPTP Server must have a Static IP or a FQDN, and maintain a Client list (account / password). The Client may be a mobile user or mobile site, and requesting the PPTP tunnel connection with its account / password.

PPTP protocol is used for establishing a PPTP VPN tunnel.

The PPTP Client's "Default Gateway/Remote Subnet" setting determines how the Internet traffic from PPTP client site is handled.

Parameter Setup Example

For Network-B at Mobile Office

Following 3 tables list the parameter configuration for above example diagram of PPTP VPN client in Network-B.

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

Configuration Path	[PPTP]-[Configuration]
PPTP	■ ***Enable***
Client/Server	***Client***

Configuration Path	[PPTP]-[PPTP Client Configuration]
PPTP Client	■ ***Enable***

Configuration Path	[PPTP]-[Configuration for A PPTP Client]
PPTP Client Name	***PPTP #1***
Interface	***WAN 1***
Remote IP/FQDN	***203.95.80.22***
User Name	***User-1***
Password	***1234***
Default Gateway/Remote Subnet	***Default Gateway***
Authentication Protocol	***MS-CHAP***
MPPE Encryption	■ ***Enable***
Tunnel	■ ***Enable***

Scenario Operation Procedure

In above diagram, Network-A is in the headquarters, and the subnet of its Intranet is 10.0.76.0/24. The security gateway for Network-A has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN interface. It serves as a PPTP server.

However, Network-B is in the mobile office and the subnet of its Intranet is 10.0.75.0/24. The security gateway for Network-B has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN interface. It serves as a PPTP client.

The PPTP client uses "User-1" user account to dial in the PPTP server at HQ for establishing a PPTP VPN tunnel. So both Intranets of 10.0.75.0/24 and 10.0.76.0/24 can securely communicate each other.

Finally, the client hosts in the Intranet of Network-B at mobile office can access the server or database resources in the Intranet of Network-A at HQ in a secured link.

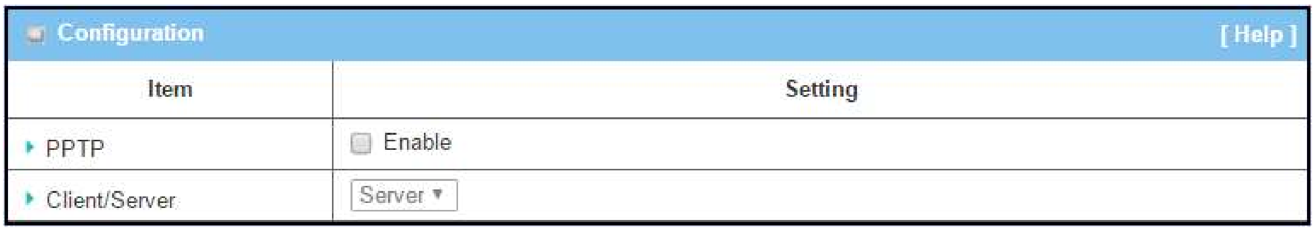
However, if the "Default Gateway/Remote Subnet" parameter in the Security Gateway 2 is configured to "Default Gateway", the Internet accessing of PPTP Client peer also go through the established PPTP VPN tunnel, and the Security Gateway 1 can control the accessing as same as the HQ resource accessing.

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

PPTP Setting

The PPTP setting allows user to create and configure PPTP tunnels. Before you proceed, ensure that the VPN is enabled and saved. To enable VPN, go to **Security > VPN > Configuration** tab.
Go to **Security > VPN > PPTP** tab.

Enable PPTP

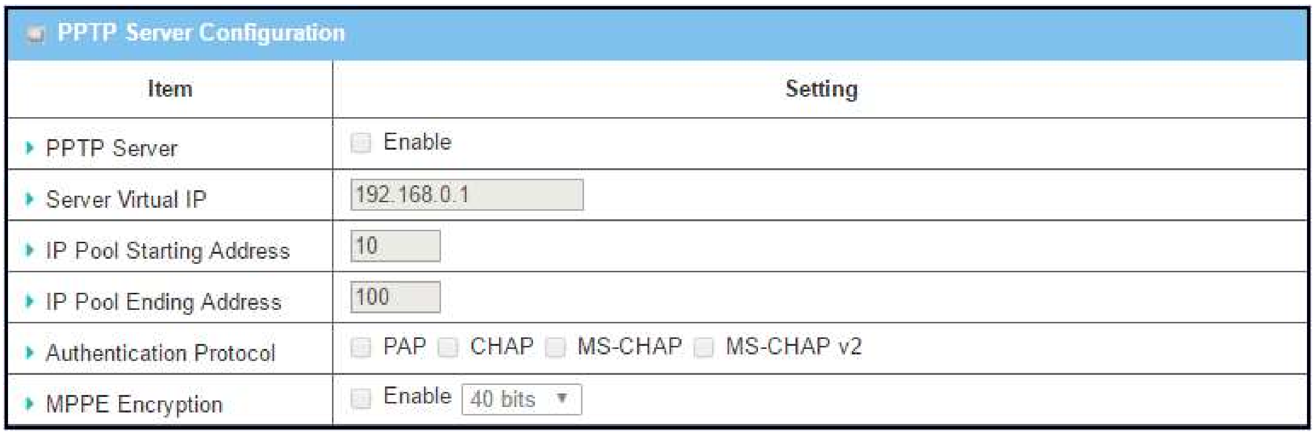


Item	Setting
PPTP	□ Enable
Client/Server	Server ▾

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

As a PPTP Server

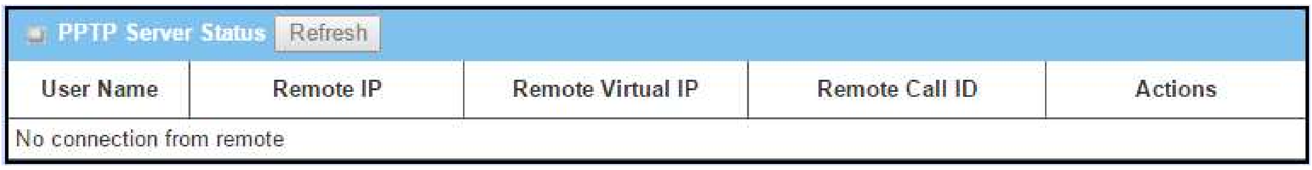
The gateway supports up to a maximum of 10 PPTP user accounts.
When Server in the Client/Server field is selected, the PPTP server configuration window will appear.



PPTP Server Configuration

Item	Setting
PPTP Server	□ Enable
Server Virtual IP	192.168.0.1
IP Pool Starting Address	10
IP Pool Ending Address	100
Authentication Protocol	□ PAP □ CHAP □ MS-CHAP □ MS-CHAP v2
MPPE Encryption	□ Enable 40 bits ▼

PPTP Server Configuration Window		
Item	**Value setting**	**Description**
PPTP Server	Unchecked by default	Check the **Enable** box to enable PPTP server role of the gateway.
Server Virtual IP	1. A Must fill setting 2. Default is 192.168.0.1	Specify the PPTP server Virtual IP address. The virtual IP address will serve as the virtual DHCP server for the PPTP clients. Clients will be assigned a virtual IP address from it after the PPTP tunnel has been established.
IP Pool Starting Address	1. A Must fill setting 2. Default is 10	This is the PPTP server's Virtual IP DHCP server. User can specify the first IP address for the subnet from which the PPTP client's IP address will be assigned.
IP Pool Ending Address	1. A Must fill setting 2. Default is 100	This is the PPTP server's Virtual IP DHCP server. User can specify the last IP address for the subnet from which the PPTP client's IP address will be assigned.
Authentication Protocol	1. A Must fill setting 2. Unchecked by default	Select single or multiple Authentication Protocols for the PPTP server with which to authenticate PPTP clients. Available authentication protocols are PAP/CHAP/MS-CHAP/MS-CHAPv2.
MPPE Encryption	A Must fill setting	Specify whether to support MPPE Protocol. Click the Enable box to enable MPPE and from dropdown box to select 40 bits/56 bits/128 bits. Note: when MPPE Encryption is enabled, the Authentication Protocol PAP/CHAP options will not be available.
Save	N/A	Click Save button to save the settings.
Undo	N/A	Click Undo button to cancel the settings.

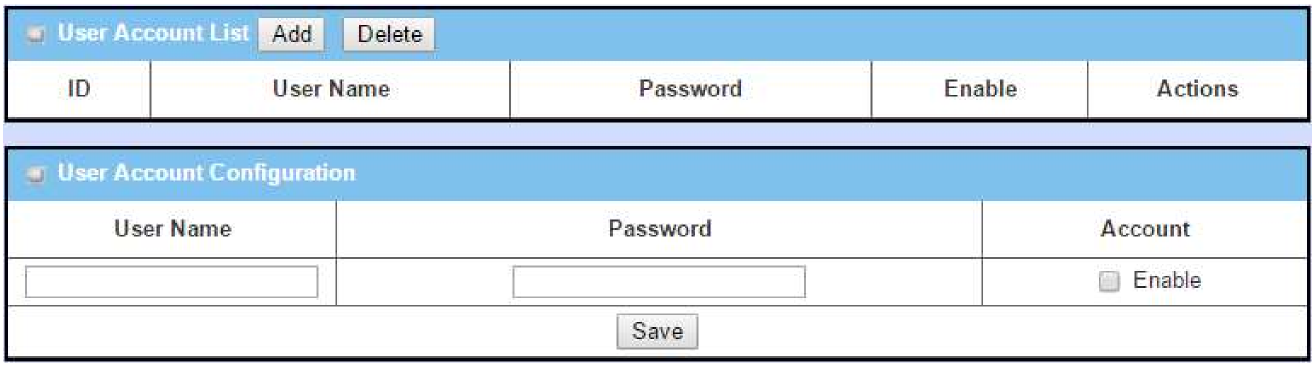


PPTP Server Status Refresh

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

PPTP Server Status Window

Item	Value setting	Description
PPTP Server Status	N/A	It displays the User Name, Remote IP, Remote Virtual IP, and Remote Call ID of the connected PPTP clients.



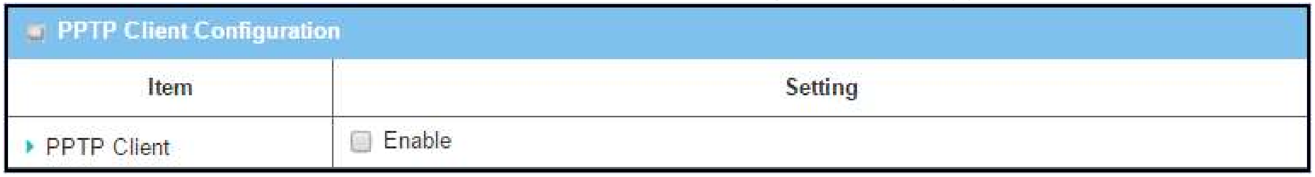
ID	User Name	Password	Enable	Actions

User Name	Password	Account
		□ Enable

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

As a PPTP Client

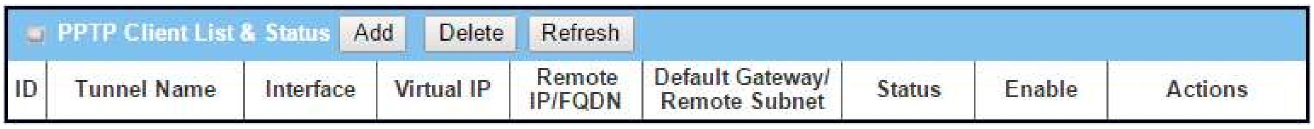
When select Client in Client/Server, a series PPTP Client Configuration will appear.



Item	Setting
PPTP Client	□ Enable

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

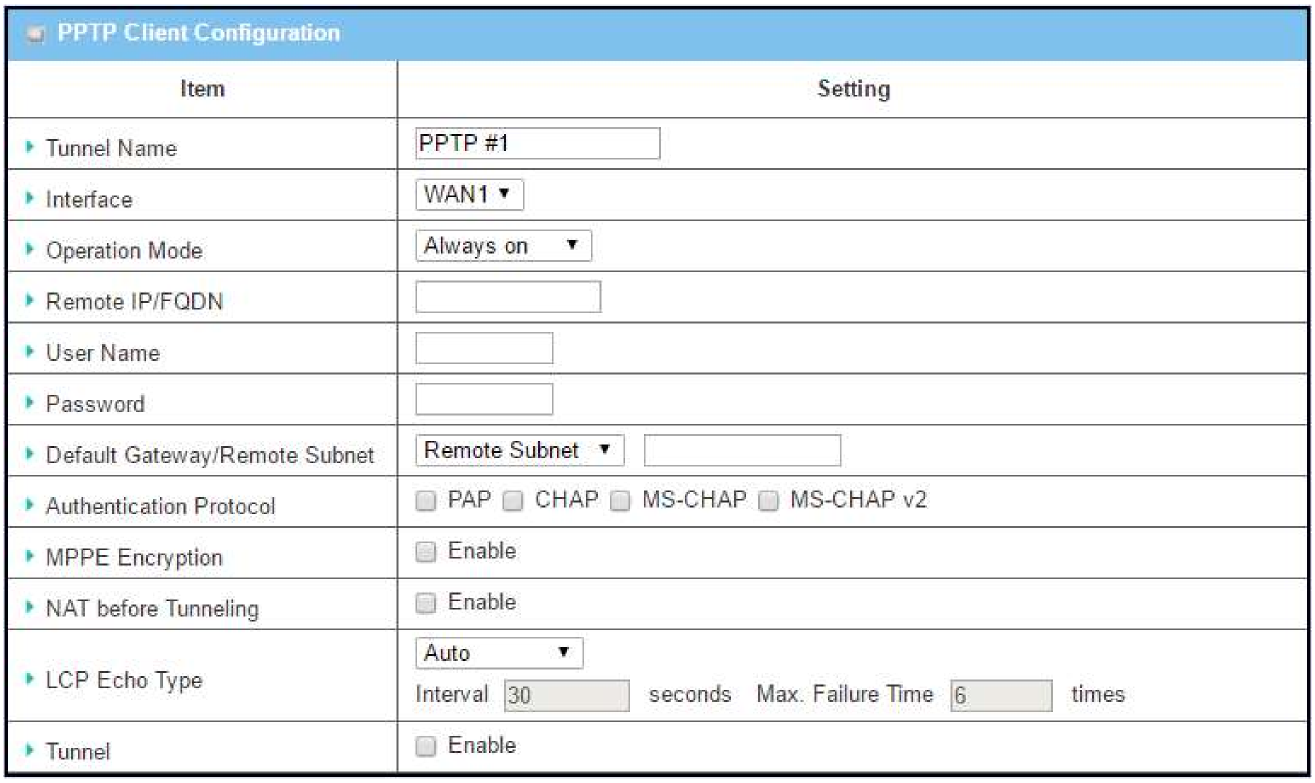
Create/Edit PPTP Client



PPTP Client List & Status Add Delete Refresh

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

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



PPTP Client Configuration

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

PPTP Client Configuration Window		
Item	**Value setting**	**Description**
Tunnel Name	A Must fill setting	Enter a tunnel name. Enter a name that is easy for you to identify.
Interface	1. A Must fill setting 2. WAN1 is selected by default	Select WAN interface on which PPTP tunneling is to be established.
Operation Mode	1. A Must fill setting 2. Alwasy on is selected by default	There are three available operation modes. Always On, Failover, Load Balance. **Failover/ Always** Define whether the PPTP client is a failover tunnel function or an always on tunnel. Note: If this PPTP is a failover tunneling, you will need to select a primary IPSec tunnel from which to failover to.

		Load Balance Define whether the PPTP tunnel connection will take part in load balance function of the gateway. You will not need to select which WAN interface as the system will automatically utilize the available WAN interfaces to balance traffic loads. For more details on WAN Load Balance, refer to Load Balance Usage in this manual. On gateway's web-based utility, go to Basic Network > WAN & Uplink > Load Balance tab.
Remote IP/FQDN	1. A Must fill setting. 2. Format can be a ipv4 address or FQDN	Enter the public IP address or the FQDN of the PPTP server.
Username	A Must fill setting	Enter the **Username** for this PPTP tunnel to be authenticated when connect to PPTP server.
Password	A Must fill setting	Enter the **Password** for this PPTP tunnel to be authenticated when connect to PPTP server.
Default Gateway / Remote Subnet	A Must fill setting	Specify a gateway for this PPTP tunnel to reach PPTP server. If the gateway uses its gateway IP address to connect to the internet to connect to the PPTP server then select Default Gateway, otherwise, specified a subnet and its netmask –the remote subnet, if the default gateway is not used to connect to the PPTP server. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24).
Authentication Protocol	1. A Must fill setting 2. Unchecked by default	Specify one ore multiple **Authentication Protocol** for this PPTP tunnel. Available authentication methods are **PAP/CHAP/MS-CHAP/MS-CHAPv2**
MPPE Encryption	1. Unchecked by default 2. an optional setting	Specify whether PPTP server supports **MPPE Protocol**. Click the **Enable** box to enable MPPE. Note: when MPPE Encryption is enabled, the Authentication Protocol PAP/CHAP options will not be available.
NAT before Tunneling	1. Unchecked by default 2. an optional setting	Check the **Enable** box to enable NAT function for this PPTP tunnel.
LCP Echo Type	Auto is set by default	Specify the LCP Echo Type for this PPTP tunnel. Auto, User-defined, Disable. **Auto** the system sets the Interval and Max. Failure Time. **User-defined** enter the Interval and Max. Failure Time. **Disable** disable the LCP Echo.
Tunnel	Unchecked by default	Check the **Enable** box to enable this PPTP tunnel.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.
Back	N/A	Click **Back** button to return to the previous page.

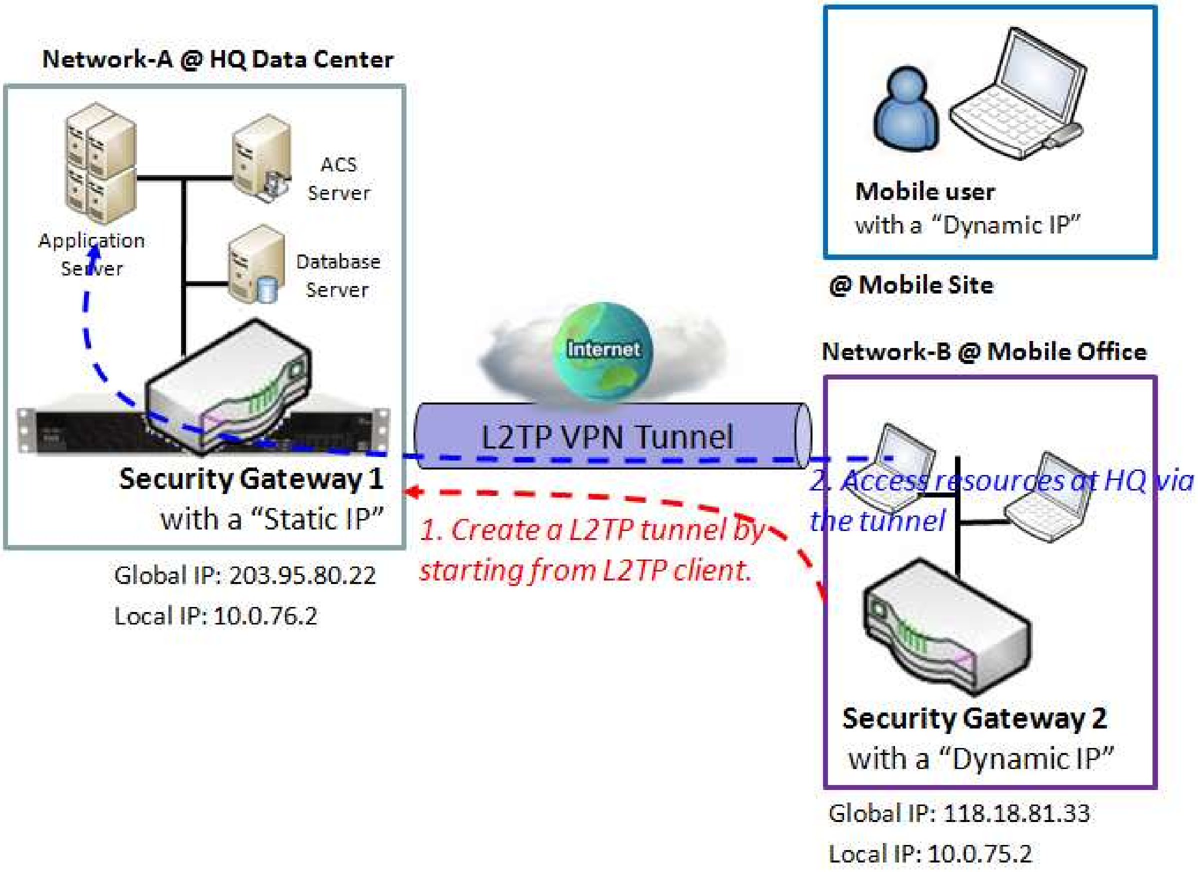
9.1.7 L2TP

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

Deploy a security gateway for local office and establish a virtual private network with the remote gateway of another office by using L2TP tunneling. So, all client hosts behind local security gateway can make data communication with others behind remote gateway.

Or when you are a mobile user with your notebook or carrying along a security gateway and you want to access the servers and database in company headquarters (HQ). Moreover, the security gateway in HQ supports the L2TP VPN server function. So you can dial in the HQ gateway and access the HQ resources by establishing an L2TP VPN tunnel. It is a virtual private network between your device and HQ gateway for your resource accessing.

L2TP VPN Server Scenario



Scenario Application Timing

Above diagram illustrates the security gateway at headquarters playing the L2TP VPN server role. The L2TP tunnel is established by starting from L2TP client, the Security Gateway 2 in Network-B or the mobile device, like notebook. All client hosts behind the Security Gateway 2 or the mobile device can access the resources in the Intranet of Network-A at headquarters via this established L2TP tunnel. Usually, these hosts at L2TP client peer access the Internet directly via the WAN interface of Security Gateway 2. Only the packets whose destination is in the dedicated subnet to Network-A will be transferred via the L2TP tunnel.

Scenario Description

L2TP Tunneling is a Client and Server based tunneling technology.

The L2TP Server must have a Static IP or a FQDN, and maintain a Client list (account / password); The Client may be a mobile user or mobile site, and requesting the L2TP tunnel connection with its account / password.

L2TP protocol is used for establishing an L2TP VPN tunnel.

Parameter Setup Example

For Network-A at HQ

Following 3 tables list the parameter configuration for above example diagram of L2TP VPN server in Network-A.

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

Configuration Path	[L2TP]-[Configuration]
L2TP	■ ***Enable***
Client/Server	**Server**

Configuration Path	[L2TP]-[L2TP Server Configuration]
L2TP Server	■ ***Enable***
L2TP over IPSec	■ ***Enable Preshare Key 12345678***
Server Virtual IP	***192.168.101.253***
IP Pool Starting Address	***10*** **(that means 192.168.101.10)**
IP Pool Ending Address	***50*** **(that means 192.168.101.50)**
Authentication Protocol	***MS-CHAP***
MPPE Encryption	■ ***Enable 128 bits***
Service Port	***1701***

Configuration Path	[L2TP]-[User Account Configuration]	
ID	**1**	**2**
User Name	***User-1***	***User-2***
Password	***1234***	***4321***
Account	■ ***Enable***	■ ***Enable***

Scenario Operation Procedure

In above diagram, Network-A is in the headquarters, and the subnet of its Intranet is 10.0.76.0/24. The security gateway for Network-A has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN interface. It serves as a L2TP server.

However, Network-B is in the mobile office and the subnet of its Intranet is 10.0.75.0/24. The security gateway for Network-B has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN interface. It serves as a L2TP client.

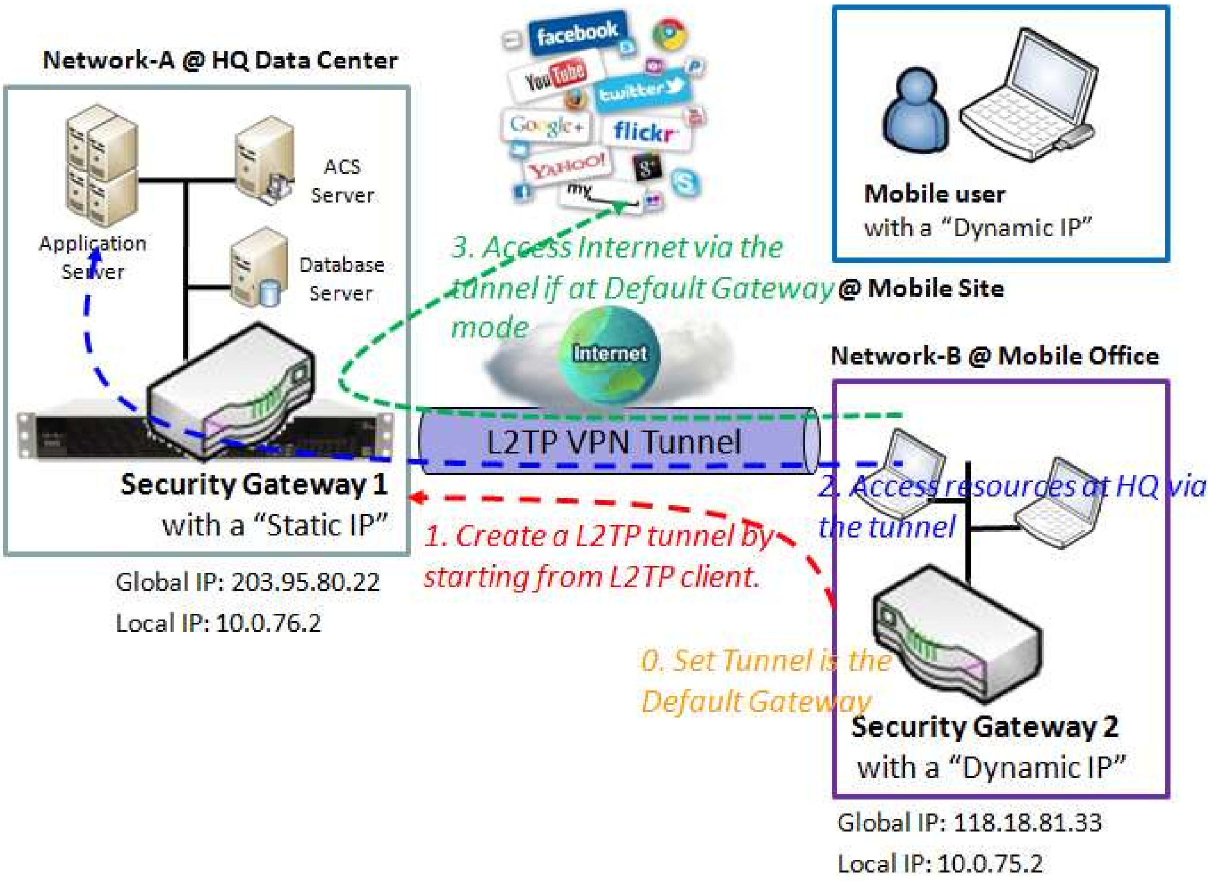
L2TP server provides two user accounts, User-1 and User-2, for L2TP clients dialing in.

Establish a L2TP VPN tunnel by starting from the L2TP client site. So both Intranets of 10.0.75.0/24 and

10.0.76.0/24 can securely communicate each other.

Finally, the client hosts in the Intranet of Network-B at mobile office can access the server or database resources in the Intranet of Network-A at HQ in a secured link.

L2TP VPN Client Scenario



Scenario Application Timing

Above diagram illustrates the Security Gateway 2 or the mobile device playing the L2TP VPN client role. The L2TP tunnel is established by the L2TP client making the tunnel connection request initiation and the Security Gateway 1 in Network-A of headquarters serves as the L2TP VPN server responding to the request. Once the tunnel has been established, all client hosts behind the Security Gateway 2 or the mobile device can access the resources in the Intranet of Network-A at headquarters via this established L2TP tunnel. Usually, these hosts at L2TP client peer access the Internet directly via the WAN interface of Security Gateway 2. Only the packets whose destination is in the dedicated subnet to Network-A will be transferred via the L2TP tunnel. But if L2TP client peer is configured to all packets are delivered via the L2TP tunnel, as shown in the diagram by configuring the L2TP tunnel is the default gateway at L2TP client peer, the Internet accessing packets will be also sent to the Security Gateway 1 in Network-A and be re-transferred to the Internet. That means the Internet accessing of L2TP Client peer is also controlled by the Security Gateway 1, the L2TP VPN server.

Scenario Description

L2TP Tunneling is a Client and Server based tunneling technology.

The L2TP Server must have a Static IP or a FQDN, and maintain a Client list (account / password). The Client may be a mobile user or mobile site, and requesting the L2TP tunnel connection with its account / password.

L2TP protocol is used for establishing a L2TP VPN tunnel.

The L2TP Client's "Default Gateway/Remote Subnet" setting determines how the Internet traffic from L2TP client site is handled.

The L2TP over IPSec is usually used for BYOD devices to establish a secure VPN tunnel between mobile employees and company office.

Parameter Setup Example

For Network-B at Mobile Office

Following 3 tables list the parameter configuration for above example diagram of L2TP VPN client in Network-B.

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

Configuration Path	[L2TP]-[Configuration]
L2TP	■ ***Enable***
Client/Server	***Client***

Configuration Path	[L2TP]-[L2TP Client Configuration]
L2TP Client	■ ***Enable***

Configuration Path	[L2TP]-[Configuration for A L2TP Client]
L2TP Client Name	***L2TP #1***
Interface	***WAN 1***
L2TP over IPSec	■ ***Enable*** Preshare Key: ***12345678***
Remote LNS IP/FQDN	***203.95.80.22***
Remote LNS Port	***1701***
User Name	***User-1***
Password	***1234***
Default Gateway/Remote Subnet	***Default Gateway***
Authentication Protocol	***MS-CHAP***
MPPE Encryption	■ ***Enable***
Service Port	***Auto***
Tunnel	■ ***Enable***

Scenario Operation Procedure

In above diagram, Network-A is in the headquarters, and the subnet of its Intranet is 10.0.76.0/24. The security gateway for Network-A has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN interface. It serves as a L2TP server.

However, Network-B is in the mobile office and the subnet of its Intranet is 10.0.75.0/24. The security gateway for Network-B has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN interface. It serves as a L2TP client.

The L2TP client uses "User-1" user account to dial in the L2TP server at HQ for establishing a L2TP VPN tunnel. So both Intranets of 10.0.75.0/24 and 10.0.76.0/24 can securely communicate each other.

Finally, the client hosts in the Intranet of Network-B at mobile office can access the server or database resources in the Intranet of Network-A at HQ in a secured link.

However, if the "Default Gateway/Remote Subnet" parameter in the Security Gateway 2 is configured to "Default Gateway", the Internet accessing of L2TP Client peer also go through the established L2TP VPN tunnel, and the Security Gateway 1 can control the accessing as same as the HQ resource accessing.

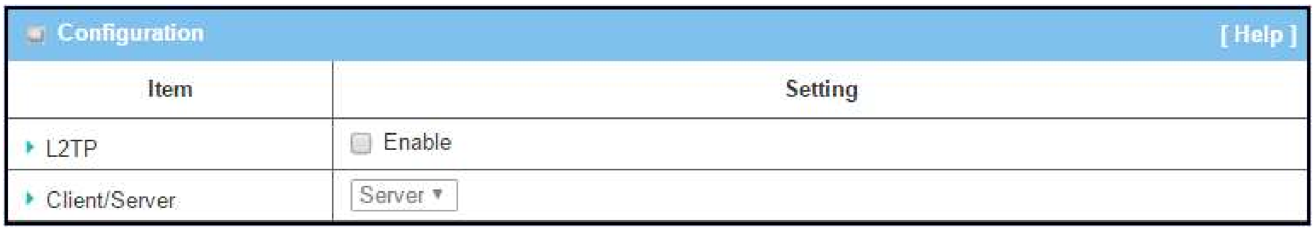
Please be noted that "Default Gateway/Remote Subnet" configuration item. There are two options, "Default Gateway" and "Remote Subnet". When you choose "Remote Subnet", you need specify one more setting: the remote subnet. It is for the Intranet of L2TP VPN server. So, at L2TP client peer, the packets whose destination is in the dedicated subnet will be transferred via the L2TP VPN tunnel. Others will be transferred based on current routing policy of the security gateway at L2TP client peer. But, if you choose "Default Gateway" option for the L2TP client peer, all packets will be transferred via the L2TP VPN tunnel. That means the remote L2TP VPN server gateway controls the flowing of any packets from the L2TP client peer. Certainly, those packets come through the L2TP VPN tunnel.

L2TP Setting

The L2TP setting allows user to create and configure L2TP tunnels. Before you proceed ensure that the VPN is enabled and saved. To enable VPN, go to **Security > VPN > Configuration** tab.

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

Enable L2TP



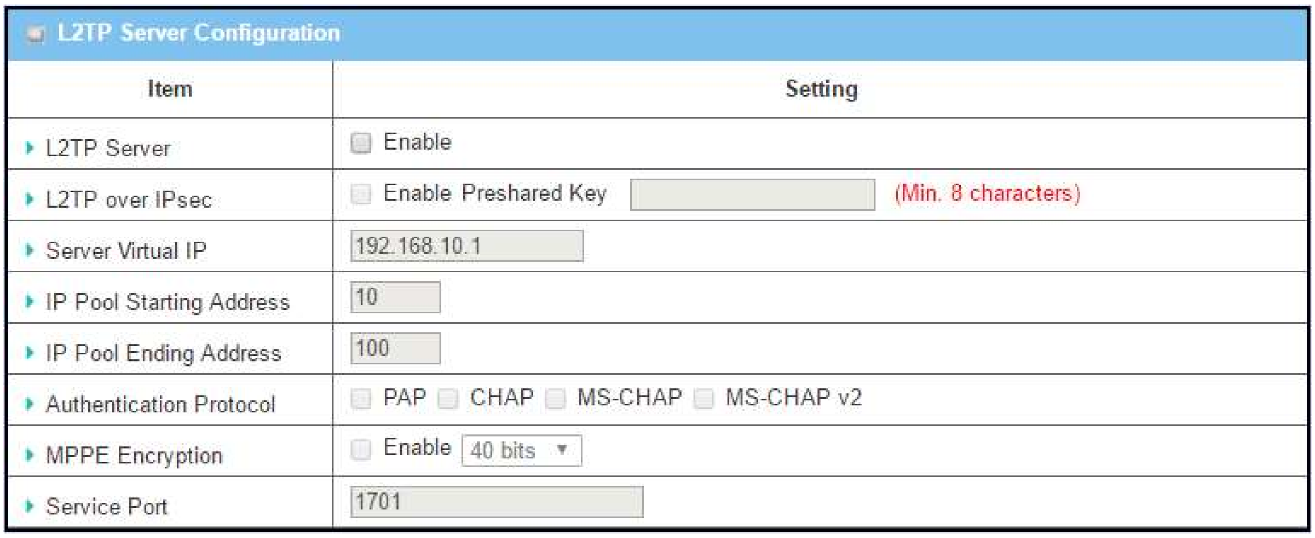
Configuration

Item	Setting
L2TP	□ Enable
Client/Server	Server ▾

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

As a L2TP Server

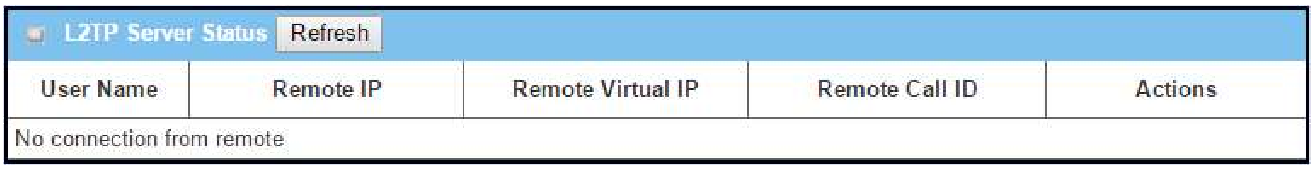
When select Server in Client/Server, the L2TP server Configuration will appear.



L2TP Server Configuration

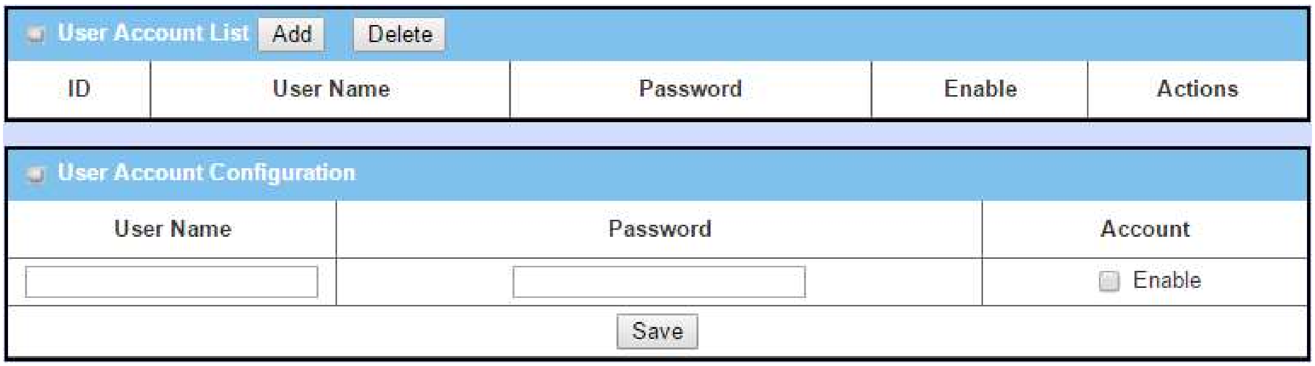
Item	Setting
L2TP Server	□ Enable
L2TP over IPsec	□ Enable Preshared Key (Min. 8 characters)
Server Virtual IP	192.168.10.1
IP Pool Starting Address	10
IP Pool Ending Address	100
Authentication Protocol	□ PAP □ CHAP □ MS-CHAP □ MS-CHAP v2
MPPE Encryption	□ Enable 40 bits ▾
Service Port	1701

L2TP Server Configuration		
Item	**Value setting**	**Description**
L2TP Server	The box is unchecked by default	When click the **Enable** box It will active L2TP server
L2TP over IPSec	The box is unchecked by default	When click the **Enable** box. It will enable L2TP over IPSec and need to fill in the Pre-shared Key.
Server Virtual IP	A Must filled setting	Specify the L2TP server Virtual IP It will set as this L2TP server local virtual IP
IP Pool Starting Address	A Must filled setting	Specify the L2TP server starting IP of virtual IP pool It will set as the starting IP which assign to L2TP client
IP Pool Ending Address	A Must filled setting	Specify the L2TP server ending IP of virtual IP pool It will set as the ending IP which assign to L2TP client
Authentication Protocol	A Must filled setting	Specify the **Authentication Protocol** which this L2TP server allowed. Selected PAP/CHAP/MS-CHAP/MS-CHAPv2 ->It will set as the authentication protocol which is checked.
MPPE Encryption	A Must filled setting	Specify the **MPPE Protocol** which this L2TP server allowed. When Click the **Enable** box ->It will enable MPPE Selected 40 bits/56 bits/128 bits ->It will set as the MPPE encryption which is chose. Note_1: If Enable box is be clock, Authentication Protocol PAP/CHAP will be available.
Service Port	A Must filled setting	Specify the **Service Port** which L2TP server use.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to recovery the configuration.



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	Show the L2TP client information which connect to this L2TP server. Click the **Refresh** button to renew the L2TP client information.



User Account List Add Delete

ID	User Name	Password	Enable	Actions

User Account Configuration

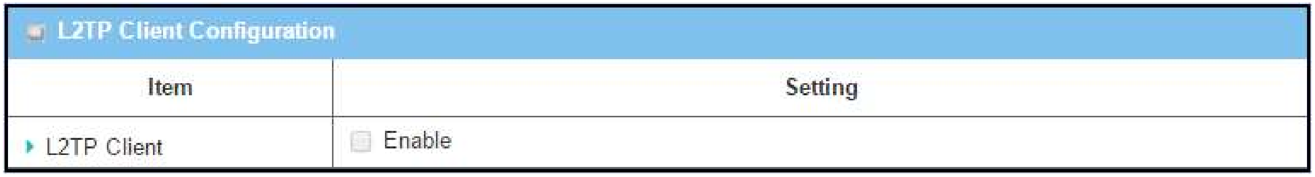
User Name	Password	Account
		□ Enable

Save

User Account List		
Item	**Value setting**	**Description**
User Account List	N/A	Specify the **User Account** which allow client to authenticate. Click **Add** button to add user account. Click **Delete** button to delete user account. Click **Enable** button to enable user account. Specify **Username** ->Fill in the username. Specify **Password** ->Fill in the password Click **save** button to save user account.

As a L2TP Client

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

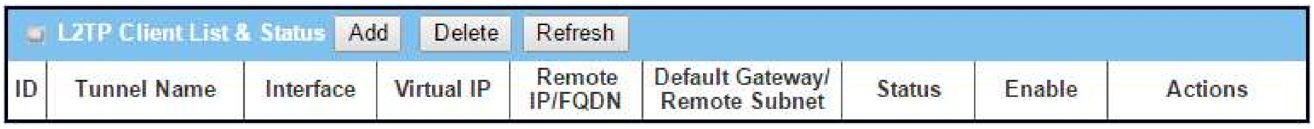


L2TP Client Configuration

Item	Setting
L2TP Client	□ Enable

L2TP Client Configuration		
Item Setting	**Value setting**	**Description**
L2TP Client	The box is unchecked by default	When click the **Enable** box It will activate L2TP Client.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to recovery the configuration.

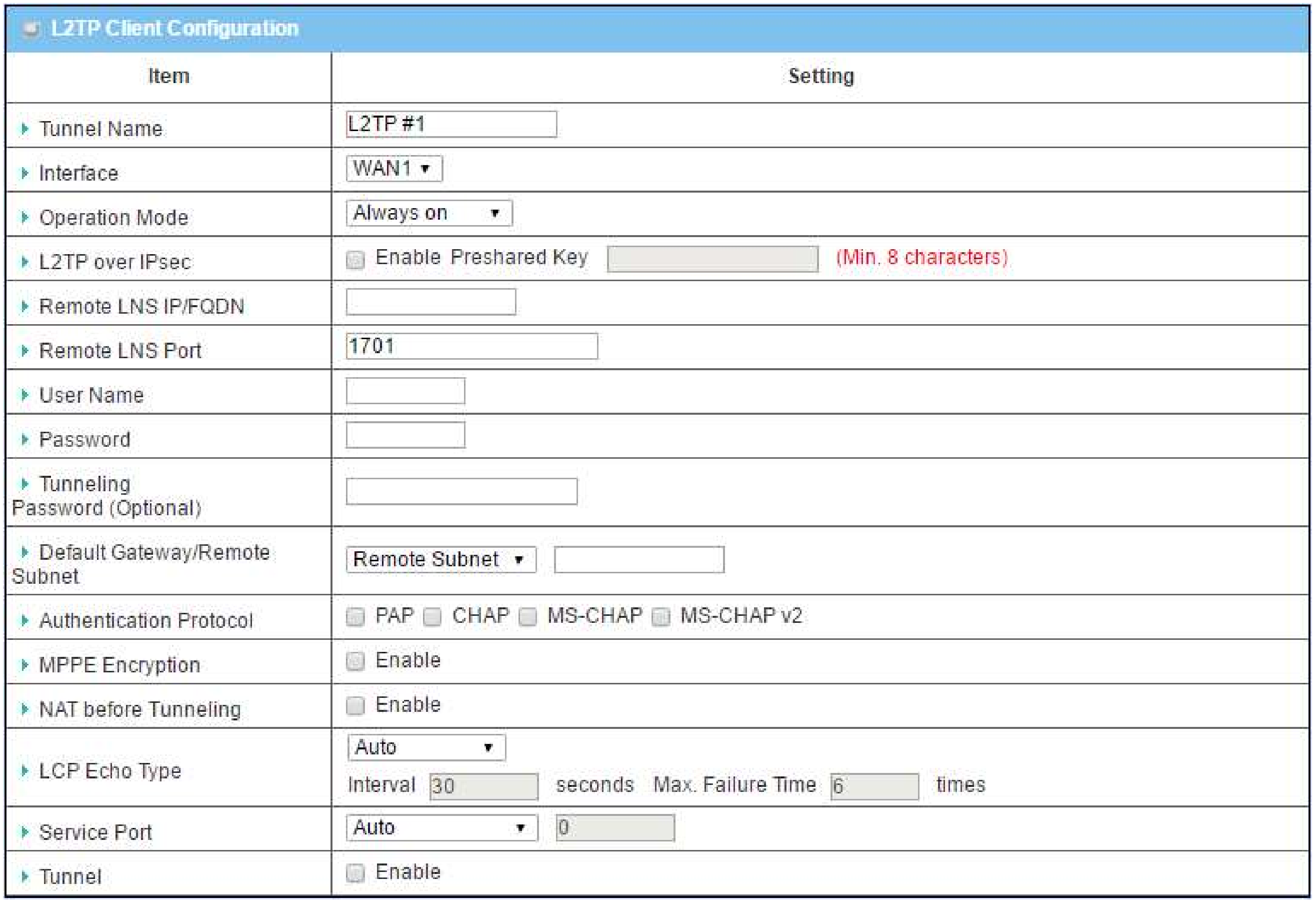
Create/Edit L2TP Client



L2TP Client List & Status [Add] [Delete] [Refresh]

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

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



L2TP Client Configuration

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

L2TP Client Configuration Item Setting	 Value setting	 Description
Tunnel Name	A Must filled setting	When fill in the name It will be used to identify it in the tunnel list
Interface	A Must filled setting	Define the selected interface to be the used for this L2TP tunnel Select **WAN-1** for this IPSec tunnel using. (WAN-1 is available only when WAN-1 interface is enabled) The same applies to other WAN interfaces (i.e. **WAN-2).**

Operation Mode	1. A Must fill setting 2. Alwasy on is selected by default	There are three available operation modes. Always On, Failover, Load Balance. **Failover/ Always** Define whether the L2TP client is a failover tunnel function or an always on tunnel. Note: If this L2TP is a failover tunneling, you will need to select a primary IPSec tunnel from which to failover to. **Load Balance** Define whether the L2TP tunnel connection will take part in load balance function of the gateway. You will not need to select which WAN interface as the system will automatically utilize the available WAN interfaces to balance traffic loads. For more details on WAN Load Balance, refer to Load Balance Usage in this manual. On gateway's web-based utility, go to Basic Network > WAN & Uplink > Load Balance tab.
L2TP over IPSec	The box is unchecked by default	When click the **Enable** box. It will enable L2TP over IPSec and need to fill in the Pre-shared Key.
Remote LNS IP/FQDN	A Must filled setting	Specify the **Remote LNS IP/FQDN** for this L2TP tunnel. Fill in the IP address or FQDN.
Remote LNS Port	A Must filled setting	Specify the **Remote LNS Port** for this L2TP tunnel. Fill in the value for LNS port.
Username	A Must filled setting	Specify the **Username** for this L2TP tunnel to authenticate when connect to server. Fill in the string as username.
Password	A Must filled setting	Specify the **Password** for this L2TP tunnel to authenticate when connect to server.
Tunneling Password(Optional)	The box is unchecked by default	Specify the **Tunneling Password** for this L2TP tunnel to authenticate.
Default Gateway / Remote Subnet	A Must filled setting	Specify Default Gateway/Remote Subnet for this L2TP tunnel. Selected Default Gateway ->The IP address box will not be available. Selected the **Remote Subnet** ->Filled the remote subnet address/remote subnet mask.
Authentication Protocol	A Must filled setting	Specify **Authentication Protocol** for this L2TP tunnel will can be used. Click the PAP/CHAP/MS-CHAP/MS-CHAP v2 ->The protocol will be enable which box is click.
MPPE Encryption	The box is unchecked by default	When click the **Enable** box ->It will enable MPPE for this L2TP tunnel. Note_1: If Enable box is be click, Authentication Protocol PAP/CHAP will be not available.
NAT before Tunneling	The box is unchecked by default	When click the **Enable** box ->It will enable NAT for this L2TP tunnel.
LCP Echo Type	A Must filled setting	Specify the LCP Echo Type for this L2TP tunnel.

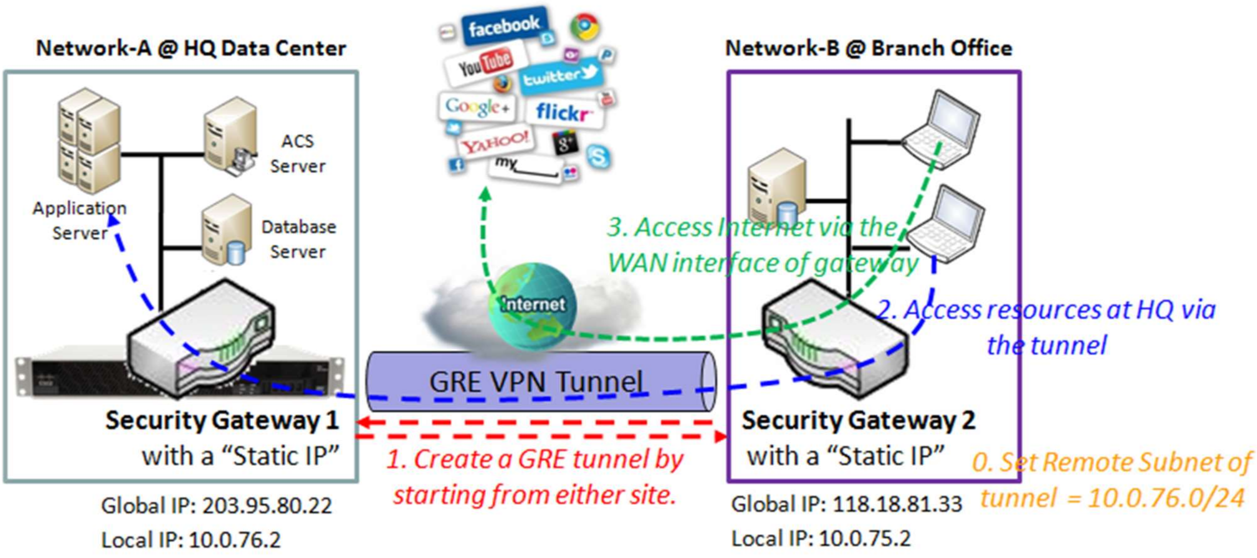
		Select **Auto** ->Auto setting the Interval and Max. Failure Time. Selected User-defined ->Fill in the Interval and Max. Failure Time for LCP. Selected **Disable** ->Disable LCP Echo and it will be not available.
Service Port	A Must filled setting	Specify the **Service Port** for this L2TP tunnel to use.
Tunnel	The box is unchecked by default	When click Enable It will enable this L2TP tunnel
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to recovery the configuration.
Back	N/A	Click the **Back** button to return the last page.

9.1.9 GRE

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

Deploy a security gateway for local office and establish a virtual private network with the remote gateway of another office by using GRE tunneling. So, all client hosts behind local security gateway can make data communication with others behind remote gateway. The most popular scenario is the security gateway is located at a branch office. Employees in the branch office want to use their client hosts or devices behind the security gateway to access the resources in headquarters. These resources are located in the Intranet of headquarters, and the security gateway in headquarters supports the GRE tunneling function. Then local security gateway can establish a GRE VPN tunnel with remote gateway in headquarters. Client hosts in these both Intranets of branch office and headquarters can make data communication each other.

GRE Tunnel at HQ Peer


Network-A @ HQ Data Center
Application Server
ACS Server
Database Server
Security Gateway 1
with a "Static IP"
Global IP: 203.95.80.22
Local IP: 10.0.76.2
Internet
GRE VPN Tunnel
1. Create a GRE tunnel by starting from either site.
3. Access Internet via the WAN interface of gateway
Network-B @ Branch Office
2. Access resources at HQ via the tunnel
Security Gateway 2
with a "Static IP"
0. Set Remote Subnet of tunnel = 10.0.76.0/24
Global IP: 118.18.81.33
Local IP: 10.0.75.2

Scenario Application Timing

Above diagram illustrates the security gateway in headquarters playing the GRE server role. In fact, the GRE tunnel establishment can be started from either site. The GRE tunnel is established by starting from GRE client, the Security Gateway 2 in Network-B. All client hosts behind the Security Gateway 2 or the mobile device can access the resources in the Intranet of Network-A at headquarters via this established GRE tunnel. Usually, these hosts at GRE client peer access the Internet directly via the

WAN interface of Security Gateway 2. Only the packets whose destination is in the dedicated subnet to Network-A will be transferred via the GRE tunnel.

Scenario Description

GRE Tunneling is similar to IPSec Tunneling, client requesting the tunnel establishment with the server. Both the client and the server must have a Static IP or a FQDN.

Any peer gateway can be worked as either a client or a server, even using the same set of configuration rule.

GRE Tunneling protocol is used for establishing a GRE VPN tunnel.

Parameter Setup Example

For Network-A at HQ

Following 2 tables list the parameter configuration for above example diagram of GRE VPN server in Network-A.

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

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

Configuration Path	[GRE]-[GRE Rule Configuration]
Tunnel Name	***GRE HQ***
Interface	***WAN 1***
Operation Mode	***Always on***
Tunnel IP	***203.95.80.22***
Remote IP	***118.18.81.33***
Key	***1234***
TTL	**255**
Default Gateway/Remote Subnet	***Remote Subnet 10.0.75.0/24***
Tunnel	■ ***Enable***

Scenario Operation Procedure

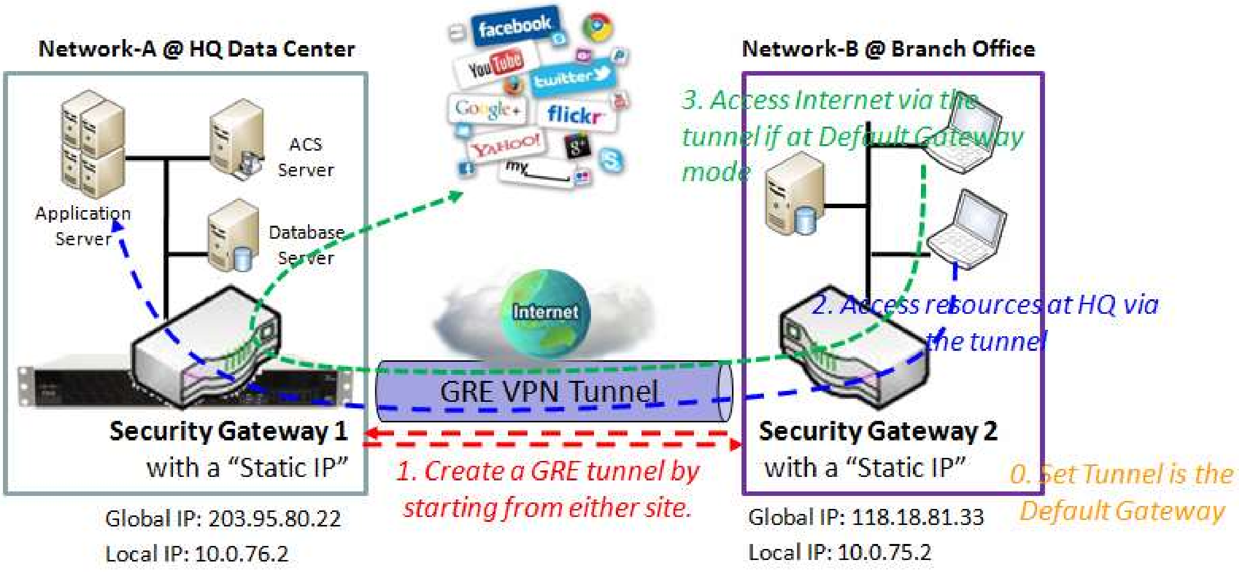
In above diagram, Network-A is in the headquarters, and the subnet of its Intranet is 10.0.76.0/24. The security gateway for Network-A has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN interface. It serves as a GRE server.

However, Network-B is in the mobile office and the subnet of its Intranet is 10.0.75.0/24. The security gateway for Network-B has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN interface. It serves as a GRE client.

Establish a GRE VPN tunnel by starting from the GRE client site. So both Intranets of 10.0.75.0/24 and 10.0.76.0/24 can communicate each other.

Finally, the client hosts in the Intranet of Network-B at mobile office can access the server or database resources in the Intranet of Network-A at HQ in a tunnel.

GRE Tunnel at Branch Office


Network-A @ HQ Data Center
Application Server
ACS Server
Database Server
Security Gateway 1
with a "Static IP"
Global IP: 203.95.80.22
Local IP: 10.0.76.2
Internet
GRE VPN Tunnel
1. Create a GRE tunnel by starting from either site.
Network-B @ Branch Office
3. Access Internet via the tunnel if at Default Gateway mode
2. Access resources at HQ via the tunnel
Security Gateway 2
with a "Static IP"
Global IP: 118.18.81.33
Local IP: 10.0.75.2
0. Set Tunnel is the Default Gateway

Scenario Application Timing

Above diagram illustrates the security gateway in headquarters playing the GRE client role. In fact, the GRE tunnel establishment can be started from either site. The GRE tunnel is established by starting from GRE client, the Security Gateway 2 in Network-B. All client hosts behind the Security Gateway 2 or the mobile device can access the resources in the Intranet of Network-A at headquarters via this established GRE tunnel. Usually, these hosts at GRE client peer access the Internet directly via the WAN interface of Security Gateway 2. Only the packets whose destination is in the dedicated subnet to Network-A will be transferred via the GRE tunnel. But if GRE client peer is configured to all packets are delivered via the GRE tunnel, as shown in the diagram by configuring the GRE tunnel is the default gateway at GRE client peer, the Internet accessing packets will be also sent to the Security Gateway 1 in Network-A and be re-transferred to the Internet. That means the Internet accessing of GRE Client peer is also controlled by the Security Gateway 1, the LGRE VPN server.

Scenario Description

GRE Tunneling is similar to IPSec Tunneling, client requesting the tunnel establishment with the server. Both the client and the server must have a Static IP or a FQDN.

Any peer gateway can be worked as either a client or a server, even using the same set of configuration.

GRE Tunneling protocol is used for establishing a GRE VPN tunnel.

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

The GRE Client's "Default Gateway/Remote Subnet" setting determines how the Internet traffic from GRE client site is handled.

Parameter Setup Example

For Network-B at Branch Office

Following 2 tables list the parameter configuration for above example diagram of GRE VPN server in Network-B.

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

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

Configuration Path	[GRE]-[GRE Rule Configuration]
Tunnel Name	*GRE BO*
Interface	*WAN 1*
Operation Mode	*Always on*
Tunnel IP	*118.18.81.33*
Remote IP	*203.95.80.22*
Key	*1234*
TTL	255
Default Gateway/Remote Subnet	*Default Gateway*
Tunnel	■ *Enable*

Scenario Operation Procedure

In above diagram, Network-A is in the headquarters, and the subnet of its Intranet is 10.0.76.0/24. The security gateway for Network-A has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN interface. It serves as a GRE server.

However, Network-B is in the branch office and the subnet of its Intranet is 10.0.75.0/24. The security gateway for Network-B has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN interface. It serves as a GRE client.

The GRE client in the Security Gateway 2 establishes a GRE VPN tunnel with the GRE server in the Security Gateway 1. So both Intranets of 10.0.75.0/24 and 10.0.76.0/24 can communicate each other.

Finally, the client hosts in the Intranet of Network-B at branch office can access the server or database resources in the Intranet of Network-A at HQ in a tunnel.

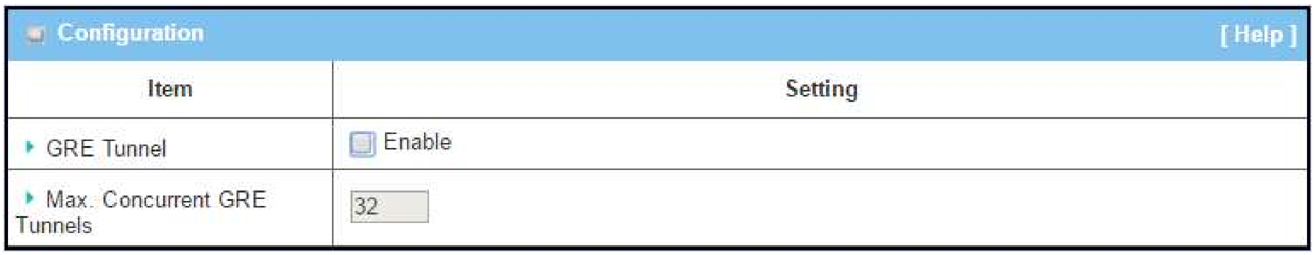
However, if the "Default Gateway/Remote Subnet" parameter in the Security Gateway 2 is configured to "Default Gateway", the Internet accessing of GRE Client peer also go through the established GRE VPN tunnel, and the Security Gateway 1 can control the accessing as same as the HQ resource accessing.

GRE Setting

The GRE setting allows user to create and configure GRE tunnels. Before you proceed, ensure that the VPN is enabled and saved. To enable VPN, go to **Security > VPN > Configuration** tab.

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

Enable GRE

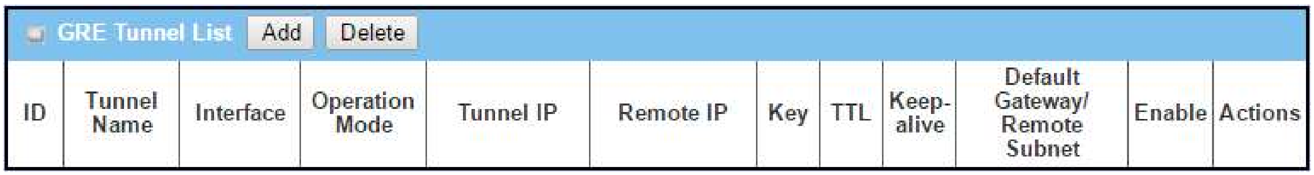


Configuration [Help]

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	1. 32 is set by default 2. Max. of 32 connections	It specifies the maximum number of simultaneous GRE tunnel connections. Note: The maximum supported tunnels can be different for the purchased gateway.
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

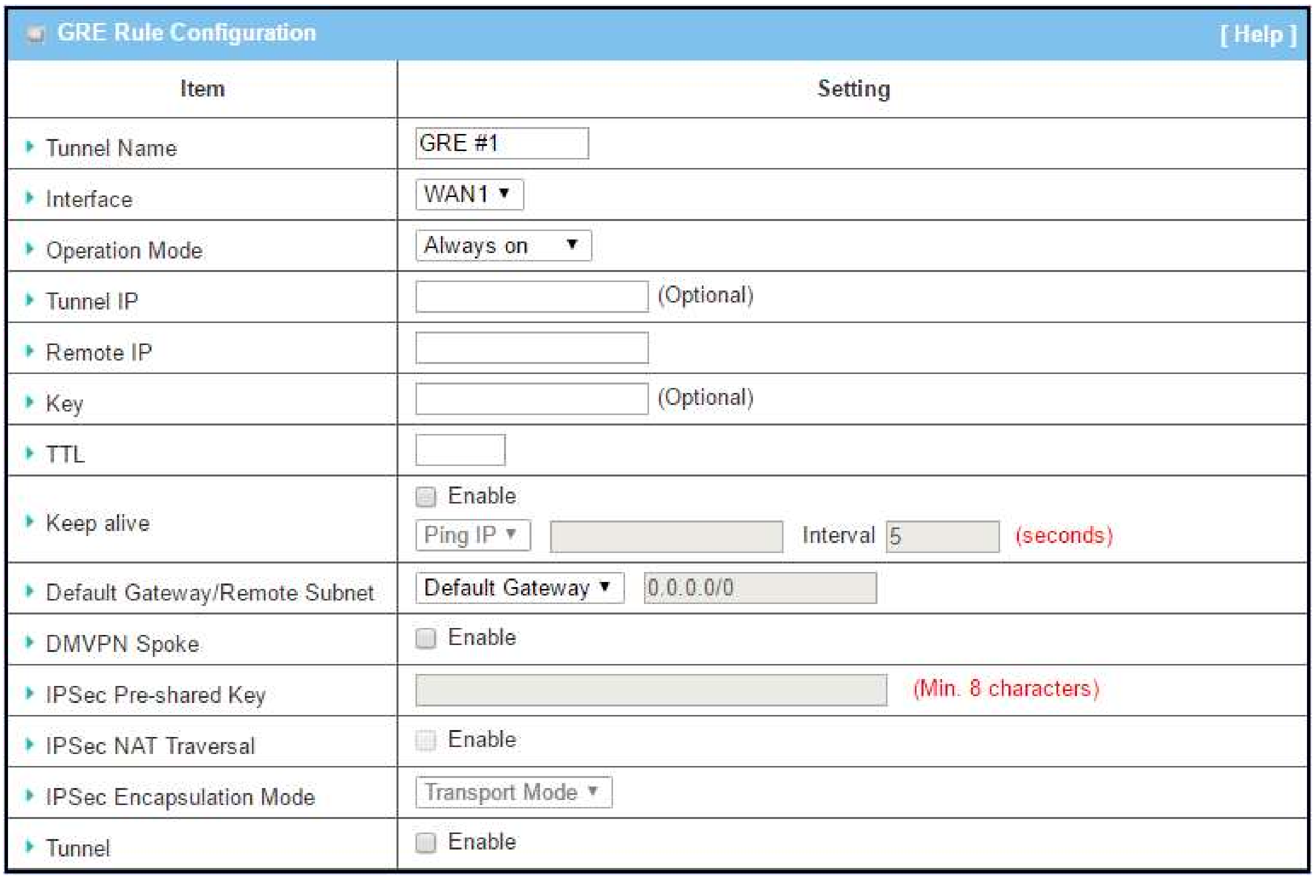
Create/Edit GRE tunnel



GRE Tunnel List Add Delete

ID	Tunnel Name	Interface	Operation Mode	Tunnel IP	Remote IP	Key	TTL	Keep-alive	Default Gateway/ Remote Subnet	Enable	Actions

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



GRE Rule Configuration [Help]

Item	Setting
Tunnel Name	GRE #1
Interface	WAN1 ▾
Operation Mode	Always on ▾
Tunnel IP	(Optional)
Remote IP	
Key	(Optional)
TTL	
Keep alive	□ Enable Ping IP ▾ Interval 5 (seconds)
Default Gateway/Remote Subnet	Default Gateway ▾ 0.0.0.0/0
DMVPN Spoke	□ Enable
IPSec Pre-shared Key	(Min. 8 characters)
IPSec NAT Traversal	□ Enable
IPSec Encapsulation Mode	Transport Mode ▾
Tunnel	□ Enable

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

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

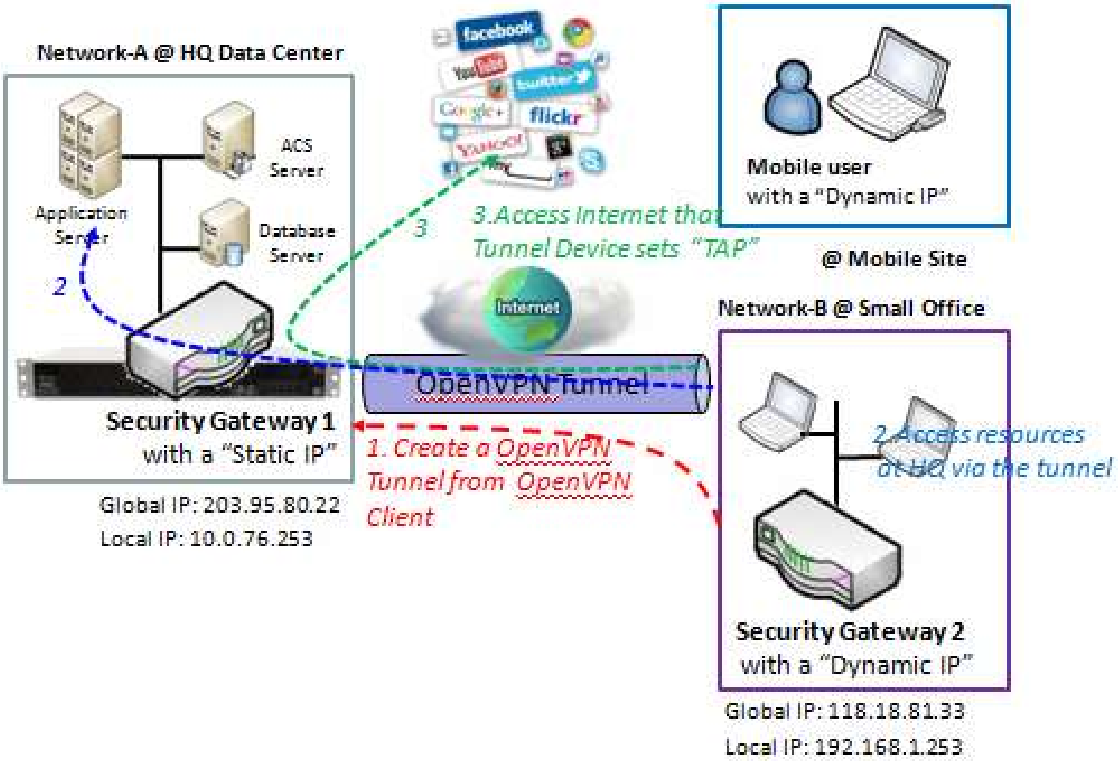
9.1.b OpenVPN

OpenVPN is an application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls. OpenVPN allows peers to authenticate each other using a Static key or certificates.When used in a multi-client-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority. It uses the OpenSSL encryption library extensively, as well as the SSLv3/TLSv1 protocol, and contains many security and control features.

Deploy a security gateway for local office and establish a virtual private network with the remote gateway of another office by using OpenVPN. So, all client hosts behind local security gateway can make data communication with others behind remote gateway.

In the case when you are a mobile user with your notebook or carrying along a security gateway to access the servers and database in company headquarters (HQ). And that the security gateway in HQ supports the OpenVPN server function. You can dial in the HQ gateway and access the HQ resources by establishing an OpenVPN tunneling. It is a virtual private network between your device and HQ gateway for your resource accessing.

OpenVPN Server Scenario



Scenario Application Timing

Above diagram illustrates the security gateway at headquarters playing the OpenVPN server role. The OpenVPN tunnel is established by starting from OpenVPN client, the Security Gateway 2 in Network-B or the mobile device, like notebook. All client hosts behind the Security Gateway 2 or the mobile device can access the resources in the Intranet of Network-A at headquarters via this established OpenVPN tunnel. Usually, these hosts at OpenVPN client peer access the Internet directly via the WAN interface of Security Gateway 2. Only the packets whose destination is in the dedicated subnet to Network-A will be transferred via the OpenVPN tunnel.

Scenario Description

OpenVPN Tunneling is a Client and Server based tunneling technology. The OpenVPN Server must have a Static IP or a FQDN, and maintain a Client list. The Client may be a mobile user or mobile site, and requesting the OpenVPN tunnel connection.

Parameter Setup Example

For Network-A at HQ, following tables list the parameter configuration for above example diagram of OpenVPN server in Network-A.

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

Configuration Path	[OpenVPN]-[Configuration]

OpenVPN	■ ***Enable***
Server/Client	**Server Configuration**

Configuration Path	[OpenVPN]-[OpenVPN Server Configuration]
OpenVPN Server	■ ***Enable***
Protocol	***TCP***
Port	***443***
Tunnel Device	***TAP*** ***PS: TAP also called "Bridging" behaves like a real network adapter and Broadcast traffic can transport.*** ***TUN called "Routing" transports only layer 3 IP packets. The user has to add routing rule according to the environment so that packets transfer smoothly.***
Authorization Mode	***TLS*** ***CA Cert: RootCA, Server Cert: Local.crt*** ***DH PEM : Default*** ***-----BEGIN DH PARAMETERS-----*** ***MIGHAoGBAMq4z88pL8X1dzmDmnr7nyV3w3L1rDU4Q+4SJiGQjR6b2nb4tf9jw/QJ*** ***W/ENgduKKXsltYSAzOZ9gXoNxwFGc9nKd4LfGpjQl9lIoHTp0eTdb9b5EKeR6B7h*** ***QxkfLBwVv1YZh9oUXm6pdewpg2QdZ2KtiOlMpgsJyaqRMQ3MlNB7AgEC*** ***-----END DH PARAMETERS-----*** ***PS: Security Gateway 1 is the role of RootCA and trusted CA.***
IP Pool Starting Address	***10.0.76.100***
IP Pool Ending Address	***10.0.76.150***
Gateway	***10.0.76.253***
Netmask	***255.255.255.0/24***
Encryption Cipher	***Blowfish***
Hash Algorithm	**SHA-1**

Scenario Operation Procedure

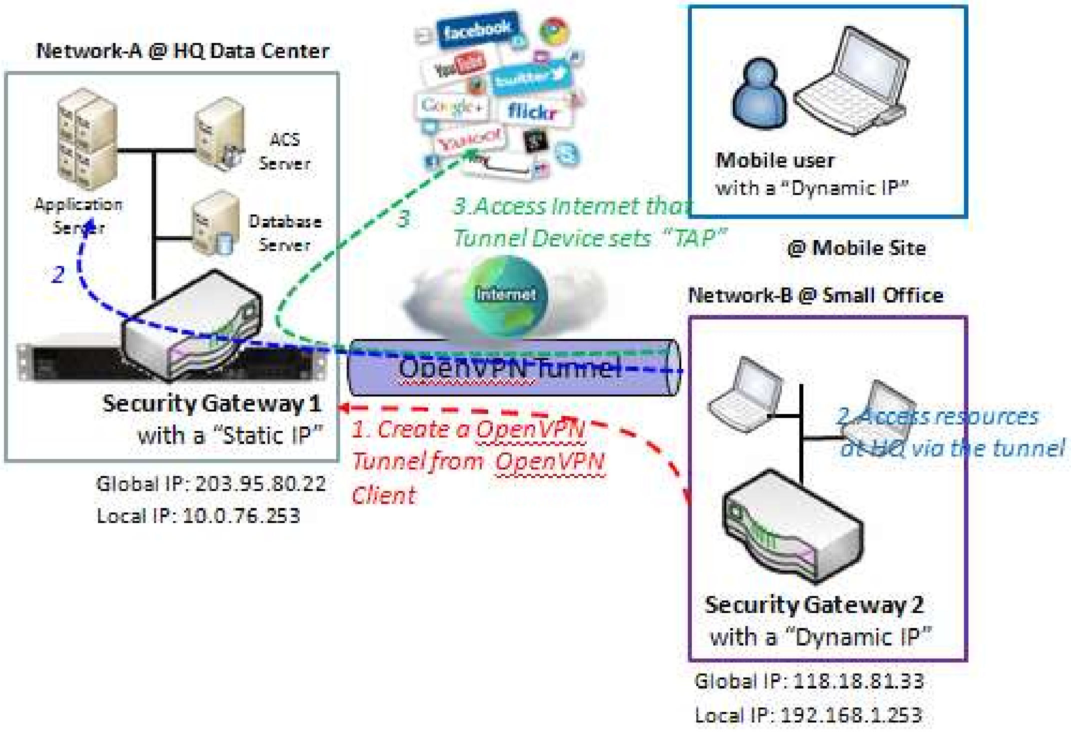
In above diagram, Network-A is in the headquarters, and the subnet of its Intranet is 10.0.76.0/24. The security gateway for Network-A has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN interface. It serves as an OpenVPN server.

Network-B is in the mobile office and the subnet of its Intranet is 10.0.75.0/24. The security gateway for Network-B has the IP address of 192.168.1.253 for LAN interface and 118.18.81.33 for WAN interface. It serves as an OpenVPN client.

Establish an OpenVPN VPN tunnel by starting from the OpenVPN client site. So hosts in Network-B can access hosts or servers in Network-A. But can't access from Network-A to Network-B.

To communicate each other securely between Intranets of 10.0.75.0/24 and 192.168.1.0/24, please add route policy according to the environment by checking the "Enable" box of Advanced Configuration.

OpenVPN Client Scenario



Scenario Application Timing

Above diagram illustrates the Security Gateway 2 or the mobile device playing the OpenVPN VPN client role. The OpenVPN tunnel is established by the OpenVPN client making the tunnel connection request initiation and the Security Gateway 1 in Network-A of headquarters serves as the OpenVPN server responding to the request. Once the tunnel has been established, all client hosts behind the Security Gateway 2 or the mobile device can access the resources in the Intranet of Network-A at headquarters via this established OpenVPN tunnel. Moreover, these hosts at OpenVPN client peer access the Internet directly via the WAN interface of Security Gateway 1. As shown in the diagram by configuring the OpenVPN tunnel set "TAP" for OpenVPN client peer, the Internet accessing packets will be also sent to the Security Gateway 1 in Network-A and be re-transferred to the Internet. That means the Internet accessing of OpenVPN Client peer is also controlled by the Security Gateway 1, the OpenVPN VPN server.

Scenario Description

OpenVPN Tunneling is a Client and Server based tunneling technology.

The OpenVPN Server must have a Static IP or a FQDN, and maintain a Client list; The Client may be a mobile user or mobile site, and requesting the OpenVPN tunnel connection.

OpenVPN protocol is used for establishing an OpenVPN tunnel.

Parameter Setup Example

For Network-B at Mobile Office, following 3 tables list the parameter configuration for above example diagram of OpenVPN VPN client in Network-B.

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

Configuration Path	[OpenVPN]-[Configuration]
OpenVPN	■ *Enable*
Server/Client	Client Configuration

Configuration Path	[OpenVPN]-[OpenVPN Client Configuration]
OpenVPN Client Name	Client1
Interface	WAN1
Protocol	*TCP*
Port	*443*
Tunnel Device	*TAP* *PS: TAP also called "Bridging" behaves like a real network adapter and Broadcast traffic can transport.* *TUN called "Routing" transports only layer 3 IP packets. The user has to add routing rule according to the environment so that packets transfer smoothly.*
Remote IP/FQDN	*203.95.80.22*
	10.0.76.0/24
Authorization Mode	*TLS* *CA Cert: RootCA, Client Cert: Remote.crt*
Encryption Cipher	*Blowfish*
Hash Algorithm	SHA-1

Scenario Operation Procedure

In above diagram, Network-A is in the headquarters, and the subnet of its Intranet is 10.0.76.0/24. The security gateway for Network-A has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN interface. It serves as an OpenVPN server.

However, Network-B is in the mobile office and the subnet of its Intranet is 10.0.75.0/24. The security gateway for Network-B has the IP address of 192.168.1.253 for LAN interface and 118.18.81.33 for WAN interface. It serves as an OpenVPN client.

The OpenVPN client dials in the OpenVPN server at HQ for establishing an OpenVPN tunnel. So hosts in Network-B can access hosts or servers in Network-A. But can't access from Network-A to Network-B.

However, if the "Default Gateway/Remote Subnet" parameter in the Security Gateway 2 is configured to "Default Gateway", the Internet accessing of OpenVPN Client peer also go through the established

OpenVPN VPN tunnel, and the Security Gateway 1 can control the accessing as same as the HQ resource accessing.

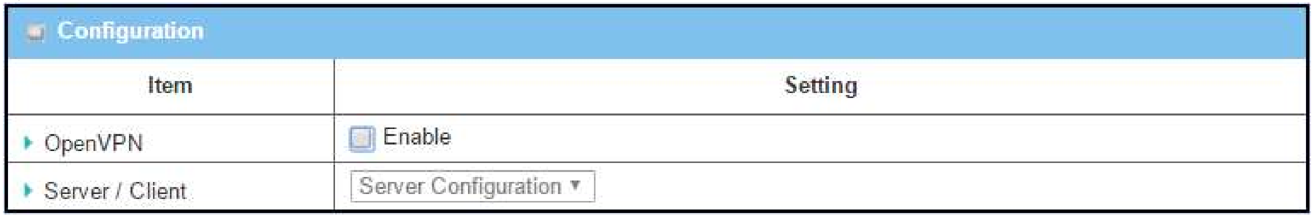
Open VPN Setting

The OpenVPN setting allows user to create and configure OpenVPN tunnels. Before you proceed ensure that the VPN is enabled and saved. To enable VPN, go to **Security > VPN > Configuration** tab.

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

Enable OpenVPN

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



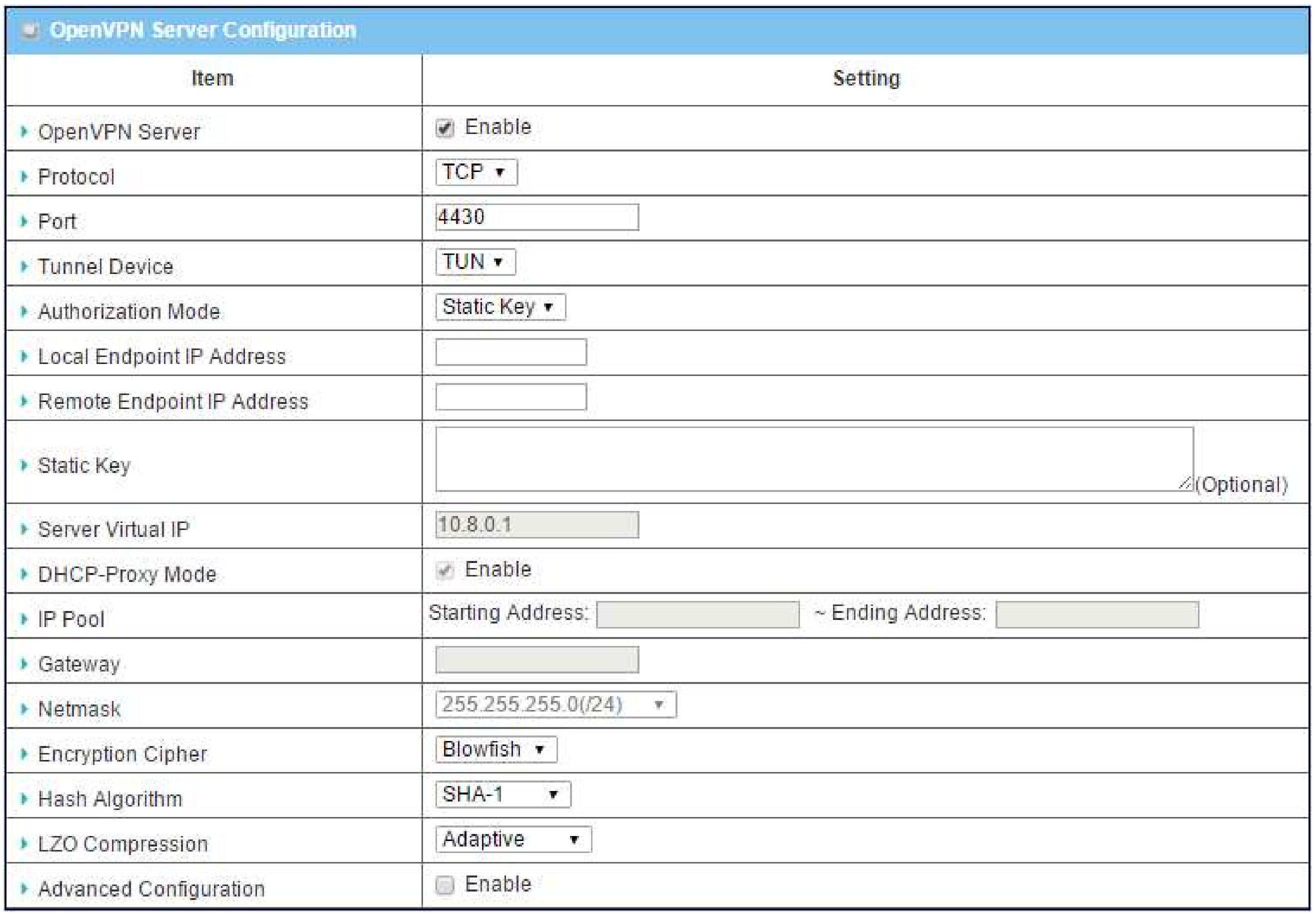
Configuration

Item	Setting
OpenVPN	□ Enable
Server / Client	Server Configuration ▾

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 Configuration** is selected, as the name indicated, server configuration will be displayed below for further setup. When **Client Configuration** is selected, you can specify the client settings in another client configuration window.

As an OpenVPN Server

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



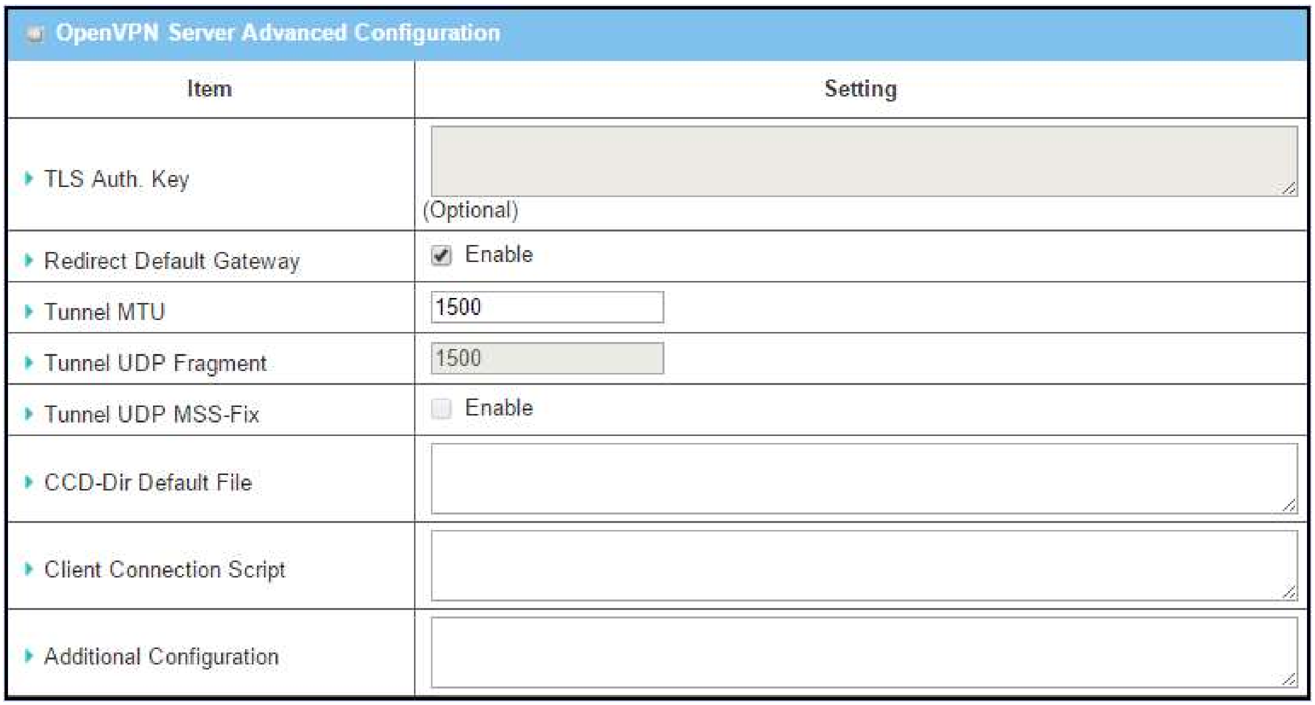
OpenVPN Server Configuration

Item	Setting
OpenVPN Server	☑ Enable
Protocol	TCP ▾
Port	4430
Tunnel Device	TUN ▾
Authorization Mode	Static Key ▾
Local Endpoint IP Address	
Remote Endpoint IP Address	
Static Key	(Optional)
Server Virtual IP	10.8.0.1
DHCP-Proxy Mode	☑ Enable
IP Pool	Starting Address: ~ Ending Address:
Gateway	
Netmask	255.255.255.0(/24) ▾
Encryption Cipher	Blowfish ▾
Hash Algorithm	SHA-1 ▾
LZO Compression	Adaptive ▾
Advanced Configuration	□ Enable

OpenVPN Server Configuration		
Item	**Value setting**	**Description**
OpenVPN Server	The box is unchecked by default.	Click the **Enable** to activate OpenVPN Server functions.
Protocol	1. A Must filled setting 2. By default **TCP** is selected.	Define the selected **Protocol** for connecting to the OpenVPN Server. • Select **TCP , or TCP /UDP** -> The TCP protocol will be used to access the OpenVPN Server, and **Port** will be set as 443 automatically. • Select **UDP** -> The UDP protocol will be used to access the OpenVPN Server, and **Port** will be set as 1194 automatically.
Port	1. A Must filled setting 2. By default **4430** is set.	Specify the **Port** for connecting to the OpenVPN Server.
Tunnel Device	1. A Must filled setting 2. By default **TUN** is selected.	Specify the type of **Tunnel Device** for connecting to the OpenVPN Server. It can be **TUN** for TUN tunnel device, or **TAP** for TAP tunnel device.
Authorization Mode	1. A Must filled setting 2. By default **Static Key** is selected.	Specify the authorization mode for the OpenVPN Server. • **Static Key** ->The OpenVPN will use static key authorization mode, and the following

		items **Local Endpoint IP Address**, **Remote Endpoint IP Address** and **Static Key** will be displayed. ● **TLS** ->The OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Server Cert.** and **DH PEM** will be displayed. **CA Cert.** could be generated in Certificate. Refer to **Object Definition** > **Certificate** > **Trusted Certificate**. **Server Cert.** could be generated in Certificate. Refer to **Object Definition** > **Certificate** > **My Certificate**. **DH PEM** should let user enter the content.
Local Endpoint IP Address	A Must filled setting	Specify the **Local Endpoint IP Address**. Note_1: Local Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Remote Endpoint IP Address	A Must filled setting	Specify the **Remote Endpoint IP Address**. Note_1: Remote Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Static Key	A Must filled setting	Specify the **Static Key**. Note_1: Static Key will be available only when Static Key is chosen in Authorization Mode.
Server Virtual IP	A Must filled setting	Specify the **Server Virtual IP**. Note_1: Server Virtual IP will be available only when TLS is chosen in Authorization Mode.
DHCP-Proxy Mode	1. A Must filled setting 2. The box is checked by default.	Specify the **DHCP-Proxy Mode**. Note_1: DHCP-Proxy Mode will be available only when TAP is chosen in Tunnel Device.
IP Pool	A Must filled setting	Specify the virtual **IP pool** for the OpenVPN server. You have to specify the **Starting Address** and **Ending Address** as the IP address pool for the OpenVPN clients. Note_1: IP Pool will be available only when TAP is chosen in Tunnel Device and DHCP-Proxy Mode is unchecked.
Gateway	A Must filled setting	Specify the **Gateway** for the OpenVPN server. Note_1: Gateway will be available only when TAP is chosen in Tunnel Device and DHCP-Proxy Mode is unchecked.
Netmask	By default **- select one -** is selected.	Specify the **Netmask** for the OpenVPN server. Note_1: Netmask will be available when TAP is chosen in Tunnel Device and DHCP-Proxy Mode is unchecked. Note_2: Netmask will be available when TUN is chosen in Tunnel Device.
Encryption Cipher	By default **Blowfish** is selected.	Specify the **Encryption Cipher.** It can be **Blowfish/AES-256/AES-192/AES-128/None.**
Hash Algorithm	By default **SHA-1** is selected.	Specify the **Hash Algorithm** It can be **SHA-1/MD5/MD4/SHA2-256/SHA2-512/None.**
LZO Compression	By default **Adaptive** is selected.	Specify the **LZO Compression** scheme. It can be **Adaptive/YES/NO/NO Adaptive.**
Advanced Configuration	The box is unchecked by default.	Specify the **Advanced Configuration** setting for the OpenVPN server. If it is checked, **Advanced Configuration** will be displayed below.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **Undo** to cancel the changes.

When selected Advanced Configuration in OpenVPN Server Configuration -



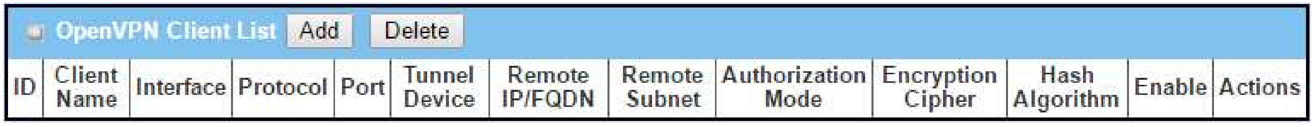
OpenVPN Server Advanced Configuration

Item	Setting
TLS Auth. Key	(Optional)
Redirect Default Gateway	☑ Enable
Tunnel MTU	1500
Tunnel UDP Fragment	1500
Tunnel UDP MSS-Fix	□ Enable
CCD-Dir Default File	
Client Connection Script	
Additional Configuration	

OpenVPN Server Advanced Configuration		
Item	**Value setting**	**Description**
TLS Auth. Key	String format: any text	Specify the **TLS Auth. Key.** Note_1: TLS Auth. Key will be available only when TLS is chosen in Authorization Mode.
Redirect Default Gateway	The box is checked by default	Check the box to enable the **Redirect Default Gateway.**
Tunnel MTU	1. A Must filled setting 2. The value is 1500 by default	Specify the **Tunnel MTU.**
Tunnel UDP Fragment	The value is 1500 by default	Specify the **Tunnel UDP Fragment.** Note_1: Tunnel UDP Fragment will be available only when UDP is chosen in Protocol.
Tunnel UDP MSS-Fix	The box is unchecked by default.	Check the box to enable the **Tunnel UDP MSS-Fix.** Note_1: Tunnel UDP MSS-Fix will be available only when UDP is chosen in Protocol.
CCD-Dir Default File	String format: any text	Specify the **CCD-Dir Default File.**
Client Connection Script	String format: any text	Specify the **Client Connection Script.**
Additional Configuration	String format: any text	Specify the **Additional Configuration.**

As an OpenVPN Client

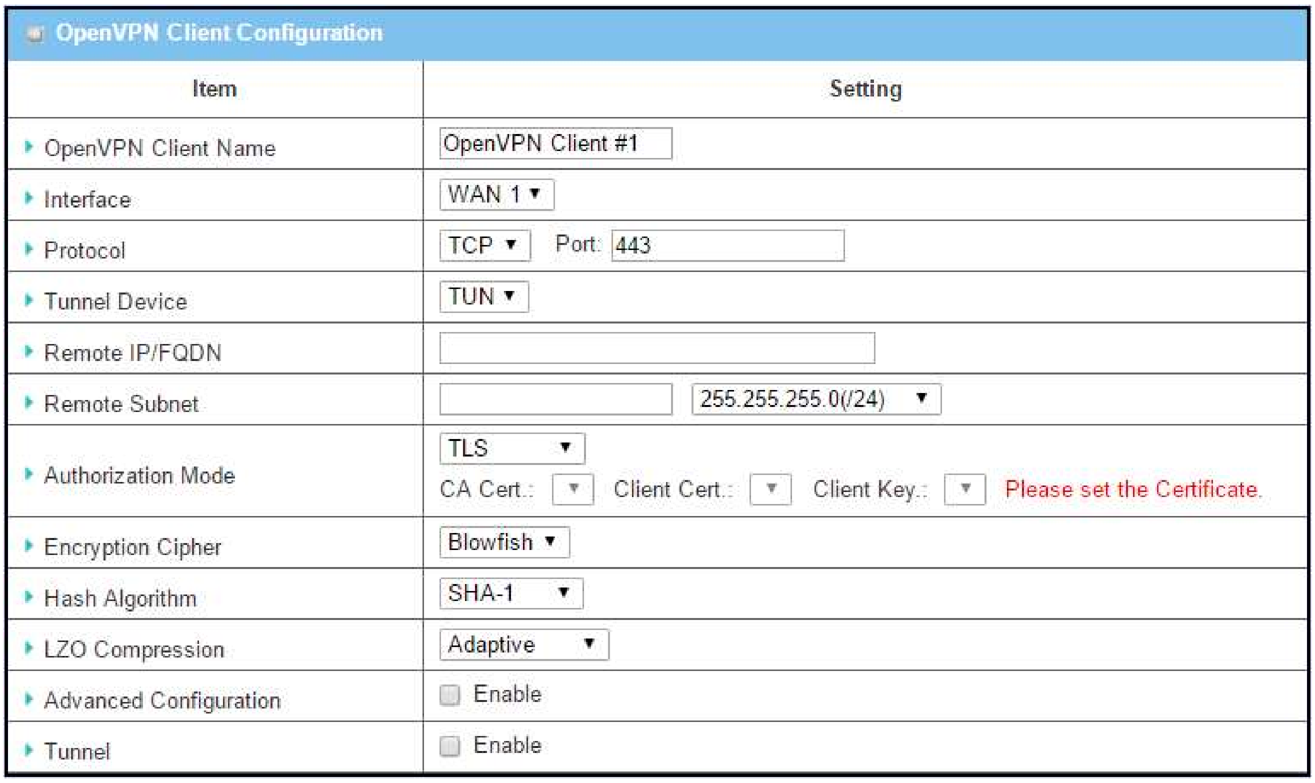
If **Client Configuration** is selected, an OpenVPN Client List screen will appear.



OpenVPN Client List Add Delete

ID	Client Name	Interface	Protocol	Port	Tunnel Device	Remote IP/FQDN	Remote Subnet	Authorization Mode	Encryption Cipher	Hash Algorithm	Enable	Actions

When Add/Edit button is applied, a series of OpenVPN Client Configuration will appear.



OpenVPN Client Configuration

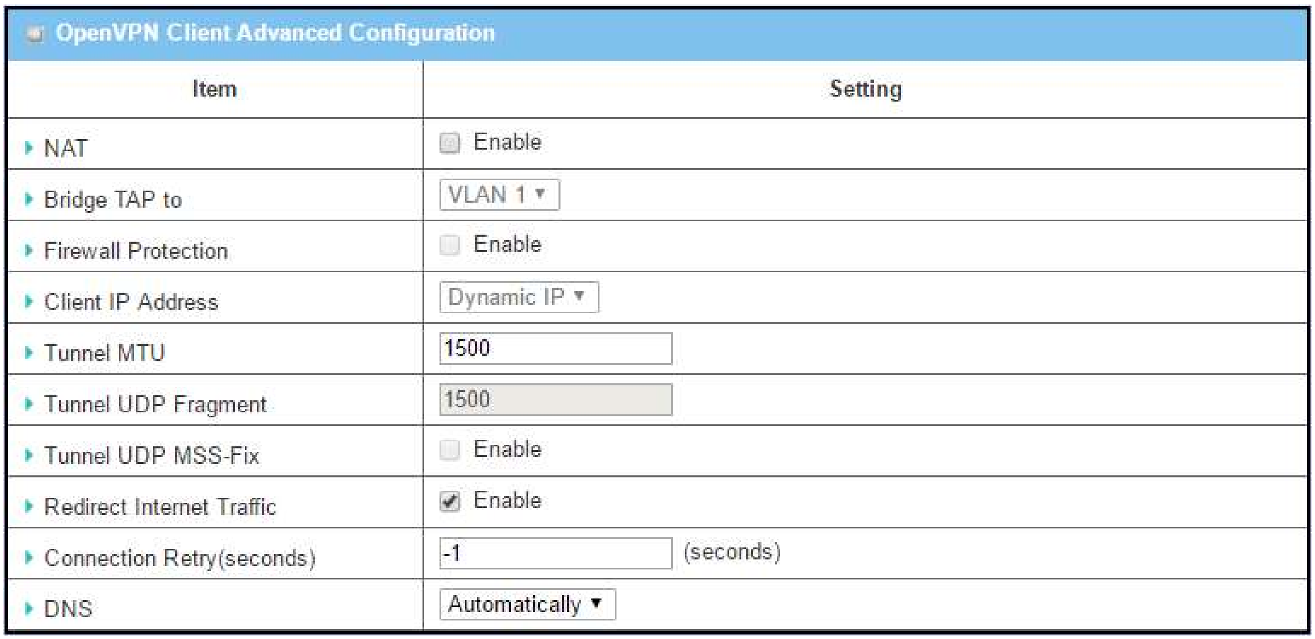
Item	Setting
OpenVPN Client Name	OpenVPN Client #1
Interface	WAN 1 ▾
Protocol	TCP ▾ Port: 443
Tunnel Device	TUN ▾
Remote IP/FQDN	
Remote Subnet	255.255.255.0(/24) ▾
Authorization Mode	TLS ▾ CA Cert.: ▾ Client Cert.: ▾ Client Key.: ▾ Please set the Certificate.
Encryption Cipher	Blowfish ▾
Hash Algorithm	SHA-1 ▾
LZO Compression	Adaptive ▾
Advanced Configuration	□ Enable
Tunnel	□ Enable

OpenVPN Client Configuration		
Item	**Value setting**	**Description**
OpenVPN Client Name	A Must filled setting	The **OpenVPN Client Name** will be used to identify the client in the tunnel list.
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	3. A Must filled setting 4. By default **TCP** is selected.	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.
Port	1. A Must filled setting 2. By default **443** is set.	Specify the **Port** for the OpenVPN Client to use.
Tunnel Device	1. A Must filled setting 2. By default **TUN** is selected.	Specify the type of **Tunnel Device** for the OpenVPN Client to use. It can be **TUN** for TUN tunnel device, or **TAP** for TAP tunnel device.
Remote IP/FQDN	A Must filled setting	Specify the **Remote IP/FQDN** of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the IP address or FQDN.
Remote Subnet	A Must filled setting	Specify **Remote Subnet** of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the remote subnet address and remote subnet mask.
Authorization Mode	1. A Must filled setting 2. By default **TLS** is selected.	Specify the authorization mode for the OpenVPN Server. - **Static Key** ->The OpenVPN will use static key authorization mode, and the following items **Local Endpoint IP Address**, **Remote Endpoint IP Address** and **Static Key** will be displayed. - **TLS** ->The OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Client Cert.** and **Client Key** will be displayed. **CA Cert.** could be selected in Trusted CA Certificate List. Refer to **Object Definition** > **Certificate** > **Trusted Certificate**. **Client Cert.** could be selected in Local Certificate List. Refer to **Object Definition** > **Certificate** > **My Certificate**. **Client Key** could be selected in Trusted Client key List. Refer to **Object Definition** > **Certificate** > **Trusted Certificate**.
Local Endpoint IP Address	A Must filled setting	Specify the **Local Endpoint IP Address**. Note_1: Local Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Remote Endpoint IP Address	A Must filled setting	Specify the **Remote Endpoint IP Address**. Note_1: Remote Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Static Key	A Must filled setting	Specify the **Static Key**. Note_1: Static Key will be available only when Static Key is chosen in Authorization Mode.
Encryption Cipher	By default **Blowfish** is selected.	Specify the **Encryption Cipher.** It can be **Blowfish/AES-256/AES-192/AES-128/None.**
Hash Algorithm	By default **SHA-1** is selected.	Specify the **Hash Algorithm.** It can be **SHA-1/MD5/MD4/SHA2-256/SHA2-512/None.**
LZO Compression	By default **Adaptive** is selected.	Specify the **LZO Compression** scheme. It can be **Adaptive/YES/NO/NO Adaptive.**

Advanced Configuration	The box is unchecked by default.	Check the box to enable the **Advanced Configuration** setting. If it is checked, **Advanced Configuration** will be displayed below.
Tunnel	The box is unchecked by default	Check the box to enable this OpenVPN tunnel.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **Undo** to cancel the changes.
Back	N/A	Click **Back** to return to last page.

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



OpenVPN Client Advanced Configuration

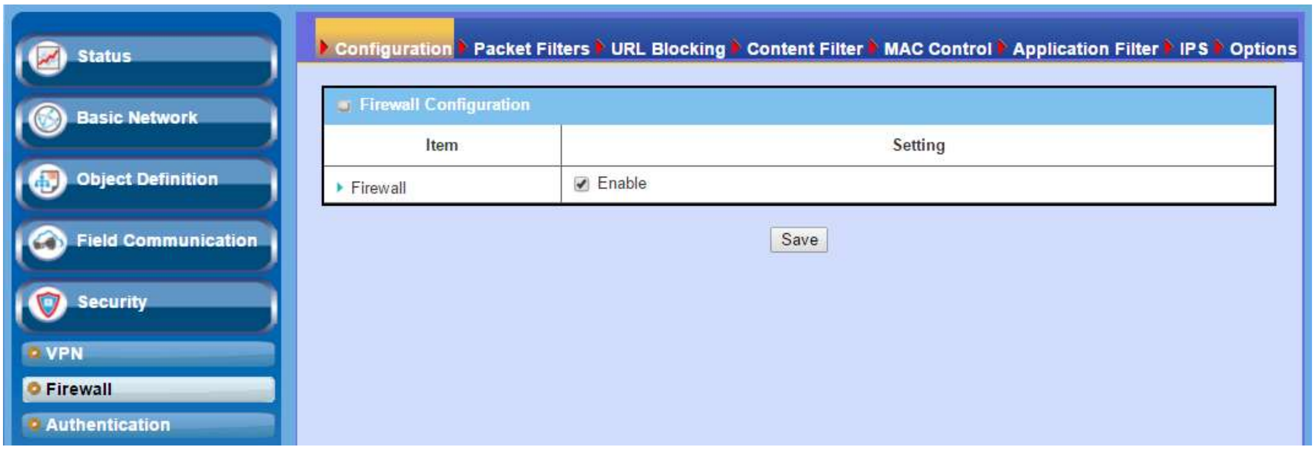
Item	Setting
NAT	□ Enable
Bridge TAP to	VLAN 1 ▾
Firewall Protection	□ Enable
Client IP Address	Dynamic IP ▾
Tunnel MTU	1500
Tunnel UDP Fragment	1500
Tunnel UDP MSS-Fix	□ Enable
Redirect Internet Traffic	☑ Enable
Connection Retry(seconds)	-1 (seconds)
DNS	Automatically ▾

OpenVPN Advanced Client Configuration		
Item	**Value setting**	**Description**
NAT	The box is unchecked by default.	Check the box to enable **NAT.**
Bridge TAP to	By default **VLAN1** is selected	Specify the setting of **Bridge TAP to.** Note_1: Bridge TAP to will be available only when TAP is chosen in Tunnel Device and NAT is unchecked.
Firewall Protection	The box is unchecked by default.	Check the box to enable **Firewall Protection.** Note_1: Firewall Protection will be available only when NAT is checked.
Client IP Address	By default **Dynamic IP** is selected	Specify the **Client IP Address.** It can be **Dynamic IP/Static IP.**
Tunnel MTU	1. A Must filled setting 2. The value is 1500	Specify the value of **Tunnel MTU.**

	by default	
Tunnel UDP Fragment	The value is 1500 by default	Specify the value of **Tunnel UDP Fragment.** Note_1: Tunnel UDP Fragment will be available only when UDP is chosen in Protocol.
Tunnel UDP MSS-Fix	The box is unchecked by default.	Check the box to enable **Tunnel UDP MSS-Fix.** Note_1: Tunnel UDP MSS-Fix will be available only when UDP is chosen in Protocol.
Redirect Internet Traffic	The box is checked by default.	Check the box to enable **Redirect Internet Traffic.**
Connection Retry(seconds)	The value is -1 by default	Specify the time interval of **Connection Retry.** The default -1 means that it is no need to execute connection retry.
DNS	By default **Automatically** is selected	Specify the setting of **DNS.** It can be **Automatically/Manually.**

9.3 Firewall

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



Firewall Configuration

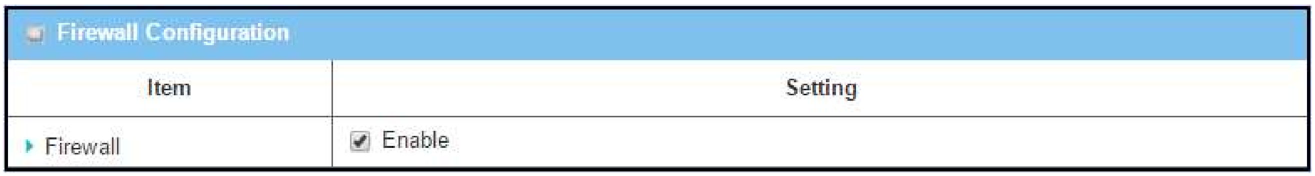
Item	Setting
Firewall	☑ Enable

9.3.1 Firewall Configuration

Enable **Firewall** check box will activate all firewall functions. The firewall configuration allows user to enable or disable all functions including Packet Filters, URL Blocking, Web Content Filters, MAC Control, Application Filters, IPS, and Firewall Options.

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

Enable Global Firewall Function



Firewall Configuration

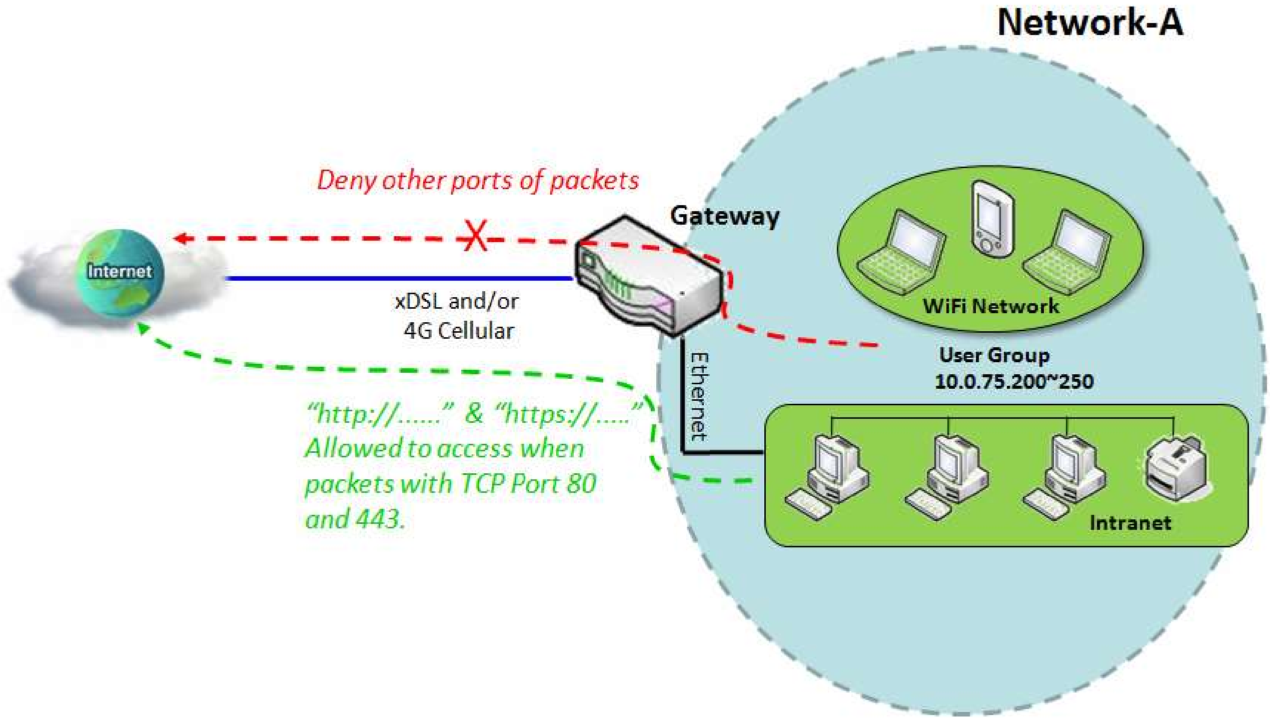
Item	Setting
Firewall	☑ Enable

Firewall Configuration Setting		
Item	**Value setting**	**Description**
Enable Firewall function	The box is checked by default	Check the **Enable** box to activate all firewall functions
Save	N/A	Click **Save** to save the settings

9.3.3 Packet Filter

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

Packet Filter with White List Scenario



Scenario Application Timing

When the administrator of the gateway wants to allow only specific packets through the gateway, he can use the "Packet Filters" function to carry out to allow specific packets by defining the white list as shown in above diagram. Certainly, when the administrator wants to deny only specific packets from going through, he can use the "Packet Filters" function by defining the black list to carry out to meet the requirement. It is contrasting to above diagram.

Scenario Description

To only allow dedicated packets that match to one packet filtering rule to flow through the gateway and block other packets that are not defined in the “Packet Filter Rule List” entry.

Parameter Setup Example

Following tables list the parameter configuration as an example for the gateway in above diagram with "Packet Filters" enabling.

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

Configuration Path	[Packet Filter]-[Configuration]
Packet Filters	■ *Enable*
Black List / White List	*Deny all to pass except those match the following rules.*

Configuration Path	[Packet Filter]-[Packet Filter Rule List]	
ID	1	2
Rule Name	*Access 80*	*Access 443*
Source IP	*IP Range: 10.0.75.200 ~ 10.0.75.250*	*IP Range: 10.0.75.200 ~ 10.0.75.250*
Destination IP	*Specific IP Address: 0.0.0.0*	*Specific IP Address: 0.0.0.0*
Destination Port	*User-defined Service: 80 ~ 80*	*User-defined Service: 443 ~ 443*
Protocol	*TCP*	*TCP*
Rule	■ *Enable*	■ *Enable*

Scenario Operation Procedure

In above diagram, the Gateway is the gateway of Network-A and the subnet of its Intranet is 10.0.75.0/24. The gateway has the IP address of 10.0.75.2 for LAN interface, 118.18.81.33 for WAN-1 interface. It serves as a NAT router.

Enable the packet filter function and specify the "Packet Filter Rule List" is a white list and configure two packet filtering rules for the gateway. Create one rule to allow HTTP packets and the other rule to allow HTTPS packets to pass through the gateway.

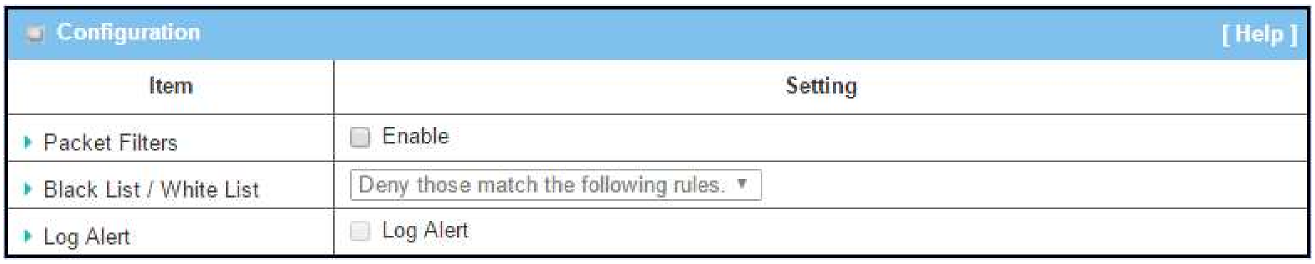
System will allow only HTTP and HTTPS packet to pass through the gateway for those hosts in the Intranet and their IP addresses are in the range from .200 to .250.

Packet Filter Setting

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

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

Enable Packet Filter



Configuration [Help]

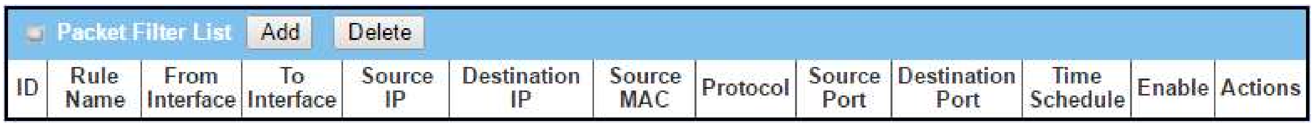
Item	Setting
Packet Filters	□ Enable
Black List / White List	Deny those match the following rules. ▼
Log Alert	□ Log Alert

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

Note: Packet Filter function is only available when Firewall feature is enabled. Refer to section 9.3.1 Firewall

Create/Edit Packet Filter Rules

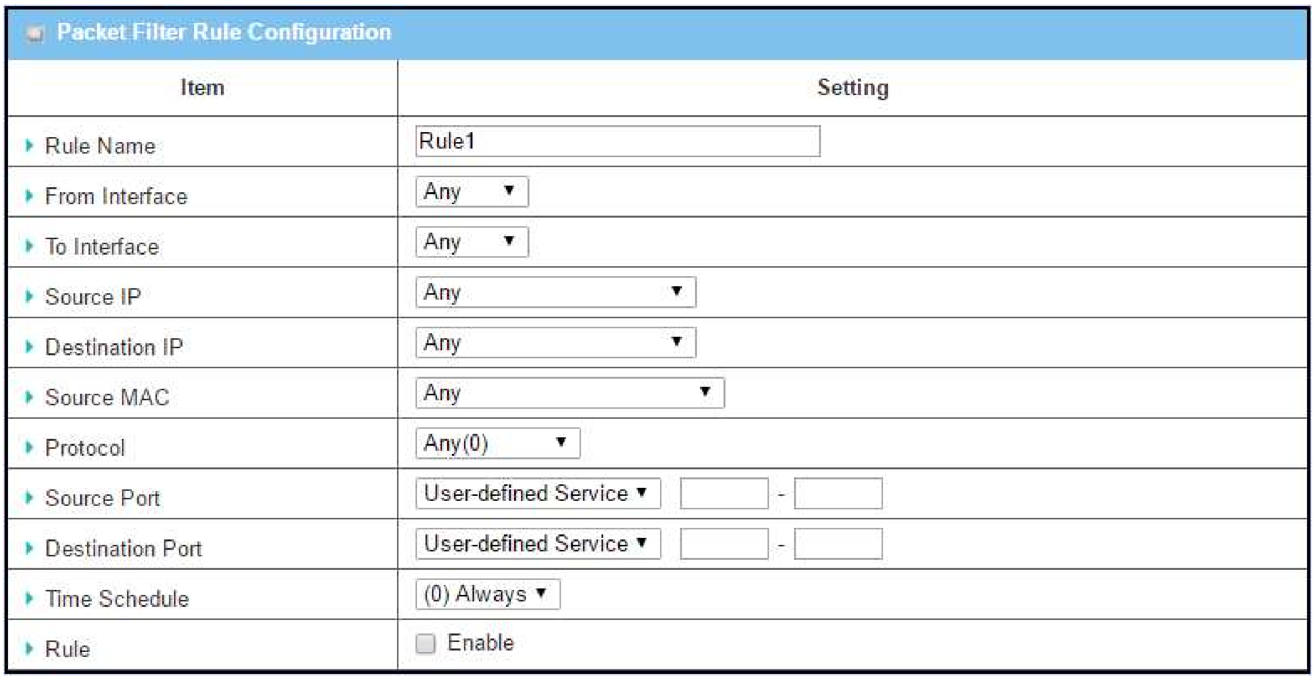
The gateway allows you to customize your packet filtering rules. It supports up to a maximum of 20 filter rule sets.



Packet Filter List

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

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



Packet Filter Rule Configuration

Item	Setting
Rule Name	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 packet filter rule name. Enter a name that is easy for you to remember.
From Interface	1. A Must filled setting **2. By default Any is selected**	Define the selected interface to be the packet-entering interface of the router. If the packets to be filtered are coming from **LAN to WAN** then select LAN for this field. Or **VLAN-1 to WAN** then select **VLAN-1** for this field. Other examples are VLAN-1 to VLAN-2. VLAN-1 to WAN. Select **Any** to filter packets coming into the router from any interfaces. Please note that two identical interfaces are not accepted by the router. i.e. VLAN-1 to VLAN-1.

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

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

9.3.5 URL Blocking

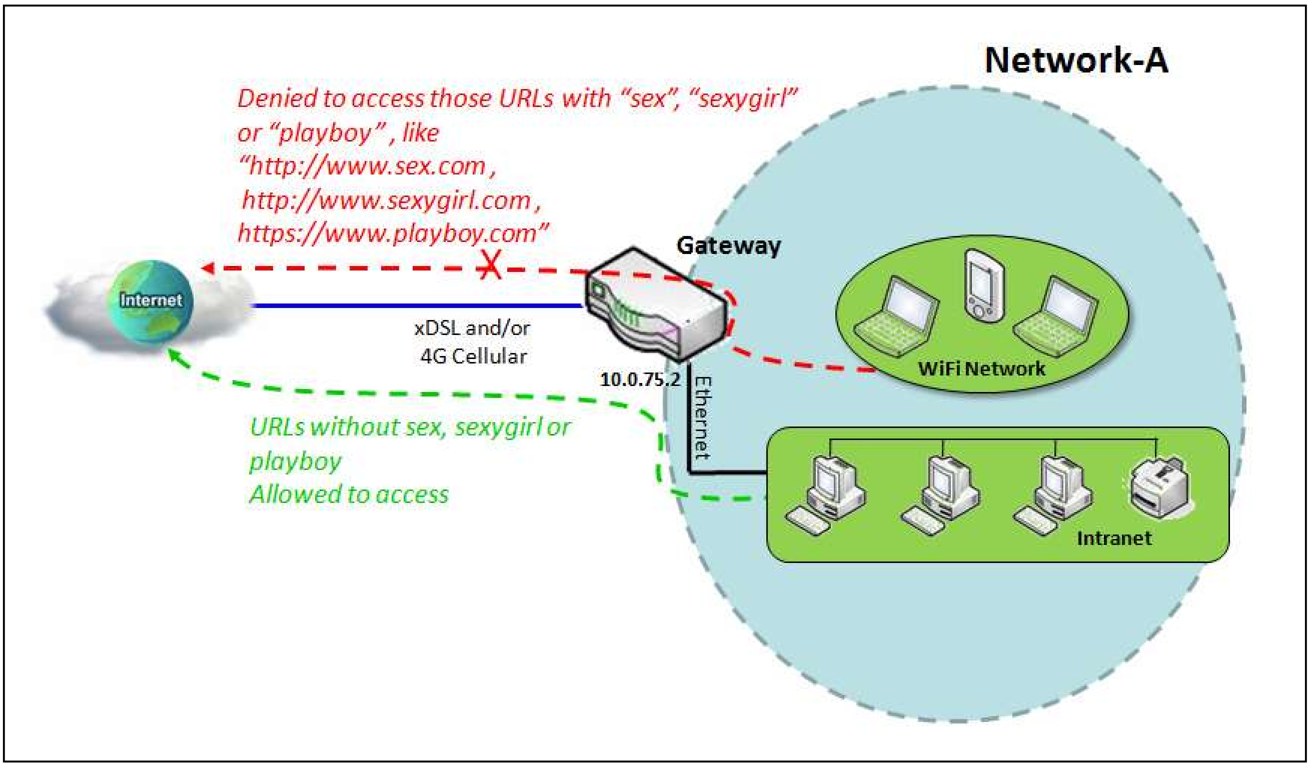
"URL Blocking" function can let you define blocking or allowing rules for incoming and outgoing Web request packets. With defined rules, gateway can control the Web requests containing the complete URL, partial domain name, or pre-defined keywords. For example, one can filter out or allow only the Web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

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

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

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

➢ URL Blocking with Black List Scenario


Network-A
Denied to access those URLs with "sex", "sexygirl" or "playboy", like "http://www.sex.com, http://www.sexygirl.com, https://www.playboy.com"
Gateway
Internet
xDSL and/or 4G Cellular
10.0.75.2
Ethernet
WiFi Network
URLs without sex, sexygirl or playboy Allowed to access
Intranet

Scenario Application Timing

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

Scenario Description

Web requests with dedicated patterns in the black list will be blocked by the gateway. The others can pass through the gateway.

Parameter Setup Example

Following tables list the parameter configuration as an example for the gateway in above diagram with "URL Blocking" enabling.

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

Configuration Path	[URL Blocking]-[Configuration]
URL Blocking	■ ***Enable***
Black List / White List	***Allow all to pass except those match the following rules.***

Configuration Path	[URL Blocking]-[URL Blocking Rule List]	
ID	1	2
Rule Name	***Block sex & sexygirl***	***Block playboy***
URL/Domain Name/Keyword	***sex; sexygirl***	***playboy***
Rule	■ ***Enable***	■ ***Enable***

Scenario Operation Procedure

In above diagram, the Gateway is the gateway of Network-A and the subnet of its Intranet is 10.0.75.0/24. The gateway has the IP address of 10.0.75.2 for LAN interface, 118.18.81.33 for WAN-1 interface. It serves as a NAT router.

Enable the URL blocking function and specify the "URL Blocking Rule List" with a black list and configure two URL blocking rules for it. Create the first rule to deny the Web requests with "sex" or "sexygirl" patterns and the other to deny the Web requests with "playboy" pattern to go through the gateway.

System will block the Web requests with "sex", "sexygirl" or "playboy" patterns to pass through the gateway.

URL Blocking Setting

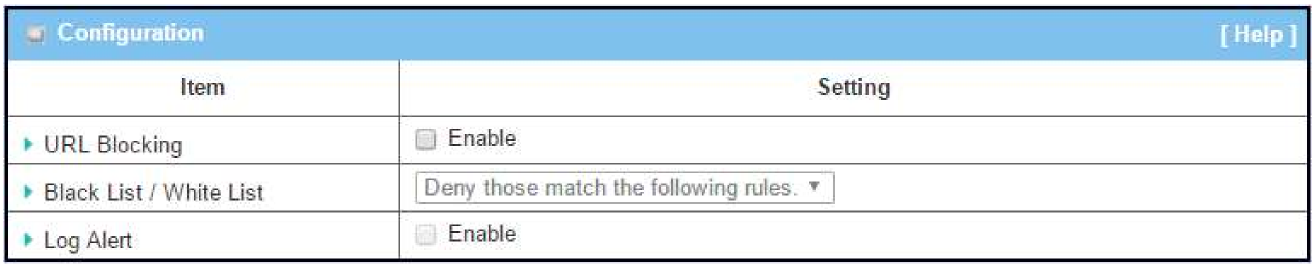
The URL Blocking setting allows user to create and customize URL blocking policies to allow or reject http packets with specific keyword, domain name, or URL. In "URL Blocking" page, there are three configuration windows. They are the "Configuration" window, "URL Blocking Rule List" window, and "URL Blocking Rule Configuration" window.

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

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

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

Enable URL Blocking



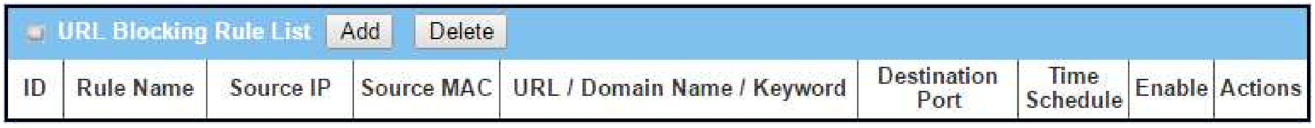
Configuration [Help]

Item	Setting
URL Blocking	□ Enable
Black List / White List	Deny those match the following rules. ▾
Log Alert	□ Enable

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

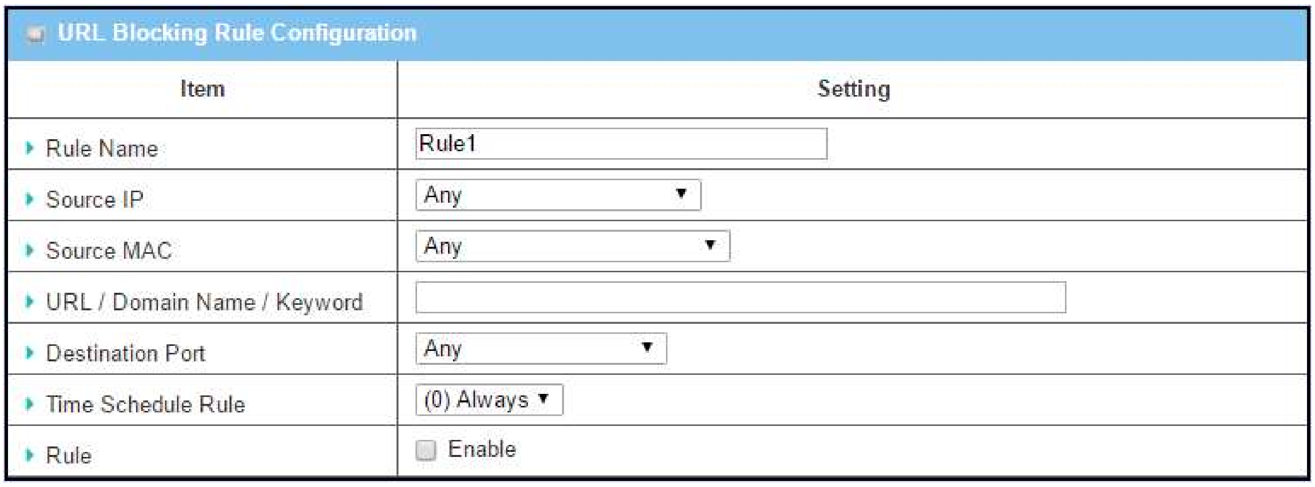
Create/Edit URL Blocking Rules

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



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

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


URL Blocking Rule Configuration

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

URL Blocking Rules Configuration

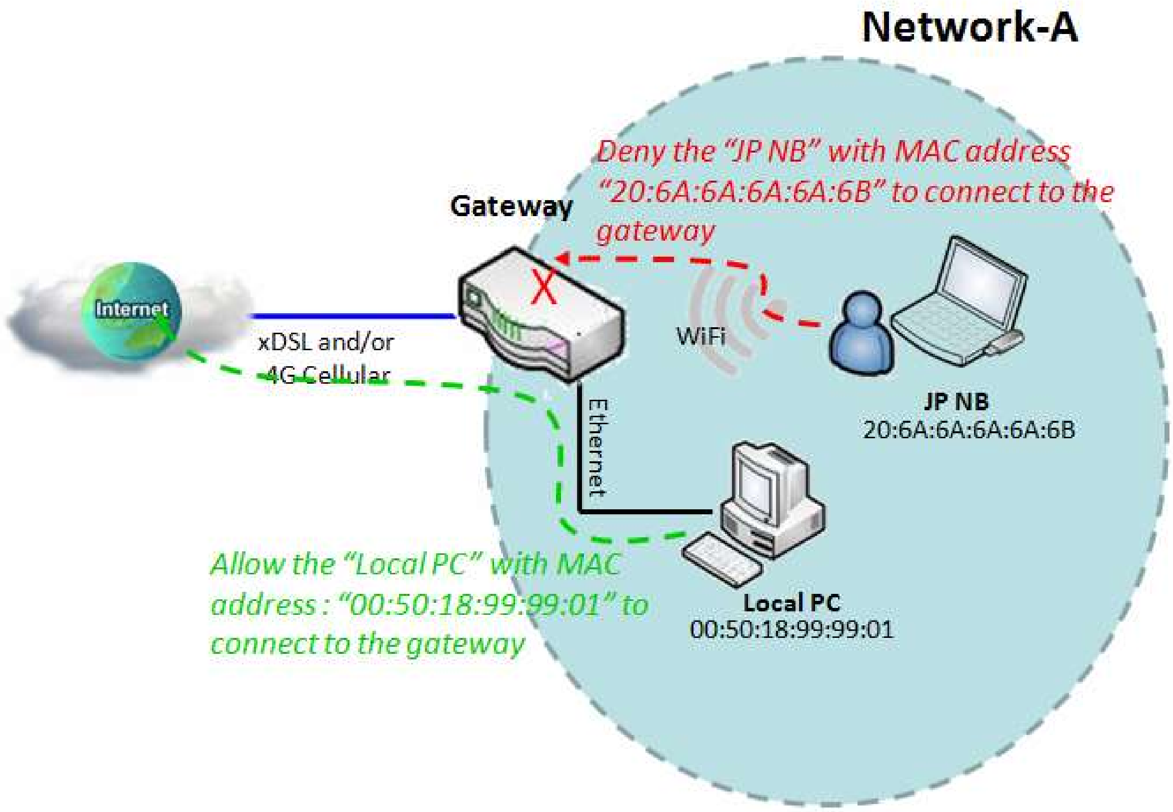
Item	Value setting	Description
Rule Name	1. String format can be any text 2. A Must filled setting	Specify an URL Blocking rule name. Enter a name that is easy for you to understand.
Source IP	1. A Must filled setting 2. **Any** is set by default	This field is to specify the **Source IP address**. • Select **Any** to filter packets coming from any IP addresses. • Select **Specific IP Address** to filter packets coming from an IP address entered in this field. • Select **IP Range** to filter packets coming from a specified range of IP address entered in this field. • Select **IP Address-based Group** to filter packets coming from a pre-defined group selected. Note: group must be pre-defined before this option become available. Refer to **Object Definition** > **Grouping > Host grouping**.
Source MAC	1. A Must filled setting 2. **Any** is set by default	This field is to specify the **Source MAC address**. • Select **Any** to filter packets coming from any MAC addresses. • Select **Specific MAC Address** to filter packets coming from a MAC address entered in this field.

		• Select **MAC Address-based Group** to filter packets coming from a pre-defined group selected. Note: group must be pre-defined before this selection become available. Refer to **Object Definition** > **Grouping > Host grouping**.
URL / Domain Name / Keyword	1. A Must filled setting 2. Supports up to a maximum of 10 Keywords in a rule by using the 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 and the 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 entered in this field. • Select **Port Range** to filter packets going to a specific range of Ports entered in this field.
Time Schedule Rule	A Must filled setting	Apply a specific **Time Schedule** to this rule, otherwise leave it as **(0) Always**. If the dropdown list is empty ensure **Time Schedule** is pre-configured. Refer to **Object Definition** > **Scheduling > Configuration** tab.
Rule	The box is unchecked by default.	Click the **Enable** box to activate this rule.
Save	*NA*	Click the **Save** button to save the settings.
Undo	*NA*	Click the **Undo** button to cancel the changes.
Back	*NA*	Click the **Back** button to return to the URL Blocking Configuration page.

9.3.9 MAC Control

"MAC Control" function allows you to assign the accessibility to the gateway for different users based on device's MAC address, including wired hosts or WiFi stations.

MAC Control with Black List Scenario


Network-A
Deny the "JP NB" with MAC address "20:6A:6A:6A:6A:6B" to connect to the gateway
Gateway
Internet
xDSL and/or 4G Cellular
WiFi
Ethernet
JP NB
20:6A:6A:6A:6A:6B
Allow the "Local PC" with MAC address : "00:50:18:99:99:01" to connect to the gateway
Local PC
00:50:18:99:99:01

Scenario Application Timing

When the administrator of the gateway wants to reject some client hosts with specific MAC addresses in the Intranet to connect to the gateway, he can use the "MAC Control" function to carry out to reject by defining the black list as shown in above diagram. Certainly, when the administrator wants to allow only the client hosts with dedicated MAC addresses to connect to the gateway, he can use the "MAC Control" function by defining the white list to carry out to meet the requirement. It is contrasting to above diagram.

Scenario Description

To only reject client hosts with dedicated MAC addresses in the black list to connect to the gateway and block other hosts that are not defined in the “MAC Control Rule List” entry.

Parameter Setup Example

Following tables list the parameter configuration as an example for the gateway in above diagram with "MAC Control" enabling.

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

Configuration Path	[MAC Control]-[Configuration]
MAC Control	■ ***Enable***
Black List / White List	***Allow all to pass except those match the following rules.***
Log Alert	■ ***Enable***

Configuration Path	[MAC Control]-[MAC Control Rule List]
ID	1
Rule Name	***Block JP NB***
MAC Address	***20:6A:6A:6A:6A:6B***
Rule	■ ***Enable***

Scenario Operation Procedure

In above diagram, the Gateway is the gateway of Network-A and the subnet of its Intranet is 10.0.75.0/24. The gateway has the IP address of 10.0.75.2 for LAN interface, 118.18.81.33 for WAN-1 interface. It serves as a NAT router.

Enable the MAC control function and specify the "MAC Control Rule List" is a black list, and configure one MAC control rule for the gateway to deny the connection request from the "JP NB" with its own MAC address.

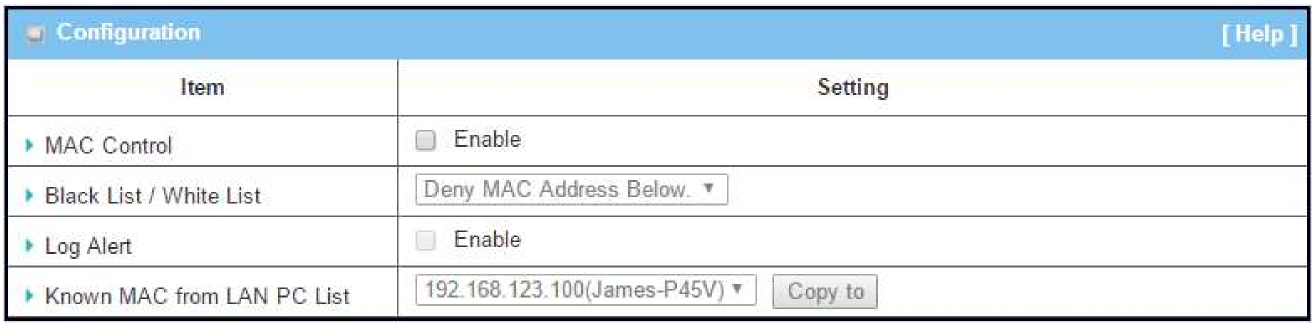
System will block the connecting from the "JP NB" to the gateway but allow others.

MAC Control Setting

The MAC control setting allows user to create and customize MAC address policies to allow or reject packets with specific source MAC address. Before you proceed, ensure that the Firewall is enabled and saved. Go to **Security > Firewall > Configuration** tab.

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

Enable MAC Control

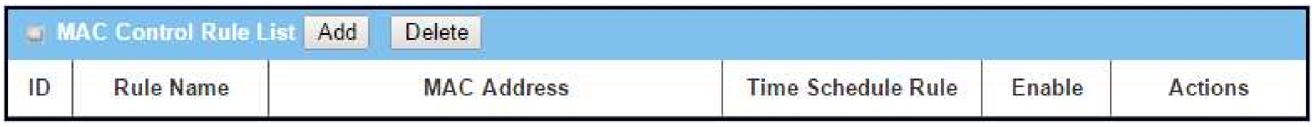


Item	Setting
MAC Control	□ Enable
Black List / White List	Deny MAC Address Below. ▾
Log Alert	□ Enable
Known MAC from LAN PC List	192.168.123.100(James-P45V) ▾ Copy to

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

Create/Edit MAC Control Rules

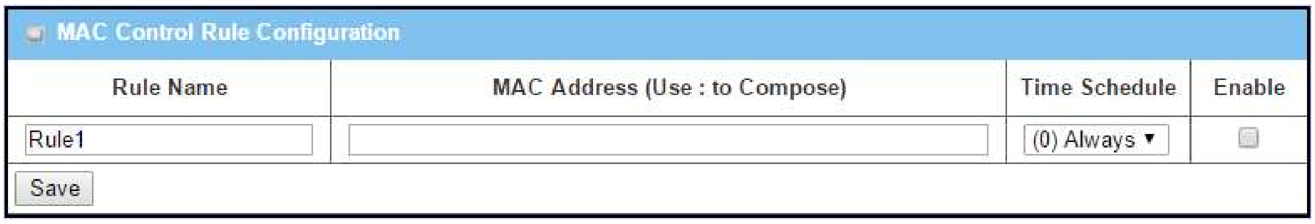
The gateway supports up to a maximum of 20 filter rule sets. Ensure that the MAC Control is enabled before we can create control rules.



MAC Control Rule List

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

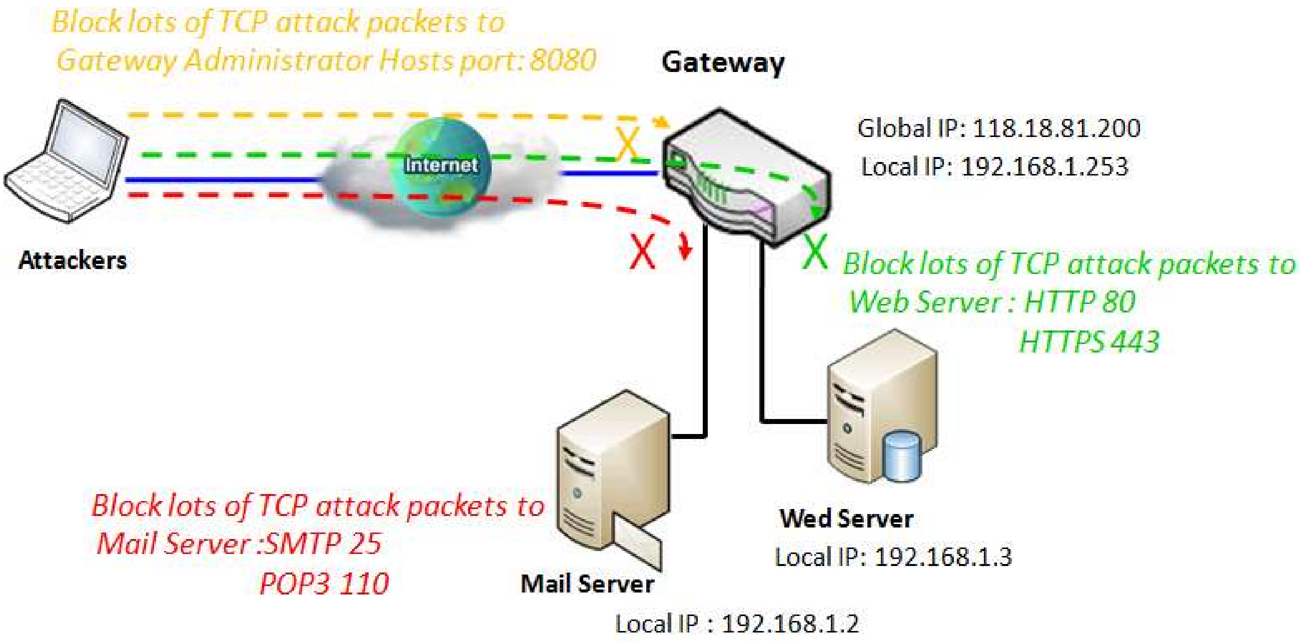
Rule Name	MAC Address (Use : to Compose)	Time Schedule	Enable
Rule1		(0) Always ▾	□

MAC Control Rule Configuration		
Item	**Value setting**	**Description**
Rule Name	1. String format can be any text 2. A Must fill setting	Enter a MAC Control rule name. Enter a name that is easy for you to remember.
MAC Address (Use: to Compose)	1. MAC Address string Format 2. A Must fill setting	Specify the **Source MAC Address** to filter rule.
Time Schedule	1. A 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.
Enable	The box is unchecked by default.	Click the **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	N/A	When the **Back** button is clicked, the screen will return to the MAC Control Configuration page.

9.3.d IPS

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

IPS Scenario



Scenario Application Timing

The administrator provides some application servers in the Intranet of deployed networking and has to open specific ports to make services for employees oversea or Internet users. There are some risks to always open service ports in the internet for admin users. In order to avoid such attacked risks, please enable IPS functions.

Scenario Description

The gateway serves as an E-mail server, Web Server and open TCP-Port 8080 allowing user to access web-based utility of Gateway, so remote users or unknown users can request those services from the gateway.

Parameter Setup Example

Following tables list the parameter configuration as an example for the gateway in above diagram with "IPS" enabling.

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

Configuration Path	[IPS]-[Configuration]
ISP	■ *Enable*
Log Alert	■ *Enable*

Configuration Path	[IPS]-[Intrusion Prevention]
SYN Flood Defense	■ *Enable 300 Packets/second*
Port Scan Detection	■ *Enable 200 Packets/second*
Block IP Spoof	■ *Enable*
Block TCP Flag Scan	■ *Enable*

Scenario Operation Procedure

In above diagram, the gateway detects incoming packets which TCP ports are 25, 80,110,443 and 8080 then forward to transfer the E-mail service requests to the LAN servers and send the replies from LAN servers back to the requester.

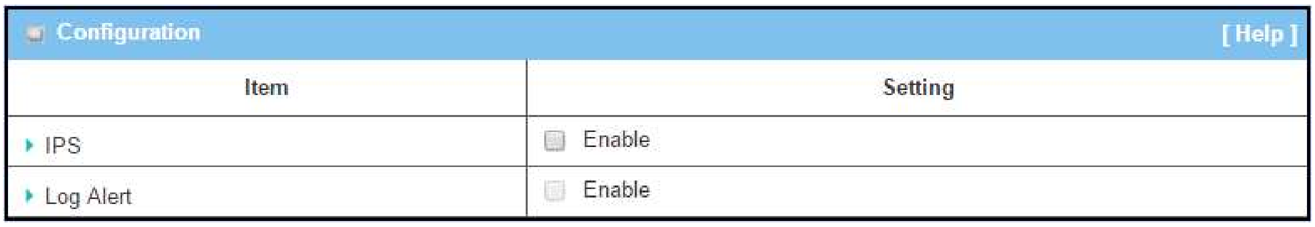
System will block lots of packets in seconds.

IPS Setting

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

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

Enable IPS Firewall

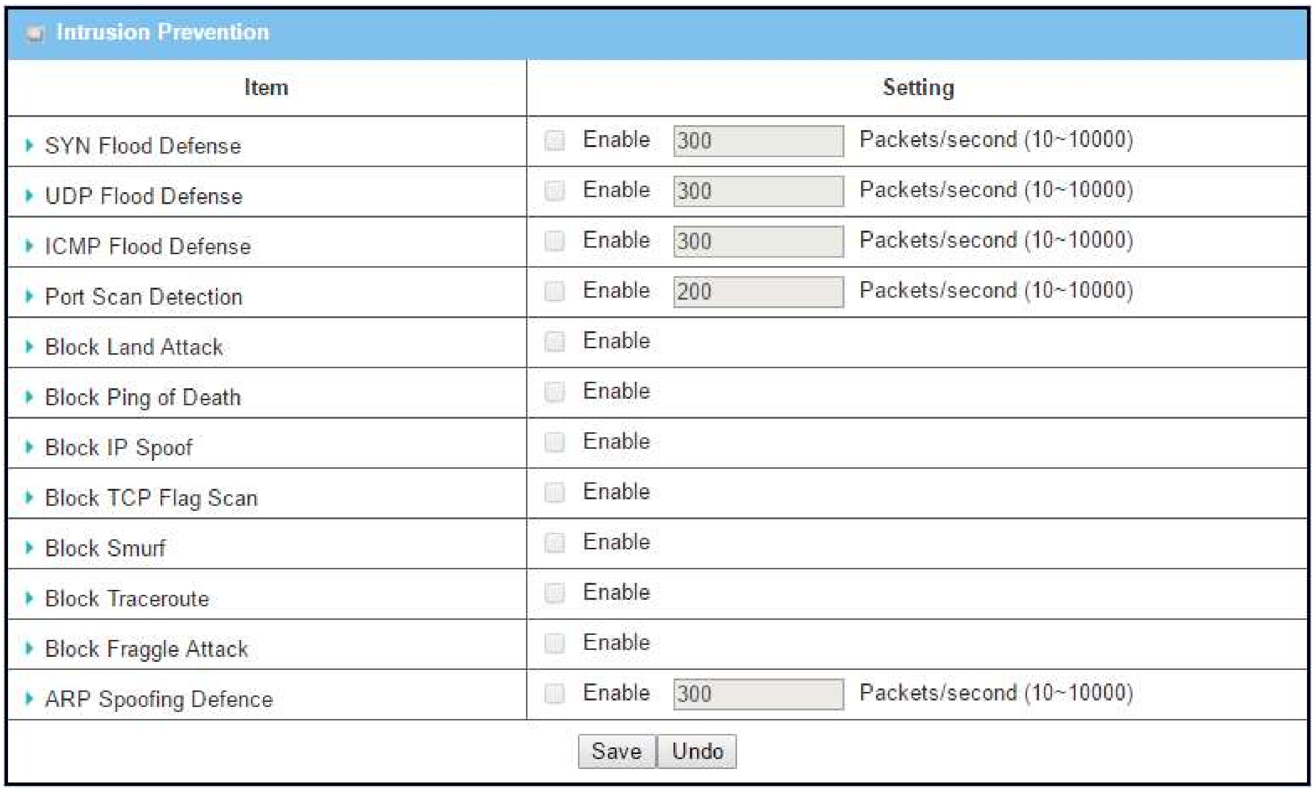


Item	Setting
IPS	□ Enable
Log Alert	□ Enable

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

Setup Intrusion Prevention Rules

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



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 Detection	□ 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 Defence	□ Enable 300 Packets/second (10~10000)

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

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

9.3.f Options

There are some useful functions in this page.

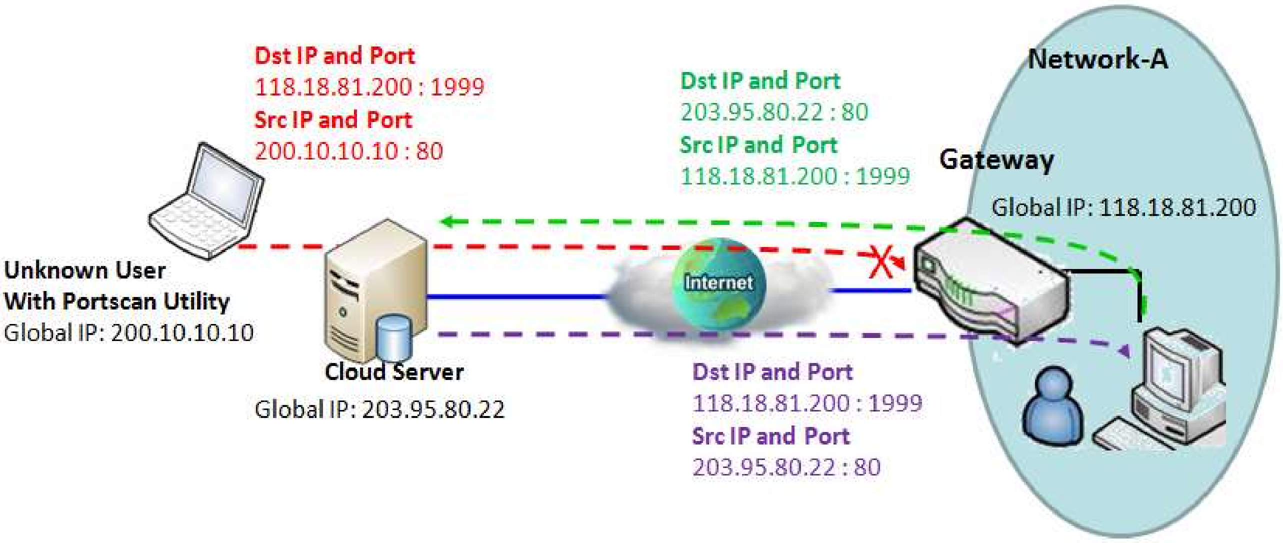
First, “Stealth Mode” lets gateway not to respond to port scans from the WAN so that makes it less susceptible to discovery and attacks on the Internet.

Second, ”SPI” enables gateway to record the packet information like IP address, port address, ACK, SEQ number and so on while they pass through the router. And the gateway checks every incoming packet to detect if this packet is valid.

Third, “Discard Ping from WAN” makes any host on the WAN side can`t ping this product. It means this device won`t reply any ICMP packet from Internet.

And finally, “Remote Administrator Hosts” enables only the LAN users to browse the web-based utility to perform administration task locally. This feature also enables you to perform administration task also from a remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can access web-based utility to perform administration task. You can use subnet mask bits '/nn' notation to specified a group of trusted IP addresses for example, '10.1.2.0/24'.

SPI Scenario



Scenario Application Timing

Users in Network-A initiate to access cloud server through Gateway which records connected sessions. Sometimes, unknown users will simulate the Packet but use different Src IP to masquerade.

Scenario Description

Enable the SPI function to prevent security leak when local users surf the internet.

Parameter Setup Example

Following tables list the parameter configuration as an example for the gateway in above diagram with "SPI" enabling.

Configuration Path	[Options]-[Firewall Options]
SPI	■ *Enable*

Scenario Operation Procedure

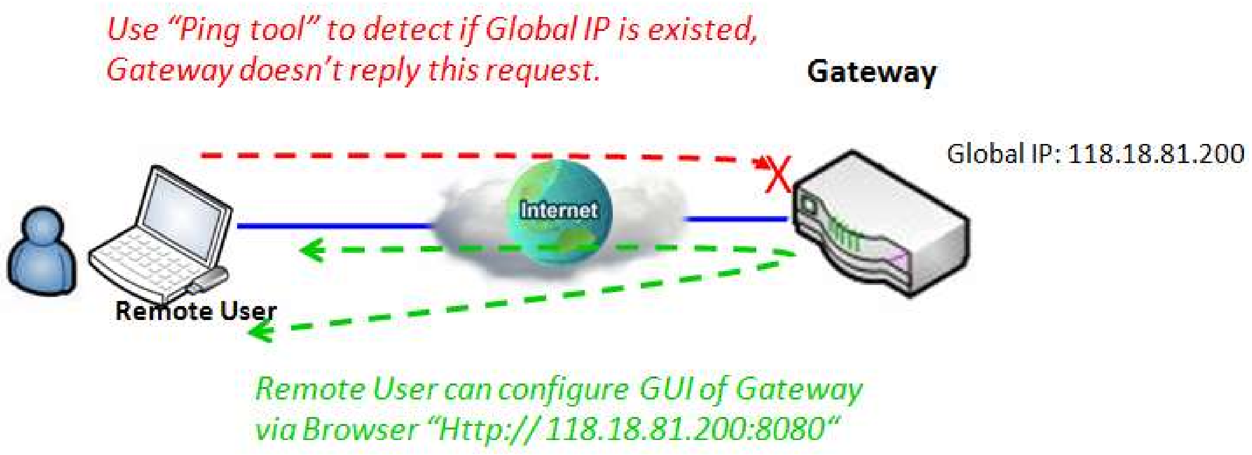
In above diagram, the Gateway is the gateway of Network-A and the subnet of its Intranet is 10.0.75.0/24. The gateway has the IP address of 10.0.75.2 for LAN interface and 118.18.81.200 for WAN interface. It serves as a NAT router.

Activate the SPI feature at the Gateway.

Users in Network-A initiate to access cloud server through Gateway. Sometimes, unknown users will simulate the Packet but use different Src IP to masquerade.

System will block such packets from unknown users.

Discard Ping from WAN and Remote Administrator Hosts Scenario


Use "Ping tool" to detect if Global IP is existed,
Gateway doesn't reply this request.
Gateway
Global IP: 118.18.81.200
Internet
Remote User
Remote User can configure GUI of Gateway
via Browser "Http:// 118.18.81.200:8080"

Scenario Application Timing

"Discard Ping from WAN" makes any host on the WAN side can`t ping this gateway reply any ICMP packet from Internet while with “Remote Administrator Hosts” allowing to browse the web-based utility to perform administration task remotely.

Scenario Description

Enable the Discard Ping from WAN function to prevent security leak when local users surf the internet.

Following tables list the parameter configuration as an example for the gateway in above diagram.

Configuration Path	[Options]-[Firewall Options]
Discard Ping from WAN	■ ***Enable***
Remote Administrator Hosts	■ ***Enable HTTPS , ANY : 8080*** ***Please disable “SPI” Function.***

Scenario Operation Procedure

In above diagram, the Gateway is the gateway of Network-A and the subnet of its Intranet is 10.0.75.0/24. The gateway has the IP address of 10.0.75.2 for LAN interface and 118.18.81.200 for WAN interface. It serves as a NAT router.

Activate the features at the Gateway.

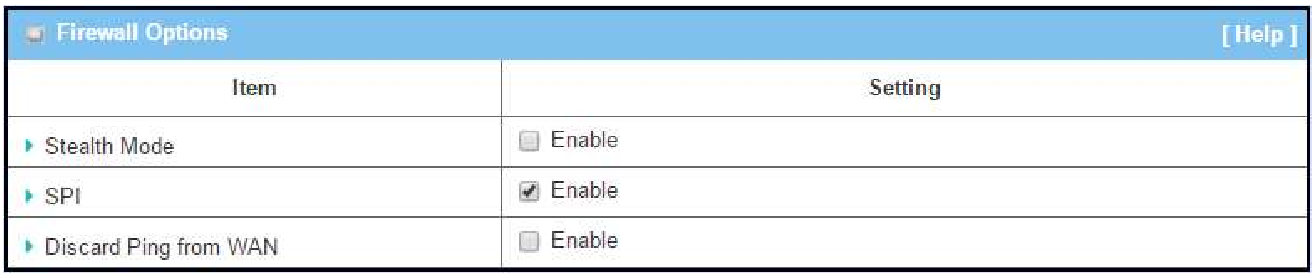
Remote users can’t get response via Ping Utility, but can access the web-based utility of Gateway via port 8080 of TCP.

Firewall Options Setting

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

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

Enable Firewall Options



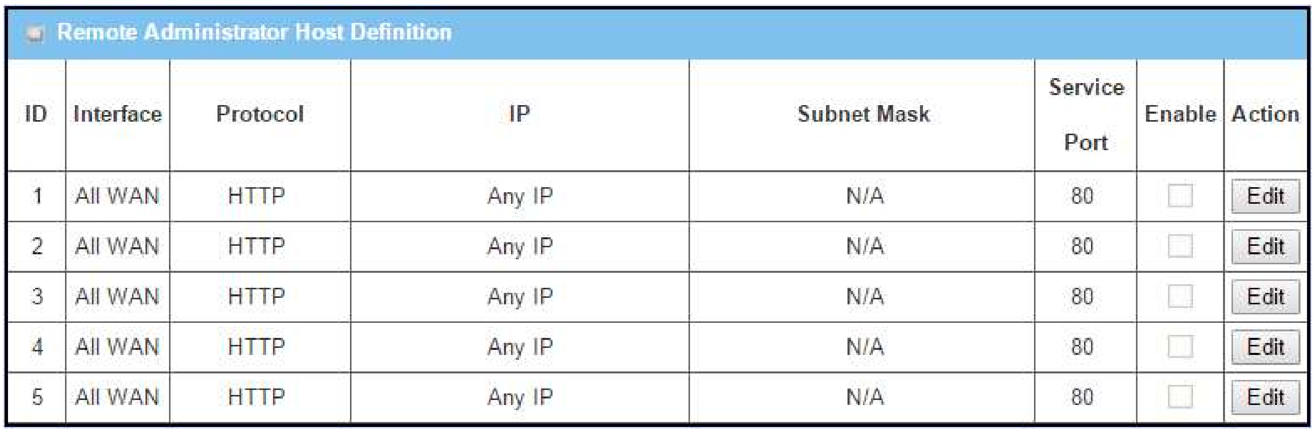
Firewall Options [Help]

Item	Setting
Stealth Mode	□ Enable
SPI	☑ Enable
Discard Ping from WAN	□ Enable

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

Define Remote Administrator Host

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

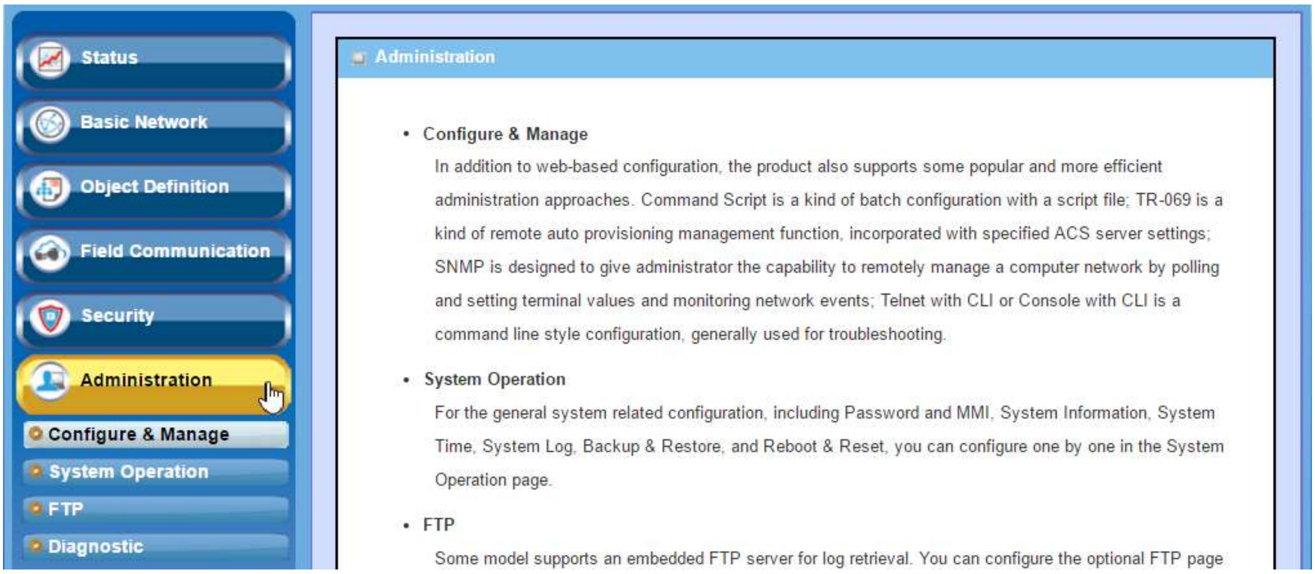


Remote Administrator Host Definition

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

Remote Administrator Host Definition		
Item	**Value setting**	**Description**
Protocol	HTTP is set by default	Select **HTTP** or **HTTPS** method for router access.
IP	A Must filled setting	This field is to specify the remote host to assign access right for remote access. Select **Any IP** to allow any remote hosts Select **Specific IP** to allow the remote host coming from a specific subnet. An IP address entered in this field and a selected **Subnet Mask** to compose the subnet**.**
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.
Enabling the rule	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click **Enable** box to activate this rule then save the settings.
Undo	N/A	Click **Undo** to cancel the settings

Chapter b Administration



Administration

- Configure & Manage
  In addition to web-based configuration, the product also supports some popular and more efficient administration approaches. Command Script is a kind of batch configuration with a script file; TR-069 is a kind of remote auto provisioning management function, incorporated with specified ACS server settings; SNMP is designed to give administrator the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events; Telnet with CLI or Console with CLI is a command line style configuration, generally used for troubleshooting.
- System Operation
  For the general system related configuration, including Password and MMI, System Information, System Time, System Log, Backup & Restore, and Reboot & Reset, you can configure one by one in the System Operation page.
- FTP
  Some model supports an embedded FTP server for log retrieval. You can configure the optional FTP page

b.1 Configure & Manage

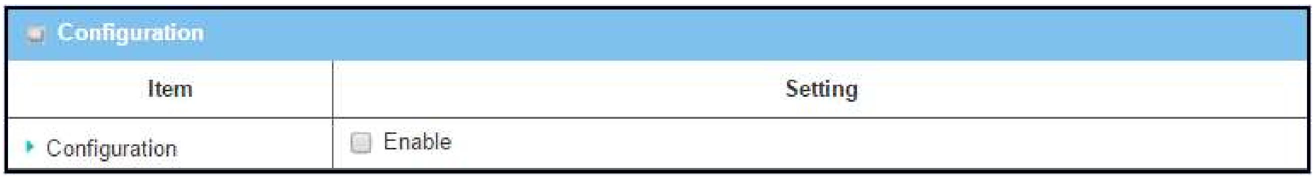
Configure & Manage refers to enterprise-wide administration of distributed systems including (and commonly in practice) computer systems. Centralized management has a time and effort trade-off that is related to the size of the company, the expertise of the IT staff, and the amount of technology being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

b.1.1 Command Script

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

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

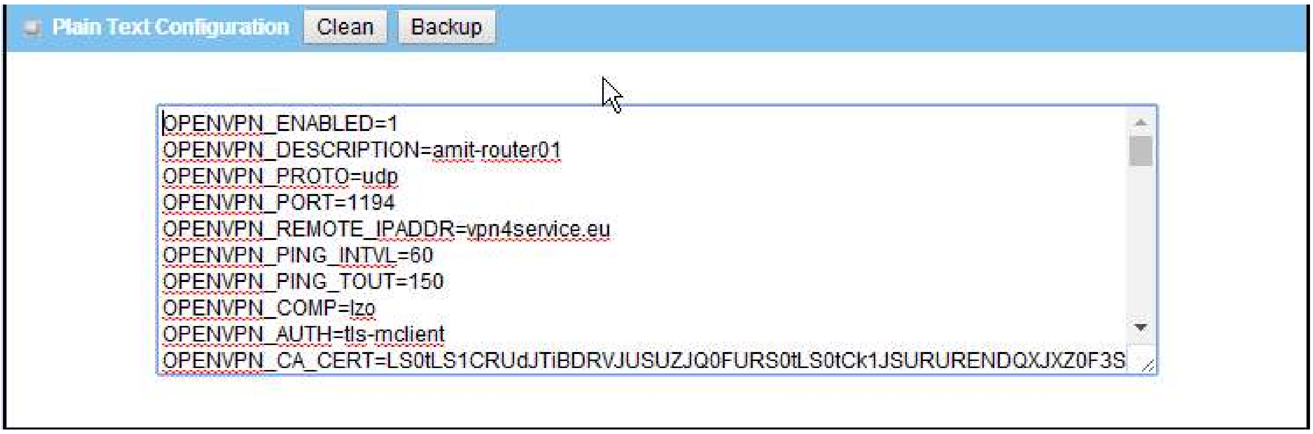
Enable Command Script Configuration



Configuration	
Item	Setting
▸ Configuration	□ Enable

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

Edit/Backup Plain Text Command Script



```
OPENVPN_ENABLED=1
OPENVPN_DESCRIPTION=amit-router01
OPENVPN_PROTO=udp
OPENVPN_PORT=1194
OPENVPN_REMOTE_IPADDR=vpn4service.eu
OPENVPN_PING_INTVL=60
OPENVPN_PING_TOUT=150
OPENVPN_COMP=lzo
OPENVPN_AUTH=tls-mclient
OPENVPN_CA_CERT=LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSURURENDQXJXZ0F3S
```

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

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

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

Configuration Content		
Key	Value setting	Description
OPENVPN_ENABLED	1 : enable 0 : disable	Enable or disable OpenVPN Client function.
OPENVPN_DESCRIPTION	A Must filled Setting	Specify the tunnel name for the OpenVPN Client connection.
OPENVPN_PROTO	udp tcp	Define the **Protocol** for the OpenVPN Client. • Select **TCP** or **TCP /UDP** ->The OpenVPN will use TCP protocol, and **Port** will be set as 443 automatically. • Select **UDP** -> The OpenVPN will use UDP protocol, and **Port** will be set as 1194 automatically.
OPENVPN_PORT	A Must filled Setting	Specify the **Port** for the OpenVPN Client to use.
OPENVPN_REMOTE_IPADDR	IP or FQDN	Specify the **Remote IP/FQDN** of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the IP address or FQDN.
OPENVPN_PING_INTVL	seconds	Specify the time interval for OpenVPN keep-alive checking.
OPENVPN_PING_TOUT	seconds	Specify the timeout value for OpenVPN Client keep-alive checking.
OPENVPN_COMP	Adaptive	Specify the **LZO Compression** algorithm for OpenVPN client.
OPENVPN_AUTH	Static Key/TLS	Specify the authorization mode for the OpenVPN tunnel. • **TLS** ->The OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Client Cert.** and **Client Key** need to specify as well.
OPENVPN_CA_CERT	A Must filled Setting	Specify the Trusted CA certificate for the OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_CERT	A Must filled Setting	Specify the local certificate for OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_KEY	A Must filled Setting	Specify the local key for the OpenVPN client. It will go through Base64 Conversion.
OPENVPN_EXTRA_OPTS	Options	Specify the extra options setting for the OpenVPN client.
IP_ADDR1	Ip	Ethernet LAN IP
IP_NETM1	Net mask	Ethernet LAN MASK
PPP_MONITORING	1 : enable 0 : disable	When the Network Monitoring feature is enabled, the router will use DNS Query or ICMP to periodically check Internet connection –connected or disconnected.
PPP_PING	0 : DNS Query 1 : ICMP Query	With **DNS Query,** the system checks the connection by sending DNS Query packets to the destination specified in PPP_PING_IPADDR.

		With **ICMP Query,** the system will check connection by sending ICMP request packets to the destination specified in PPP_PING_IPADDR.
PPP_PING_IPADDR	IP	Specify an IP address as the target for sending DNS query/ICMP request.
PPP_PING_INTVL	seconds	Specify the time interval for between two DNS Query or ICMP checking packets.

STARTUP	Script file	For the configurations that can be configured with standard Linux commands, you can put them in a script file, and apply the script file with STARTUP command.
		For example,
		STARTUP=#!/bin/sh
		STARTUP=echo “startup done” > /tmp/demo

Plain Text System Configuration with Telnet

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

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

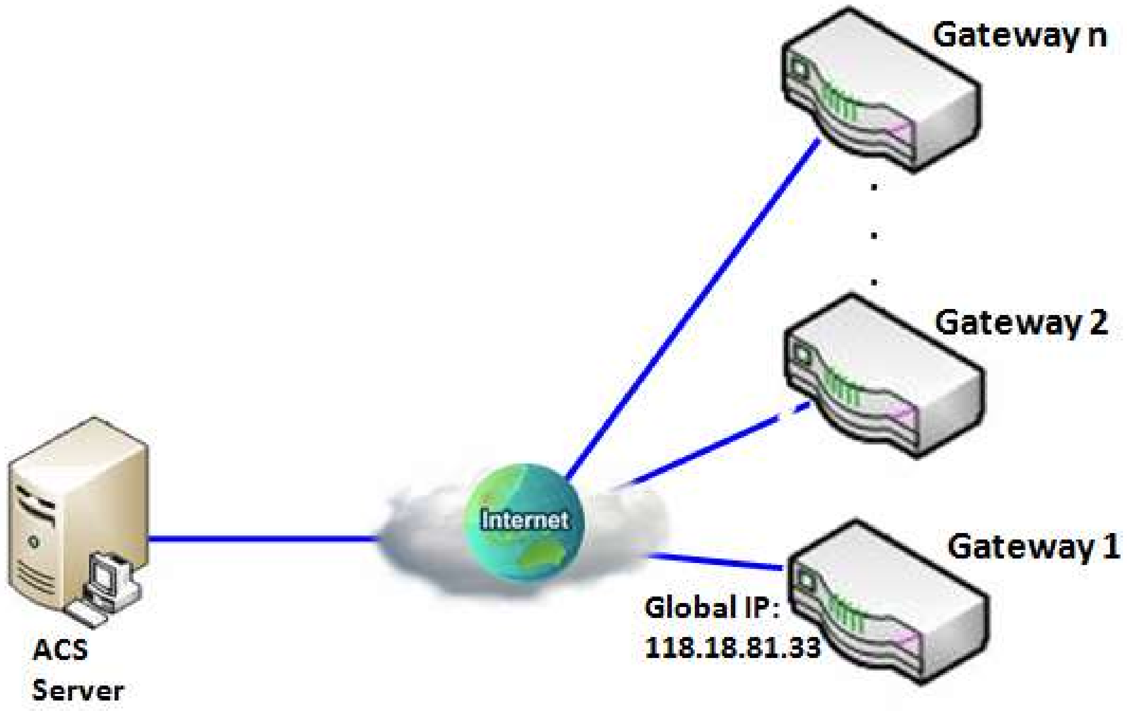
Action	Option	Description
clone	*Output file*	Duplicate the configuration content from database and stored as a configuration file. (ex: *txtConfig clone /tmp/config*) The contents in the configuration file are the same as the plain text commands mentioned above. This action is exactly the same as performing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

b.1.3 TR-069

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

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

Scenario - Managing deployed gateways through an ACS Server



Scenario Application Timing

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

M2M LTE Gateway with serial port

Scenario Description

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

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

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

Parameter Setup Example

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

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

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

Scenario Operation Procedure

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

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

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

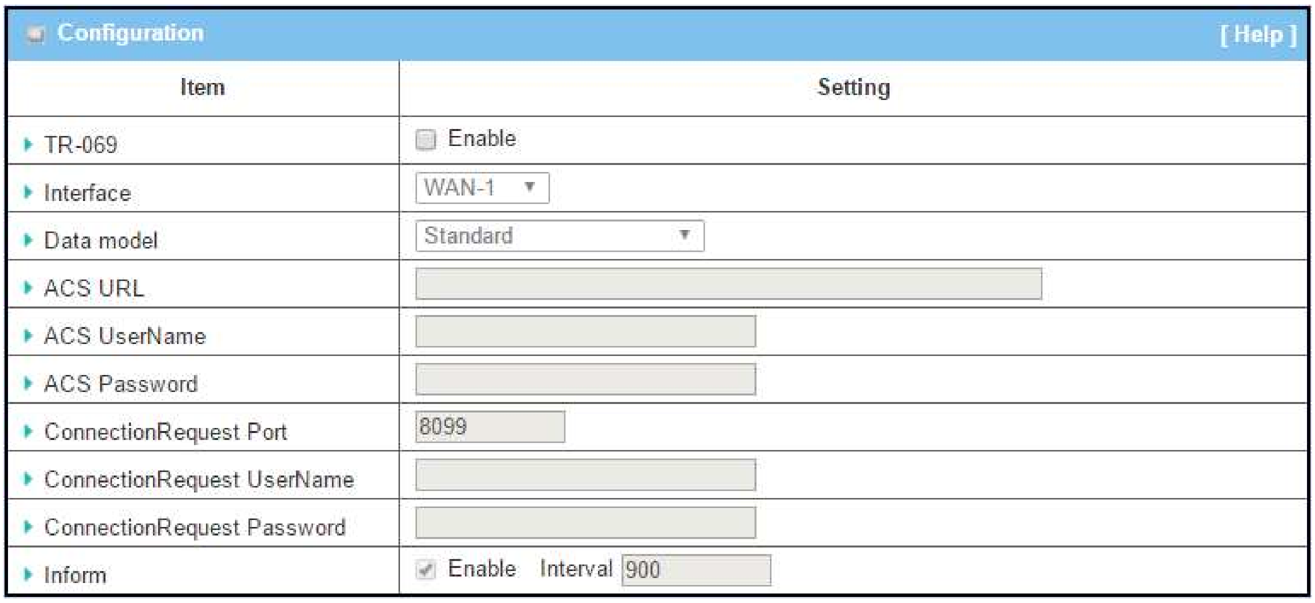
Remote gateways inquire the ACS server for jobs to do in each time period.

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

TR-069 Setting

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

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



Item	Setting
TR-069	□ Enable
Interface	WAN-1 ▼
Data model	Standard ▼
ACS URL	
ACS UserName	
ACS Password	
ConnectionRequest Port	8099
ConnectionRequest UserName	
ConnectionRequest Password	
Inform	☑ Enable Interval 900

TR-069		
Item	**Value setting**	**Description**
TR-069	The box is unchecked by default	Check the **Enable** box for activate TR-069
Interface	WAN-1 is selected by default.	When you finish set basic network wan 1~wan n, you can choose wan 1~wan n When you finish set **Security > VPN > IPSec/PPTP/L2TP/GRE**, you can choose IPSec/PPTP/L2TP/GRE tunnel, the interface like **"IPSec #1"**

Data Model	Standard is selected by default.	Select the TR-069 dat model for the remote management. **Standard** : the ACS Server is a standard one, which is fully comply with TR-069.
ACS URL	A Must filled setting	You can ask ACS manager provide ACS URL and manually set
ACS Username	A Must filled setting	You can ask ACS manager provide ACS username and manually set
ACS Password	A Must filled setting	You can ask ACS manager provide ACS password and manually set
ConnectionRequest Port	1. A Must filled setting **2. By default 8099 is set**	You can ask ACS manager provide ACS ConnectionRequest Port and manually set
ConnectionRequest UserName	A Must filled setting	You can ask ACS manager provide ACS ConnectionRequest Username and manually set
ConnectionRequest Password	A Must filled setting	You can ask ACS manager provide ACS ConnectionRequest Password and manually set
Inform	The box is checked by default	When the **Enable** box is checked, the gateway (CPE) will periodicly send inform message to ACS Server.
Inform Interval	The value is 900 by default	This value is decide how long send inform to ACS
Save	N/A	Click **Save** to save the settings

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

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

b.1.5 SNMP

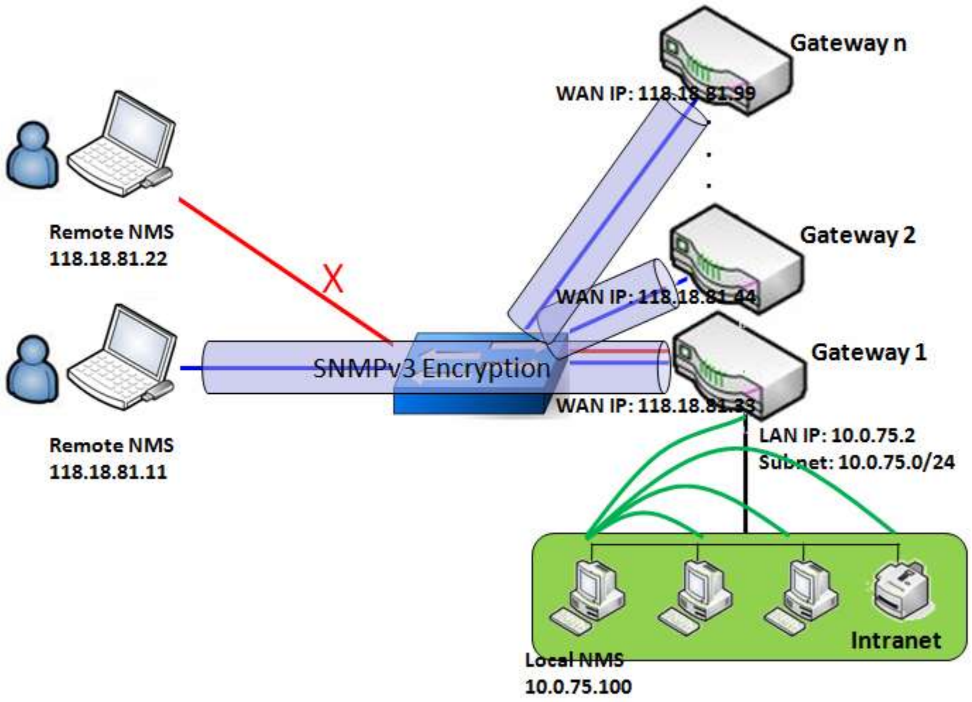
In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

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

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

The device supports several public MIBs and one private MIB for the SNMP agent. The supported MIBs are as follow: MIB-II (RFC 1213, Include IPv6), IF-MIB, IP-MIB, TCP-MIB, UDP-MIB, SMIv1 and SMIv2, SNMPv2-TM and SNMPv2-MIB, and AMIB (AirLive Private MIB)

SNMP Management Scenario



Scenario Application Timing

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

Scenario Description

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

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

Use SNMPv3 version of protocol can protected the transmitting of SNMP commands and responses.

The remote NMS with privilege IP address can manage the devices, but other remote NMS can't.

Parameter Setup Example

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

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

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

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

Scenario Operation Procedure

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

At first stage, the NMS manager prepares related information for all managed devices and records them in the NMS system. Then NMS system gets the status of all managed devices by using SNMP get commands.

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

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

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

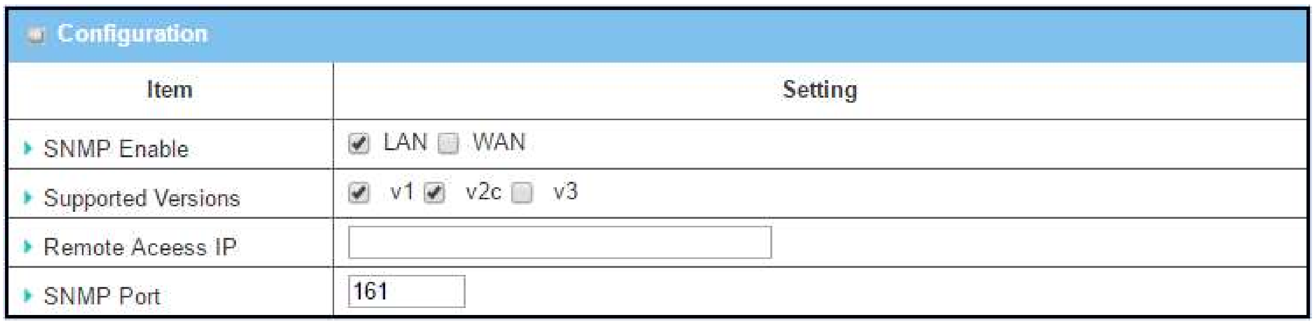
The remote NMS without privilege IP address can't manage the "Gateway 1", since "Gateway 1" allows only the NMS with privilege IP address can manage it via its WAN interface.

SNMP Setting

The SNMP allows user to configure SNMP relevant setting which includes interface, version, access control and trap receiver.

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

Enable SNMP



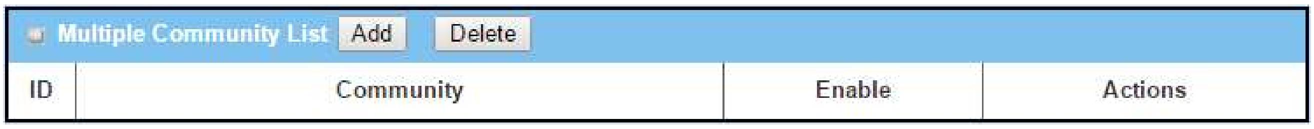
Item	Setting
SNMP Enable	☑ LAN ☐ WAN
Supported Versions	☑ v1 ☑ v2c ☐ v3
Remote Aceess IP	
SNMP Port	161

SNMP Item	Value setting	Description
SNMP Enable	1.The **LAN** box is checked by default	Select the interface for the SNMP and enable SNMP functions. When Check the **LAN** box. It will activate SNMP functions and you can access SNMP from LAN side. When Check the **WAN** box. It will activate SNMP functions and you can access SNMP from WAN side.
Supported Versions	1.The **v1** box is checked by default 2.The **v2c** box is checked by default	Select the version for the SNMP When Check the **v1** box. It means you can access SNMP by version 1. When Check the **v2c** box. It means you can access SNMP by version 2c. When Check the **v3** box. It means you can access SNMP by version 3.
Remote Aceess IP	1. String format: any Ipv4 address 2. It is an optional item.	Specify the **Remote Access IP** for WAN. If you filled in the IP address. It means only this IP address can access SNMP from WAN side. If you not filled. It means any IP address can access SNMP from WAN side.
SNMP Port	1. String format: any port number 2. The default SNMP port is 161 3. A Must filled setting	Specify the **SNMP Port**. You can fill in any port number. But you must ensure the port number is not to be used.

Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Create/Edit Multiple Community

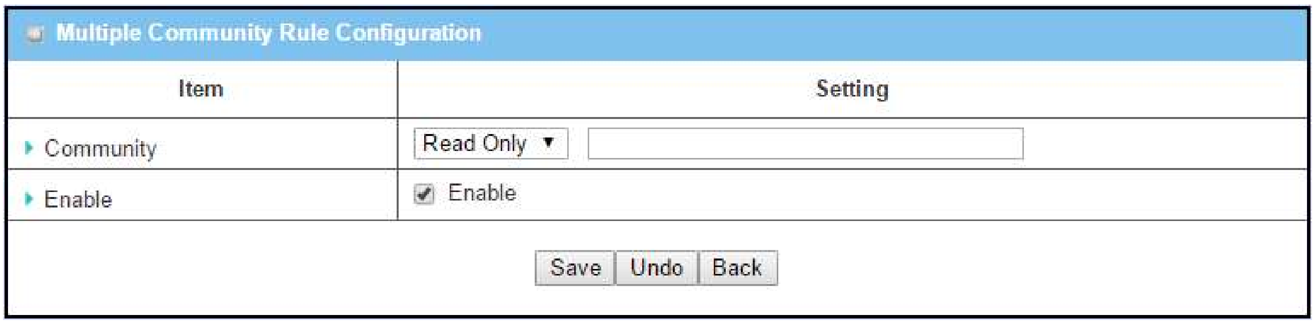
The SNMP allows you to custom your access control for version 1 and version 2 user. The router supports up to a maximum of 10 community sets.



Multiple Community List [Add] [Delete]

ID	Community	Enable	Actions

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



Multiple Community Rule Configuration

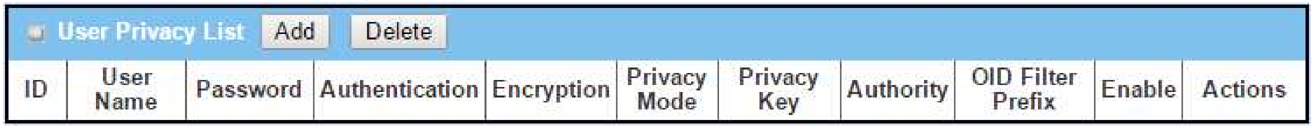
Item	Setting
Community	Read Only ▼
Enable	☑ Enable

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 this version 1 or version v2c user's community that will be allowed Read Only (GET and GETNEXT) or Read-Write (GET, GETNEXT and SET) access respectively. The maximum length of the community is 32.
Enable	1.The box is checked by default	Click the **Enable** button to enable this version 1 or version v2c user.
Save	N/A	Click the **Save** button to save the configuration. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show "Click on save button to apply your changes" remind user to click main page **Save** button.
Undo	N/A	Click the **Undo** button to cancel the settings.
Back	N/A	Click the **Back** button to return to last page.

M2M LTE Gateway with serial port

Create/Edit User Privacy

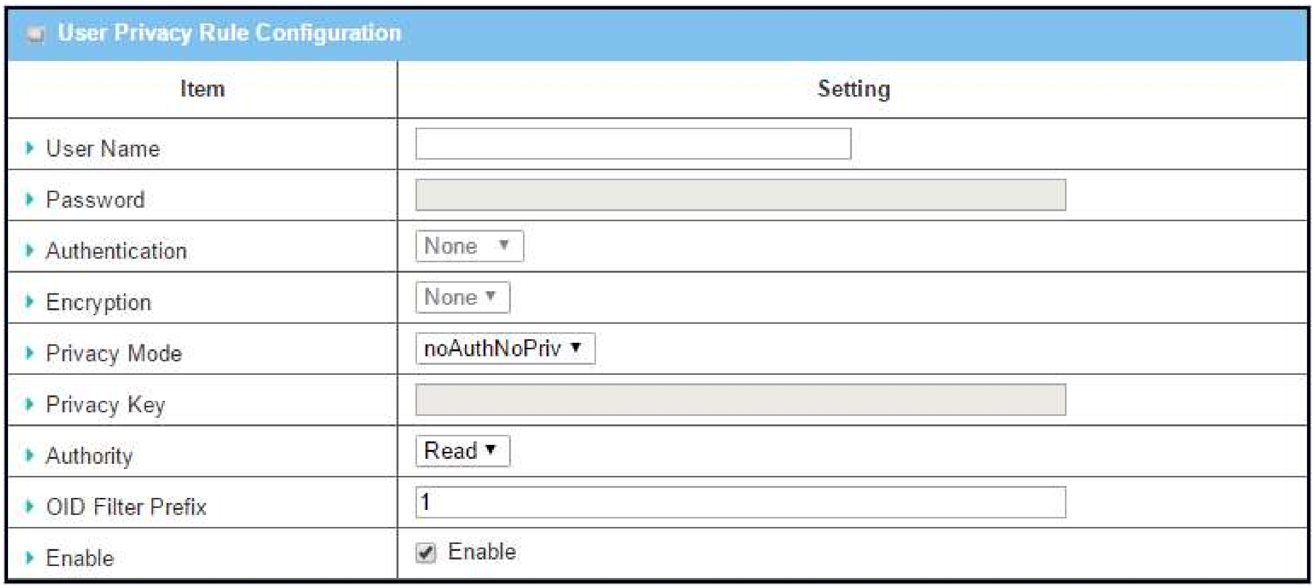
The SNMP allows you to custom your access control for version 3 user. The router supports up to a maximum of 128 User Privacy sets.



User Privacy List Add Delete

ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	OID Filter Prefix	Enable	Actions

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



User Privacy Rule Configuration

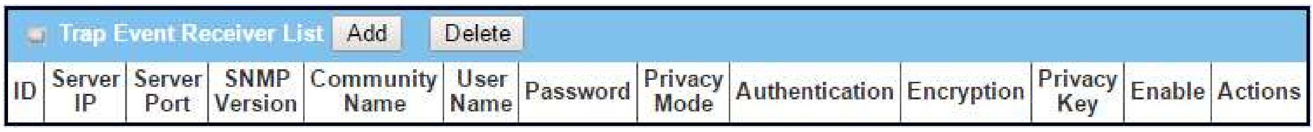
Item	Setting
User Name	
Password	
Authentication	None ▾
Encryption	None ▾
Privacy Mode	noAuthNoPriv ▾
Privacy Key	
Authority	Read ▾
OID Filter Prefix	1
Enable	☑ Enable

User Privacy Rule Configuration Item	Value setting	Description
User Name	1. A Must filled setting 2. String format: any text	Specify the **User Name** for this version 3 user. The maximum length of the user name is 32.
Password	1. String format: any text	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Password** for this version 3 user. The minimum length of the password is 8. The maximum length of the password is 64.
Authentication	1. **None** is selected by default	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Authentication** types for this version 3 user. Selected the authentication types **MD5/ SHA-1** to use.
Encryption	1. **None** is selected by default	When your **Privacy Mode** is **authPriv**, you must specify the **Encryption** protocols for this version 3 user.

		Selected the encryption protocols **DES / AES** to use.
Privacy Mode	1. **noAuthNoPriv** is selected by default	Specify the **Privacy Mode** for this version 3 user. Selected the **noAuthNoPriv**. You do not use any authentication types and encryption protocols. Selected the **authNoPriv**. You must specify the **Authentication** and **Password**. Selected the **authPriv**. You must specify the Authentication, Password, Encryption and Privacy Key.
Privacy Key	1. String format: any text	When your **Privacy Mode** is **authPriv**, you must specify the **Privacy Key** for this version 3 user. The minimum length of the privacy key is 8. The maximum length of the privacy key is 64.
Authority	1. **Read** is selected by default	Specify this version 3 user's **Authority** that will be allowed **Read Only** (GET and GETNEXT) or **Read-Write** (GET, GETNEXT and SET) access respectively.
OID Filter Prefix	1. The default value is 1 2. A Must filled setting 3. String format: any legal OID	The **OID Filter Prefix** restricts access for this version 3 user to the sub-tree rooted at the given OID. The range of the each OID number is 1-2080768.
Enable	1.The box is checked by default	Click **Enable** to enable this version 3 user.
Save	N/A	Click the **Save** button to save the configuration. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show "Click on save button to apply your changes" remind user to click main page **Save** button.
Undo	N/A	Click **Undo** to cancel the settings
Back	N/A	Click the **Back** button to return the last page.

Create/Edit Trap Event Receiver

The SNMP allows you to custom your trap event receiver. The router supports up to a maximum of 4 Trap Event Receiver sets.

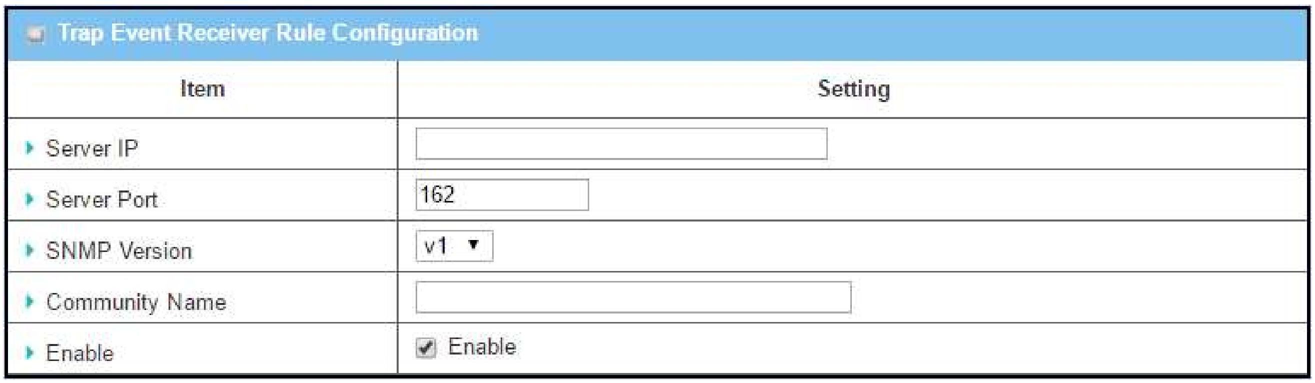


Trap Event Receiver List Add Delete

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

When **Add** button is applied, **Trap Event Receiver Rule Configuration** screen will appear. The default

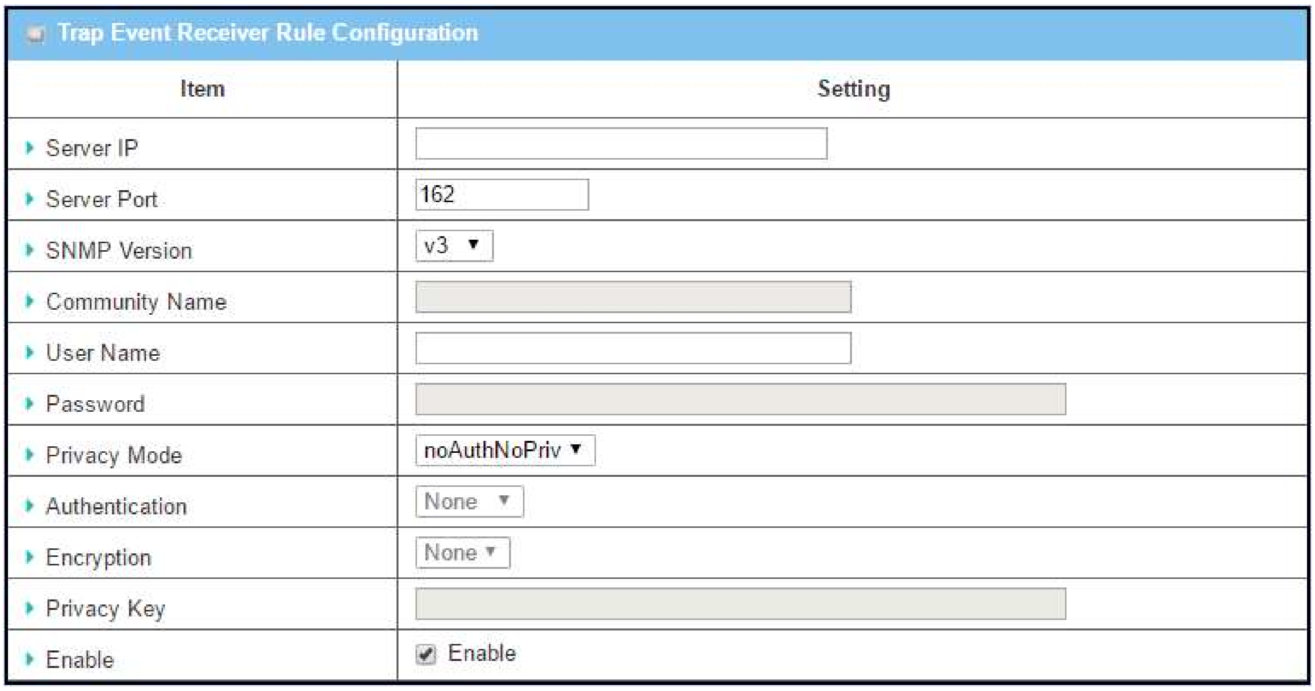
SNMP Version is v1. The configuration screen will provide the version 1 must filled items.



Trap Event Receiver Rule Configuration

Item	Setting
Server IP	
Server Port	162
SNMP Version	v1 ▼
Community Name	
Enable	☑ Enable

When you selected v2c, the configuration screen is exactly the same as that of v1, except the version. When you selected v3, the configuration screen will provide more setting items for the version 3 Trap.



Trap Event Receiver Rule Configuration

Item	Setting
Server IP	
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	Specify the trap **Server IP**. The DUT will send trap to the server IP.
Server Port	1. String format: any port number 2. The default SNMP trap port is 162	Specify the trap **Server Port**. You can fill in any port number. But you must ensure the port number is not to be used.

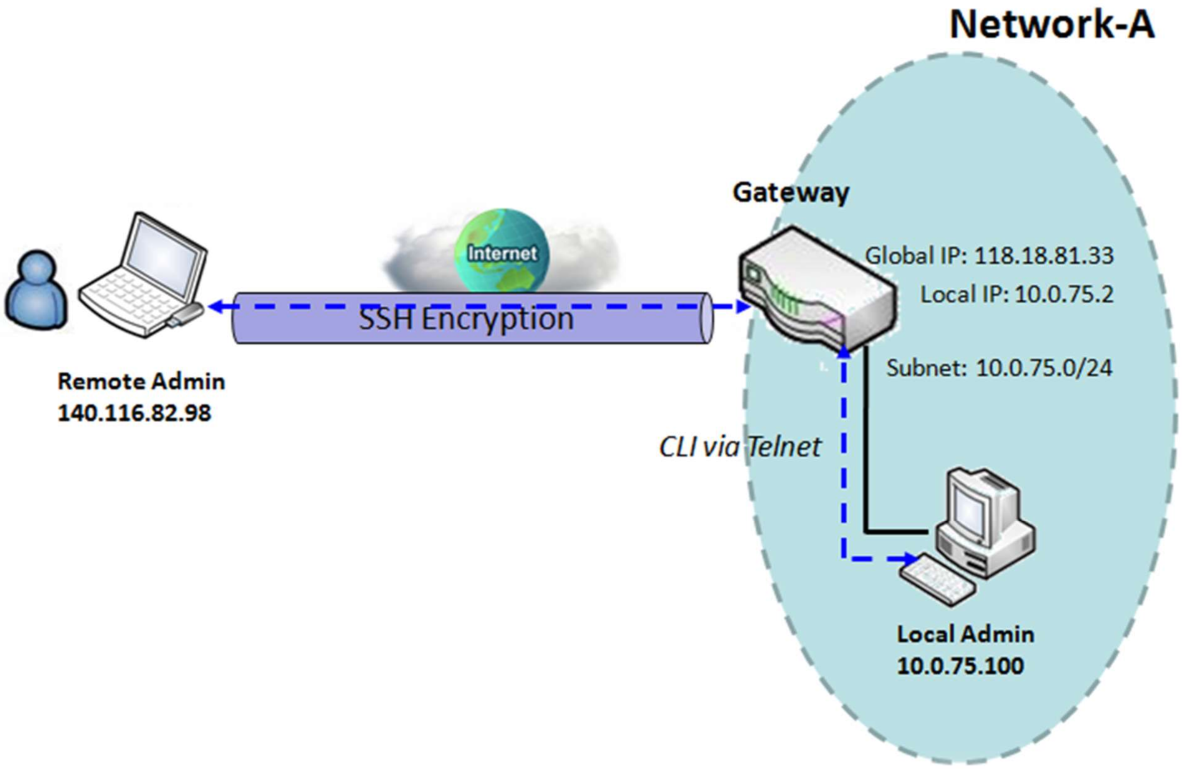
	3. A Must filled setting	
SNMP Version	1. **v1** is selected by default	Select the version for the trap Selected the **v1**. The configuration screen will provide the version 1 must filled items. Selected the **v2c**. The configuration screen will provide the version 2c must filled items. Selected the **v3**. The configuration screen will provide the version 3 must filled items.
Community Name	1. A **v1** and **v2c** Must filled setting 2. String format: any text	Specify the **Community Name** for this version 1 or version v2c trap. The maximum length of the community name is 32.
User Name	1. A **v3** Must filled setting 2. String format: any text	Specify the **User Name** for this version 3 trap. The maximum length of the user name is 32.
Password	1. A **v3** Must filled setting 2. String format: any text	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Password** for this version 3 trap. The minimum length of the password is 8. The maximum length of the password is 64.
Privacy Mode	1. A **v3** Must filled setting 2. **noAuthNoPriv** is selected by default	Specify the **Privacy Mode** for this version 3 trap. Selected the **noAuthNoPriv**. You do not use any authentication types and encryption protocols. Selected the **authNoPriv**. You must specify the **Authentication** and **Password**. Selected the **authPriv**. You must specify the Authentication, Password, Encryption and Privacy Key.
Authentication	1. A **v3** Must filled setting 2. **None** is selected by default	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Authentication** types for this version 3 trap. Selected the authentication types **MD5/ SHA-1** to use.
Encryption	1. A **v3** Must filled setting 2. **None** is selected by default	When your **Privacy Mode** is **authPriv**, you must specify the **Encryption** protocols for this version 3 trap. Selected the encryption protocols **DES / AES** to use.
Privacy Key	1. A **v3** Must filled setting 2. String format: any text	When your **Privacy Mode** is **authPriv**, you must specify the **Privacy Key** for this version 3 trap. The minimum length of the privacy key is 8. The maximum length of the privacy key is 64.
Enable	1.The box is checked by default	Click **Enable** to enable this trap receiver.

Save	N/A	Click the **Save** button to save the configuration. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show “Click on save button to apply your changes” remind user to click main page **Save** button.
Undo	N/A	Click **Undo** to cancel the settings.
Back	N/A	Click the **Back** button to return the last page.

b.1.7 Telnet with CLI

A command-line interface (CLI), also known as command-line user interface, and console user interface are means of interacting with a computer program where the user (or client) issues commands to the program in the form of successive lines of text (command lines). The interface is usually implemented with a command line shell, which is a program that accepts commands as text input and converts commands to appropriate operating system functions. Programs with command-line interfaces are generally easier to automate via scripting. The device supports both Telnet and SSH (Secure Shell) CLI with default service port 23 and 22, respectively.

Telnet & SSH Scenario



Scenario Application Timing

When the administrator of the gateway wants to manage it from remote site in the Intranet or Internet, he may use "Telnet with CLI" function to do that by using "Telnet" or "SSH" utility.

Scenario Description

The Local Admin or the Remote Admin can manage the Gateway by using "Telnet" or "SSH" utility with privileged user name and password.

The data packets between the Local Admin and the Gateway or between the Remote Admin and the Gateway can be plain texts or encrypted texts. Suggest they are plain texts in the Intranet for Local Admin to use "Telnet" utility, and encrypted texts in the Internet for Remote Admin to use "SSH" utility.

Parameter Setup Example

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

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

Configuration Path	[Telnet with CLI]-[Configuration]
Telnet with CLI	LAN: ■ ***Enable*** WAN: ■ ***Enable***
Connection Type	Telnet: Service Port ***23*** ■ ***Enable*** SSH: Service Port ***22*** ■ ***Enable***

Scenario Operation Procedure

In above diagram, "Local Admin" or "Remote Admin" can manage the "Gateway" in the Intranet or Internet. The "Gateway" is the gateway of Network-A, and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. It serves as a NAT gateway.

The "Local Admin" in the Intranet uses "Telnet" utility with privileged account to login the Gateway.

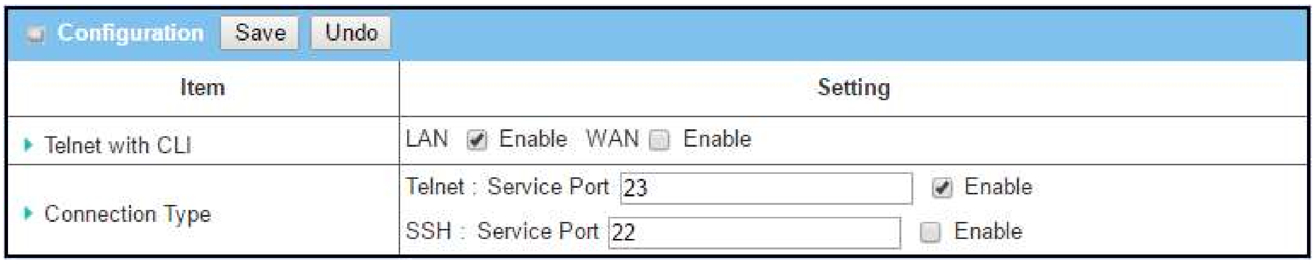
Or the "Remote Admin" in the Internet uses "SSH" utility with privileged account to login the Gateway.

The administrator of the gateway can control the device as like he is in front of the gateway.

Telnet with CLI Setting

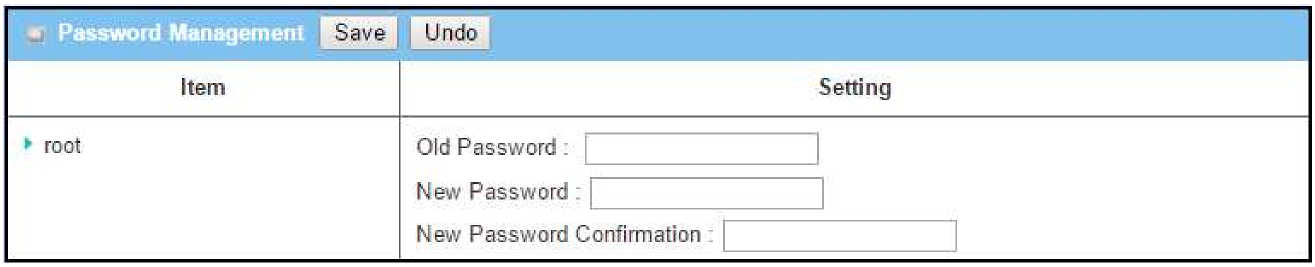
The Telnet with CLI setting allows administrator to access this device through the traditional Telnet program. Before you can telnet (login) to the device, please configure the related settings and password with care. The password management part allows you to set root password for logging telnet and SSH.

Go to Administration > Configure & Manage > Telnet with CLI tab.



Item	Setting
Telnet with CLI	LAN ☑ Enable WAN □ Enable
Connection Type	Telnet : Service Port 23 ☑ Enable SSH : Service Port 22 □ Enable

Configuration		
Item	**Value setting**	**Description**
Telnet with CLI	1. The LAN Enable box is checked by default. 2. The WAN Enable box is unchecked by default.	Check the **Enable** box to activate the Telnet with CLI function for connecting from WAN/LAN interfaces.
Connection Type	1. The Telnet Enable box is checked by default. By default **Service Port** is 23. 2. The SSH Enable box is unchecked by default. By default **Service Port** is 22.	Check the Telnet **Enable** box to activate telnet service. Check the SSH **Enable** box to activate SSH service. You can set which number of **Service Port** you want to provide for the corresponding service.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings



Item	Setting
root	Old Password : New Password : New Password Confirmation :

Configuration Item	Value setting	Description
root	1. String: any text but no blank character 2. The default password for telnet is ‘m2mamit’.	Type old password and specify new password to change root password. ***Note: You are highly recommended to change the default telnet password with yours before the device is deployed.***
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

b.3 System Operation

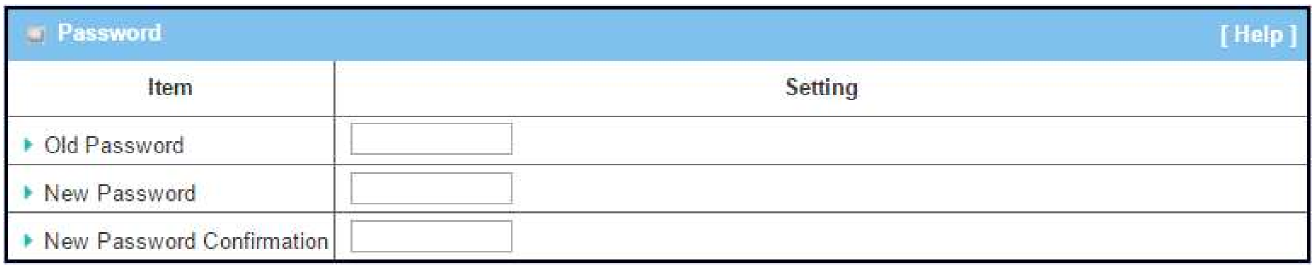
System Operation allows the network administrator to manage system, settings such as web-based utility access password change, system information, system time, system log, firmware/configuration backup & restore, and reset & reboot.

b.3.1 Password & MMI

Go to **Administration > System Operation > Password & MMI** tab.

Change Password

Change password screen allows network administrator to change the web-based MMI login password to access gateway.



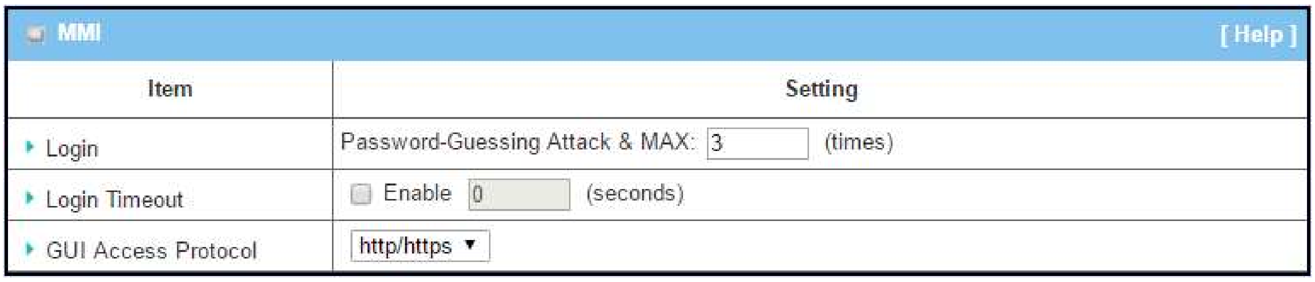
Password [Help]

Item	Setting
Old Password	
New Password	
New Password Confirmation	

Change Password		
Item	**Value Setting**	**Description**
Old Password	1. String: any text **2. The default password for web-based MMI is 'admin'.**	Enter the current password to enable you unlock to change password.
New Password	String: any text	Enter new password.
New Password Confirmation	String: any text	Enter new password again to confirm.

Change MMI Setting for Accessing

This is the gateway's web-based MMI access which allows administrator to access the gateway for management. The gateway's web-based MMI will automatically logout when the idle time has elapsed. The setting allows administrator to enable automatic logout and set the logout idle time. When the login timeout is disabled, the system won't logout the administrator automatically.



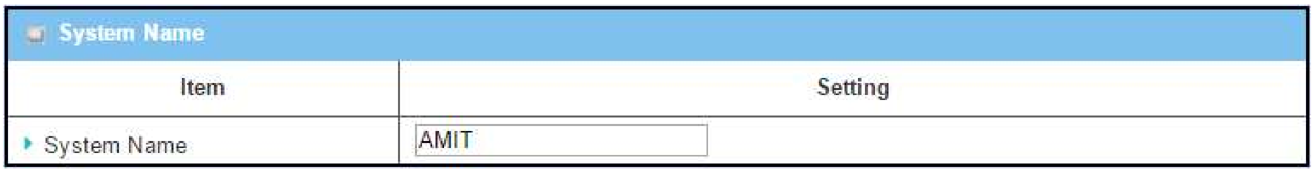
Item	Setting
Login	Password-Guessing Attack & MAX: 3 (times)
Login Timeout	□ Enable 0 (seconds)
GUI Access Protocol	http/https ▾

Web UI Item	Value Setting	Description
Login	3 times is set by default	Enter the login trial counting value. If someone tried to login the web GUI with incorrect password for more than the counting value, an warning message "***Already reaching maximum Password-Guessing times, please wait a few seconds!***" will be displayed and ignore the following login trials.
Login Timeout	The Enable box is unchecked by default	Check the Enable box to activate the auto logout function, and specify the maximum idle time as well.
GUI Access Protocol	http/https is selected by default.	Select the protocol that will be used for GUI access. It can be **http/https**, **http only**, or **https only**.
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

b.3.3 System Information

System Information screen gives network administrator a quick look up on the type of WAN connection being used. The display also shows the current System time. It is particularly useful when firmware has been upgraded and system configuration file has been loaded.

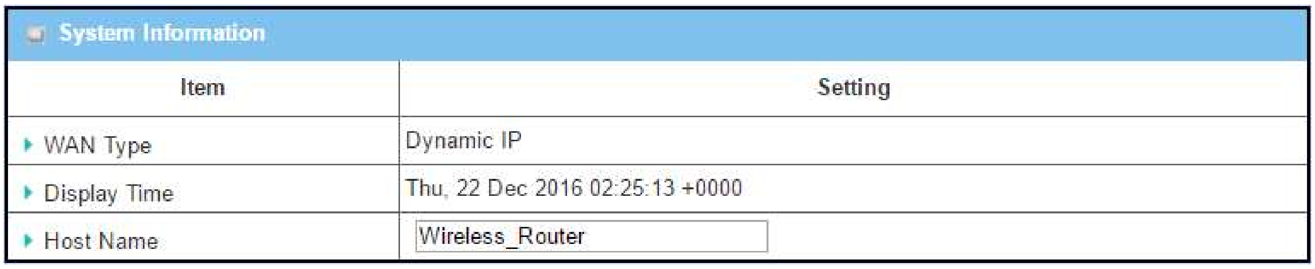
Go to **Administration > System Operation > System Information** tab.



System Name

Item	Setting
System Name	AMIT

System Name		
Item	**Value Setting**	**Description**
System Name	1. an optional item 2. AirLive is set by default.	Enter the system name for identification purpose. It can be the manufacture, or any name for a device deployment.



System Information

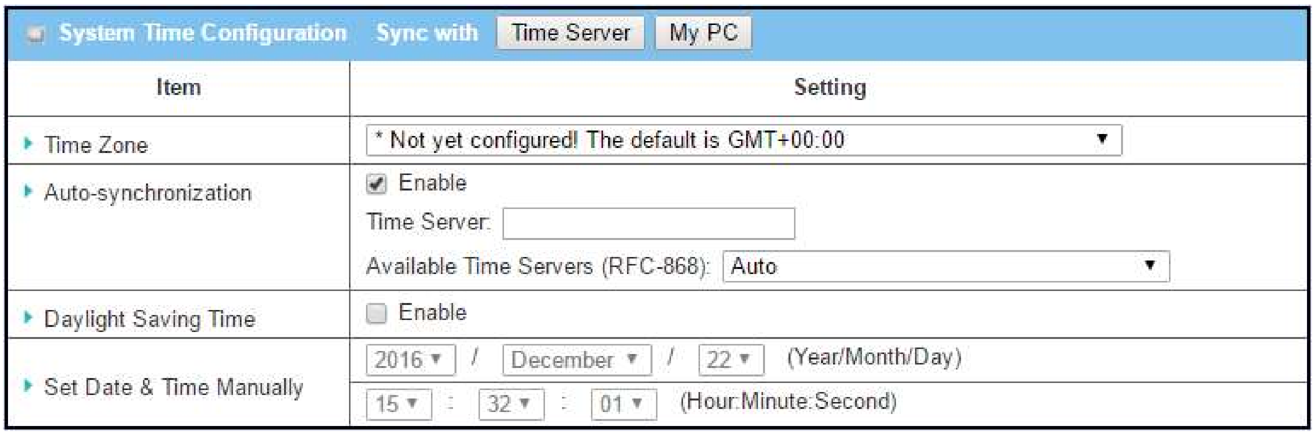
Item	Setting
WAN Type	Dynamic IP
Display Time	Thu, 22 Dec 2016 02:25:13 +0000
Host Name	Wireless_Router

System Information		
Item	**Value Setting**	**Description**
WAN Type	N/A	It displays the WAN Type of WAN-1 Interface Internet connection configured.
Display Time	N/A	It displays the current system time that you browsed this web page.
Host Name	1. It is an optional item 2. Wireless_Router is set by default.	Enter the host name for the gateway. It can be used to interact with external network servers for identifying the name of requesting device.
Save	N/A	Click **Save** button to save the settings.
Refresh	N/A	Click **Refresh** button to update the system Information immediately.

b.3.5 System Time

The gateway provides manually setup and auto-synchronized approaches for the administrator to setup the system time for the gateway.

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



Item	Setting
Time Zone	* Not yet configured! The default is GMT+00:00 ▼
Auto-synchronization	☑ Enable Time Server: Available Time Servers (RFC-868): Auto ▼
Daylight Saving Time	□ Enable
Set Date & Time Manually	2016 ▼ / December ▼ / 22 ▼ (Year/Month/Day) 15 ▼ : 32 ▼ : 01 ▼ (Hour:Minute:Second)

System Time Information Item	 Value Setting	 Description
Time Zone	1. It is an optional item. 2. Not yet configured is selected by default.	Select a time zone where this device locates.
Auto-synchronization	1. Checked by default. 2. Auto is selected by default.	Check the **Enable** button to activate the time auto-synchronization function with a certain NTP server. You can enter the IP or FQDN for the NTP server you expected, or leave it as auto mode so that the available server will be used for time synchronization one by one.
Daylight Saving Time	1. It is an optional item. 2. Un-checked by default	Check the **Enable** button to activate the daylight saving function. When you enabled this function, you have to specify the start date and end date for the daylight saving time duration.
Set Date & Time	1. It is an optional item.	If you do not enable the time auto-synchronization function, you can also manually set the date (Year/Month/Day(and time (Hour:Minute:Second).
Save	N/A	Click **Save** button to save the settings.
Refresh	N/A	Click **Refresh** button to update the system time immediately.

Instead of manually configuring the system time for the gateway, there are two simple and quick solutions for you to set the correct time information and set it as the system time for the gateway.

The first one is “Sync with Timer Server”. Based on your selection of time zone and time server in above time information configuration window, system will communicate with time server by NTP Protocol to get system date and time after you click on the **Sync with Timer Server** button.

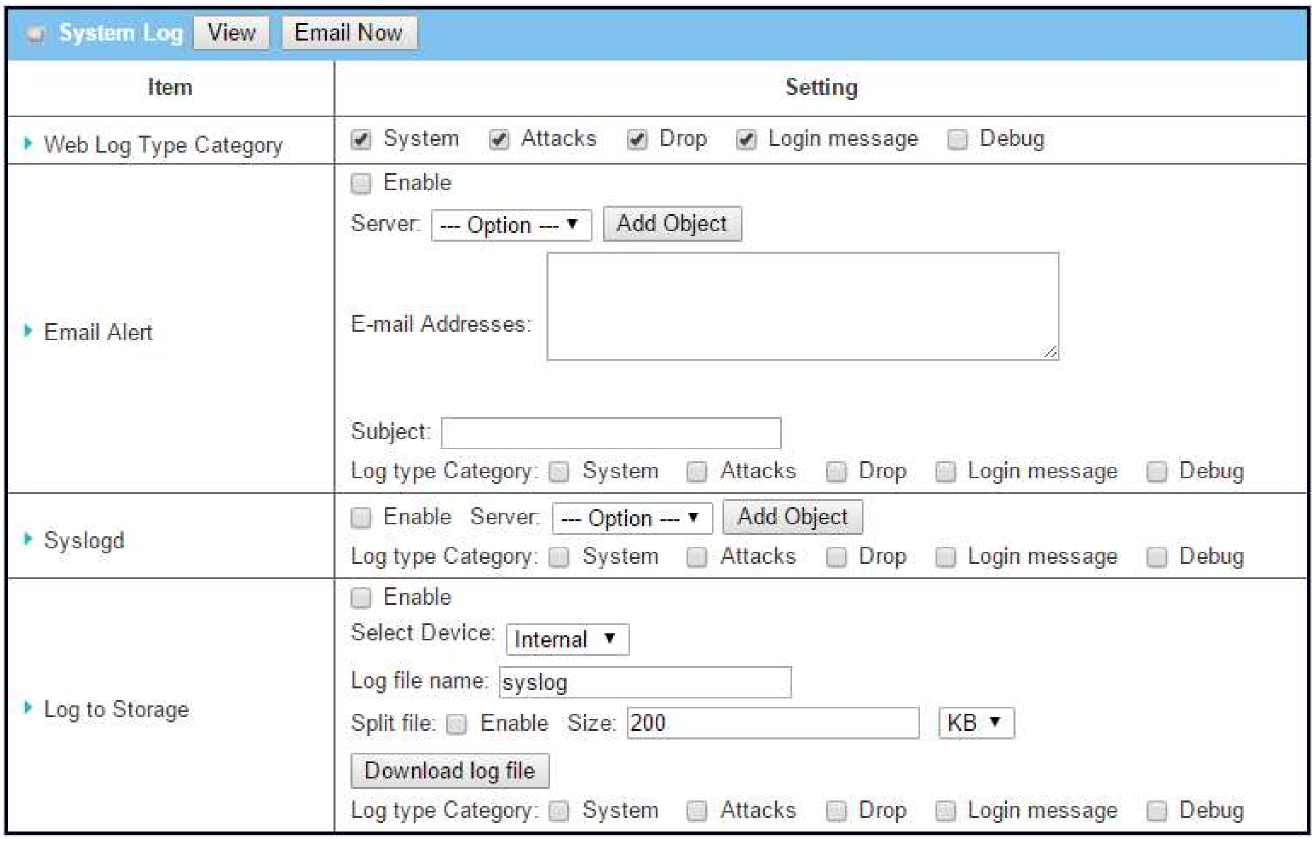
Note: Remember to select a correct time zone for the device, otherwise, you will just get the UTC (Coordinated Universal Time) time, not the local time for the device.

The second one is “Sync with my PC”. Click on the **Sync with my PC** button to let system synchronize its date and time to the time of the administration PC.

b.3.7 System Log

System Log screen contains various event log tools facilitating network administrator to perform local event logging and remote reporting.

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



System Log | View | Email Now

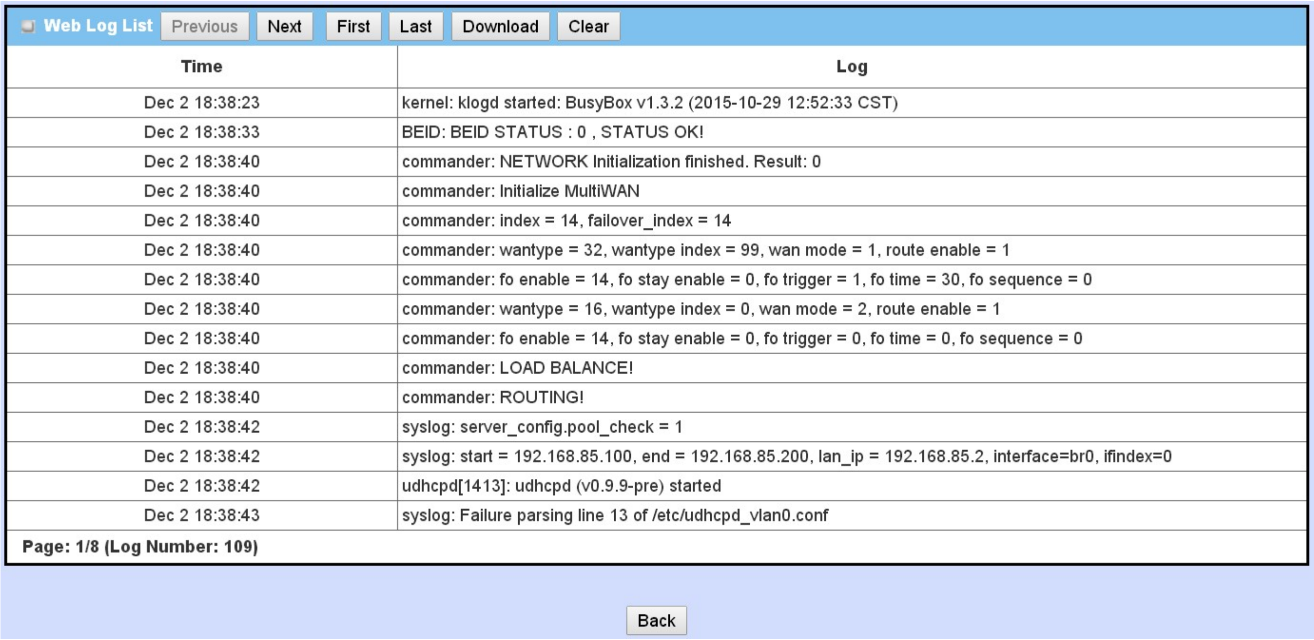
Item	Setting
Web Log Type Category	☑ System ☑ Attacks ☑ Drop ☑ Login message □ Debug
Email Alert	□ Enable Server: --- Option --- ▾ Add Object E-mail Addresses: Subject: Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug
Syslogd	□ Enable Server: --- Option --- ▾ Add Object Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug
Log to Storage	□ Enable Select Device: Internal ▾ Log file name: syslog Split file: □ Enable Size: 200 KB ▾ Download log file Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug

View & Email Log History

View button is provided for network administrator to view log history on the gateway. **Email Now** button enables administrator to send instant Email for analysis.

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

button



Time	Log
Dec 2 18:38:23	kernel: klogd started: BusyBox v1.3.2 (2015-10-29 12:52:33 CST)
Dec 2 18:38:33	BEID: BEID STATUS : 0 , STATUS OK!
Dec 2 18:38:40	commander: NETWORK Initialization finished. Result: 0
Dec 2 18:38:40	commander: Initialize MultiWAN
Dec 2 18:38:40	commander: index = 14, failover_index = 14
Dec 2 18:38:40	commander: wantype = 32, wantype index = 99, wan mode = 1, route enable = 1
Dec 2 18:38:40	commander: fo enable = 14, fo stay enable = 0, fo trigger = 1, fo time = 30, fo sequence = 0
Dec 2 18:38:40	commander: wantype = 16, wantype index = 0, wan mode = 2, route enable = 1
Dec 2 18:38:40	commander: fo enable = 14, fo stay enable = 0, fo trigger = 0, fo time = 0, fo sequence = 0
Dec 2 18:38:40	commander: LOAD BALANCE!
Dec 2 18:38:40	commander: ROUTING!
Dec 2 18:38:42	syslog: server_config.pool_check = 1
Dec 2 18:38:42	syslog: start = 192.168.85.100, end = 192.168.85.200, lan_ip = 192.168.85.2, interface=br0, ifindex=0
Dec 2 18:38:42	udhcpd[1413]: udhcpd (v0.9.9-pre) started
Dec 2 18:38:43	syslog: Failure parsing line 13 of /etc/udhcpd_vlan0.conf

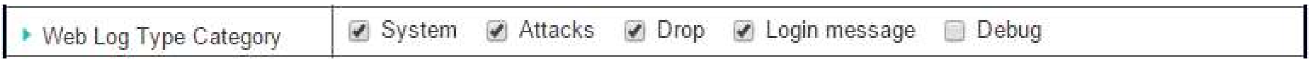
Page: 1/8 (Log Number: 109)

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

Web Log List Button Description		
Item	**Value setting**	**Description**
Previous	N/A	Click the **Previous** button to move to the previous page.
Next	N/A	Click the **Next** button to move to the next page.
First	N/A	Click the **First** button to jump to the first page.
Last	N/A	Click the **Last** button to jump to the last page.
Download	N/A	Click the **Download** button to download log to your PC in tar file format.
Clear	N/A	Click the **Clear** button to clear all log.
Back	N/A	Click **Back** button to return to the previous page.

Web Log Type Category

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



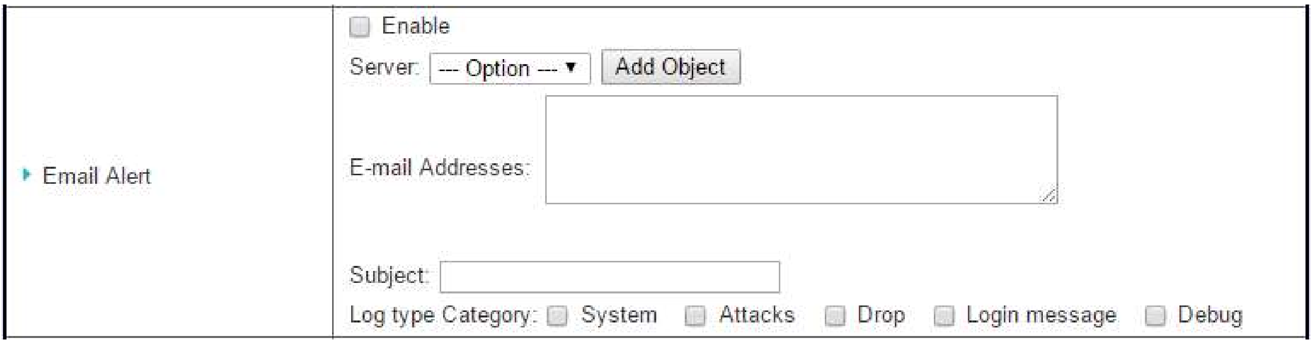
‣ Web Log Type Category	☑ System ☑ Attacks ☑ Drop ☑ Login message □ Debug

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

Email Alert screen allows network administrator to select the type of event to log and be sent to the destined Email account.



‣ Email Alert	□ Enable Server: --- Option --- ▾ [Add Object] E-mail Addresses: Subject: Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug

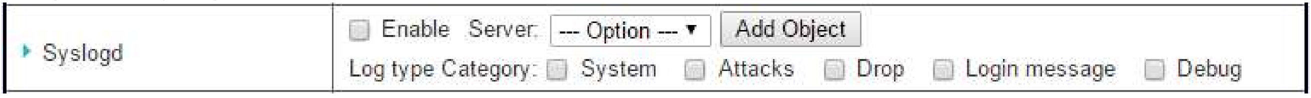
Email Alert Setting Window

Item	Value Setting	Description
Enable	Un-checked by default	Check **Enable** box to enable sending event log messages to destined Email account defined in the E-mail Addresses blank space.
Server	N/A	Select one email server from the Server dropdown box to send Email. If none has been available, click the **Add Object** button to create an outgoing Email server. You may also add an outgoing Email server from Object Definition > External Server > External Server tab.
E-mail address	String : email format	Enter the recipient's Email address. Separate Email addresses with comma ',' or semicolon ' ;' Enter the Email address in the format of '*myemail@domain.com*'
Subject	String : any text	Enter an Email subject that is easy for you to identify on the Email client.

Log type category	Default unchecked	Select the type of events to log and be sent to the designated Email account. Available events are System, Attacks, Drop, Login message, and Debug.

Syslogd

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



Syslogd

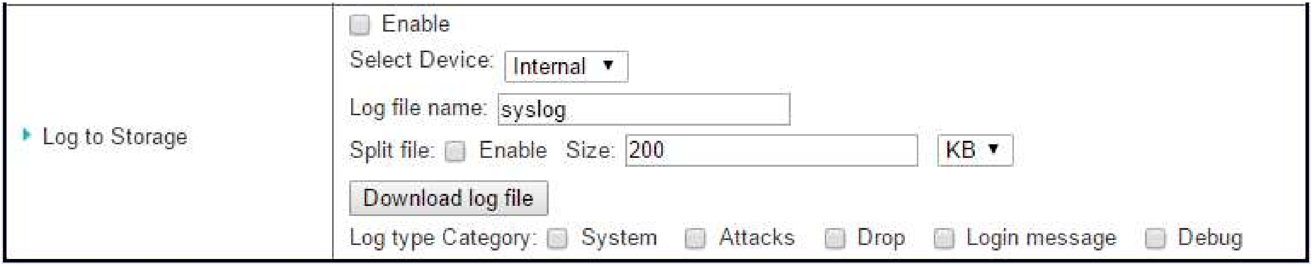
□ Enable Server: --- Option --- Add Object

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

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

Log to Storage

Log to Storage screen allows network administrator to select the type of events to log and be stored at an internal or an external storage.



Log to Storage

□ Enable

Select Device: Internal

Log file name: syslog

Split file: □ Enable Size: 200 KB

Download log file

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 sending log to storage.
Select Device	Internal is selected by default	Select internal or external storage.
Log file name	Un-checked by default	Enter log file name to save logs in designated storage.
Split file Enable	Un-checked by default	Check **enable** box to split file whenever log file reaching the specified limit.
Split file Size	200 KB is set by default	Enter the file size limit for each split log file.
Log type category	Un-checked by default	Check which type of logs to send: System, Attacks, Drop, Login message, Debug

Log to Storage Button Description

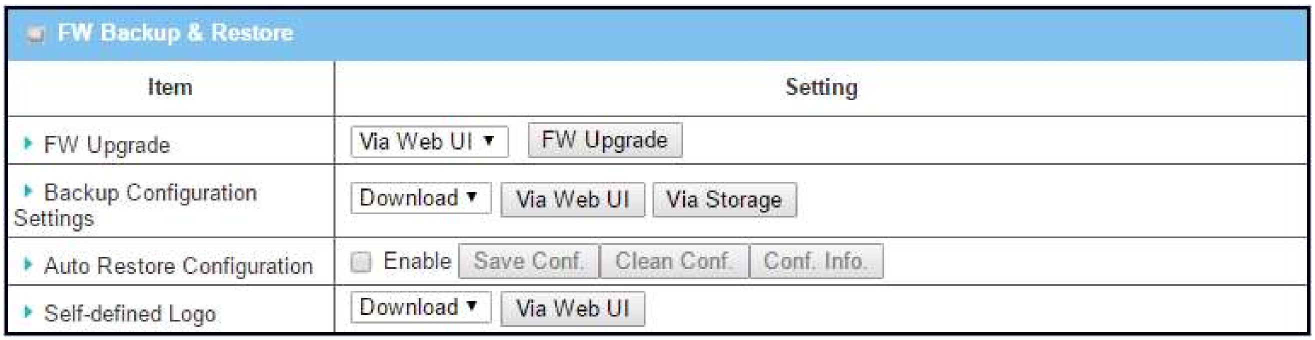
Item	Value setting	Description
Download log file	N/A	Click the **Download log file** button to download log files to a log.tar file.

b.3.9 Backup & Restore

In the Backup & Restore window, you can upgrade the device firmware when new firmware is available, and also backup / restore the device configuration.

In addition to the factory default settings, you can also customize a special configuration setting as a customized default value. With this customized default value, you can reset the device to the expected default setting if needed.

Go to **Administration > System Operation > Backup & Restore** tab.



FW Backup & Restore

Item	Setting
FW Upgrade	Via Web UI ▾ FW Upgrade
Backup Configuration Settings	Download ▾ Via Web UI Via Storage
Auto Restore Configuration	□ Enable Save Conf. Clean Conf. Conf. Info.
Self-defined Logo	Download ▾ Via Web UI

Log to Storage Setting Window		
Item	**Value Setting**	**Description**
FW Upgrade	Via Web UI is selected by default	If new firmware is available, click the **FW Upgrade** button to upgrade the device firmware **via Web UI**, or **Via Storage**. After clicking on the “FW Upgrade” command button, you need to specify the file name of new firmware by using “Browse” button, and then click “Upgrade” button to start the FW upgrading process on this device. If you want to upgrade a firmware which is from GPL policy, please check “Accept unofficial firmware”
Backup Configuration Settings	Download is selected by default	You can backup or restore the device configuration settings by clicking the *Via Web UI* or **Via Storage** button. **Download**: for backup the device configuration to a config.bin file. **Upload**: for restore a designated configuration file to the device. **Via Web UI**: to retrieve the configuration file via Web GUI. **Via Storage**: to retrieve the configuration file via local attached storage.
Auto Restore Configuration	The Enable box is unchecked by default	Chick the **Enable** button to activate the customized default setting function. Once the function is activated, you can save the expected setting as a customized default setting by clicking the **Save Conf.** button, or clicking the **Clean Conf.** button to erase the stored customized configuration.

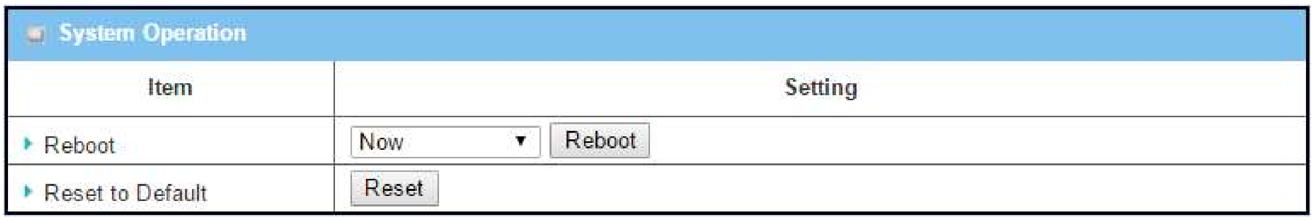
M2M LTE Gateway with serial port

b.3.b Reboot & Reset

For some special reason or situation, you may need to reboot the gateway or reset the device configuration to its default value. In addition to perform these operations through the Power ON/OFF, or pressing the reset button on the device panel, you can do it through the web GUI too.

In the Reboot & Reset window, you can reboot this device by clicking the “Reboot” button, and reset this device to default settings by clicking the “Reset” button.

Go to **Administration > System Operation > Reboot & Reset** tab.



System Operation

Item	Setting
Reboot	Now ▾ Reboot
Reset to Default	Reset

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

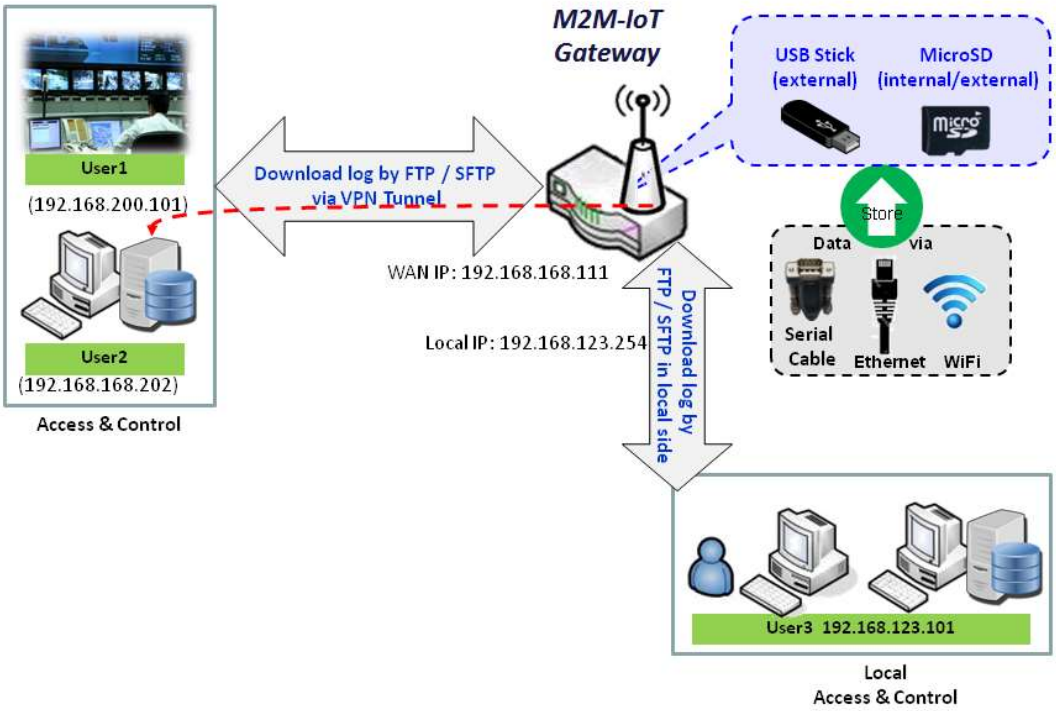
b.5 FTP

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

For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). Besides, SSH File Transfer Protocol (SFTP) is sometimes also used instead, but is technologically different.

This gateway embedded FTP / SFTP server for administrator to download the log files to his computer or database. In the following two sections, you can configure the FTP server and create the user accounts that can login to the server. After login to the FTP server, you can browse the log directory and have the permission to download the stored log files and delete the files you have downloaded to make more storage space for further data logs.

The available log files can be system logs (refer to Administration > System Operation > System Log), Network Packets (refer to Administrator > Diagnostic > Packet Analyzer), Data Log (refer to Field Communication > Data Logging > Log File Management), and GNSS Log (refer to Service > Location Tracking > GNSS). With proper configuration for the various log functions that supported on your purchased product, you can download the log via FTP / SFTP connections.

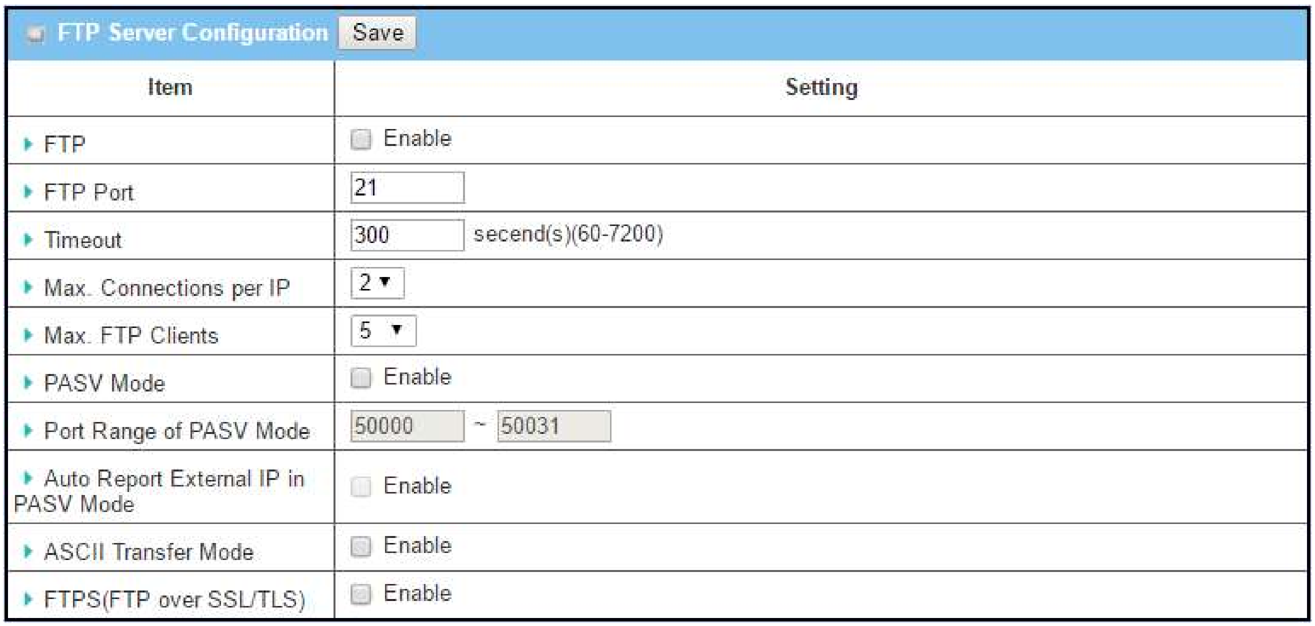


b.5.1 Server Configuration

This section allows user to setup the embedded FTP and SFTP server for retrieving the interested fog files.

Go to Administration > FTP > Server Configuration tab.

Enable FTP Server



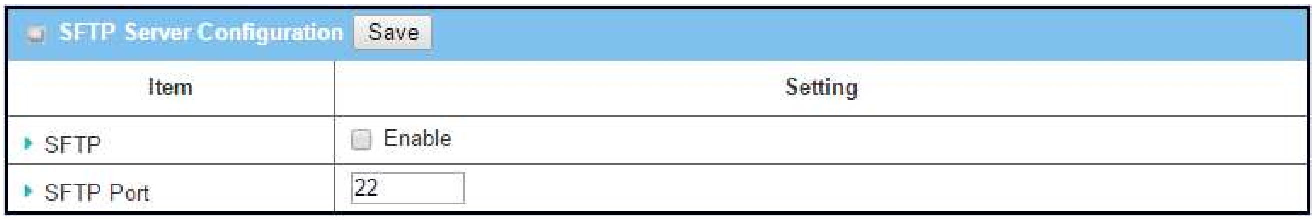
FTP Server Configuration

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.	Check **Enable** box to activate the embedded FTP Server function. With the FTP Server enabled, you can retrieve or delete the stored log files via FTP connection. Note: The embedded FTP Server is only for log downloading, so no any write permission is implemented for user file upload to the storage.
FTP Port	Port **21** is set by default	Specify a port number for FTP connection. The gateway will listen for incoming FTP connections on the specified port.
Timeout	**300** seconds is set by default.	Specify the maximum timeout interval for the FTP connection. Supported range is 60 to 7200 seconds.
Max. Connections per IP	**2** Clients are set by default.	Specify the maximum number of clients from the same IP address for the FTP connection. Up to 5 clients from the same IP address is supported.
Max. FTP	**5** Clients are set by	Specify the maximum number of clients for the FTP connection. Up to 32

Clients	default.	clients is supported.
PASV Mode	Optional setting	Check the **Enable** box to activate the support of PASV mode for a FTP connection from FTP clients.
Port Range of PASV Mode	Port **50000** ~ **50031** is set by default.	Specify the port range to allocate for PASV style data connection.
Auto Report External IP in PASV Mode	Optional setting	Check the **Enable** box to activate the support of overriding the IP address advertising in response to the PASV command.
ASCII Transfer Mode	Optional setting	Check the **Enable** box to activate the support of ASCII mode data transfers. Binary mode is supported by default.
FTPS (FTP over SSL/TLS)	Optional setting	Check the **Enable** box to activate the support of secure connections via SSL/TLS.

Enable SFTP Server



SFTP Server Configuration [Save]

Item	Setting
SFTP	□ Enable
SFTP Port	22

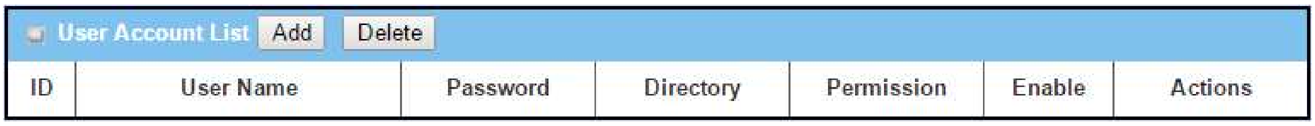
Configuration Item	Value setting	Description
SFTP	The box is unchecked by default.	Check **Enable** box to activate the embedded SFTP Server function. With the SFTP Server enabled, you can retrieve or delete the stored log files via secure SFTP connection.
SFTP Port	Default 22	Specify a port number for SFTP connection. The gateway will listen for incoming SFTP connections on the specified port.

b.5.3 User Account

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

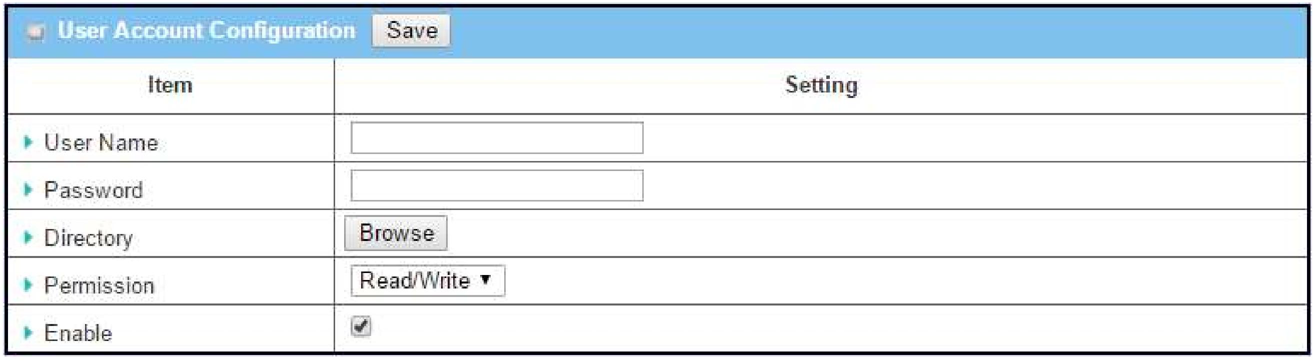
Go to Administration > FTP > User Account tab.

Create/Edit FTP User Accounts



ID	User Name	Password	Directory	Permission	Enable	Actions

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



Item	Setting
User Name	
Password	
Directory	Browse
Permission	Read/Write ▾
Enable	☑

Configuration Item	Value setting	Description
User Name	String : non-blank string	Enter the user account for login to the FTP server.
Password	String : no blank	Enter the user password for login to the FTP server.
Directory	N/A	Select a root directory after user login.
Permission	**Read/Write** is selected by default.	Select the Read/write permission. Note: The embedded FTP Server is only for log downloading, so no any write permission is implemented for user file upload to the storage, even **Read/Write** option is selected.
Enable	The box is checked by default.	Check the box to activate the FTP user account.

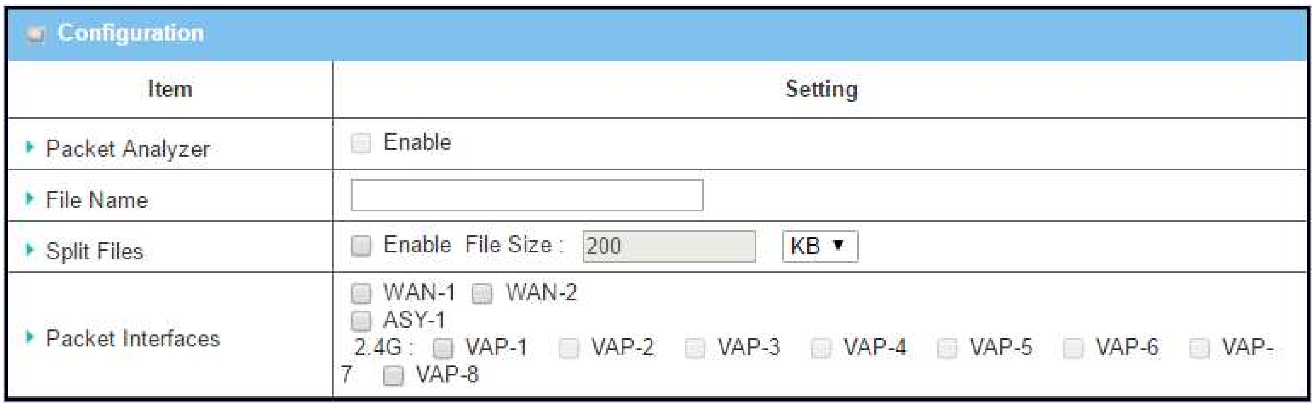
b.7 Diagnostic

This gateway supports simple network diagnosis tools for the administrator to troubleshoot and find the root cause of the abnormal behavior or traffics passing through the gateway. There can be a Packet Analyzer to help record the packets for a designated interface or specific source/destination host, and another Ping and Tracert tools for testing the network connectivity issues.

b.7.1 Packet Analyzer

The Packet Analyzer can capture packets depend on user settings. User can specify interfaces to capture packets and filter by setting rule. Ensure the log storage is available (either embedded SD-Card or external USB Storage), otherwise **Packet Analyzer** can not be enabled.

Go to Administration > Diagnostic > Packet Analyzer tab.



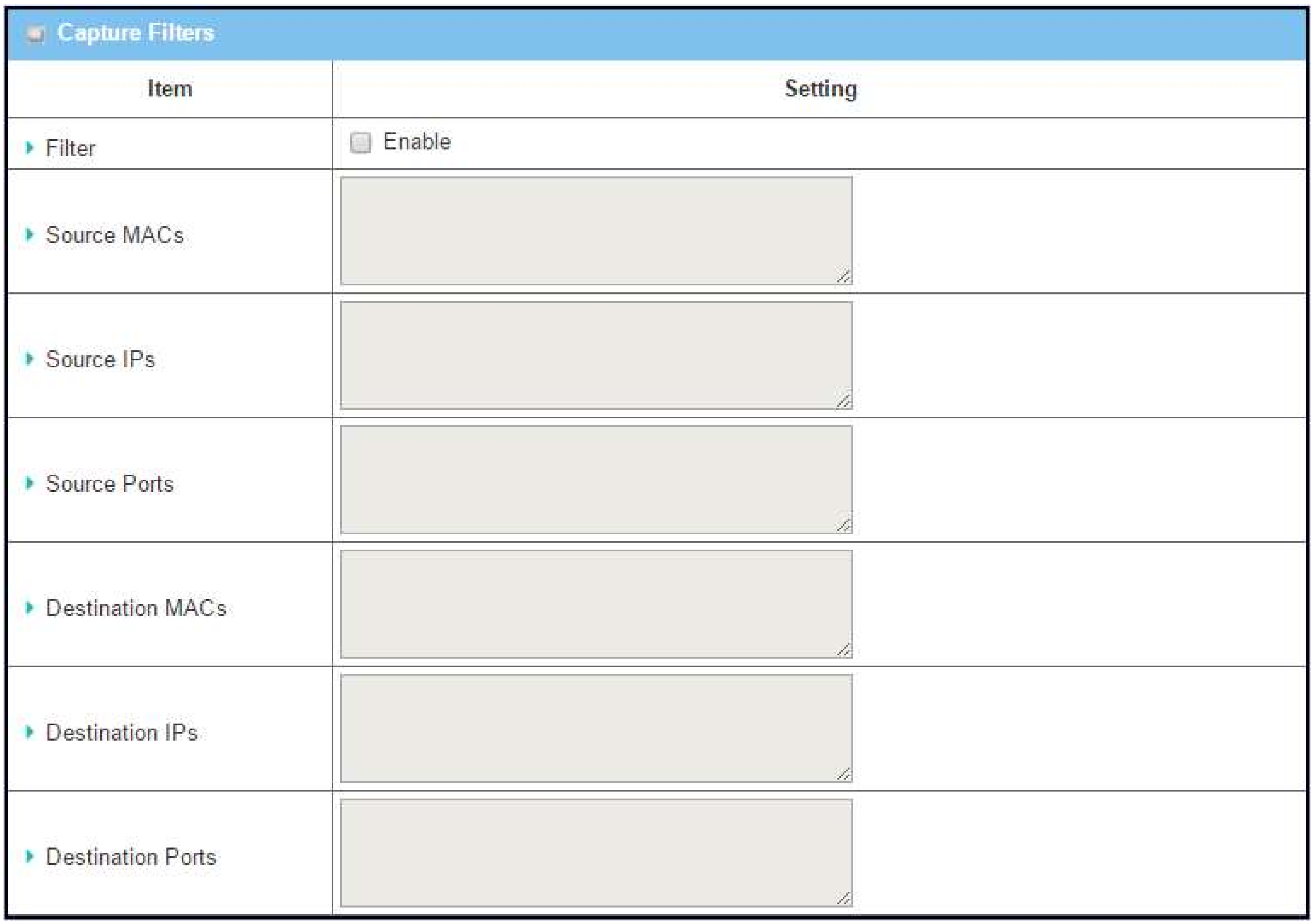
Configuration

Item	Setting
Packet Analyzer	□ Enable
File Name	
Split Files	□ Enable File Size : 200 KB ▾
Packet Interfaces	□ WAN-1 □ WAN-2 □ ASY-1 2.4G : □ VAP-1 □ VAP-2 □ VAP-3 □ VAP-4 □ VAP-5 □ VAP-6 □ VAP-7 □ VAP-8

Configuration		
Item	**Value setting**	**Description**
Packet Analyzer	The box is unchecked by default.	Check **Enable** box to activate the Packet Analyzer function. If you can not enable the checkbox, please check if the storage is available or not. Plug in the USB storage and then enable the Package Analyzer function.
File Name	1. An optional setting 2. Blank is set by default, and the default file name is **<Interface>_<Date>_<index>.**	Enter the file name to save the captured packets in log storage. If **Split Files** option is also enabled, the file name will be appended with an index code "**_<index>**"**.** The extension file name is **.pcap**.
Split Files	1. An optional setting 2. The default value of **File Size** is 200 KB. 3. NOTE that **File Size** can not	Check **enable** box to split file whenever log file reaching the specified limit. If the **Split Files** option is enabled, you can further specify the **File Size** and **Unit** for the split files.

	be less than 4 KB	
Packet Interfaces	An optional setting	Define the interface(s) that **Packet Analyzer** should work on. At least, one interface is required, but multiple selections are also accepted. The supported interfaces can be: ● **WAN**: When the WAN is enabled at **Physical Interface**, it can be selected here. ● **ASY**: This means the serial communication interface. It is used to capture packets appearing in the **Field Communication**. Therefore, it can only be selected when specific field communication protocol, like Modbus, is enabled. ● **VAP**: This means the virtual AP. When WiFi and VAP are enabled, it can be selected here.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.

Once you enabled the Packet Analyzer function on specific Interface(s), you can further specify some filter rules to capture the packets which matched the rules.



Capture Filters

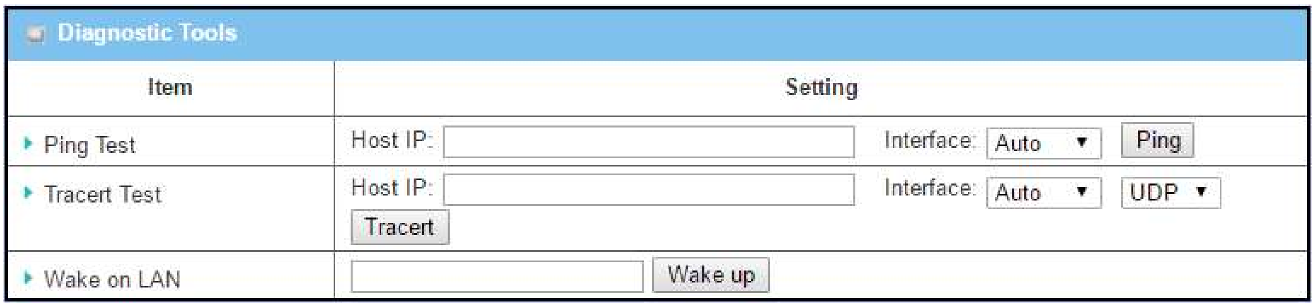
Item	Setting
Filter	□ Enable
Source MACs	
Source IPs	
Source Ports	
Destination MACs	
Destination IPs	
Destination Ports	

Capture Fitters		
Item	Value setting	Description
Filter	Optional setting	Check **Enable** box to activate the Capture Filter function.
Source MACs	Optional setting	Define the filter rule with **Source MACs**, which means the source MAC address of packets. Packets which match the rule will be captured. Up to 10 MACs are supported, but they must be separated with “**;**”, e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when match any one MAC in the rule.
Source IPs	Optional setting	Define the filter rule with **Source IPs**, which means the source IP address of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with “**;**”, e.g. 192.168.1.1; 192.168.1.2 The packets will be captured when match any one IP in the rule.
Source Ports	Optional setting	Define the filter rule with **Source Ports**, which means the source port of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with “**;**”, e.g. 80; 53 The packets will be captured when match any port in the rule.
Destination MACs	Optional setting	Define the filter rule with **Destination MACs**, which means the destination MAC address of packets. Packets which match the rule will be captured. Up to 10 MACs are supported, but they must be separated with “**;**”, e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when match any one MAC in the rule.
Destination IPs	Optional setting	Define the filter rule with **Destination IPs**, which means the destination IP address of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with “**;**”, e.g. 192.168.1.1; 192.168.1.2 The packets will be captured when match any one IP in the rule.
Destination Ports	Optional setting	Define the filter rule with **Destination Ports**, which means the destination port of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with “**;**”, e.g. 80; 53 The packets will be captured when match any port in the rule.

b.7.3 Diagnostic Tools

The Diagnostic Tools provide some frequently used network connectivity diagnostic tools (approaches) for the network administrator to check the device connectivity.

Go to Administration > Diagnostic > Diagnostic Tools tab.

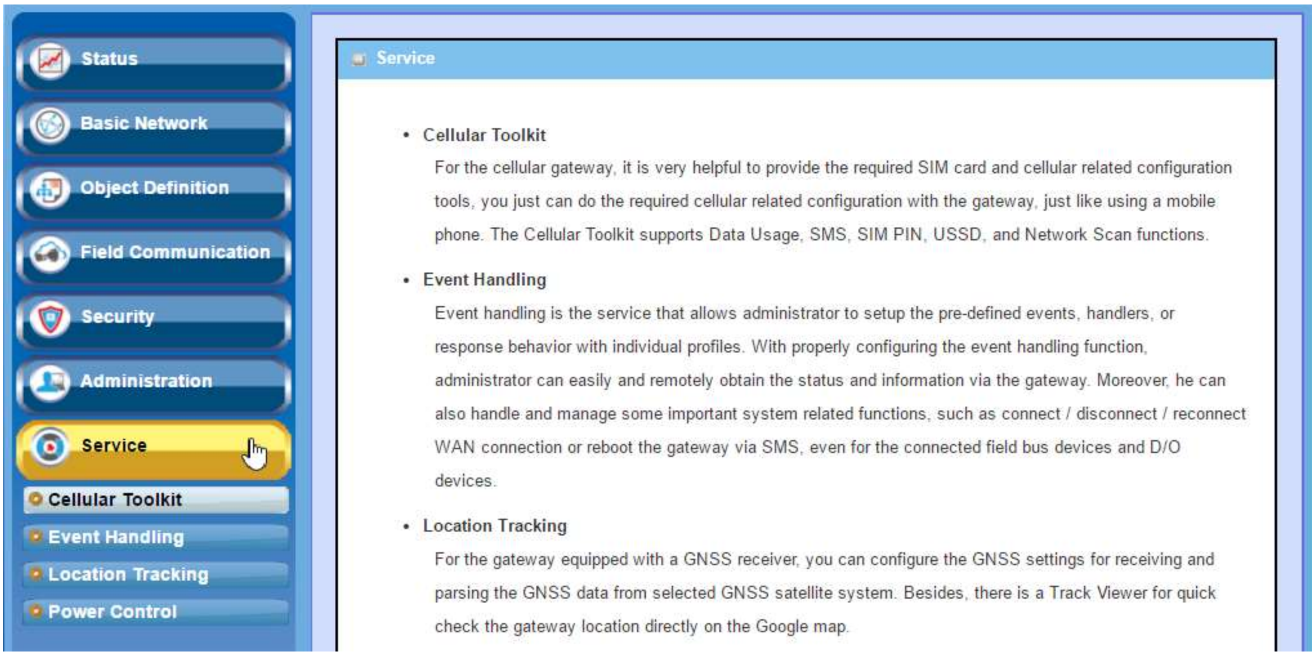


Diagnostic Tools

Item	Setting
Ping Test	Host IP: [ ] Interface: Auto ▼ Ping
Tracert Test	Host IP: [ ] Interface: Auto ▼ UDP ▼ Tracert
Wake on LAN	[ ] Wake up

Diagnostic Tools		
Item	**Value setting**	**Description**
Ping Test	Optional Setting	This allows you to specify an IP / FQDN and the test interface, so system will try to ping the specified device to test whether it is alive after clicking on the **Ping** button. A test result window will appear beneath it.
Tracert Test	Optional setting	Trace route (tracert) command is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Trace route proceeds until all (three) sent packets are lost for more than twice, then the connection is lost and the route cannot be evaluated. First, you need to specify an IP / FQDN, the test interface and the protocol (UDP or ICMP), and by default, it is **UDP**. Then, system will try to trace the specified host to test whether it is alive after clicking on the **Tracert** button. A test result window will appear beneath it.
Wake on LAN	Optional setting	Wake on LAN (WOL) is an Ethernet networking standard that allows a computer to be turned on or awakened by a network message. You can specify the MAC address of the computer, in your LAN network, to be remotely turned on by clicking on the **Wake up** command button.
Save	N/A	Click the **Save** button to save the configuration.

Chapter d Service



Service

- Cellular Toolkit

  For the cellular gateway, it is very helpful to provide the required SIM card and cellular related configuration tools, you just can do the required cellular related configuration with the gateway, just like using a mobile phone. The Cellular Toolkit supports Data Usage, SMS, SIM PIN, USSD, and Network Scan functions.

- Event Handling

  Event handling is the service that allows administrator to setup the pre-defined events, handlers, or response behavior with individual profiles. With properly configuring the event handling function, administrator can easily and remotely obtain the status and information via the gateway. Moreover, he can also handle and manage some important system related functions, such as connect / disconnect / reconnect WAN connection or reboot the gateway via SMS, even for the connected field bus devices and D/O devices.

- Location Tracking

  For the gateway equipped with a GNSS receiver, you can configure the GNSS settings for receiving and parsing the GNSS data from selected GNSS satellite system. Besides, there is a Track Viewer for quick check the gateway location directly on the Google map.

d.1 Cellular Toolkit

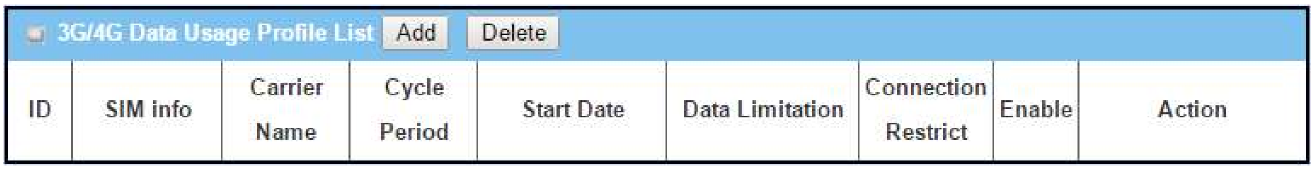
In Cellular Toolkit Service section, the device supports Data Usage, SMS, SIM PIN, USSD, and Network Scan. You can setup these aspects of cellular applications by using embedded 3G/LTE module in the device.

d.1.1 Data Usage

Most mobile phone users have no unlimited data plan so the telecom charges may exceed the bill upper limit. Data Usage feature can monitor the network traffic and show a simple chart so that users can easily control the condition.

Go to **System** > **System Related** > **Data Usage** tab.

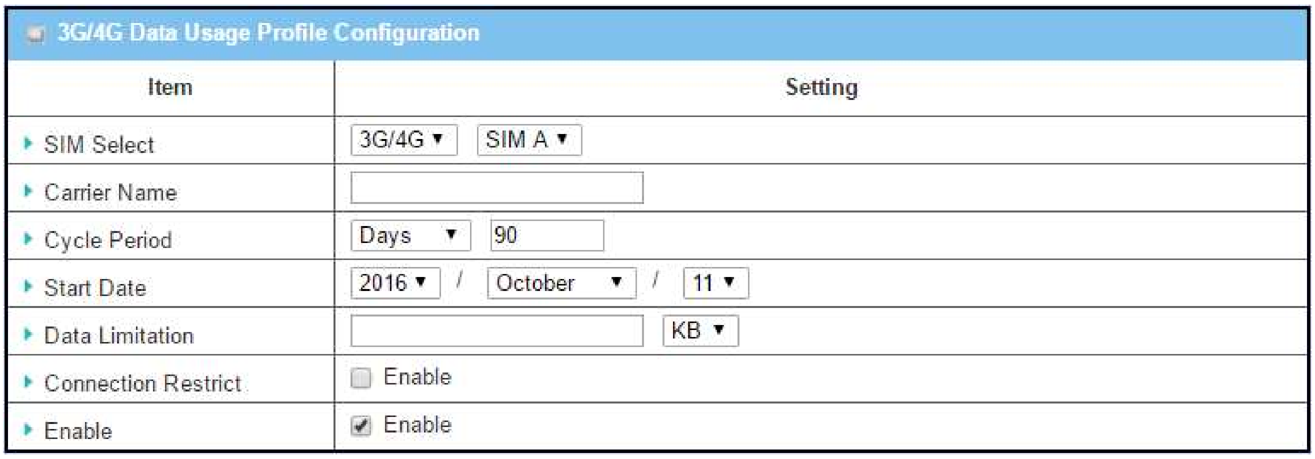
Create / Edit 3G/4G Data Usage Profile



3G/4G Data Usage Profile List Add Delete

ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable	Action

When **Add** button is applied, 3G/4G Data Usage Profile Configuration screen will appear. You can create up to four data usage profiles, one profile for each SIM card used in the Gateway.



3G/4G Data Usage Profile Configuration

Item	Setting
SIM Select	3G/4G ▾ SIM A ▾
Carrier Name	
Cycle Period	Days ▾ 90
Start Date	2016 ▾ / October ▾ / 11 ▾
Data Limitation	KB ▾
Connection Restrict	□ Enable
Enable	☑ Enable

3G/4G Data Usage Profile Configuration		
Item Setting	**Value setting**	**Description**
SIM Select	3G/4G-1 and SIM A by default.	Choose a cellular interface (**3G/4G-**1 or **3G/4G-2**), and a SIM card bound to the selected cellular interface to configure its data usage profile.
Carrier Name	It is an optional item.	Fill in the Carrier Name for the selected SIM card for identification.
Cycle Period	Days by default	The first box has three types for cycle period. They are **Days**, **Weekly** and **Monthly**. **Days**: For per Days cycle periods, you have to further specify the number of days in the second box. Its range is from 1 to 90 days. **Weekly**, **Monthly**: The cycle period is one week or one month.
Start Date	N/A	Specify the date to start measure network traffic. Please don't select the day before now, otherwise, the traffic statistics will be incorrect.
Data Limitation	N/A	Specify the allowable data limitation for the defined cycle period.
Connection Restrict	Un-Checked by default.	Check the **Enable** box to activate the connection restriction function. During the specified cycle period, if the actual data usage exceeds the allowable data limitation, the cellular connection will be forced to disconnect.
Enable	Un-Checked by default.	Check the **Enable** box to activate the data usage profile.

d.1.3 SMS

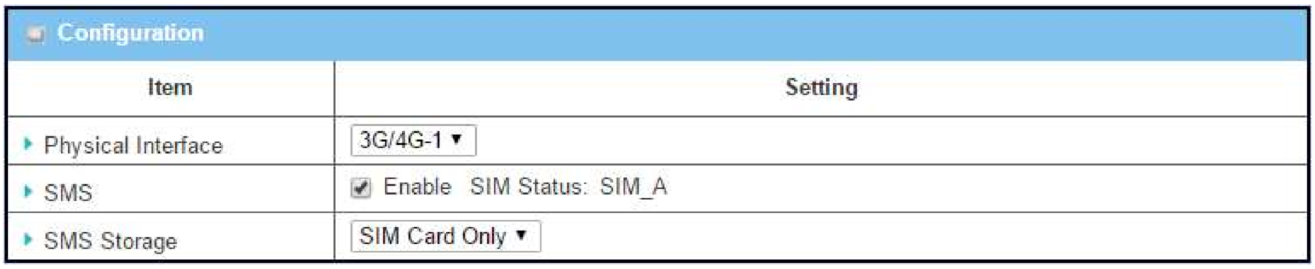
Short Message Service (SMS) is a text messaging service component of phone, Web, or mobile communication systems. It uses standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages. [12]

SMS as used on modern handsets originated from radio telegraphy in radio memo pagers using standardized phone protocols. These were defined in 1985 as part of the Global System for Mobile Communications (GSM) series of standards as a means of sending messages of up to 160 characters to and from GSM mobile handsets. Though most SMS messages are mobile-to-mobile text messages, support for the service has expanded to include other mobile technologies, such as ANSI CDMA networks and Digital AMPS, as well as satellite and landline networks.[11]

The SMS function allows user to send SMS, read and delete SMS from SIM Card.

Go to **Service** > **Cellular Toolkit** > **SMS** tab

Setup SMS Configuration



Configuration

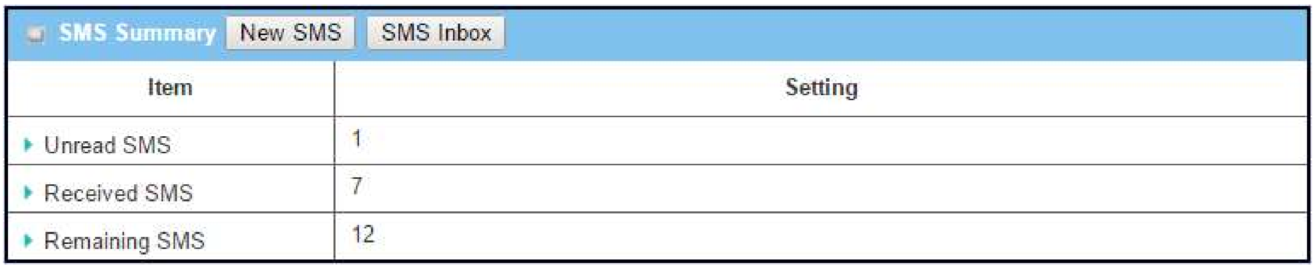
Item	Setting
Physical Interface	3G/4G-1 ▾
SMS	☑ Enable SIM Status: SIM_A
SMS Storage	SIM Card Only ▾

Configuration Item	Value setting	Description
Physical Interface	The box is 3G/4G-1 by default	Choose a cellular interface (**3G/4G-1** or **3G/4G-2**) for the following SMS function configuration.
SMS	The box is checked by default	This is the SMS switch. If the box checked that the SMS function enable, if the box unchecked that the SMS function disable.
SIM Status	N/A	Depend on currently SIM status. The possible value will be **SIM_A** or **SIM_B**.
SMS Storage	The box is **SIM Card Only** by default	This is the SMS storage location. Currently the option only **SIM Card Only.**
Save	N/A	Click **Save** to save the settings

[11] http://en.wikipedia.org/wiki/Short_Message_Service.

SMS Summary

Show **Unread SMS**, **Received SMS**, **Remaining SMS**, and edit SMS context to send, read SMS from SIM card.

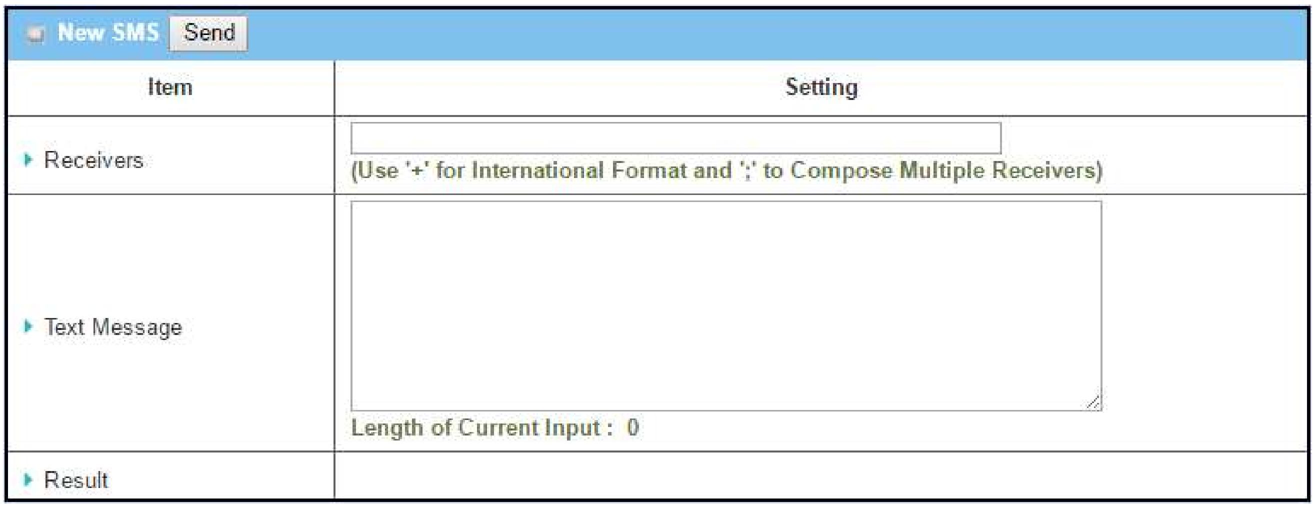


Item	Setting
Unread SMS	1
Received SMS	7
Remaining SMS	12

SMS Summary		
Item	**Value setting**	**Description**
Unread SMS	N/A	If SIM card insert to router first time, unread SMS value is zero. When received the new SMS but didn't read, this value plus one.
Received SMS	N/A	This value record the existing SMS numbers from SIM card, When received the new SMS, this value plus one.
Remaining SMS	N/A	This value is SMS capacity minus received SMS, When received the new SMS, this value minus one.
New SMS	N/A	Click **New SMS** button, a **New SMS** screen appears. User can set the SMS setting from this screen. Refer to New SMS in the next page.
SMS Inbox	N/A	Click **SMS Inbox** button, a **SMS Inbox List** screen appears. User can read or delete SMS, reply SMS or forward SMS from this screen. Refer to SMS Inbox List in the next page.

New SMS

You can set the SMS setting from this screen.



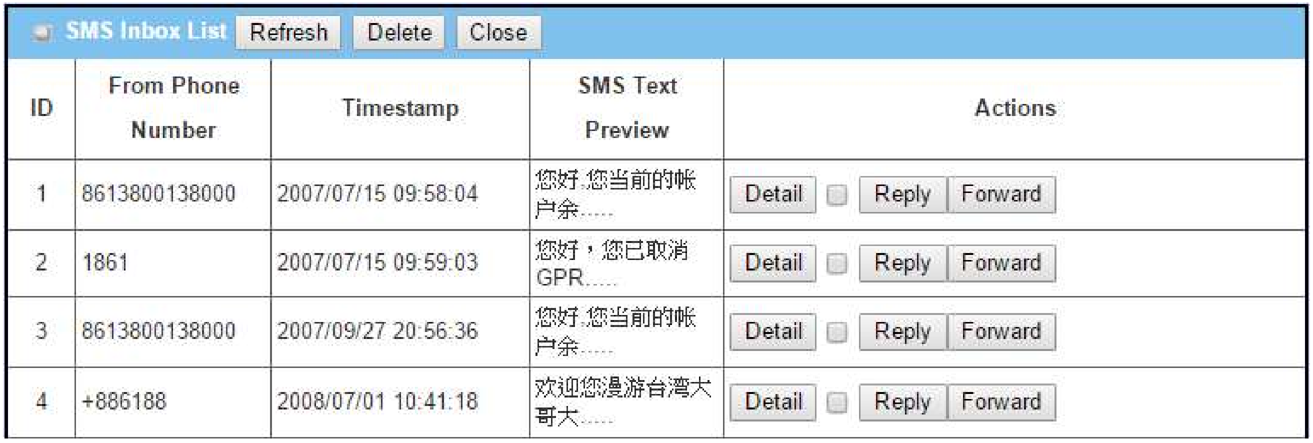
New SMS | Send

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	Write the receivers to send SMS. User need to add the semicolon and compose multiple receivers that can group send SMS.
Text Message	N/A	Write the SMS context to send SMS. The router supports up to a maximum of 1023 character for SMS context length.
Result	N/A	If send SMS OK, result will show **Send OK**, otherwise **Send Failed** will be displayed.
Send	N/A	Click **Send** button, SMS will send.

SMS Inbox List

You can read or delete SMS, reply SMS or forward SMS from this screen.



SMS Inbox List | Refresh | Delete | Close

ID	From Phone Number	Timestamp	SMS Text Preview	Actions
1	8613800138000	2007/07/15 09:58:04	您好.您当前的帐户余.....	Detail □ Reply Forward
2	1861	2007/07/15 09:59:03	您好，您已取消GPR.....	Detail □ Reply Forward
3	8613800138000	2007/09/27 20:56:36	您好.您当前的帐户余.....	Detail □ Reply Forward
4	+886188	2008/07/01 10:41:18	欢迎您漫游台湾大哥大.....	Detail □ Reply Forward

SMS Inbox List Item	Value setting	Description
ID	N/A	The number or SMS.

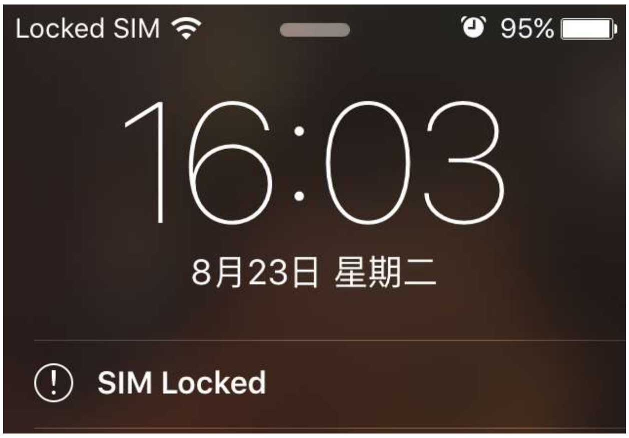
From Phone Number	N/A	What the phone number from SMS
Timestamp	N/A	What time receive SMS
SMS Text Preview	N/A	Preview the SMS text. Click the **Detail** button to read a certain message.
Action	The box is unchecked by default	Click the **Detail** button to read the SMS detail; Click the **Reply** / **Forward** button to reply/forward SMS. Besides, you can check the box(es), and then click the **Delete** button to delete the checked SMS(s).
Refresh	N/A	Refresh the SMS Inbox List.
Delete	N/A	Delete the SMS for all checked box from Action.
Close	N/A	Close the Detail SMS Message screen.

d.1.5 SIM PIN

Sometimes we will activate a password on mobile phones to prevent other people accessing our phones when phones get lost or stolen. Generally speaking, this password setting can be applied on end devices (e.g. mobile phone) or SIM card. The later one is what we are going to focus at this section.

With most cases in the world, users need to insert a SIM card (a.k.a. UICC) into end devices to get on cellular network for voice service or data surfing. The SIM card is usually released by mobile operators or service providers. Each SIM card has a unique number (so-called ICCID) for network owners or service providers to identify each subscriber. As SIM card plays an important role between service providers and subscribers, some security mechanisms are required on SIM card to prevent any unauthorized access. Imagining you are not aware that your SIM card was lost, but somehow you got an unexpected bill from subscribed Telecom the next month that included fees for hundreds of international calls. Fortunately, a simple way is available to prevent this disaster happened. Just needs to activate a PIN (Personal Identification Number) code on SIM card!

If PIN code is activated on a SIM card, you can always see the similar message (as the snapshot below) when devices are powered on. It means you have to enter the correct PIN code to unlock SIM card. Otherwise, there is no way to use cellular-related functions, such as GSM voice service, SMS text, 3G or LTE Internet surfing …etc.



Locked SIM

95%

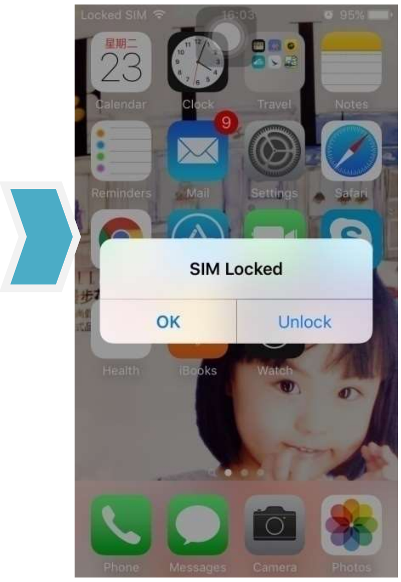
16:03

8月23日 星期二

SIM Locked

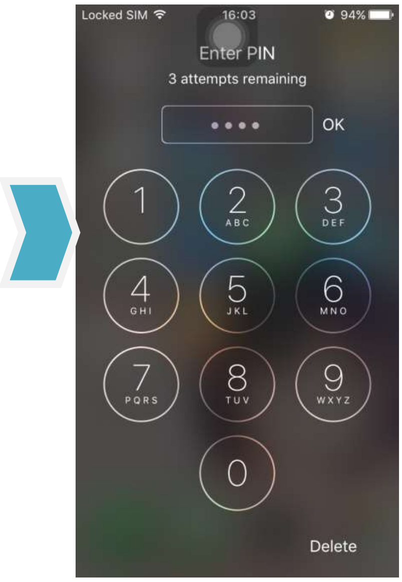
Following steps show typical procedures for unlocking a SIM card on mobile phone.

[Step 1]



SIM Locked

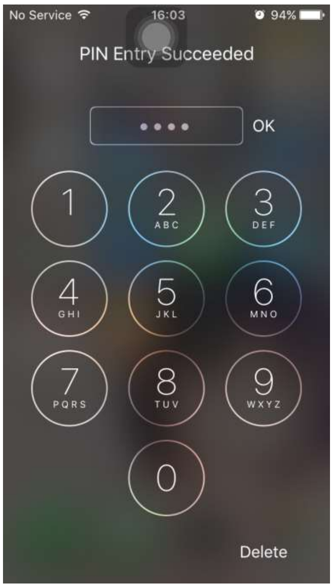
[Step 2]



Enter PIN

3 attempts remaining

[Step 3]



PIN Entry Succeeded

Step 1: Pres “Unlock” button to unlock a SIM card.

Step 2: Enter the correct PIN code, and then press “OK”. Please note an important message “**3 attempts remaining**” on top of screen. The maximum times of failure trial are 3. If you enter incorrect PIN code for three times, this SIM card will be locked and you can’t try your PIN code anymore. In this situation, you need to request a PUK (PIN unlock Key) code from your service provider to reset PIN code on SIM card.

Step 3: If the PIN code is correct, you can see a successful message on screen. Then mobile phone will start to connect to cellular tower nearby and start to provide cellular-related services.

After understanding the potential risk and purpose of SIM lock, you should know how important and easy to finish this job. Speaking of the purchased cellular gateway, similar to mobile phones, users also need to insert SIM cards into gateway’s SIM slot to get cellular-related functions. Although there is always a metal SIM cover with screws fastened to protect SIM cards from being taken away, it still strongly recommended activating PIN code on SIM card. Especially most of M2M-IoT gateways are installed at remote sites, and usually there is no dedicated guard to take care of these devices.

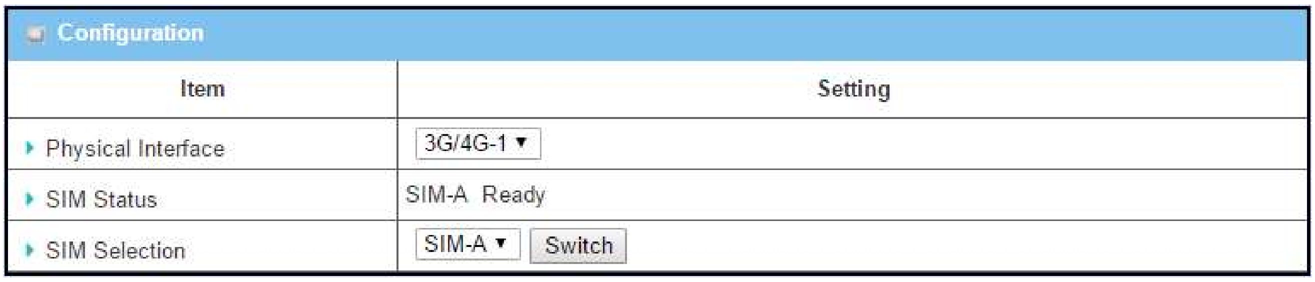
How to activate and manage PIN code on a SIM card through gateway’s web GUI? It is as easy as what you have done on a mobile phone. Let’s check it out.

SIM PIN Setting

With the SIM PIN Function window, it allows you to enable or disable SIM lock (which means protected by PIN code), or change PIN code. You can also see the information of remaining times of failure trials as we mentioned earlier. If you run out of these failure trials, you need to get a PUK code to unlock SIM card.

Go to **Applications** > **Mobile Application** > **SIM PIN** Tab

Select a SIM Card



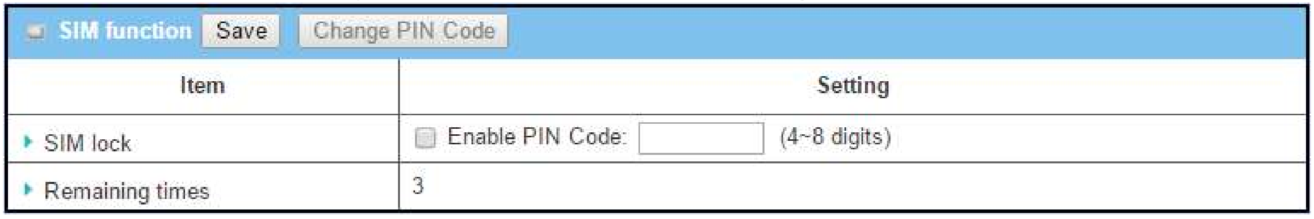
Configuration

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

Configuration Window		
Item	**Value setting**	**Description**
Physical Interface	The box is 3G/4G-1 by default	Choose a cellular interface (**3G/4G-**1 or **3G/4G-2**) to change the SIM PIN setting for the selected SIM Card. The number of physical modems depends on the gateway model you purchased.
SIM Status	N/A	Indication for the selected SIM card and the SIM card status. The status could be **Ready**, **Not Insert**, or **SIM PIN**. **Ready** -- SIM card is inserted and ready to use. It can be a SIM card without PIN protection or that SIM card is already unlocked by correct PIN code. **Not Insert** -- No SIM card is inserted in that SIM slot. **SIM PIN** -- SIM card is protected by PIN code, and it's not unlocked by a correct PIN code yet. That SIM card is still at locked status.
SIM Selection	N/A	Select the SIM card for further SIM PIN configuration. Press the **Switch** button, then the Gateway will switch SIM card to another one. After that, you can configure the SIM card.

Enable / Change PIN Code

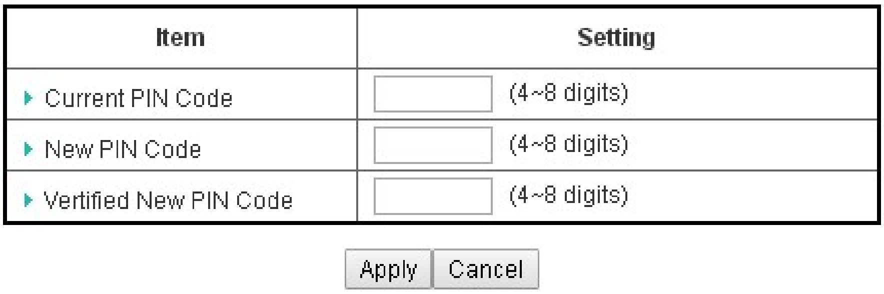
Enable or Disable PIN code (password) function, and even change PIN code function.



Item	Setting
SIM lock	□ Enable PIN Code: ▭ (4~8 digits)
Remaining times	3

SIM function Window		
Item Setting	**Value setting**	**Description**
SIM lock	Depend on SIM card	Click the **Enable** button to activate the SIM lock function. For the first time you want to enable the SIM lock function, you have to fill in the PIN code as well, and then click **Save** button to apply the setting.
Remaining times	Depend on SIM card	Represent the remaining trial times for the SIM PIN unlocking.
Save	*NA*	Click the **Save** button to apply the setting.
Change PIN Code	*NA*	Click the **Change PIN code** button to change the PIN code (password). If the **SIM Lock** function is not enabled, the **Change PIN code** button is disabled. In the case, if you still want to change the PIN code, you have to enable the SIM Lock function first, fill in the PIN code, and then click the **Save** button to enable. After that, You can click the **Change PIN code** button to change the PIN code.

When **Change PIN Code** button is clicked, the following screen will appear.



Item	Setting
Current PIN Code	▭ (4~8 digits)
New PIN Code	▭ (4~8 digits)
Vertified New PIN Code	▭ (4~8 digits)

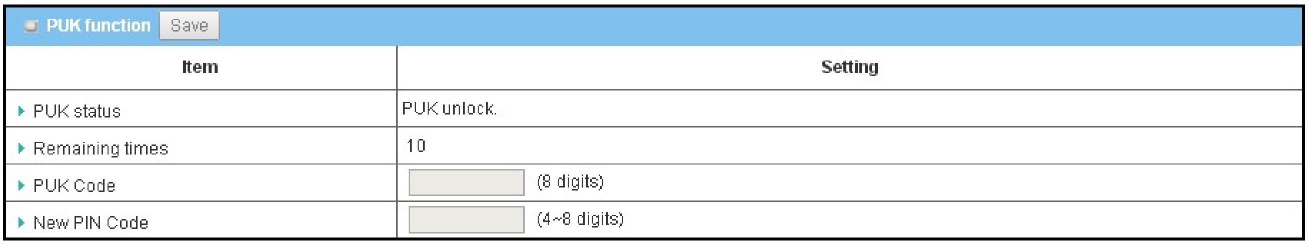
Item Setting	Value setting	Description
Current PIN Code	A Must filled setting	Fill in the current (old) PIN code of the SIM card.
New PIN Code	A Must filled setting	Fill in the new PIN Code you want to change.
Verified New PIN Code	A Must filled setting	Confirm the new PIN Code again.

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 changed the PIN code for a certain SIM card, you must also change the corresponding PIN code specified in the **Basic Network** > **WAN & Uplink** > **Internet Setup** > **Connection with SIM Card** page. Otherwise, it may result in wrong SIM PIN trials with invalid (old) PIN code.

Unlock with a PUK Code

The PUK Function window is only available for configuration if that SIM card is locked by PUK code. It means that SIM card is locked and needs additional PUK code to unlock. Usually it happens after too many trials of incorrect PIN code, and the remaining times in SIM Function table turns to 0. In this situation, you need to contact your service provider and request a PUK code for your SIM card, and try to unlock the locked SIM card with the provided PUK code. After unlocking a SIM card by PUK code successfully, the SIM lock function will be activated automatically.



Item	Setting
PUK status	PUK unlock.
Remaining times	10
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 trials of failure PIN code. In this case, the PUK Status will turns to **PUK Lock**. In a normal situation, it will display **PUK Unlock**.
Remaining times	Depend on SIM card	Represent the remaining trial times for the PUK unlocking. Note : **DO NOT make the remaining times down to zero, it will damage the SIM card FOREVER !** Call for your ISP's help to get a correct PUK and unlock the SIM if you don't have the PUK code.
PUK Code	A Must filled setting	Fill in the PUK code (8 digits) that can unlock the SIM card in PUK unlock status.
New PIN Code	A Must filled setting	Fill in the New PIN Code (4~8 digits) for the SIM card. You have to determine your new PIN code to replace the old, forgotten one. Keep the PIN code (password) in mind with care.
Save	N/A	Click the **Save** button to apply the setting.

Note: If you changed the PUK code and PIN code for a certain SIM card, you must also change the corresponding PIN code specified in the **Basic Network** > **WAN & Uplink** > **Internet Setup** > **Connection with SIM Card** page. Otherwise, it may result in wrong SIM PIN trials with invalid (old) PIN code.

- **Scenario of activating PIN code on SIM card**

An operation owner would like to enable SIM lock function with a default PIN code "0000" on a new SIM card. This SIM card was inserted in SIM-A slot for 3G/4G-1 WAN connection.

Configuration:

Configuration Path	[Cellular Toolkit]-[SIM PIN]-[Configuration]
Physical Interface	*3G/4G-1*
SIM Status	*Ready*
SIM Selection	*SIM-A*

SIM Function

Configuration Path	[Cellular Toolkit]-[SIM PIN]-[SIM Function]
SIM Lock	*Enable, PIN Code: 0000*
Remaining Times	*[Display Remaining Times]*

- **Scenario of changing PIN code on SIM card**

An operation owner would like to change PIN code from default "0000" to "1234" on a SIM card. This SIM card was inserted in SIM-A slot for 3G/4G-1 WAN connection.

Configuration:

Configuration Path	[Cellular Toolkit]-[SIM PIN]-[Configuration]
Physical Interface	*3G/4G-1*
SIM Status	*SIM PIN*
SIM Selection	*SIM-A*

SIM Function

Configuration Path	[Cellular Toolkit]-[SIM PIN]-[SIM Function]-[Change PIN Code]
Current PIN Code	*0000*
New PIN Code	*1234*
Verified New PIN Code	*1234*

- **Scenario of unlocking SIM card by PUK code**

An operation owner entered incorrect PIN code at configuration page for 3G/4G-1 WAN, and then it caused that SIM card was locked by PUK code. He called service number, and he was informed the PUK code for his SIM card is “12345678”. Then he tried to unlock that SIM card with that PUK code, and set a new PIN code “5678”.

Configuration:

Configuration Path	[Cellular Toolkit]-[SIM PIN]-[Configuration]
Physical Interface	***3G/4G-1***
SIM Status	***SIM PIN***
SIM Selection	***SIM-A***

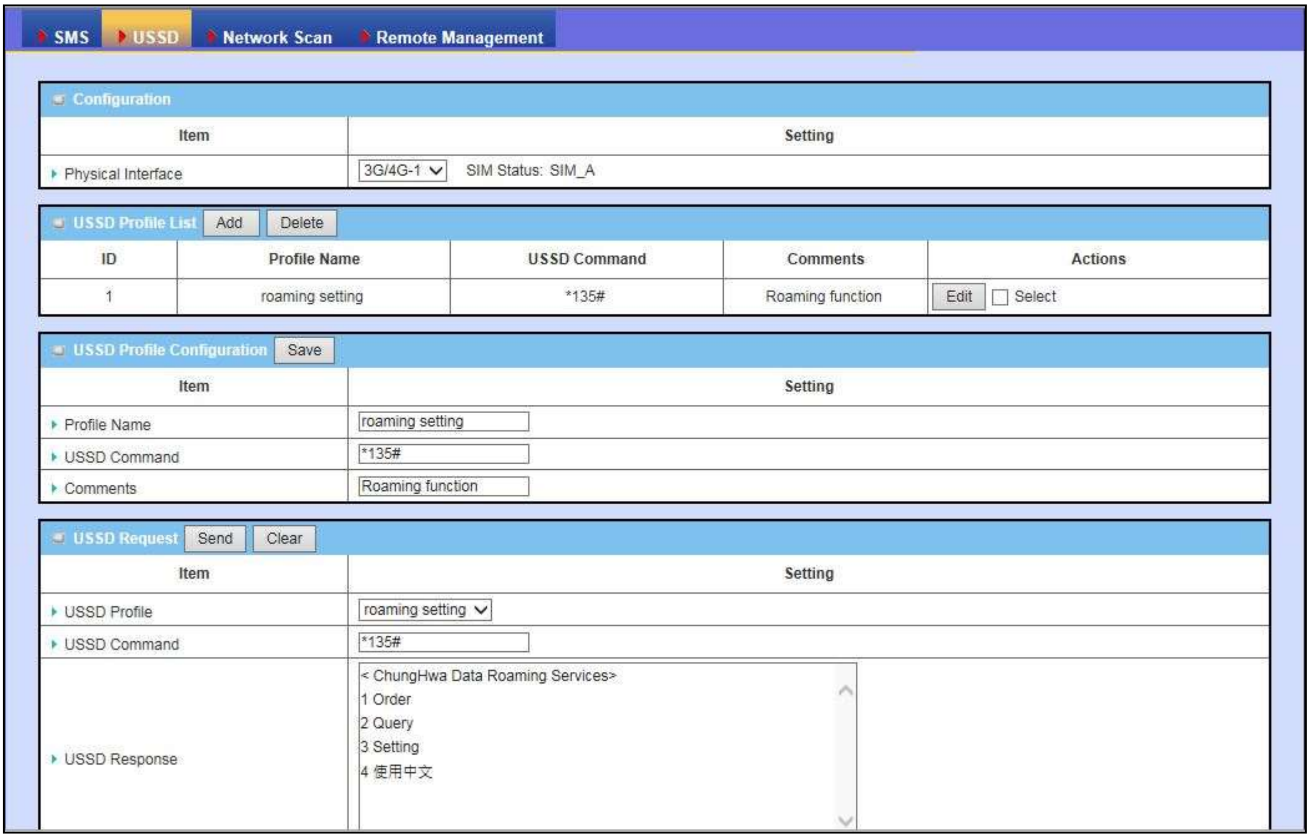
PUK Function

Configuration Path	[Service]-[SIM PIN]-[PUK Function]
PUK Status	***PUK Lock***
Remaining Times	***[Display Remaining Times]***
PUK Code	***12345678***
New PIN Code	***5678***

d.1.7 USSD

Unstructured Supplementary Service Data (USSD) is a protocol used by GSM cellular telephones to communicate with the service provider's computers. USSD can be used for WAP browsing, prepaid callback service, mobile-money services, location-based content services, menu-based information services, and as part of configuring the phone on the network. [13]

An USSD message is up to 182 alphanumeric characters in length. Unlike Short Message Service (SMS) messages, USSD messages create a real-time connection during an USSD session. The connection remains open, allowing a two-way exchange of a sequence of data. This makes USSD more responsive than services that use SMS.[13]



Configuration

Item	Setting
Physical Interface	3G/4G-1 SIM Status: SIM_A

USSD Profile List

ID	Profile Name	USSD Command	Comments	Actions
1	roaming setting	*135#	Roaming function	Edit □ Select

USSD Profile Configuration

Item	Setting
Profile Name	roaming setting
USSD Command	*135#
Comments	Roaming function

USSD Request

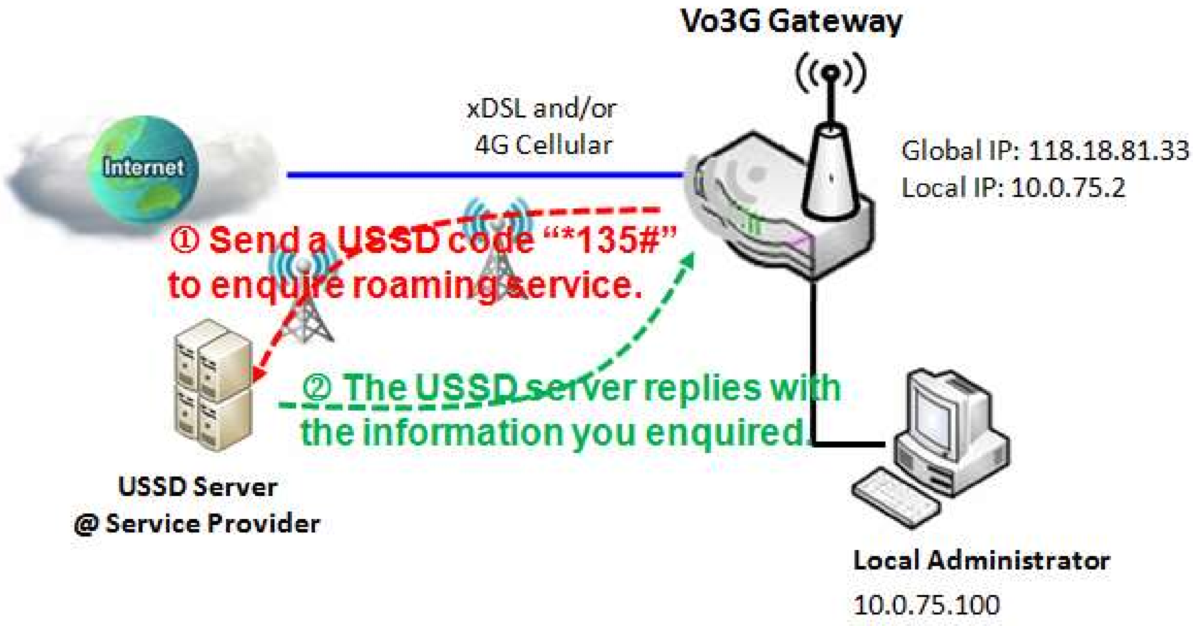
Item	Setting
USSD Profile	roaming setting
USSD Command	*135#
USSD Response	< ChungHwa Data Roaming Services> 1 Order 2 Query 3 Setting 4 使用中文

In "USSD" page, there are four windows for the USSD function. The "Configuration" window can let you specify which 3G/4G module (physical interface) is used for the USSD function, and system will show which SIM card in the module is the current used one. The second window is the "USSD Profile List" and it shows all your defined USSD profiles that store pre-commands for activating an USSD session. An "Add" button in the window can let you add one new USSD profile and define the command for the profile in

[13] http://en.wikipedia.org/wiki/Unstructured_Supplementary_Service_Data

the third window, the "USSD Profile Configuration". When you want to start the activation of an USSD connection session to the USSD server, select the USSD profile or type in the correct pre-command, and then click on the "Send" button for the session. The responses from the USSD server will be displayed beneath the "USSD Command" line. When commands typed in the "USSD Command" field are sent, received responses will be displayed in the "USSD Response" blank space. User can communicate with the USSD server by sending USSD commands and getting USSD responses via the gateway.

An USSD Session Scenario



Scenario Application Timing

When the administrator wants to uses the Voice Gateway to ask for some ISP's services through an USSD session, the scenario is adequate for the application. Following example is the roaming subscription for Hinet service in Taiwan.

Scenario Description

An USSD session can be established from the voice Vo3G Gateway to ask for services that are provided by ISP.

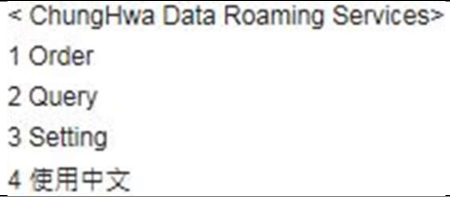
Parameter Setup Example

Following tables list the parameter configuration as an example for "USSD" function, as shown in above diagram.

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

Configuration Path	[USSD]-[Configuration]
Physical Interface	***3G/4G-1*** SIM Status: SIM_A

Configuration Path	[USSD]-[USSD Profile Configuration]
Profile Name	***roaming setting***
USSD Command	****135#***
Comments	***Roaming function***

Configuration Path	[USSD]-[USSD Request]
Profile Name	***roaming setting***
USSD Command	****135#***
USSD Response	 < ChungHwa Data Roaming Services> 1 Order 2 Query 3 Setting 4 使用中文

Scenario Operation Procedure

In above diagram, the "Vo3G Gateway" is the initiator of an USSD session requesting for data roaming services in ChungHwa mobile operator.

First, administrator selects one 3G/4G module as the physical interface of the USSD session. And then, he defines an USSD profile named as "roaming setting" with command "*135#" for further use.

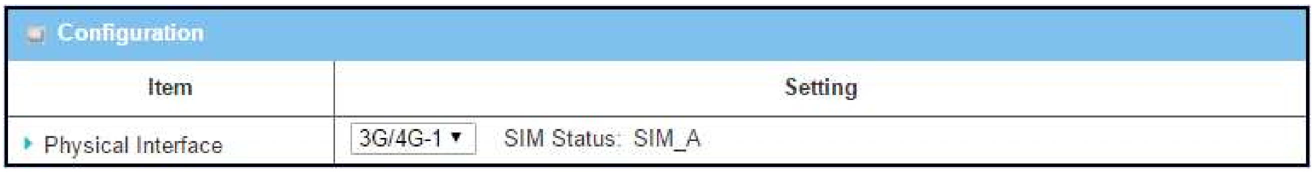
In the "USSD Request" window, from the USSD Profile dropdown box select the "roaming setting" profile and the "USSD Command" field shows "*135#". Click on the "Send" button to send out the USSD request via the gateway, and the received response will appear at "USSD Response" line. As you type in more commands in the "USSD Command" line, you will get more responses from the USSD server. It is an interactive communication session for the administrator to request for available services from ISP via USSD sessions.

USSD Setting

The USSD function allow user to send USSD to ISP, then ISP will provide some service for user.

Go to **Service** > **Cellular Toolkit** > **USSD** tab.

USSD Configuration

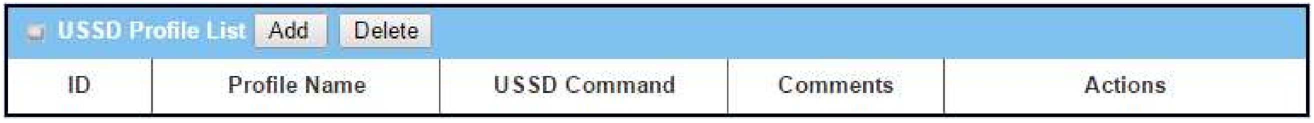

Configuration

Item	Setting
Physical Interface	3G/4G-1 ▾ SIM Status: SIM_A

Configuration Item	Value setting	Description
Physical Interface	The box is 3G/4G-1 by default.	Choose a cellular interface (**3G/4G-**1 or **3G/4G-2**) to configure the USSD setting for the connoted cellular service (identified with **SIM_A** or **SIM_B**).
SIM Status	N/A	Show the connoted cellular service (identified with **SIM_A** or **SIM_B**).

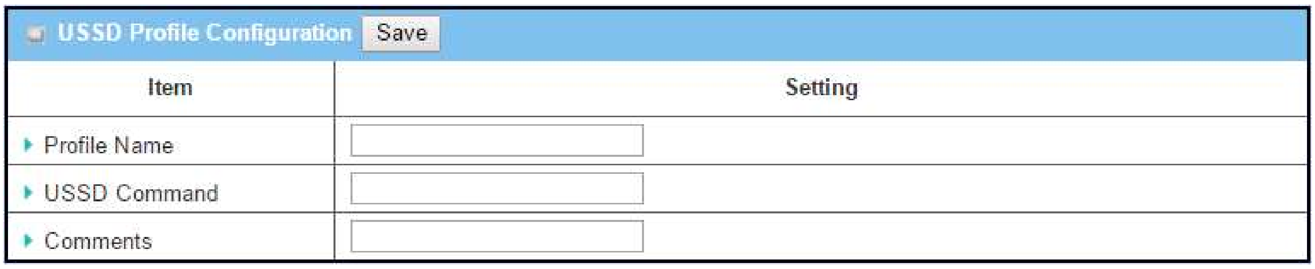
Create / Edit USSD Profile

The cellular gateway allows you to custom your USSD profile. It supports up to a maximum of 35 USSD profiles.


USSD Profile List Add Delete

ID	Profile Name	USSD Command	Comments	Actions

When Add button is applied, USSD Profile List Configuration screen will appear.

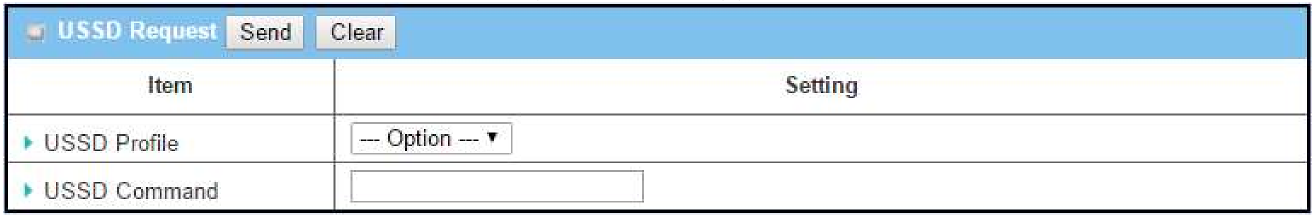

USSD Profile Configuration Save

Item	Setting
Profile Name	
USSD Command	
Comments	

USSD Profile List		
Item	**Value setting**	**Description**
Profile Name	N/A	Enter a name for the USSD profile.
USSD Command	N/A	Enter the USSD command defined for the profile. Normally, it is a command string composed with numeric keypad “0~9”, “*”, and “#”. The USSD commands are highly related to the cellular service, please check with your service provider for the details.
Comments	N/A	Enter a brief comment for the profile.

Send USSD Request

When send the USSD command, the USSD Response screen will appear.
When click the Clear button, the USSD Response will disappear.



Item	Setting
USSD Profile	--- Option --- ▾
USSD Command	

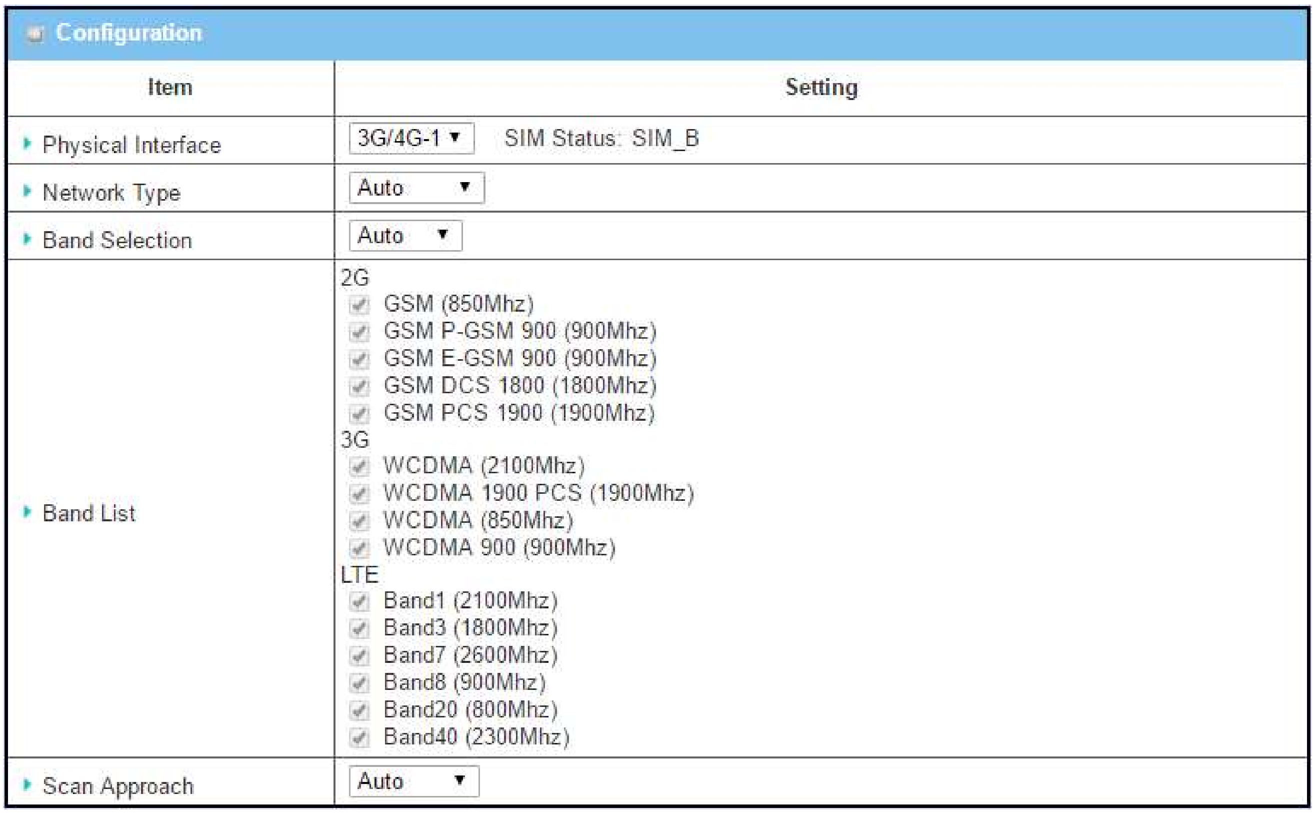
USSD Request		
Item	**Value setting**	**Description**
USSD Profile	N/A	Select a USSD profile name from the dropdown list.
USSD Command	N/A	The USSD Command string of the selected profile will be shown here.
USSD Response	N/A	Click the **Send** button to send the USSD command, and the **USSD Response** screen will appear. You will see the response message of the corresponding service, receive the service SMS.

d.1.9 Network Scan

"Network Scan" function can let administrator specify the device how to connect to the mobile system for data communication in each 3G/4G interface. For example, administrator can specify which generation of mobile system is used for connection, 2G, 3G or LTE. Moreover, he can define their connection sequence for the gateway device to connect to the mobile system automatically. Administrator also can scan the mobile systems in the air manually, select the target operator system and apply it. The manual scanning approach is used for problem diagnosis; however, the gateway system will scan the mobile system automatically during normal operation.

Go to **Service** > **Cellular Toolkit** > **Network Scan** tab.

Network Scan Configuration



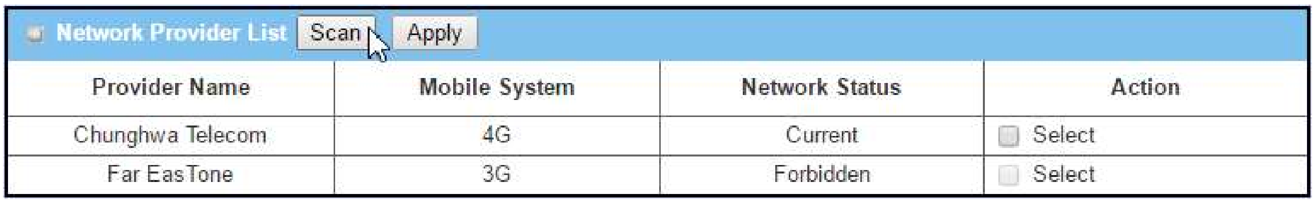
Configuration

Item	Setting
Physical Interface	3G/4G-1 ▾ SIM Status: SIM_B
Network Type	Auto ▾
Band Selection	Auto ▾
Band List	2G ☑ GSM (850Mhz) ☑ GSM P-GSM 900 (900Mhz) ☑ GSM E-GSM 900 (900Mhz) ☑ GSM DCS 1800 (1800Mhz) ☑ GSM PCS 1900 (1900Mhz) 3G ☑ WCDMA (2100Mhz) ☑ WCDMA 1900 PCS (1900Mhz) ☑ WCDMA (850Mhz) ☑ WCDMA 900 (900Mhz) LTE ☑ Band1 (2100Mhz) ☑ Band3 (1800Mhz) ☑ Band7 (2600Mhz) ☑ Band8 (900Mhz) ☑ Band20 (800Mhz) ☑ Band40 (2300Mhz)
Scan Approach	Auto ▾

In "Network Scan" page, there are two windows for the Network Scan function. The "Configuration" window can let you select which 3G/4G module (physical interface) is used to perform Network Scan, and system will show the current used SIM card in the module. You can configure each 3G/4G WAN interface by executing the network scanning one after another. You can also specify the connection sequence of the targeted generation of mobile system, 2G/3G/LTE. The second window is the "Network

Provider List" window and it appears when the **Manually** Scan Approach is selected in the Configuration window. By clicking on the "Scan" button and wait for 1 to 3 minutes, the found mobile operator system will be displayed for you to choose. Click again on the "Apply" button to drive system to connect to that mobile operator system for the dedicated 3G/4G interface.

Configuration Item	Value setting	Description
Physical Interface	The box is 3G/4G-1 by default	Choose a cellular interface (**3G/4G-**1 or **3G/4G-2**) for the network scan function.
SIM Status	N/A	Show the connoted cellular service (identified with **SIM_A** or **SIM_B**).
Network Type	Auto is selected by default.	When **Auto** selected, the network will be register automatically. If the **prefer** option selected, network will be register for your option first. If the **only** option selected, network will be register for your option only.
Band Selection	Auto is selected by default.	When **Auto** selected, **Band List** all box checked, and user can't select any option. If the **Manual** option is selected, you can change the **Band List** setting.
Band List	All box is checked by default.	The **Band List's** options depend on the embedded cellular module, and user need to select option at least one for all network type.
Scan Approach	Auto is selected by default.	When **Auto** selected, cellular module register automatically. If the **Manually** option is selected, a **Network Provider List** screen appears. Press **Scan** button to scan for the nearest base stations. Select (check the box) the preferred base stations then click **Apply** button to apply settings.
Save	N/A	Click **Save** to save the settings



Provider Name	Mobile System	Network Status	Action
Chunghwa Telecom	4G	Current	□ Select
Far EasTone	3G	Forbidden	□ Select

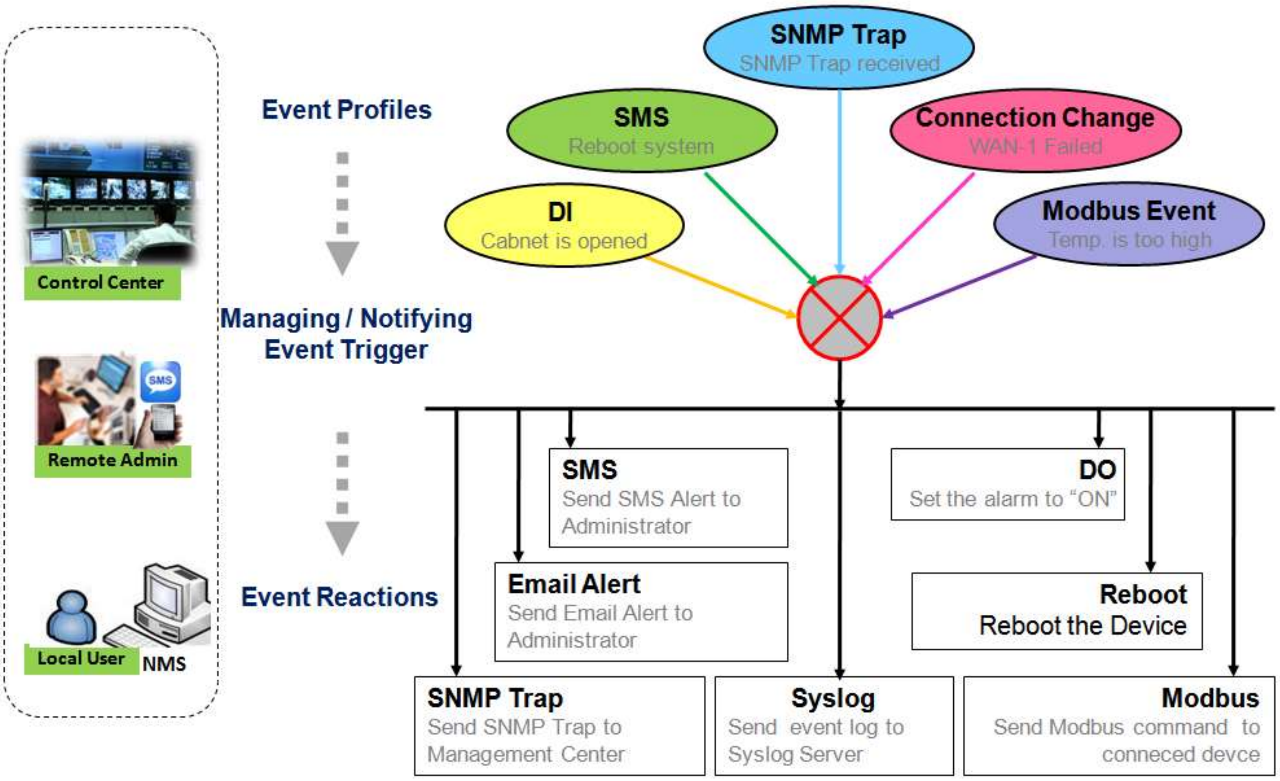
d.3 Event Handling

Event handling is the application that allows administrator to setup the pre-defined events, handlers, or response behavior with individual profiles. With properly configuring the event management function, administrator can easily and remotely obtain the status and information via the purchased gateway. Moreover, he can also handle and manage some important system related functions, even to the field bus devices and D/O devices which are already well connected to.

The supported events are categorized into two groups: the **managing events** and **notifying events**.

The **managing events** are the events that are used to manage the gateway or change the setting / status of the specific functionality of the gateway. On receiving the managing event, the gateway will take action to change the functionality, collect the required status for administration, and also change the status of a certain connected field bus device simultaneously.

The **notifying events** are the events that some related objects have been triggered and take corresponding actions on the occurrence of the events. It could be an event generated from the connected sensor, or a certain connected field bus device for alerting the administrator something happened with SMS message, Email, and SNMP Trap, etc..



For ease of configuration, administrator can create and edit the common pre-defined managing /

notifying event profiles for taking instant reaction on a certain event or managing the devices for some advanced useful purposes. For example, sending/receiving remote managing SMS for the gateway's routine maintaining, the field bus device status monitoring, digital sensors detection controlling, and so on. All of such management and notification function can be realized effectively via the Event Handling feature.

The following is the summary lists for the provided profiles, and events:

- Profiles (Rules):
    - SMS Configuration and Accounts
    - Email Accounts
    - Digital Input (DI) profiles
    - Digital Output (DO) profiles
    - Modbus Managing Event profiles
    - Modbus Notifying Event profiles

- Managing Events:
    - Trigger Type: SMS, SNMP Trap, and Digital Input (DI).
    - Actions: Get the Network Status; or Configure the LAN/VLAN behavior, WIFI behavior, NAT behavior, Firewall behavior, VPN behavior, System Management, Administration, Digital Output behavior, and connected Modbus devices.

- Notifying Events:
    - Trigger Type: Digital Input, Power Change, Connection Change (WAN, LAN & VLAN, WiFi, DDNS), Administration, Modbus, and Data Usage.
    - Actions: Notify the administrator with SMS, Syslog, SNMP Trap or Email Alert; Change the status of connected Digital Output or Modbus devices.

To use the event handling function, First of all, you have to enable the event management setting and configure the event details with the provided profile settings. You can create or edit pre-defined profiles for individual managing / notifying events. The profile settings are separated into several items, they are the SMS Account Definition, Email Service Definition, Digital Input (DI) Profile Configuration, Digital Output (DO) Profile Configuration, and Modbus Definition. The supported configuration items may be different for the purchased product, please check the product specification.

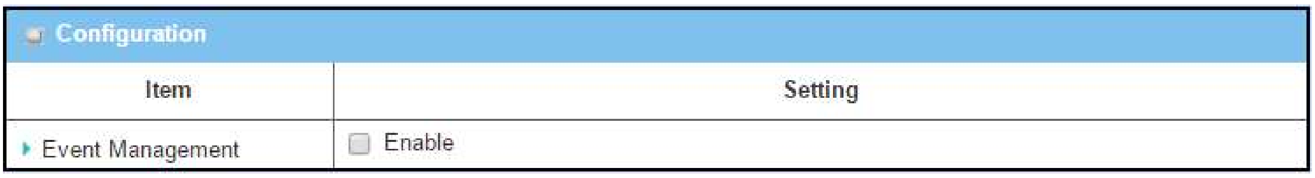
Then, you have to configure each managing / notifying event with identifying the event's trigger condition, and the corresponding actions (reaction for the event) for the event. For each event, more than one actions can be activated simultaneously.

d.3.1 Configuration

Event handling is the service that allows administrator to setup the pre-defined events, handlers, or response behavior with individual profiles. The supported configuration items may be different for the purchased product, please check the product specification.

Go to **Service** > **Event Handling** > **Configuration** Tab.

Enable Event Management



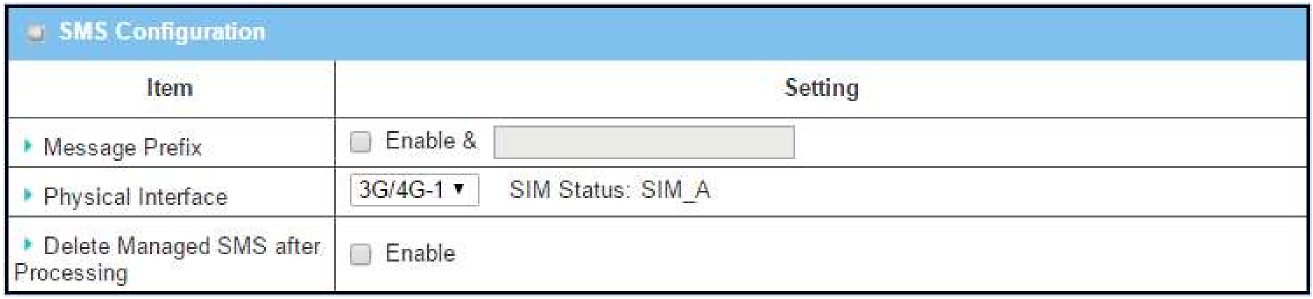
Configuration

Item	Setting
Event Management	□ Enable

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

Enable SMS Management (Cellular support required)

To use the SMS management function, you have to configure some important settings first.



SMS Configuration

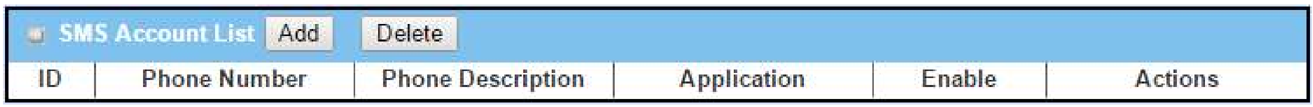
Item	Setting
Message Prefix	□ Enable &
Physical Interface	3G/4G-1 ▼ SIM Status: SIM_A
Delete Managed SMS after Processing	□ Enable

SMS Configuration		
Item	**Value setting**	**Description**
Message Prefix	The box is unchecked by default	Click the **Enable** box to enable the SMS prefix for validating the received SMS. Once the function is enabled, you have to enter the prefix behind the checkbox. The received managing events SMS must have the designated prefix as an initial identifier, then corresponding handlers will become effective for further processing.

Physical Interface	The box is 3G/4G-1 by default.	Choose a cellular interface (**3G/4G-**1 or **3G/4G-2**) to configure the SMS management setting.
SIM Status	N/A	Show the connoted cellular service (identified with **SIM_A** or **SIM_B**).
Delete Managed SMS after Processing	The box is unchecked by default	Check the **Enable** box to delete the received managing event SMS after it has been processed.

Create / Edit SMS Account (Cellular support required)

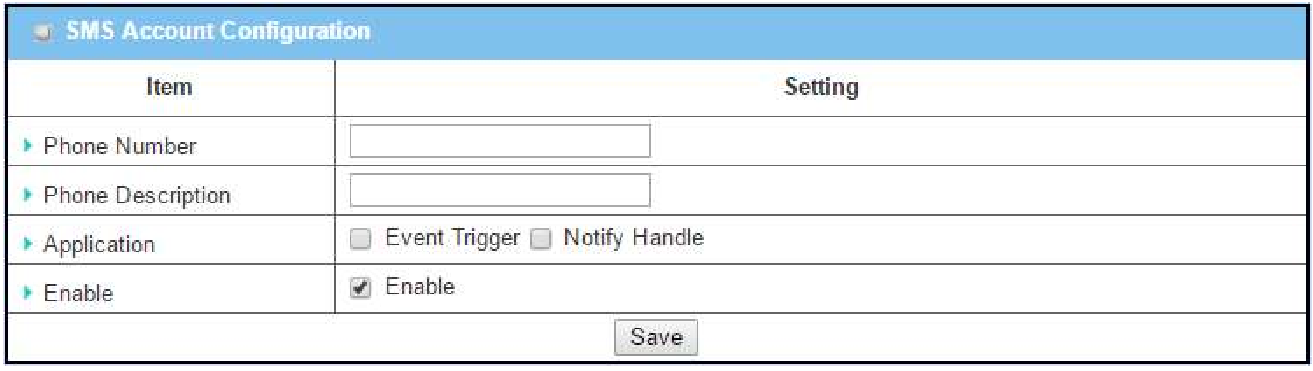
Setup the SMS Account for managing the gateway through the SMS. It supports up to a maximum of 5 accounts.



SMS Account List Add Delete

ID	Phone Number	Phone Description	Application	Enable	Actions

You can click the **Add / Edit** button to configure the SMS account.



SMS Account Configuration

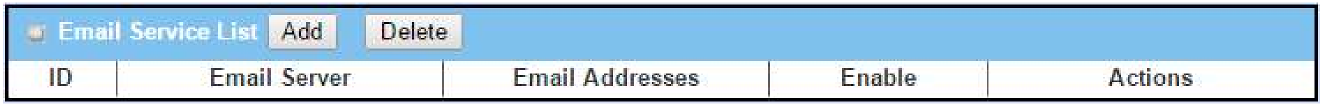
Item	Setting
Phone Number	
Phone Description	
Application	☐ Event Trigger ☐ Notify Handle
Enable	☑ Enable

Save

SMS Account Configuration		
Item	**Value setting**	**Description**
Phone Number	1. Mobile phone number format 2. A Must filled setting	Specify a mobile phone number as the SMS account identifier.
Phone Description	1. Any text 2. An Optional setting	Specify a brief description for the SMS account.
Application	A Must filled setting	Specify the application type. It could be **Event Trigger, Notify Handle,** or **both**.
Enable	The box is unchecked by default.	Click **Enable** box to activate this account.
Save	*NA*	Click the **Save** button to save the configuration.

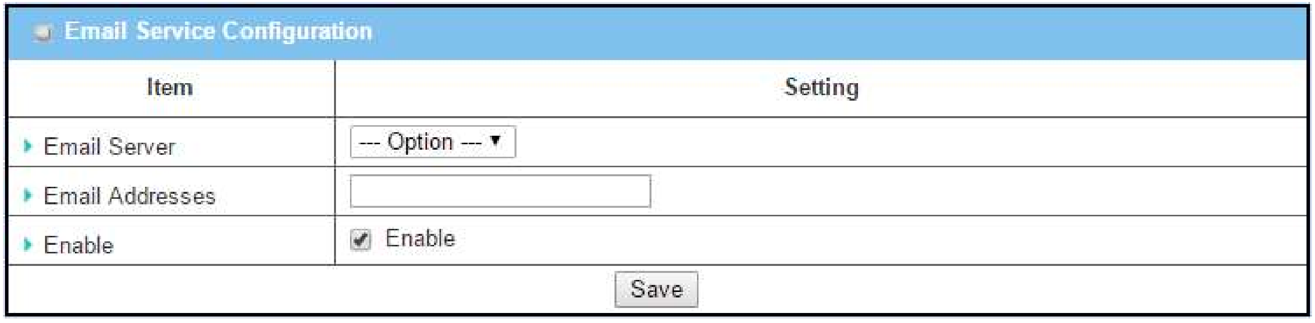
Create / Edit Email Service Account

Setup the Email Service Account for event notification. It supports up to a maximum of 5 accounts.



ID	Email Server	Email Addresses	Enable	Actions

You can click the **Add / Edit** button to configure the Email account.

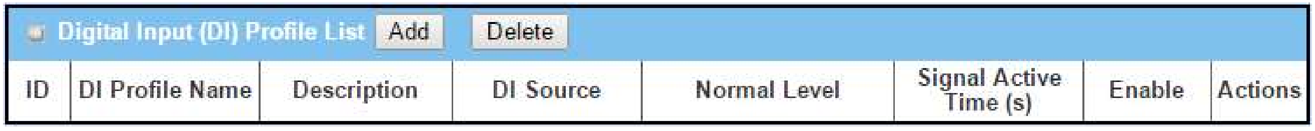


Item	Setting
Email Server	--- Option --- ▾
Email Addresses	
Enable	☑ Enable

Email Service Configuration		
Item	**Value setting**	**Description**
Email Server	--- Option ---	Select an Email Server profile from **External Server** setting for the email account setting.
Email Addresses	1. Internet E-mail address format 2. A Must filled setting	Specify the Destination Email Addresses.
Enable	The box is unchecked by default.	Click **Enable** box to activate this account.
Save	*NA*	Click the **Save** button to save the configuration

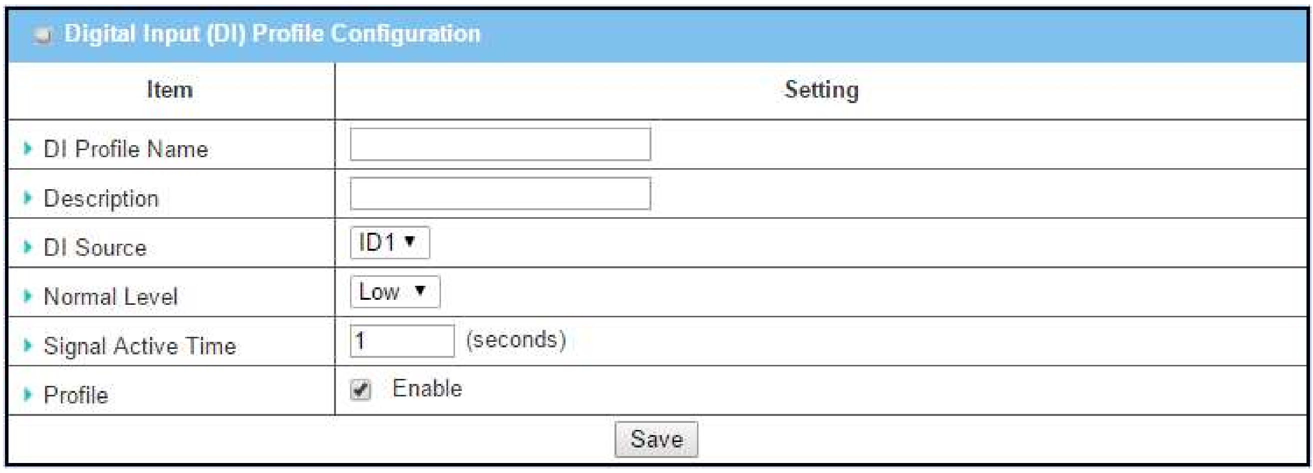
Create/Edit Digital Input (DI) Profile Rule (DI/DO support required)

Setup the Digital Input (DI) Profile rules. It supports up to a maximum of 10 profiles.



ID	DI Profile Name	Description	DI Source	Normal Level	Signal Active Time (s)	Enable	Actions

When **Add** button is applied, the **Digital Input (DI) Profile Configuration** screen will appear.

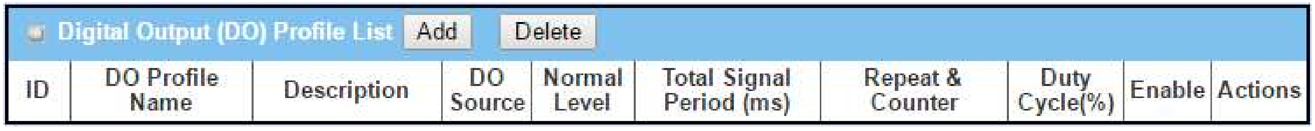


Item	Setting
DI Profile Name	
Description	
DI Source	ID1 ▾
Normal Level	Low ▾
Signal Active Time	1 (seconds)
Profile	☑ Enable

Digital Input (DI) Profile Configuration		
Item	**Value setting**	**Description**
DI Profile Name	1. String format 2. A Must filled setting	Specify the DI Profile Name.
Description	1. Any text 2. An Optional setting	Specify a brief description for the profile.
DI Source	**ID1** by default	Specify the DI Source. It could be **ID1** or **ID2**. The number of available DI source could be different for the purchased product.
Normal Level	Low by default	Specify the Normal Level. It could be **Low** or **High**.
Signal Active Time	1. Numberic String format 2. A Must filled setting	Specify the Signal Active Time. It could be from 1 to 10 seconds.
Profile	The box is unchecked by default.	Click **Enable** box to activate this profile setting.
Save	*NA*	Click the **Save** button to save the configuration.

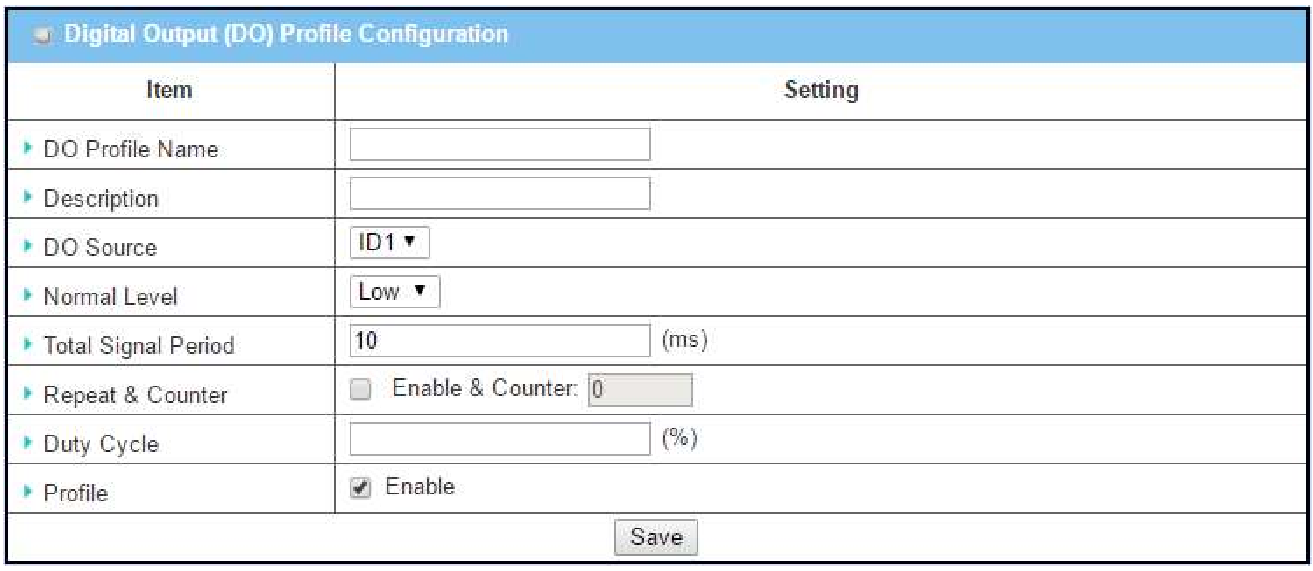
Create/Edit Digital Output (DI) Profile Rule (DI/DO support required)

Setup the Digital Output (DO) Profile rules. It supports up to a maximum of 10 profiles.



ID	DO Profile Name	Description	DO Source	Normal Level	Total Signal Period (ms)	Repeat & Counter	Duty Cycle(%)	Enable	Actions

When **Add** button is applied, the **Digital Output (DO) Profile Configuration** screen will appear.

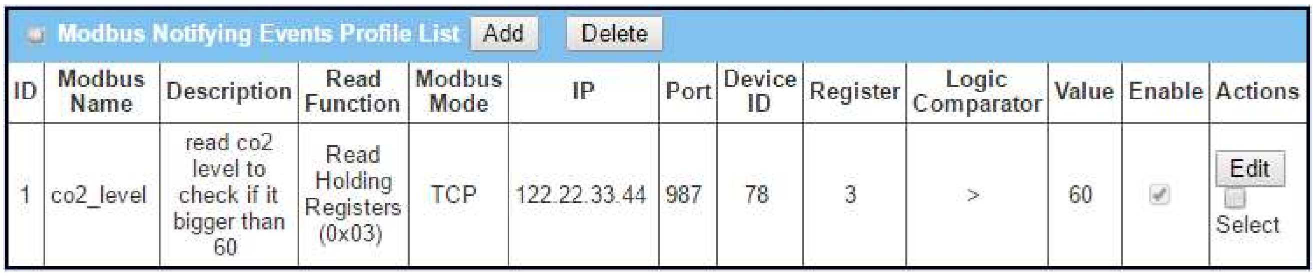


Item	Setting
DO Profile Name	
Description	
DO Source	ID1 ▾
Normal Level	Low ▾
Total Signal Period	10 (ms)
Repeat & Counter	□ Enable & Counter: 0
Duty Cycle	(%)
Profile	☑ Enable

Digital Output (DO) Profile Configuration		
Item	**Value setting**	**Description**
DO Profile Name	1. String format 2. A Must filled setting	Specify the DO Profile Name.
Description	1. Any text 2. An Optional setting	Specify a brief description for the profile.
DO Source	**ID1** by default	Specify the DO Source. It could be **ID1**.
Normal Level	Low by default	Specify the Normal Level. It could be **Low** or **High**.
Total Signal Period	1. Numberic String format 2. A Must filled setting	Specify the Total Signal Period. It could be from 10 to 10000 milliseconds.
Repeat & Counter	The box is unchecked by default.	Check the Enable box to activate the repeated Digital Output, and specify the Repeat times. The Repeat Counter could be from 0 to 9999.
Duty Cycle	1. Numberic String format 2. A Must filled setting	Specify the Duty Cycle for the Digital Output. It could be from 1 to 100 %.
Profile	The box is unchecked by default.	Click **Enable** box to activate this profile setting.
Save	*NA*	Click the **Save** button to save the configuration.

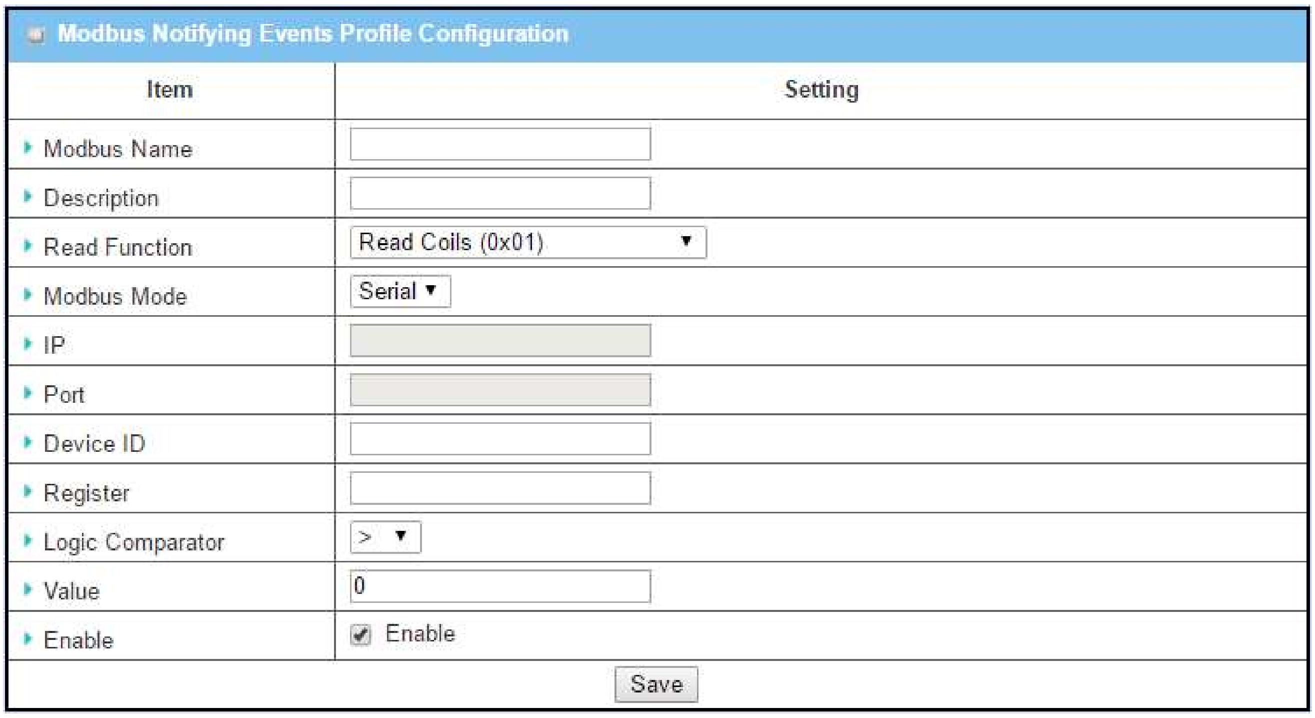
Create/Edit Modbus Notifying Events Profile (Modbus support required)

Setup the Modbus Notifying Events Profile. It supports up to a maximum of 10 profiles.



ID	Modbus Name	Description	Read Function	Modbus Mode	IP	Port	Device ID	Register	Logic Comparator	Value	Enable	Actions
1	co2_level	read co2 level to check if it bigger than 60	Read Holding Registers (0x03)	TCP	122.22.33.44	987	78	3	>	60	☑	Edit □ Select

You can click the **Add / Edit** button to configure the profile.



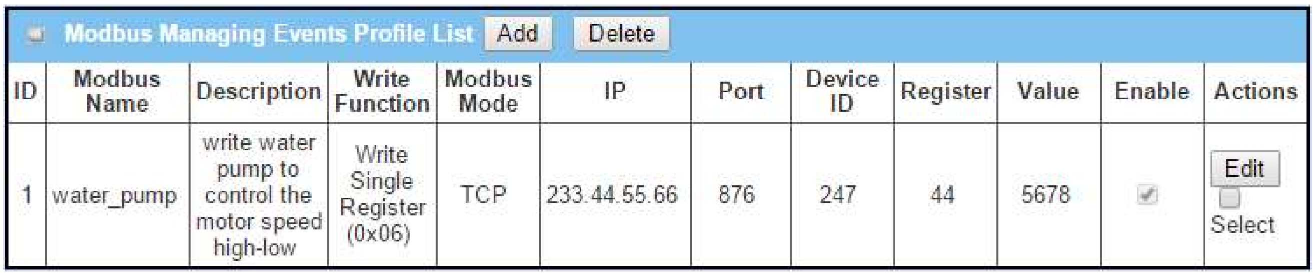
Item	Setting
Modbus Name	
Description	
Read Function	Read Coils (0x01) ▼
Modbus Mode	Serial ▼
IP	
Port	
Device ID	
Register	
Logic Comparator	> ▼
Value	0
Enable	☑ Enable

Modbus Notifying Events Profile		
Item	**Value setting**	**Description**
Modbus Name	1. String format 2. A Must filled setting	Specify the Modbus profile name.
Description	1. Any text 2. An Optional setting	Specify a brief description for the profile.
Read Function	Read Holding Registers by default	Specify the Read Function for **Notifying Events**.

Modbus Mode	**Serial** by default	Specify the Modbus Mode. It could be **Serial** or **TCP**.
IP	1. NA for Serial on Modbus Mode. 2. A Must filled setting for TCP on Modbus Mode.	Specify the IP for TCP on Modbus Mode. IPv4 Format.
Port	1. NA for Serial on Modbus Mode. 2. A Must filled setting for TCP on Modbus Mode.	Specify the Port for TCP on Modbus Mode. It could be from 1 to 65535.
Device ID	1. Numberic String format 2. A Must filled setting	Specify the Device ID of the modbus device. It could be from 1 to 247.
Register	1. Numberic String format 2. A Must filled setting	Specify the Register number of the modbus device. It could be from 0 to 65535.
Logic Comparator	Logic Comparator '>' by default.	Specify the Logic Comparator for **Notifying Events**. It could be '>', '<', '=', '>=', or '<='.
Value	1. Numberic String format 2. A Must filled setting	Specify the Value. It could be from 0 to 65535.
Enable	The box is unchecked by default.	Click **Enable** box to activate this profile setting.
Save	*NA*	Click the **Save** button to save the configuration
Undo	*NA*	Click the **Undo** button to restore what you just configured back to the previous setting.

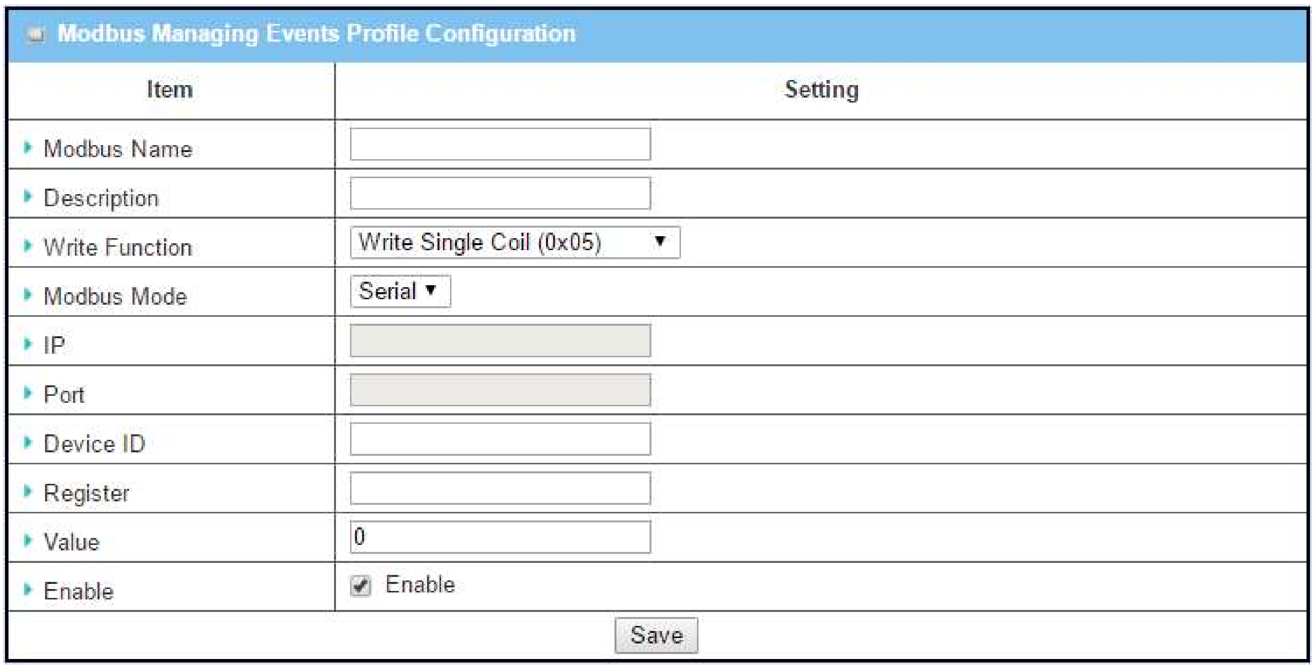
Create/Edit Modbus Managing Events Profile (Modbus support required)

Setup the Modbus Managing Events Profile. It supports up to a maximum of 10 profiles.



ID	Modbus Name	Description	Write Function	Modbus Mode	IP	Port	Device ID	Register	Value	Enable	Actions
1	water_pump	write water pump to control the motor speed high-low	Write Single Register (0x06)	TCP	233.44.55.66	876	247	44	5678	☑	Edit □ Select

You can click the **Add / Edit** button to configure the profile.



Item	Setting
Modbus Name	
Description	
Write Function	Write Single Coil (0x05) ▼
Modbus Mode	Serial ▼
IP	
Port	
Device ID	
Register	
Value	0
Enable	☑ Enable

Modbus Managing Events Profile

Item	Value setting	Description
Modbus Name	1. String format 2. A Must filled setting	Specify the Modbus profile name.
Description	1. Any text 2. An Optional setting	Specify a brief description for the profile.
Write Function	Write Single Registers by default	Specify the Write Function for **Managing Events**.
Modbus Mode	**Serial** by default	Specify the Modbus Mode. It could be **Serial or TCP**.

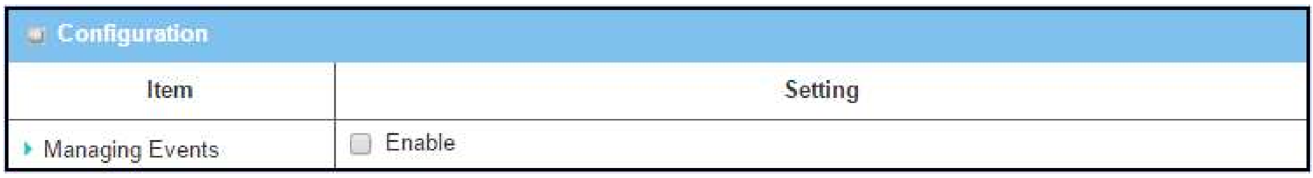
IP	1. NA for Serial on Modbus Mode. 2. A Must filled setting for TCP on Modbus Mode.	Specify the IP for TCP on Modbus Mode. IPv4 Format.
Port	1. NA for Serial on Modbus Mode. 2. A Must filled setting for TCP on Modbus Mode.	Specify the Port for TCP on Modbus Mode. It could be from 1 to 65535.
Device ID	1. Numberic String format 2. A Must filled setting	Specify the Device ID of the modbus device. It could be from 1 to 247.
Register	1. Numberic String format 2. A Must filled setting	Specify the Register number of the modbus device. It could be from 0 to 65535.
Value	1. Numberic String format 2. A Must filled setting	Specify the Value. It could be from 0 to 65535.
Enable	The box is unchecked by default.	Click **Enable** box to activate this profile setting.
Save	*NA*	Click the **Save** button to save the configuration
Undo	*NA*	Click the **Undo** button to restore what you just configured back to the previous setting.

d.3.3 Managing Events

Managing Events allow administrator to define the relationship (rule) among event trigger, handlers and response.

Go to **Service** > **Event Handling** > **Managing Events** Tab.

Enable Managing Events



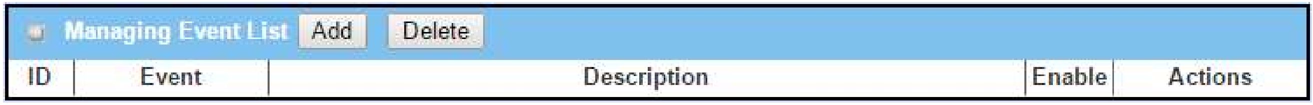
Configuration

Item	Setting
Managing Events	□ Enable

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

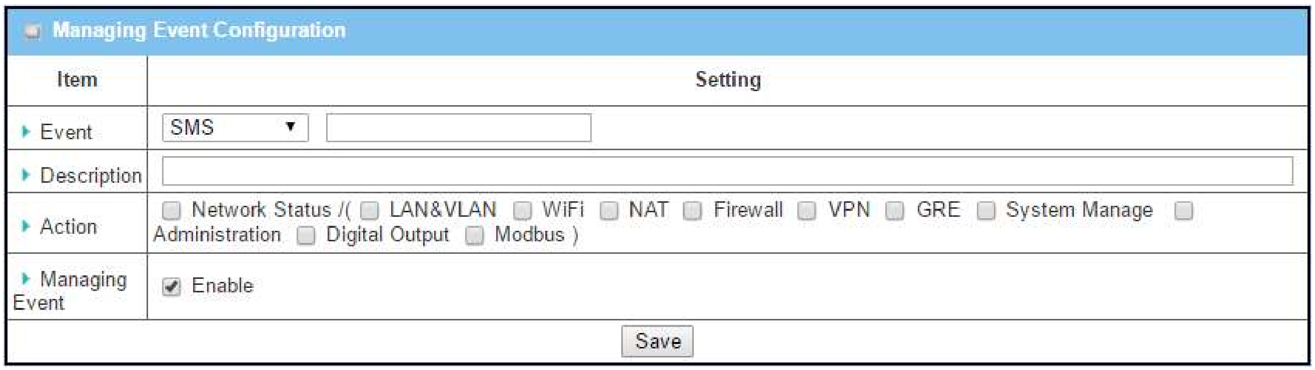
Create/Edit Managing Events Rules

Setup the Managing Event rules. It supports up to a maximum of 128 rules.



ID	Event	Description	Enable	Actions

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



Managing Event Configuration

Item	Setting
Event	SMS ▾
Description	
Action	□ Network Status /(□ LAN&VLAN □ WiFi □ NAT □ Firewall □ VPN □ GRE □ System Manage □ Administration □ Digital Output □ Modbus)
Managing Event	☑ Enable

Managing Event Configuration		
Item	**Value setting**	**Description**
Event	**SMS** (or **SNMP Trap**) by default	Specify the Event type (**SMS**, **SNMP Trap**, or **DI**) and an event identifier / profile. **SMS**: Select **SMS** and fill the message in the textbox to as the trigger condition for the event; **SNMP**: Select **SNMP Trap** and fill the message in the textbox to specify SNMP Trap Event;

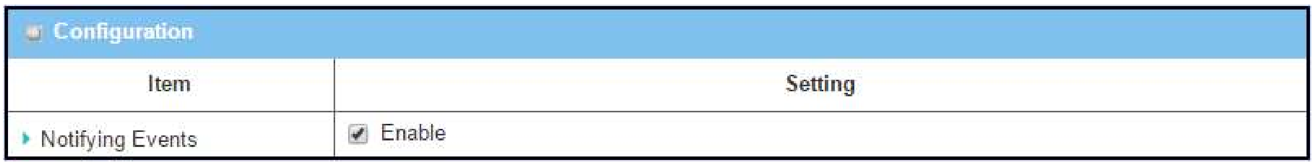
		Digital Input: Select **Digital Input** and a DI profile you defined to specify a certain Digital Input Event; *Note: The available Event Type could be different for the purchased product.*
Description	String format : any text.	Enter a brief description for the Managing Event.
Action	All box is unchecked by default.	Specify **Network Status**, or at least one rest action to take when the expected event is triggered. **Network Status**: Select Network Status Checkbox to get the network status as the action for the event; **LAN&VLAN**: Select **LAN&VLAN** Checkbox and the interested sub-items (Port link On/Off), the gateway will to change the settings as the action for the event; **WiFi**: Select **WiFi** Checkbox and the interested sub-items (WiFi radio On/Off), the gateway will to change the settings as the action for the event; **NAT**: Select **NAT** Checkbox and the interested sub-items (Virtual Server Rule On/Off, DMZ On/Off), the gateway will to change the settings as the action for the event; **Firewall**: Select **Firewall** Checkbox and the interested sub-items (Remote Administrator Host ID On/Off), the gateway will to change the settings as the action for the event; **VPN**: Select **VPN** Checkbox and the interested sub-items (IPSec Tunnel ON/Off, PPTP Client On/Off, L2TP Client On/Off, OpenVPN Client On/Off), the gateway will to change the settings as the action for the event; **GRE**: Select **GRE** Checkbox and the interested sub-items (GRE Tunnel On/Off), the gateway will to change the settings as the action for the event; **System Manage**: Select **System Manage** Checkbox and the interested sub-items (WAN SSH Service On/Off, TR-069 On/Off), the gateway will to change the settings as the action for the event; **Administration**: Select **Administration** Checkbox and the interested sub-items (Backup Configuration, Restore Configuration, Reboot, Save Current Setting as Default), the gateway will to change the settings as the action for the event; **Digital Output**: Select **Digital Output** checkbox and a DO profile you defined as the action for the event; **Modbus**: Select **Modbus** checkbox and a Modbus Managing Event profile you defined as the action for the event; *Note: The available Event Type could be different for the purchased product.*
Managing Event	The box is unchecked by default.	Click **Enable** box to activate this Managing Event setting.
Save	*NA*	Click the **Save** button to save the configuration
Undo	*NA*	Click the **Undo** button to restore what you just configured back to the previous setting.

d.3.5 Notifying Events

Notifying Events Setting allows administrator to define the relationship (rule) between event trigger and handlers.

Go to **Service** > **Event Handling** > **Notifying Events** Tab.

Enable Notifying Events



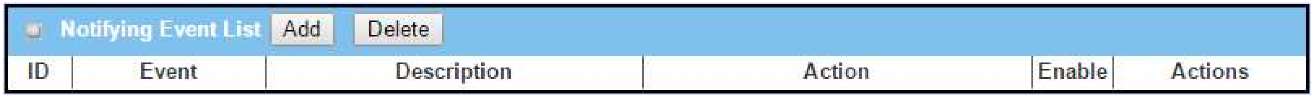
Configuration

Item	Setting
Notifying Events	☑ Enable

Notifying Events		
Item	**Value setting**	**Description**
Notifying Events	The box is unchecked by default	Check the **Enable** box to activate the Notifying Events function.

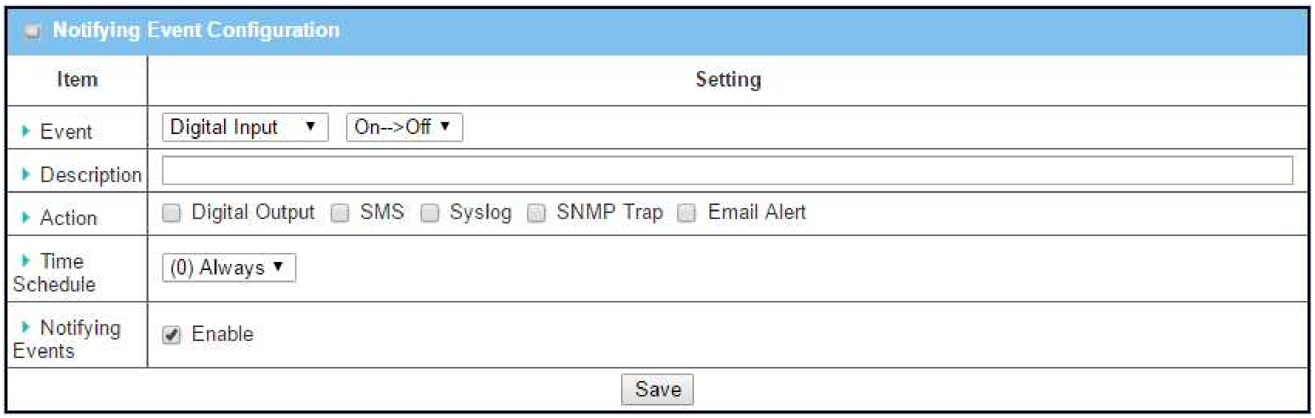
Create/Edit Notifying Events Rules

Setup your Notifying Event rules. It supports up to a maximum of 128 rules.



ID	Event	Description	Action	Enable	Actions

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



Notifying Event Configuration

Item	Setting
Event	Digital Input ▾ On-->Off ▾
Description	
Action	□ Digital Output □ SMS □ Syslog □ SNMP Trap □ Email Alert
Time Schedule	(0) Always ▾
Notifying Events	☑ Enable

Notifying Event Configuration		
Item	**Value setting**	**Description**
Event	**Digital Input** (or **WAN**) by default	Specify the Event type and corresponding event configuration. The supported Event Type could be: **Digital Input**: Select **Digital Input** and a DI profile you defined to specify

		a certain Digital Input Event; **WAN**: Select **WAN** and a trigger condition to specify a certain WAN Event; **LAN&VLAN**: Select **LAN&VLAN** and a trigger condition to specify a certain LAN&VLAN Event; **WiFi**: Select **WiFi** and a trigger condition to specify a certain WiFi Event; **DDNS**: Select **DDNS** and a trigger condition to specify a certain DDNS Event; **Administration**: Select **Administration** and a trigger condition to specify a certain Administration Event; **Modbus**: Select **Modbus** and a Modbus Notifying Event profile you defined to specify a certain Modbus Event; **Data Usage**: Select **Data Usage**, the SIM Card (Cellular Service) and a trigger condition to specify a certain Data Usage Event; *Note: The available Event Type could be different for the purchased product.*
Description	String format : any text.	Enter a brief description for the Notifying Event.
Action	All box is unchecked by default.	Specify at least one action to take when the expected event is triggered. **Digital Output**: Select **Digital Output** checkbox and a DO profile you defined as the action for the event; **SMS**: Select **SMS**, and the gateway will send out a SMS to all the defined SMS accounts as the action for the event; **Syslog**: Select **Syslog** and select/unselect the Enable Checkbox to as the action for the event; **SNMP Trap**: Select **SNMP Trap**, and the gateway will send out SNMP Trap to the defined SNMP Event Receivers as the action for the event; **Email Alert**: Select **Email Alert**, and the gateway will send out an Email to the defined Email accounts as the action for the event; *Note: The available Event Type could be different for the purchased product.*
Time Schedule	**(0) Always** is selected by default	Select a time scheduling rule for the Notifying Event.
Notifying Events	The box is unchecked by default.	Click **Enable** box to activate this Notifying Event setting.
Save	*NA*	Click the **Save** button to save the configuration
Undo	*NA*	Click the **Undo** button to restore what you just configured back to the previous setting.

d.5 Location Tracking

Location tracking applications are usually referred to applications that take benefits from Global Navigation Satellite System (GNSS). GNSS is the infrastructure that allows devices to determine its position, velocity, and time by processing satellites signals from outer space. GNSS includes varieties of satellite systems and Satellite-Based Augmentation Systems (SBAS). SBAS is usually used for improving positioning accuracy. The tables below show 4 major GNSS system in the world, and SBAS system in different areas.

Major GNSS System in the world

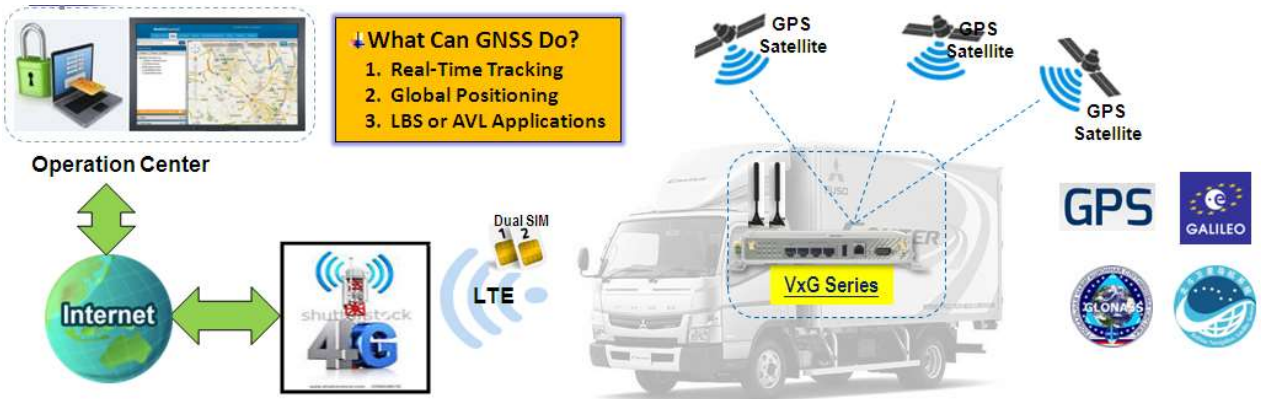
GNSS System	Owner
GPS	USA
GLONASS	Russia
Galileo	European Union
BeiDou (COMPASS)	China

Satellite-Based Augmentation System (SBAS)

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

Position applications are widely-used by varieties of industrial applications, including Location-Based Services (LBS), Automatic Vehicle Location (AVL), Fleet Management, or assets tracking. However, in most case, GNSS is a one-way communication. That means GNSS-compatible device can only locate its location by receiving GNSS signal, but it can’t forward its location data to any other identity through GNSS system. According to this limitation by GNSS system, devices usually need to equip other technology to transmit their location data to back-end server for track or further analysis. Furthermore, as the position applications are more applied on moving objects, a kind of wireless technology would be more suitable to be adopted to transmit location data. Nowadays, thanks to popularity and wide coverage of cellular technology (GSM, 3G, 4G/LTE), transmitting location data to remote center in real time is no longer a hurdle. In addition, the data format of location data is NMEA 0183 compatible, so the back-end server will be easy to interpret the collected location data.

Hereunder are the main features of GNSS function in the VxG In-Vehicle Gateway.



- Retrieve GNSS data from satellites and send to remote operation center periodically or save in local storage.
- Global positioning with multiple GNSS systems, including GPS, and optional for GLONASS, Galileo, or BeiDou.
- Mandatory for varieties of LBS (Location-Based Service) applications, such as advertisement, emergent call.
- Easy integration with AVL (Automatic Vehicle Location) applications, for managing fleet of service vehicles.
- Other value-added applications, such as asset tracking, electronic toll collection, intelligent transport system.

d.5.1 GNSS

With GNSS configuration page, you can configure those functions that are mentioned above. Please note the available GNSS features on different models may be different. Please check product datasheet for details.

The configuration steps include following items.

- Activate GNSS feature in gateway and finish settings of cellular WAN.
- Support NMEA 0183 (compatible to 3.0) protocol, and allow customized prefix and suffix.
- Configurable GPS data logging on local microSD card storage for route record tracking.
- Indicate remote host, time interval, TCP/UDP, and type of GPS data that would be sent.

- **GPS Message Type**

This item shows all supported types of NMEA 0183 data format. NMEA 0183 data format was defined and maintained by National Marine Electronics Association (NMEA). Select one or more types that you want to use for transmitting GPS data. In most case, this configuration depends on which data format that your central server can recognize. Only select the type you need, otherwise it will consume unnecessary network bandwidth. The table below shows more information for different types of NMEA 0183 message.

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

Please note this option is hardware dependent. The available options of GPS message type show on this page is according to product specification. You may not see all options if your product doesn’t support all of them.

- **SBAS**

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

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

Please note this option is hardware dependent. You may not see this option if your product doesn’t support it.

- **Assisted GPS**

Assisted GPS (as known as A-GPS) is used for speeding up location fix, especially when satellite signal is weak. If activating this option, gateway will download almanac data from A-GPS server through IP network instead of from satellite. You can also choose different valid period of almanac data. The shorter almanac data will get higher accuracy. However, the almanac data with shorter valid period needs to be updated more frequently. It will consume more network bandwidth. Please note this option is hardware dependent. You may not see this option if your product doesn’t support it.

- **Data to Storage**

Besides transmitting location data to remote server, you can also store location data into internal storage (e.g. microSD card) or external storage (e.g. USB drive) if any. Regarding to data format, either can be NMEA 0183 raw data format or save it as GPX file format. The location data will be saved to a new file if the original file size is bigger than the pre-defined file size. The “Download log file” button allows you to browse all saved log files and download to your personal devices.

- **Scenario of location tracking for fleet management**

A fleet owner would like to see the locations of his trucks in real time. He also likes to know where his trucks have been passed through with time information. In his operation office, there is a server (IP: 100.100.100.1) which can interpret NMEA RMC data format and shows truck's location and track on map. This server is listening on TCP port 888 to receive NMEA RMC packet from trucks. IMEI number will be added before NMEA RMC data for identification of each truck. Hereunder is the configuration on each truck.

Basic Settings:

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

Settings for Remote Host:

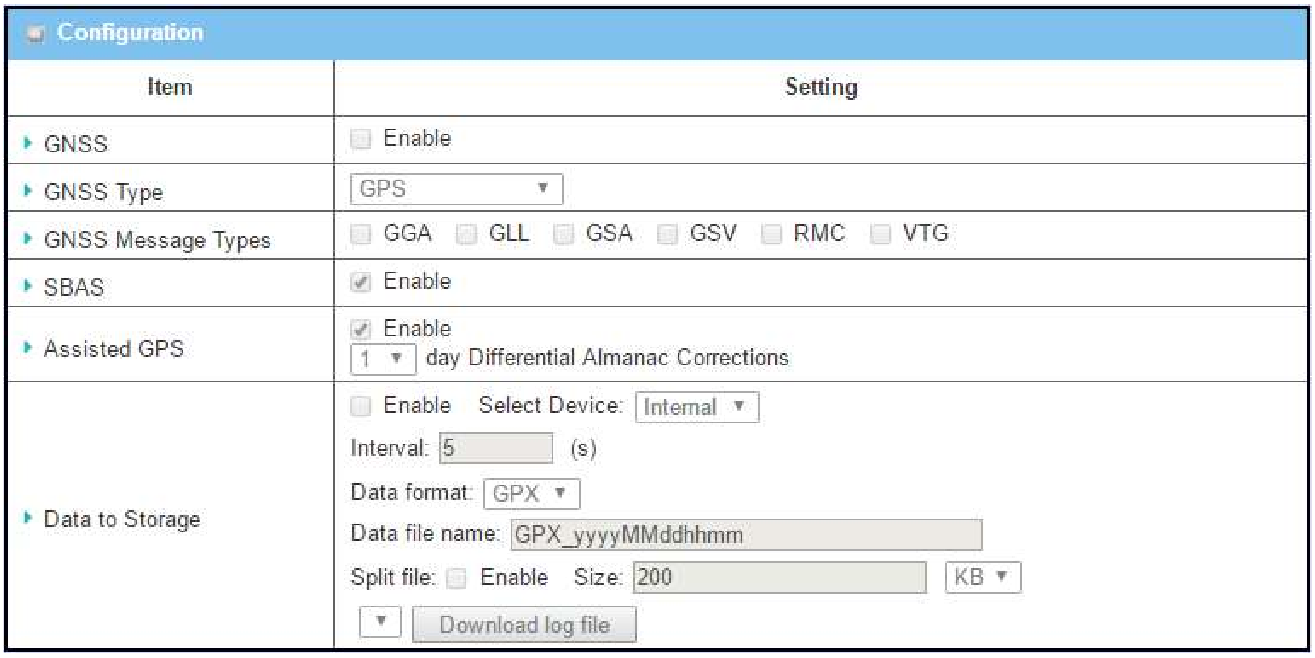
Configuration Path	[GNSS]-[Remote Host Configuration]
Host Name	*Truck-1*
Host IP	*100.100.100.1*
Protocol Type	*TCP*
Port Number	*888*
Interval(s)	*15*
Prefix Message	*123456789012345*
Suffix Message	*[blank]*
Enable Checkbox	*[Checked]*

GNSS Setting

The GNSS allows user to set the configuration of GNSS, log NMEA data to storage, and send data to remote host. Ensure GNSS is enabled and saved

Go to **Service > Location Tracking > GNSS** Tab

Setup GNSS Configuration



Configuration

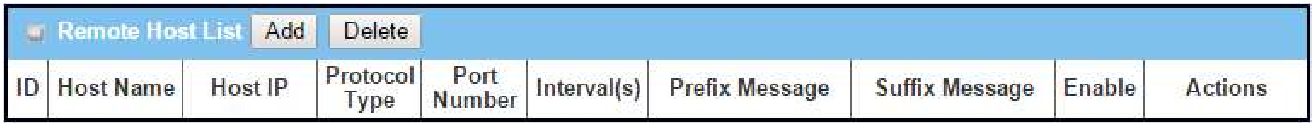
Item	Setting
GNSS	☐ Enable
GNSS Type	GPS ▼
GNSS Message Types	☐ GGA ☐ GLL ☐ GSA ☐ GSV ☐ RMC ☐ VTG
SBAS	☑ Enable
Assisted GPS	☑ Enable 1 ▼ day Differential Almanac Corrections
Data to Storage	☐ Enable Select Device: Internal ▼ Interval: 5 (s) Data format: GPX ▼ Data file name: GPX_yyyyMMddhhmm Split file: ☐ Enable Size: 200 KB ▼ ▼ Download log file

GNSS		
Item	**Value setting**	**Description**
GNSS Enable	The box is unchecked by default	Check **Enable** box to 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. The available options of GNSS type show on this page is according to product specification. You may not see all of these four options if your product doesn't support all of them.
GNSS Message Types	These box is unchecked by default.	Select one or more **GNSS Message Types** that you want to use for transmitting or recording GPS data. There are many sentences in the NMEA standard for selecting, **GGA, GLL, GSA, GSV, RMC and VTG**. **ALL Other** includes DTM, GNS, GRS, GST, ZDA, and GBS sentences. Only select the type you need, otherwise it

		will consume unnecessary network bandwidth.
SBAS	The box is unchecked by default	Check **Enable** box to activate satellite-based augmentation system (**SBAS**). Note: Some devices do not support this function.
Assisted GPS	The box is checked by default	Check **Enable** box to activate Assisted GPS (A-GPS). Select the duration for downloading the **Differential Almanac Corrections** data from A-GPS server through IP network. Note: Some devices may not support this function.
Data to Storage	The box is unchecked by default	● **Enable** (The box is unchecked by default) Check **Enable** box to activate data to storage function. ● **Select Device** (A Must filled setting) Select **Internal** or **External** device to store log data. ● **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 activate file splitting function. ● **Split Size& Unit** Define file size and unit for log file. ● **Download log file** Select a log file and Click **Download log file** to download through Web GUI. If the log format which is specified to download is GPX, we will convert standard GPX format for used.
Save	*NA*	Click the **Save** button to save the configuration

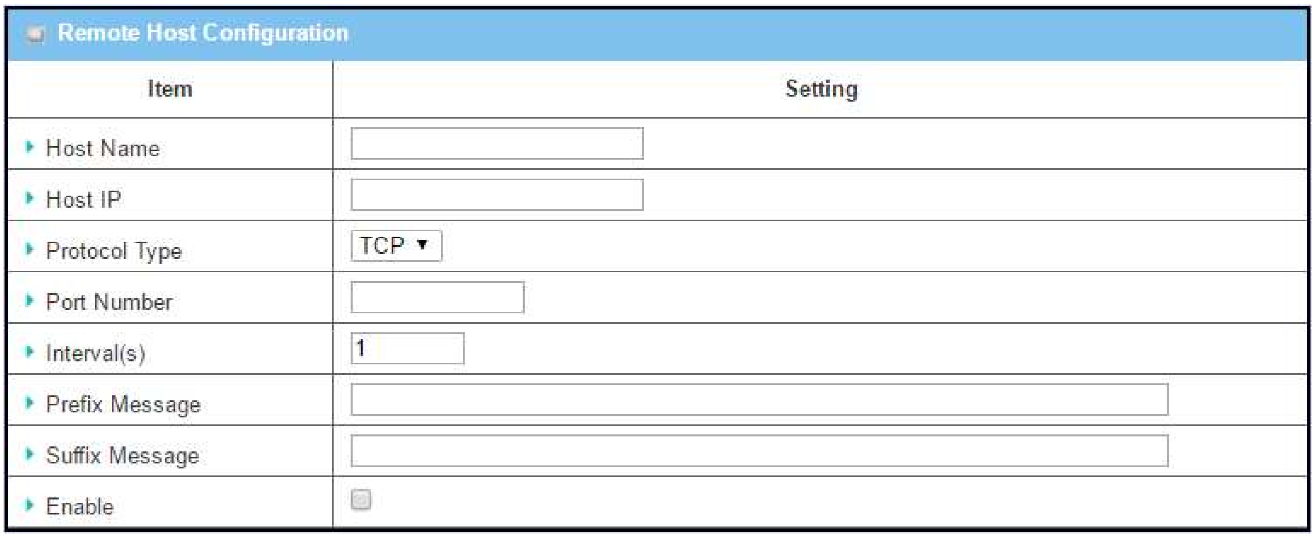
Create/Edit Remote Host

The Remote Host allows you to customize your rules for sending NMEA data to specific IP address and Port. The router supports up to a maximum of 10 rule sets.



ID	Host Name	Host IP	Protocol Type	Port Number	Interval(s)	Prefix Message	Suffix Message	Enable	Actions

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



Remote Host Configuration

Item	Setting
Host Name	
Host IP	
Protocol Type	TCP ▾
Port Number	
Interval(s)	1
Prefix Message	
Suffix Message	
Enable	□

Remote Host Configuration		
Item	**Value setting**	**Description**
Host Name	String format: any text	Enter the host name for the designated remote host.
Host IP	A Must filled setting	Specify the **IP Address** of remote host. It will be use as destination IP for sending NMEA packets.
Protocol Type	**TCP** is selected by default	Specify the **Protocol** (**TCP** or **UDP**) to use for sending NMEA packets.
Port Number	A Must filled setting	Specify a **Port Number** as destination port for sending NMEA packets.
Interval(s)	A Must filled setting	Specify the time **interval** (seconds) between two NMEA packets.
Prefix Message	String format: any text	Specify optional prefix string with specific information if your backend server can recognize. For example, you can input the IMEI code of this device here, and then your backend server can recognize this GPS data is sent from this device. You can also leave this field blank.
Suffix Message	String format: any text	Specify optional suffix string with specific information if your backend server can recognize.
Enable	The box is unchecked by default	Check **Enable** box to activate this remote host rule.
Save	*NA*	Click the **Save** button to save the configuration