M2M Cellular Gateway

IDG700AM-0T001

User Manual

Index skipping is used to reserve slots for new function insertion, when required.

Chapter 1 Introduction 6
1.1 Introduction 6
1.2 Contents List 7
1.2.1 Package Contents 7
1.3 Hardware Configuration 8
1.4 LED Indication 10
1.5 Installation Requirement 11
1.5.1 WARNING 11
1.5.2 SYSTEM REQUIREMENTS 11
1.6 Hardware Installation 12
1.6.1 Mount the Unit 12
1.6.2 Insert the SIM Card 12
1.6.3 Connecting Power 13
1.6.4 Connecting to the Network or a Host 14
Chapter 2 Getting Started 15
2.1 Wizard 15
Network Setup Wizard 15
VPN Setup Wizard 24
2.3 Status 30
2.3.3 Network Status 30
2.3.7 Client List 38
2.3.9 Firewall Status 39
2.3.b VPN Status 43
2.3.d System Mgmt. Status 46
Chapter 3 Basic Network 48
3.1 WAN 48
3.1.1 Physical Interface 49
3.1.3 Internet Setup 61
3.3 LAN & VLAN 71
3.3.1 Ethernet LAN 71

Index skipping is used to reserve slots for new function insertion, when required.

3.3.3 VLAN........71
3.7 IPv6........87
3.7.1 IPv6 Configuration........91
3.9 NAT / Bridge........98
3.9.1 NAT Configuration........98
3.9.3 Virtual Server & Virtual Computer........102
3.9.5 Special AP & ALG........110
3.9.7 DMZ & Pass Through........117
3.b Routing........120
3.b.1 Static Routing........120
3.b.3 Dynamic Routing........125
3.b.5 Routing Information........137
3.d Client & Server & Proxy........138
3.d.1 DNS & DDNS........138
3.d.3 DHCP Server........143
Chapter5 Advanced Network........149
5.1 Firewall........149
5.1.1 Firewall Configuration........149
5.1.3 Packet Filters........150
5.1.5 URL Blocking........157
5.1.9 Web Content Filters........163
5.1.b MAC Control........168
5.1.d Application Filters........173
5.1.f IPS........177
5.1.h Options........182
5.3 QoS & BWM........187
5.3.1 Configuration........187
5.3.3 Rule-based QoS........190
5.5 VPN........204
5.5.1 Configuration........204

5.5.3 IPSec 206
5.5.5 PPTP 227
5.5.7 L2TP 239
5.5.9 GRE 251
5.5.d OpenVPN 259
5.7 Redundancy 275
5.7.1 VRRP 275
5.9 System Management 279
5.9.1 TR-069 279
5.9.3 SNMP 283
5.9.5 Telnet with CLI 294
5.9.7 UPnP 297
5.b Certificate 300
5.b.1 Configuration 300
5.b.3 My Certificates 302
5.b.5 Trusted Certificates 309
5.b.7 Issue Certificates 315
Chapter 7 Applications 320
7.1 Mobile Application 320
7.1.1 SMS 320
7.1.3 USSD 324
7.1.5 Network Scan 329
7.1.7 SMS Management 331
7.5 Captive Portal 340
7.5.1 Configuration 340
Chapter 9 System 346
9.1 System Related 346
9.1.1 System Related 346
9.3 Scheduling 354
9.7 Grouping 356

9.9 External Servers 359
9.b MMI 362

Index skipping is used to reserve slots for new function insertion, when required.

Chapter 1 Introduction

1.1 Introduction

Congratulations on your purchase of this outstanding product: M2M Cellular Gateway. For M2M (Machine-to-Machine) applications, AMIT M2M Cellular Gateway is absolutely the right choice. With built-in world-class 3G HSPA+ or 4G LTE module, you can just insert the SIM card from local mobile carrier then connect to Internet. The redundant SIM design provides a reliable WAN connection for critical applications. By VPN tunneling technology, it's easily to make remote sites network being an Intranet, all data will be transmitted via the security link (256-bit AES encryption). To meet a variety of M2M application requirements, AMIT M2M Cellular Gateway products are based on modular design. A new functional module can replace current one to support new application in short time, such as for NFC or GPS applications.

This IDG700AM 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 3G/LTE WAN connection.
- Support dual SIM cards for the redundant wireless WAN connection.
- Provide one Ethernet port for comprehensive LAN connection.
- 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 M2M 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

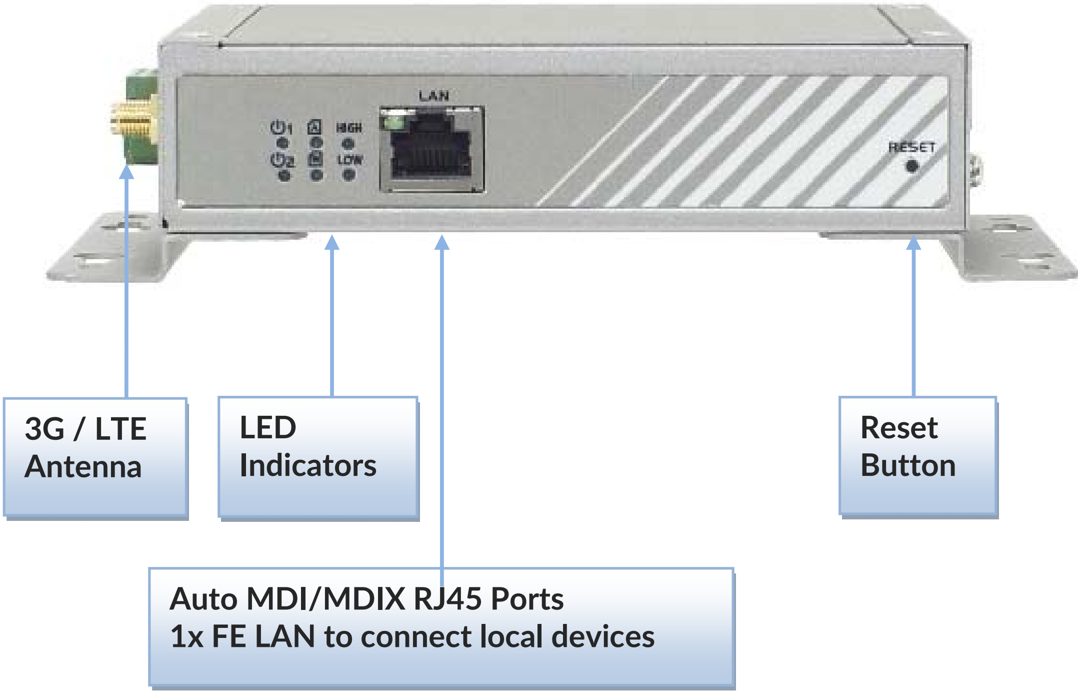
#Standard Package

Items	Description	Contents	Quantity
1	IDG700AM-0T001 M2M Cellular Gateway		1pcs
2	**Cellular Antenna**		2pcs
3	**Power Adapter (DC 12V/1A)** (*[1])		1pcs
4	**RJ45 Cable**		1pcs
5	**CD (Manual)**		1pcs
6	**Mounting Bracket**		2pcs
7	DIN-Rail Bracket		1pcs

[1] The maximum power consumption of IDG700-0T001 is 9.3W.

1.3 Hardware Configuration

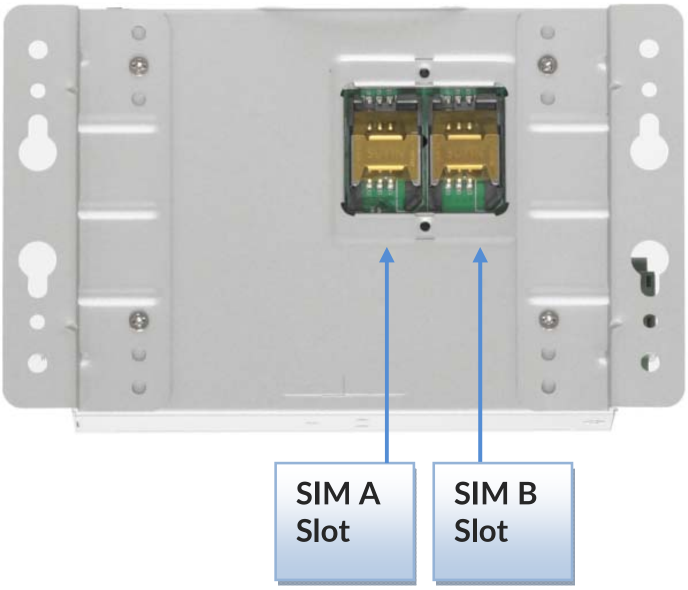
➢ Front View



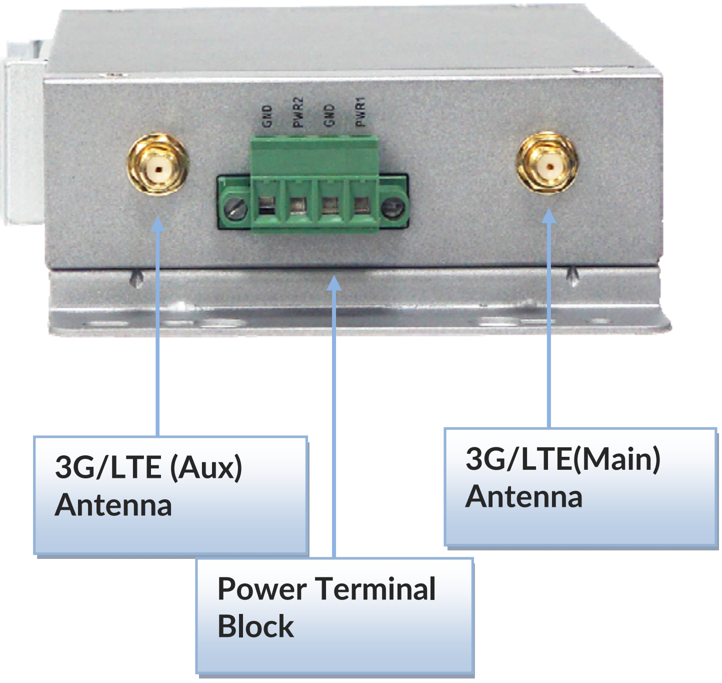
※**Reset Button**

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.

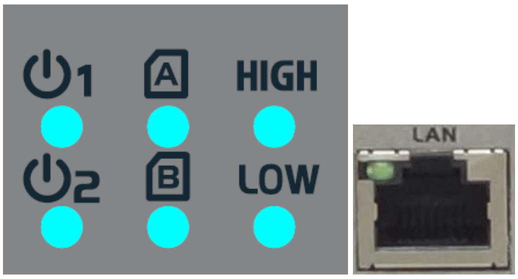
- Bottom View



- 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
A	SIM A (*[3])	Green	**Steady ON:** SIM card A is chosen for connection
B	SIM B	Green	**Steady ON:** SIM card B is chosen for connection
HIGH	High Cellular Signal	Green	**Steady ON:** The signal strength of Cellular is strong
LOW	Low Cellular Signal	Green	**Steady ON:** The signal strength of Cellular is weak
	LAN	Green	**Steady ON:** Ethernet connection of LAN WAN is established **Flash:** Data packets are transferred

[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.

[3] The SIM LED indicates which SIM socket will be chosen for connection by system setting, no matter SIM card is inserted or not.

1.5 Installation Requirement

1.5.1 WARNING

Attention

- Do not use the product in high humidity or high temperatures.
- 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

1.5.2 SYSTEM REQUIREMENTS

Network Requirements	• 3G / LTE cellular service subscription • 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

Index skipping is used to reserve slots for new function insertion, when required.

1.6 Hardware Installation

This chapter describes how to install and configure the hardware

1.6.1 Mount the Unit

The IDG700AM series can be placed on a desktop, mounted on the wall or mounted on a DIN-rail. The DIN-rail bracket is not screwed on the product when out of factory. Please screw the DIN-rail bracket on the product first if necessary.

1.6.2 Insert the SIM Card

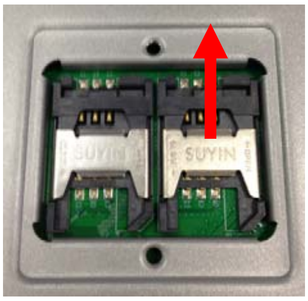
WARNNING: BEFORE INSERTING OR CHANGING THE SIM CARD, PLEASE MAKE SURE THAT POWER OF THE DEVICE IS SWITCHED OFF.

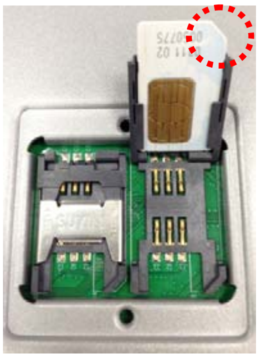
The SIM card slots are located at the bottom side of IDG700 series housing in order to protect the SIM card. You need to unscrew and remove the outer SIM card cover before installing or removing the SIM card. Please follow the instructions to insert a SIM card. After SIM card is well placed, screw back the outer SIM card cover.

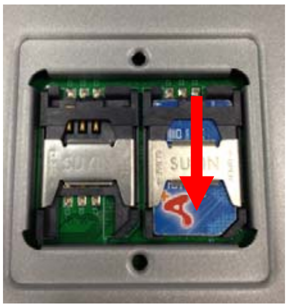
Step 1:
Follow red arrow to unlock SIM socket

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

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

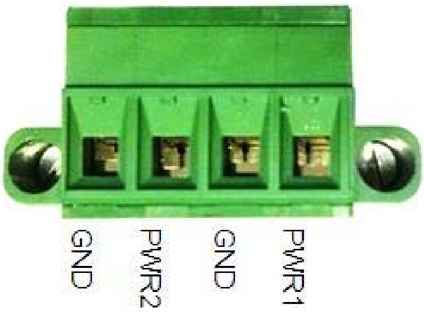




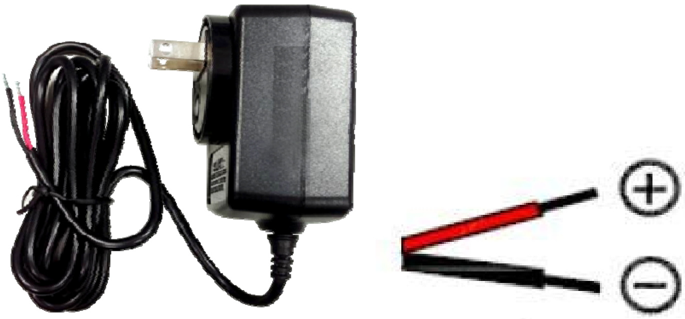


1.6.3 Connecting Power

The IDG700AM series can be powered by connecting one or two power sources to the terminal block. **It supports dual 9 to 48VDC power inputs**[4]. Following picture is the power terminal block pin assignments and it is located at the right side of device. Please check carefully and connect to the right power requirements and polarity.



There are a DC converter and a DC12V/1A power adapter[5] 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.

[4] If both of power source 1 and power source 2 are connected, the device will choose power source 1 first. If power outage occurred from power source 1, this device will switch to power source 2 automatically and seamlessly.

[5] The maximum power consumption of IDG700-0T001 is 9.3W.

1.6.4 Connecting to the Network or a Host

The IDG700AM series provides one RJ45 port to connect 10/100Mbps Ethernet. It can auto detect the transmission speed on the network and configure itself automatically. Connect one Ethernet cable to the RJ45 port (LAN) of the device on the front panel and plug another end of the Ethernet cable into your computer’s network port. In this way, you can use the RJ45 Ethernet cable to connect the IDG700AM series to the host PC’s Ethernet port for configuring or troubleshooting the device.

Index skipping is used to reserve slots for new function insertion, when required.

Chapter 2 Getting Started

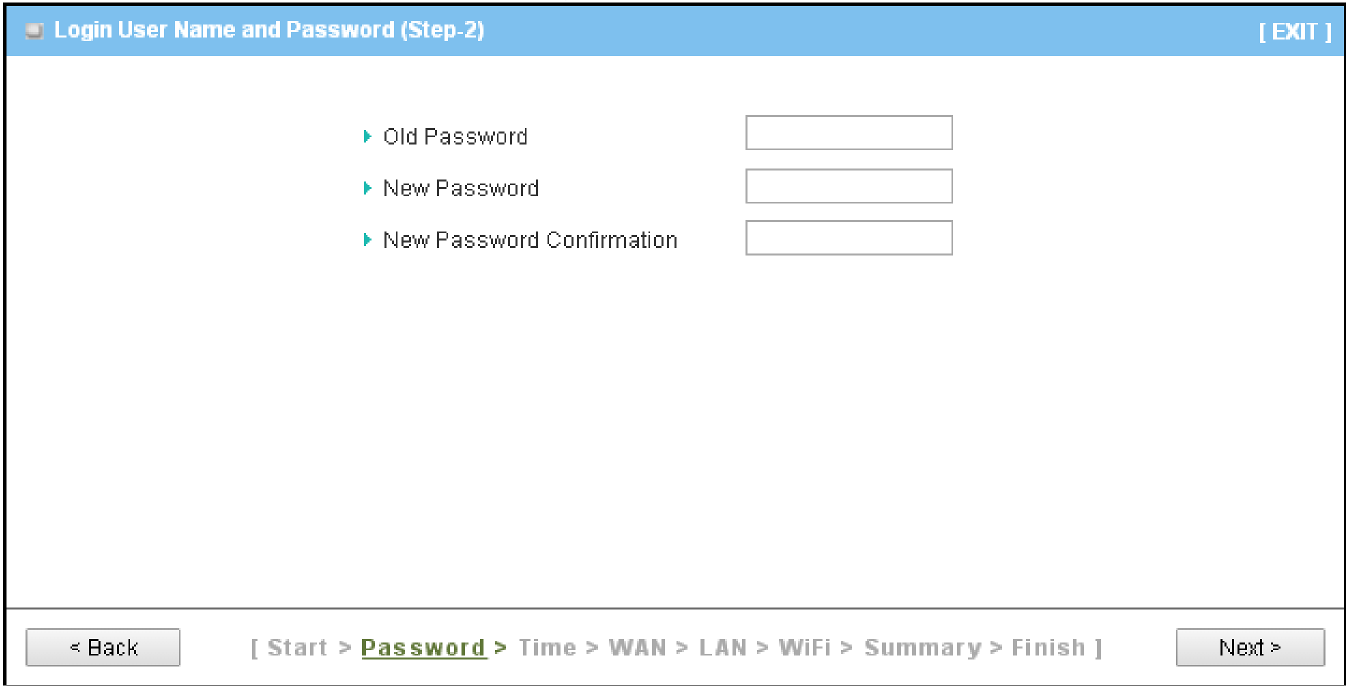
2.1 Wizard

Network Setup Wizard

Wired Router Network Setup Wizard will guide you through a basic configuration procedure step by step.

Step-2 is to change your login password.

Go to Wizard > Network Setup Wizard > Step-2



Login User Name and Password (Step-2)

Old Password

New Password

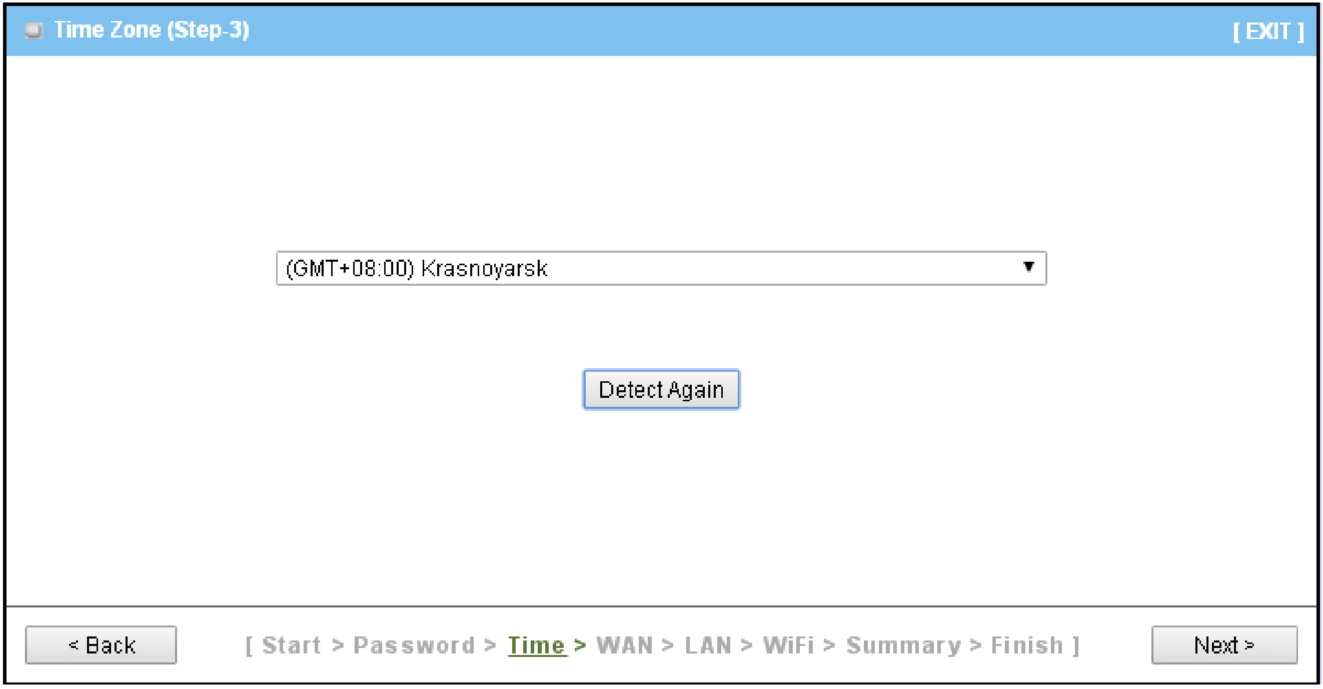
New Password Confirmation

< Back
[Start > Password > Time > WAN > LAN > WiFi > Summary > Finish]
Next >

Item	Value setting	Description
Old Password	1. String format: any text	If you want to change password, Enter the current password in this item.
New Password	1. String format: any text	Enter the new password.
New Password Confirmation	The box is unchecked by default	Enter the new password to re-confirm.
Exit	NA	Click the Exit button to cancel Setup Wizard.
Back	NA	Click the Back button to go to the previous step.
Next	NA	Click the Next button to go to the next step.

Step-3 is to change the time zone.

Go to Wizard > Network Setup Wizard > Step-3



Item	Value setting	Description
Time zone list	1. A Must filled setting	Select the time zone for the system clock.
Detect Again	NA	Click the **Detect Again** button to detect the time zone from network.
Exit	NA	Click the **Exit** button to cancel Setup Wizard.
Back	NA	Click the **Back** button to go to the previous step.
Next	NA	Click the **Next** button to go to the next step.

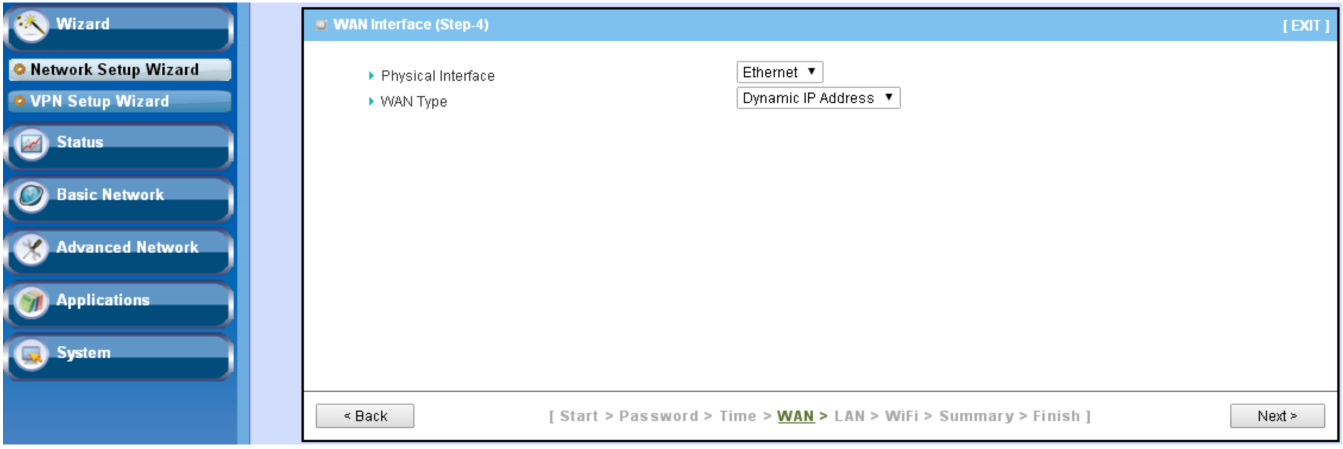
Item	Value setting	Description
Rule Name	1. String format: any text 2. A Must filled setting 3. By default **Always** is selected. 4. The box is unchecked by default. 5. *NA*	

Index skipping is used to reserve slots for new function insertion, when required.

Step 4. Internet Connection (WAN Interface Setting)

In this step of the Wizard you will be specifying how your router connects to the Internet by selecting the appropriate Physical Interface and WAN Type. For detail settings, refer to the following pages for your required settings.

Go to Wizard > Network Setup Wizard > Step 4. WAN interface



Physical Interface: Ethernet

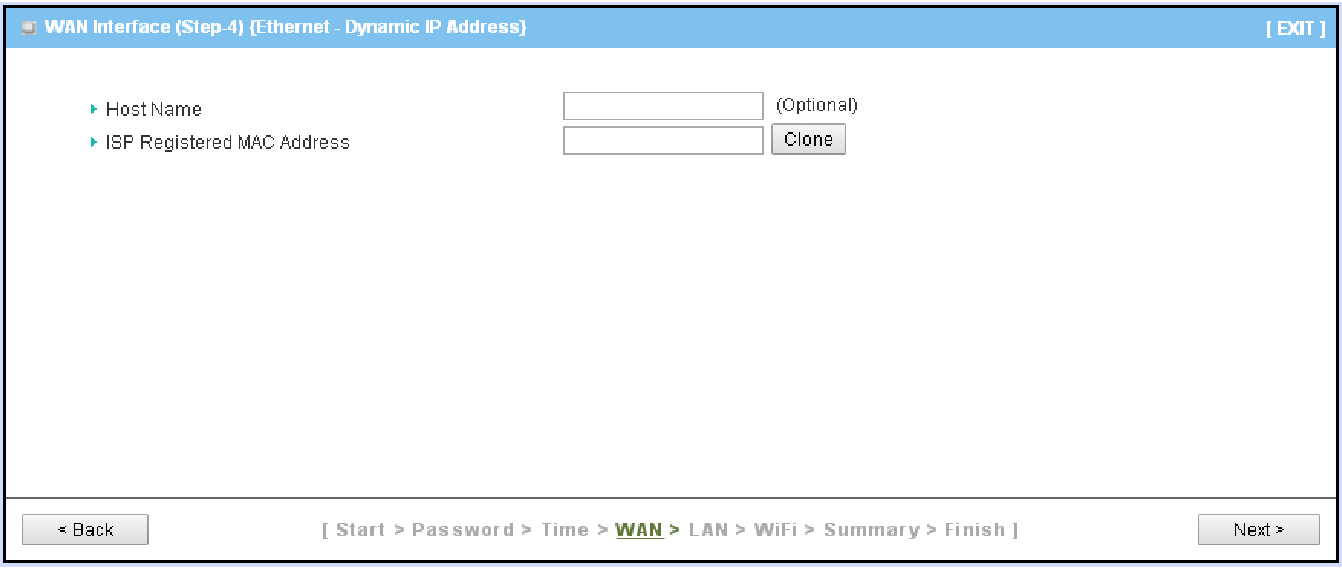
WAN Type: Dynamic IP Address

Step 4. WAN interface Setting		
Item	**Value setting**	**Description**
Physical Interface	A Must filled setting	Here you specify the Physical Interface that connects your router to the Internet. The type of available Interfaces will depend on the router model. They are normally the Ethernet port and the 3G/4G wireless interface.
WAN Type	A Must filled setting	Choose the WAN type for the selected Physical Interface above.
Back	N/A	Click **Back** button to go to previous step
Next	N/A	Click **Next** button to go to next sub-steps

Index skipping is used to reserve slots for new function insertion, when required.

Physical Interface: Ethernet

WAN Type: Dynamic IP Address



WAN Interface (Step-4) {Ethernet - Dynamic IP Address} [EXIT]

- Host Name (Optional)
- ISP Registered MAC Address Clone

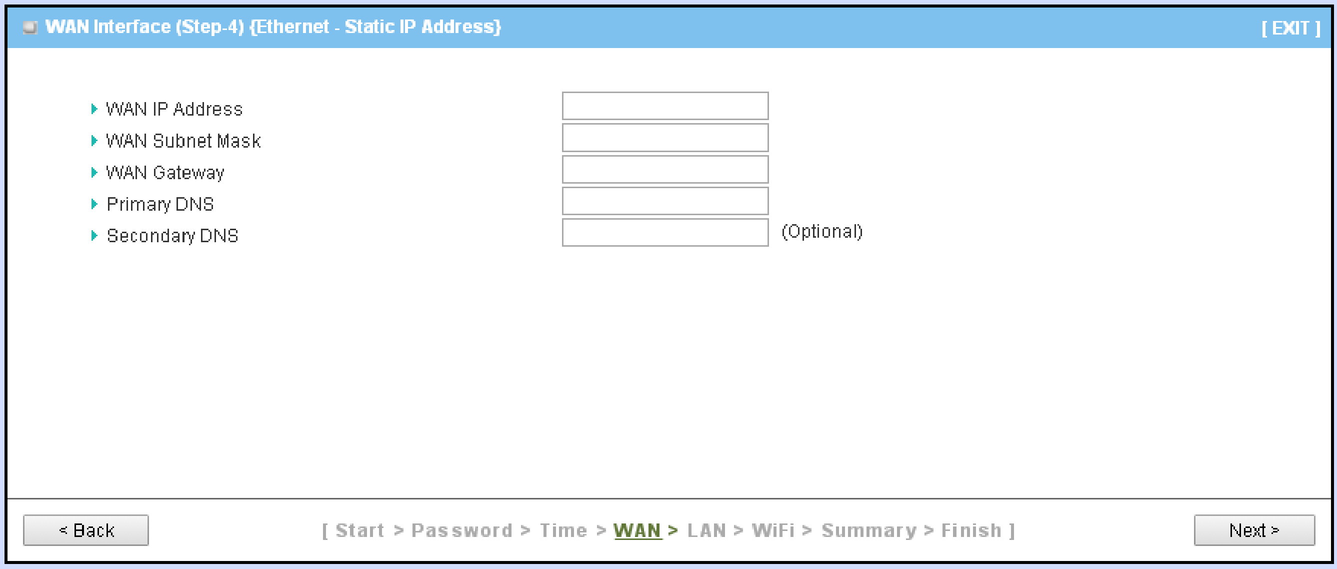
< Back
[Start > Password > Time > WAN > LAN > WiFi > Summary > Finish]
Next >

Dynamic IP Settings		
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.
Back	N/A	Click **Back** button to go to previous step
Next	N/A	Click **Next** button to go to next step

Index skipping is used to reserve slots for new function insertion, when required.

Physical Interface: Ethernet

WAN Type: Static IP Address



WAN Interface (Step-4) {Ethernet - Static IP Address}

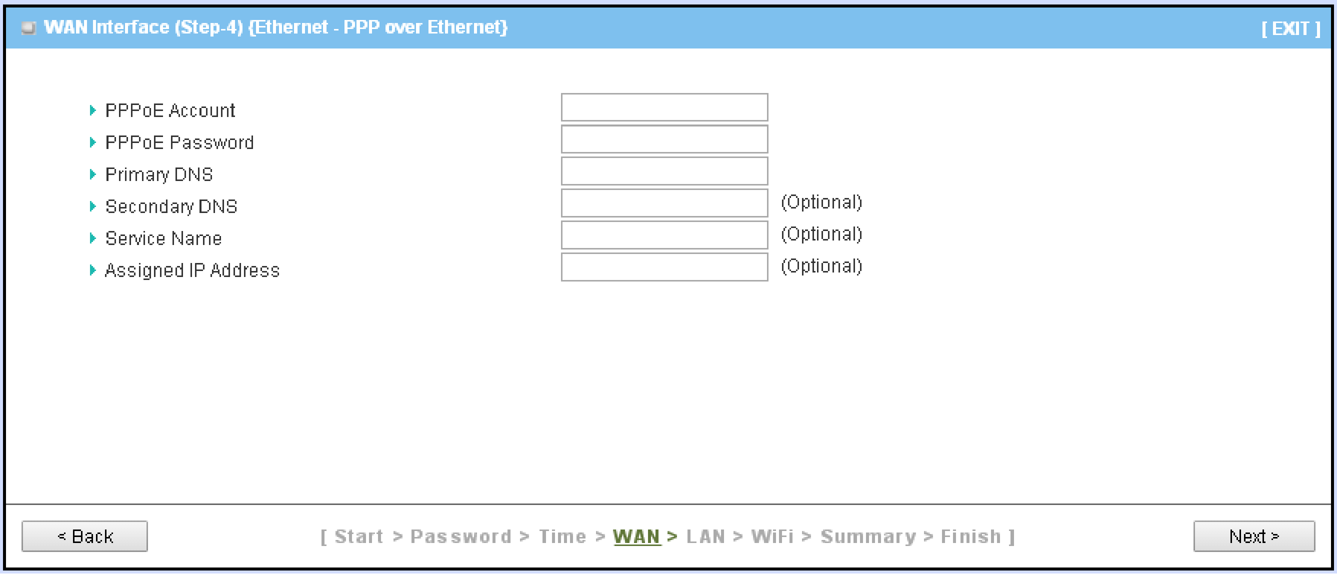
- WAN IP Address
- WAN Subnet Mask
- WAN Gateway
- Primary DNS
- Secondary DNS (Optional)

[EXIT]
< Back
[Start > Password > Time > WAN > LAN > WiFi > Summary > Finish]
Next >

Static IP Settings		
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	Optional setting	Enter the secondary WAN DNS IP address given by your Service Provider
Back	N/A	Click **Back** button to go to previous step
Next	N/A	Click **Next** button to go to next step

Physical Interface: Ethernet

WAN Type: PPP over Ethernet



WAN Interface (Step-4) {Ethernet - PPP over Ethernet}

- PPPoE Account
- PPPoE Password
- Primary DNS
- Secondary DNS (Optional)
- Service Name (Optional)
- Assigned IP Address (Optional)

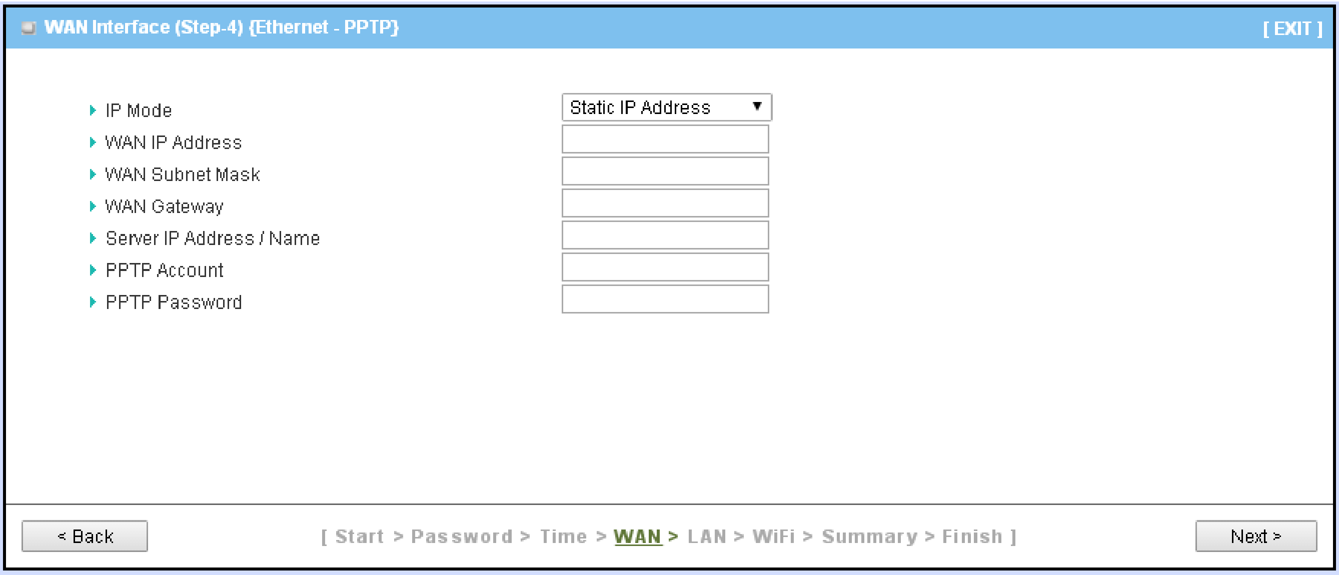
[EXIT]
< Back
[Start > Password > Time > WAN > LAN > WiFi > Summary > Finish]
Next >

PPPoE Settings 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	A Must filled setting	Enter the IP address of Primary DNS server.
Secondary DNS	Optional setting	Enter the IP address of Secondary DNS server.
Service Name	Optional setting	Enter the service name if your ISP requires it
Assigned IP Address	Optional setting	Enter the IP address assigned by your Service Provider.
Back	N/A	Click **Back** button to go to previous step
Next	N/A	Click **Next** button to go to next step

Index skipping is used to reserve slots for new function insertion, when required.

Physical Interface: Ethernet

WAN Type: PPTP



WAN Interface (Step-4) {Ethernet - PPTP}

- IP Mode: Static IP Address
- WAN IP Address
- WAN Subnet Mask
- WAN Gateway
- Server IP Address / Name
- PPTP Account
- PPTP Password

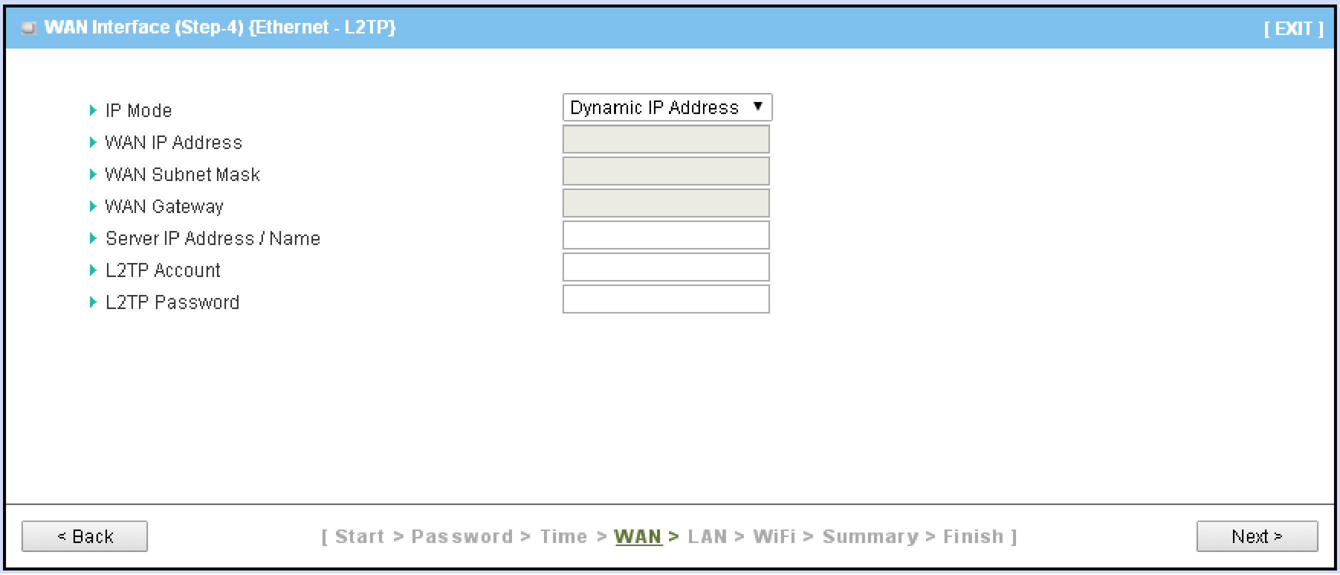
[EXIT]
< Back
[Start > Password > Time > WAN > LAN > WiFi > Summary > Finish]
Next >

PPTP Settings 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.
Back	N/A	Click **Back** button to go to previous step
Next	N/A	Click **Next** button to go to next step

Index skipping is used to reserve slots for new function insertion, when required.

Physical Interface: Ethernet

WAN Type: L2TP



WAN Interface (Step-4) {Ethernet - L2TP}

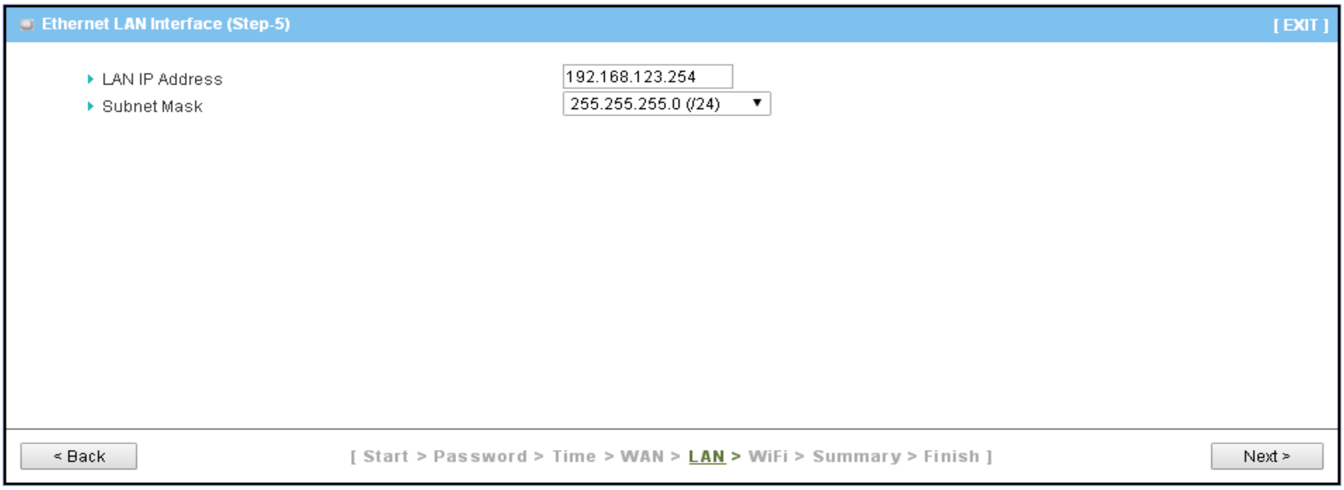
- IP Mode: Dynamic IP Address
- WAN IP Address
- WAN Subnet Mask
- WAN Gateway
- Server IP Address / Name
- L2TP Account
- L2TP Password

[EXIT]
< Back
[Start > Password > Time > WAN > LAN > WiFi > Summary > Finish]
Next >

L2TP Settings 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.
PPTP Account	A Must filled setting	Enter the L2TP username provided by your Service Provider.
PPTP Password	A Must filled setting	Enter the L2TP connection password provided by your Service Provider.
Back	N/A	Click **Back** button to go to previous step
Next	N/A	Click **Next** button to go to next step

Index skipping is used to reserve slots for new function insertion, when required.

In Ethernet LAN Interface (Step-5), configure the LAN IP Address and Subnet Mask of the device. The


Ethernet LAN Interface (Step-5)
[EXIT]
< Back
[Start > Password > Time > WAN > LAN > WiFi > Summary > Finish]
Next >

LAN IP Address 192.168.123.254

Subnet Mask 255.255.255.0 (/24)

Ethernet LAN Interface		
Item	**Value setting**	**Description**
LAN IP Address	A Must filled setting	Assign an **IP Address** for LAN, this IP address is a gateway IP.
Subnet Mask	By default **255.255.255.0/24** is selected.	Select a **Subnet Mask** for the default LAN, and it will be assigned to DHCP server to distribute IP address for client.
Back	N/A	Click **Back** button to go to previous step
Next	N/A	Click **Next** button to go to next step

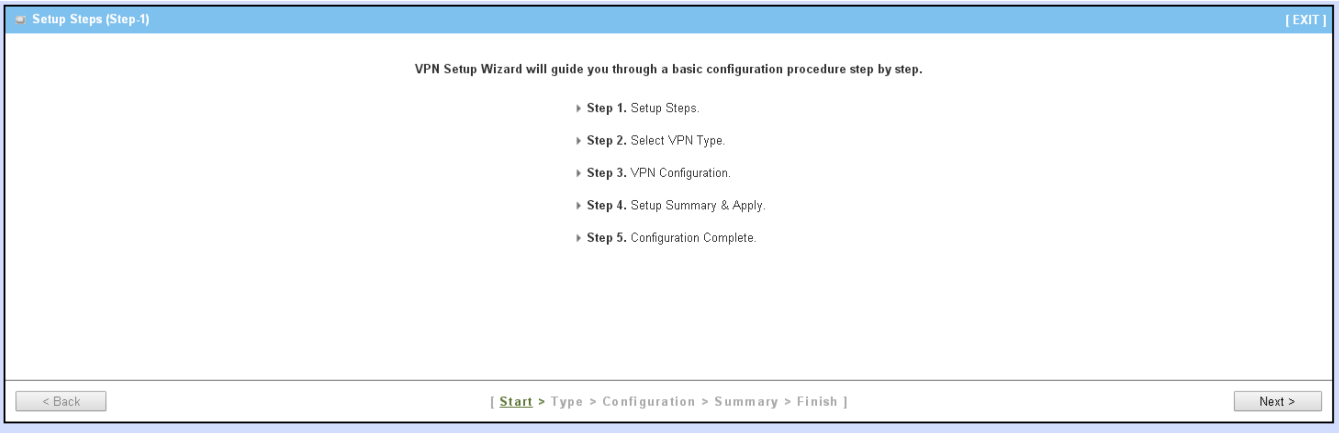
Index skipping is used to reserve slots for new function insertion, when required.

VPN Setup Wizard

VPN Wizard will step by step guide you through to complete VPN tunnel setup.

Step-1: Setup Steps

In Step-1, the VPN Setup Step is a screen that displays the summary of steps for VPN setup.
Click **Next** button to begin VPN setup.

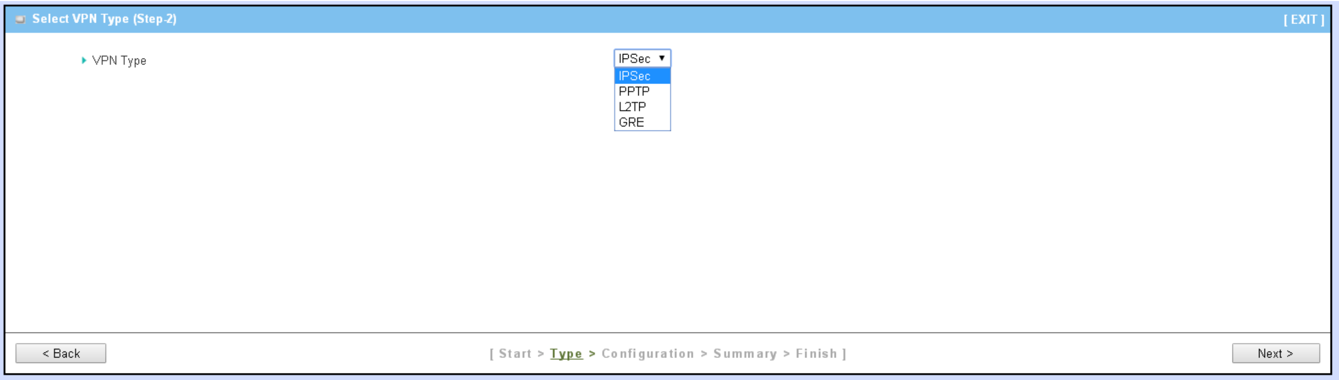


VPN Setup Wizard will guide you through a basic configuration procedure step by step.

- **Step 1.** Setup Steps.
- **Step 2.** Select VPN Type.
- **Step 3.** VPN Configuration.
- **Step 4.** Setup Summary & Apply.
- **Step 5.** Configuration Complete.

Step-2: Select VPN Type

From **VPN Type** dropdown box choose a VPN method to deploy.
Click the **Next** button to go to the next step.



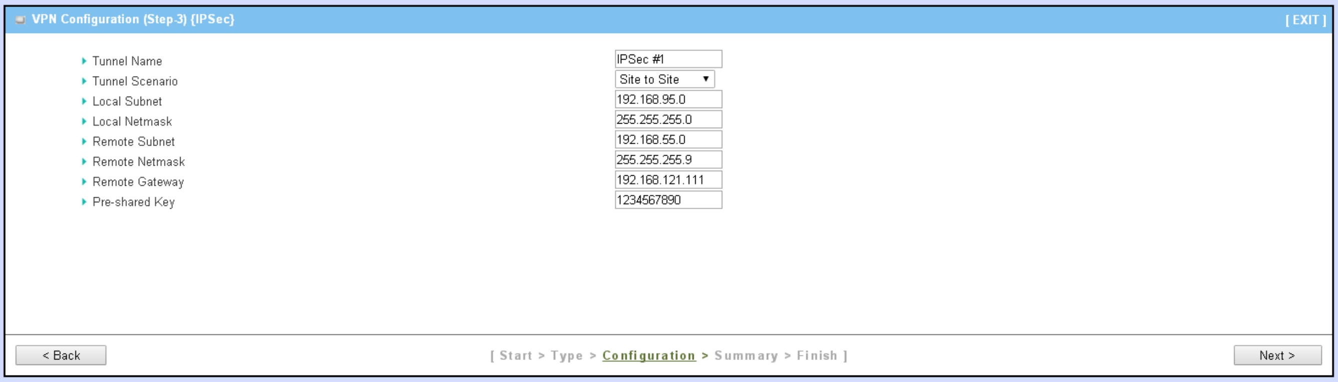
VPN Type: IPSec

Step-3: Sub-steps

When IPSec is selected, go to (Step-3) IPSec in the following page.
When PPTP is selected, go to (Step-3) PPTP in the following page.
When L2TP is selected, go to (Step-3) L2TP in the following page.
When GRE is selected, go to (Step-3) GRE in the following page.

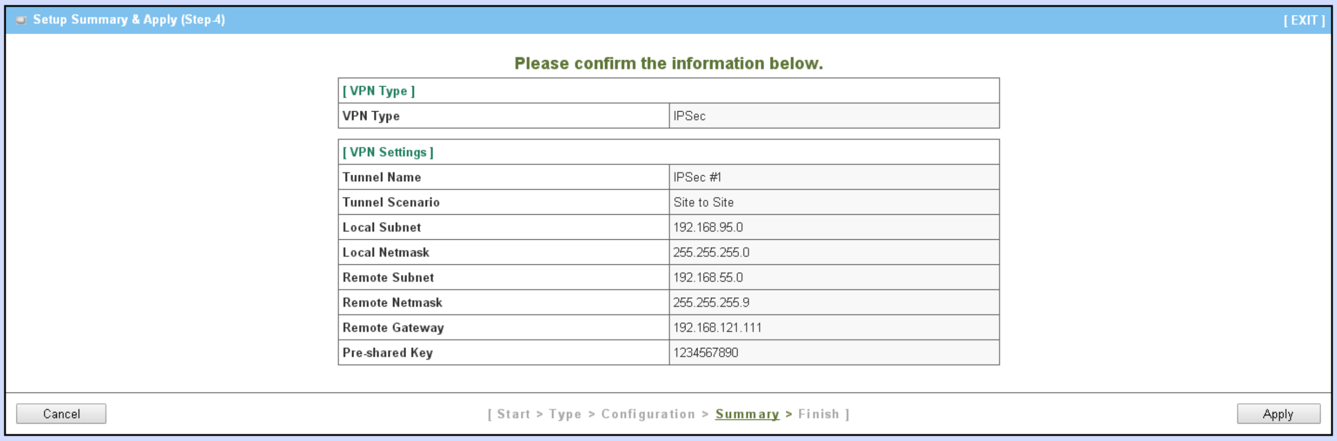
(Step-3) IPSec

When **IPSec** is selected in Step-2 for VPN Type, IPSec configuration window will appear.


VPN Configuration (Step-3) (IPSec)
[EXIT]
< Back
[Start > Type > Configuration > Summary > Finish]
Next >

Tunnel Name	IPSec #1
Tunnel Scenario	Site to Site
Local Subnet	192.168.95.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.55.0
Remote Netmask	255.255.255.9
Remote Gateway	192.168.121.111
Pre-shared Key	1234567890

When complete the IPSec configuration, click Next button, a setup summary will display.
Confirm the setting then click the Apply button to complete the setting.


Setup Summary & Apply (Step-4)
[EXIT]
Cancel
[Start > Type > Configuration > Summary > Finish]
Apply

Please confirm the information below.

[VPN Type]	
VPN Type	IPSec

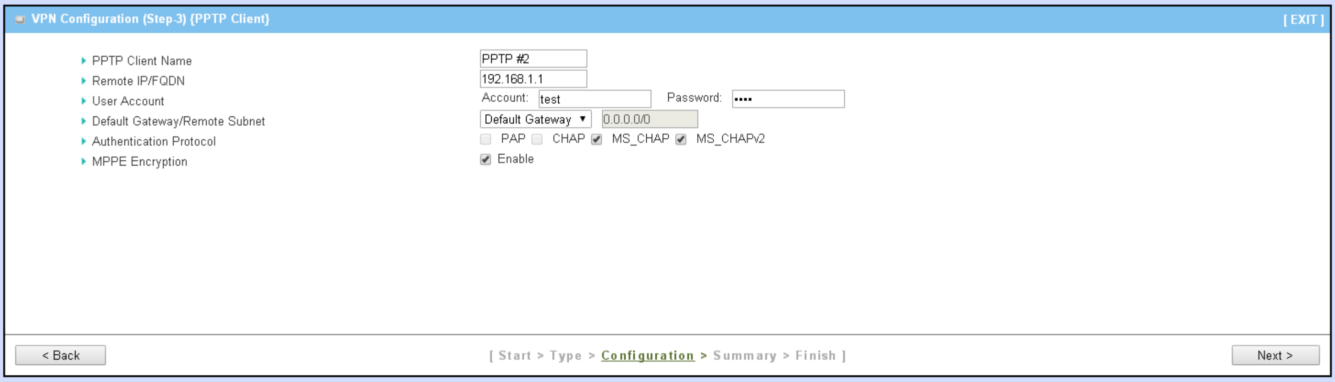
[VPN Settings]	
Tunnel Name	IPSec #1
Tunnel Scenario	Site to Site
Local Subnet	192.168.95.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.55.0
Remote Netmask	255.255.255.9
Remote Gateway	192.168.121.111
Pre-shared Key	1234567890

(Step-3) PPTP

When **PPTP** is selected in Step-2 for VPN Type and either PPTP client or server is selected the client or server configuration window will appear.

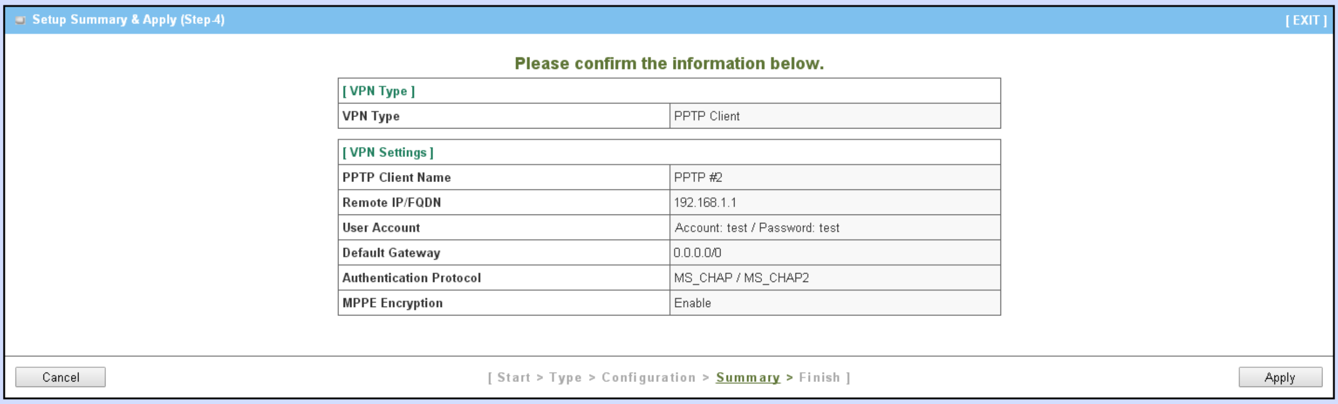
PPTP Client

When **PPTP Client** is selected in Step-2 for VPN Type, PPTP configuration window will appear.


VPN Configuration (Step-3) {PPTP Client}
[EXIT]
< Back
[Start > Type > Configuration > Summary > Finish]
Next >

- PPTP Client Name: PPTP #2
- Remote IP/FQDN: 192.168.1.1
- User Account: Account: test Password: ••••
- Default Gateway/Remote Subnet: Default Gateway ▾ 0.0.0.0/0
- Authentication Protocol: □ PAP □ CHAP ☑ MS_CHAP ☑ MS_CHAPv2
- MPPE Encryption: ☑ Enable

When complete the PPTP Client configuration, click Next button, a setup summary will display. Confirm the setting then click the Apply button to complete the setting.


Setup Summary & Apply (Step-4)
[EXIT]
Cancel
[Start > Type > Configuration > Summary > Finish]
Apply

Please confirm the information below.

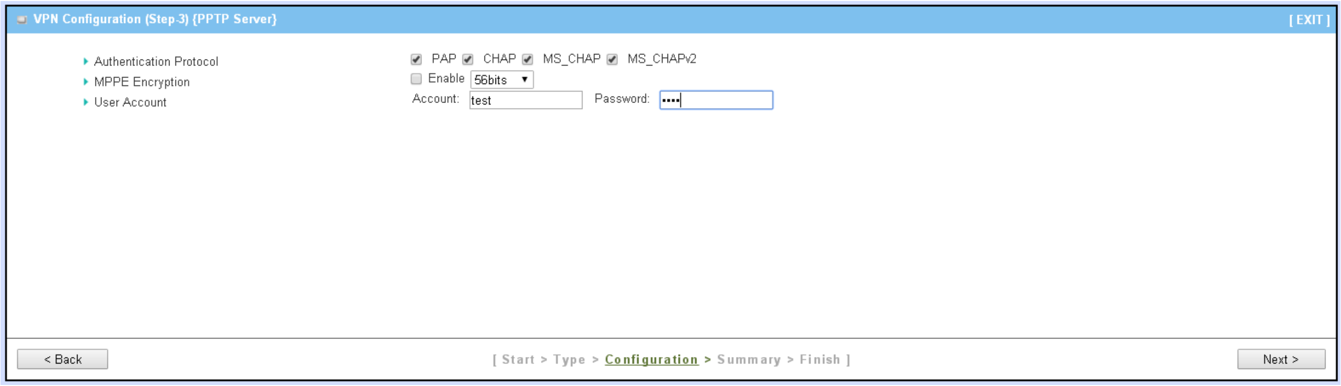
[VPN Type]	
VPN Type	PPTP Client

[VPN Settings]	
PPTP Client Name	PPTP #2
Remote IP/FQDN	192.168.1.1
User Account	Account: test / Password: test
Default Gateway	0.0.0.0/0
Authentication Protocol	MS_CHAP / MS_CHAP2
MPPE Encryption	Enable

Index skipping is used to reserve slots for new function insertion, when required.

PPTP Server

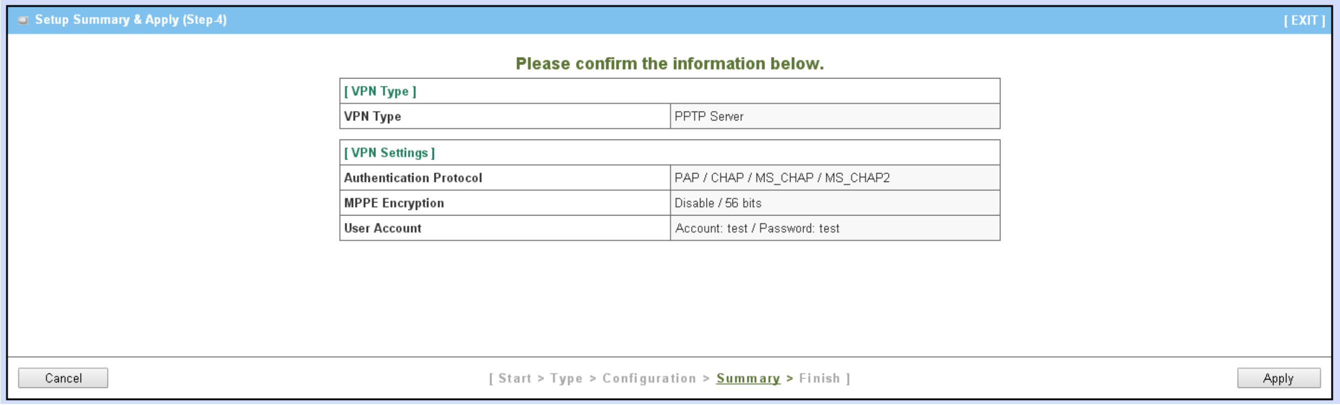
When **PPTP Server** is selected in Step-2 for VPN Type, PPTP configuration window will appear.



VPN Configuration (Step-3) (PPTP Server)

- Authentication Protocol: ☑ PAP ☑ CHAP ☑ MS_CHAP ☑ MS_CHAPv2
- MPPE Encryption: □ Enable 56bits ▾
- User Account: Account: test Password: ••••

When complete the PPTP Server configuration, click Next button, a setup summary will display. Confirm the setting then click the Apply button to complete the setting.



Setup Summary & Apply (Step-4)

Please confirm the information below.

[VPN Type]	
VPN Type	PPTP Server

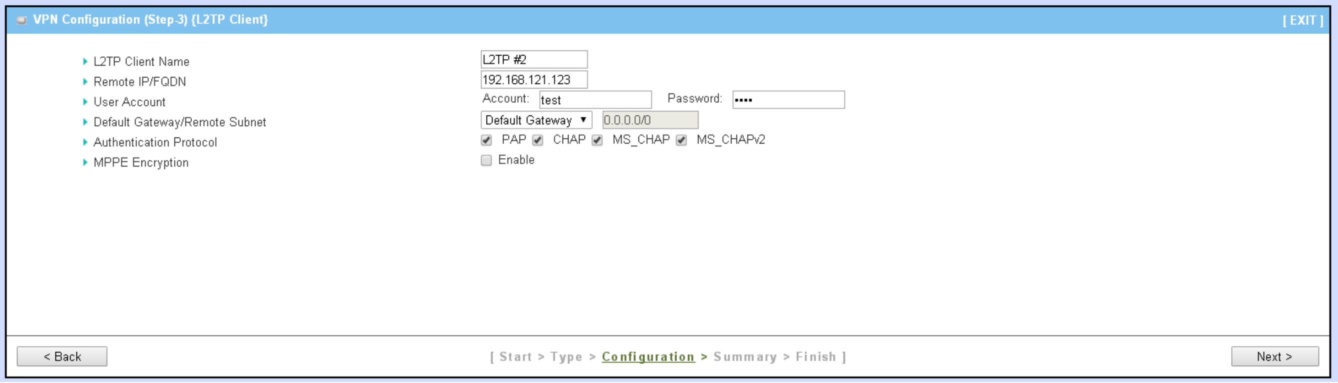
[VPN Settings]	
Authentication Protocol	PAP / CHAP / MS_CHAP / MS_CHAP2
MPPE Encryption	Disable / 56 bits
User Account	Account: test / Password: test

(Step-3) L2TP

When **L2TP** is selected in Step-2 for VPN Type and either L2TP client or server is selected the client or server configuration window will appear.

L2TP Client

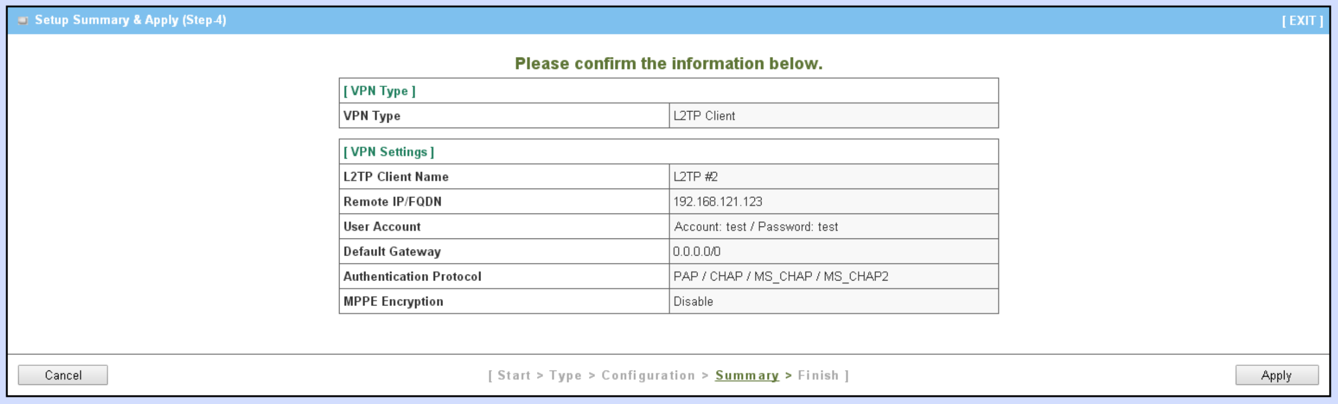
When **L2TP Client** is selected in Step-2 for VPN Type, L2TP configuration window will appear.



VPN Configuration (Step-3) {L2TP Client}

L2TP Client Name	L2TP #2
Remote IP/FQDN	192.168.121.123
User Account	Account: test Password: ••••
Default Gateway/Remote Subnet	Default Gateway ▾ 0.0.0.0/0
Authentication Protocol	☑ PAP ☑ CHAP ☑ MS_CHAP ☑ MS_CHAPv2
MPPE Encryption	□ Enable

When complete the L2TP Client configuration, click Next button, a setup summary will display. Confirm the setting then click the Apply button to complete the setting.



Setup Summary & Apply (Step-4)

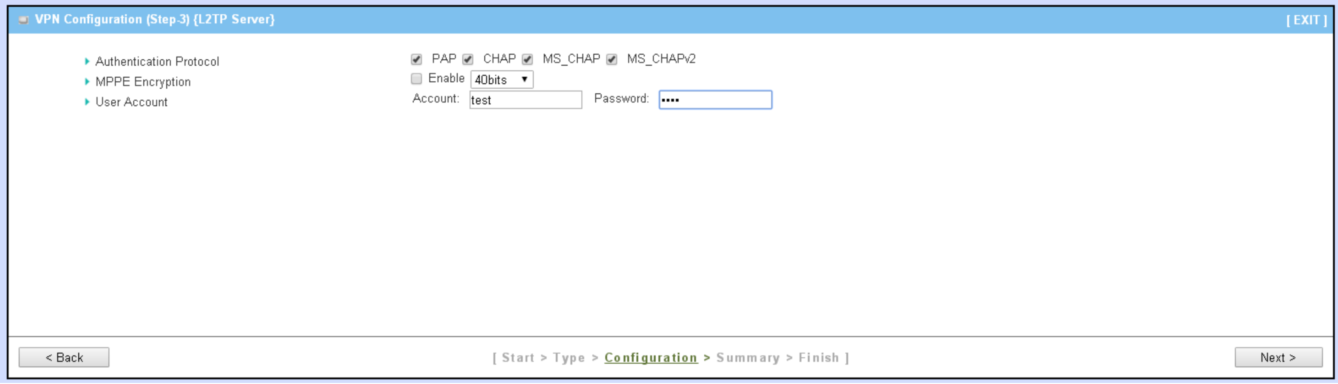
Please confirm the information below.

[VPN Type]	
VPN Type	L2TP Client

[VPN Settings]	
L2TP Client Name	L2TP #2
Remote IP/FQDN	192.168.121.123
User Account	Account: test / Password: test
Default Gateway	0.0.0.0/0
Authentication Protocol	PAP / CHAP / MS_CHAP / MS_CHAP2
MPPE Encryption	Disable

L2TP Server

When **L2TP Server** is selected in Step-2 for VPN Type, L2TP configuration window will appear.

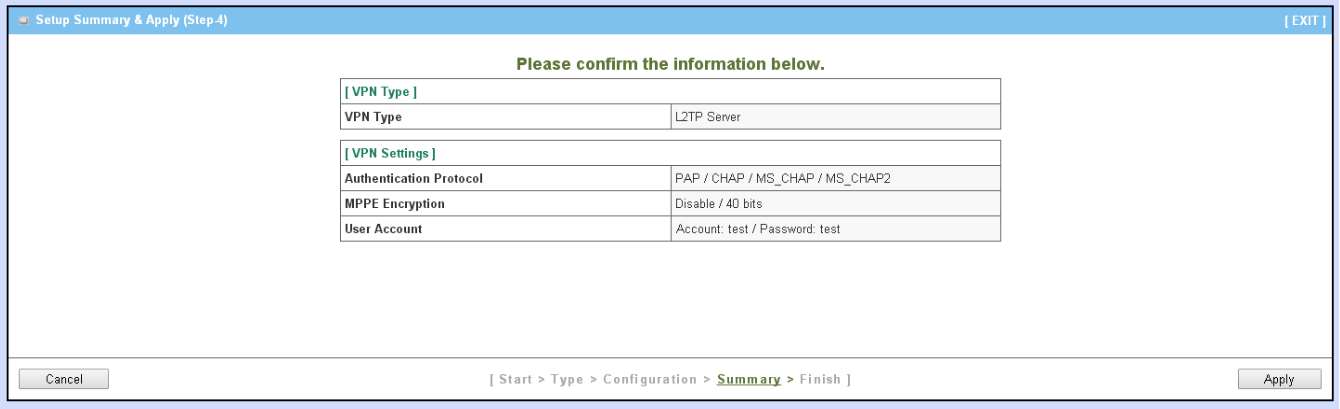


VPN Configuration (Step-3) {L2TP Server}

Authentication Protocol	☑ PAP ☑ CHAP ☑ MS_CHAP ☑ MS_CHAPv2
MPPE Encryption	□ Enable 40bits ▾
User Account	Account: test Password: ••••

When complete the L2TP Server configuration, click Next button, a setup summary will display. Confirm the setting then click the Apply button to complete the setting.

Index skipping is used to reserve slots for new function insertion, when required.


Setup Summary & Apply (Step-4)
[EXIT]
Cancel
[Start > Type > Configuration > Summary > Finish]
Apply

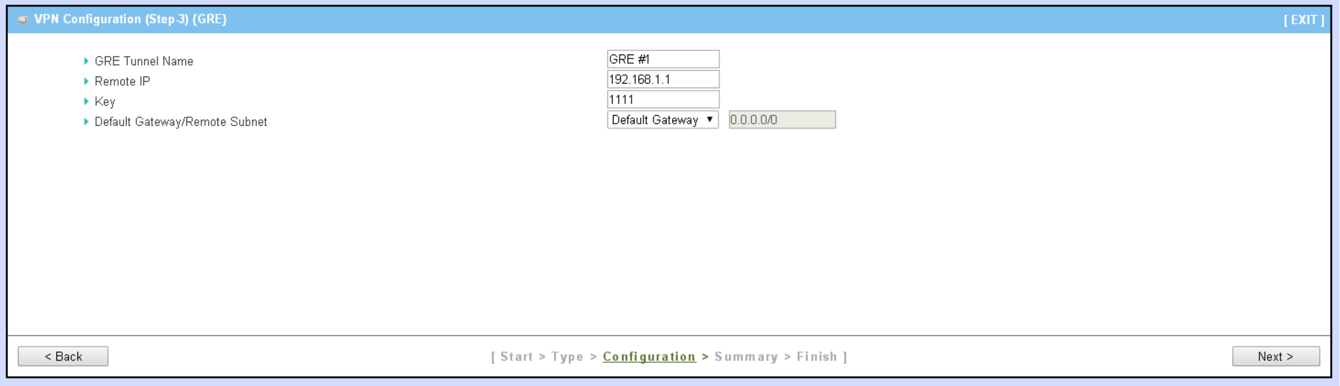
Please confirm the information below.

[VPN Type]	
VPN Type	L2TP Server

[VPN Settings]	
Authentication Protocol	PAP / CHAP / MS_CHAP / MS_CHAP2
MPPE Encryption	Disable / 40 bits
User Account	Account: test / Password: test

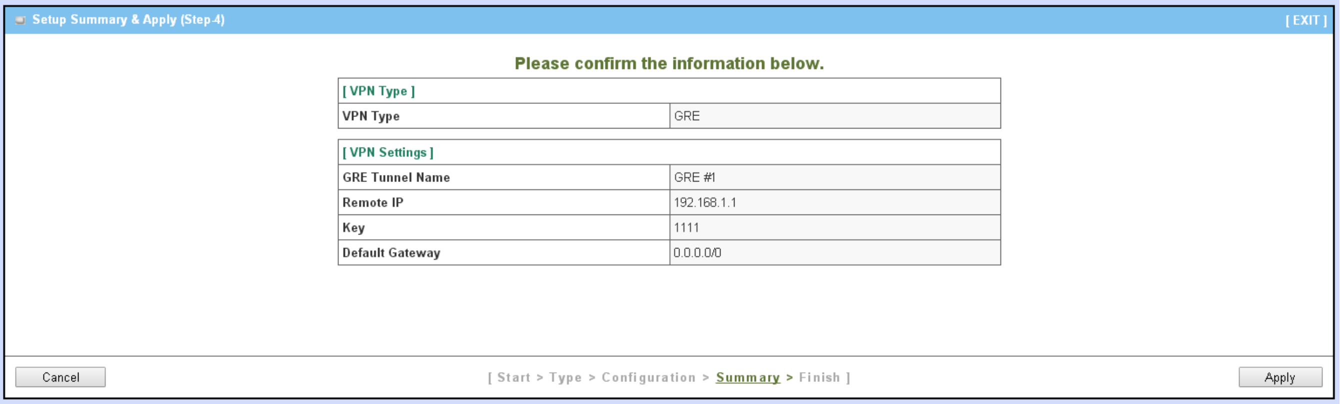
(Step-3) GRE

When **GRE** is selected in Step-2 for VPN Type, GRE configuration window will appear.


VPN Configuration (Step-3) (GRE)
[EXIT]
< Back
[Start > Type > Configuration > Summary > Finish]
Next >

GRE Tunnel Name	GRE #1
Remote IP	192.168.1.1
Key	1111
Default Gateway/Remote Subnet	Default Gateway ▾ 0.0.0.0/0

When complete the GRE configuration, click Next button, a setup summary will display. Confirm the setting then click the Apply button to complete the setting.


Setup Summary & Apply (Step-4)
[EXIT]
Cancel
[Start > Type > Configuration > Summary > Finish]
Apply

Please confirm the information below.

[VPN Type]	
VPN Type	GRE

[VPN Settings]	
GRE Tunnel Name	GRE #1
Remote IP	192.168.1.1
Key	1111
Default Gateway	0.0.0.0/0

2.3 Status

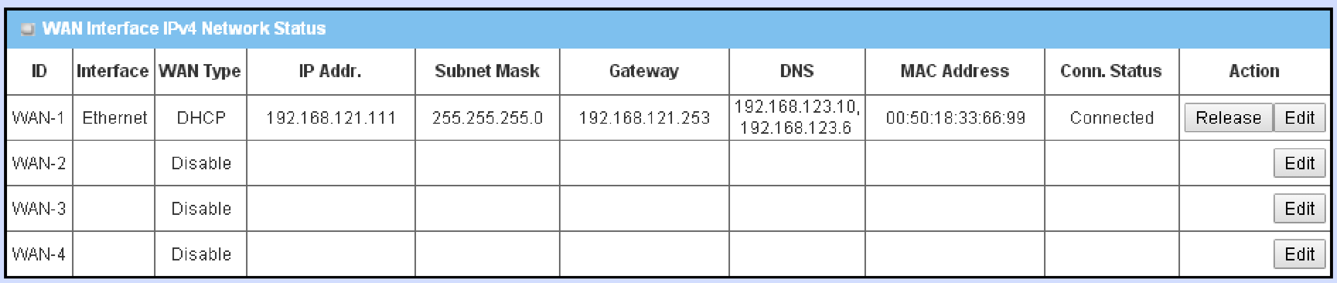
2.3.3 Network Status

The Network 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 > Network Status

WAN interface IPv4 Network Status

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



WAN Interface IPv4 Network Status

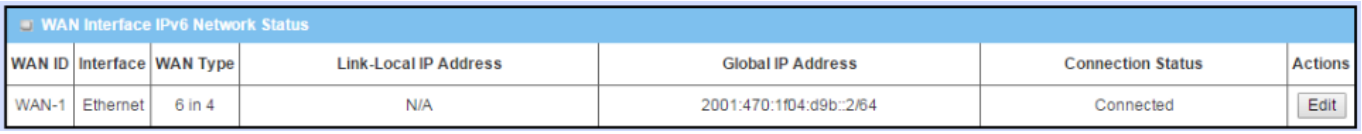
ID	Interface	WAN Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Action
WAN-1	Ethernet	DHCP	192.168.121.111	255.255.255.0	192.168.121.253	192.168.123.10, 192.168.123.6	00:50:18:33:66:99	Connected	Release Edit
WAN-2		Disable							Edit
WAN-3		Disable							Edit
WAN-4		Disable							Edit

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 unconfigured.
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 unconfigured.
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 unconfigured.
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 unconfigured.
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 > 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 > 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

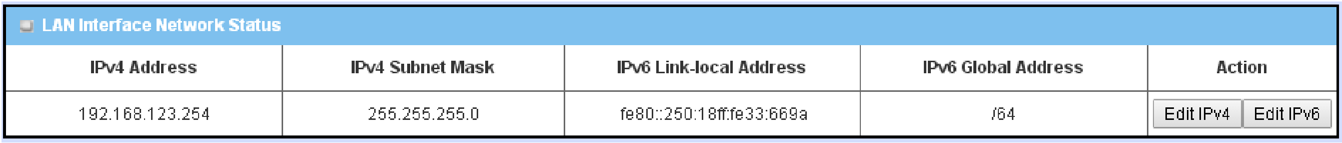
WAN ID	Interface	WAN Type	Link-Local IP Address	Global IP Address	Connection Status	Actions
WAN-1	Ethernet	6 in 4	N/A	2001:470:1f04:d9b::2/64	Connected	Edit

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.)

Index skipping is used to reserve slots for new function insertion, when required.

LAN Interface Network Status

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



LAN Interface Network Status

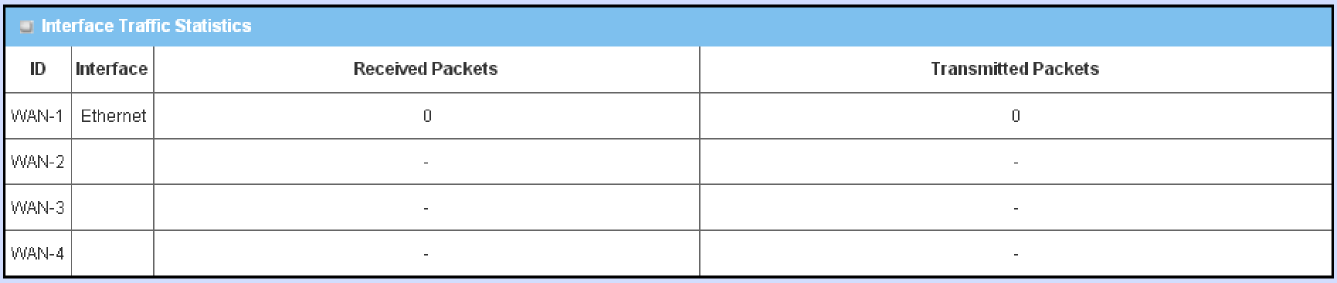
IPv4 Address	IPv4 Subnet Mask	IPv6 Link-local Address	IPv6 Global Address	Action
192.168.123.254	255.255.255.0	fe80::250:18ff:fe33:669a	/64	Edit IPv4 Edit IPv6

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 Address	N/A	It displays the current LAN IPv6 Link-Local address. This is also the IPv6 IP Address user use to access Router's Web-based Utility.
IPv6 Global Address	N/A	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.)

Index skipping is used to reserve slots for new function insertion, when required.

Interface Traffic Statistics

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



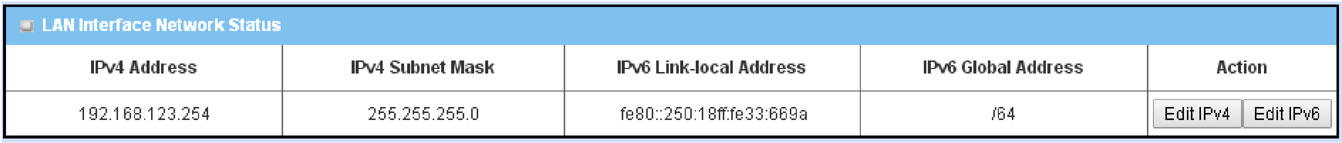
Interface Traffic Statistics

ID	Interface	Received Packets	Transmitted Packets
WAN-1	Ethernet	0	0
WAN-2		-	-
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.

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
192.168.123.254	255.255.255.0	fe80::250:18ff:fe33:669a	/64	Edit IPv4 Edit IPv6

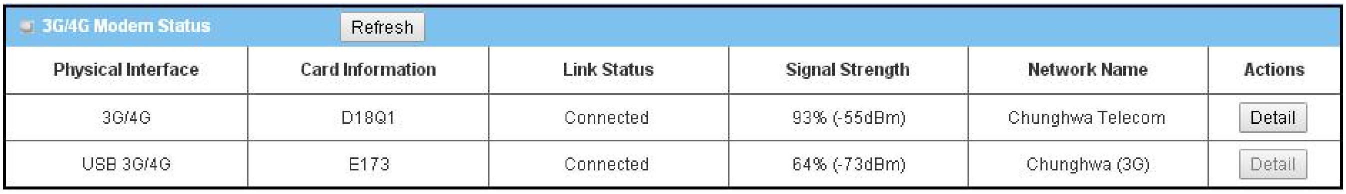
LAN Interface Network Status		
Item	**Value setting**	**Description**
IPv4 Address	N/A	It displays the current IPv4 IP Address of the gateway This is also the IP Address user use to access Router's Web-based Utility.
IPv4 Subnet Mask	N/A	It displays the current mask of the subnet.
IPv6 Link-local Address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

The Network 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 > Network Status

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



3G/4G Modem Status Refresh

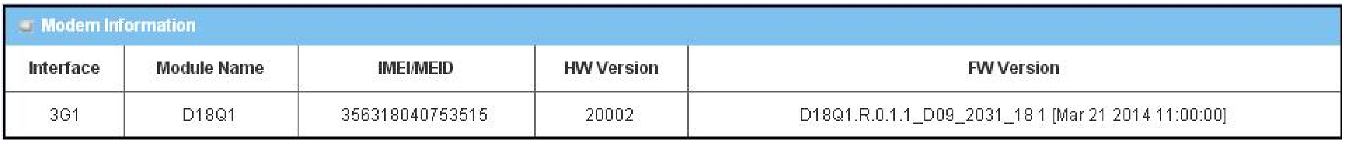
Physical Interface	Card Information	Link Status	Signal Strength	Network Name	Actions
3G/4G	D18Q1	Connected	93% (-55dBm)	Chunghwa Telecom	Detail
USB 3G/4G	E173	Connected	64% (-73dBm)	Chunghwa (3G)	Detail

3G/4G Modem Status		
Item	**Value setting**	**Description**
Physical Interface	N/A	It displays the type of WAN physical interface. Depending on the model 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 th Detail button in the Action column is pressed, 3G/4G modem information windows such as Modem Information, SIM Status, and Service Information will appear. These windows are explained below.

Index skipping is used to reserve slots for new function insertion, when required.

Show Modem Information (Detail Button)

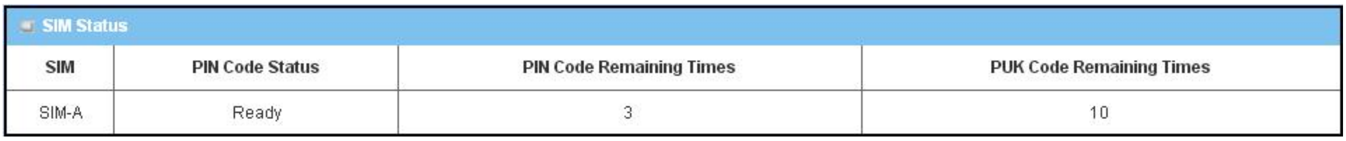


Modem Information

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. It can be 3G1 or 3G2. Note: 3G2 is only for devices that support dual modules.
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.

Show SIM Status



SIM Status

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

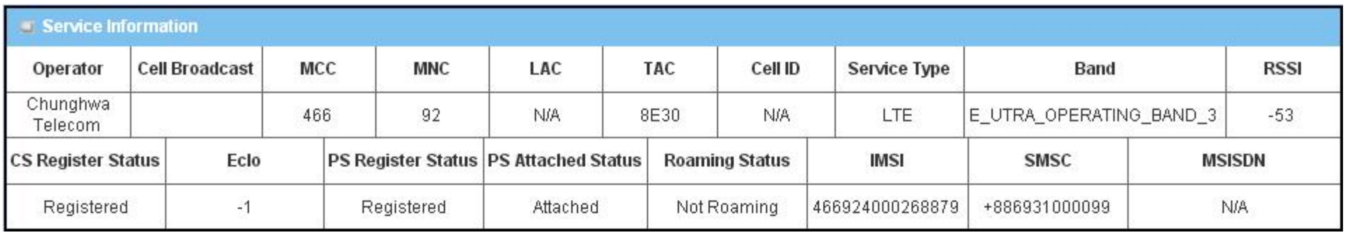
SIM Status (after Detail button)

Item	Value setting	Description
SIM	N/A	It displays the operating SIM card. The display can be SIM-A or SIM-B. Note: In some AMIT’s products, the device supports one SIM slot and only SIM-A is available.
PIN Code Status	N/A	It displays the stutus of whether the SIM is requied 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 Times	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 been exhused 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 exhused 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 > Internet Setup > Connection with SIM-A Card.

Index skipping is used to reserve slots for new function insertion, when required.

Show 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

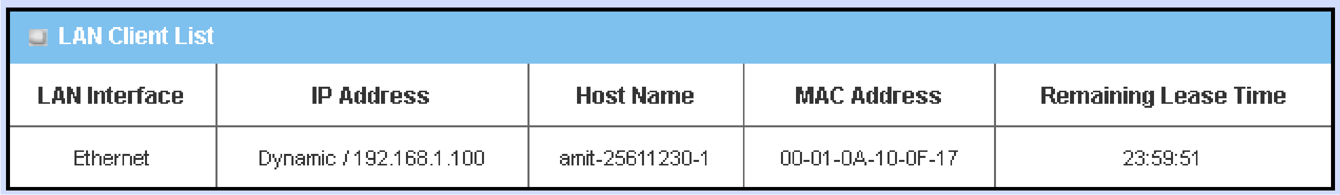
CS Register Status	EcIo	PS Register Status	PS Attached Status	Roaming Status	IMSI	SMSC	MSISDN
Registered	-1	Registered	Attached	Not Roaming	466924000268879	+886931000099	N/A

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.

2.3.7 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.

Go to **Status** > **LAN Client List**



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.

2.3.9 Firewall Status

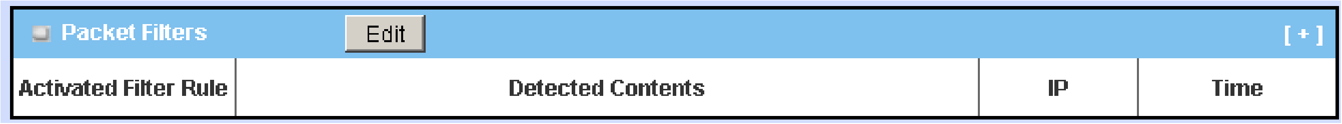
The Firewall Status Viewer provides user a quick view of the firewall status and current firewall settings. The Firewall Status Viewer also keeps the log history of the dropped packets by the firewall rule policies. It also includes the administrator remote login settings specified in the Firewall Options. Before Status Viewer can log history ensure to enable Log Alert box for each of the Filter specified under Advanced Network > Firewall

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.

From the menu on the left, select Status > Firewall Status > Firewall Status Tab

Packet Filter Status

.



Activated Filter Rule	Detected Contents	IP	Time

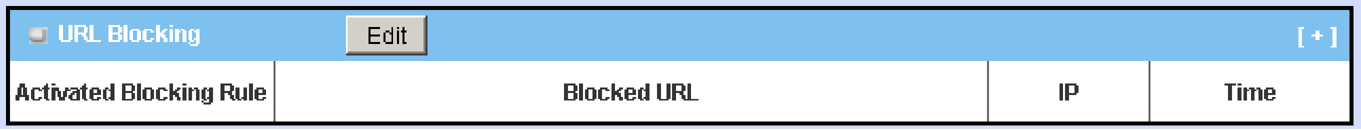
Packet Filter Status		
Item	**Value setting**	**Description**
Activated Filter Rule	N/A	This is the Packet Filter Rule name.
Detected Contents	N/A	This is the logged packet information, including the source IP, destination IP, protocol, and destination port –the TCP or UDP. String format: Source IP to 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":"Minues":"Seconds")

Note: Ensure Packet Filter Log Alert is enabled.

Refer to Advanced Network > Firewall > Packet Filters tab. Check Log Alert and save the setting

Index skipping is used to reserve slots for new function insertion, when required.

URL Blocking Status



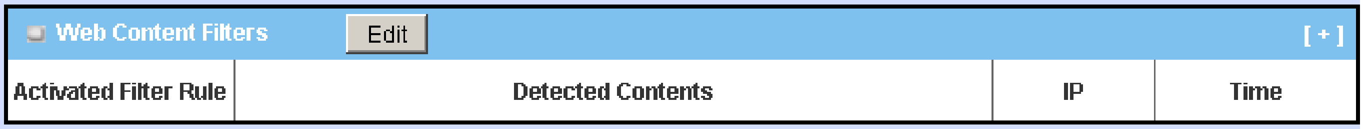
Activated Blocking Rule	Blocked URL	IP	Time

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":"Minues":"Seconds")

Note: Ensure URL Blocking Log Alert is enabled.

Refer to Advanced Network > Firewall > URL Blocking tab. Check Log Alert and save the setting.

Web Content Filter Status



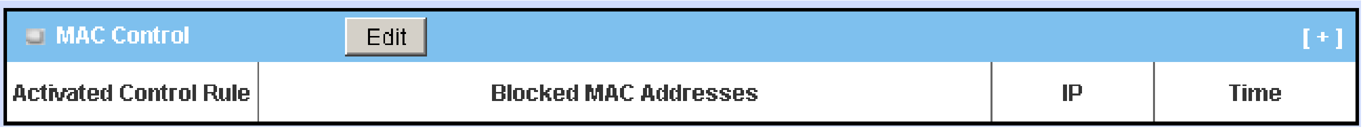
Activated Filter Rule	Detected Contents	IP	Time

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. Datetime format ("Month" "Day" "Hours":"Minues":"Seconds")

Note: Ensure Web Content Filter Log Alert is enabled.

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

MAC Control Status

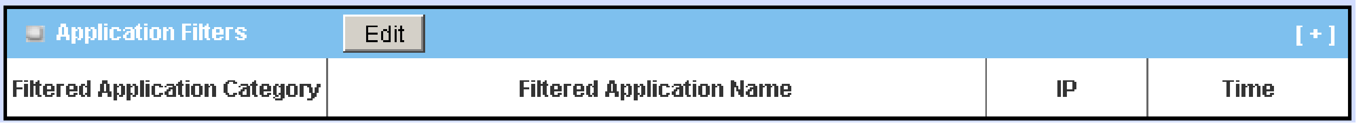


Activated Control Rule	Blocked MAC Addresses	IP	Time

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":"Minues":"Seconds")

Note: Ensure MAC Control Log Alert is enabled.
Refer to Advanced Network > Firewall > MAC Control tab. Check Log Alert and save the setting.

Plication Filters Status



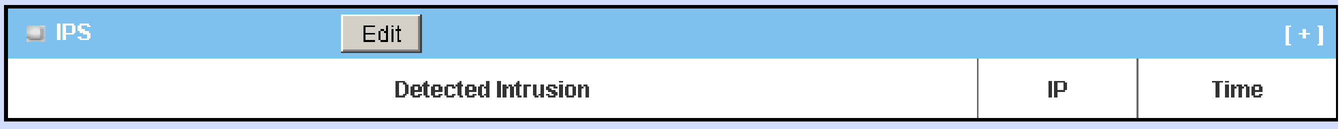
Filtered Application Category	Filtered Application Name	IP	Time

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":"Minues":"Seconds")

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

Index skipping is used to reserve slots for new function insertion, when required.

IPS Firewall Status



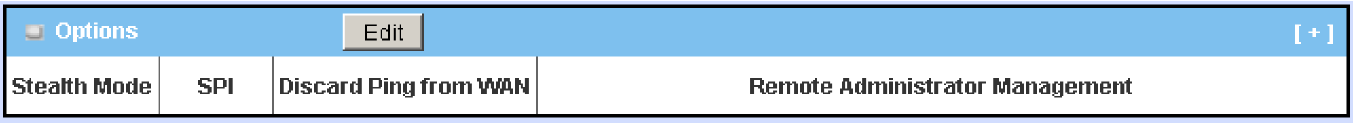
Detected Intrusion	IP	Time

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":"Minues":"Seconds")

Note: Ensure IPS Log Alert is enabled.

Refer to Advanced Network > 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. Formate: IP : "Source IP", User Name: "Login User Name", Time: "Datetime" 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 Advanced Network > Firewall > Options tab.Check Log Alert and save the setting.

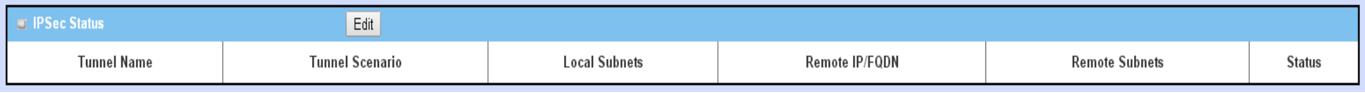
2.3.b VPN Status

The VPN Status widow shows the overall VPN tunnel status.

From the menu on the left, select Status > VPN Status

IPSec Status

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



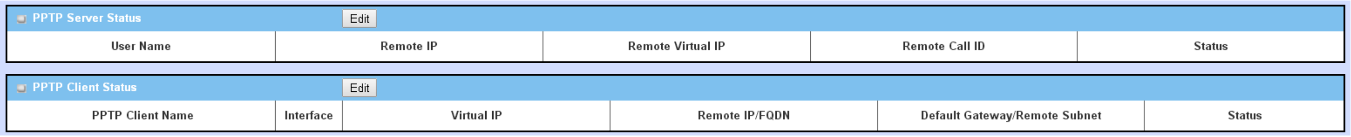
Tunnel Name	Tunnel Scenario	Local Subnets	Remote IP/FQDN	Remote Subnets	Status

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 Subnets	N/A	It displays the Remote Subnets specified.
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. (Advanced Network > VPN > IPSec tab)

Index skipping is used to reserve slots for new function insertion, when required.

PPTP Server/Client Status

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



PPTP Server Status

User Name	Remote IP	Remote Virtual IP	Remote Call ID	Status

PPTP Client Status

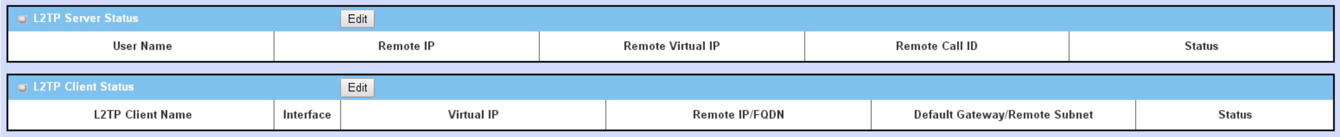
PPTP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Status

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.
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. (Advanced Network > VPN > PPTP tab)

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 the 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.
Status	N/A	It displays the Status of the VPN connection. The status displays Connected, Disconnect, 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. (Advanced Network > VPN > PPTP tab)

L2TP Server/Client Status

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



L2TP Server Status Edit

User Name	Remote IP	Remote Virtual IP	Remote Call ID	Status

L2TP Client Status Edit

L2TP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	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.
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. (Advanced Network > VPN > L2TP tab)

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 the 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.
Status	N/A	It displays the Status of the VPN connection. The status displays Connected, Disconnect, 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. (Advanced Network > VPN > L2TP tab)

Index skipping is used to reserve slots for new function insertion, when required.

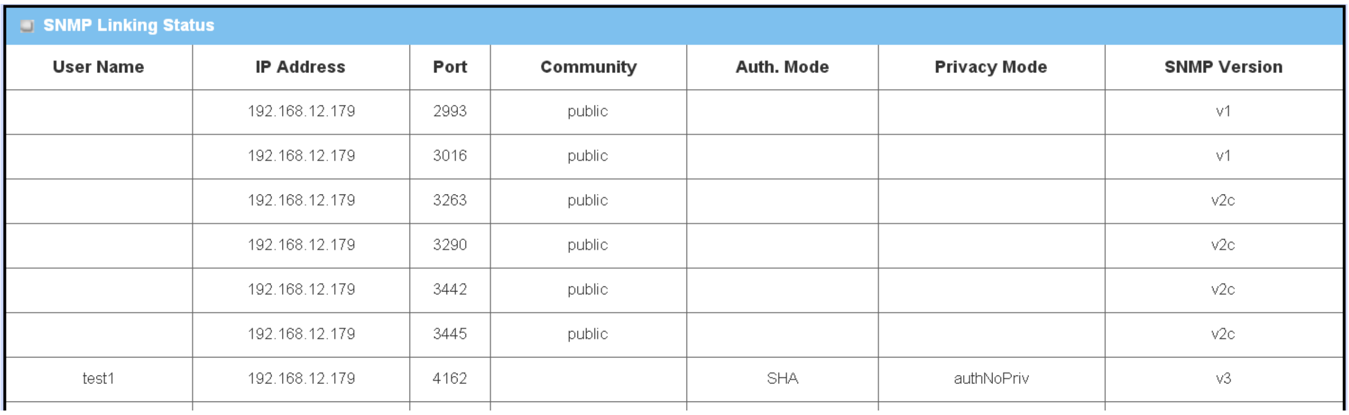
2.3.d System Mgmt. Status

The System Management 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 > System Mgmt. Status

SNMP Linking Status

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



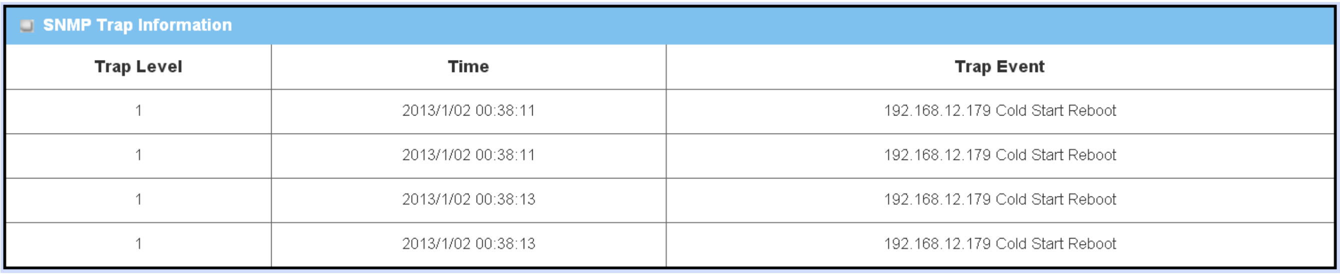
SNMP Linking Status

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

Show the status of current received SNMP traps.



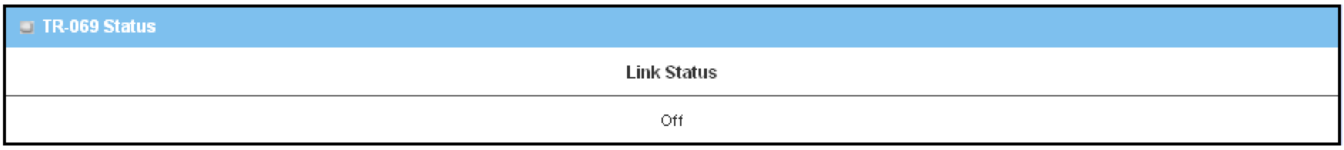
SNMP Trap Information

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

The TR-069 Status window 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.

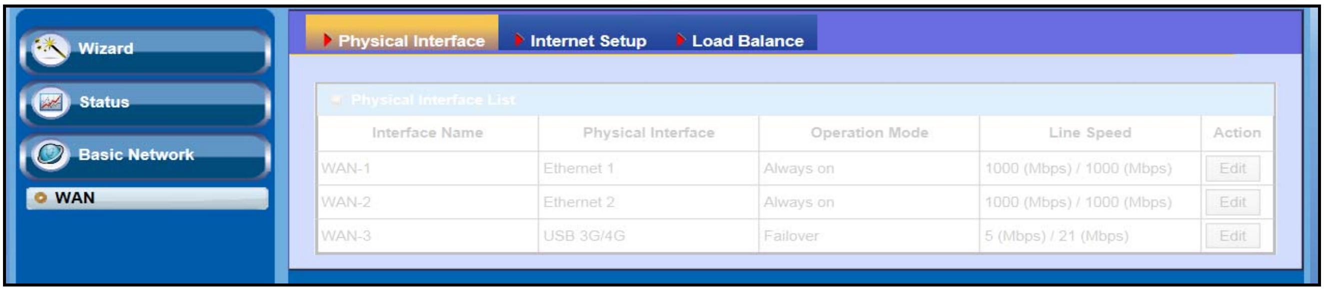
Chapter 3 Basic Network

3.1 WAN

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

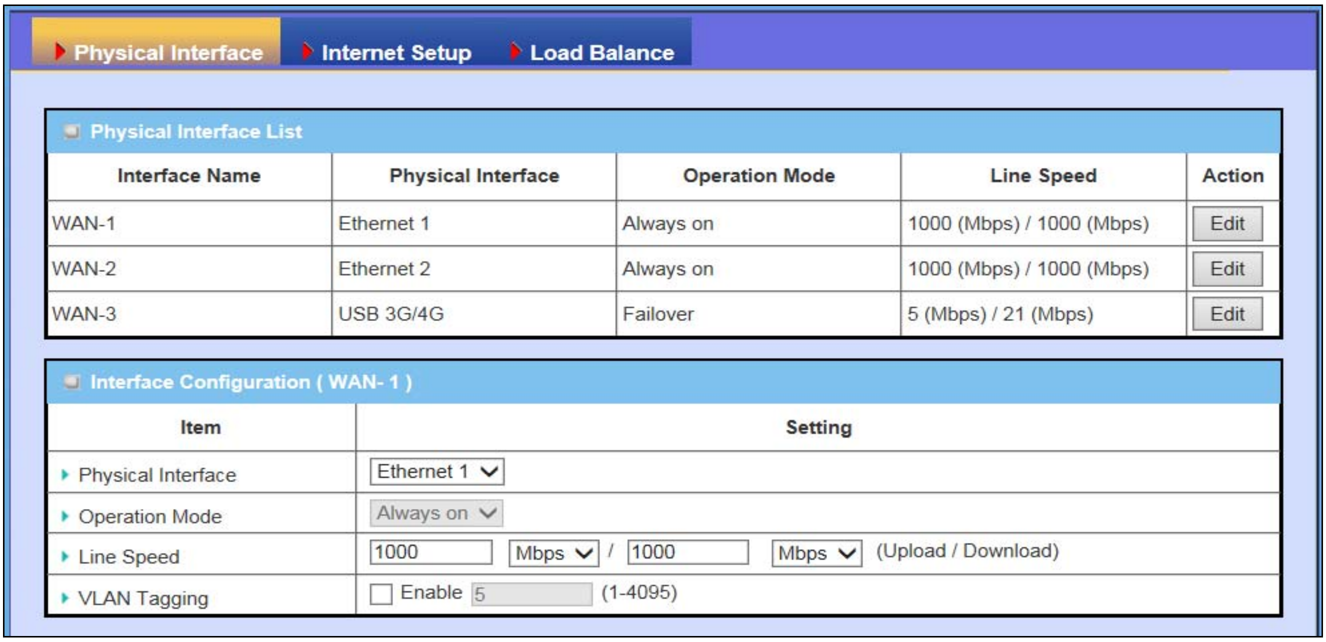
Interface Name	Physical Interface	Operation Mode	Line Speed	Action
WAN-1	Ethernet 1	Always on	1000 (Mbps) / 1000 (Mbps)	Edit
WAN-2	Ethernet 2	Always on	1000 (Mbps) / 1000 (Mbps)	Edit
WAN-3	USB 3G/4G	Failover	5 (Mbps) / 21 (Mbps)	Edit

Index skipping is used to reserve slots for new function insertion, when required.

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 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

Interface Configuration (WAN- 1)

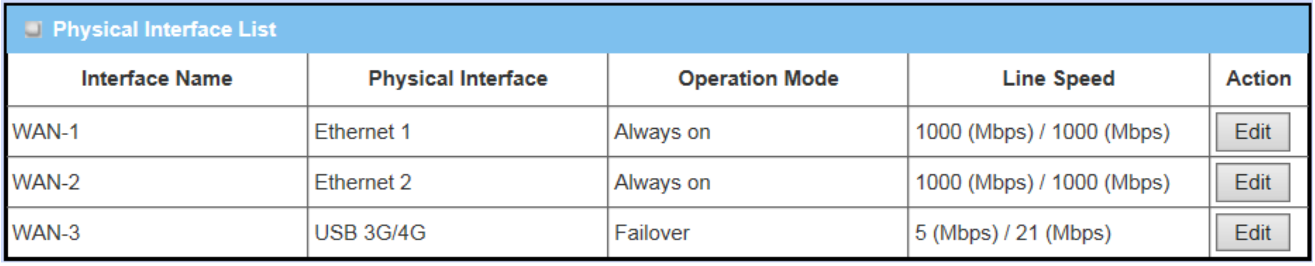
Item	Setting
Physical Interface	Ethernet 1
Operation Mode	Always on
Line Speed	1000 Mbps / 1000 Mbps (Upload / Download)
VLAN Tagging	□ Enable 5 (1-4095)

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.

Index skipping is used to reserve slots for new function insertion, when required.

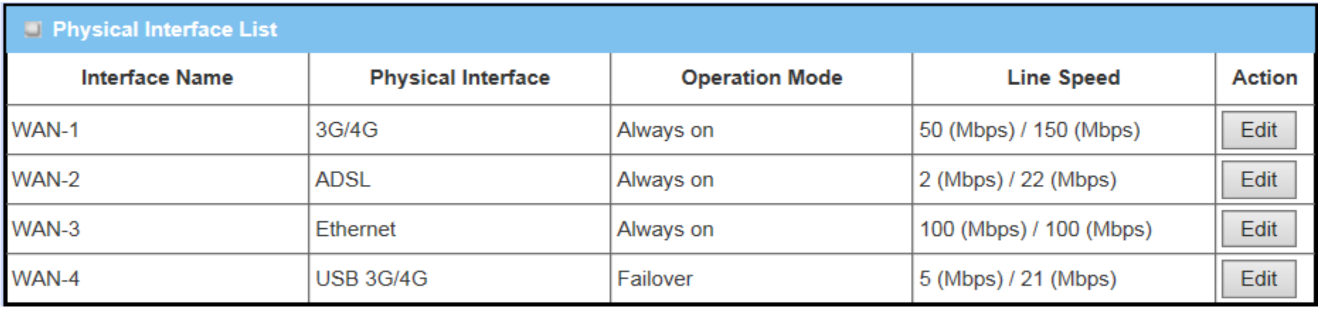
An example of a SDE852AM-00001 device



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

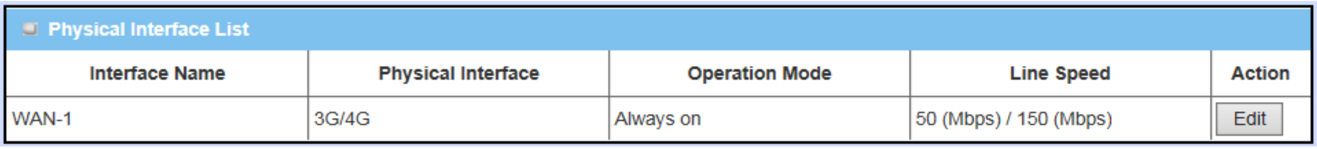
An example of an IOG761AM-0TDA1 device



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

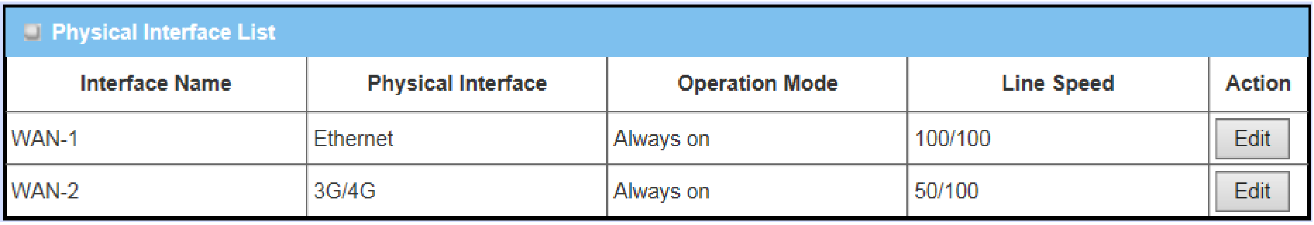
An example of an ODG761AM-0T1 device



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 an 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 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 AMIT Product List in Appendix A for number of interfaces, the type of physical interface and suggested logic WAN name in the device,

Index skipping is used to reserve slots for new function insertion, when required.

- **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**

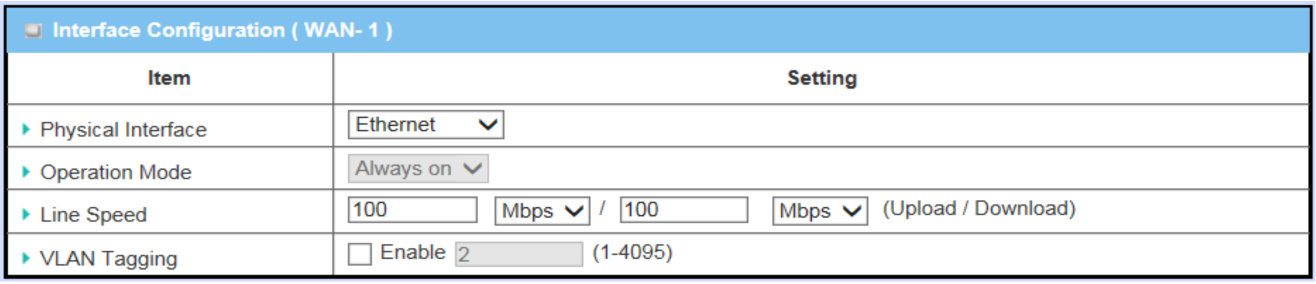
Specify the correct line speed (bandwidth) of uploading and downloading for each WAN interface allow the device to operate its QoS&BWM and WAN Load Balance functions normally. It is necessary to configure the parameters if you want to use QoS&BWM and WAN Load Balance functions on the gateway device.

- **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.

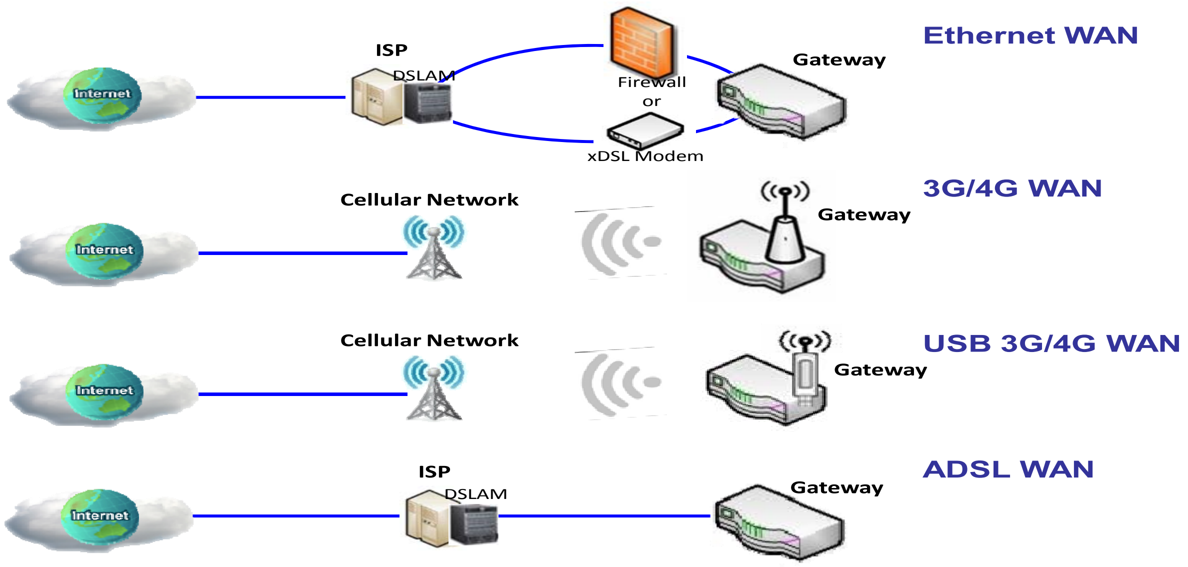
- **Physical Interface**

AMIT gateway supports Ethernet, 3G/4G, USB 3G/4G and ADSL physical interfaces. The kinds of physical interface in the device depend on the specification of gateway product purchased.

Following are some physical interface configuration examples and their illustration diagram. 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".

Index skipping is used to reserve slots for new function insertion, when required.

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.

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

USB 3G/4G WAN: The gateway has one USB port that can support 3G/4G USB modem[7] for a WAN connection. Please plug 3G/LTE 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 keep 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.

[7] Please refer to compatibility list to check which 3G or LTE dongles are supported by this device.

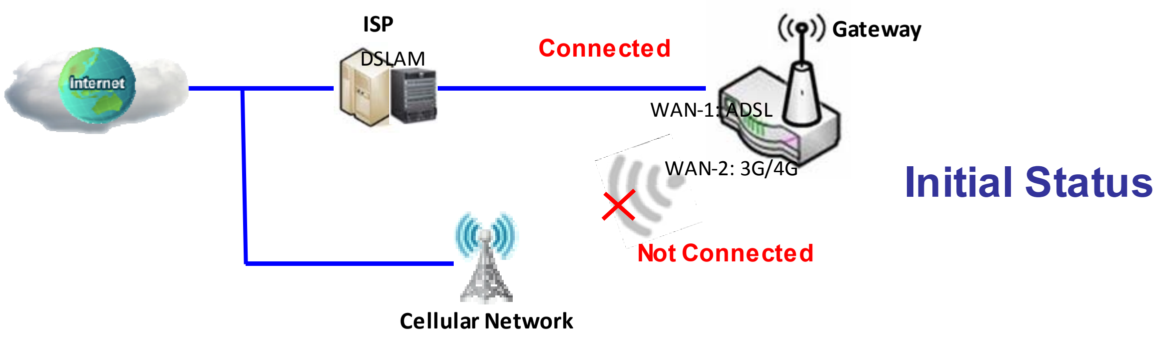
Configuration Path	[Physical Interface]-[Interface Configuration (WAN-n)], n=1, 2	
Interface Name	WAN-1	WAN-2
Physical Interface	***ADSL***	***USB 3G/4G***
Operation Mode	***Always on***	***Failover WAN-1 □Seamless***
Line Speed	***2Mbps / 22Mbps***	***5Mbps / 21Mbps***

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:

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

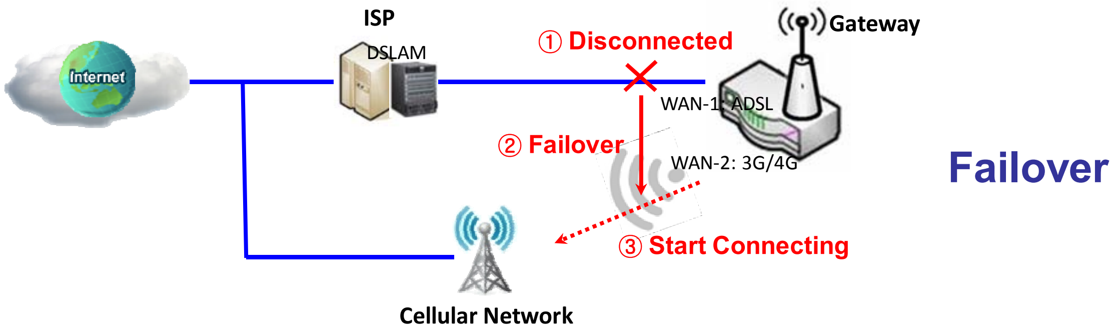
S 2: System starts the failover process.

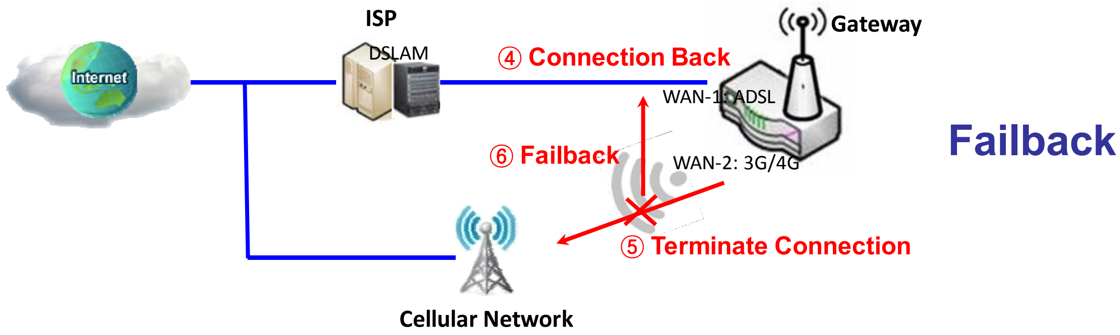
S 3: System tries to create the WAN connection by using Failover WAN interface, and use it for incoming data transmitting mission.

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 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.





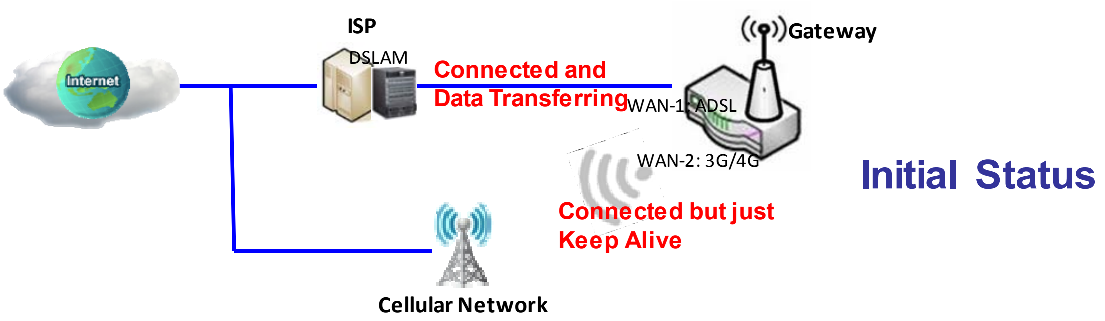
➢ **Seamless Failover Scenario:**

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. For some mission-critical applications, this gateway supports "Seamless Failover"[8] to shorten switch time during WAN interface failover process.

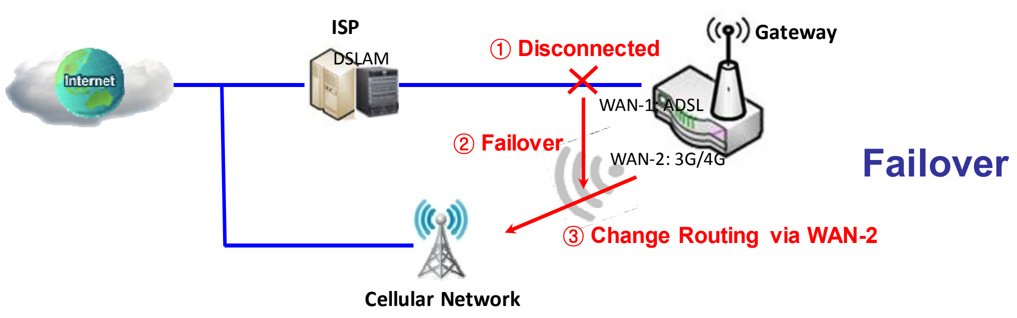
So, the initial status of two WAN connections for Seamless Failover is shown in following diagram.

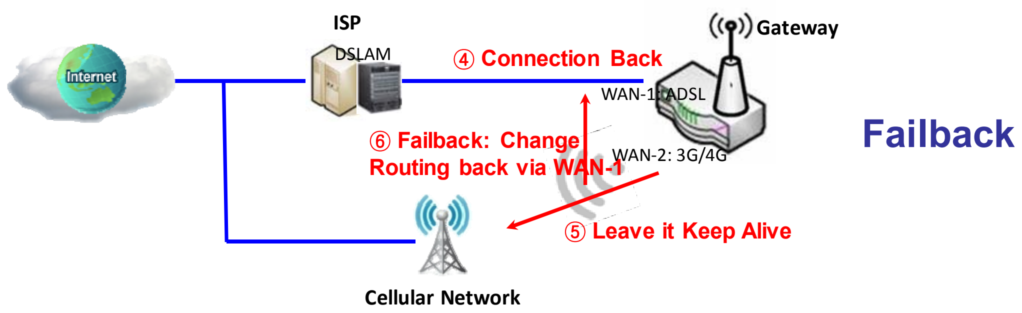


Next, Failover and Failback processes are shown in following diagram. Their steps are:

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.

Index skipping is used to reserve slots for new function insertion, when required.





- **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.

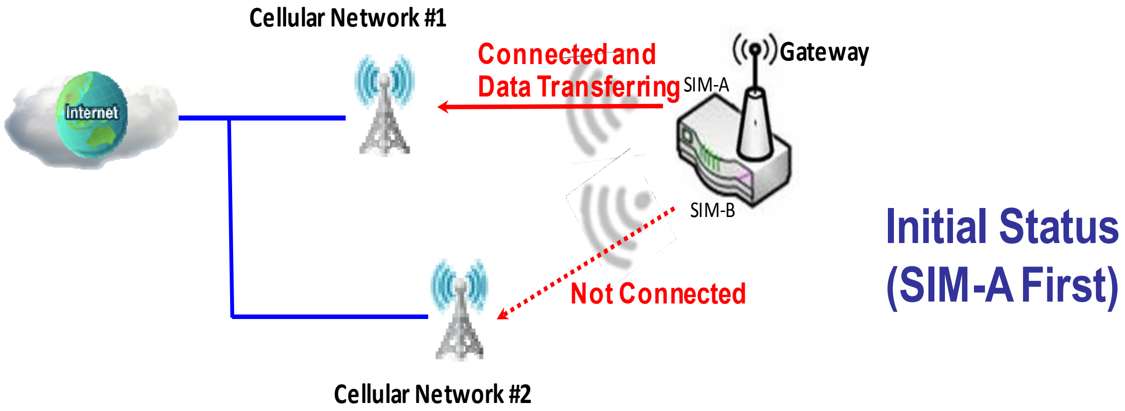
Index skipping is used to reserve slots for new function insertion, when required.

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:

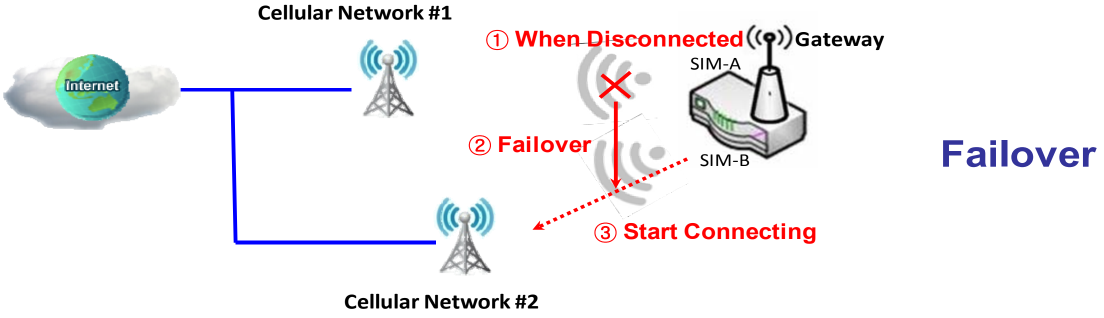
Pre-state: System tries to connect to mobile system for an Internet connection by using connection profile in SIM-A (for SIM-A First scenario) after system rebooting. If the connection is successful, data transfer from Intranet to Internet will be executed in this WAN connection. Call the connection 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'.

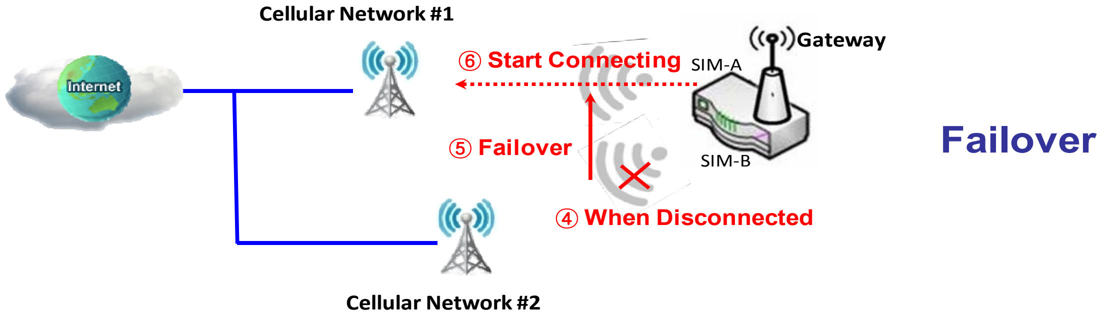
S 1: When system discovers the SIM-m connection is failed, system starts the failover process.

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'.

Index skipping is used to reserve slots for new function insertion, when required.

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&BWM 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.

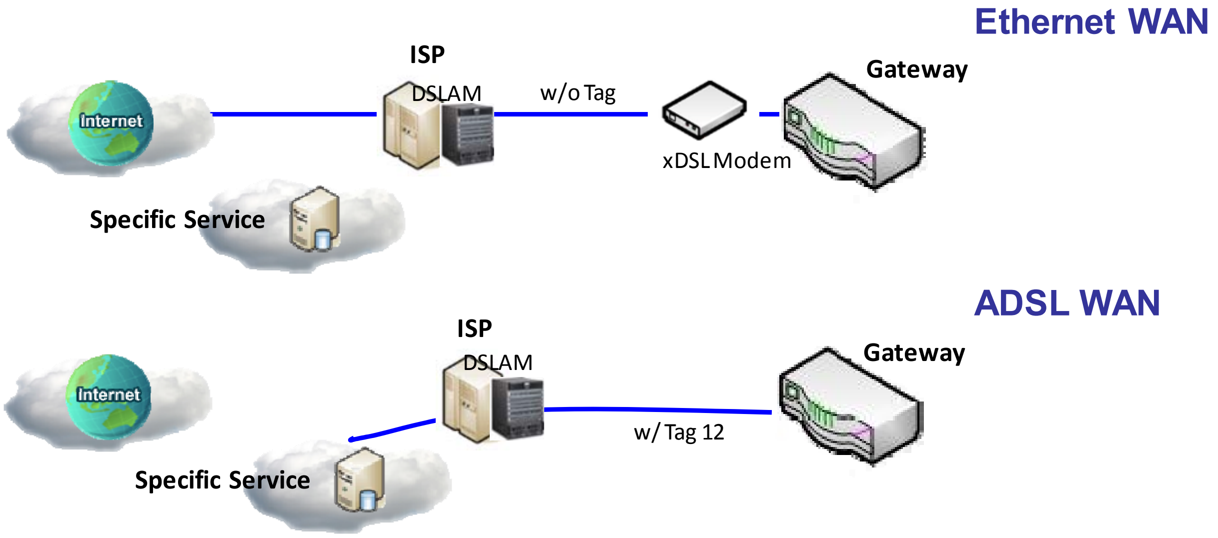
- **VLAN Tagging**

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

Index skipping is used to reserve slots for new function insertion, when required.

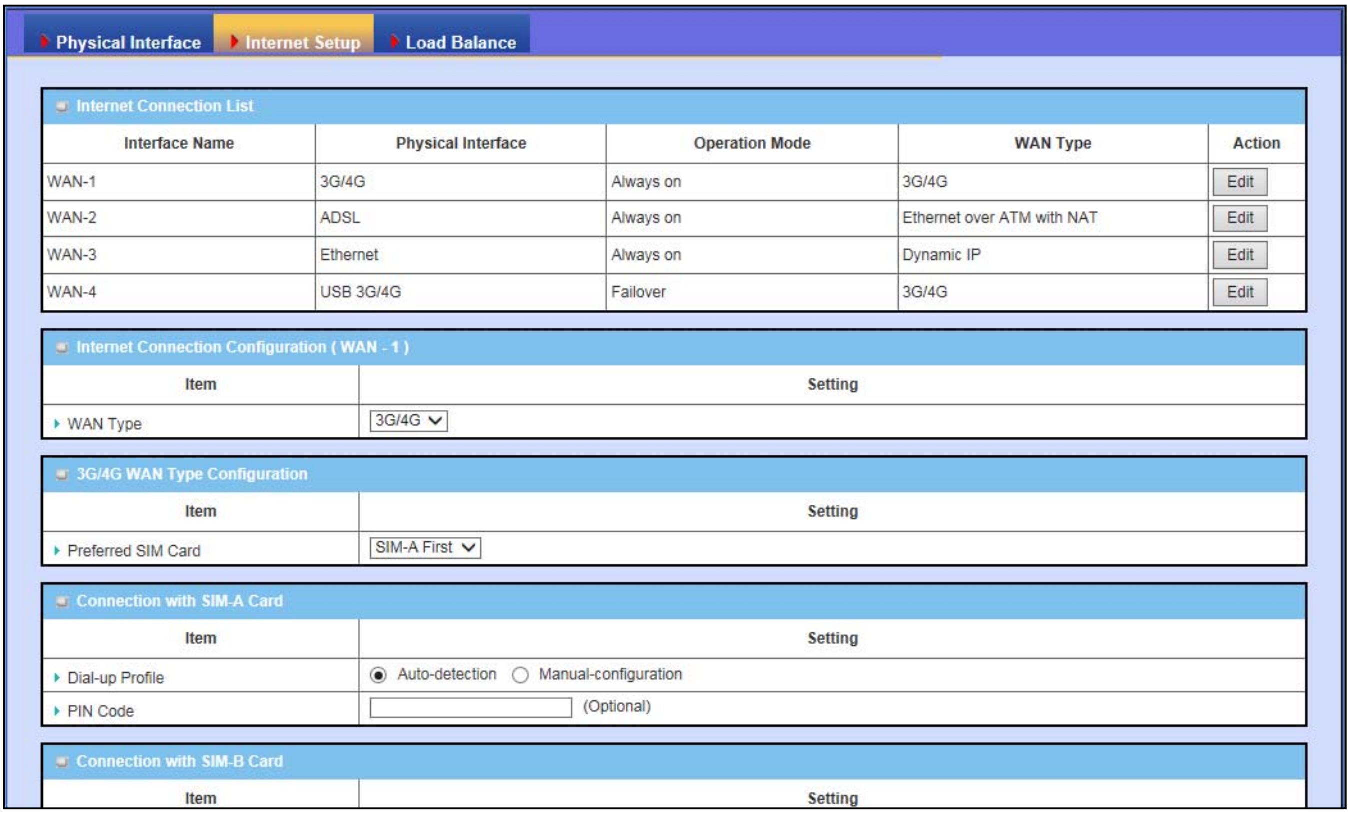
3.1.3 Internet Setup

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.

"Internet Setup List" window shows your target WAN type for each WAN interface that gateway provides.

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	3G/4G	Always on	3G/4G	Edit
WAN-2	ADSL	Always on	Ethernet over ATM with NAT	Edit
WAN-3	Ethernet	Always on	Dynamic IP	Edit
WAN-4	USB 3G/4G	Failover	3G/4G	Edit

Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	3G/4G

3G/4G WAN Type Configuration

Item	Setting
Preferred SIM Card	SIM-A First

Connection with SIM-A Card

Item	Setting
Dial-up Profile	● Auto-detection ○ Manual-configuration
PIN Code	(Optional)

Connection with SIM-B Card

Item	Setting

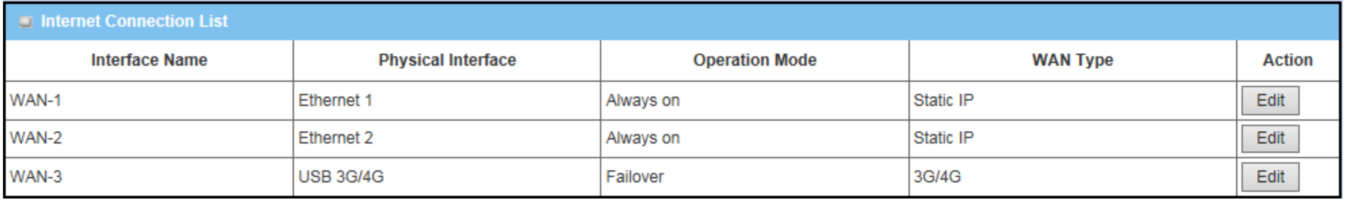
Index skipping is used to reserve slots for new function insertion, when required.

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

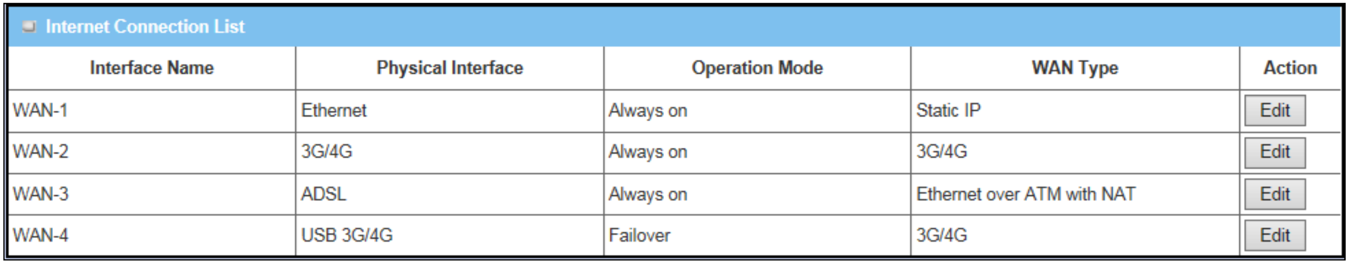
SDE852AM-00001 example



Internet Connection List

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

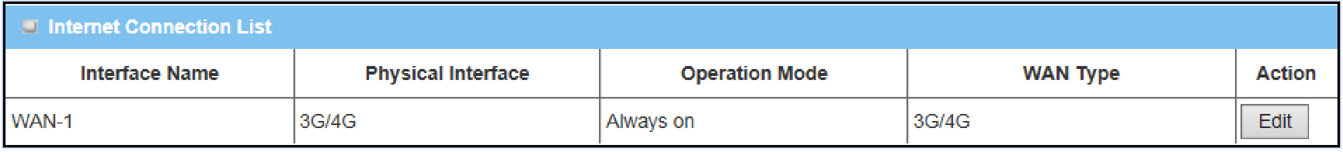
IOG761AM-0TDA1 example



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
WAN-4	USB 3G/4G	Failover	3G/4G	Edit

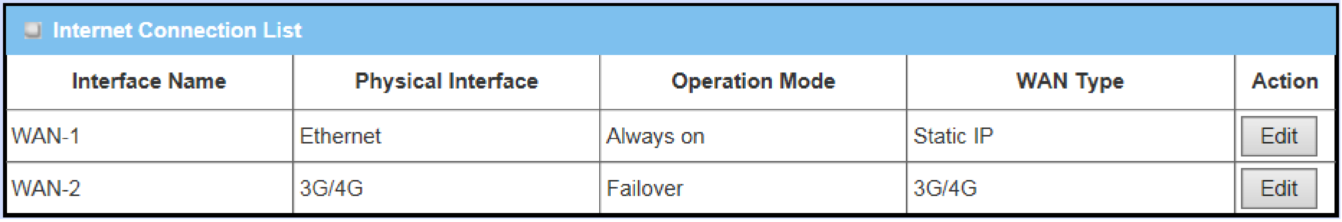
ODG761AM-0T1 example



Internet Connection List

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

BDG761AM-0T1 example



Internet Connection List

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 purchased.

Index skipping is used to reserve slots for new function insertion, when required.

- **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]-[Physical Interface]** section (3.1.1).

- **Operation Mode**

  It is "Always on", "Failover" or "Disable". Please refer to **[Basic Network]- [WAN]-[Physical Interface]** section (3.1.1).

- **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: The ISP is a mobile operator that can provide LTE, HSPA+, HSPA, WCDMA, EDGE, GPRS data services[9].
    - 3G/4G WAN type: If you have subscribed 3G/LTE 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

[9] Different models have different specifications of embedded 3G module. Please refer to specification file for details.

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.

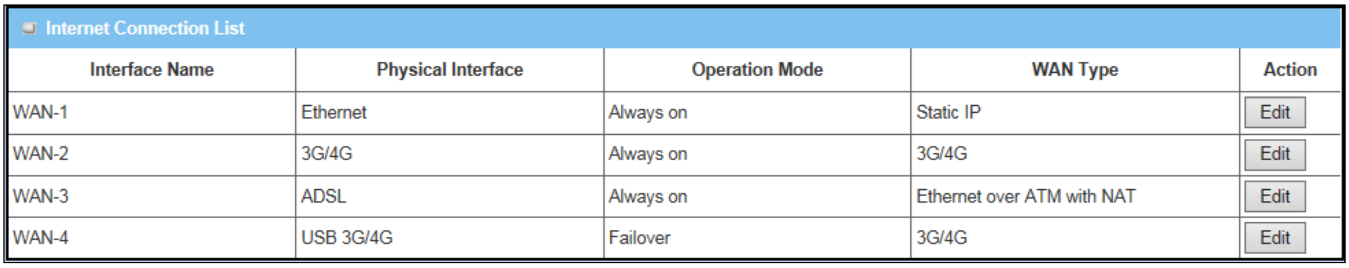
- ✧ ADSL interface: Asymmetric digital subscriber line (ADSL) is a type of digital subscriber line (DSL) technology, a data communications technology that enables faster data transmission over copper telephone lines than a conventional voiceband modem can provide. Use a RJ11 cable to connect the ADSL 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.

Index skipping is used to reserve slots for new function insertion, when required.



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
WAN-4	USB 3G/4G	Failover	3G/4G	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.

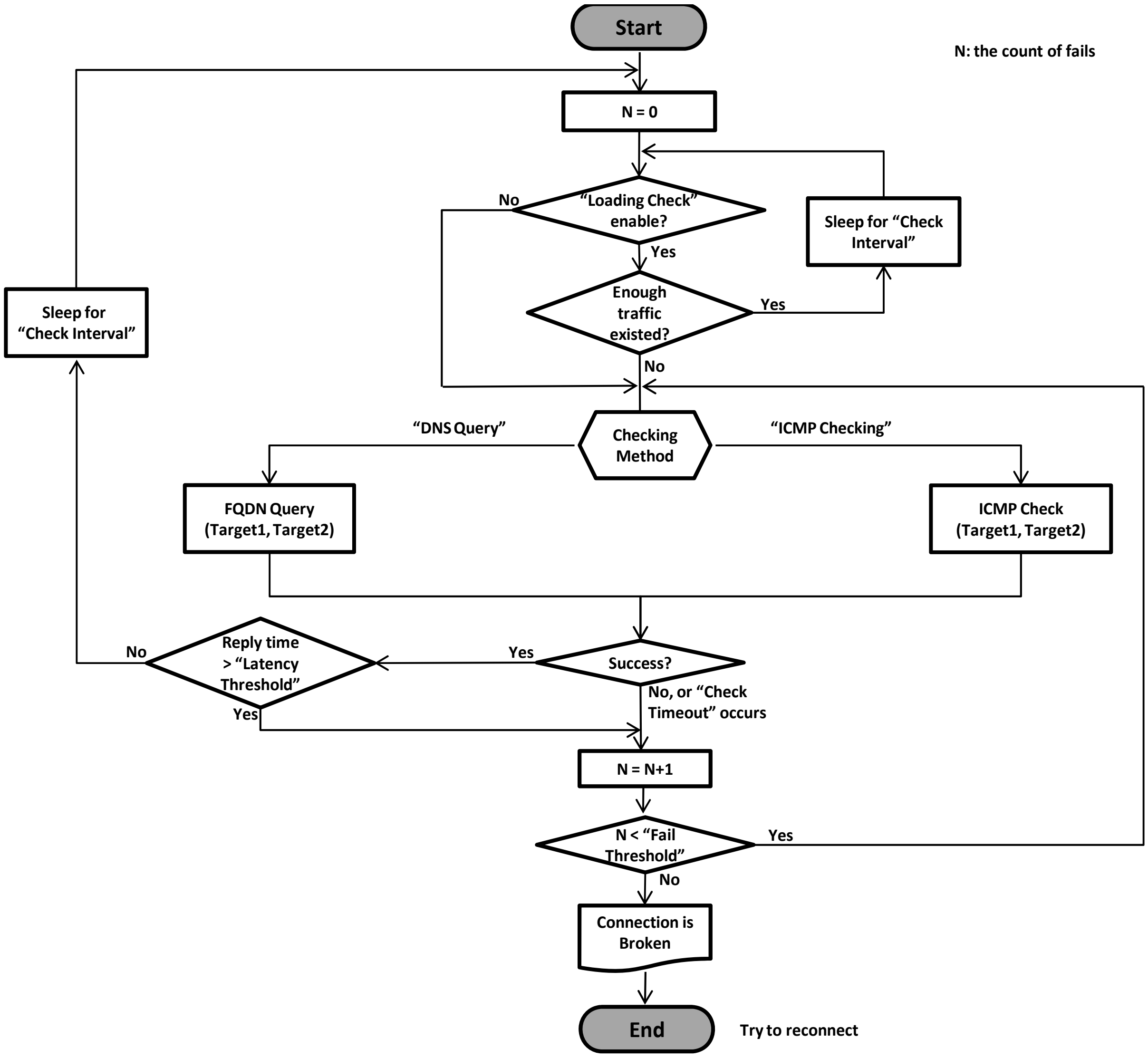
There are some common and important configuration parameters common to all WAN Type as listed below.

- **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**:

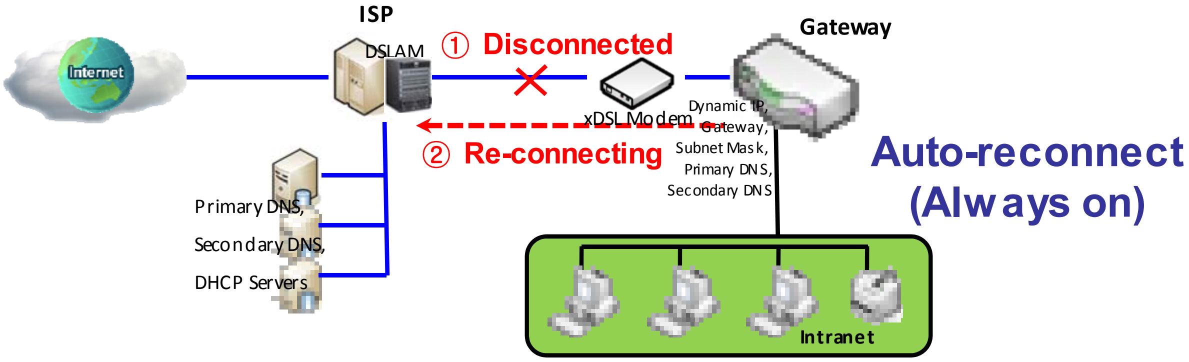
As an example, WAN-1, WAN-2 and WAN-3 are all Ethernet interfaces with "Always on" operation mode. Their WAN Type is set to "Dynamic IP" but with different Connection Control approaches. WAN-1 uses "Auto-reconnect (Always on)", WAN-2 uses "Dial-on-demand" and WAN-3 uses "Manually". Following 3 tables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

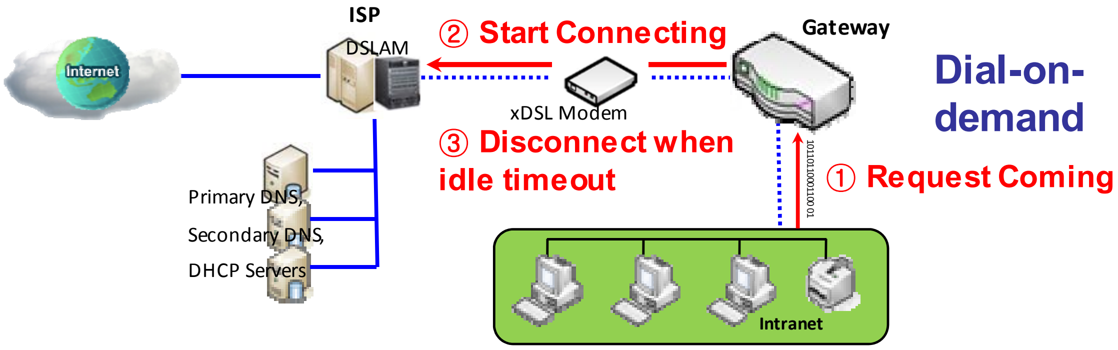


Index skipping is used to reserve slots for new function insertion, when required.

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.

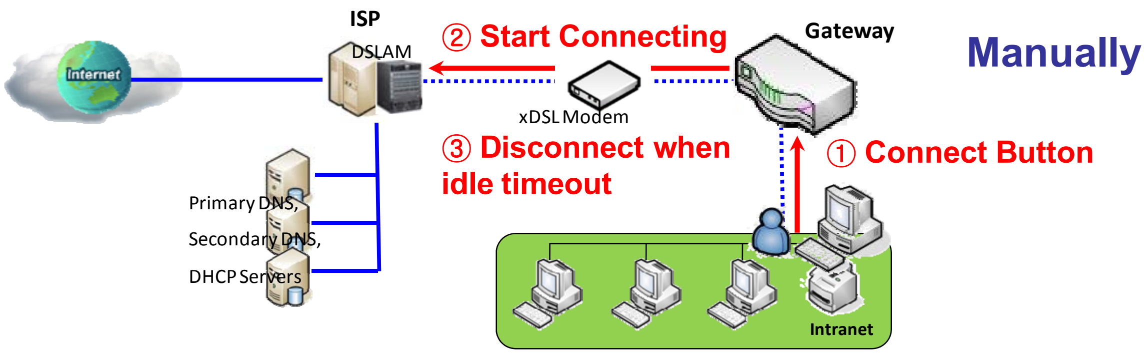
In the "Dial-on-demand" scenario, system will not make the WAN connection until gateway receives an Internet accessing request from Intranet. And then the connection will keep alive only when there still is data transfer. If there is no data transfer for a period that is longer than the Maximum Idle 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 idles 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.

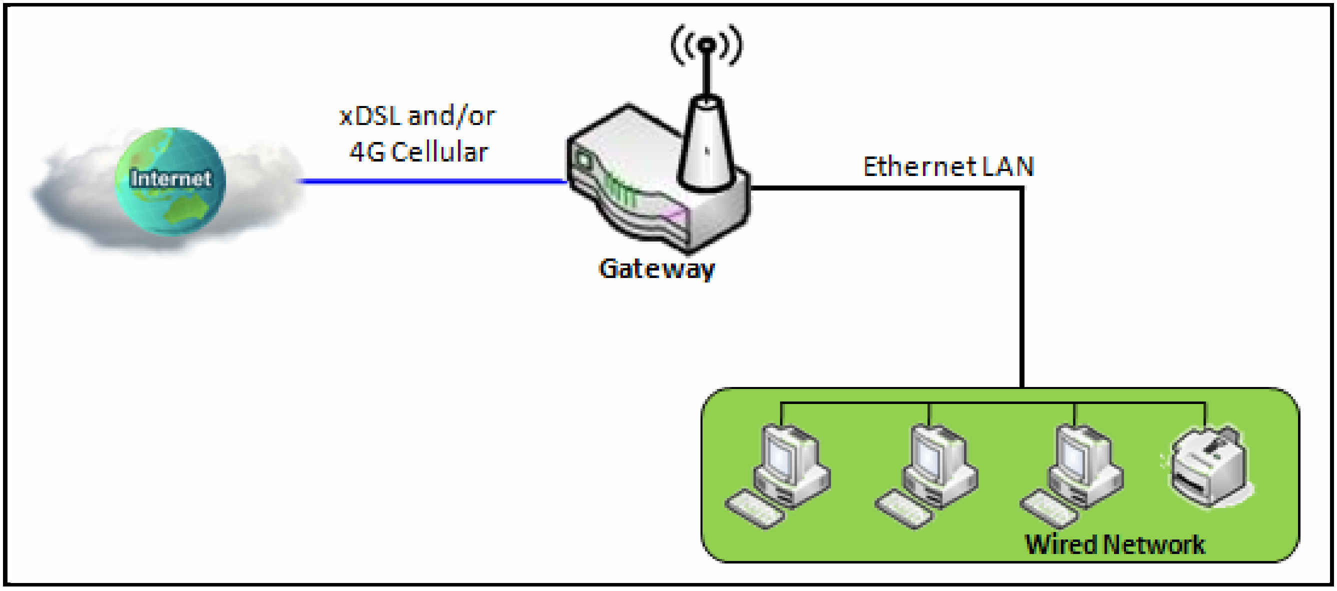
S 3: If the WAN connection idles timeout, system will disconnect it and return to its Pre-state.

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.

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.



3.3.3 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.

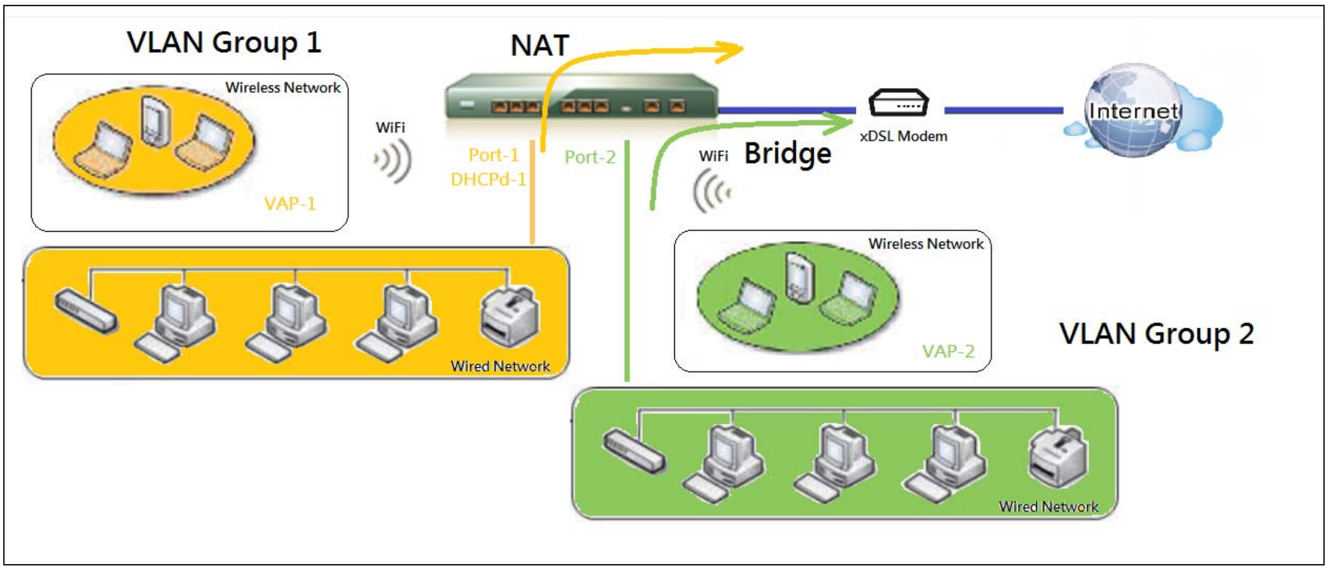
The VLAN function allows you to divide local network into different “virtual LANs”. In some cases, ISP may need router to support “VLAN tag” for certain kinds of services (e.g. IPTV) to work properly. In some cases, SMB departments are separated and located at any floor of building. All client hosts 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:

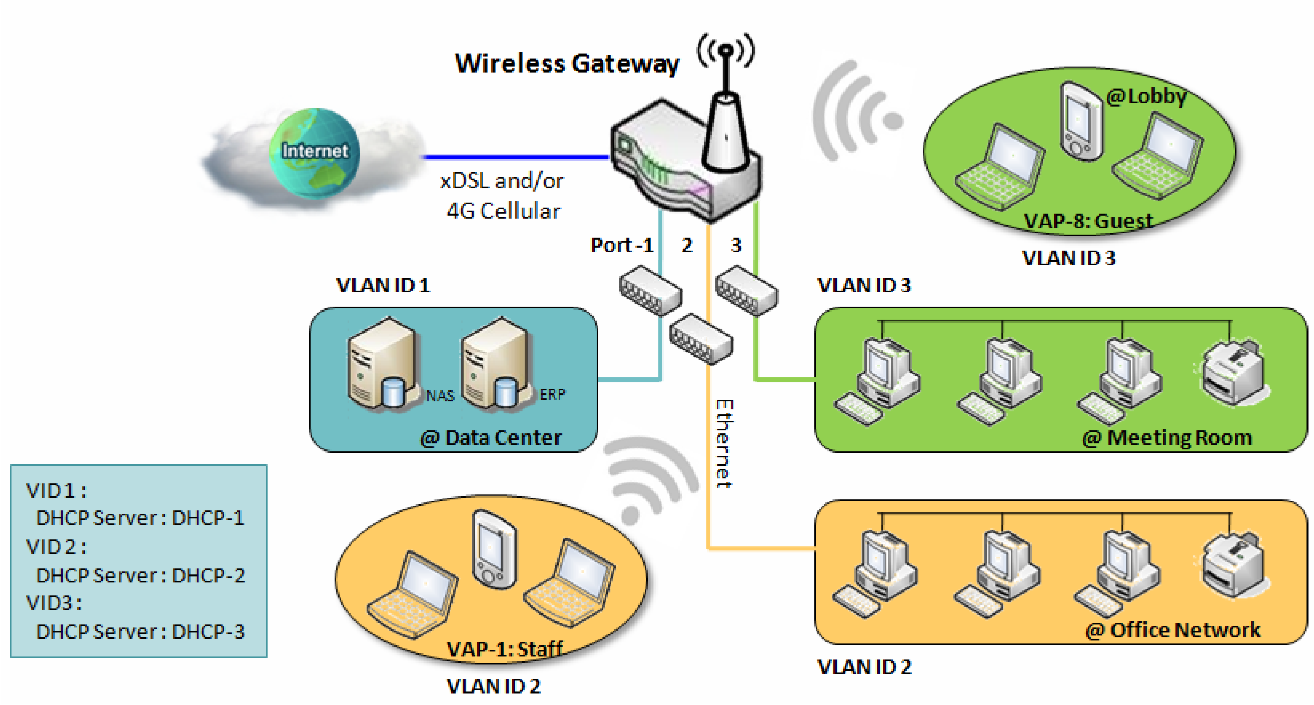
Port-Based VLAN Tagging for Differentiated Services

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.

In SMB or a company, administrator schemes out 3 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.

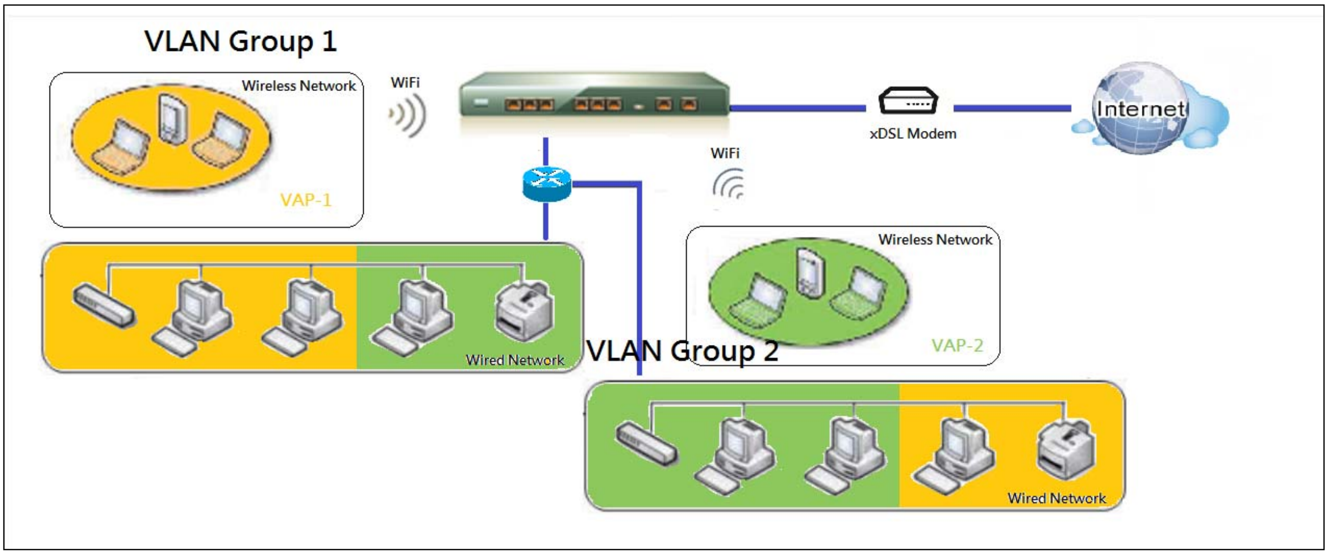


Above is the general case for 3 Ethernet LAN ports in the gateway. But if the device just has one Ethernet LAN port, there will be only one VLAN group for the device. Under such situation, it still supports both the NAT and Bridge mode for the Port-based VLAN configuration.

Tag-based VLAN Tagging for Location-free Departments

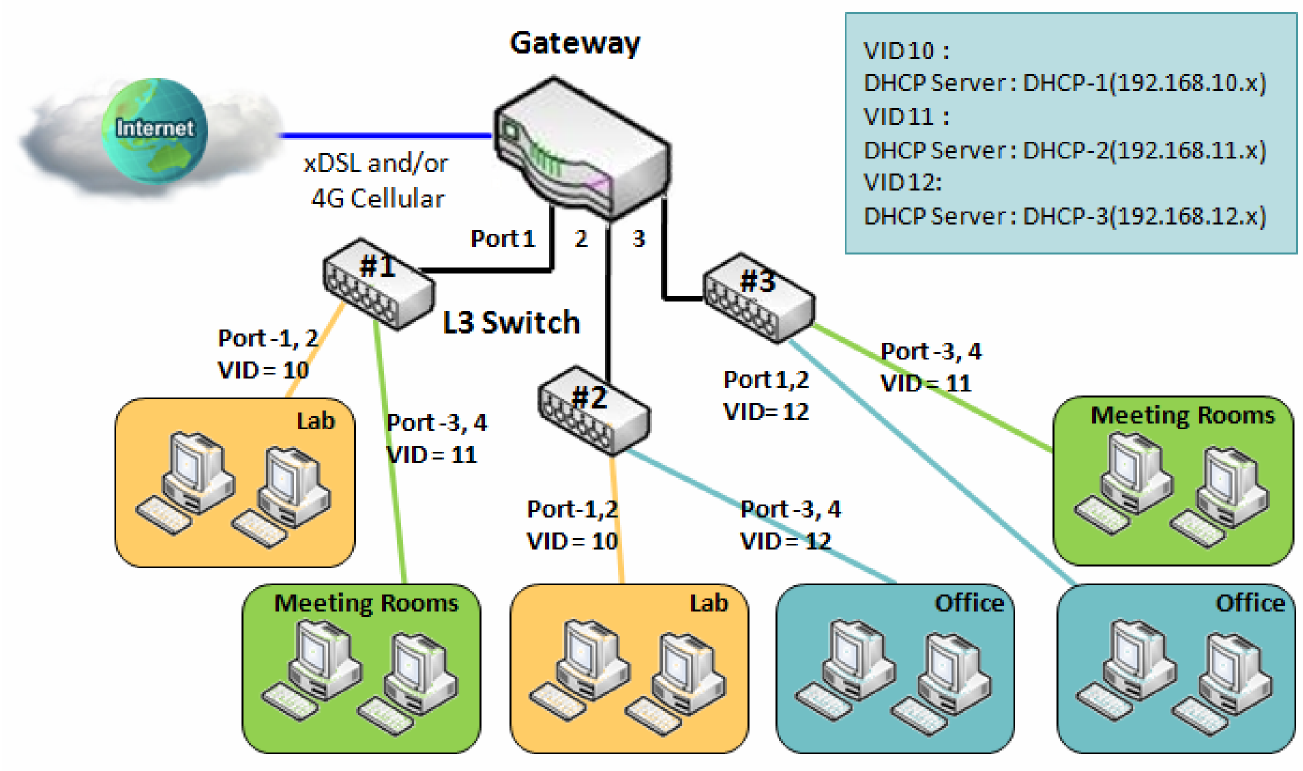
Tag-based VLAN function can group Ethernet ports, Port-1 ~ Port-4, and WiFi Virtual Access Points, VAP-1 ~ VAP-8, together with different VLAN tags for deploying department subnets in Intranet. All packet flows can carry with different VLAN tags even at the same physical Ethernet port for Intranet. These 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 department.

Index skipping is used to reserve slots for new function insertion, when required.



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.

In a SMB company, administrator schemes out 3 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.



VID 10 :
DHCP Server : DHCP-1(192.168.10.x)
VID 11 :
DHCP Server : DHCP-2(192.168.11.x)
VID 12:
DHCP Server : DHCP-3(192.168.12.x)

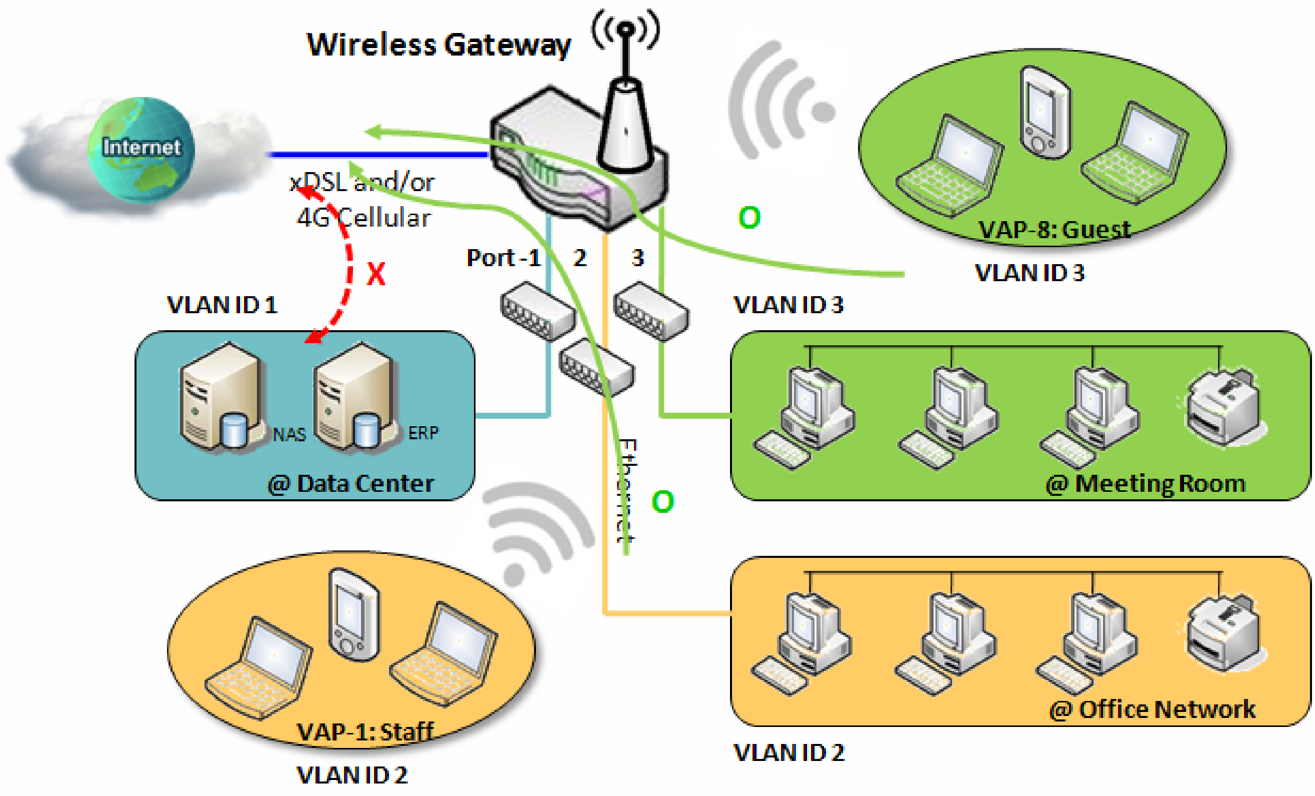
VLAN Group Access Control

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

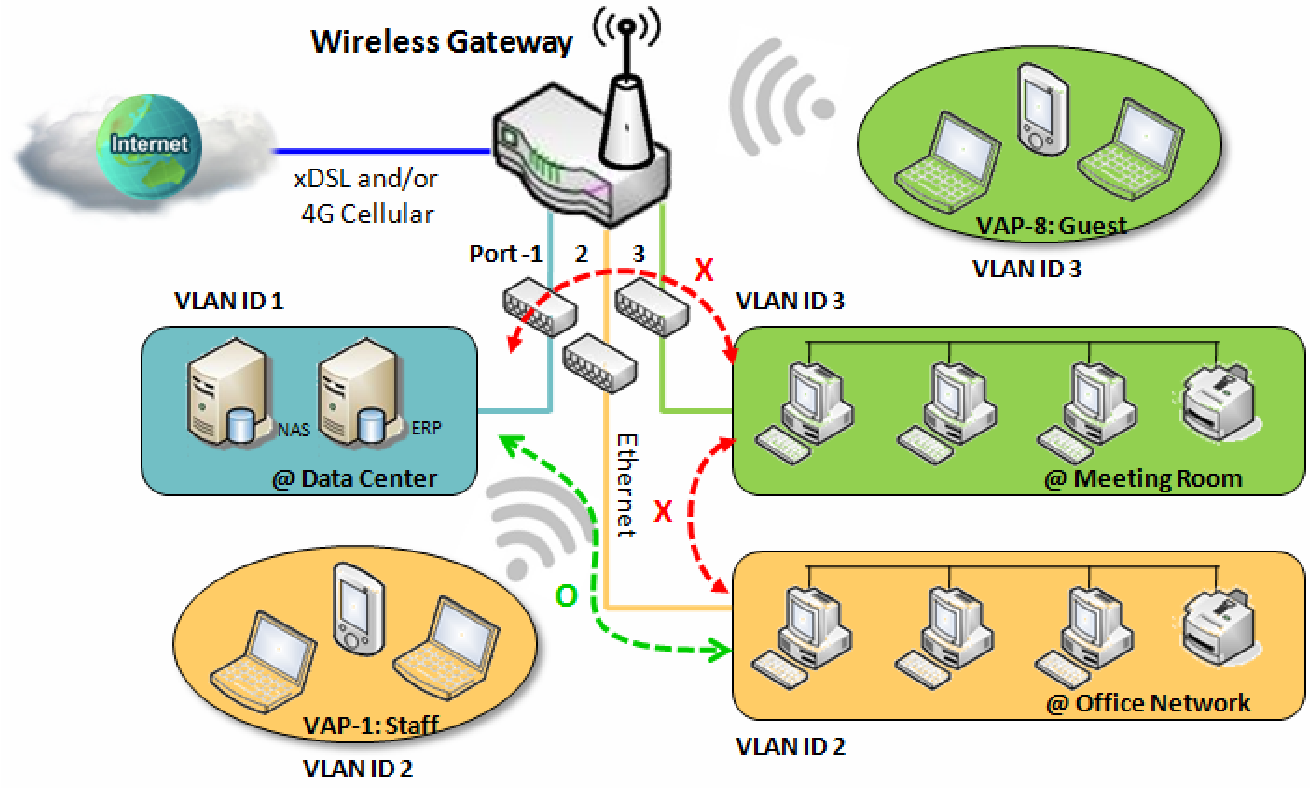
Administrator can specify members of one VLAN group to be able to access Internet or not. Following is an example that VLAN groups of VID is 2 and 3 can access Internet but the one with VID is 1 cannot. That is, visitors in meeting room and staffs in office network can access Internet. But the computers/servers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

Index skipping is used to reserve slots for new function insertion, when required.



Inter VLAN Group Routing:

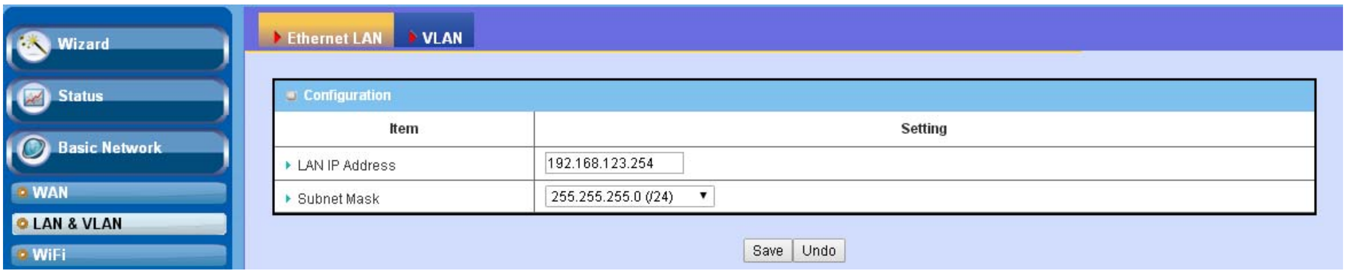
In Port-based tagging, administrator can specify member hosts of one VLAN group to be able to communicate with the ones of another VLAN group or not. This is a communication pair, and one VLAN group can join many communication pairs. But communication pair doesn’t have the transitive property. That is, 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.



LAN & VLAN Setting

The Ethernet LAN allows user to setup the LAN IP address for device. Setting LAN IP address and subnet mask will affect the IP that LAN devices can get.

Go to Basic Network > LAN & VLAN > Ethernet LAN



Configuration

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

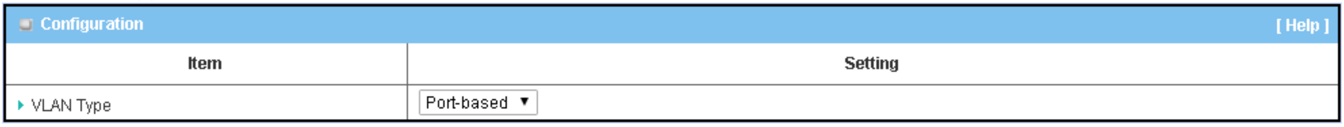
Index skipping is used to reserve slots for new function insertion, when required.

Ethernet LAN		
Item	**Value setting**	**Description**
LAN IP Address	A Must filled setting	LAN IP can let user to access device from LAN. Changing LAN IP means to change the DHCP server IP pool on device.
Subnet Mask	A Must filled setting	**Subnet Mask** is used to define the range of IP pool and it will affect the IP address that LAN devices can get.
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.

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

For Port-based VLAN Type
Go to Basic Network > LAN & VLAN > VLAN Tab

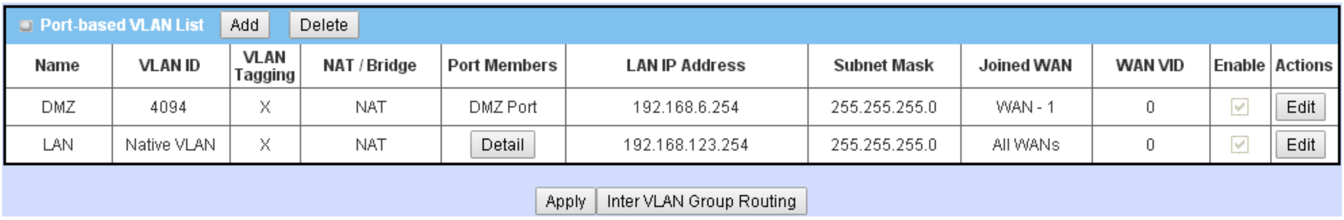
In VLAN type select **Port-based.**



Item	Setting
VLAN Type	Port-based ▼

VLAN Configuration		
Item	**Value setting**	**Description**
VLAN Type	**Port-based** is selected by default	Select **Port-based** allow you to add rule for each LAN port, and you can do advantaged control of according to its VLAN ID. Select **Tag-based** allow 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

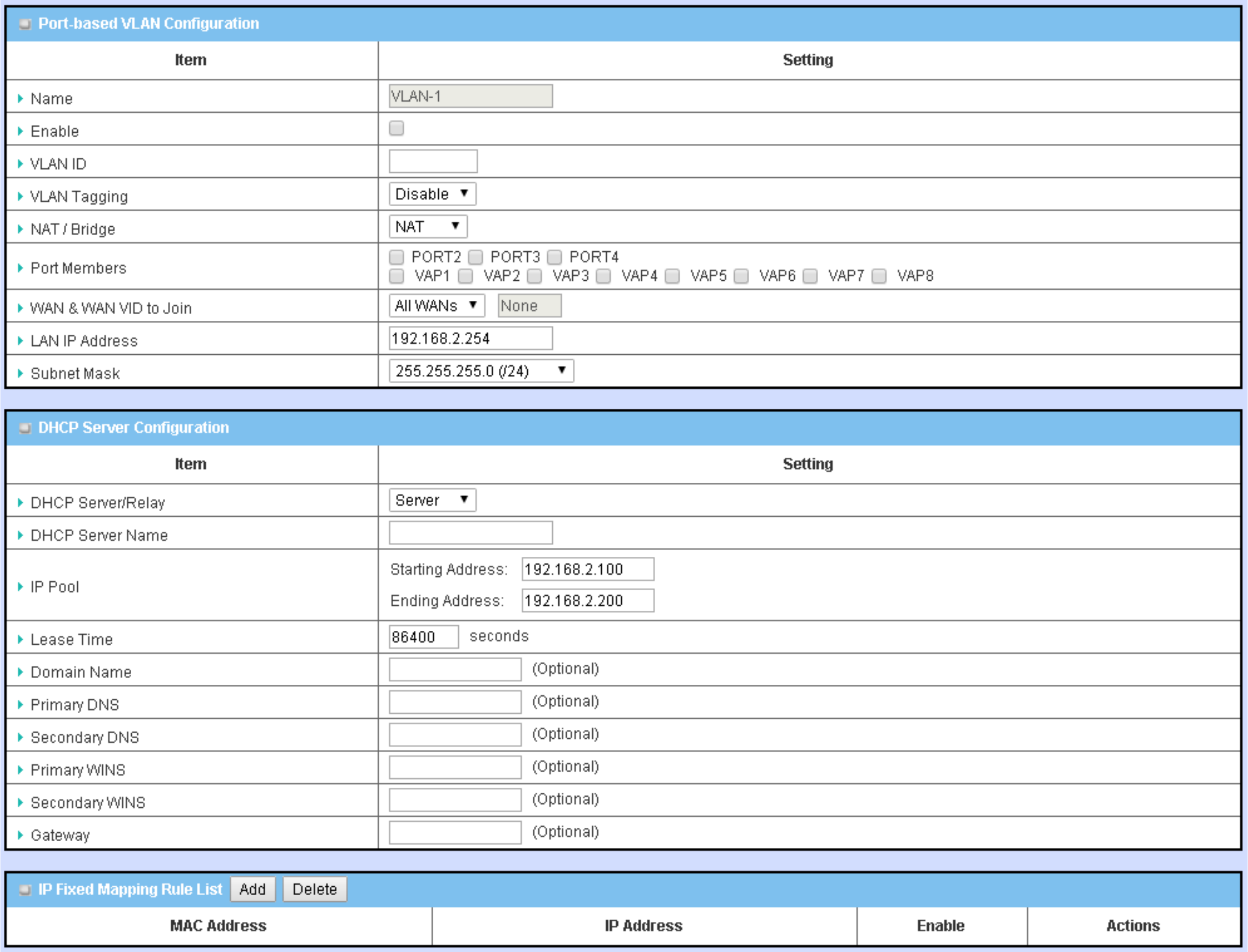
Create/Edit Port-based VLAN Rules
The port-based VLAN allows you to custom each LAN port. There is a default rule shows the configuration of all LAN port. Also, If your device has a DMZ port, you will see DMZ configuration, too. The maxima rule numbers is based on LAN port numbers.



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

Index skipping is used to reserve slots for new function insertion, when required.

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



Port-based VLAN Configuration

Item	Setting
Name	VLAN-1
Enable	☐
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 Configuration

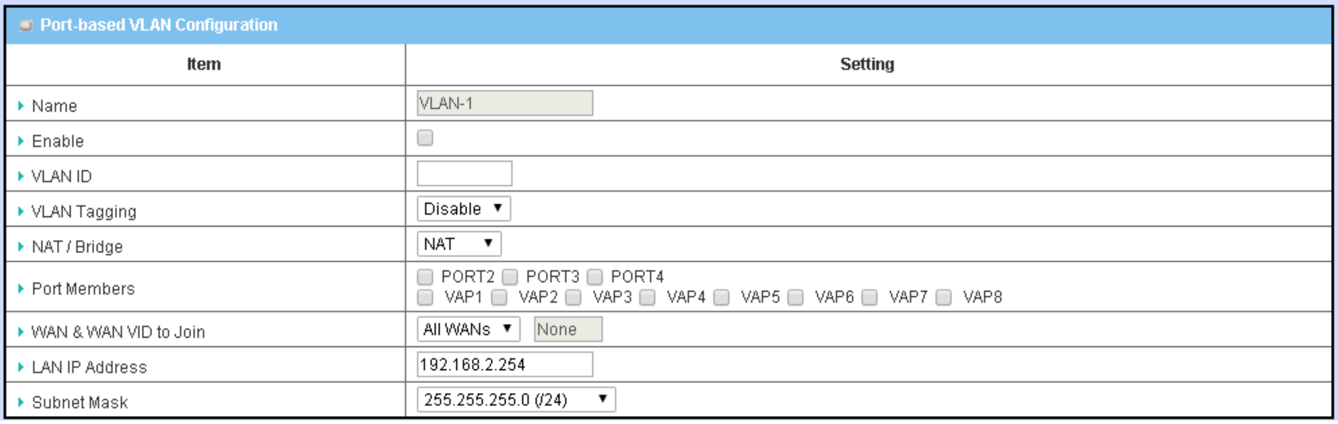
Item	Setting
DHCP Server/Relay	Server ▼
DHCP Server Name	
IP Pool	Starting Address: 192.168.2.100 Ending Address: 192.168.2.200
Lease Time	86400 seconds
Domain Name	(Optional)
Primary DNS	(Optional)
Secondary DNS	(Optional)
Primary WINS	(Optional)
Secondary WINS	(Optional)
Gateway	(Optional)

IP Fixed Mapping Rule List Add Delete

MAC Address	IP Address	Enable	Actions

Index skipping is used to reserve slots for new function insertion, when required.

Port-based VLAN Configuration



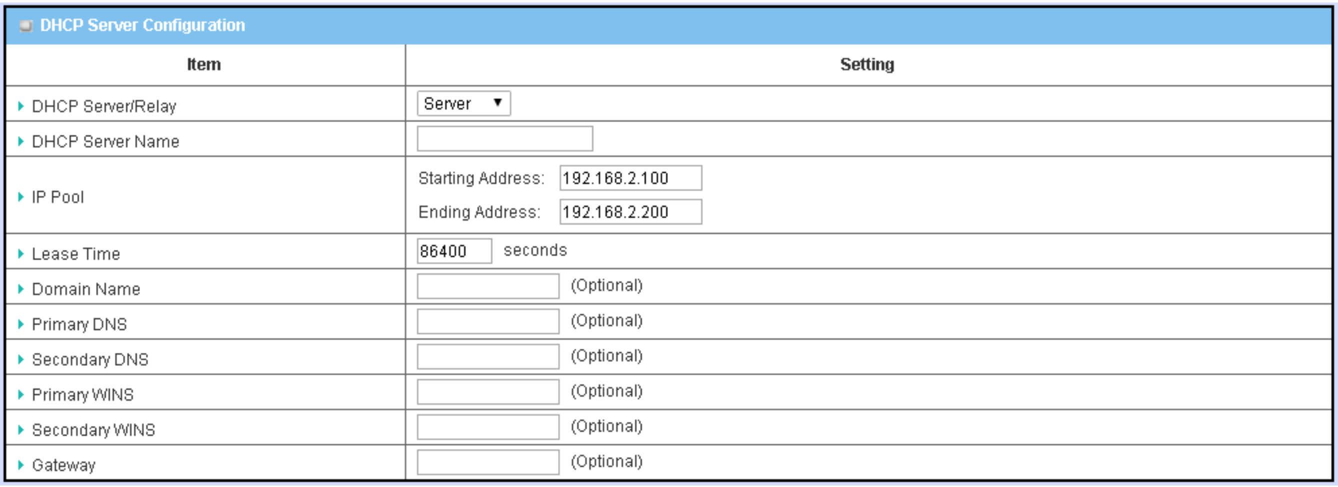
Port-based VLAN Configuration

Item	Setting
Name	VLAN-1
Enable	□
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) ▼

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.
Enable	The box is unchecked by default.	Click **Enable** box to activate this rule.
VLAN ID	A Must filled setting	Define the VLAN ID number, range is 1~4094.
VLAN Tagging	By default **Disable** is selected.	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	By default **NAT** is selected.	Select **NAT** mode or **Bridge** mode for the rule.
Port Members	These box is unchecked by default.	Select which LAN port and VAP that you want to add to the rule. Disappear Port-1 when it is configured as WAN interface. Disappear VAP if the router doesn't support Wireless function. Disappear VAP when Selecting Bridge mode.
WAN & WAN VID to Join	By default **All WANs** is selected.	Select which **WAN** or **All WANs** that allow accessing Internet. If mode is NAT type and the WAN is 3G type then gray VID field out If mode is Bridge type, you need to select a WAN and fill the VID field.
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	By default **255.255.255.0(/24)** is selected.	Select a **Subnet Mask** for the DHCP Server.

Index skipping is used to reserve slots for new function insertion, when required.

DHCP Server Configuration



DHCP Server Configuration

Item	Setting
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)

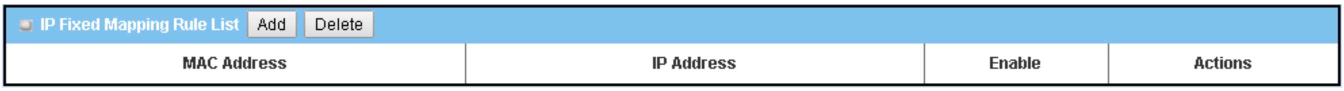
DHCP Server Configuration		
Item	**Value setting**	**Description**
DHCP Server /Relay	By default **Server** is selected.	Define the **DHCP Server** type. There are three types you can select: **Server**, **Relay**, and **Disable**. If selecting **Server** or **Disable**, just go to **DHCP Server Name** field to start setting Server information. If selecting **Relay** type, only have to fill the **DHCP Server IP Address** field. Go to **DHCP Server IP Address**
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. When your lease expires, you must stop using the IP address.
Domain Name	NA	It's optional field, please follow rules of CHCP Server page. Go to **Basic Network > Client / Server / Proxy > DHCP Server**
Primary DNS	NA	It's optional field, please follow rules of CHCP Server page. Go to **Basic Network > Client / Server / Proxy > DHCP Server**
Secondary DNS	NA	It's optional field, please follow rules of CHCP Server page. Go to **Basic Network > Client / Server / Proxy > DHCP Server**
Primary WINS	NA	It's optional field, please follow rules of CHCP Server page. Go to **Basic Network > Client / Server / Proxy > DHCP Server**
Secondary WINS	NA	It's optional field, please follow rules of CHCP Server page. Go to **Basic Network > Client / Server / Proxy > DHCP Server**
Gateway	NA	It's optional field, please follow rules of CHCP Server page. Go to **Basic Network > Client / Server / Proxy > DHCP Server**
DHCP Server IP Address	A Must filled setting	If selecting **Relay** type of DHCP Server, assign a **DHCP Server IP Address** that clients can request from.

Index skipping is used to reserve slots for new function insertion, when required.

(for DHCP **Relay** settings only)		
Save	NA	Click the **Save** button to save the configuration and back to **Port-based VLAN List**.

IP Fixed Mapping Rule List

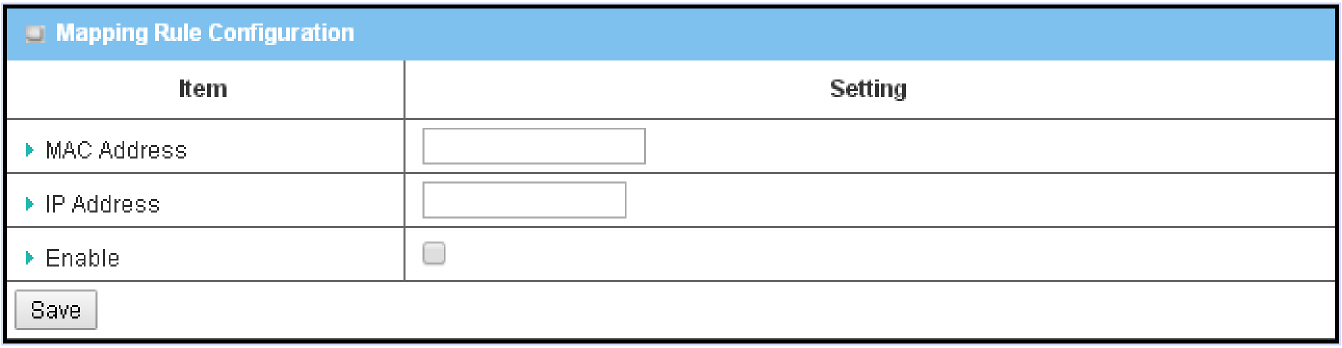
Additionally, you can add rule in the **IP Fixed Mapping Rule List**, and the rule list in only for **Server/Disable** type of **DHCP Server /Relay** field. This table is the same with **Basic Network > Client / Server / Proxy > DHCP Server > Fixed Mapping Tab**



IP Fixed Mapping Rule List | Add | Delete

MAC Address	IP Address	Enable	Actions

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



Mapping Rule Configuration

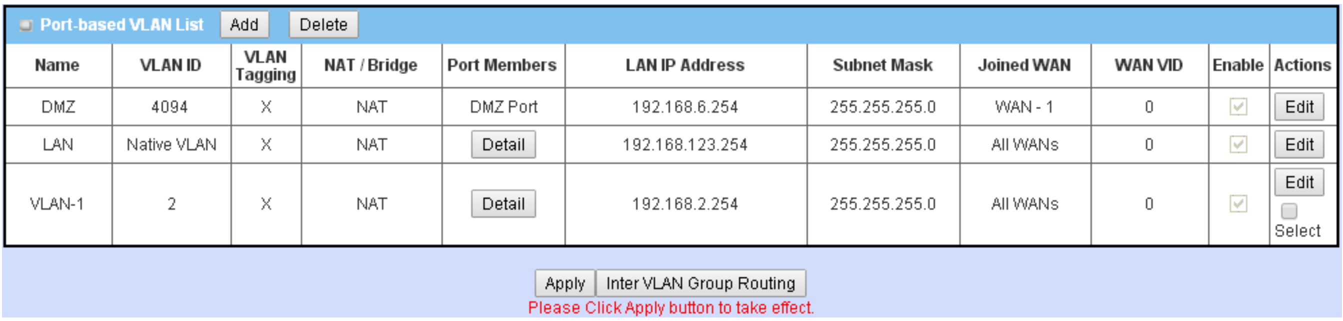
Item	Setting
MAC Address	
IP Address	
Enable	□

Save

Mapping Rule Configuration		
Item	**Value setting**	**Description**
MAC Address	A Must filled setting	Define the **MAC Address** target that the DHCP Server wants to filter.
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 **MAC Address**.
Enable	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	NA	Click the **Save** button to save the configuration. The web browser will take you back to the VLAN page. There you will need to click on **Apply** button.
Apply		Click on **Apply** button to apply the changes.

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

Index skipping is used to reserve slots for new function insertion, when required.

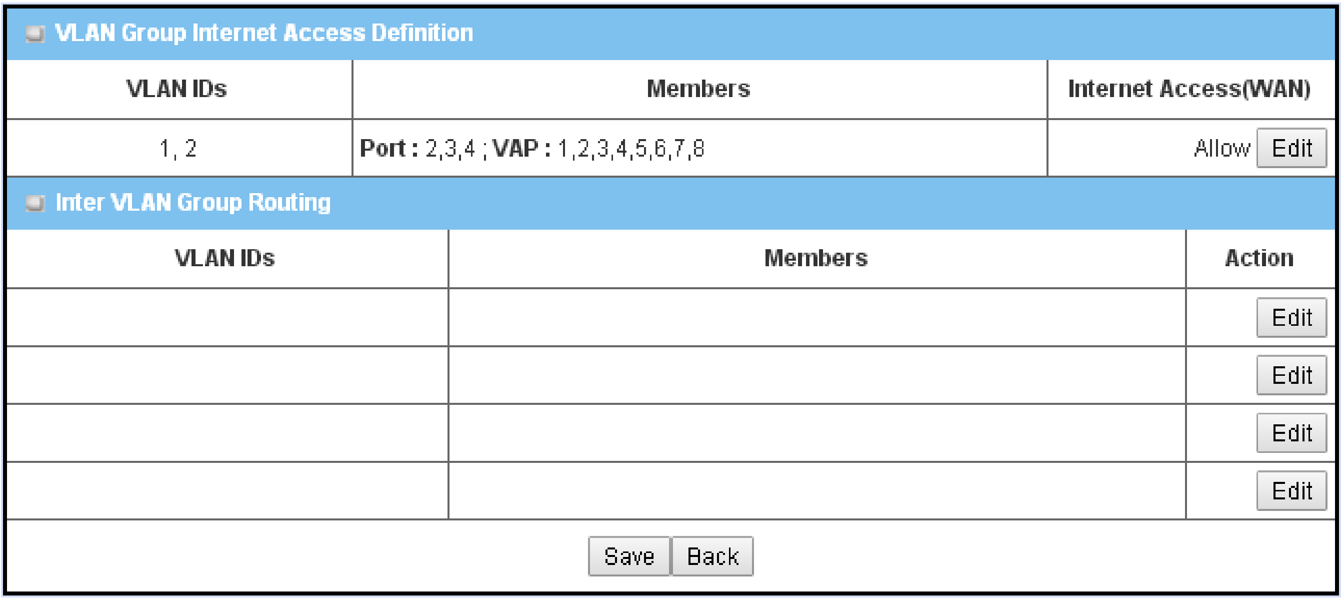


Name	VLAN ID	VLAN Tagging	NAT / Bridge	Port Members	LAN IP Address	Subnet Mask	Joined WAN	WAN VID	Enable	Actions
DMZ	4094	X	NAT	DMZ Port	192.168.6.254	255.255.255.0	WAN - 1	0	☑	Edit
LAN	Native VLAN	X	NAT	Detail	192.168.123.254	255.255.255.0	All WANs	0	☑	Edit
VLAN-1	2	X	NAT	Detail	192.168.2.254	255.255.255.0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

Please Click Apply button to take effect.

Inter VLAN Group Routing

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



VLAN Group Internet Access Definition

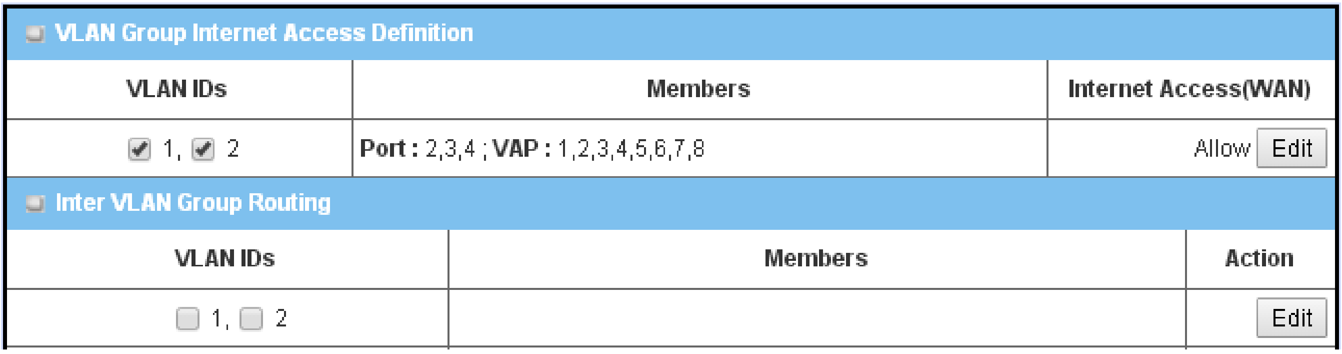
VLAN IDs	Members	Internet Access(WAN)
1 , 2	**Port :** 2,3,4 ; **VAP :** 1,2,3,4,5,6,7,8	Allow Edit

Inter VLAN Group Routing

VLAN IDs	Members	Action
		Edit
		Edit
		Edit
		Edit

The screen in the figure shows the default setting. Each member in different **VLAN IDs** can't access each other. Click on Edit to modify the setting.

When clicking Edit button, 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

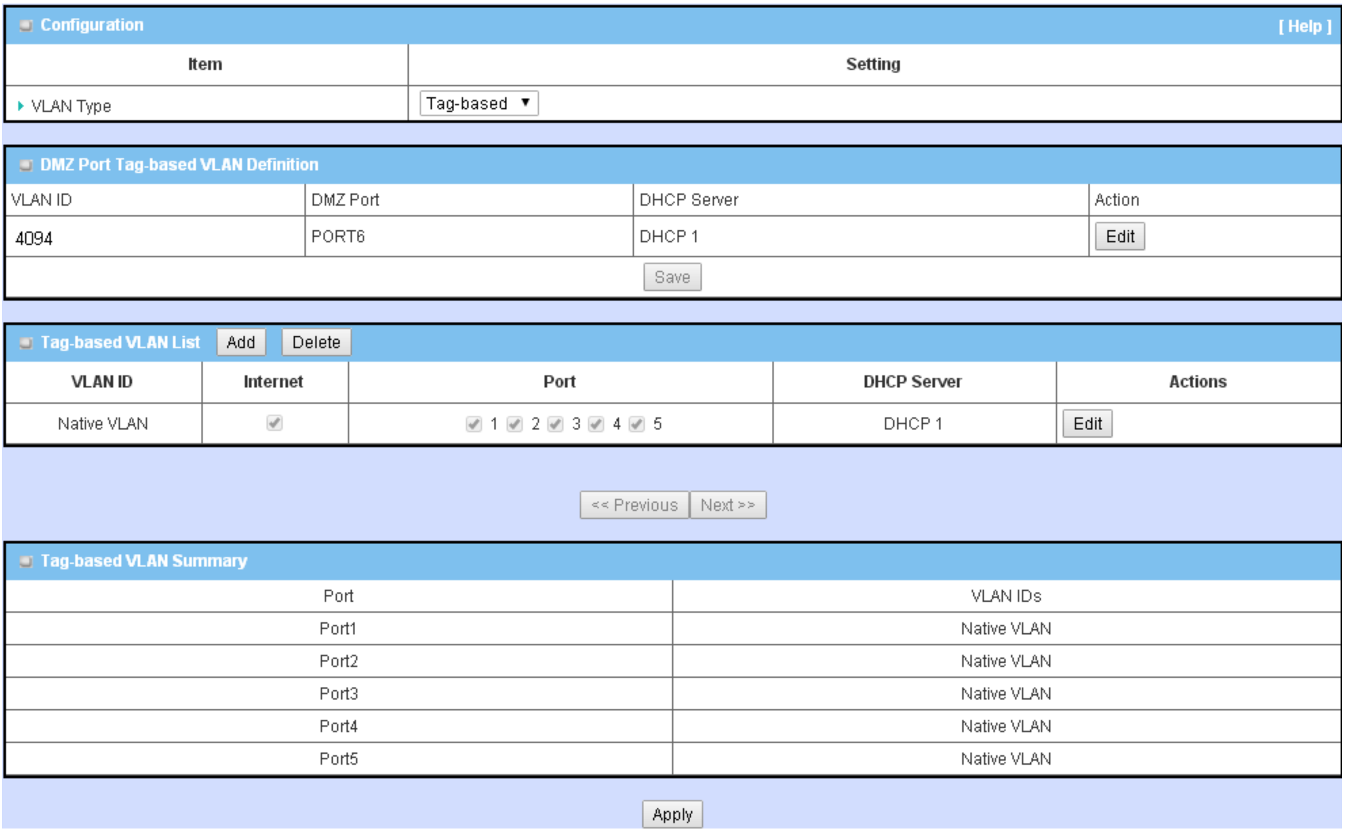
VLAN IDs	Members	Action
□ 1, □ 2		Edit

Index skipping is used to reserve slots for new function insertion, when required.

VLAN Group 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 **VLAN ID** box, it means the VLAN ID member can't access Internet anymore. (**VLAN ID 1** is available always, it is the default VLAN ID of **LAN** rule) (**VLAN ID 2** is available only when **VLAN ID 2** is enabled) The same applies to other VLAN IDs. (i.e. **VLAN ID 3).**
Inter VLAN Group Routing	The box is unchecked by default.	By default, members in different VLAN IDs can't access each other. Our device supports 4 rules for **Inter VLAN Group Routing.** If ID_1 and ID_2 are checked, it means members in VLAN ID_1 and VLAN ID_2 are defined as a group member. Members of VLAN ID_1 can access members of VLAN ID_2, so as VLAN ID_2 to VLAN ID_1. (**VLAN ID 1** is available always, it is the default VLAN ID of **LAN** rule) (**VLAN ID 2** is available only when **VLAN ID 2** is enabled) The same applies to other VLAN IDs. (i.e. **VLAN ID 3).**
Save	*NA*	Click the **Save** button to save the configuration

For Tag-based VLAN Type

The **Tag-based VLAN** allows you to custom 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 tad-based VLAN rule sets.
Go to Basic Network > LAN & VLAN > VLAN Tab
In VLAN type select **Tag-based**



Configuration [Help]

Item	Setting
VLAN Type	Tag-based ▼

DMZ Port Tag-based VLAN Definition

VLAN ID	DMZ Port	DHCP Server	Action
4094	PORT6	DHCP 1	Edit

Tag-based VLAN List

VLAN ID	Internet	Port	DHCP Server	Actions
Native VLAN	☑	☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5	DHCP 1	Edit

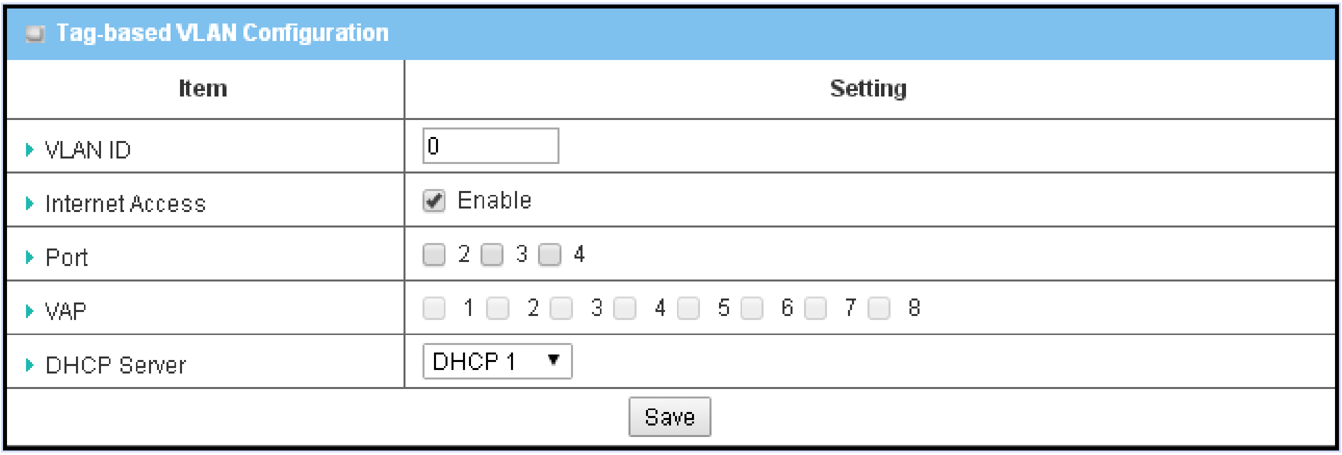
Tag-based VLAN Summary

Port	VLAN IDs
Port1	Native VLAN
Port2	Native VLAN
Port3	Native VLAN
Port4	Native VLAN
Port5	Native VLAN

Index skipping is used to reserve slots for new function insertion, when required.

Create/Edit Tag-based VLAN Rules

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 ▼

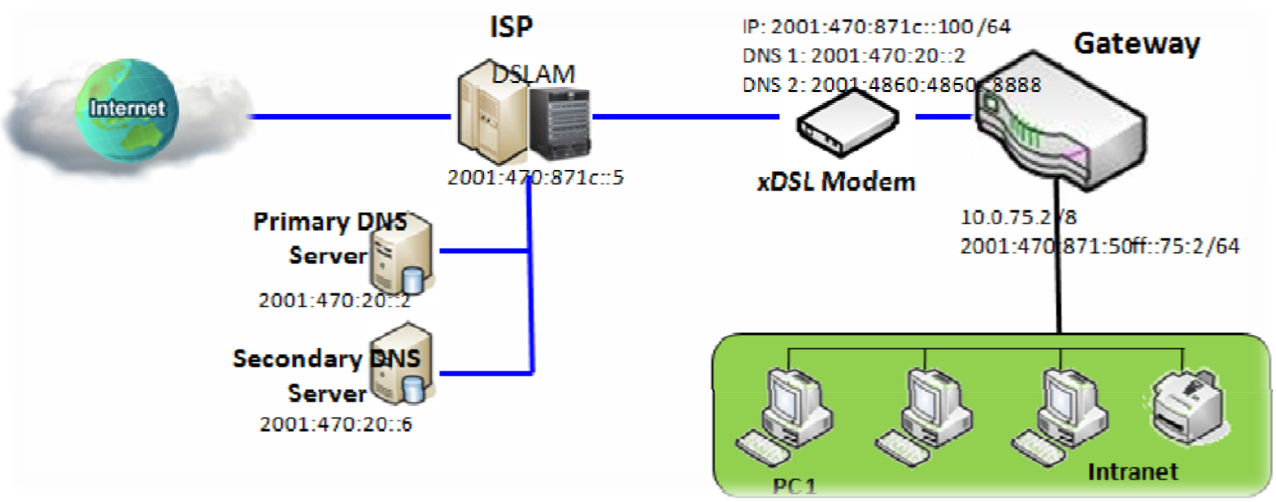
Tag-based VLAN		
Item	**Value setting**	**Description**
VALN ID	A Must filled setting	Define the **VLAN ID** number, range is 6~4094.
Internet Access	The box is checked by default.	Define the **VLAN ID** member can access Internet or not.
Port	The box is unchecked by default.	Define which LAN port is part of the **VLAN ID**.
VAP	The box is unchecked by default.	Define which **VAP** is part of the **VLAN ID**. Notice that a **VAP** is only belong to a **VLAN ID**. Disappear **VAP** if the router doesn't support Wireless function.
DHCP Server	By default **DHCP 1** is selected.	Assign a **DHCP Server** to these members of this **VLAN ID**. The field list available **DHCP server** and **None** items for select. To create or edit DHCP server for VLAN, refer **to Basic Network > Client/Server/Proxy > DHCP Server**
Save	NA	Click the **Save** button to save the configuration Notice that after clicking **Save** button, always click **Apply** button to take these rules effect

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

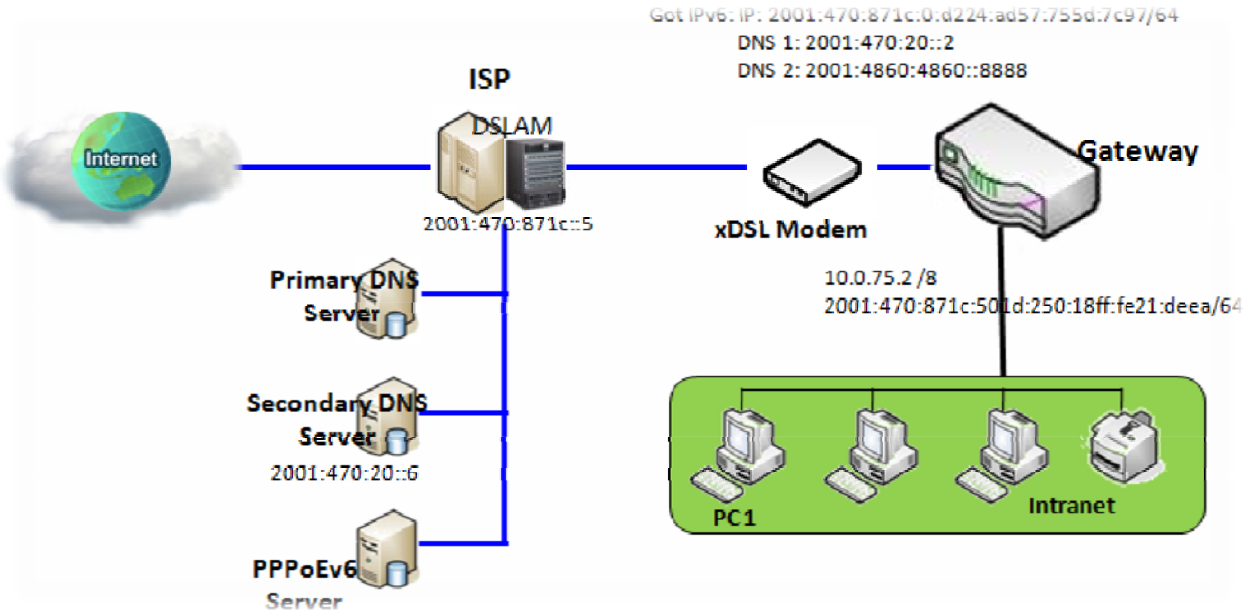
Static IPv6 does the same function as static IPv4. The static IPv6 provides manual setting of IPv6 address, IPv6 default gateway address, and IPv6 DNS.



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

DHCPv6

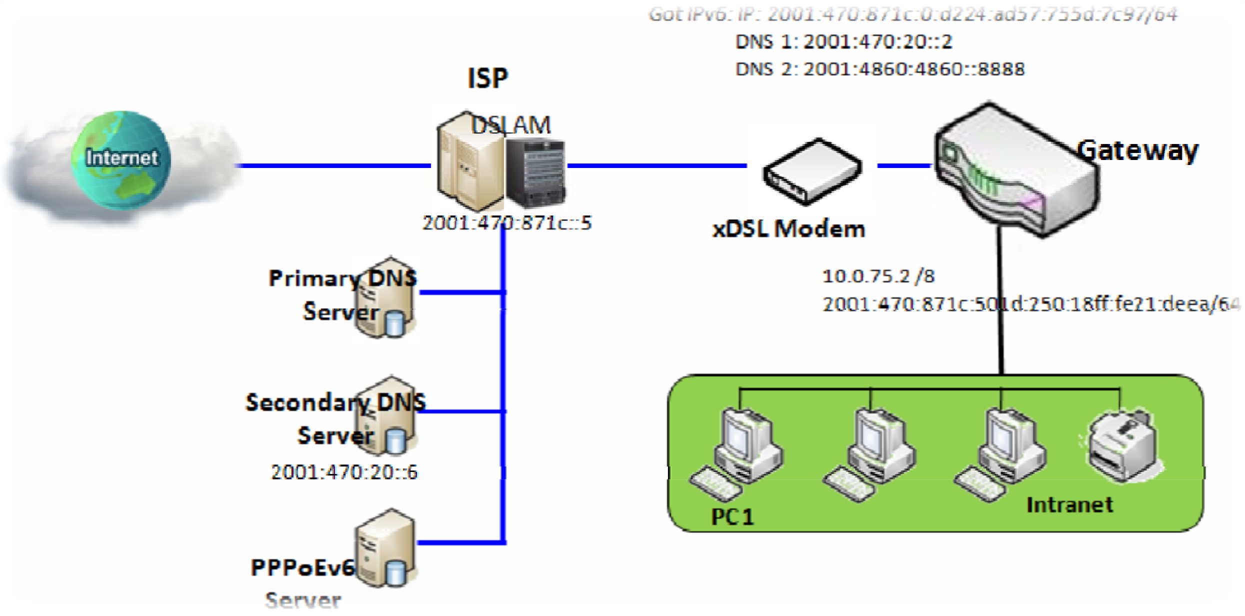
DHCP in IPv6 does the same function as DHCP in IPv4. The DHCP server sends IP address, DNS server addresses and other possible data to the DHCP client to configure automatically. The server also sends a lease time of the address and time to recontact the server for IPv6 address renewal. The client has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



In 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.

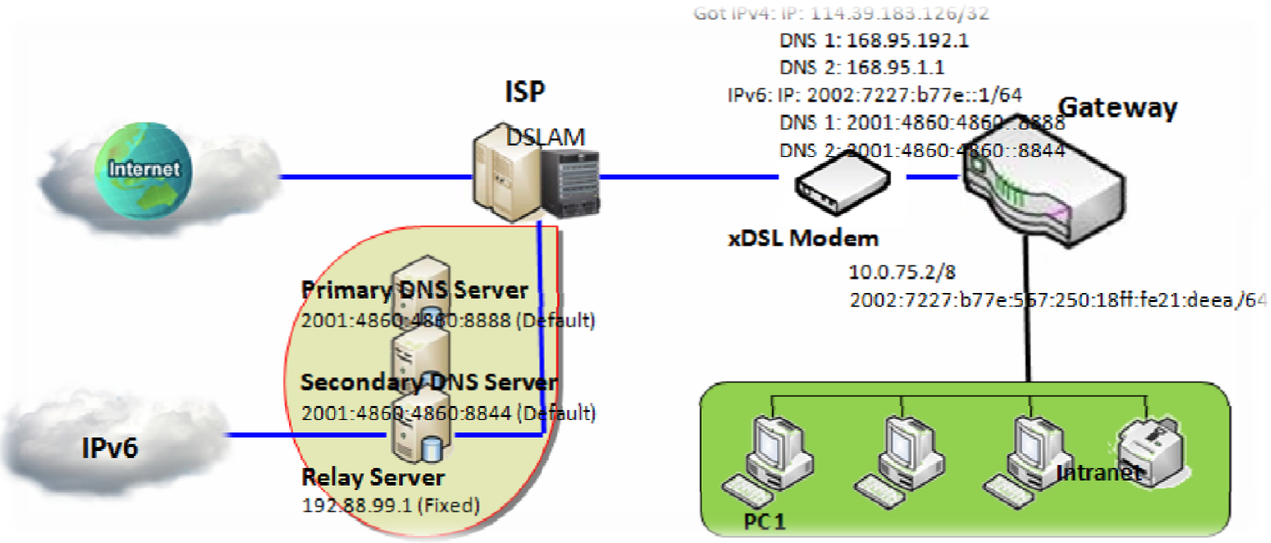


The diagram above depicts the IPv6 addressing through PPPoE, PPPoEv6 server (DSLAM) on the ISP side provides IPv6 configuration upon receiving PPPoEv6 client request. When PPPoEv6 server gets client request and successfully authenticates it, the server sends IP address, DNS server addresses and other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

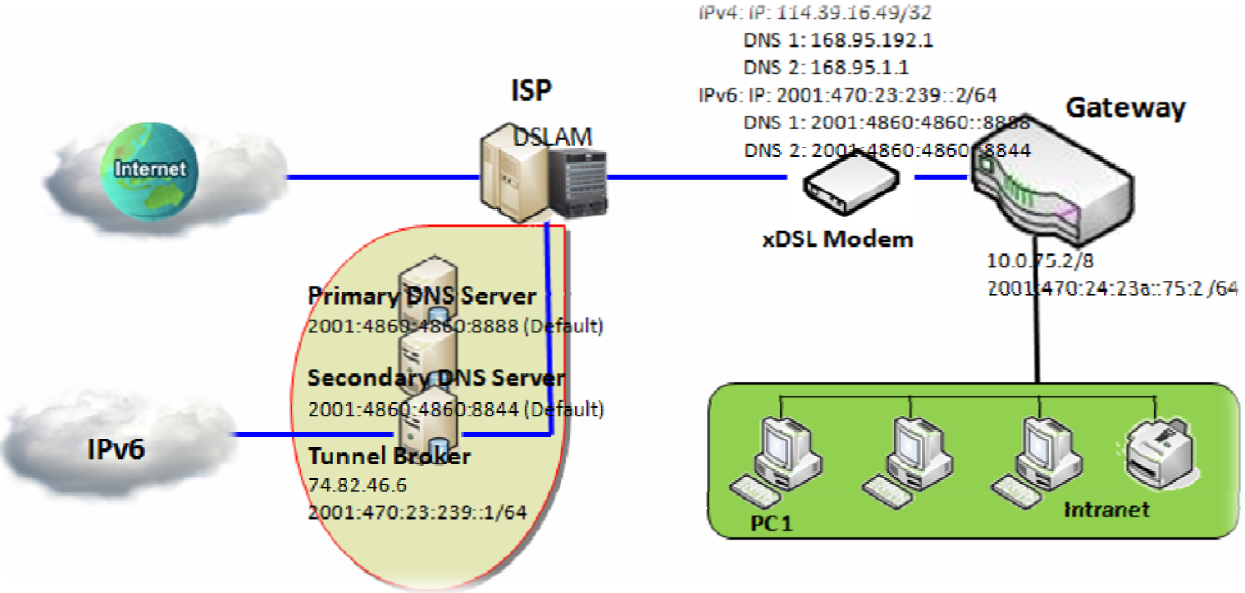
6to4 may be used by an individual host, or by a local IPv6 network. When used by a host, it must have a global IPv4 address connected, and the host is responsible for encapsulation of outgoing IPv6 packets and decapsulation of incoming 6to4 packets. If the host is configured to forward packets for other 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:557:250:18ff: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 anycast 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

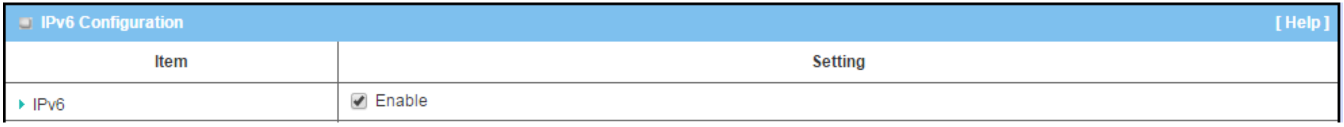
In above diagram, the 6in4 usually needs to register to a 6in4 tunnel service, known as Tunnel Broker, in order to use. It also need end point global IPv4 address as 114.39.16.49 to complete 6in4 setting.

3.7.1 IPv6 Configuration

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

Ensure IPv6 is enabled and saved

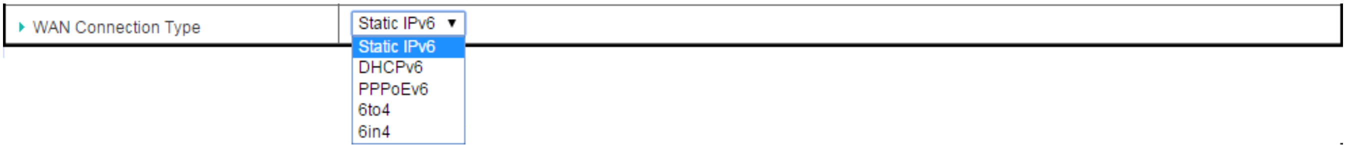
Go to Basic Network > IPv6 > Configuration Tab



IPv6 Configuration [Help]

Item	Setting
IPv6	☑ Enable

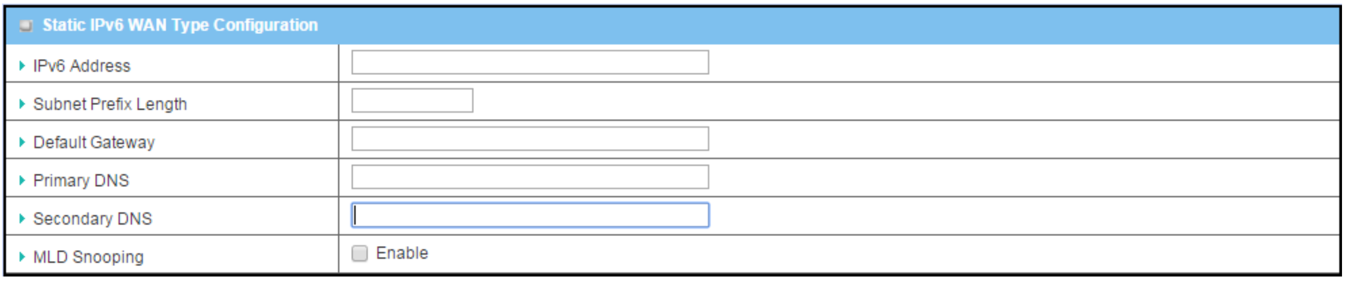
Select IPv6 WAN Connection Type



WAN Connection Type	Static IPv6 ▼

IPv6 Configuration		
Item	**Value setting**	**Description**
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

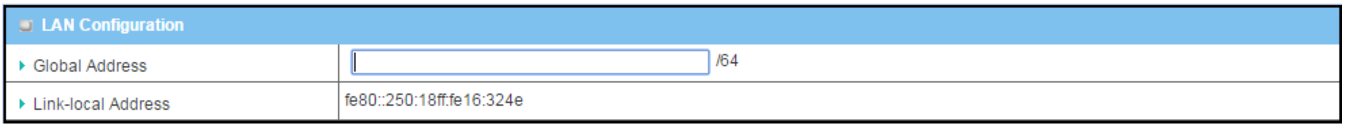


Static IPv6 WAN Type Configuration

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

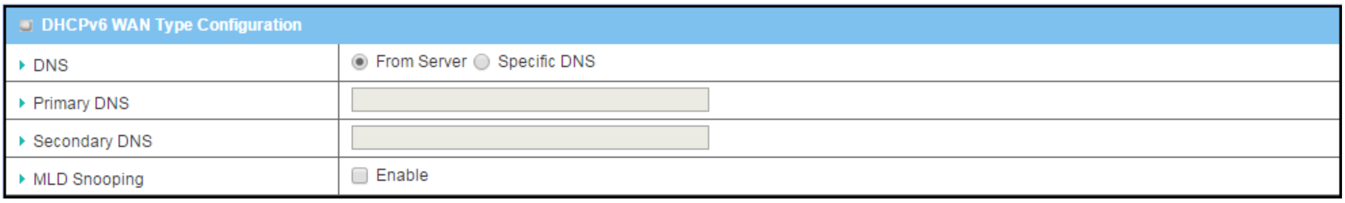
Global Address	/64
Link-local Address	fe80::250:18ff:fe16:324e

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 set, click the **save button** to save the configuration and click **reboot button** to reboot the router.

DHCPv6 WAN Type Configuration

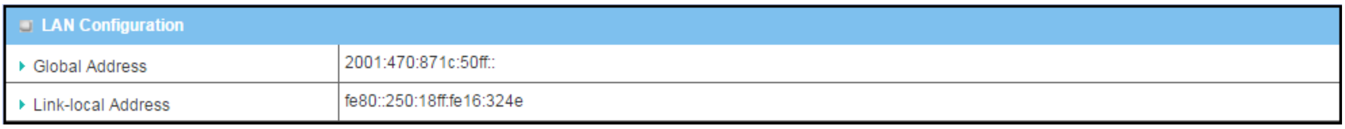


DHCPv6 WAN Type Configuration

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

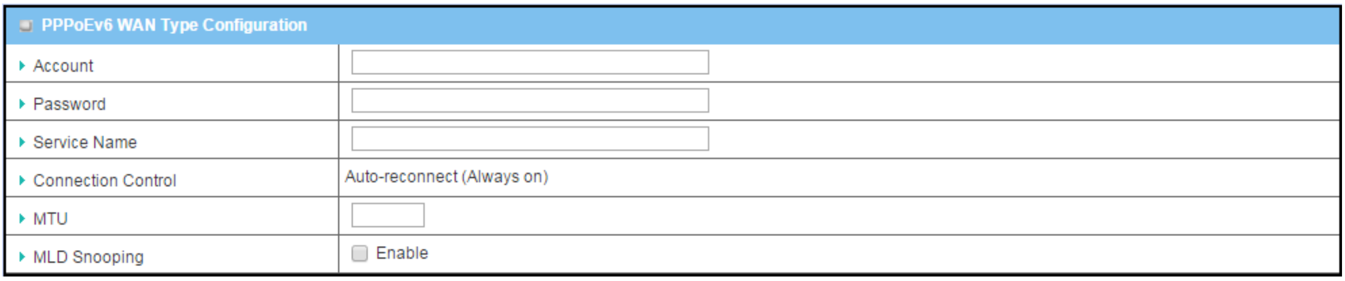
Global Address	2001:470:871c:50ff::
Link-local Address	fe80::250:18ff:fe16:324e

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 set, click the **save button** to save the configuration and click **reboot button** to reboot the router.

PPPoEv6 WAN Type Configuration

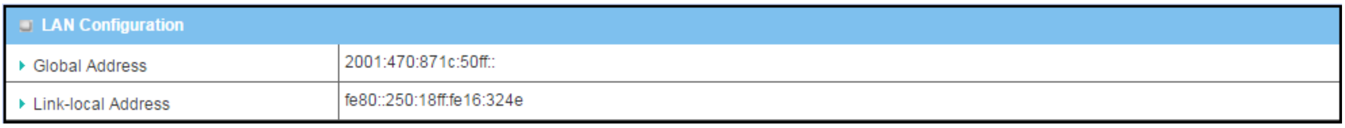


PPPoEv6 WAN Type Configuration

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	2001:470:871c:50ff::
Link-local Address	fe80::250:18ff:fe16:324e

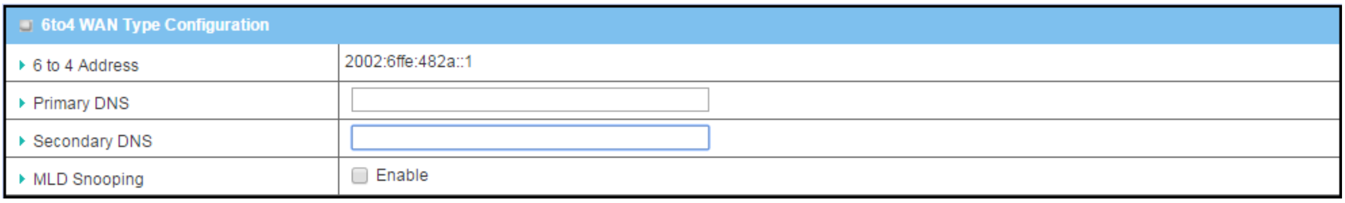
LAN Configuration		
Item	**Value setting**	**Description**
Global Address	Value auto-created	The LAN **IPv6 Address** for the router.
Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

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

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

Index skipping is used to reserve slots for new function insertion, when required.

6to4 WAN Type Configuration

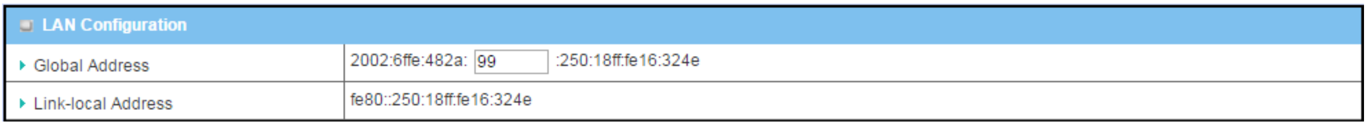


6to4 WAN Type Configuration

6 to 4 Address	2002:6ffe:482a::1
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	2002:6ffe:482a: 99 :250:18ff:fe16:324e
Link-local Address	fe80::250:18ff:fe16:324e

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.

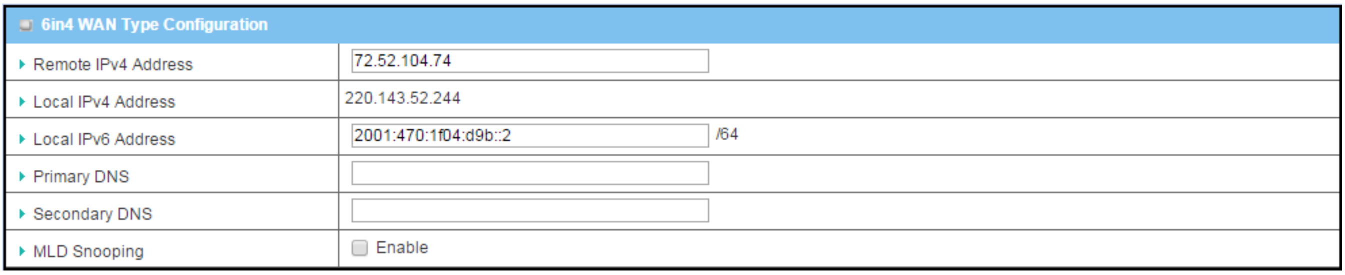
Then go to **Address Auto-configuration (summary)** for setting LAN environment.

If above setting is set, 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. (can find List of IPv6 tunnel brokers that support 6in4 service from wiki)

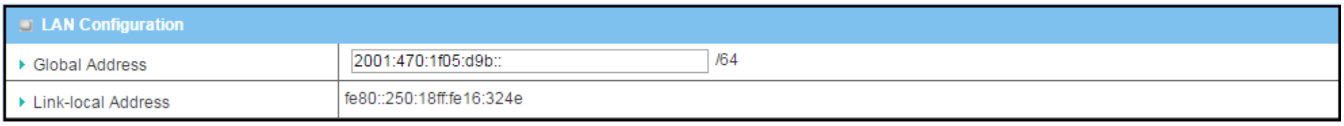
Then filled the **Local IPv4 address** of router into **Client IPv4 Address** field in IPv6 tunnel broker setting page.



6in4 WAN Type Configuration	
Remote IPv4 Address	72.52.104.74
Local IPv4 Address	220.143.52.244
Local IPv6 Address	2001:470:1f04:d9b::2 /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 tunnelbroker 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 tunnelbroker 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



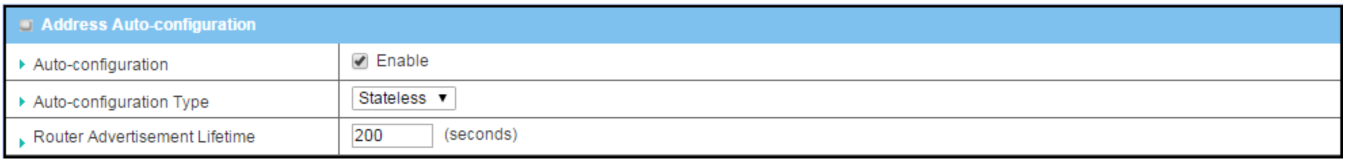
LAN Configuration	
Global Address	2001:470:1f05:d9b:: /64
Link-local Address	fe80::250:18ff:fe16:324e

LAN Configuration		
Item	**Value setting**	**Description**
Global Address	A Must filled setting	Filled **Routed /64** gotten from tunnelbroker in this field.
Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

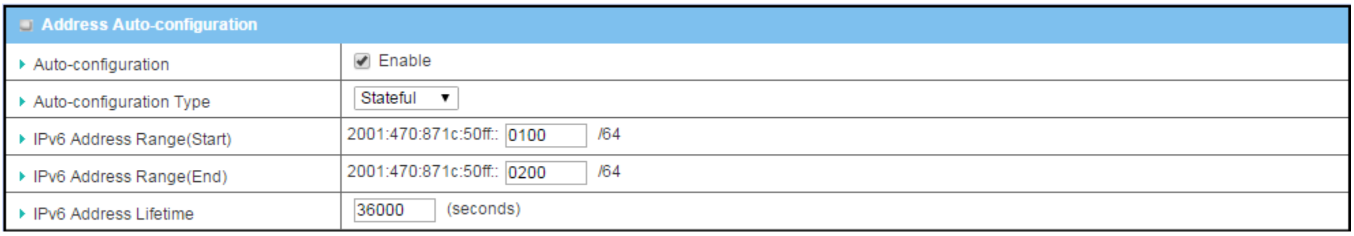
Then go to **Address Auto-configuration (summary)** for setting LAN environment.
If above setting is set, click the **save button** to save the configuration and click **reboot button** to reboot the router.

Index skipping is used to reserve slots for new function insertion, when required.

Address Auto-configuration (summary)



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)	2001:470:871c:50ff:: 0100 /64
IPv6 Address Range(End)	2001:470:871c:50ff:: 0200 /64
IPv6 Address Lifetime	36000 (seconds)

Address Auto-configuration Item	Value setting	Description
Auto-configuration	The box is unchecked by default	Check to enable the Autoconfiguration 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 NAT / Bridge

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. AMIT products embed and activate the NAT function by default except the Access Point series of products. You also can disable it in **[Basic Network]-[WAN]-[Internet Setup]-[WAN Type Configuration]**.

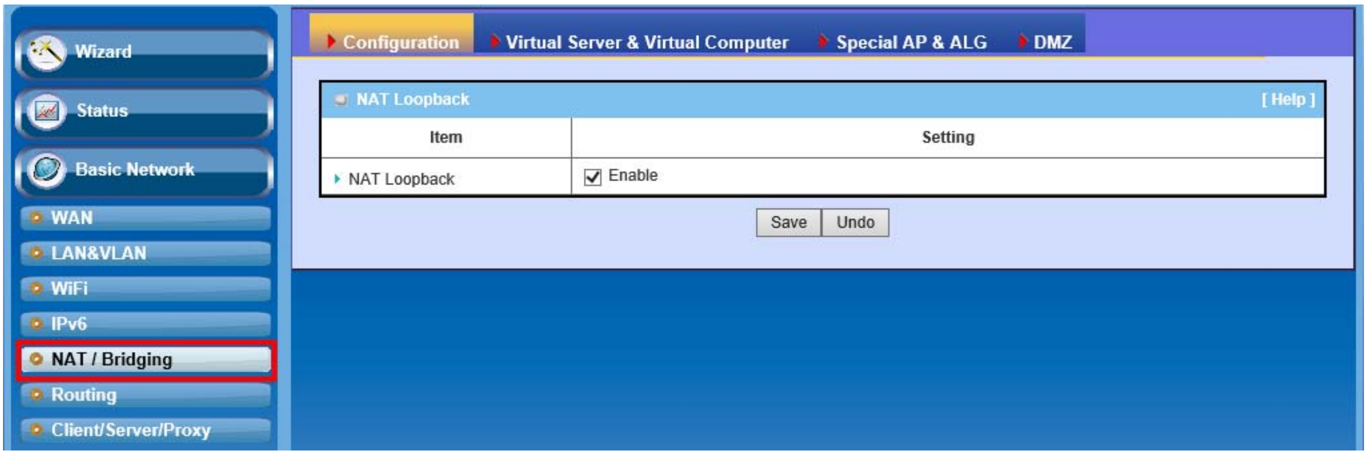
Following features are included in the NAT function: NAT Loopback, Virtual Server, Virtual Computer, Special AP, ALG and DMZ Host.

3.9.1 NAT Configuration

For gateway products, NAT function is activated by default. For device supporting multiple WAN interfaces, enabling and disabling NAT function can be done on each WAN. You can configure it in **[Basic Network]-[WAN]-[Internet Setup]-[WAN Type Configuration]** page.

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. In web-based utility, refer to "Configuration" page, for "NAT Loopback" feature which can be found in **[Basic Network]-[NAT/Bridging]-[Configuration]**. "Virtual Server" feature can be found in **[Basic Network]-[NAT/Bridging]-[Virtual Server & Virtual Computer]**.

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.

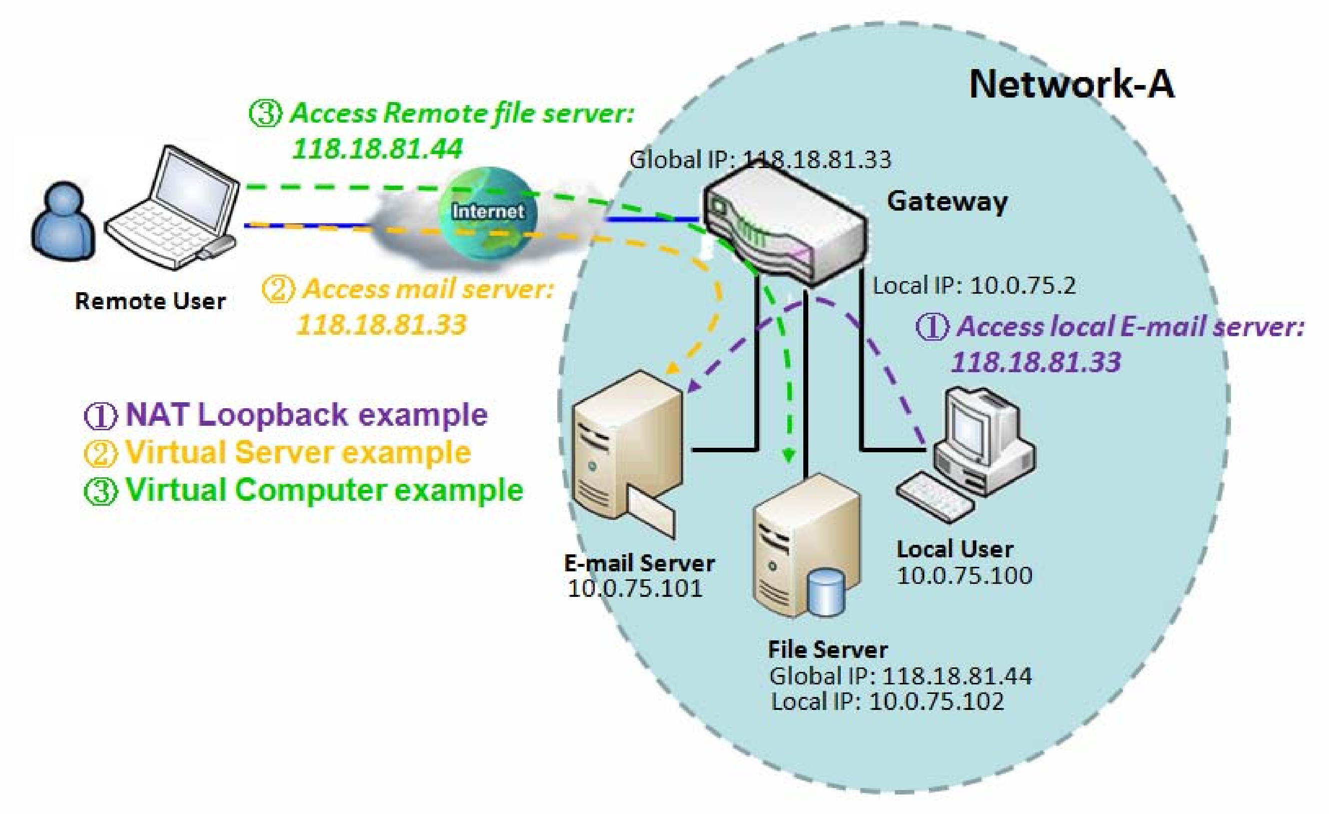


NAT Loopback

Item	Setting
NAT Loopback	☑ Enable

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 □ 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.

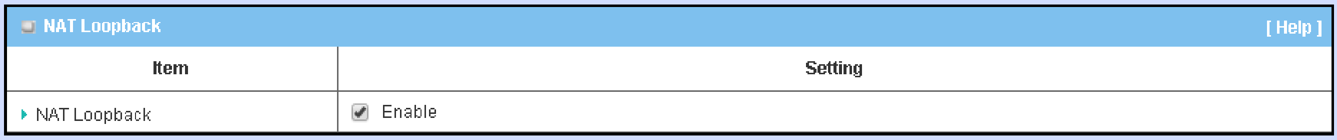
So, the local user at host with IP address 10.0.75.100 can access the E-mail server by using the global IP 118.18.81.33. But in reality the E-mail request packets from the local host will not reach the WAN interface, but just loop back to the E-mail server in the Intranet.

Index skipping is used to reserve slots for new function insertion, when required.

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

Enable NAT Loopback

Go to Basic Network > NAT / Bridging > Configuration tab



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

Index skipping is used to reserve slots for new function insertion, when required.

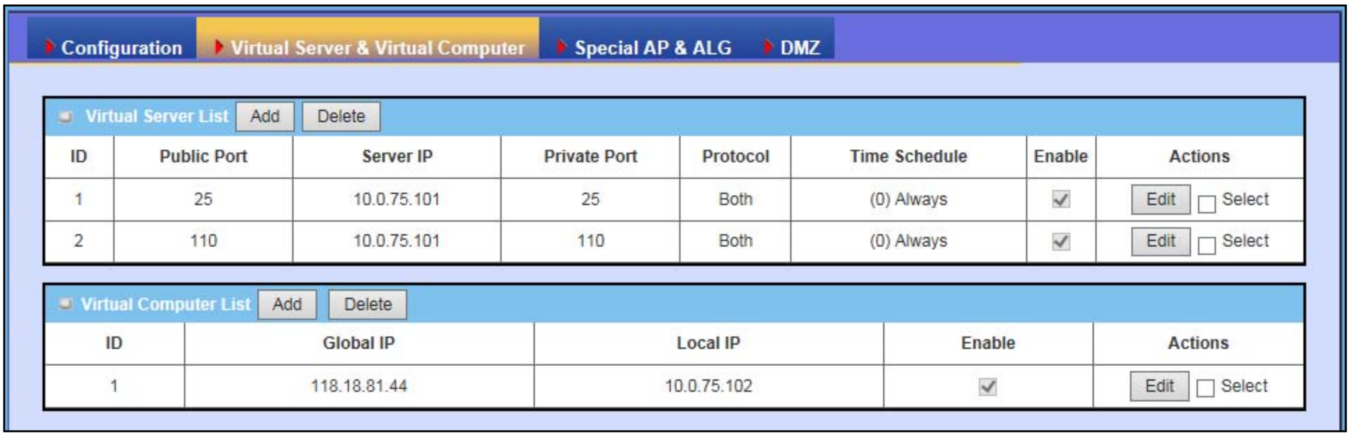
3.9.3 Virtual Server & Virtual Computer

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 a "Add" button for you to add and create new virtual computer, and the "Edit" button to modify the existed virtual computer.



Virtual Server List Add Delete

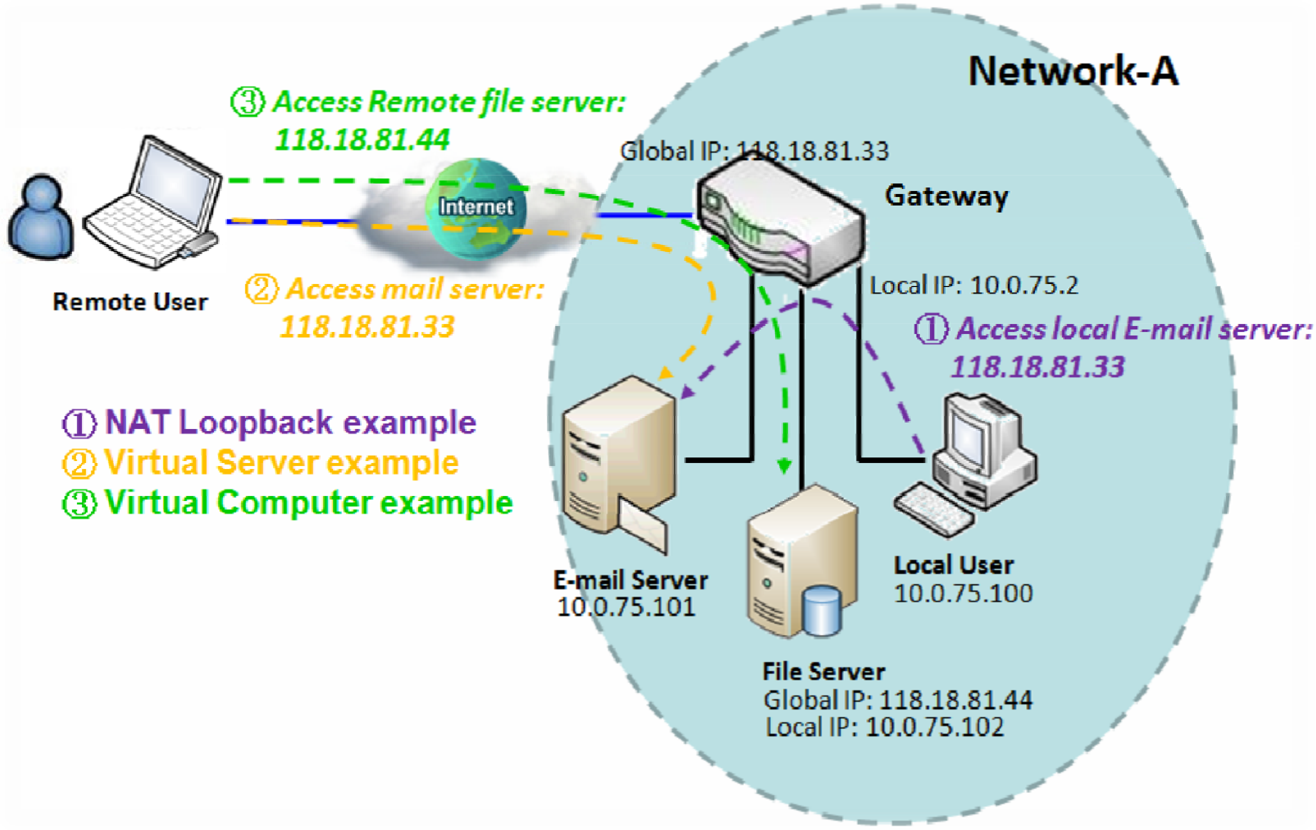
ID	Public Port	Server IP	Private Port	Protocol	Time Schedule	Enable	Actions
1	25	10.0.75.101	25	Both	(0) Always	☑	Edit □ Select
2	110	10.0.75.101	110	Both	(0) Always	☑	Edit □ Select

Virtual Computer List Add Delete

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

Virtual Server List

"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 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.

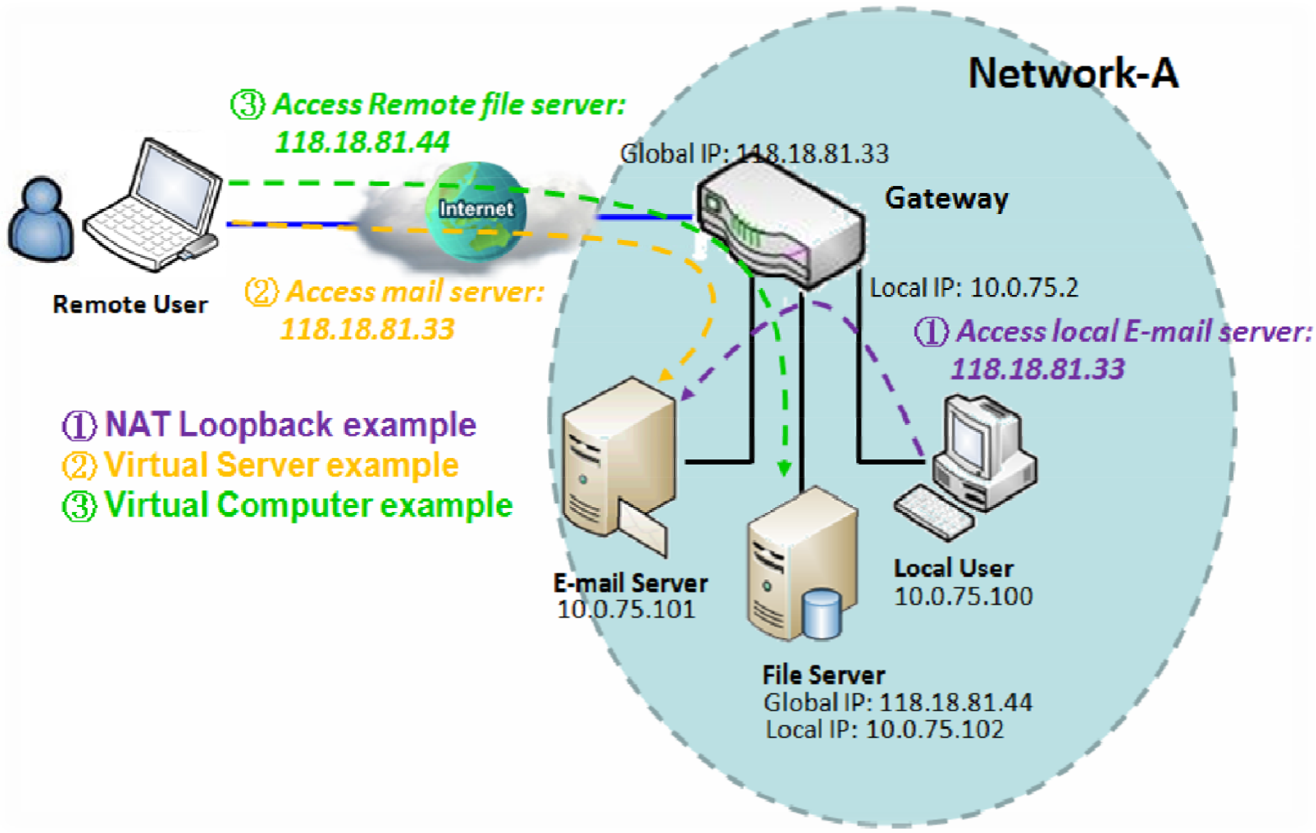
So, the remote user can access the E-mail server in the gateway that has the global IP 118.18.81.33 at its WAN side. But the real E-mail server is located at LAN side and the gateway is the port forwarder for E-mail service.

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 List

"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 □ of following diagram**.**

Index skipping is used to reserve slots for new function insertion, when required.



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.

Index skipping is used to reserve slots for new function insertion, when required.

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.

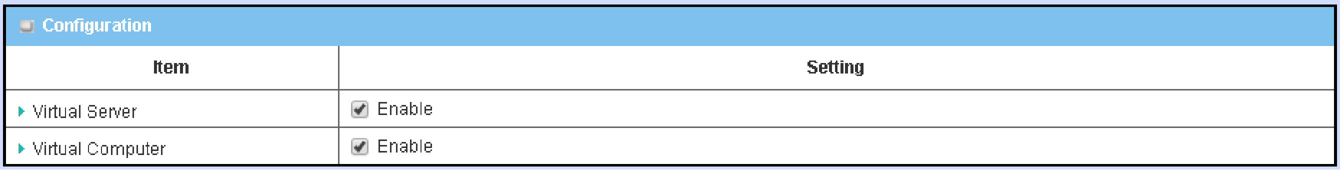
So remote users can request for file services from the FTP file server, even it is existed in a LAN host.

The Virtual Server setting allows user to redirect 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.

The Virtual Computer setting allows user to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple pairs of global IP address and local IP address.

Enable Virtual Server and Virtual Computer

Go to Basic Network > NAT / Bridging > Virtual Server & Virtual Computer tab



Configuration

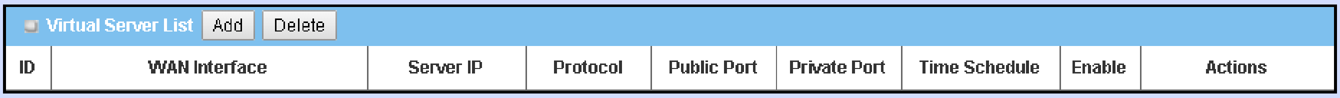
Item	Setting
Virtual Server	☑ Enable
Virtual Computer	☑ Enable

Configuration Item	Value setting	Description
Virtual Server	The box is unchecked by default	Check the **Enable** box to activate this NAT function
Virtual Computer	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.

Index skipping is used to reserve slots for new function insertion, when required.

Create/Edit Virtual Server

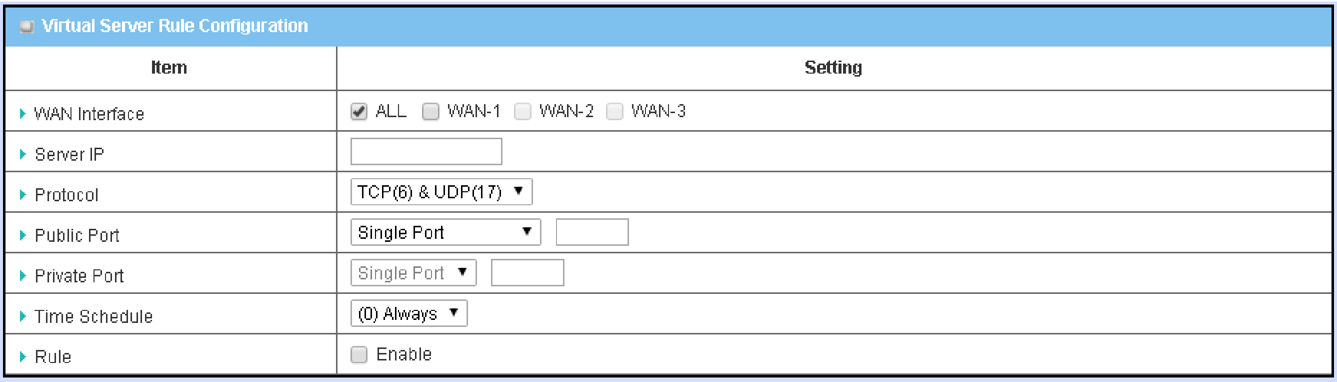
The router allows you to custom your Virtual Server rules. The router supports up to a maximum of 20 rule-based Virtual Server sets.



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
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 **System**) 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**

Index skipping is used to reserve slots for new function insertion, when required.

setting under **System)**

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 **System)**

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 **System)**

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 **System)**

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 **System)**

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 **System)**

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.

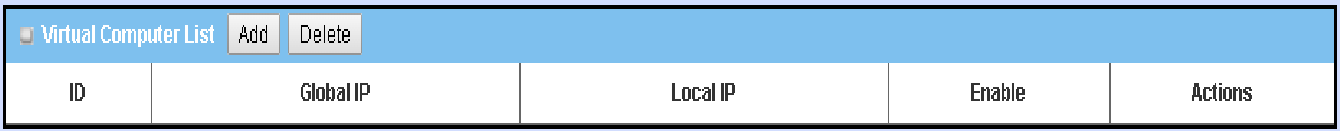
Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **System)**

Index skipping is used to reserve slots for new function insertion, when required.

		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.

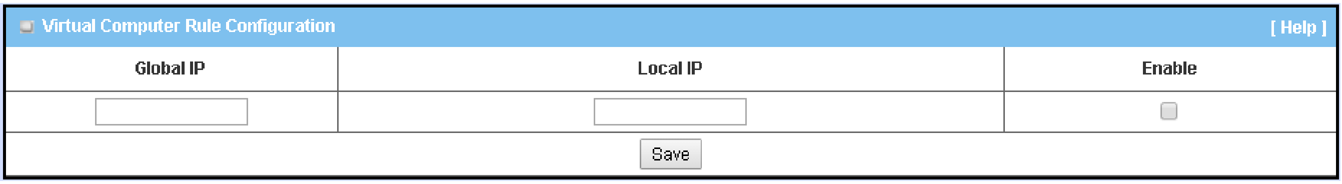
Create/Edit Virtual Computer

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
		□

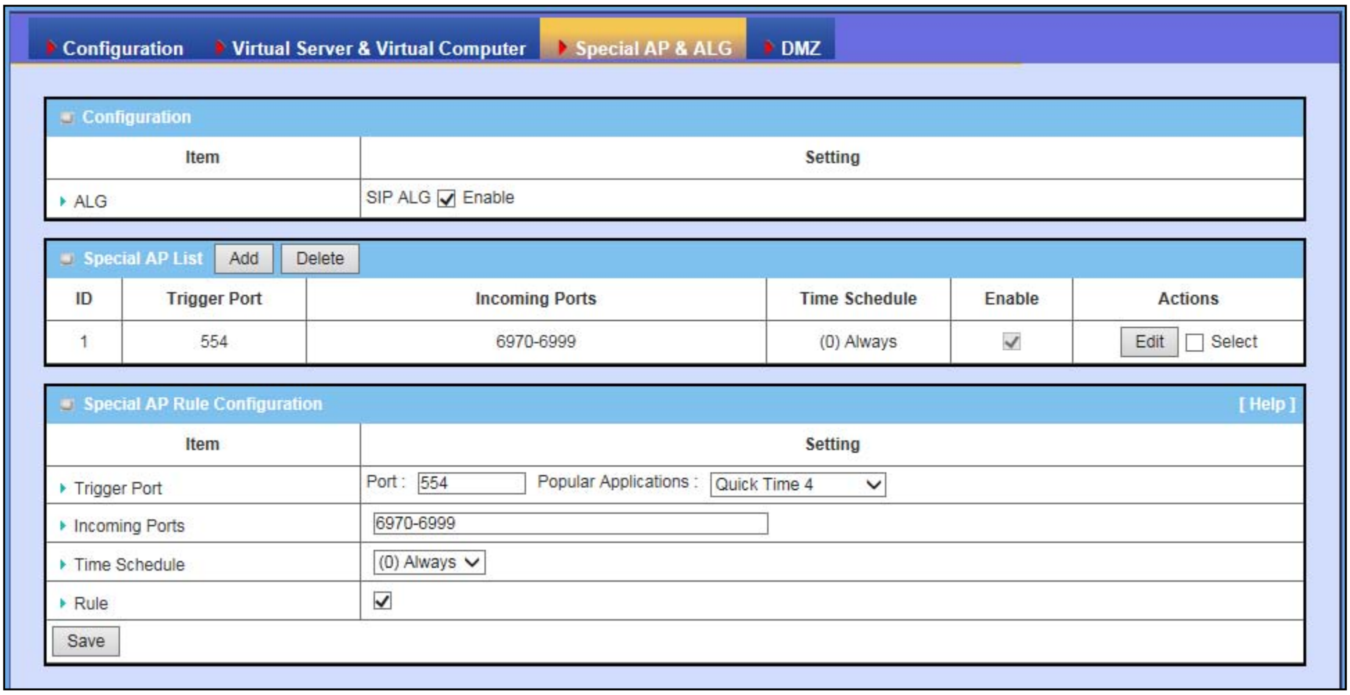
Virtual Computer Rule Configuration		
Item	**Value setting**	**Description**
Global IP	A Must filled setting	This field is to specify the IP address of the WAN IP.
Local IP	A Must filled setting	This field is to specify the IP address of the LAN IP.
Enable	N/A	Then check **Enable** box to enable this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

Index skipping is used to reserve slots for new function insertion, when required.

3.9.5 Special AP & ALG

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

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



Configuration

Item	Setting
ALG	SIP ALG ☑ Enable

Special AP List

ID	Trigger Port	Incoming Ports	Time Schedule	Enable	Actions
1	554	6970-6999	(0) Always	☑	Edit □ Select

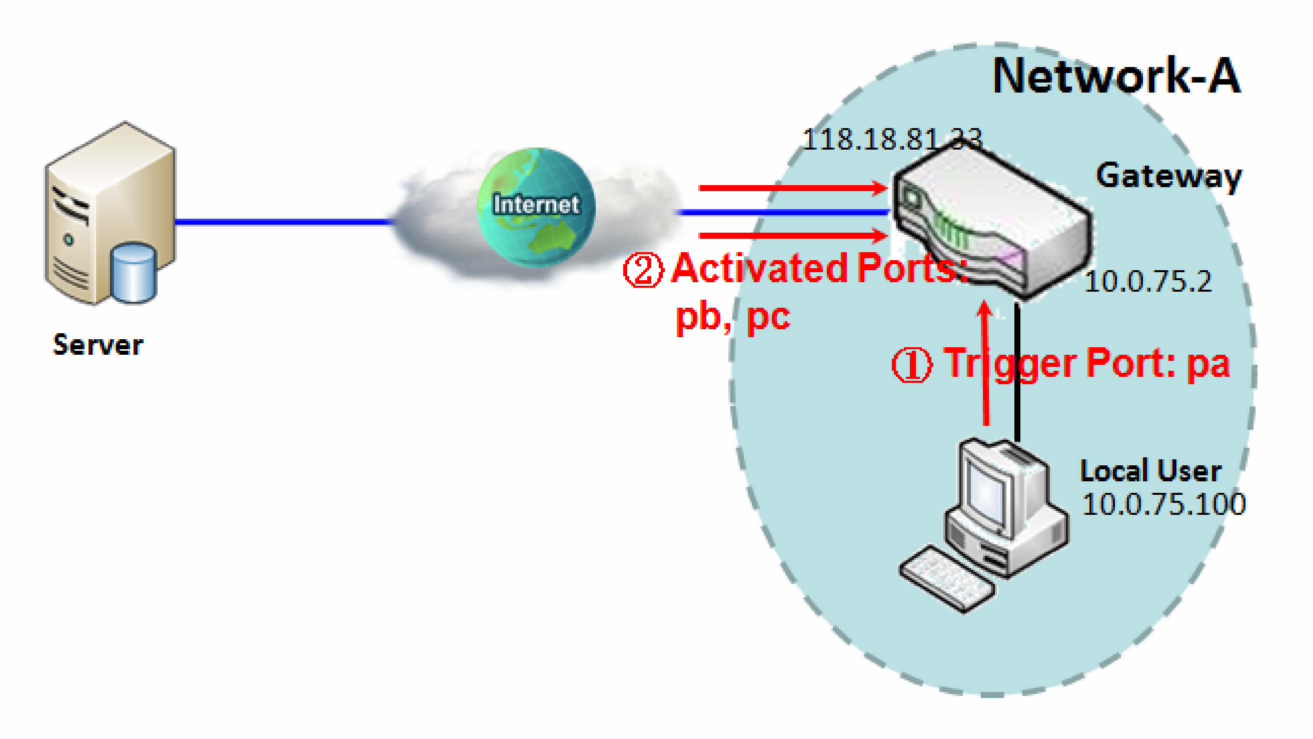
Special AP Rule Configuration

Item	Setting
Trigger Port	Port : 554 Popular Applications : Quick Time 4
Incoming Ports	6970-6999
Time Schedule	(0) Always
Rule	☑

In "Special AP & ALG" page, there is one configuration window for "ALG" feature. The gateway provides "SIP ALG" here. In addition, there also be one "Special AP List" window to list all your defined special applications. Using "Add" or "Edit" button to add and create one new special application or to modify an existed one. When "Add" or "Edit" button is applied the "Special AP Rule Configuration" window will appear to let you define a application rule. The parameters include the trigger port, the allowed incoming ports, the integrated time schedule rule, and the rule activation.

Special AP List

This feature allows you to request the gateway open a pre-defined set range service ports for incoming packets to pass through once the trigger port is toggled in the gateway by the Intranet packets. As shown in following diagram, one defined special application rule is that the trigger port is ***pa*** and the activated ports are ***pb*** and ***pc*** once the ***pa*** port is toggled at LAN interface of gateway.



Scenario Application Timing

When local user wants to run an application to access the server in the Internet and the application need more than one connection session with different service ports to finish its function. You can define one special application rule for it. The rule can be integrated with one schedule rule. That is, the special application rule can be activated only at the pre-defined schedule.

Scenario Description

Local user runs an application to access the Internet server by a trigger packet with the dedicated destination port.

Gateway opens more service ports for incoming packets to pass through the gateway into the Intranet from the Internet if the application requires.

Parameter Setup Example

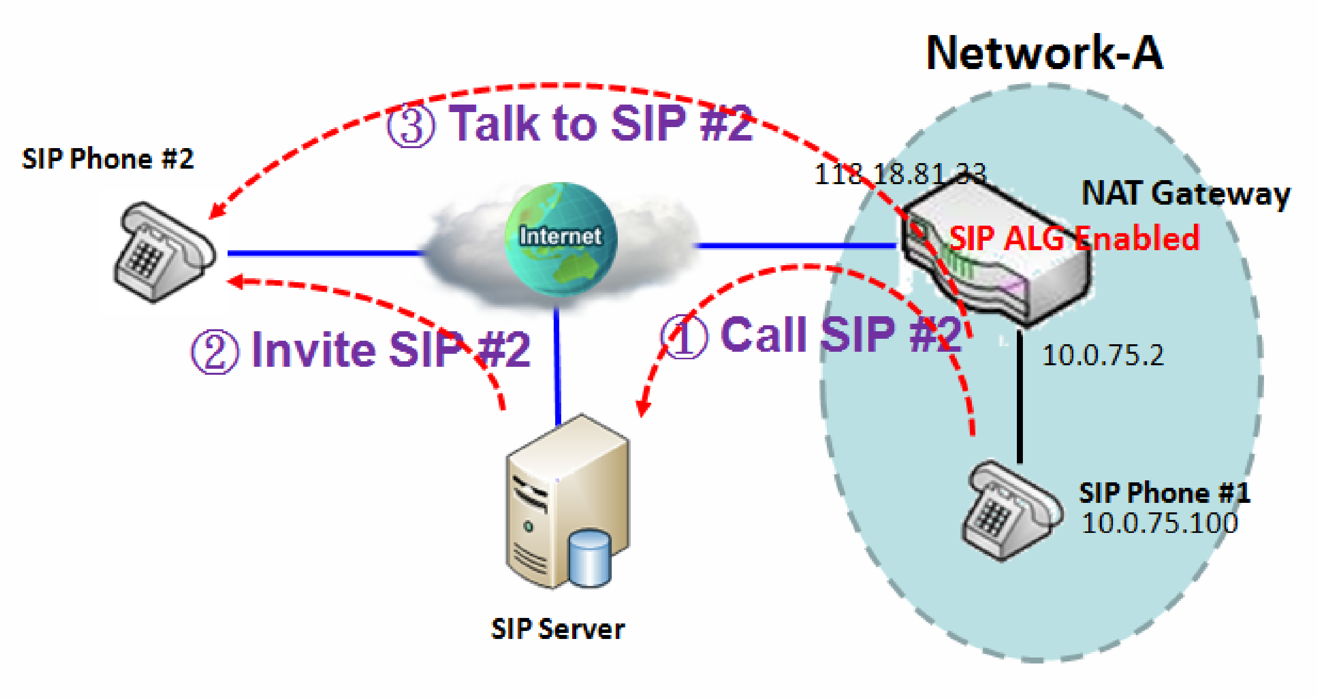
Following table lists the parameter configuration as an example for the gateway in above diagram with one special application rule to be defined.
Use default value for those parameters that are not mentioned in the table.

Configuration Path	[Special AP & ALG]-[Special AP List]
ID	***1***
Trigger Port	***554 (Quick Time 4)***
Incoming Ports	***6970-6999***
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.
Define a special application rule with the trigger port 554 (Quick Time 4) and incoming ports 6970-6999, and activate the rule.
So, the local user at host with IP address 10.0.75.100 can enjoy the music by using Quick Time 4 application. The media server is in the Internet.

ALG Configuration

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



Scenario Application Timing

When a SIP phone is behind a NAT gateway, and it is expected to make a call to or receive a call from the Internet. The "SIP ALG" feature must be activated in the NAT gateway.

Scenario Description

The "SIP ALG" feature in the NAT Gateway is enabled to monitor, open up ports and make the address and port translation for the voice communication of the SIP phone behind the gateway.

A SIP phone behind a NAT gateway can call another SIP phone with the help of the SIP server in the Internet.

Parameter Setup Example

Following table lists the parameter configuration for the NAT gateway in above diagram.

Configuration Path	[Special AP & ALG]-[Configuration]
ALG	**SIP ALG ■ *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 the NAT gateway with SIP ALG being enabled.

When the SIP Phone #1 behind the NAT gateway has booted up, it will register to the SIP server in the Internet. So, the SIP server knows where the SIP Phone #1 is. In the same way, the SIP Phone #2 also registers to the SIP server.

A local user wants to make one call to the SIP Phone #2 by using the SIP Phone #1, the NAT Gateway will monitor the calling process, open up required service ports for incoming packets and make the address and port translation for the voice communication.

First, the calling starts from the SIP Phone #1 to the SIP server. Then the SIP server invites the SIP Phone #2 and finally, the SIP Phone #1 talks to the SIP Phone #2, as shown in above diagram.

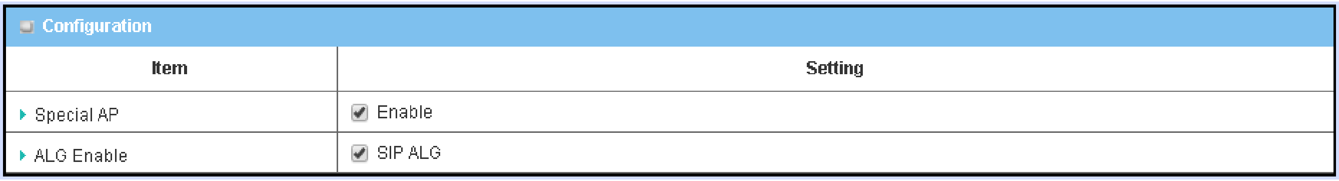
Special AP & ALG Setting

The Special AP setting allows some applications require multiple connections.

The ALG setting allows user to Support some SIP ALG, like STUN.

Enable Special AP and Virtual Computer

Go to Basic Network > NAT/ Bridging > Special AP & ALG tab



Configuration

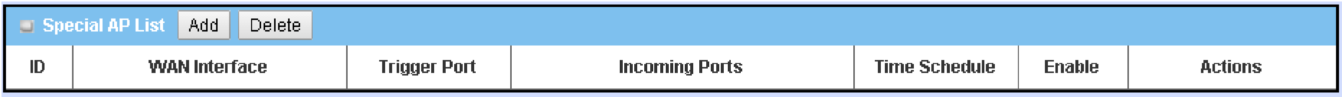
Item	Setting
Special AP	☑ Enable
ALG Enable	☑ SIP ALG

Special AP & ALG tab		
Item	**Value setting**	**Description**
Special AP	The box is checked by default	Check the **Enable** box to activate this NAT function
ALG Enable	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 setting
Undo	N/A	Click **Undo** to cancel the settings

Index skipping is used to reserve slots for new function insertion, when required.

Create/Edit Special AP

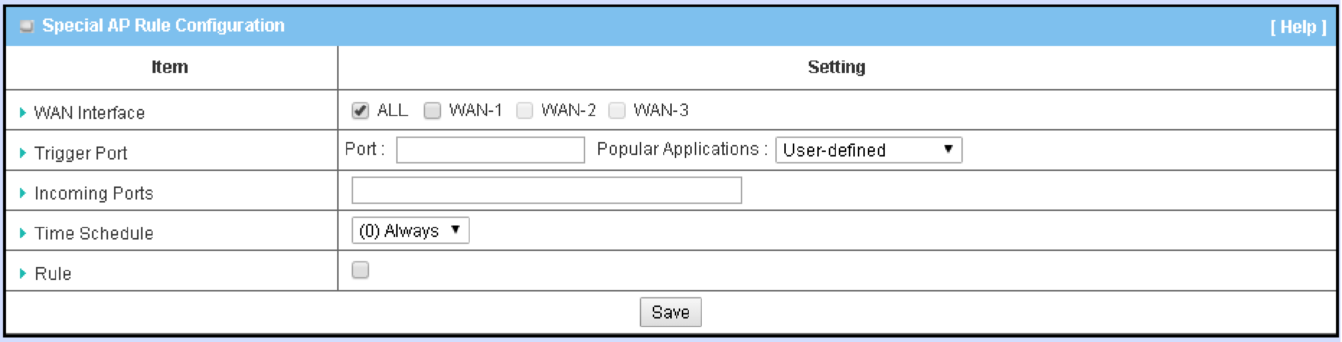
The router allows you to custom your Special AP rules. The router supports up to a maximum of 8 rule-based Special AP sets.



Special AP List   Add   Delete

ID	WAN Interface	Trigger Port	Incoming Ports	Time Schedule	Enable	Actions

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



Special AP Rule Configuration   [Help]

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

Save

Special AP List

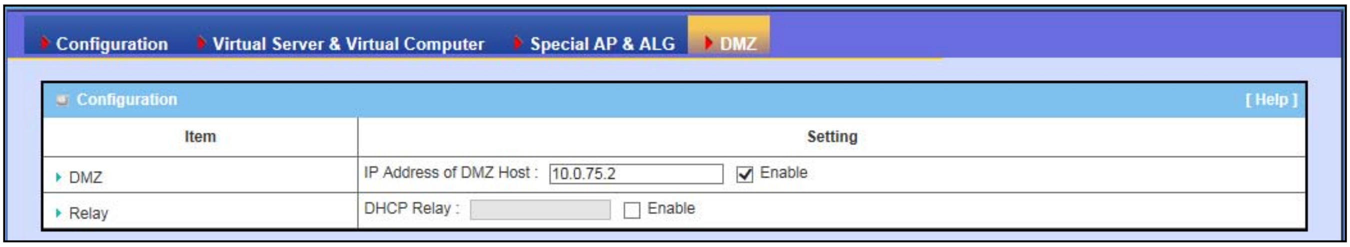
Item	Value setting	Description
WAN Interface	1. A Must filled setting 2. Default is **ALL**.	Define the selected interface to be the packet-entering interface of the router. If the packets to be filtered are coming from **WAN-x** then select **WAN-x** for this field. Select **ALL** for packets coming into the router from any interfaces. It can be selected **WAN-x** box when **WAN-x** enabled.
Trigger Port	A Must filled setting	When Popular Applications is selected "User-defined" **Port** is set a port number, and **Incoming Ports** can be set a port number or a port range. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. (refer to **Scheduling setting** under **System**) Then check **Rule** box to enable this rule. When Popular Applications is selected "Battle.net" **Port** and **Incoming Ports** will be defined automatically. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. (refer to **Scheduling setting** under **System**) Then check **Rule** box to enable this rule. When Popular Applications is selected "Dialpad" **Port** and **Incoming Ports** will be defined automatically. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. (refer to **Scheduling setting** under **System**) Then check **Rule** box to enable this rule.

Index skipping is used to reserve slots for new function insertion, when required.

		When Popular Applications is selected “ICU II” Port is the same with Incoming Ports. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **System)** Then check **Rule** box to enable this rule. When Popular Applications is selected “MSN Gaming Zone” Port is the same with Incoming Ports. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **System)** Then check **Rule** box to enable this rule. When Popular Applications is selected “PC-to-Phone” Port is the same with Incoming Ports. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **System)** Then check **Rule** box to enable this rule. When Popular Applications is selected “Quick Time 4” Port is the same with Incoming Ports. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **System)** Then check **Rule** box to enable this rule.
Save	N/A	Click **Save** to save the settings.

3.9.7 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.

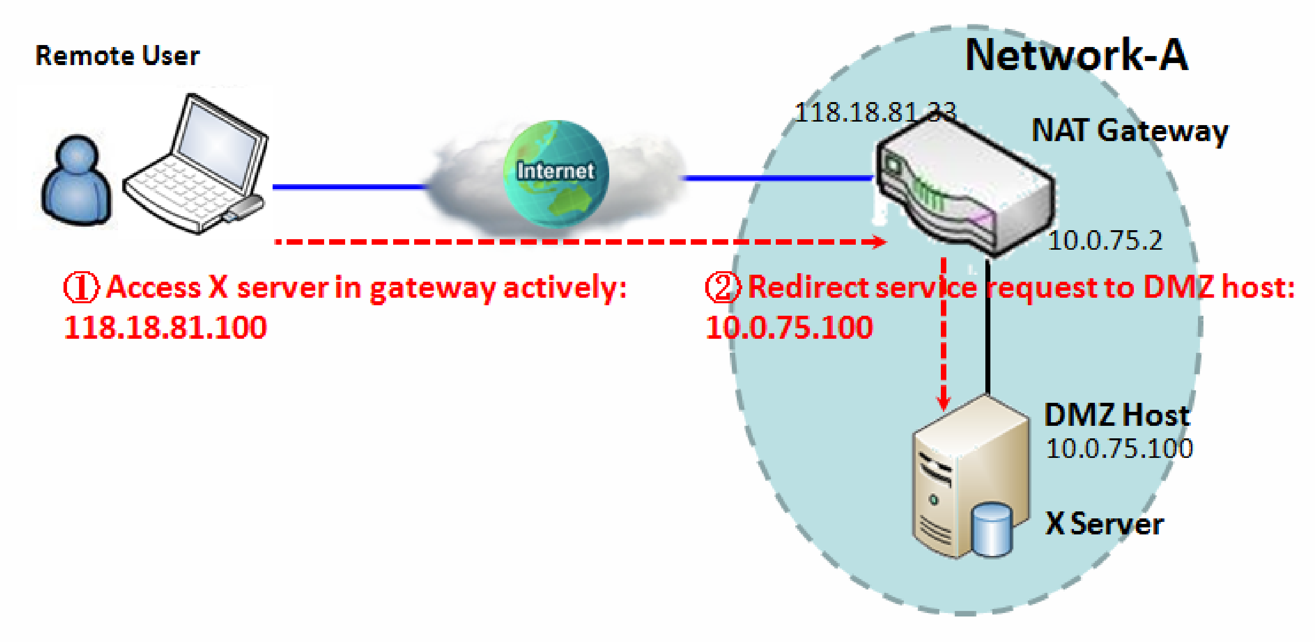


Item	Setting
DMZ	IP Address of DMZ Host : 10.0.75.2 ☑ Enable
Relay	DHCP Relay : ☐ Enable

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.

Configuration

This feature 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.



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***

Index skipping is used to reserve slots for new function insertion, when required.

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.

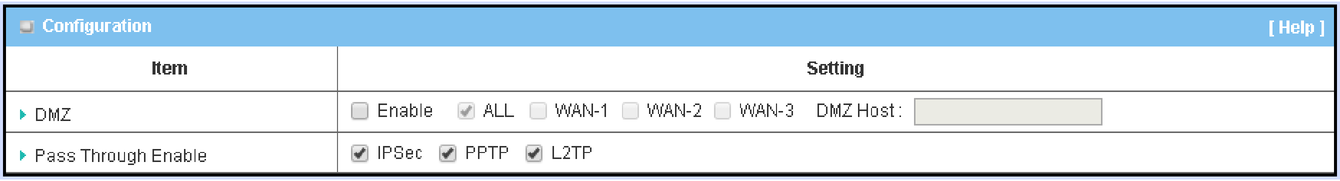
Assume there is an X server installed in the DMZ host. Then, the remote user can request services from the X server in the DMZ host by skipping the NAT checking by the gateway.

DMZ & Pass Through Setting

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

Enable DMZ and Pass Through Enable

Go to Basic Network > NAT / Bridging > DMZ tab



Configuration [Help]

Item	Setting
DMZ	□ Enable ☑ ALL □ WAN-1 □ WAN-2 □ WAN-3 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 NAT 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 box is checked by IPSec, PPTP, L2TP	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

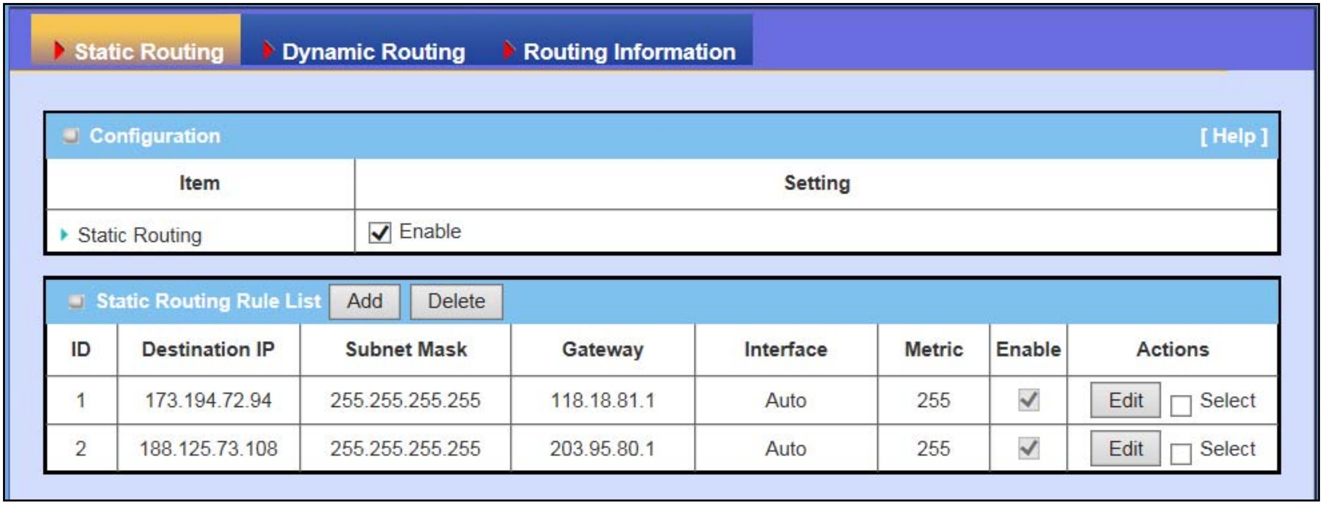
3.b Routing

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.



Item	Setting
Static Routing	☑ Enable

ID	Destination IP	Subnet Mask	Gateway	Interface	Metric	Enable	Actions
1	173.194.72.94	255.255.255.255	118.18.81.1	Auto	255	☑	Edit □ Select
2	188.125.73.108	255.255.255.255	203.95.80.1	Auto	255	☑	Edit □ Select

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.

Configuration

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

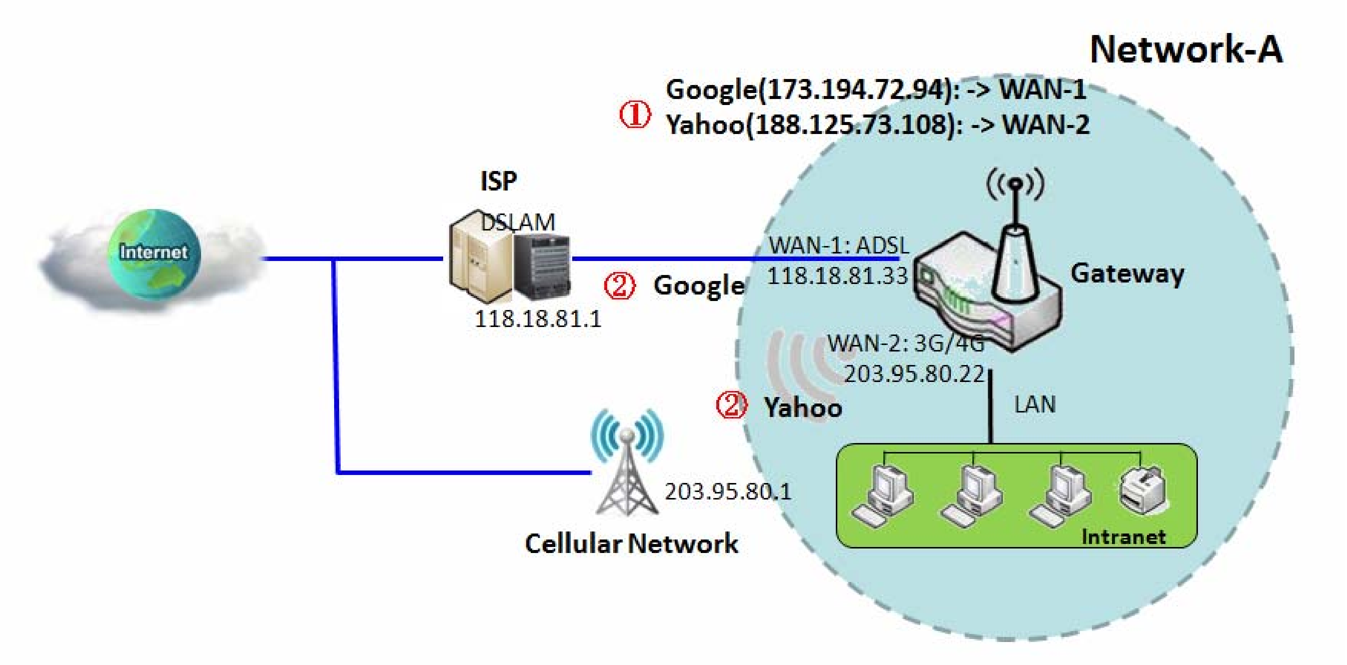
Static Routing Rule List

The Static Routing Rule List shows the setup parameters of all static routing rule enteries. There also be one "Add" button at the "Static Routing Rule List" caption, that can let you add one new static routing rule. While the "Edit" button at the end of each static routing rule can let you modify the rule.

Static Routing Rule Configuration

To configure one 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. Following diagram is an example.

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.

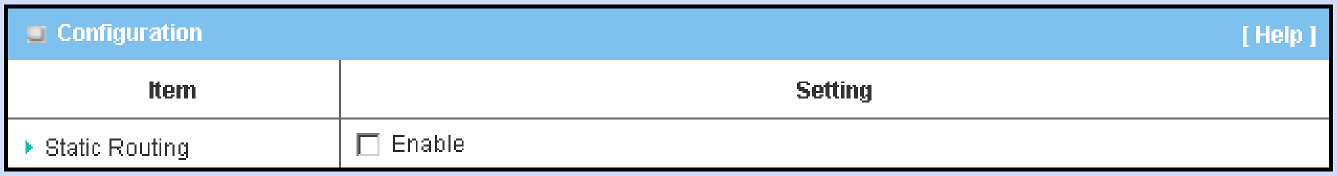
System will route the packets from the Intranet to Google site and Yahoo site based on above settings.

Index skipping is used to reserve slots for new function insertion, when required.

Static Routing Setting

The static routing setting allows user to create and customize static routing rules through the router based on their office setting.

Go to Basic Network > Routing > Static Routing Tab



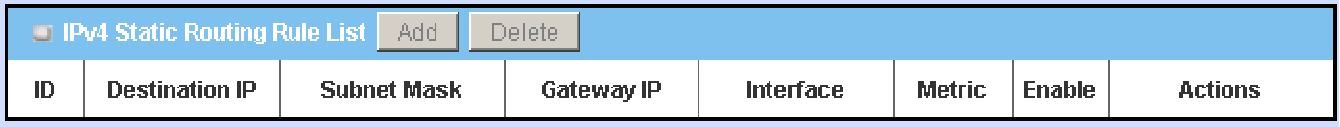
Configuration [Help]

Item	Setting
Static Routing	□ Enable

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

Create/Edit Static Routing Rules

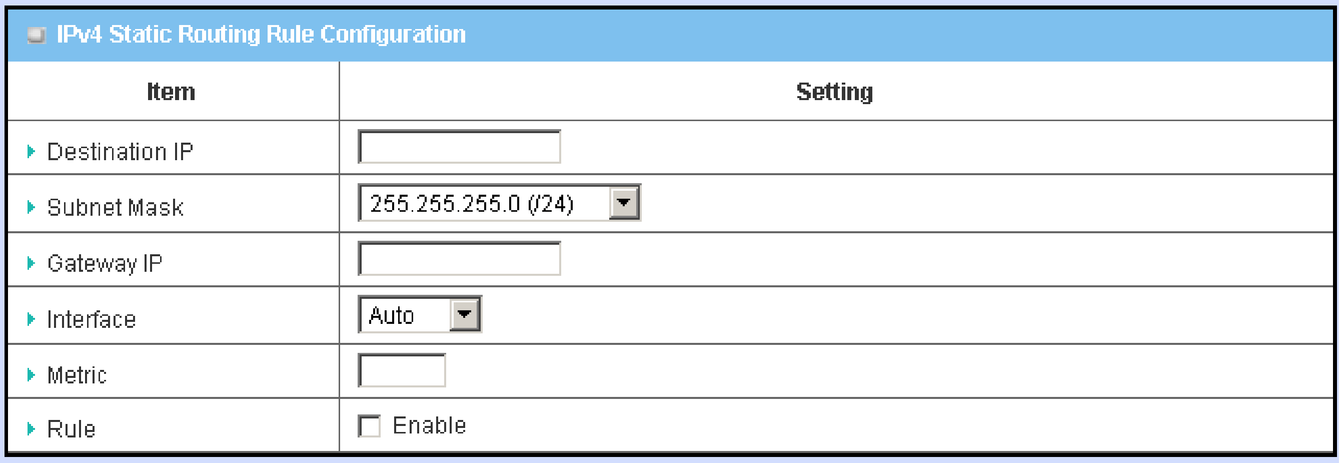
The router allows you to custom your static routing rules. It supports up to a maximum of 64 rule sets.



IPv4 Static Routing Rule List

ID	Destination IP	Subnet Mask	Gateway IP	Interface	Metric	Enable	Actions

When Add button is applied Static Routing Rule Configuration screen will appear.



IPv4 Static Routing Rule Configuration

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

Index skipping is used to reserve slots for new function insertion, when required.

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.
Enabling the rule	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. 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

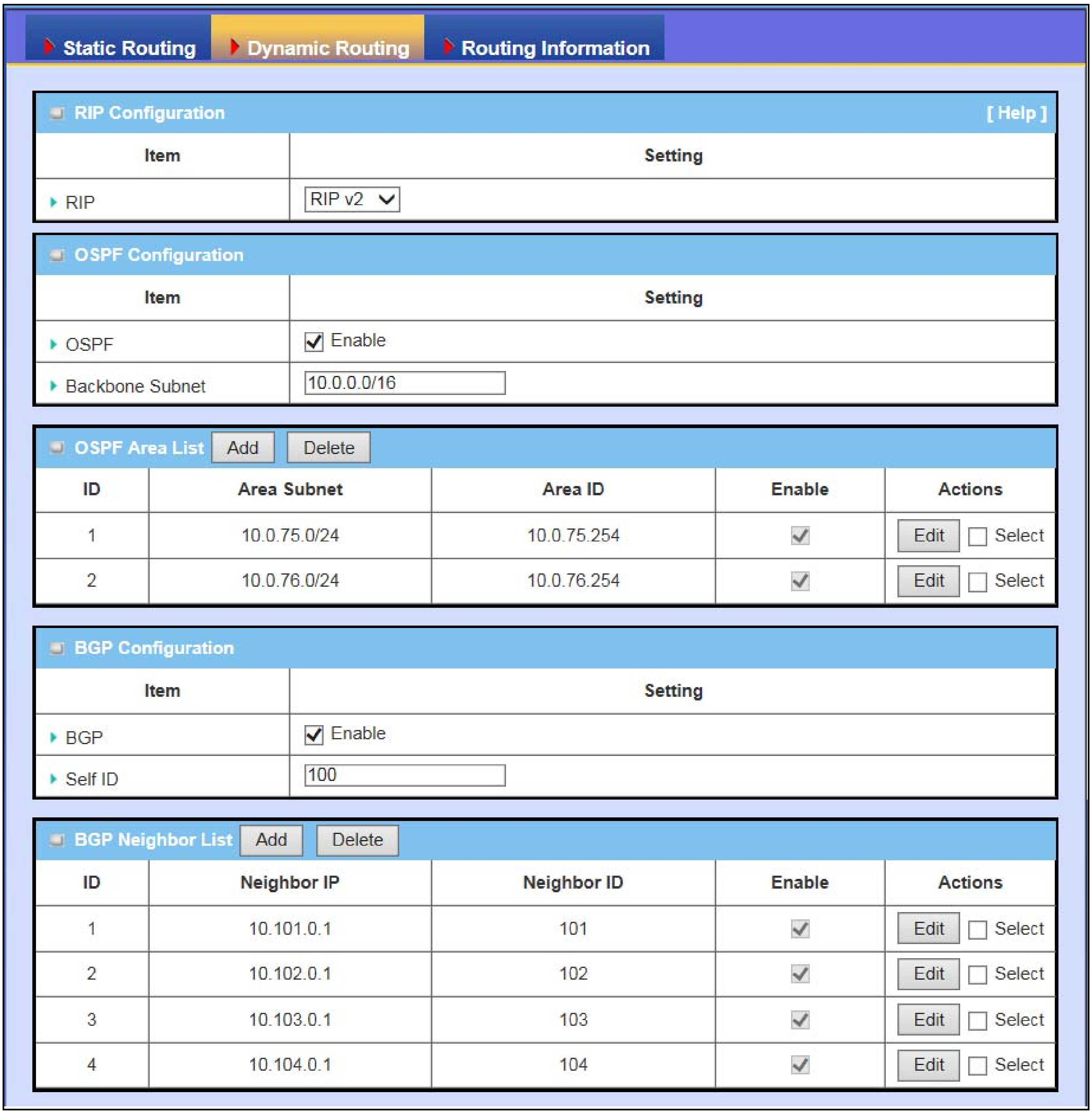
Dynamic Routing, also called adaptive routing, describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in network conditions. The adaptation is intended to allow as many routes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

This gateway supports dynamic routing protocol, such as RIPv1/RIPv2 (Routing Information Protocol), OSPF (Open Shortest Path First), 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.

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. Using the "Add" button to add and create one new OSPF area and the "Edit" button to modify an existed one. Creation and modification can be done in the "OSPF Area Configuration" window. 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. By using the "Add" button to add and create one new BGP neighbor and the "Edit" button to modify an existed one. You can do them in the "BGP Neighbor Configuration" window.

Index skipping is used to reserve slots for new function insertion, when required.



RIP Configuration [Help]

Item	Setting
RIP	RIP v2

OSPF Configuration

Item	Setting
OSPF	☑ Enable
Backbone Subnet	10.0.0.0/16

OSPF Area List Add Delete

ID	Area Subnet	Area ID	Enable	Actions
1	10.0.75.0/24	10.0.75.254	✓	Edit □ Select
2	10.0.76.0/24	10.0.76.254	✓	Edit □ Select

BGP Configuration

Item	Setting
BGP	☑ Enable
Self ID	100

BGP Neighbor List Add Delete

ID	Neighbor IP	Neighbor ID	Enable	Actions
1	10.101.0.1	101	✓	Edit □ Select
2	10.102.0.1	102	✓	Edit □ Select
3	10.103.0.1	103	✓	Edit □ Select
4	10.104.0.1	104	✓	Edit □ Select

These three 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 holddown mechanisms to prevent incorrect routing information from being propagated.

RIP Configuration

In the "RIP Configuration" window, you can just choose the version of RIP protocol to activate the dynamic routing feature, or disable it.

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 unitless 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.

OSPF Configuration

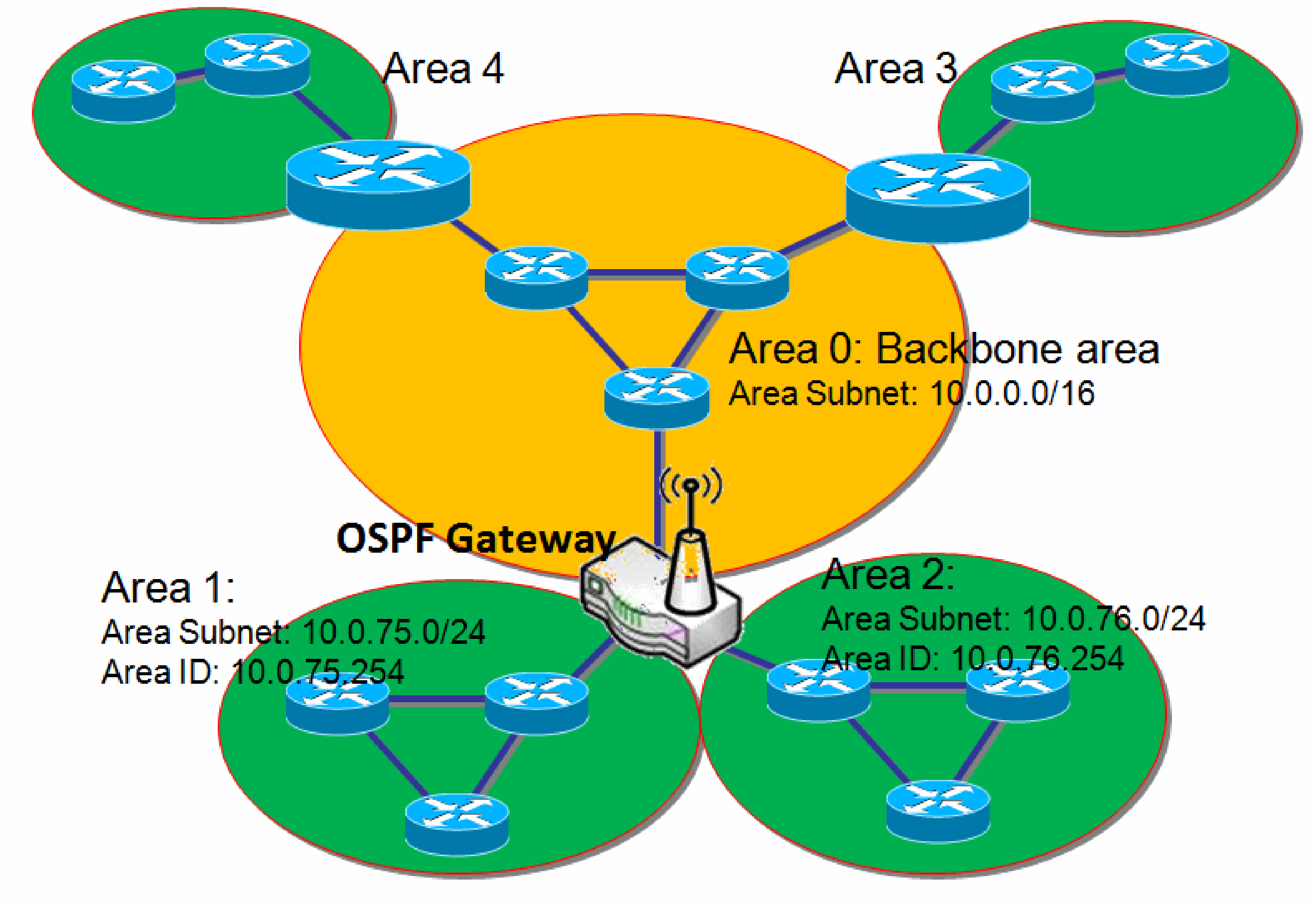
In the "OSPF Configuration" window, you can just check the "Enable" box to activate the OSPF dynamic routing protocol and specify its backbone subnet.

OSPF Area List

The OSPF Area List shows all OSPF area definition. There also be one "Add" button at the "OSPF Area List" caption to allow you to add one new OSPF area. The "Edit" button at the end of each OSPF area definition can let you modify it.

OSPF Area Configuration

To configure one OSPF area, you must specify related parameters including the area subnet, the area ID and area activation by an "Enable" box. Following diagram is an example for the scenario.



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.

BGP Configuration

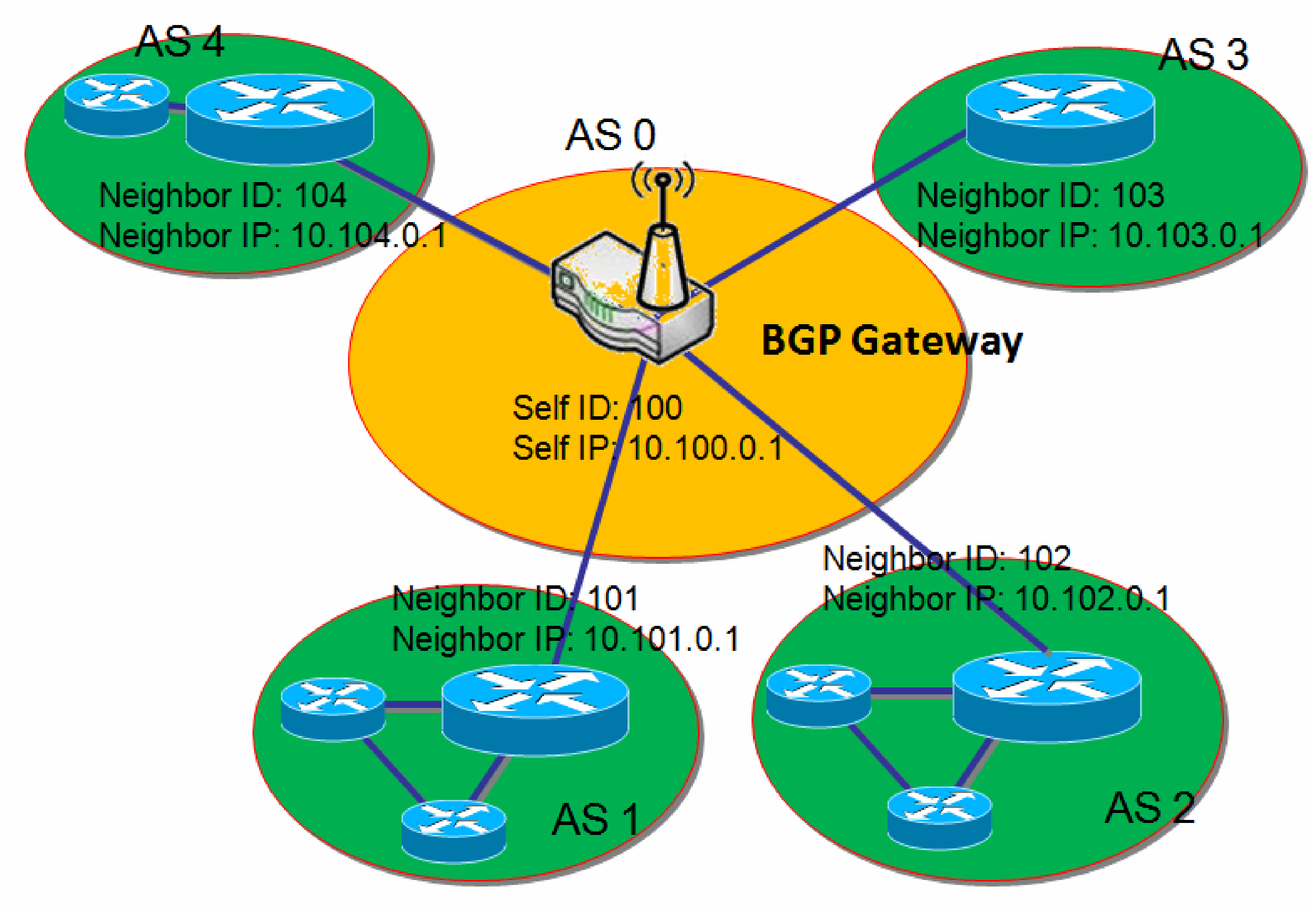
The "BGP Configuration" window allows you to check "Enable" box to activate the BGP dynamic routing protocol and specify its self code.

BGP Neighbor List

The BGP Neighbor List shows all BGP neighbors definition. There also be one "Add" button at the "BGP Neighbor List" caption that can let you add and create one new BGP neighbor. The "Edit" button at the end of each BGP neighbor definition can let you modify it.

BGP Neighbor Configuration

To configure one BGP neighbor, you must specify related parameters including the neighbor IP, the neighbor ID and neighbor activation by an "Enable" box. Following diagram is an example for the scenario.



Scenario Application Timing

Most Internet service providers (ISPs) must use BGP to establish routing between one another (especially if they are multihomed). 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 multihoming 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.

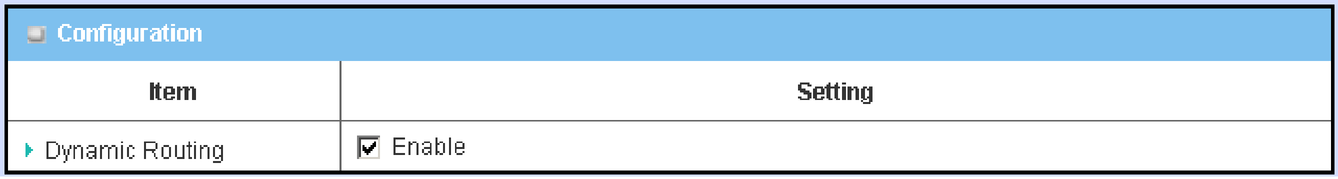
By operating with BGP protocol, the BGP gateway can gather the routing information from other BGP gateways in the Internet. And then it forwards the routing information to the routers in its dominated AS.

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.

Go to Basic Network > Routing > Dynamic Routing Tab

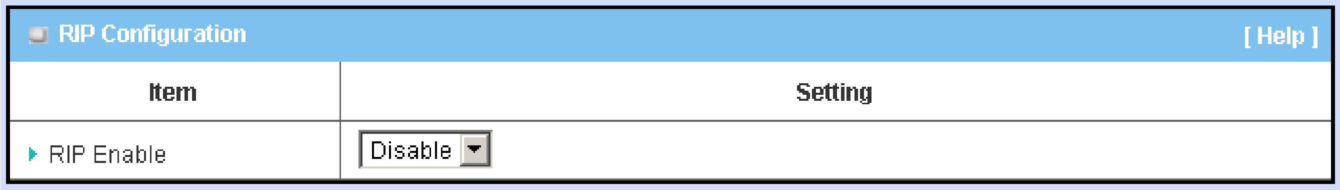


Configuration

Item	Setting
Dynamic Routing	☑ Enable

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

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



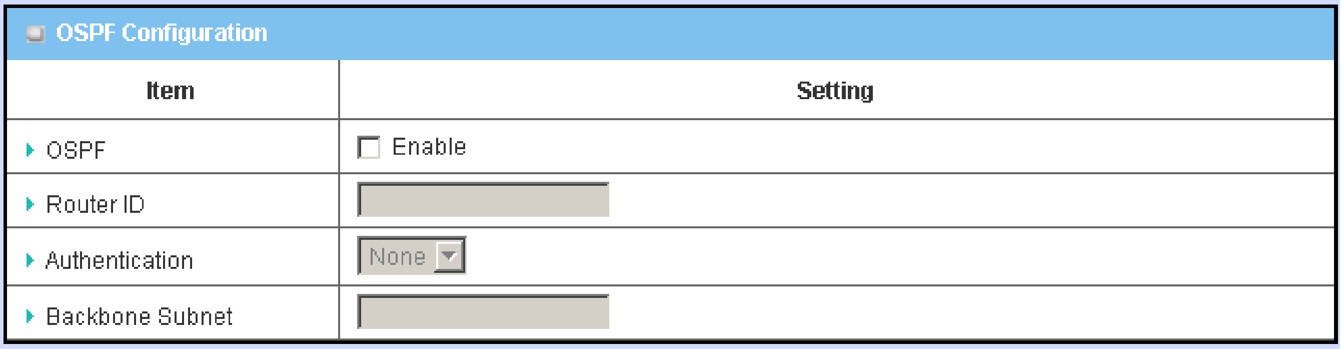
RIP Configuration

Item	Setting
RIP Enable	Disable

Item	Value setting	Description
Enable RIP	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.

Index skipping is used to reserve slots for new function insertion, when required.

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



OSPF Configuration

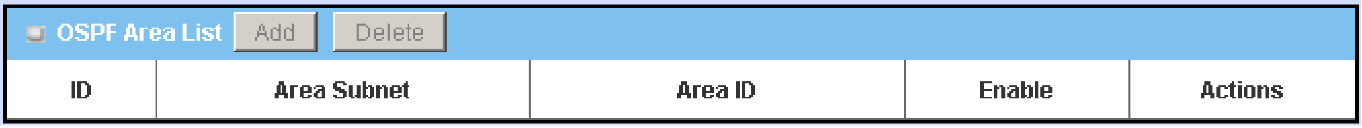
Item	Setting
OSPF	□ Enable
Router ID	
Authentication	None
Backbone Subnet	

Item	Value setting	Description
Enable 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.

Index skipping is used to reserve slots for new function insertion, when required.

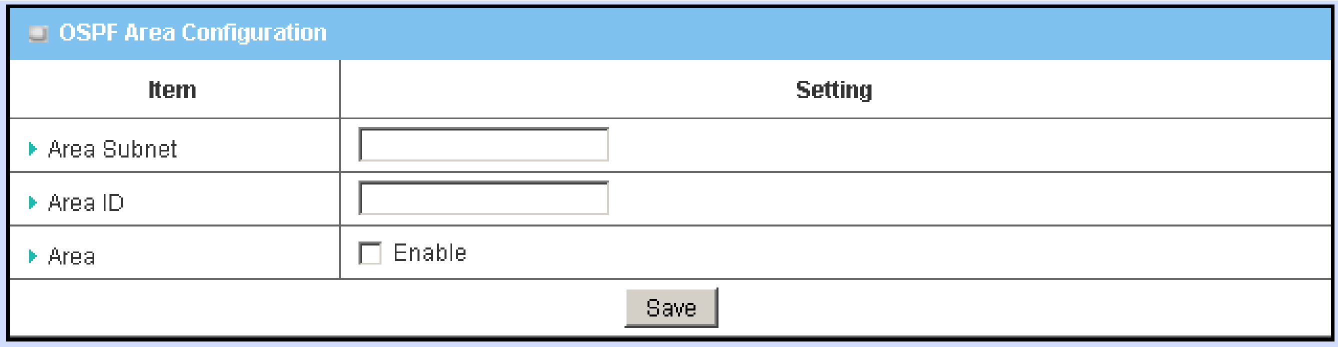
Create/Edit OSPF Area Rules

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



ID	Area Subnet	Area ID	Enable	Actions

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

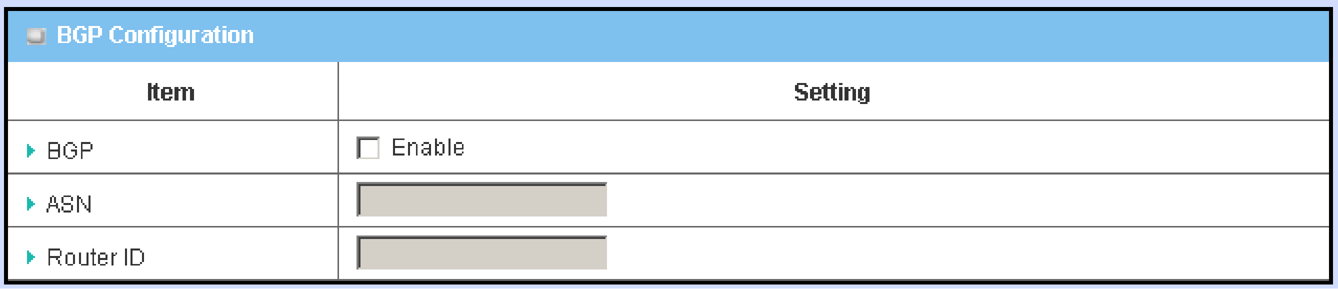


Item	Setting
Area Subnet	
Area ID	
Area	□ Enable

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 Enable	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration

Index skipping is used to reserve slots for new function insertion, when required.

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



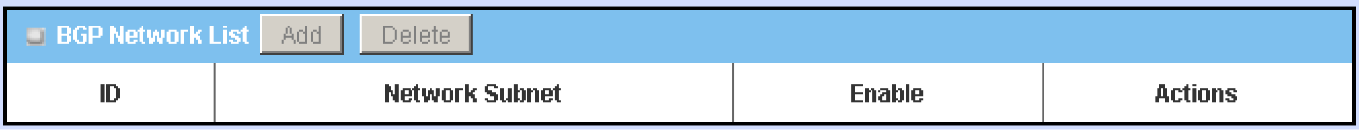
BGP Configuration

Item	Setting
BGP	□ Enable
ASN	
Router ID	

Item	Value setting	Description
Enable BGP function	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.

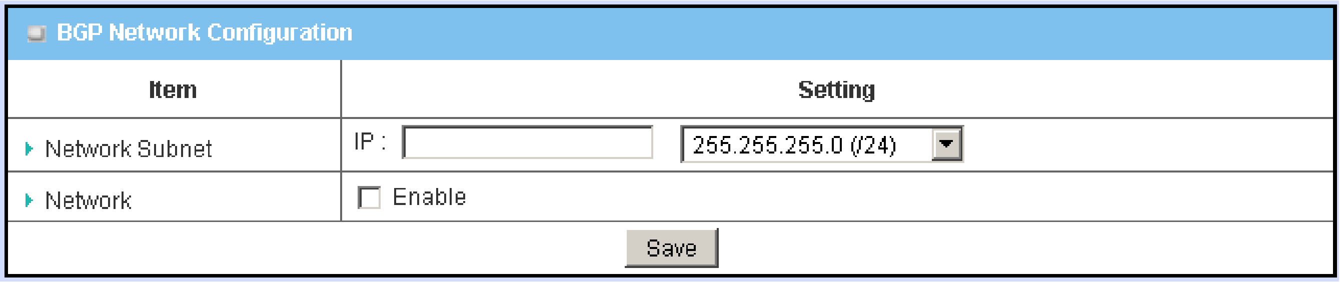
Create/Edit BGP Network Rules

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

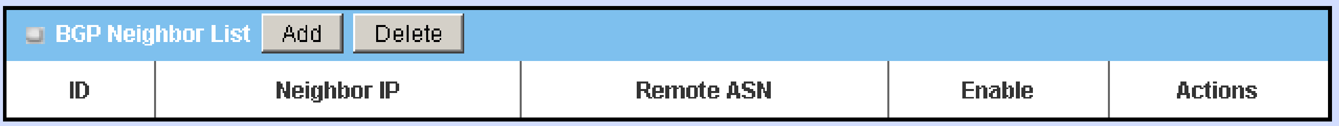
Item	Setting
Network Subnet	IP : ______ 255.255.255.0 (/24)
Network	□ Enable

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 Enable	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration

Index skipping is used to reserve slots for new function insertion, when required.

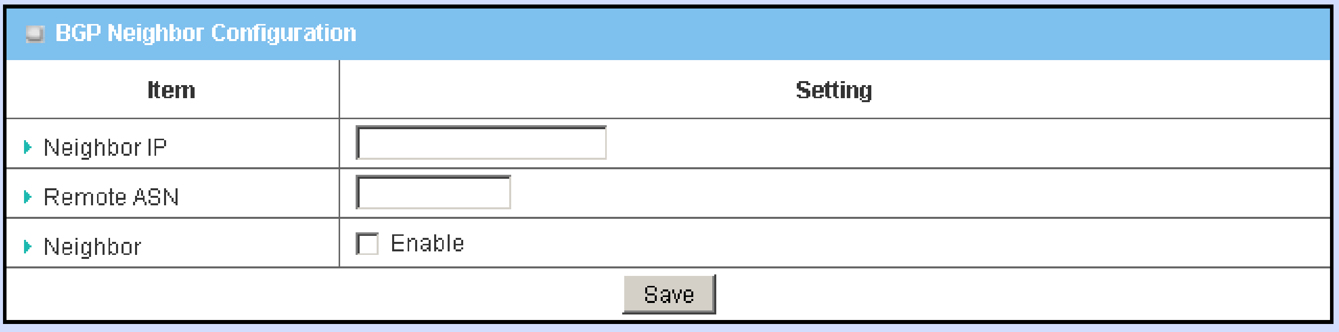
Create/Edit BGP Neighbor Rules

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.



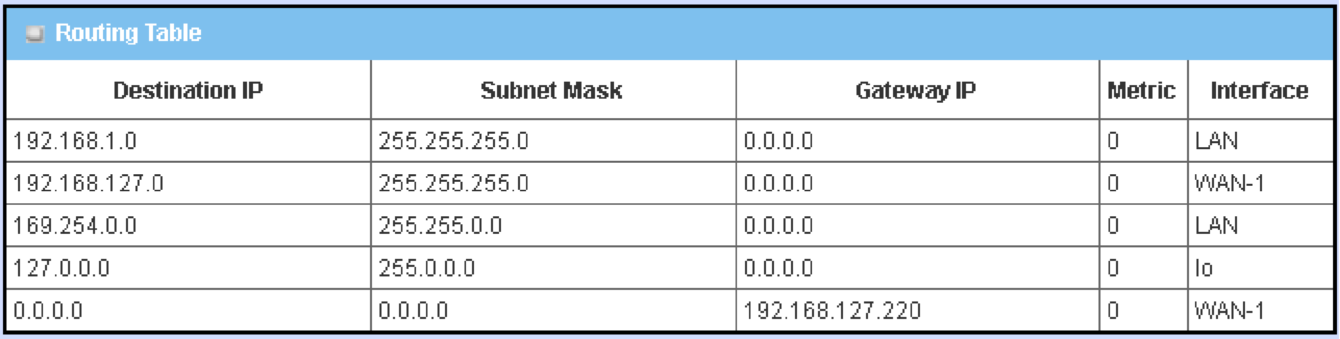
Item	Setting
Neighbor IP	
Remote ASN	
Neighbor	□ Enable

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 Enable	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 Balanced is enabled and the Load Balance Strategy is By User Policy.

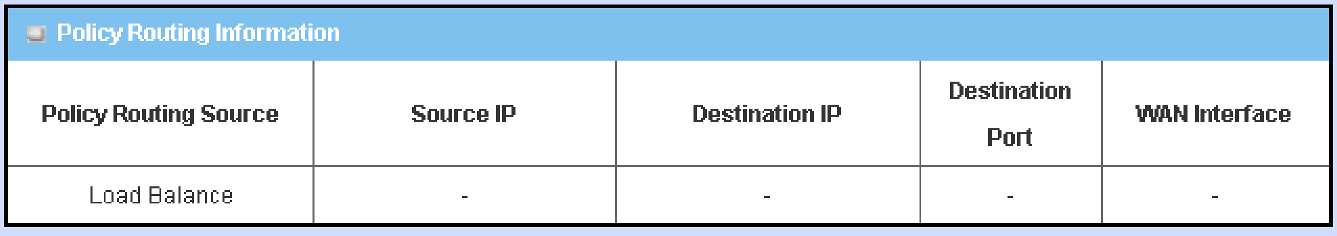
Go to Basic Network > Routing > Routing Information Tab



Routing Table

Destination IP	Subnet Mask	Gateway IP	Metric	Interface
192.168.1.0	255.255.255.0	0.0.0.0	0	LAN
192.168.127.0	255.255.255.0	0.0.0.0	0	WAN-1
169.254.0.0	255.255.0.0	0.0.0.0	0	LAN
127.0.0.0	255.0.0.0	0.0.0.0	0	lo
0.0.0.0	0.0.0.0	192.168.127.220	0	WAN-1

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	-	-	-	-

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.

Index skipping is used to reserve slots for new function insertion, when required.

3.d Client & Server & Proxy

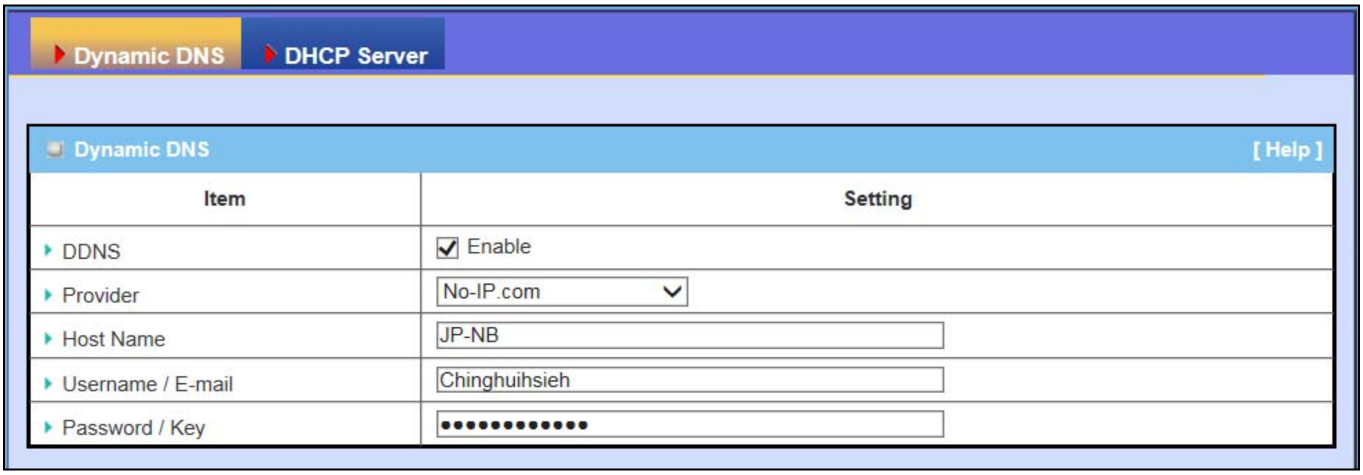
This section presents application clients, servers or proxies running in the gateway system. There are mainly Dynamic DNS client and DHCP server in the current gateway device.

3.d.1 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[10,11].

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.



Dynamic DNS

Item	Setting
DDNS	☑ Enable
Provider	No-IP.com
Host Name	JP-NB
Username / E-mail	Chinghuihsieh
Password / Key	●●●●●●●●●●●●●

In the "Dynamic DNS" page, there is only one configuration window to set up the necessary parameters for Dynamic DNS function.

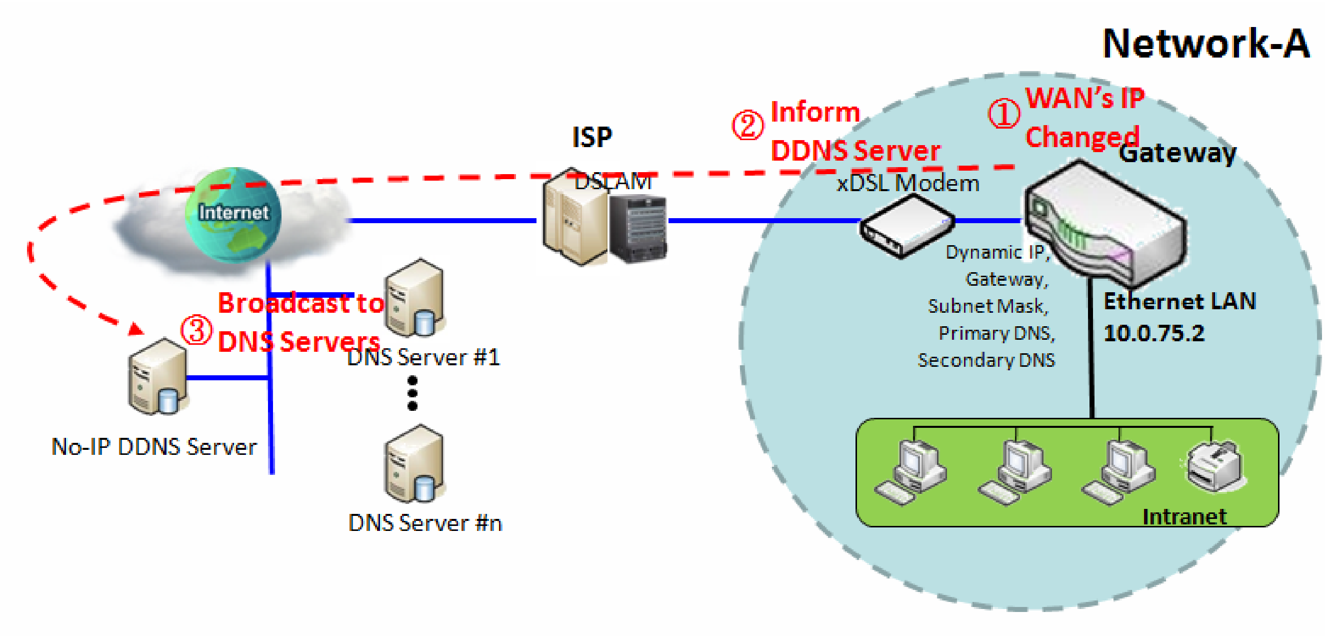
[10] http://en.wikipedia.org/wiki/Domain_Name_System
[11] http://en.wikipedia.org/wiki/Dynamic_DNS

Dynamic DNS

The required parameters for the dynamic DNS agent in the gateway system include the DDNS service provider, the host name of the gateway, and the user name (or E-mail address) and password (or key) for authenticating to the service provider successfully. This device supports most popular third-party DDNS service provider, including DynDNS.org(Dynamic), DynDNS.org(Custom), No-IP.com, TZO.com, and DHS.org. Before you enable Dynamic DNS, you need to register an account with one of these Dynamic DNS servers that we list in Provider field.

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 adress.

Dynamic DNS Scenario



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.

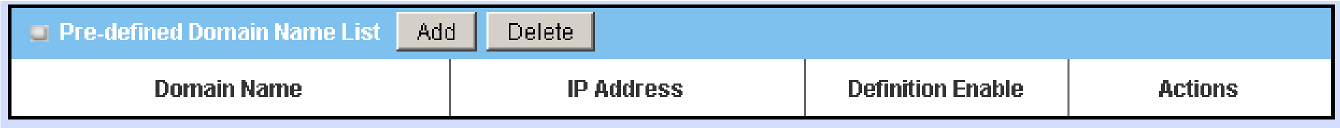
DNS & DDNS Setting

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

Go to **Basic Network** > **Client / Server / Proxy** > **Dynamic DNS Tab**

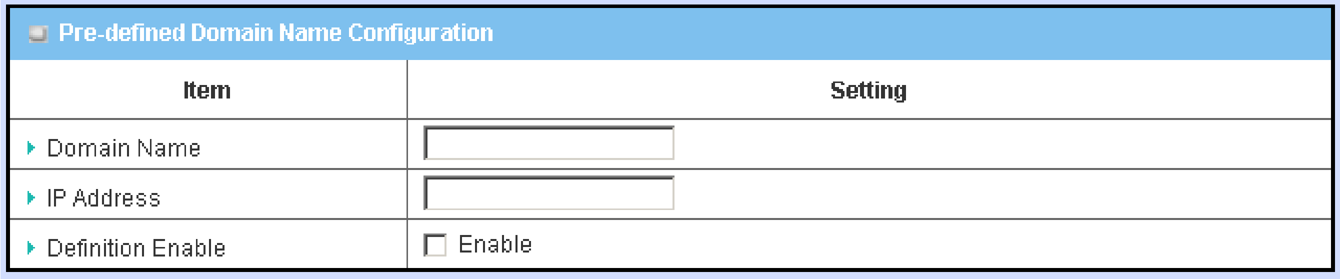
Create/Edit Pre-defined Domain Name List

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



Domain Name	IP Address	Definition Enable	Actions

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



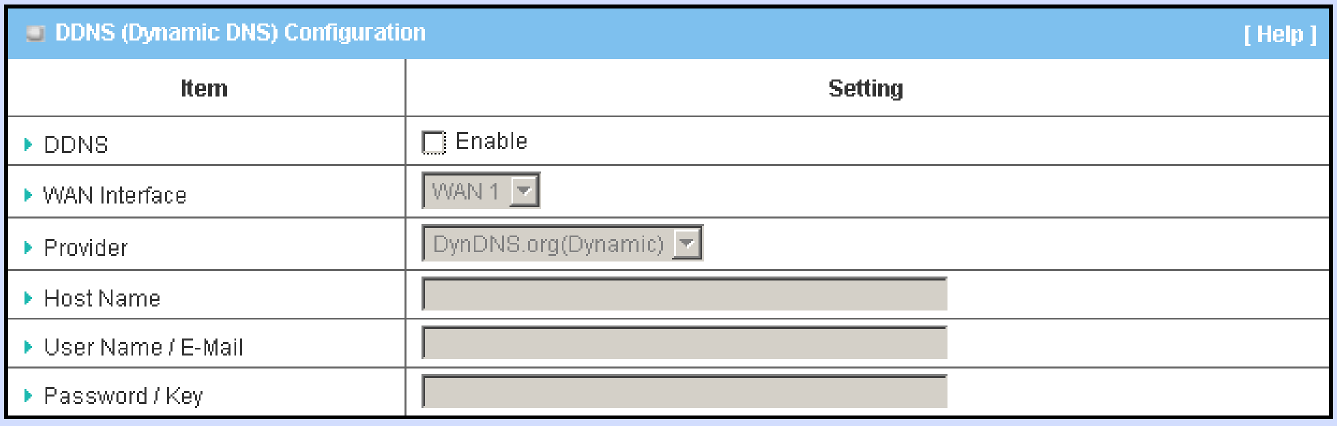
Item	Setting
Domain Name	
IP Address	
Definition Enable	□ Enable

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.
Enabling the rule	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.

Index skipping is used to reserve slots for new function insertion, when required.

Setup Dynamic DNS

The router allows you to custom your Dynamic DNS settings.



DDNS (Dynamic DNS) Configuration [Help]

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**
Enable DDNS function	The box is unchecked by default	Check the **Enable** box to activate this function
WAN Interface	WAN 1 is set by default	Selected 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

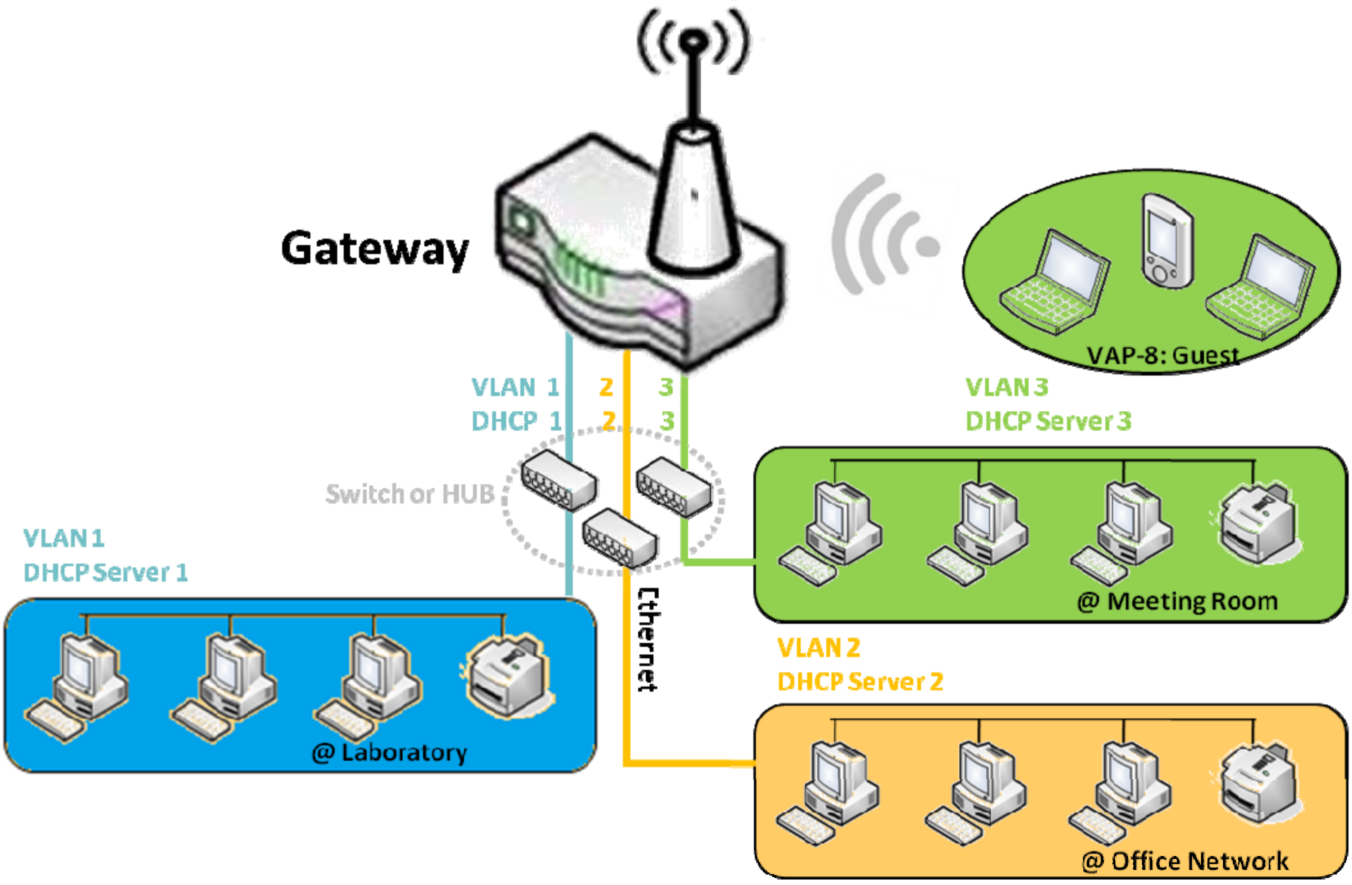
3.d.3 DHCP Server

➢ DHCP Server

The gateway supports up to 4 DHCP servers to fulfill the DHCP requests from different VLAN groups (please refer to VLAN section for 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.

Also, user can select DHCP Server and delete it by clicking on the “Select” check-box and the “Delete” button.



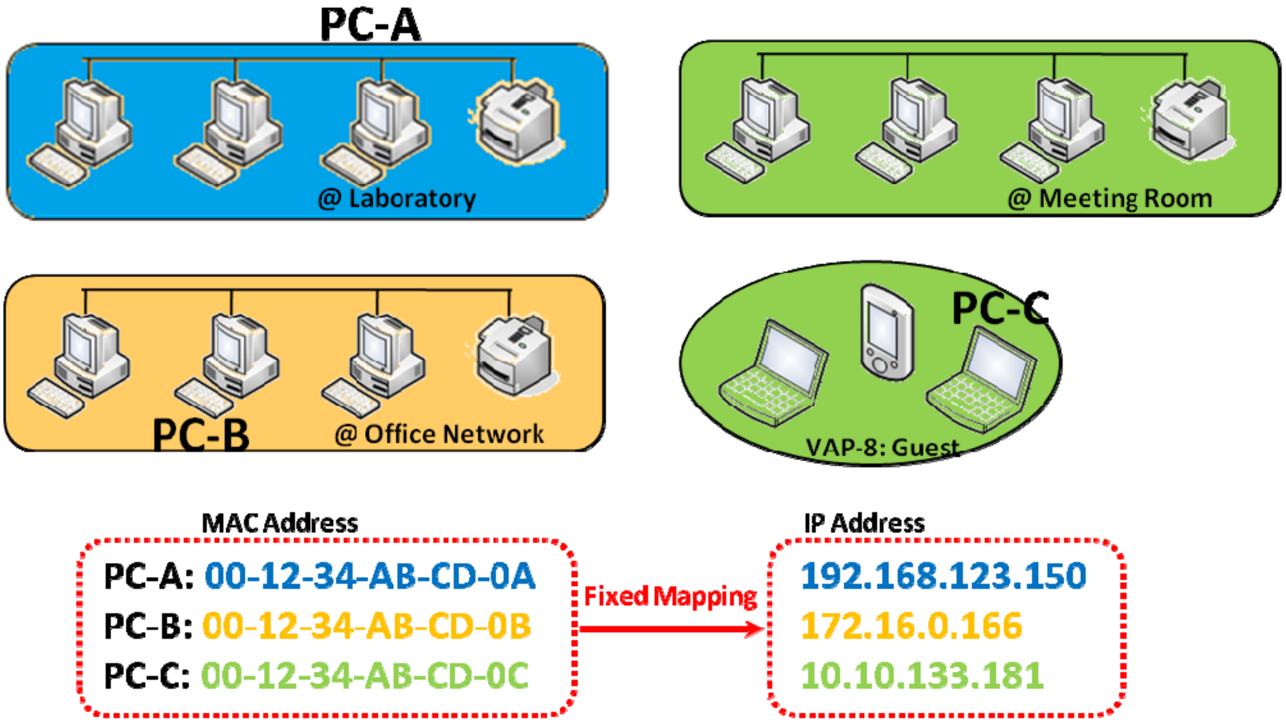
Index skipping is used to reserve slots for new function insertion, when required.

➢ DHCP Clients List

To show the DHCP clients list with some details/information like the LAN Interface, IP Address, Host Name, MAC Address and the Remaining Lease Time.

➢ 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.



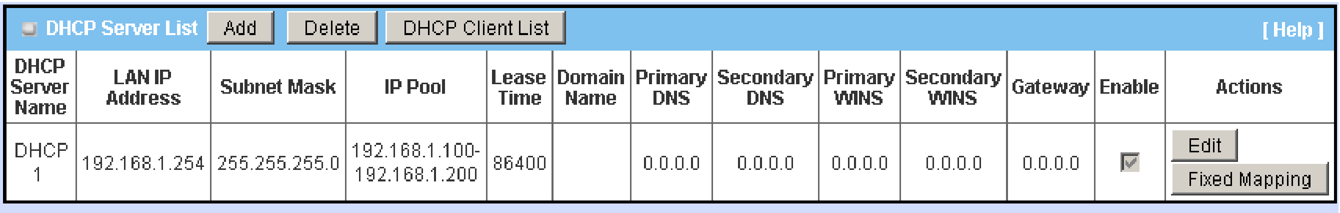
DHCP Server Setting

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 > Client / Server / Proxy > DHCP Server Tab

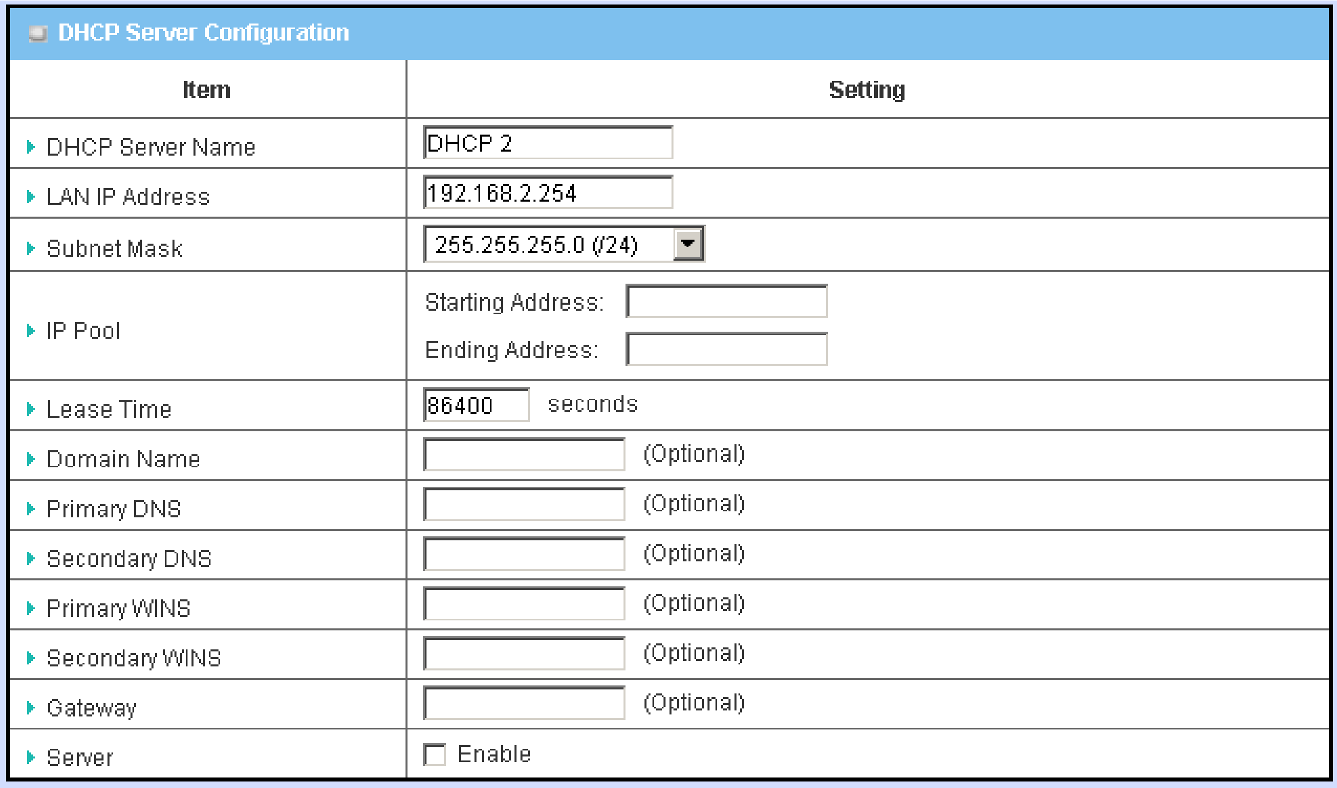
Create/Edit DHCP Server Policy

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	86400		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.


DHCP Server Configuration

Item	Setting
DHCP Server Name	DHCP 2
LAN IP Address	192.168.2.254
Subnet Mask	255.255.255.0 (/24)
IP Pool	Starting Address: Ending Address:
Lease Time	86400 seconds
Domain Name	(Optional)
Primary DNS	(Optional)
Secondary DNS	(Optional)
Primary WINS	(Optional)
Secondary WINS	(Optional)
Gateway	(Optional)
Server	□ Enable

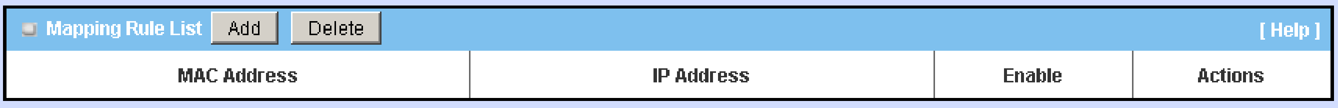
Index skipping is used to reserve slots for new function insertion, when required.

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.
Enabling the Server	The box is unchecked by default.	Click **Enable** box to activate this 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.

Index skipping is used to reserve slots for new function insertion, when required.

Create/Edit Mapping Rule List on DHCP Server

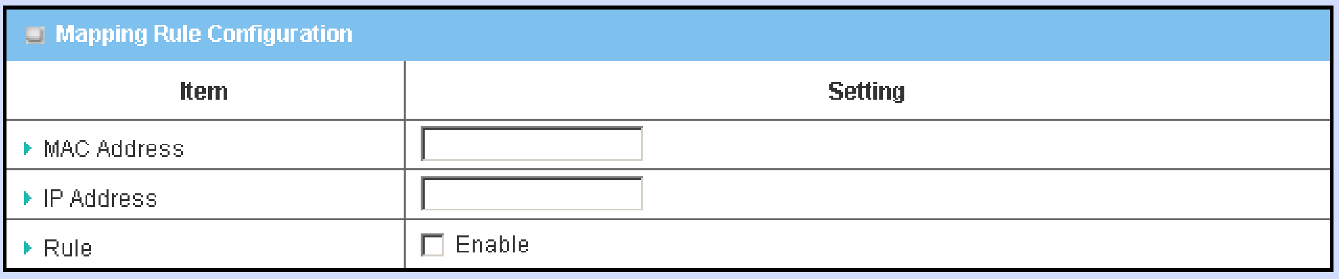
The router allows you to custom your Mapping Rule List on DHCP Server. It supports up to a maximum of 64 rule sets. When **Fix Mapping** button is applied, the Mapping Rule List screen will appear.



Mapping Rule List Add Delete [Help]

MAC Address	IP Address	Enable	Actions

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



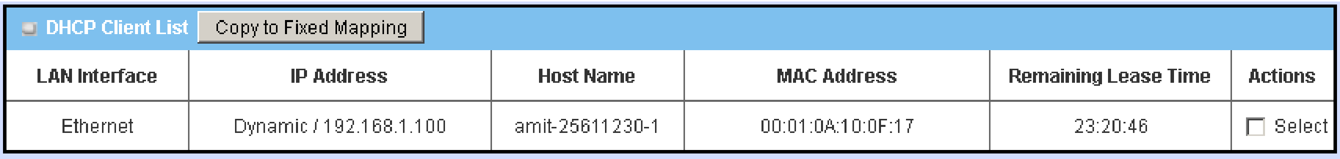
Mapping Rule Configuration

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.

Index skipping is used to reserve slots for new function insertion, when required.

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	amit-25611230-1	00:01:0A:10:0F:17	23:20:46	□ Select

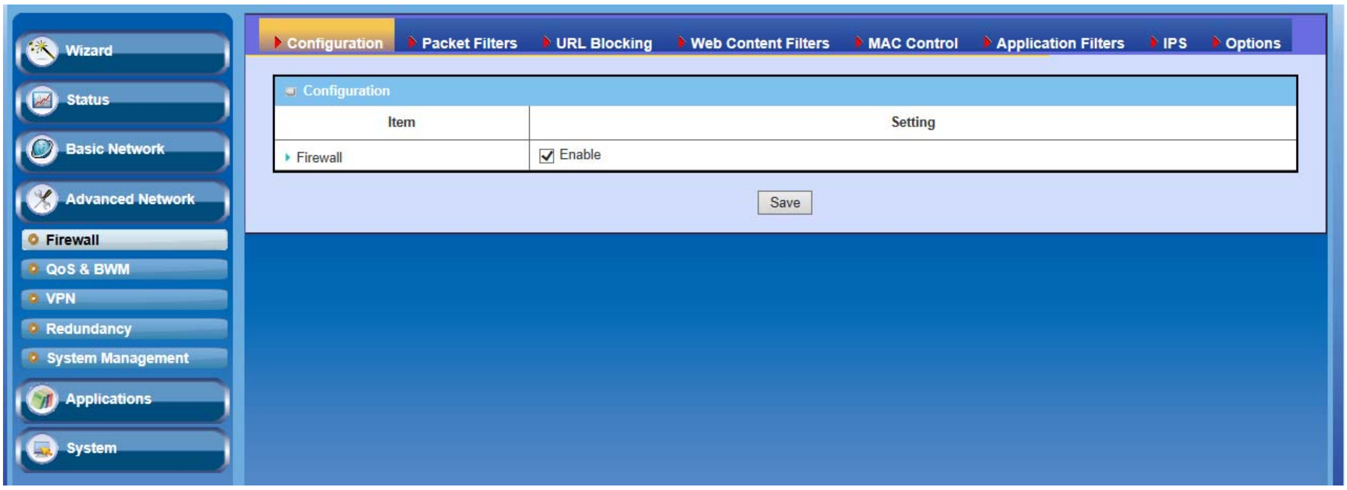
When the DHCP Client is selected and Copy to Fixed Mapping button is applied. The IP and MAC address of DHCP Client will apply to the Mapping Rule List on specific DHCP Server automatically.

Chapter5 Advanced Network

5.1 Firewall

The firewall functions include Packet Filters, URL Blocking, Web Content Filters, MAC Control, Application Filters, IPS and some firewall options.

5.1.1 Firewall Configuration



Configuration

Item	Setting
Firewall	☑ Enable

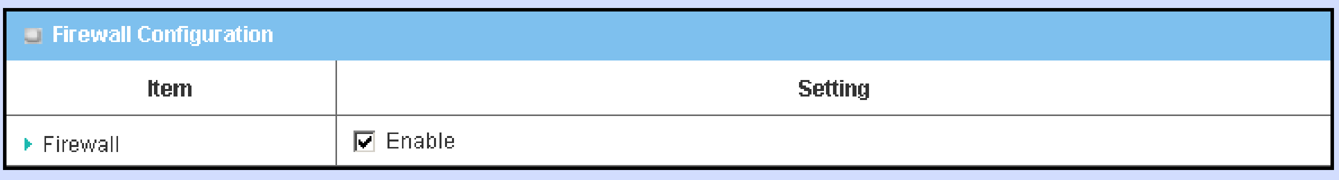
Firewall Configuration

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.

Enabling Global Firewall Function

Go to Advanced Network > Firewall > Configuration Tab



Firewall Configuration

Item	Setting
Firewall	☑ Enable

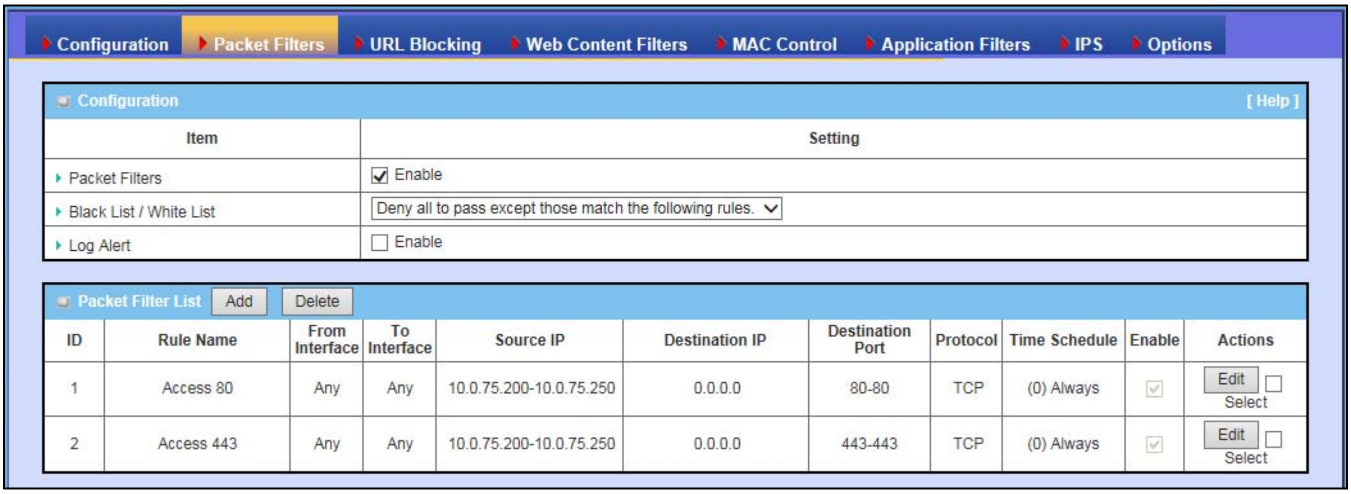
Firewall Configuration Setting

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

Index skipping is used to reserve slots for new function insertion, when required.

5.1.3 Packet Filters

"Packet Filters" 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. Lastly, the time schedule to which the rule will be active.



Configuration

Item	Setting
Packet Filters	☑ Enable
Black List / White List	Deny all to pass except those match the following rules.
Log Alert	□ Enable

Packet Filter List

ID	Rule Name	From Interface	To Interface	Source IP	Destination IP	Destination Port	Protocol	Time Schedule	Enable	Actions
1	Access 80	Any	Any	10.0.75.200-10.0.75.250	0.0.0.0	80-80	TCP	(0) Always	☑	Edit □ Select
2	Access 443	Any	Any	10.0.75.200-10.0.75.250	0.0.0.0	443-443	TCP	(0) Always	☑	Edit □ Select

In "Packet Filters" page, there are three configuration windows for packet filtering function. They are the "Configuration" window, "Packet Filter Rule List" window, and "Packet Filter Rule Configuration" window.

The "Configuration" window can let you activate the packet filtering function and specify to black listing or to white listing Inbound or Outbound packets defined in the "Packet Filter Rule List" entry. In addition, log alerting can be enabled through an “Enable” checkbox to log events. Second, the "Packet Filter Rule List" window lists all your defined packet filtering rule entry. At last, the "Packet Filter Rule Configuration" window can let you define one packet filtering rule.

Configuration

Check the "Enable" box to activate the "Packet Filters" function. Select either the black list or the white list for following "Packet Filter Rule List". Finally, enable the log alerting when needed.

When you choose "Allow all to pass except those match the following rules" for the "Packet Filter Rule List", you are setting the defined packet filtering rules to belong to the black list. The packets, listed in the rule list, will be blocked from entering or leaving the gateway if they match to one rule. Other packets can pass through the gateway. In contrast, when you choose "Deny all to pass except those match the following rules" for the "Packet Filter Rule List", you are setting the defined packet filtering rules to belong to the white list. The packets, listed in the rule, will be allowed to enter or leave the gateway if they match to one of the rules. Other packets will be blocked.

Index skipping is used to reserve slots for new function insertion, when required.

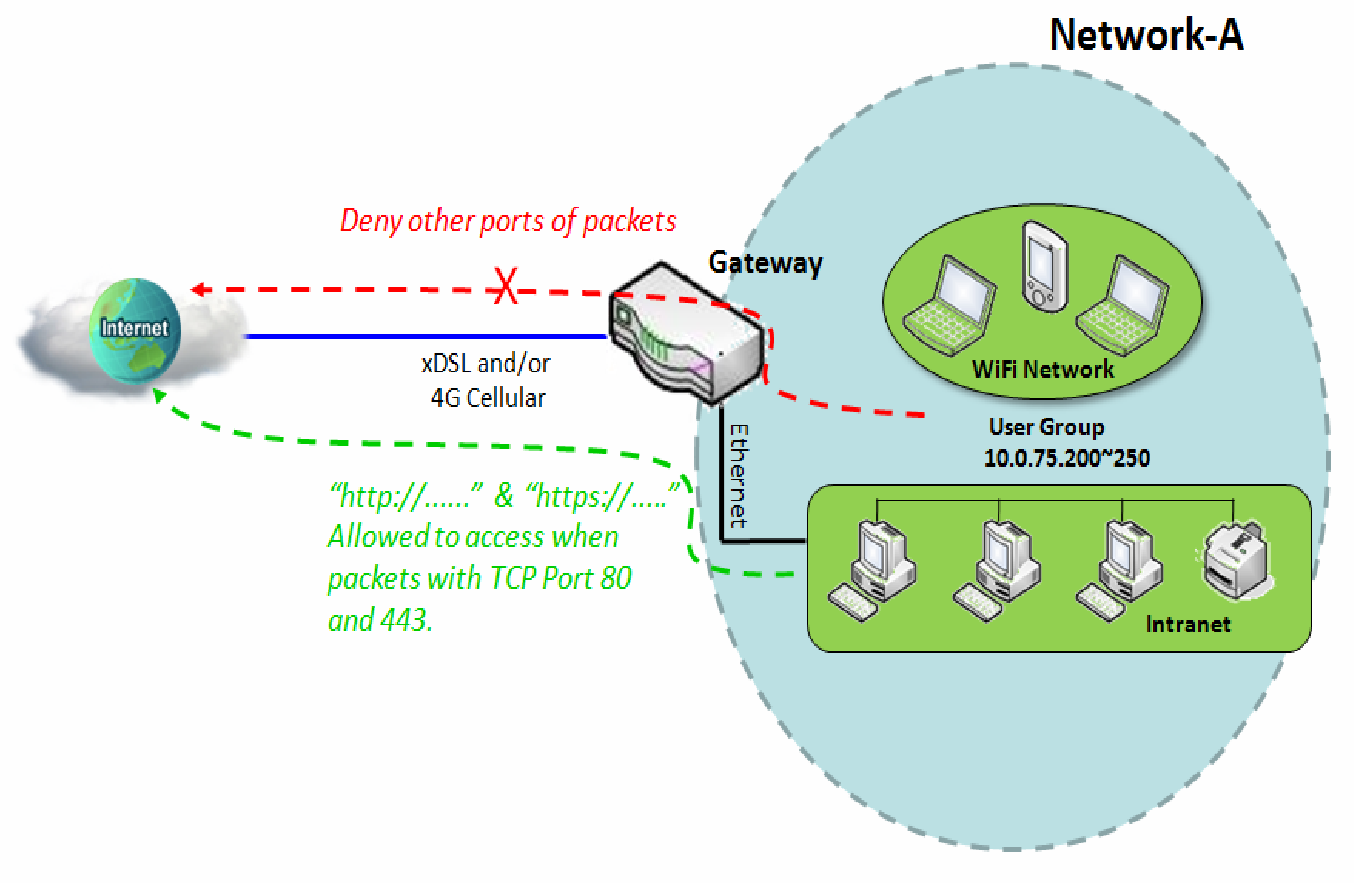
Packet Filter Rule List

The "Packet Filter Rule List" shows the setup parameters of all packet filtering rules. There also be one "Add" button at the "Packet Filter Rule List" caption, that can let you add and create one new packet filtering rule. The "Edit" button at the end of each packet filtering rule can let you modify the rule. Refer to the following sub-sections for more reference.

Packet Filter Rule Configuration

When you want to add a new packet filtering rule or edit one already existed, the "Packet Filter Rule Configuration" window shows up for you to configure. The parameters in a rule include the rule name, the from and to which interface the packet enters and leaves, the source and destination IP addresses, the destination service port type and port number, the integrated time schedule rule and the rule activation. Refer to 6.2.1 Scheduling Settings section in this user manual on how to configure a time schedule. See following scenario example.

Packet Filters 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 Filters]-[Configuration]
Packet Filters	■ ***Enable***
Black List / White List	***Deny all to pass except those match the following rules.***

Configuration Path	[Packet Filters]-[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.

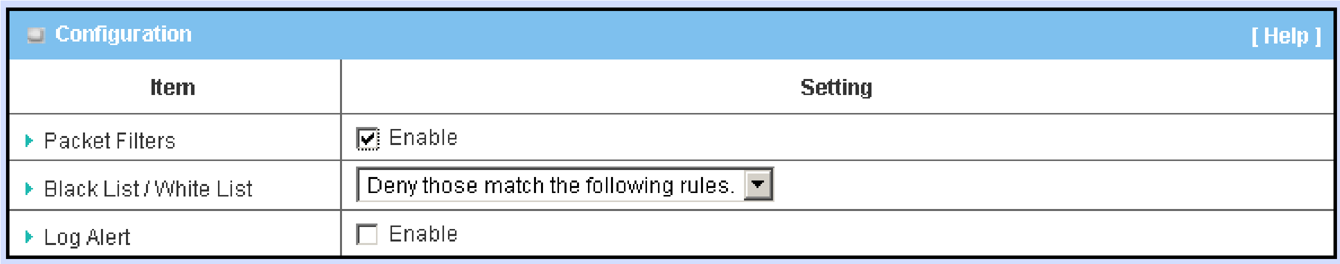
Index skipping is used to reserve slots for new function insertion, when required.

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.

Enabling Packet Filter

Go to Advanced Network > Firewall > Packet Filters Tab



Configuration [Help]

Item	Setting
Packet Filters	☑ Enable
Black List / White List	Deny those match the following rules. ▾
Log Alert	□ Enable

Enabling Packet Filters

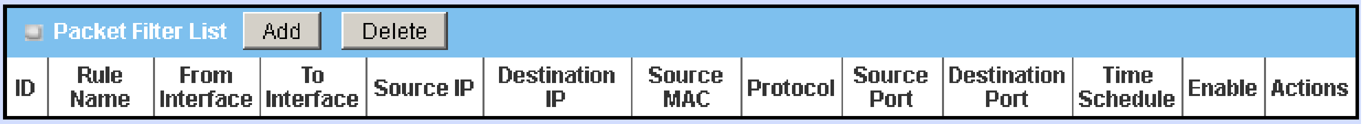
Item Name	Value setting	Description
Enable Packet Filter function	The box is unchecked by default	Check the **Enable** box to activate Packet Filter function
Black List / White List (Filter Method Selection)	Deny those match the following rules is set by default	When ***Deny those match the following 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 4.1 Firewall

Index skipping is used to reserve slots for new function insertion, when required.

Create/Edit Filter Rules

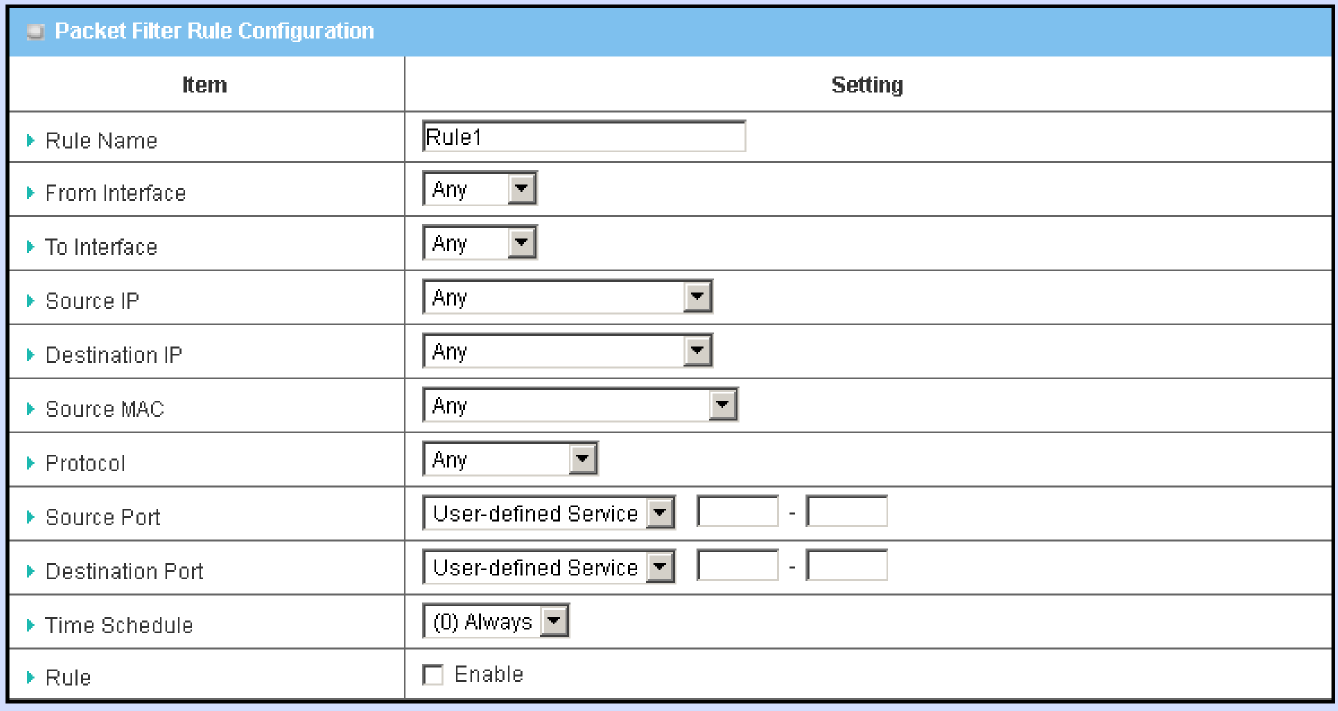
The router allows you to customize your packet filtering rules. It supports up to a maximum of 20 filter rule sets.



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 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
Source Port	User-defined Service -
Destination Port	User-defined Service -
Time Schedule	(0) Always
Rule	□ Enable

Create/Edit Filter Rules		
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	A Must filled setting	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	A Must filled setting	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	A Must filled setting	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 **System** > **Grouping > Host grouping.** You may also access to create a group by the **Add Rule** shortcut button.
Destination IP	A Must filled setting	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 **System** > **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	A Must filled setting	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 **System** > **Grouping > Host grouping.** You may also access to create a group by the **Add Rule** shortcut button.
Protocol	A Must filled setting	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-**

Index skipping is used to reserve slots for new function insertion, when required.

		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 **System > Scheduling > Scheduling Setting tab**
Enabling the 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.

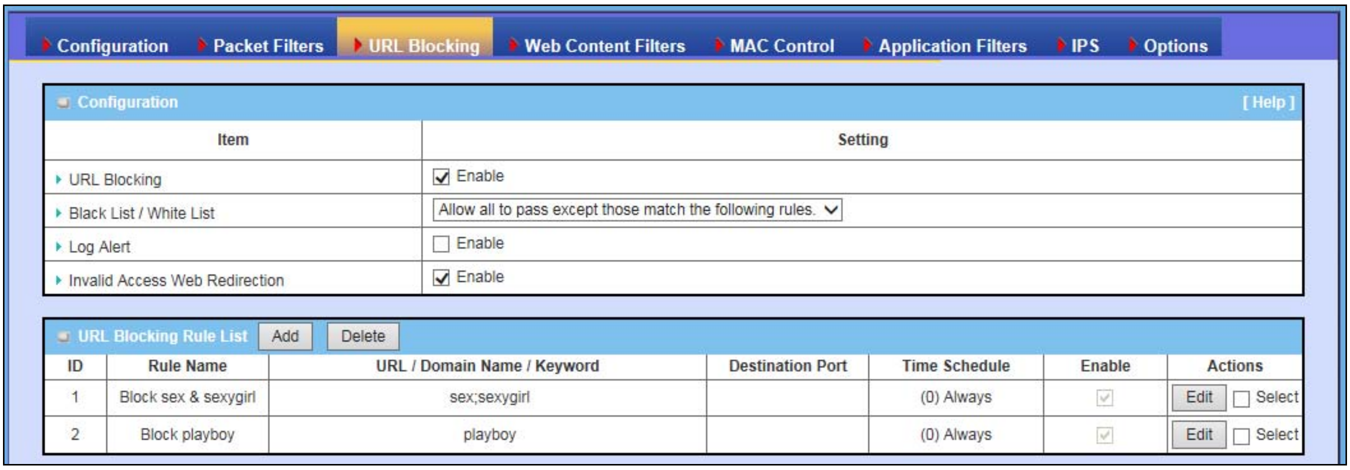
Index skipping is used to reserve slots for new function insertion, when required.

5.1.5 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 indicate the URL, partial domain name or included keywords in the Web requests from and to the gateway and what destination service port. In addition, the integrated time schedule can be applied to activate rules based on date and time.

Gateway logs and displays illegal web accessing, in the web-based utility, that matches rules in the defined URL blocking rule entry in the black-list or in the exclusion of the white-list.



Configuration [Help]

Item	Setting
URL Blocking	☑ Enable
Black List / White List	Allow all to pass except those match the following rules.
Log Alert	□ Enable
Invalid Access Web Redirection	☑ Enable

URL Blocking Rule List [Add] [Delete]

ID	Rule Name	URL / Domain Name / Keyword	Destination Port	Time Schedule	Enable	Actions
1	Block sex & sexygirl	sex;sexygirl		(0) Always	☑	Edit □ Select
2	Block playboy	playboy		(0) Always	☑	Edit □ Select

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 through an “Enable” checkbox to log on-going events. Refer to "System Status" in "6.1.1 System Related" section in this user manual on where and how to view log.

Another "Enable" checkbox for Invalid Access Web Redirection allow you to enable warning message to be displayed on your browser during an illegal web accessing. Second, the "URL Blocking Rule List" window lists all your defined URL blocking rule entry. At last, the "URL Blocking Rule Configuration" window can let you define one URL blocking rule.

Configuration

Check the "Enable" box to activate the "URL Blocking" function. Select either the black list or the white list for following "URL Blocking Rule List". Finally, enable the log alerting and the Web redirection for invalid accessing when needed.

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 Rule List

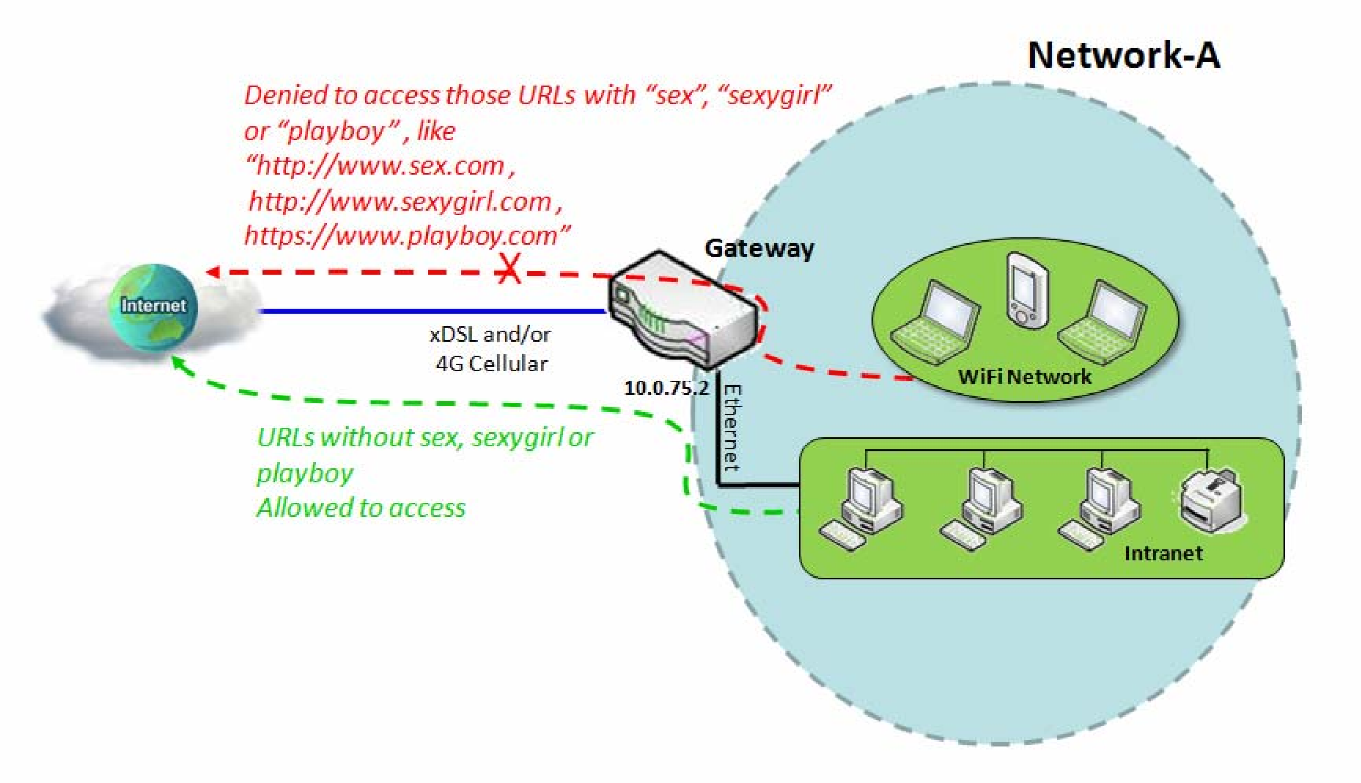
The "URL Blocking Rule List" shows the setup parameters of all URL blocking rules. There also be one "Add" button at the "URL Blocking Rule List" caption, that can let you add and create one new URL blocking rule. The "Edit" button at the end of each URL blocking rule can let you modify the rule. Refer to the following sub-sections for more reference.

URL Blocking Rule Configuration

When you want to add a new URL blocking rule or edit one existed rule, the "URL Blocking Rule Configuration" window shows up for you to configure the rule. The parameters in a rule include the rule name, the URL/Domain Name/Keyword, the destination service ports, the integrated time schedule rule and the rule activation. Refer to 6.2.1 Scheduling Settings section in this user manual on how to configure a time schedule. See following scenario example.

Index skipping is used to reserve slots for new function insertion, when required.

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 carry out 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 carry out 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. Other ones 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.

Index skipping is used to reserve slots for new function insertion, when required.

Configuration Path	[URL Blocking]-[Configuration]
URL Blocking	■ *Enable*
Black List / White List	***Allow all to pass except those match the following rules.***
Invalid Access Web Redirection	■ *Enable*

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.

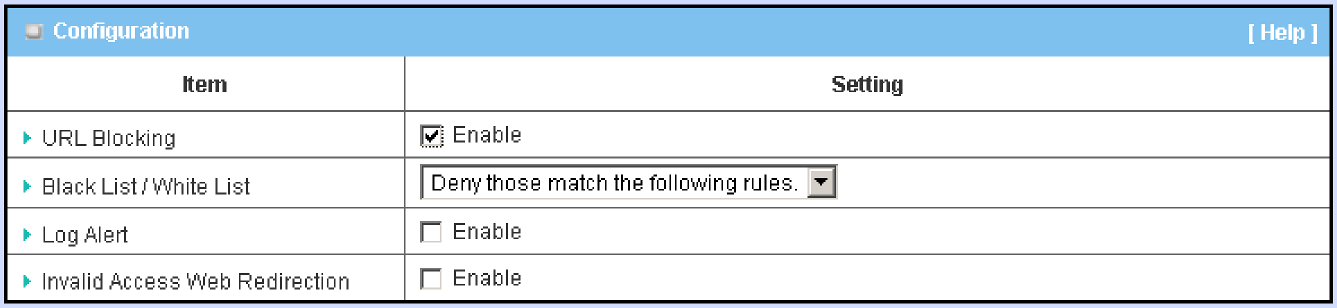
Enable the URL blocking function and specify the "URL Blocking Rule List" is a black list and configure two URL blocking rules for the gateway. Create one rule to deny the Web requests with "sex" or "sexygirl" patterns and the other to deny the Web requests with "playboy" pattern to go through the gateway.

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 through the router based on their office setting.

Go to Advanced Network > Firewall > URL Blocking Tab



Configuration [Help]

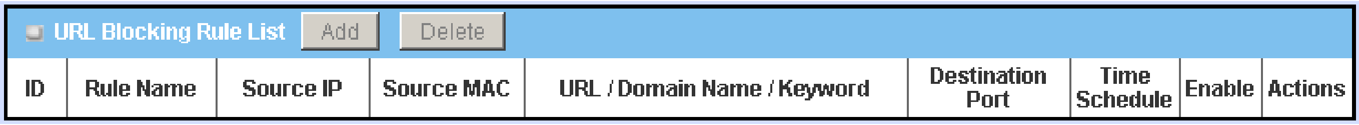
Item	Setting
URL Blocking	☑ Enable
Black List / White List	Deny those match the following rules. ▼
Log Alert	□ Enable
Invalid Access Web Redirection	□ Enable

Index skipping is used to reserve slots for new function insertion, when required.

Item	Value setting	Description
Enable URL Blocking function	The box is unchecked by default	Check the **Enable** box to activate this filter function
Black List / White List (Filter Method Selection)	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 to activate Event Log.
Invalid Access Web Redirection	The box is unchecked by default	Check the **Enable** box to activate this function. When the user attempts to open a blocked http URL by the web browser, it will redirect to a warning page.

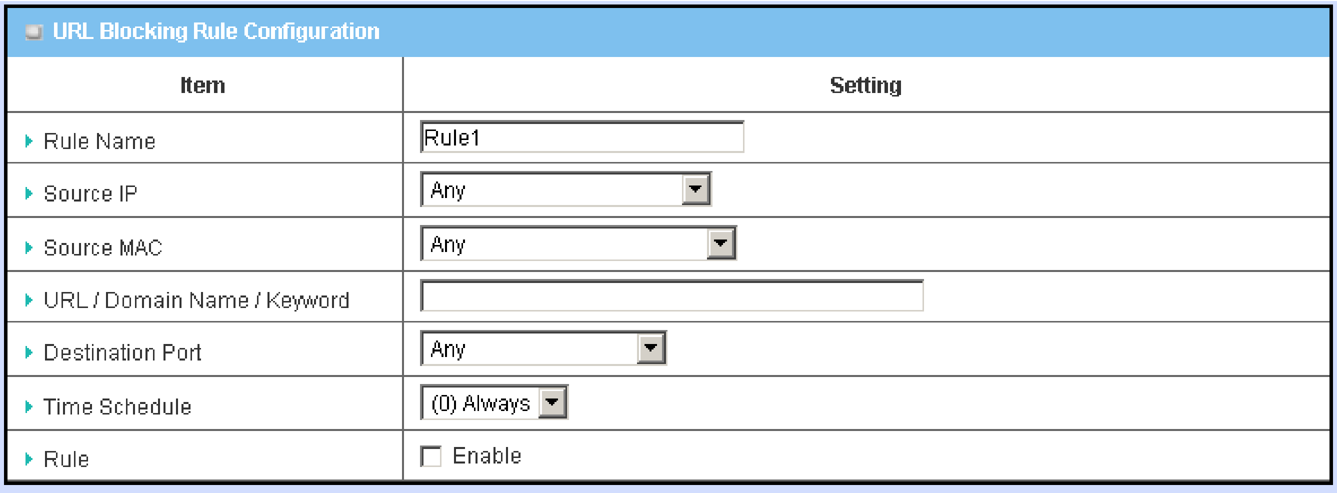
Create/Edit Filter Rules

The router supports up to a maximum of 20 URL blocking rule sets. Ensure that the URL Blocking is enabled before we can create blocking rules.


URL Blocking Rule List

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

When Add button is applied Filter 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	(0) Always
Rule	□ Enable

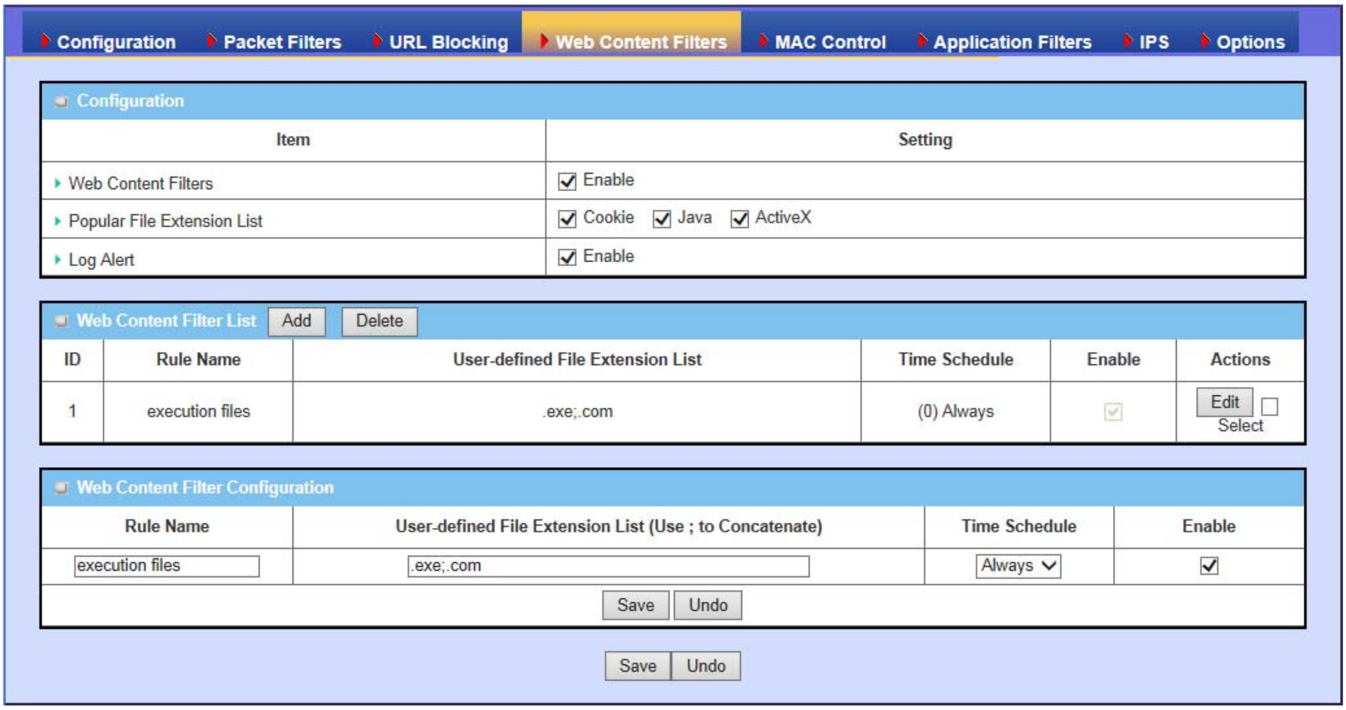
Item	Value setting	Description
Rule Name	1. String format can be any text 2. A Must filled setting	Enter a url blocking rule name. Enter a name that is easy for you to understand.
Source IP	A Must filled setting	This field is to specify the **Source IP address.** Select **Any** to filter packets coming from any IP addresses. Select **Specific IP Address** to filter packets coming from an IP address entered in this field.

Index skipping is used to reserve slots for new function insertion, when required.

		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 selection become available. Refer to **System** > **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	A Must filled setting	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 **System** > **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.
URL / Domain Name / Keyword	A Must filled setting	Specify URL, Domain Name, or Keyword list to filtering rule. It supports up to a maximum of 10 Keywords in a rule by using the delimiter ";". In the **Black List** mode, if the matching rule is found, the packets with http header will be dropped. In the **White List** mode, if the matching rule is found, the packets with http header will be accepted and other packets with http header will be dropped.
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 **System** > **Scheduling setting**.
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 URL Blocking Configuration page.

5.1.9 Web Content Filters

"Web Content Filters" function can block HTML requests with some specific extension file names, like ".exe", ".bat" (applications), "mpeg" (video), and so on. It also blocks HTML requests with some script types, like Java Applet, Java Scripts, cookies and Active X.



Configuration

Item	Setting
Web Content Filters	☑ Enable
Popular File Extension List	☑ Cookie ☑ Java ☑ ActiveX
Log Alert	☑ Enable

Web Content Filter List Add Delete

ID	Rule Name	User-defined File Extension List	Time Schedule	Enable	Actions
1	execution files	.exe;.com	(0) Always	☑	Edit □ Select

Web Content Filter Configuration

Rule Name	User-defined File Extension List (Use ; to Concatenate)	Time Schedule	Enable
execution files	.exe;.com	Always	☑

Save Undo

Save Undo

In "Web Content Filters" page, there are three configuration windows for the filtering function. They are the "Configuration" window, "Web Content Filter List" window, and "Web Content Filter Configuration" window.

The "Configuration" window can let you activate the Web content filtering function. Some popular script types, like Java Applet, Java Scripts, cookies and Active X are in the window and you can check their boxes to enable the gateway to filter out the Web requests with corresponding patterns. Furthermore, log alerting can be enabled by clicking an "Enable" checkbox to log events. Second, the "Web Content Filter List" window lists all your defined file extension lists that are used by the gateway to filter out unwanted Web requests. At last, the "Web Content Filter Configuration" window can let you define one Web content filtering rule.

Configuration

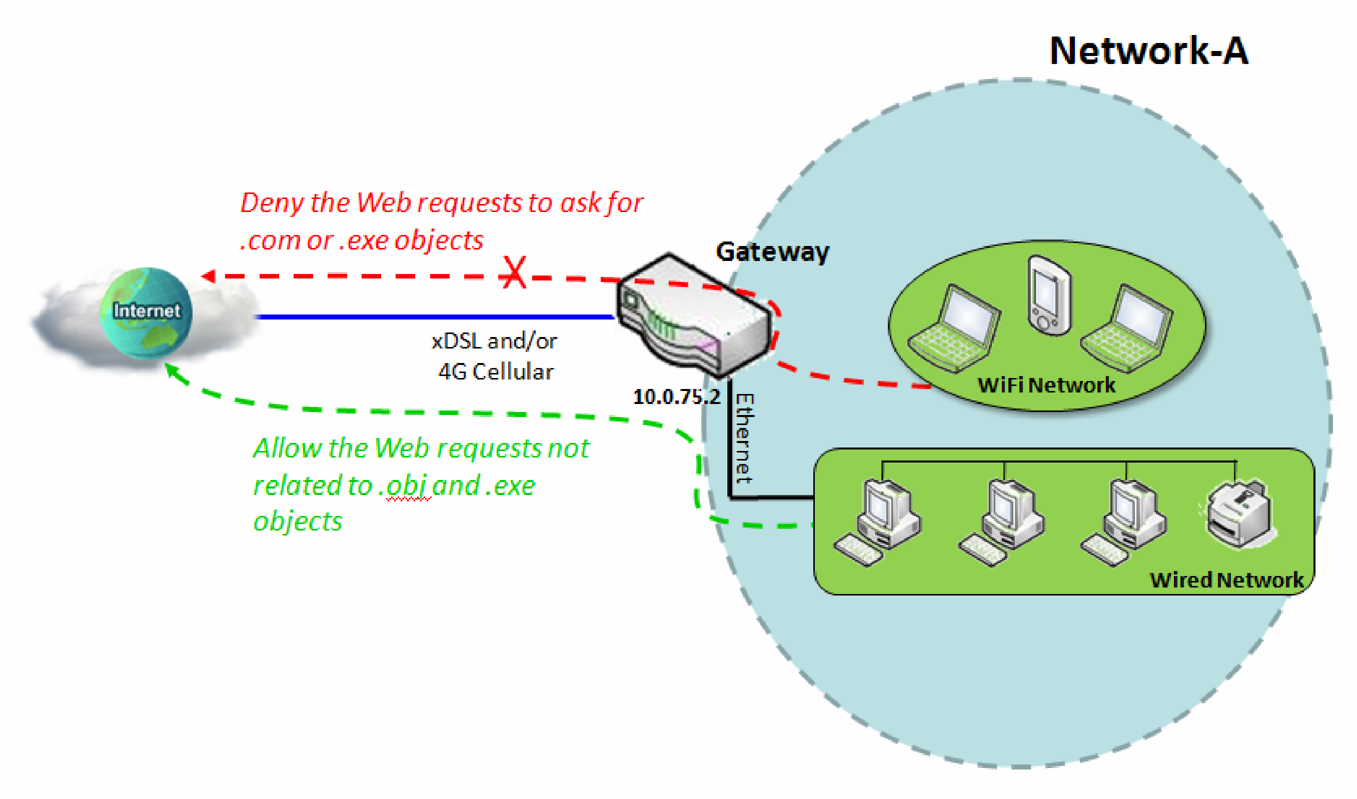
Check the "Enable" box to activate the "Web Content Filters" function. Select some popular script types that you want to block. Finally, enable the log alerting when needed.

Web Content Filter List

The "Web Content Filter List" shows the setup parameters of all filtering rules. There also be one "Add" button at the "Web Content Filter List" caption, that can let you add and create one new Web content filtering rule. The "Edit" button at the end of each filtering rule can let you modify the rule. Refer to the following sub-sections for more reference.

Web Content Filter Configuration

When you want to add a new Web content filtering rule or edit one existed rule, the "Web Content Filter Configuration" window will appear when you click on the Add or Edit button to configure. The parameters in a rule include the rule name, the defined file extension list to be filtered out, the integrated time schedule rule and the rule activation. See following scenario example for your reference.


Network-A
Deny the Web requests to ask for .com or .exe objects
Gateway
Internet
xDSL and/or
4G Cellular
10.0.75.2
Ethernet
WiFi Network
Allow the Web requests not related to .obj and .exe objects
Wired Network

Scenario Application Timing

When the administrator of the gateway wants to block the Web requests for dedicated contents or objects, he can use the "Web Content Filters" function to carry out such request blocking.

Scenario Description

Web requests for dedicated contents or objects in the defined list will be blocked by the gateway. Other ones can pass through the gateway.

Parameter Setup Example

Following tables list the parameter configuration as an example for the gateway in above diagram with "Web Content Filters" enabling.

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

Configuration Path	[Web Content Filters]-[Configuration]
Web Content Filter	■ *Enable*
Popular File Extension List	■ *Cookie* ■ *Java* ■ *ActiveX*
Log Alert	■ *Enable*

Configuration Path	[Web Content Filters]-[Web Content Filter List]
ID	1
Rule Name	*execution files*
User-defined File Extension List	*.exe; .com*
Rule	■ *Enable*

Scenario Operation Procedure

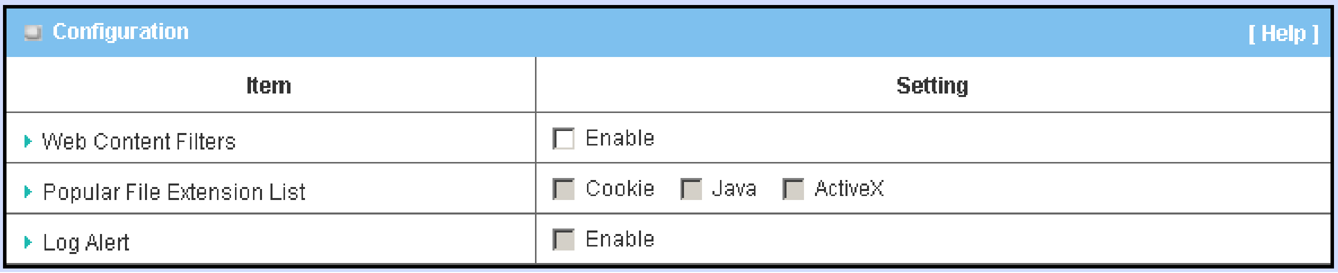
In above diagram, the Gateway is the gateway of Network-A and the subnet of its Intranet is 10.0.75.0/24. The gateway has the IP address of 10.0.75.2 for LAN interface, 118.18.81.33 for WAN-1 interface. It serves as a NAT router.

Enable the Web content filters function to check and filter out Web requests on Cookie, Java and ActiveX objects then define further with objects in the “Web Content Filter List” that may include extension ".exe" and ".com".

System will block requests containing objects with extension ".exe" or ".com".

The web content filters setting allows user to create and customize blocking policies to allow or reject http packets with specific file extension list through the router based on their office setting.

Go to Advanced Network > Firewall > Web Content Filters Tab



Configuration [Help]

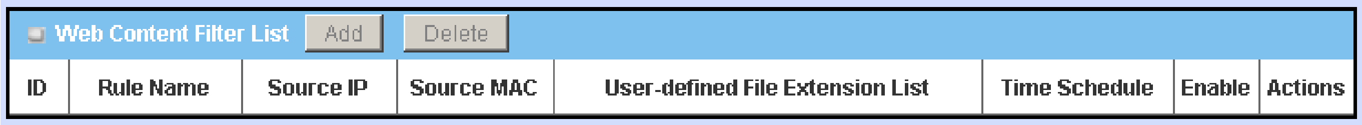
Item	Setting
Web Content Filters	□ Enable
Popular File Extension List	□ Cookie □ Java □ ActiveX
Log Alert	□ Enable

Index skipping is used to reserve slots for new function insertion, when required.

Web Content Filters Tab		
Item	**Value setting**	**Description**
Enable Web Content Filters function	The box is unchecked by default	Check the **Enable** box to activate this filter function
Popular File Extension List Selection	The boxes are unchecked by default	Check the **Cookie** box to activate this filter function, as the name suggests, this pattern matching rule define as the packet with the keyword **"Cookie:".** Check the **Java** box to activate this filter function, as the name suggests, this pattern matching rule define as the packet with the keyword ".js", ".class", ".jar", ".jsp", " .java", ".jse", ".jcm", ".jtk" , or ".jad". Check the **ActiveX** box to activate this filter function, as the name suggests, this pattern matching rule define as the packet with the keyword **".ocx", ".cab", ".ole", ".olb", ".com", ".vbs", ".vrm", or ".viv".** If one of the matching rules is found, the packets with http header will be dropped.
Log Alert	The box is unchecked by default	Check the **Enable** box to activate to activate Event Log.

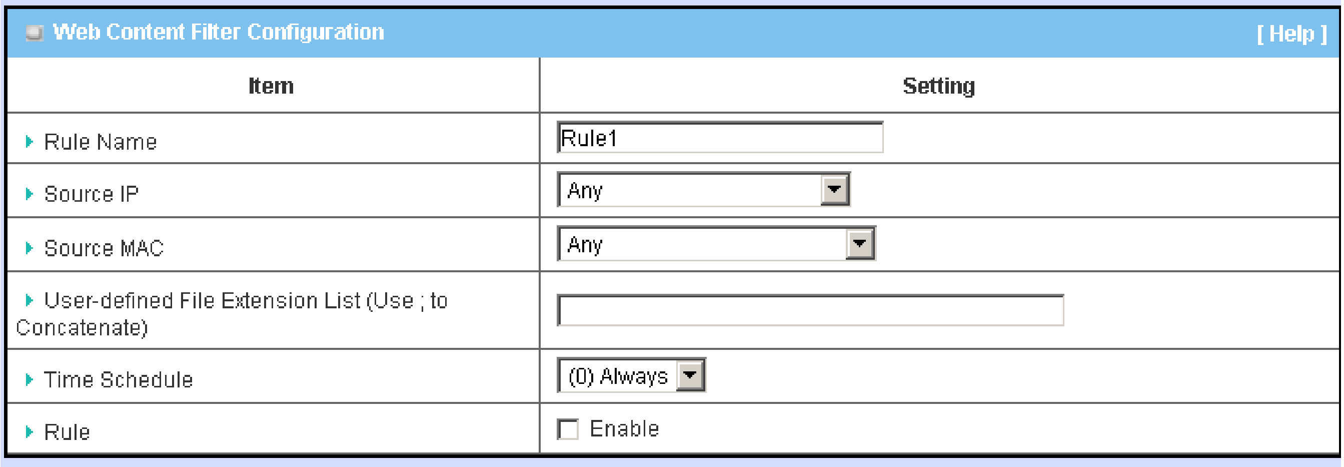
Create/Edit Filter Rules

The router supports up to a maximum of 20 filter rule sets. Ensure that the Web Content Filers is enabled before we can create filter rules.



ID	Rule Name	Source IP	Source MAC	User-defined File Extension List	Time Schedule	Enable	Actions

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



Item	Setting
Rule Name	Rule1
Source IP	Any
Source MAC	Any
User-defined File Extension List (Use ; to Concatenate)	
Time Schedule	(0) Always
Rule	□ Enable

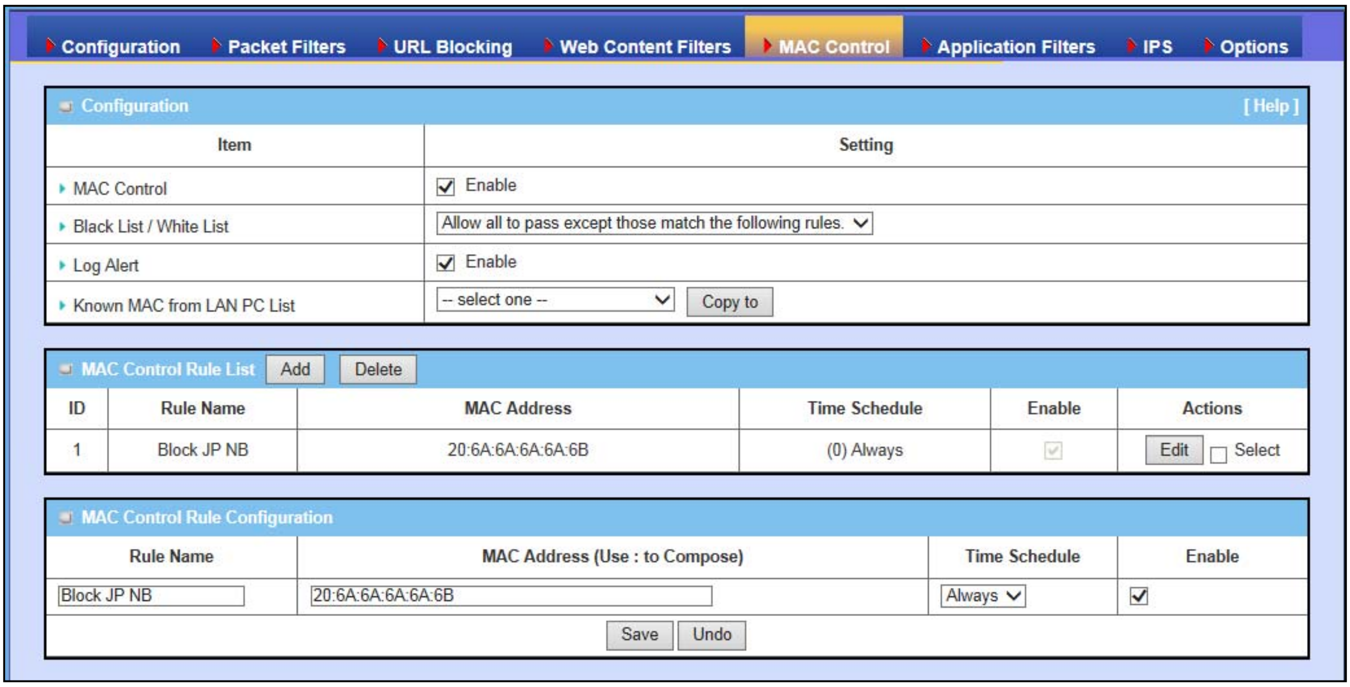
Index skipping is used to reserve slots for new function insertion, when required.

Web Content Filter Configuration		
Item	**Value setting**	**Description**
Rule Name	1. String format can be any text 2. A Must filled setting	Enter a web content filter rule name. Enter a name that is easy for you to understand.
Source IP	A Must filled setting	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 selection become available. Refer to **System** > **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	A Must filled setting	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 **System** > **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.
User-defined File Extension List (Use ; to Concatenate)	A Must filled setting	Specify file extension list to filtering rule. It supports up to a maximum of 10 file extension names in a rule by using the delimiter ";". If the matching rule is found, the packets with http header will be dropped.
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 System > Scheduling setting.
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 Web Content Filters Configuration page.

Index skipping is used to reserve slots for new function insertion, when required.

5.1.b 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.



Configuration [Help]

Item	Setting
MAC Control	☑ Enable
Black List / White List	Allow all to pass except those match the following rules.
Log Alert	☑ Enable
Known MAC from LAN PC List	-- select one -- [Copy to]

MAC Control Rule List [Add] [Delete]

ID	Rule Name	MAC Address	Time Schedule	Enable	Actions
1	Block JP NB	20:6A:6A:6A:6A:6B	(0) Always	☑	[Edit] □ Select

MAC Control Rule Configuration

Rule Name	MAC Address (Use : to Compose)	Time Schedule	Enable
Block JP NB	20:6A:6A:6A:6A:6B	Always	☑

[Save] [Undo]

In "MAC Control" page, there are three configuration windows for MAC control function. They are the "Configuration" window, "MAC Control Rule List" window, and "MAC Control Rule Configuration" window.

The "Configuration" window can let you activate the MAC Control function and specify to black listing or to white listing the devices in the "MAC Control Rule List" entry. Furthermore, log alerting can be enabled through an "Enable" checkbox to log events. Another "Known MAC from LAN PC List" is a tool that you can use to do quick copy the known MAC address of client hosts in the Intranet to facilitate creating rules. Use the "Copy to" button to copy. Second, the "MAC Control Rule List" window lists all your defined MAC control rule entry. At last, the "MAC Control Rule Configuration" window can let you define one MAC control rule.

Configuration

Check the "Enable" box to activate the "MAC Control" function. Select either the black list or the white list for following "MAC Control Rule List". Finally, enable the log alerting during MAC controlling process when needed.

When you choose "Allow all to pass except those match the following rules" for the "MAC Control Rule List", you are setting the defined MAC control rules to belong to the black list. The client hosts, listed in the rule list, in the Intranet will be rejected for the connection to the gateway if their MAC addresses match to one rule. Other client hosts can connect to the gateway. In contrast, when you choose "Deny all to pass except those match the following rules" for the "MAC Control Rule List", you are setting the defined MAC control rules to belong to the white list. The client hosts, listed in the rule, in the Intranet will be allowed for the connection to the gateway if their MAC addresses match to one rule. Other client hosts can't connect to the gateway.

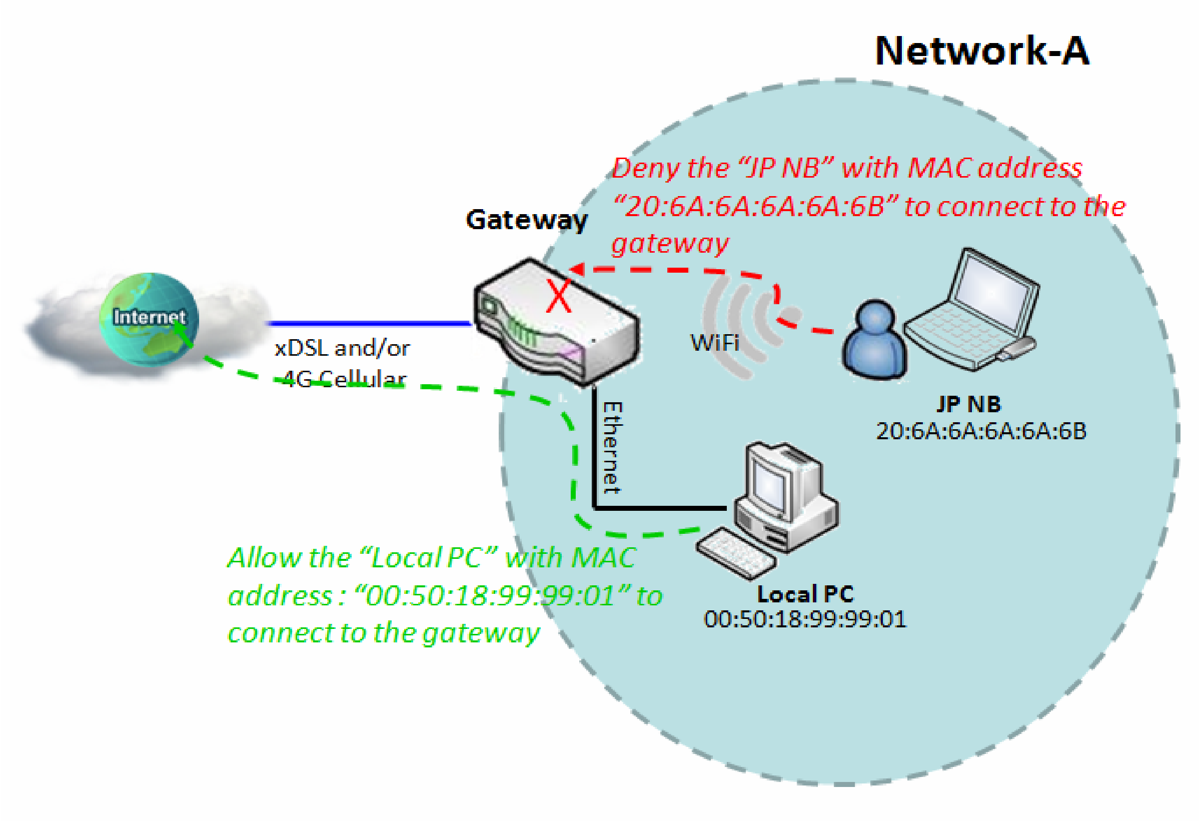
MAC Control Rule List

The "MAC Control Rule List" shows the setup parameters of all MAC control rules. There also be one "Add" button at the “MAC Control Rule List" caption, that can let you add and create one new MAC control rule. The "Edit" button at the end of each MAC control rule can let you modify the rule. Refer to the following sub-sections for more reference.

MAC Control Rule Configuration

When you want to add a new MAC control rule or edit one already existed, the "MAC Control Rule Configuration" window shows up for you to configure. The parameters in a rule include the rule name, the MAC address, the integrated time schedule rule and the rule activation. Refer to 6.2.1 Scheduling Settings section in this user manual on how to configure a time schedule. See following scenario for example.

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
Local PC
00:50:18:99:99:01
Allow the “Local PC” with MAC address : “00:50:18:99:99:01” to connect to the gateway

Index skipping is used to reserve slots for new function insertion, when required.

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.

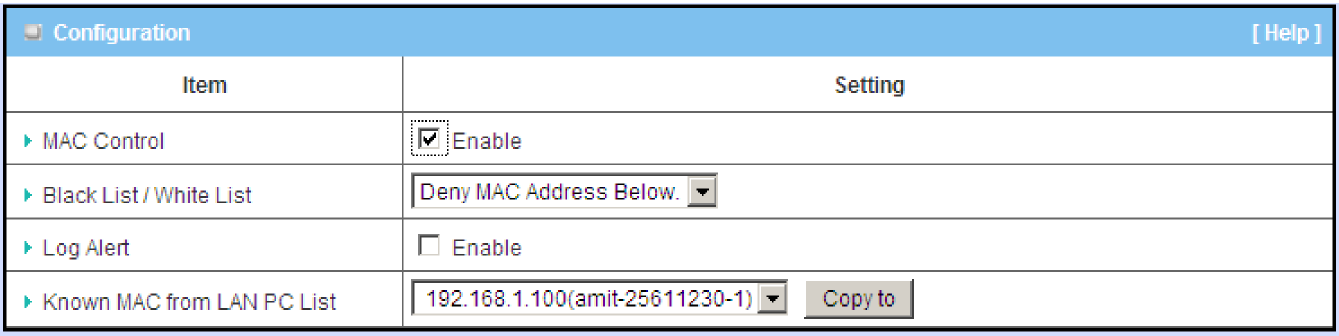
System will block the connecting from the "JP NB" to the gateway but allow others.

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 Advanced Network > Firewall > Configuration tab.

Enabling MAC Control

Go to Advanced Network > Firewall > MAC Control Tab



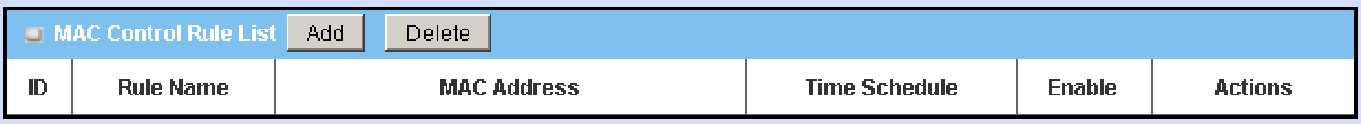
Item	Setting
MAC Control	☑ Enable
Black List / White List	Deny MAC Address Below. ▾
Log Alert	□ Enable
Known MAC from LAN PC List	192.168.1.100(amit-25611230-1) ▾ Copy to

Enabling MAC Control		
Item	**Value setting**	**Description**
Enable MAC Control function	The box is unchecked by default	Check the **Enable** box to activate the MAC filter function
Black List / White List (Filter Method Selection)	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 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

Index skipping is used to reserve slots for new function insertion, when required.

Create/Edit MAC Control Rules

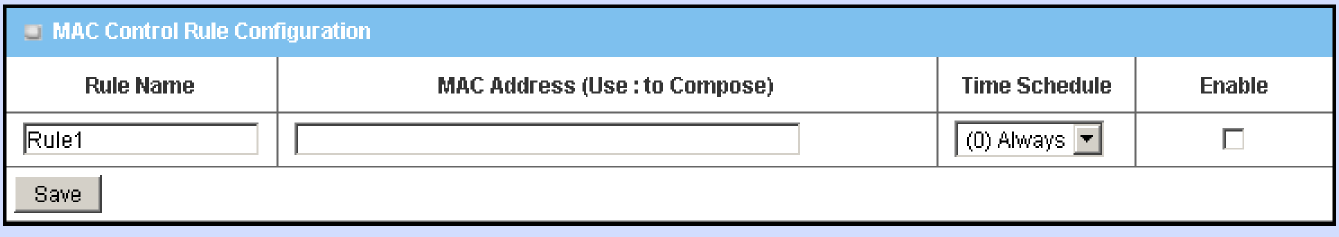
The router supports up to a maximum of 20 filter rule sets. Ensure that the MAC Control is enabled before we can create control rules.



MAC Control Rule List

ID	Rule Name	MAC Address	Time Schedule	Enable	Actions

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



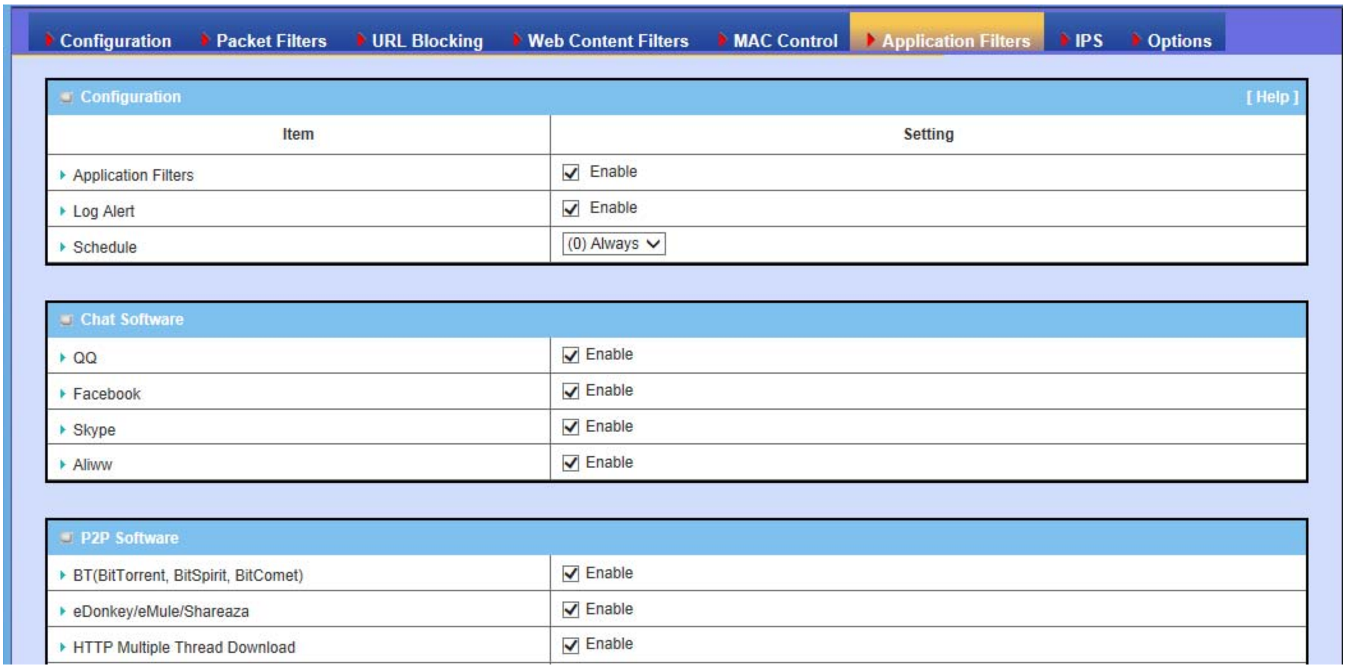
MAC Control Rule Configuration

Rule Name	MAC Address (Use : to Compose)	Time Schedule	Enable
Rule1		(0) Always	□

Create/Edit MAC Control Rules 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 (Ues: to Compose)	1. MAC Address string Format 2. A Must fill setting	Specify the **Source MAC Address** to filter rule.
Time Schedule	A Must fill 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 **System > Scheduling > Scheduling Setting tab**
Enabling the 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	Click Back button to return to the MAC Control Configuration page.

Index skipping is used to reserve slots for new function insertion, when required.

5.1.d Application Filters



Configuration [Help]

Item	Setting
Application Filters	☑ Enable
Log Alert	☑ Enable
Schedule	(0) Always

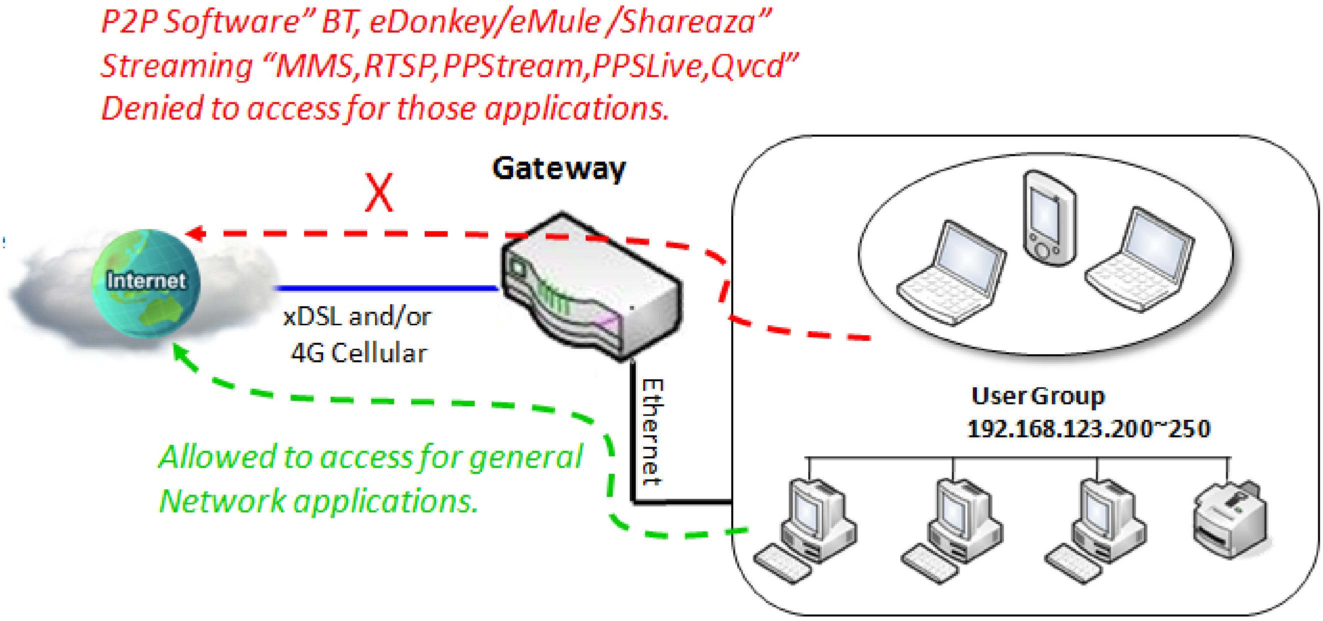
Chat Software

QQ	☑ Enable
Facebook	☑ Enable
Skype	☑ Enable
Aliww	☑ Enable

P2P Software

BT(BitTorrent, BitSpirit, BitComet)	☑ Enable
eDonkey/eMule/Shareaza	☑ Enable
HTTP Multiple Thread Download	☑ Enable

Application Filter function can categorize Internet Protocol packets based on their application layer data and allow or deny their passing of gateway. It supports the application filters for various Internet chat software, P2P download, Proxy, and A/V streaming. You can select the applications to be blocked after the function is enabled, and may also specify schedule rule to apply.


P2P Software" BT, eDonkey/eMule /Shareaza"
Streaming "MMS,RTSP,PPStream,PPSLive,Qvcd"
Denied to access for those applications.
X
Gateway
Internet
xDSL and/or
4G Cellular
Ethernet
User Group
192.168.123.200~250
Allowed to access for general
Network applications.

Scenario Application Timing

When the administrator of the gateway wants to block some P2P or Stream applications, he can use the "Application Filters" function to activate by checking the "Enable" box.

Scenario Description

Applications, by checking the "Enable" box, will be rejected or limited connection sessions to access the Internet.

Parameter Setup Example

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

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

Configuration Path	[Application Filters]-[Configuration]
Application Filter	■ ***Enable***
Log Alert	■ ***Enable***

Configuration Path	[Application Filters]-[Application Filter List]
Rule Name	***Rule 1***
Source IP	***IP Range : 192.168.123.200 - 192.168.123.250***
P2P Software	■***BT(BitTorrent, BitSpirit, BitComet)*** ■***eDonkey/eMule/Shareaza***
Streaming	■**MMS** ■**RTSP** ■**PPStream** ■**PPSLive** ■**Qvcd**
Rule	■ ***Enable***

Scenario Operation Procedure

In above diagram, the Gateway is the gateway as a NAT router. The subnet of Gateway is 192.168.123.0/24.

Select IP Range and entry IP Address 192.168.123.200 - 192.168.123.250

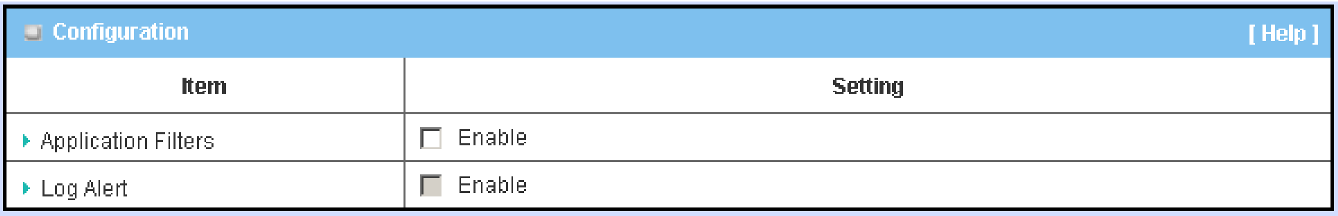
Enable the Application filters function and activate “BT(BitTorrent, BitSpirit, BitComet)”, “eDonkey/eMule/Shareaza”, “MMS”, “RTSP”, “PPStream”, “PPSLive” and “Qvcd” by checking the "Enable" box.

Application Filters Setting

The Application Filters setting allows user to create and customize Application Filters policies to reject packets related to specific applications through the router based on their office setting.

Go to Advanced Network > Firewall > Application Filters Tab

Index skipping is used to reserve slots for new function insertion, when required.



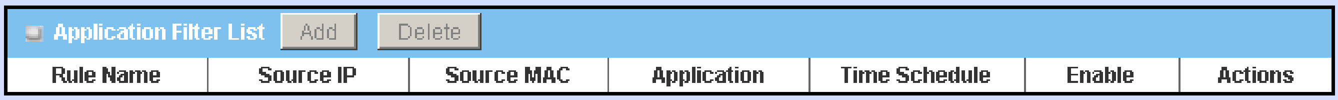
Configuration [Help]

Item	Setting
Application Filters	□ Enable
Log Alert	□ Enable

Application Filters		
Item Setting	**Value setting**	**Description**
Enable Application Filters function	The box is unchecked by default	Check the **Enable** box to activate this filter function
Log Alert	The box is unchecked by default	Check the **Enable** box to activate Event Log.

Create/Edit Filter Rules

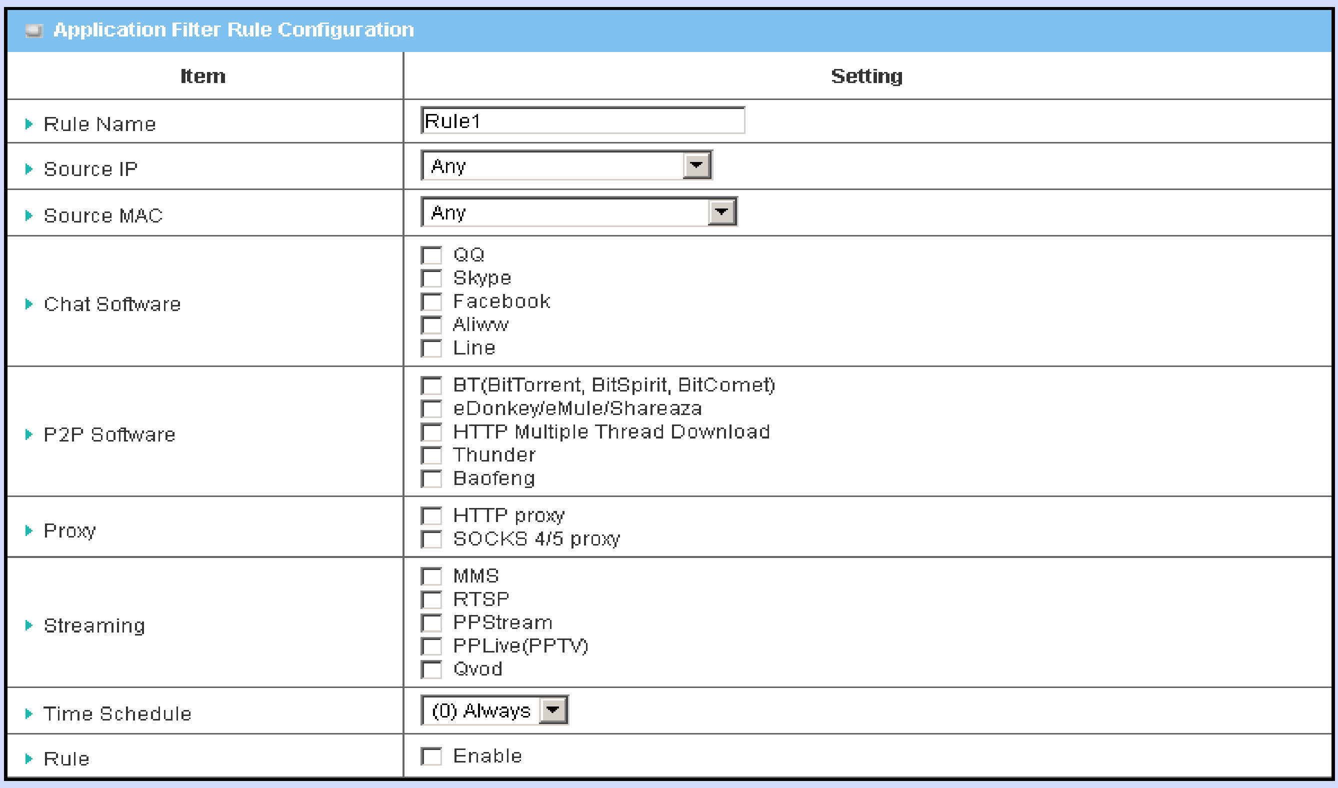
The router supports up to a maximum of 20 filter rule sets. Ensure that the Application Filers is enabled before we can create filter rules.



Application Filter List Add Delete

Rule Name	Source IP	Source MAC	Application	Time Schedule	Enable	Actions

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



Application Filter Rule Configuration

Item	Setting
Rule Name	Rule1
Source IP	Any
Source MAC	Any
Chat Software	□ QQ □ Skype □ Facebook □ Aliww □ Line
P2P Software	□ BT(BitTorrent, BitSpirit, BitComet) □ eDonkey/eMule/Shareaza □ HTTP Multiple Thread Download □ Thunder □ Baofeng
Proxy	□ HTTP proxy □ SOCKS 4/5 proxy
Streaming	□ MMS □ RTSP □ PPStream □ PPLive(PPTV) □ Qvod
Time Schedule	(0) Always
Rule	□ Enable

Index skipping is used to reserve slots for new function insertion, when required.

Application Filter Rule Configuration		
Item	**Value setting**	**Description**
Rule Name	1. String format can be any text 2. A Must filled setting	Enter a Application filter rule name. Enter a name that is easy for you to understand.
Source IP	A Must filled setting	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 selection become available. Refer to **System** > **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	A Must filled setting	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 **System** > **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.
Chat Software	All boxes are unchecked by default.	Check the boxes to activate the application filter functions you want on this rule**.**
P2P Software	All boxes are unchecked by default.	Check the boxes to activate the application filter functions you want on this rule**.**
Proxy	All boxes are unchecked by default.	Check the boxes to activate the application filter functions you want on this rule**.**
Streaming	All boxes are unchecked by default.	Check the boxes to activate the application filter functions you want on this rule**.**
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 **System** > **Scheduling setting**.
Enabling the rule	The box is unchecked by default.	Click **Enable** box to activate this rule then save the configuration.
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 Application Filters Configuration page.

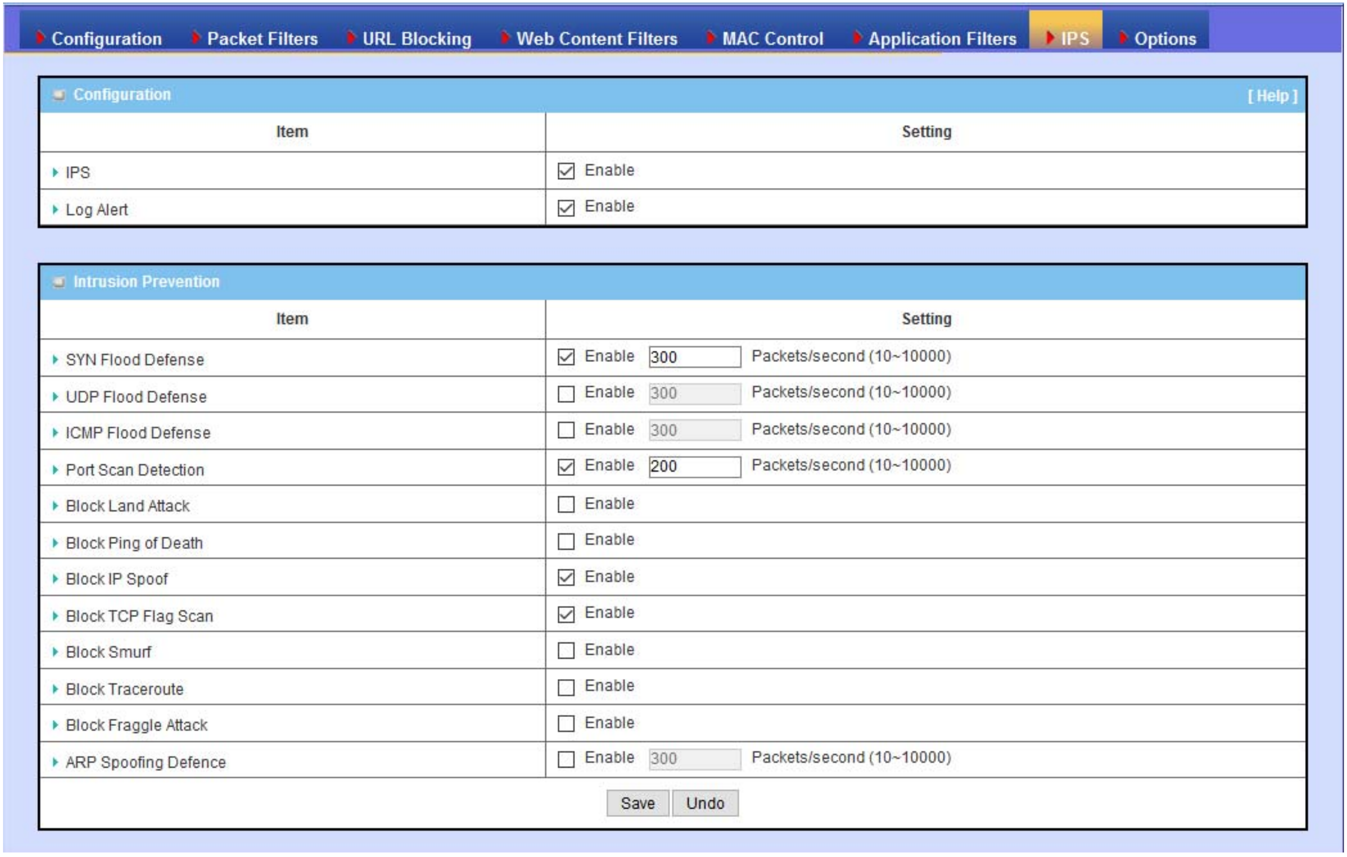
Index skipping is used to reserve slots for new function insertion, when required.

5.1.f IPS

Intrusion Prevention Systems are 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.

Configuration

Please check the "Enable" box to activate the "IPS" function and the log alerting when needed.



Configuration

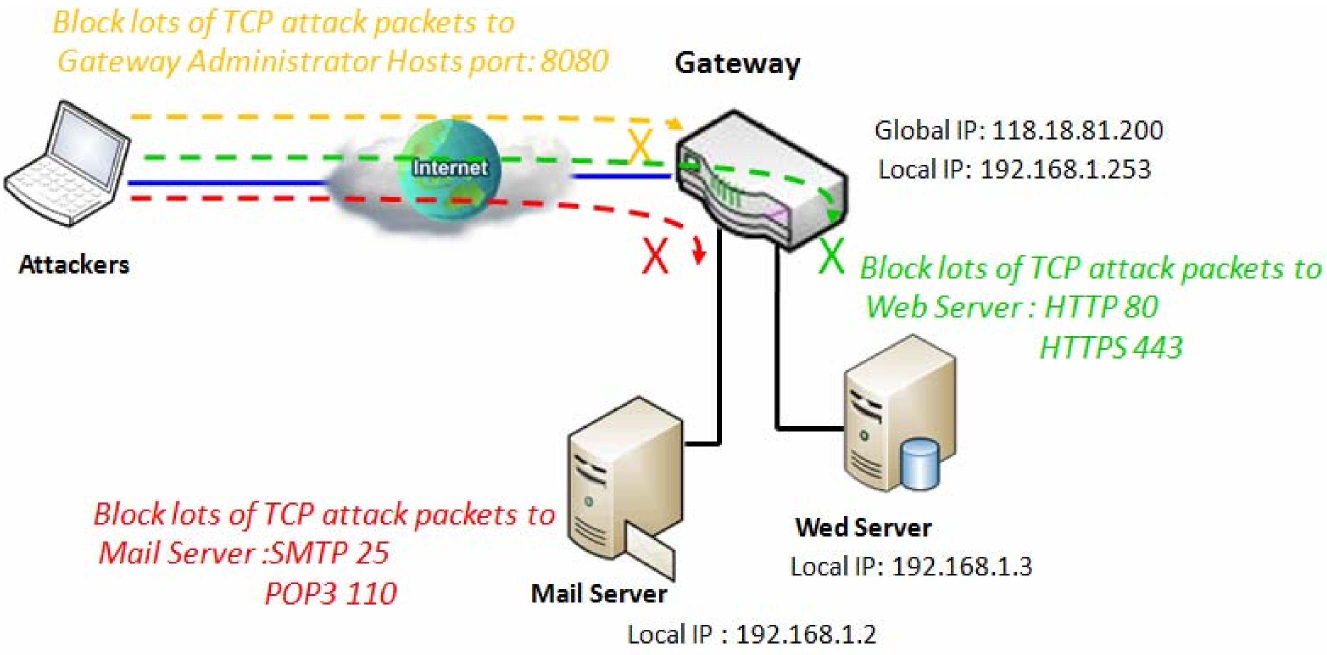
Item	Setting
IPS	☑ Enable
Log Alert	☑ Enable

Intrusion Prevention

Item	Setting
SYN Flood Defense	☑ Enable 300 Packets/second (10~10000)
UDP Flood Defense	□ Enable 300 Packets/second (10~10000)
ICMP Flood Defense	□ Enable 300 Packets/second (10~10000)
Port Scan 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)

The "Configuration" window can let you enable some features. In addition to enabling, you can specify threshold in packets per second for each detection.

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***

Index skipping is used to reserve slots for new function insertion, when required.

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.

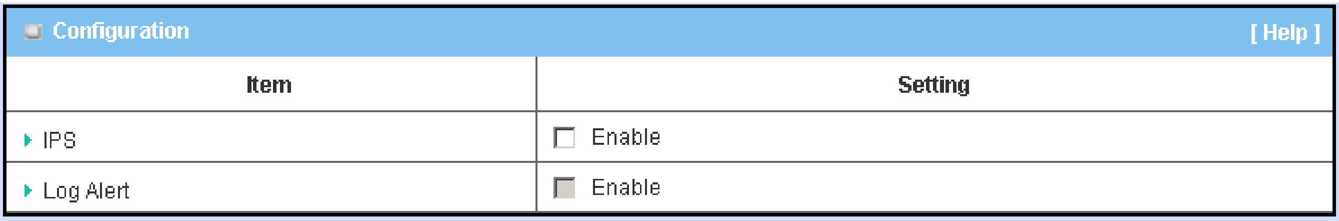
System will block lots of packets in seconds.

IPS Setting

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

Enabling IPS Firewall

Go to **Advanced Network** > **Firewall** > **IPS Tab**



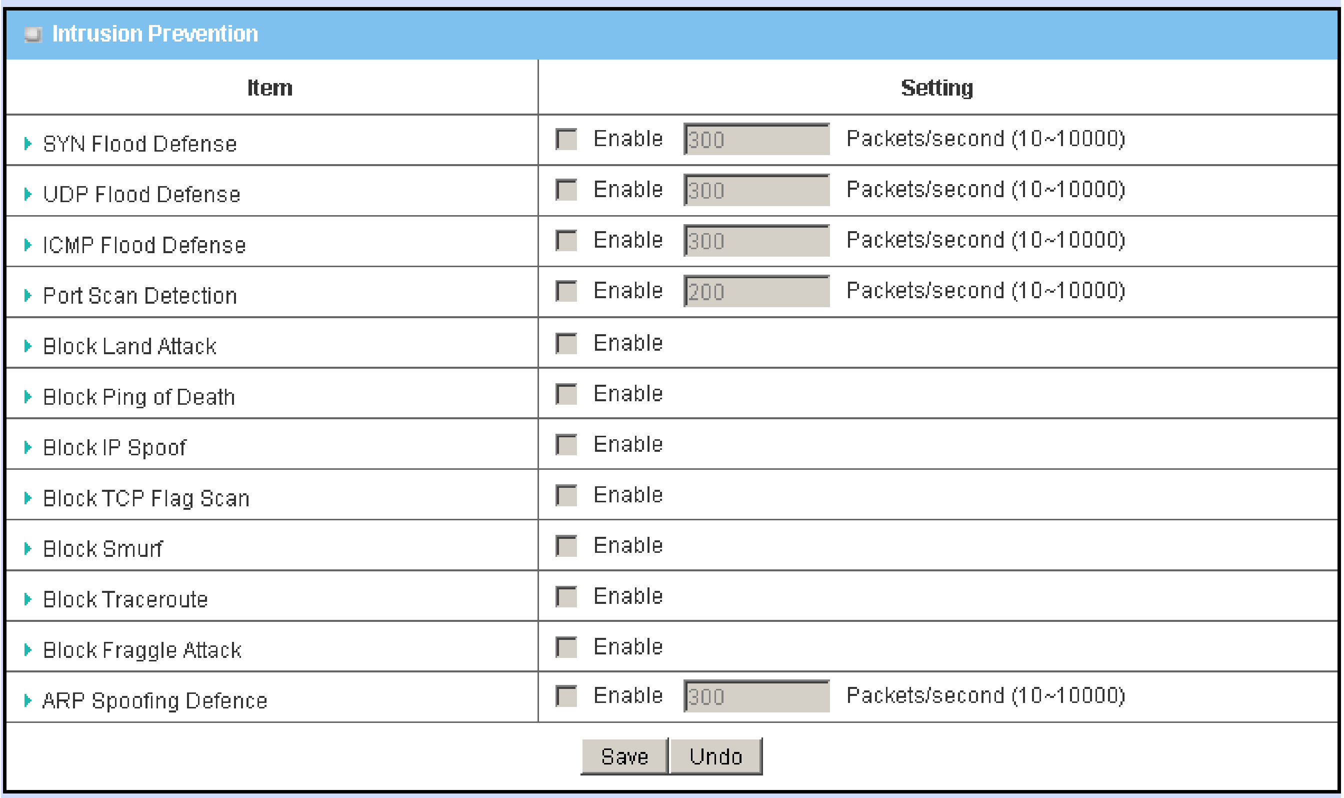
Item	Setting
IPS	□ Enable
Log Alert	□ Enable

Enabling IPS Firewall		
Item	**Value setting**	**Description**
Enable IPS function	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 to activate Event Log.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Index skipping is used to reserve slots for new function insertion, when required.

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 defenses.



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)

Setup Intrusion Prevention Rules		
Item Name	**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	The box is unchecked by default.	Click **Enable** box to activate this intrusion prevention rule.

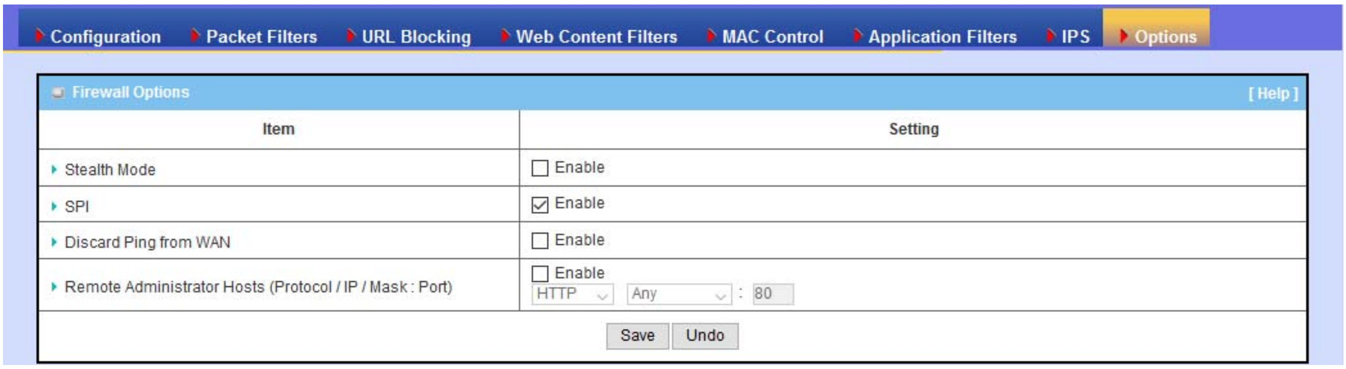
		Index skipping is used to reserve slots for new function insertion, when required.
Block Ping of Death **Block IP Spoof** **Block TCP Flag Scan** **Block Smurf** **Block Traceroute** **Block Fraggle Attack**		
ARP Spoofing Defence	1. A Must filled setting 2. The box is unchecked by default. 3. traffic 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

5.1.h Options

There are some useful functions in this page. “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. ”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. “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. “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'.

Firewall Options

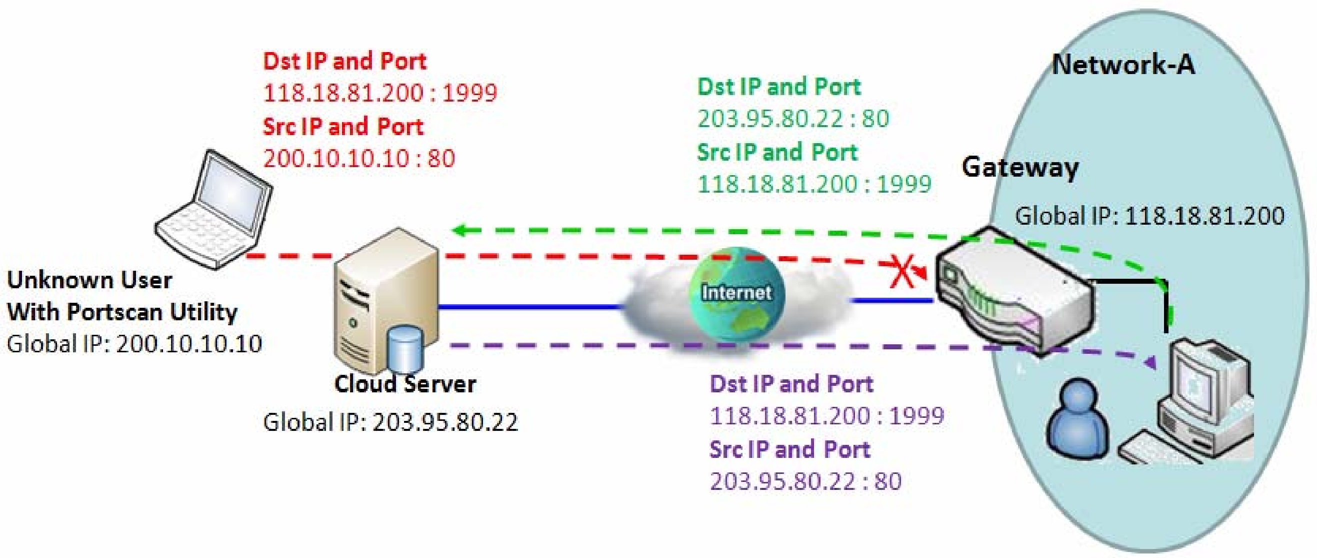
Please check the "Enable" box to activate the functions needed.



Firewall Options [Help]

Item	Setting
Stealth Mode	□ Enable
SPI	☑ Enable
Discard Ping from WAN	□ Enable
Remote Administrator Hosts (Protocol / IP / Mask : Port)	□ Enable HTTP Any : 80

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

In order 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

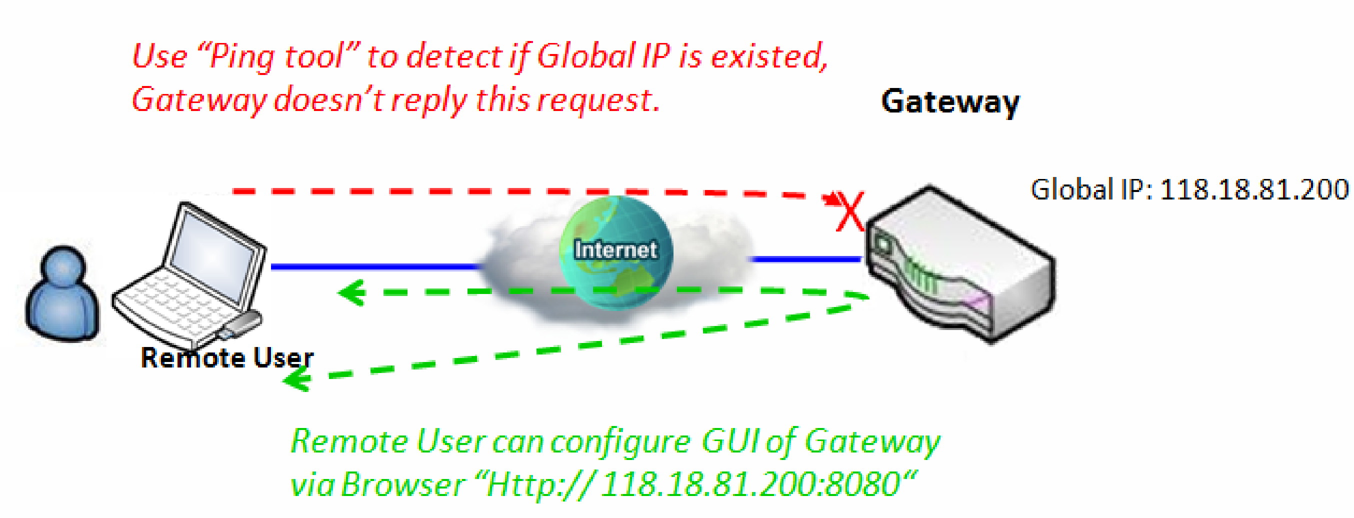
In above diagram, the Gateway is the gateway of Network-A and the subnet of its Intranet is 10.0.75.0/24. The gateway has the IP address of 10.0.75.2 for LAN interface and 118.18.81.200 for WAN interface. It serves as a NAT router.

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

In order 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.

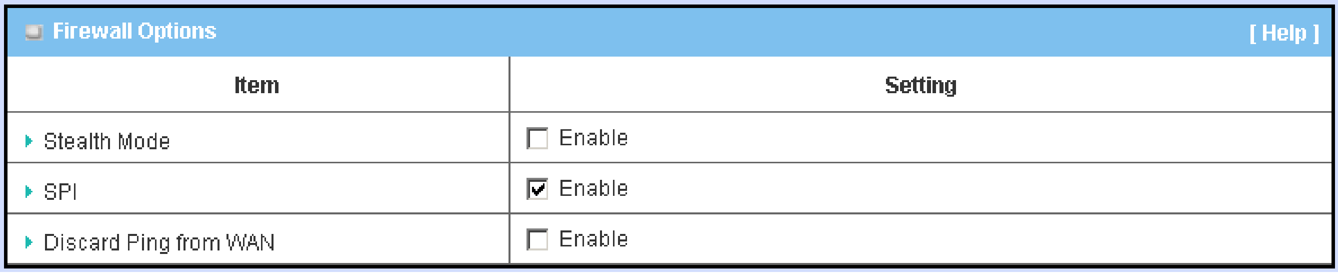
Remote users can't get response via Ping Utility, but can access the web-based utility of Gateway via port 8080 of TCP.

Firewall Setting

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

Enabling Firewall Options

Go to **Advanced Network** > **Firewall** > **Options Tab**



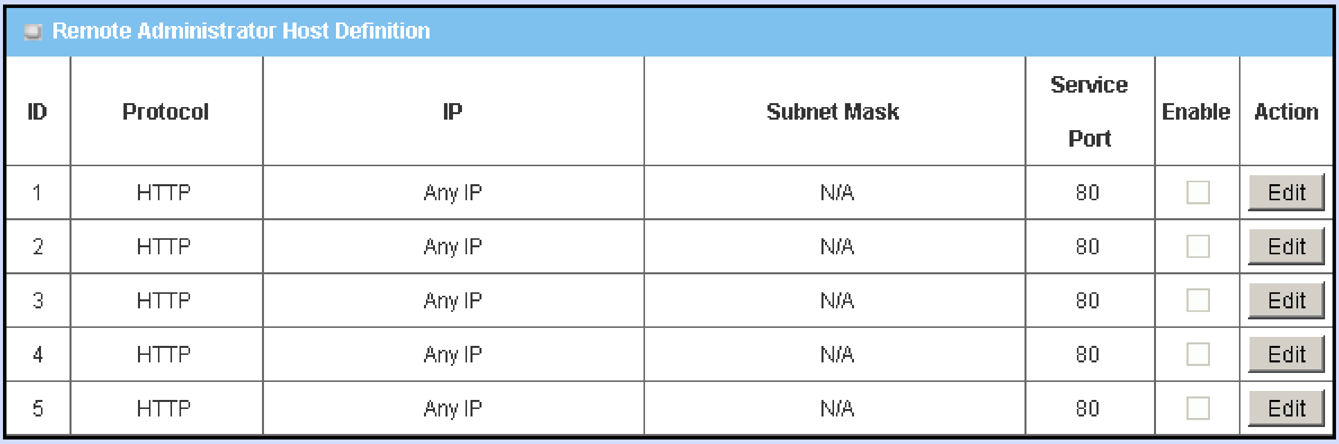
Firewall Options [Help]

Item	Setting
Stealth Mode	□ Enable
SPI	☑ Enable
Discard Ping from WAN	□ Enable

Enabling Firewall Options		
Item	**Value setting**	**Description**
Enable Stealth mode function	The box is unchecked by default	Check the **Enable** box to activate Stealth Mode function
Enable SPI function	The box is checked by default	Check the **Enable** box to activate SPI function
Discard Ping from WAN	The box is unchecked by default	Check the **Enable** box to activate Discarding Ping function

Remote Router Access Control

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	Protocol	IP	Subnet Mask	Service Port	Enable	Action
1	HTTP	Any IP	N/A	80	□	Edit
2	HTTP	Any IP	N/A	80	□	Edit
3	HTTP	Any IP	N/A	80	□	Edit
4	HTTP	Any IP	N/A	80	□	Edit
5	HTTP	Any IP	N/A	80	□	Edit

Index skipping is used to reserve slots for new function insertion, when required.

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

Index skipping is used to reserve slots for new function insertion, when required.

5.3 QoS & BWM

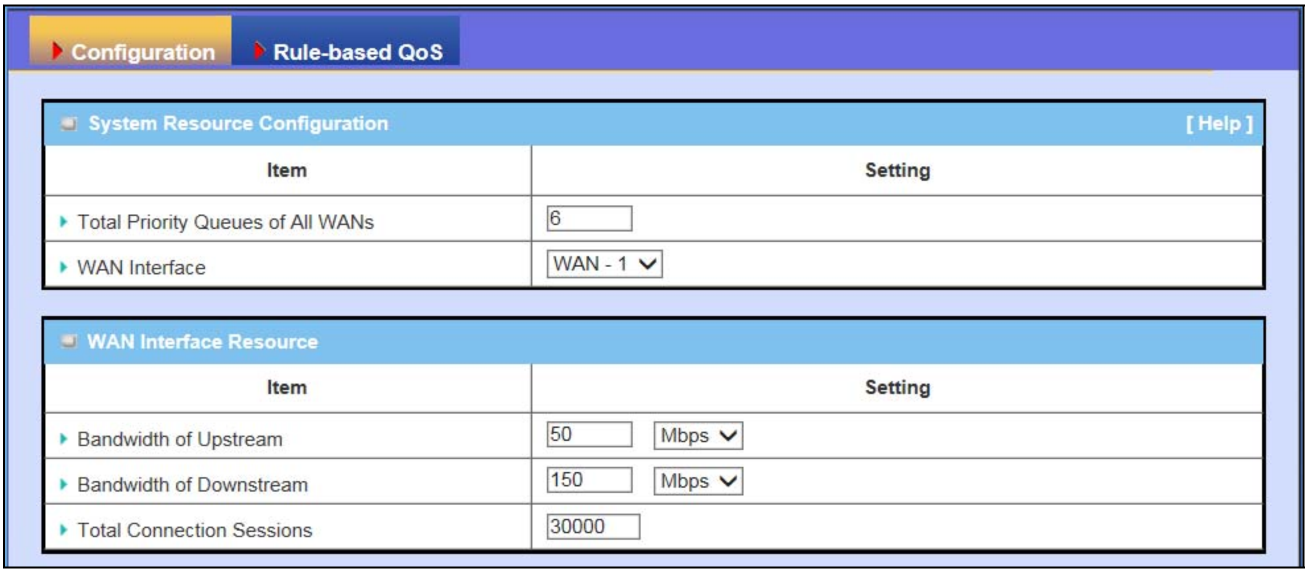
The total amount of data traffic increases nowadays as the higher demand of mobile applications, like Game / Chat / VoIP / P2P / Video / Web access. In order to pose new requirements for data transport, e.g. low latency, low data loss, the entire network must ensure them via a connection service guarantee.

The main goal of QoS & BWM (Quality of Service and Bandwidth Management) 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. AMIT Security Gateway provides a Rule-based QoS to carry out the requirements.

5.3.1 Configuration

AMIT gateways adopt rule-based approach to define the QoS & BWM function. Before the function works as expected, some system resources must be allocated correctly in "Configuration" page as below.



System Resource Configuration [Help]

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

WAN Interface Resource

Item	Setting
Bandwidth of Upstream	50 Mbps
Bandwidth of Downstream	150 Mbps
Total Connection Sessions	30000

In "Configuration" page, there are some configuration windows for QoS & BWM function. They are the "System Resource Configuration" window and "WAN Interface Resource" window. The number of supported WAN interfaces in the gateway will have same number of "WAN Interface Resource" windows available. Specify a WAN interface in the "System Resource Configuration" window with which the bandwidth will be managed, and then configure the Bandwidth resource for that WAN interface in the corresponding "WAN Interface Resource" window. The system resource information provides important parameters for the QoS & BWM function. Incorrect information will result in poor bandwidth utilization.

System Resource Configuration

The gateway system needs to know some system resource status for QoS & BWM function to work normally. The system resources include the number of total priority queues in system and the resource status for each WAN interface.

WAN Interface Resource

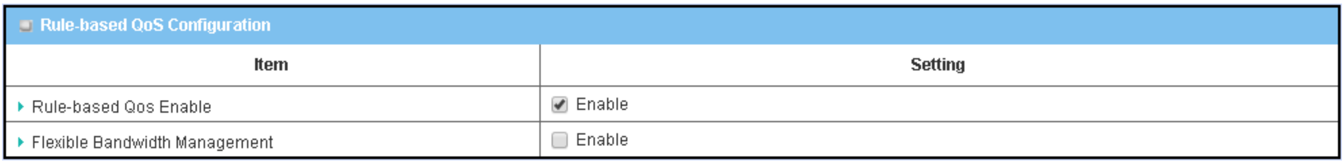
Each WAN interface should be configured carefully for its upstream bandwidth, downstream bandwidth and maximum number of connection sessions.

The Configuration of QoS allows user to configure total bandwidth and session of each WAN.

Index skipping is used to reserve slots for new function insertion, when required.

Ensure QoS are enabled and saved

Go to Advanced Network > QoS & BWM > Rule-based QoS Tab

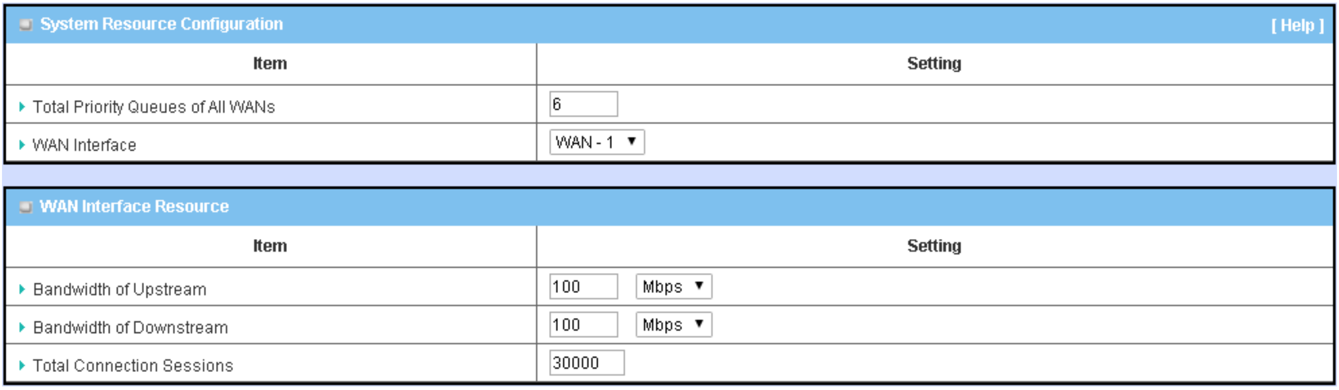


Rule-based QoS Configuration

Item	Setting
Rule-based Qos Enable	☑ Enable
Flexible Bandwidth Management	☐ Enable

Configure Bandwidth and Session

Go to Advanced Network > QoS & BWM > Configuration Tab



System Resource Configuration [Help]

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

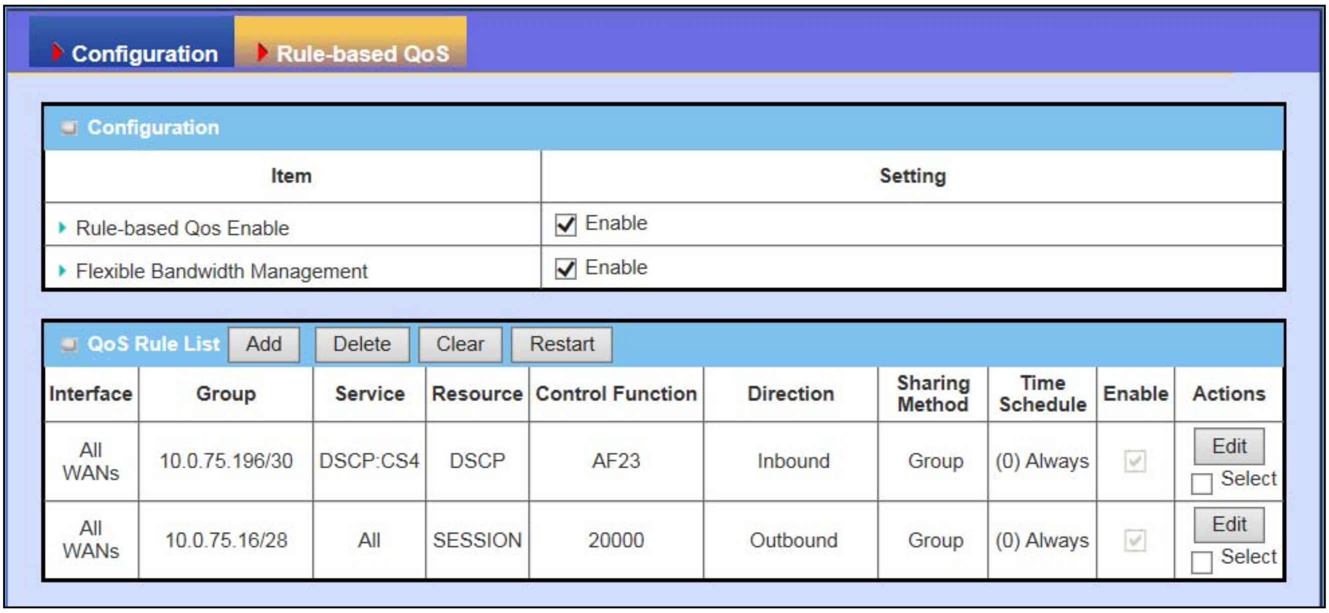
WAN Interface Resource

Item	Setting
Bandwidth of Upstream	100 Mbps ▼
Bandwidth of Downstream	100 Mbps ▼
Total Connection Sessions	30000

System Resource Configuration Item	Value setting	Description
Total Priority Queues of All WANs	A Must filled setting	Define the total priority that is related to configure of each rule-based QoS if select **Priority Queues** of **Resource.** It is also related to default banwidth of WANs.
WAN Interface	By default **WAN-1** is selected.	Select **WAN-1** and then the following will show setting function that you can configure. (WAN-1 is available only when WAN-1 interface is enabled) The same applies to other WAN interfaces (i.e. **WAN-2**). Bandwidth of Upstream Specify total upload bandwidth of WAN-n. Bandwidth of Downstream Specify total download bandwidth of WAN-n. Total Connection Sessions Specify total connection sessions of WAN-n
Save	N/A	Click the **Save** button to save the settings.

5.3.3 Rule-based QoS

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.



Configuration

Item	Setting
Rule-based Qos Enable	☑ Enable
Flexible Bandwidth Management	☑ Enable

Interface	Group	Service	Resource	Control Function	Direction	Sharing Method	Time Schedule	Enable	Actions
All WANs	10.0.75.196/30	DSCP:CS4	DSCP	AF23	Inbound	Group	(0) Always	☑	Edit □ Select
All WANs	10.0.75.16/28	All	SESSION	20000	Outbound	Group	(0) Always	☑	Edit □ Select

In "Rule-based QoS" page, there are three configuration windows for QoS & BWM function. They are the "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 "QoS Rule List" window lists all your defined QoS rules. At last, the "QoS Rule Configuration" window can let you define one QoS rule.

Configuration

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.

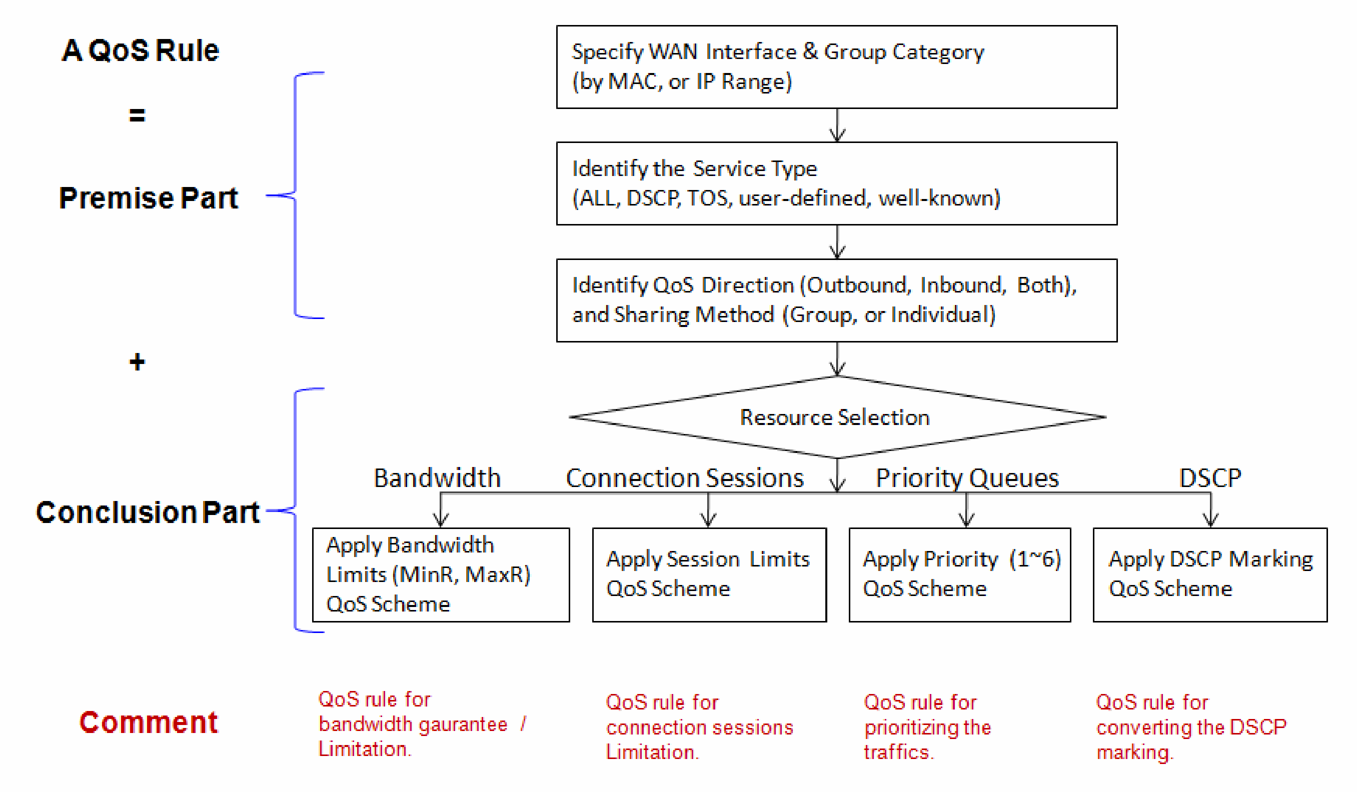
Index skipping is used to reserve slots for new function insertion, when required.

QoS Rule List

The "QoS Rule List" shows the parameter settings of all QoS rule entry. There also be one "Add" button at the "QoS Rule List" caption, that can let you add and create one new QoS rule. The "Edit" button at the end of each QoS rule can let you modify the rule. Please see following sub-section. Refer to the following sub-sections for more reference.

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. Refer to 6.2.1 Scheduling Settings section in this user manual on how to configure a time schedule. Following diagram illustrates how to organize an QoS rule.


A QoS Rule
=
Premise Part
+
Conclusion Part
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
Comment
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 diagram above, 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.

Flexible QoS Rule Definition

Multiple Group Categories

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

Group Category can bases on VLAN ID, MAC Address, IP Address, Host Name or Packet Length. Category depends on product model.

Differentiated Services

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

Differentiated services can be base 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

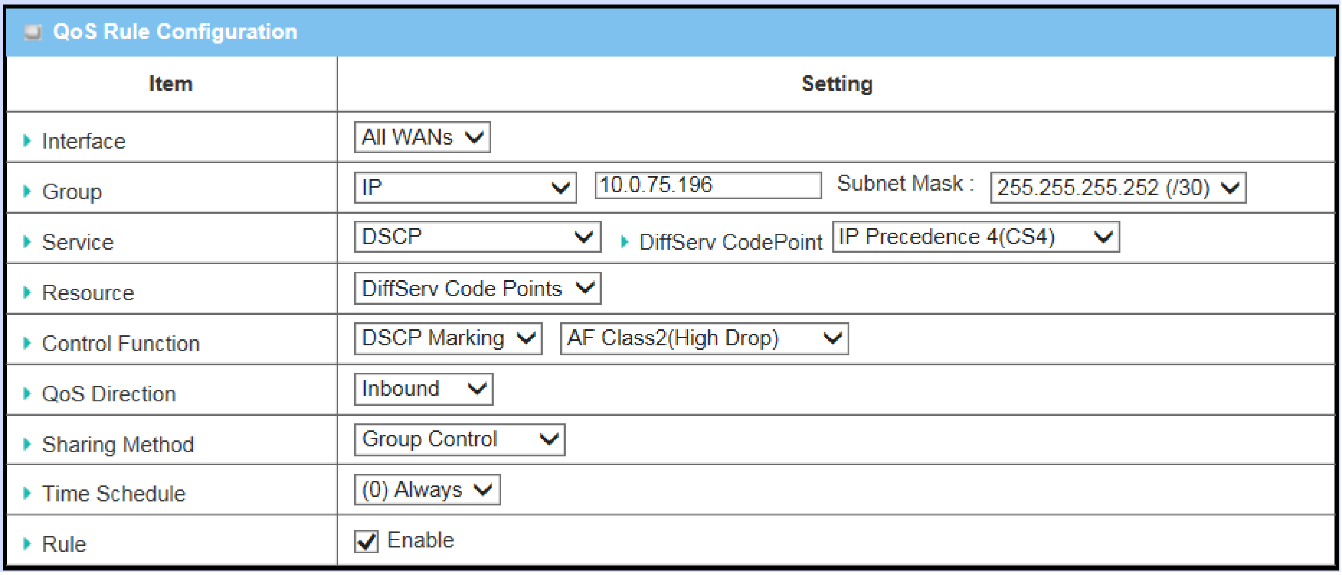
One QoS rule can be applied to individual member or whole group in the target group. This feature depends on model.

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***

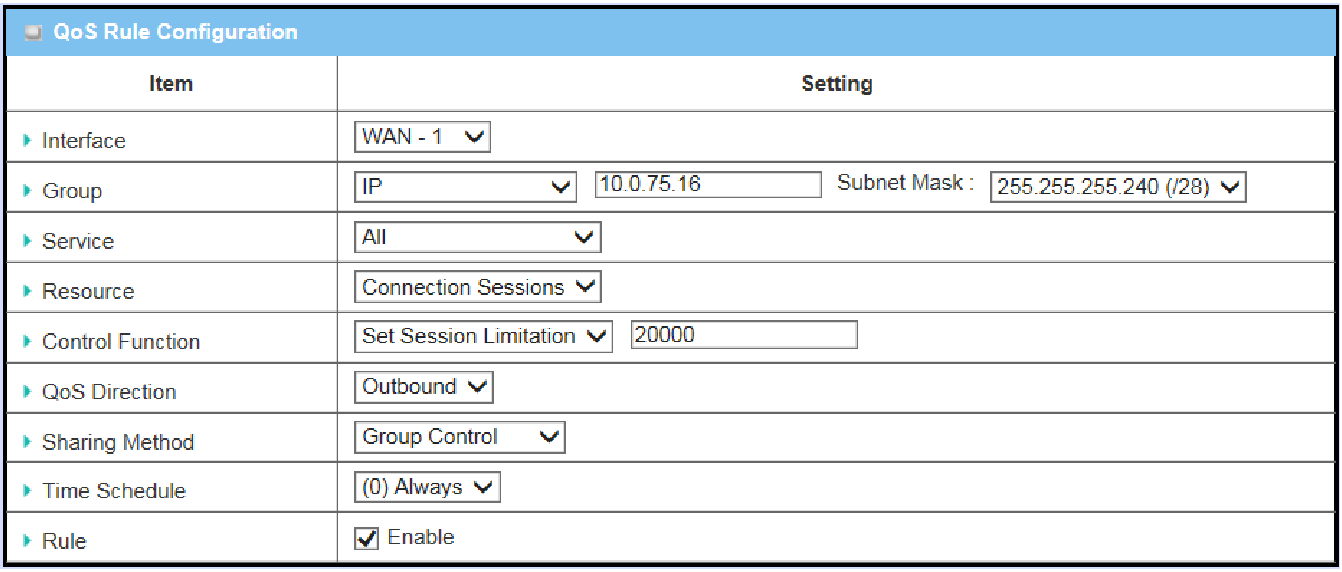
Index skipping is used to reserve slots for new function insertion, when required.

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***

Index skipping is used to reserve slots for new function insertion, when required.

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***

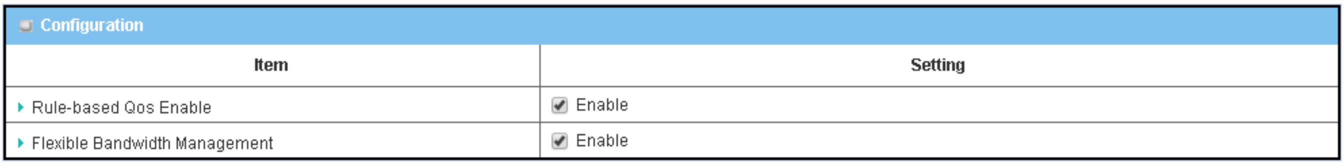
Scenario Operation Procedure

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

The Rule Based QoS allows user to configure QoS and bandwidth to set the limitation of total bandwidth of each WAN connection.

Ensure QoS and Bandwidth are enabled and saved

Go to Advanced Network > QoS & BWM > Rule-based QoS Tab



Configuration

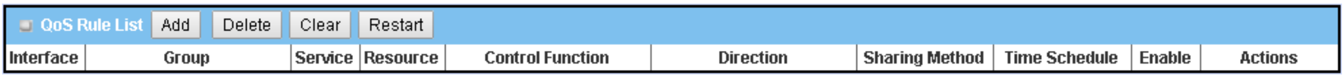
Item	Setting
Rule-based Qos Enable	☑ Enable
Flexible Bandwidth Management	☑ Enable

Configuration Item	Value setting	Description
Rule-based QoS Enable	The box is unchecked by default	When Check the **Enable** box It will activate Rule-based QoS functions.
Flexible Bandwidth Management	The box is unchecked by default	When Check the **Enable** box It will activate Flexible Bandwidth Management function.
Save	N/A	Click the **Save** button to save the settings.

Index skipping is used to reserve slots for new function insertion, when required.

Create/Edit QoS Rules

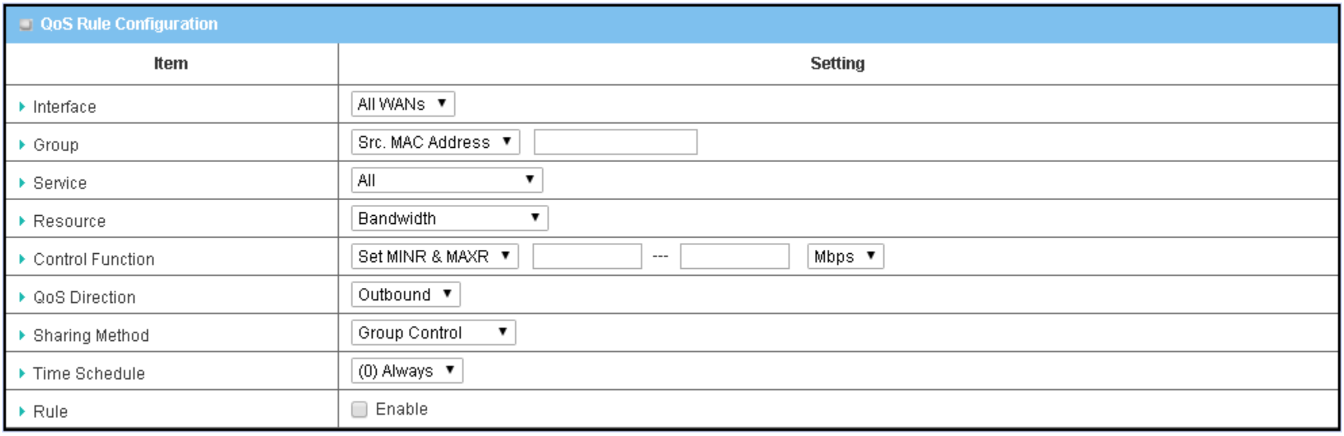
The QoS & BWM allows you to custom your rule-based QoS rules. The router supports up to a maximum of 128 rule-based QoS rule sets.



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 ▼
Sharing Method	Group Control ▼
Time Schedule	(0) Always ▼
Rule	□ Enable

QoS Rule Configuration		
Item	**Value setting**	**Description**
Interface	A Must filled setting	Define the selected interface to be the packet-entering/packet-leaving interface of the router. Select **All WANs** to filter the packets entering to or leaving from any WAN interface. Select **WAN-1** to filter the packets entering to or leaving from WAN-1. (WAN-1 is available only when WAN-1 interface is enabled) The same applies to other WAN interfaces **(i.e. WAN-2).**
Group	A Must filled setting	This field is to specify the **Group** of the interface selected in the **Interface** setting above. 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 preconfigured group of host from the dropdown list. If the dropdown list empty ensure if any group is pre-configured **(Note_1)** and ensure that QoS is enabled in the group **(Note_2)**. Configure **Service** in the next line, then go to **Resource_3.** **Note_1:** Group must be pre-defined before this selection become available. Refer to **System > 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. **Note_2:** Ensure that QoS in the **Multiple Bound Services** field is checked. Refer to System > Grouping > Host grouping then click Edit button of one of the host group created.
Service	A Must filled setting	Select **All** to filter packets entering to or leaving from any service. Select **DSCP** to filter packets entering to or leaving from a DSCP packet type. Select **TOS** to filter packets entering to or leaving from a TOS packet type. Select **User-defined Service** to filter packets entering to or leaving from a user-defined port or port range, and the protocol could be TCP/UDP/Both protocol for these ports. Select **Well-known Service** to filter packets entering to or leaving from a well-known service list.
Resource_1 (for Group Src. MAC Address settings only)	A Must filled setting	Specify resource to the QoS rule. When **Bandwidth** is selected It means the option Resource of rule-based QoS Rule is bandwidth. In Control Function when Set MINR & MAXR is selected It means the option Control Function of rule-based QoS Rule is set MINR & MAXR. You can assign min rate, max rate and rate unit for this rule. **QoS Direction** (A Must filled setting) When **Outbound** is selected It means the option QoS Direction of rule-based QoS Rule is outbound. Outbound means the Group option is a source group. When **Inbound** is selected It means the option QoS Direction of rule-based QoS Rule is inbound. Inbound means the Group option is a destination group. When **Both** is selected It means the option QoS Direction of rule-based QoS Rule is both. **Time Schedule** (A Must filled setting) Apply **Time Schedule** to this rule**,** otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **System)** Enabling the rule Click **Enable** box to activate this rule. Click the **Save** button to save the settings
		When Connection Sessions is selected It means the option Resource of rule-based QoS Rule is connection sessions. In Control Function when Set Session Limitation is selected It means the option Control Function of rule-based QoS Rule is set session limitation. You must fill the session number in the textbox. **QoS Direction** (A Must filled setting) When **Outbound** is selected It means the option QoS Direction of rule-based QoS Rule is outbound. Outbound means the Group option is a source group. When **Inbound** is selected

Index skipping is used to reserve slots for new function insertion, when required.

	It means the option QoS Direction of rule-based QoS Rule is inbound. Inbound means the Group option is a destination group. When **Both** is selected It means the option QoS Direction of rule-based QoS Rule is both. **Time Schedule** (A Must filled setting) Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **System)** Enabling the rule Click **Enable** box to activate this rule. Click the **Save** button to save the settings
	When **Priority Queues** is selected It means the option Resource of rule-based QoS Rule is priority queues. In Control Function when Set Priority is selected It means the option Control Function of rule-based QoS Rule is set priority. You must fill the priority queue number in the textbox. Each priority have its own bandwidth. **QoS Direction** (A Must filled setting) When **Outbound** is selected It means the option QoS Direction of rule-based QoS Rule is outbound. Outbound means the Group option is a source group. When **Inbound** is selected It means the option QoS Direction of rule-based QoS Rule is inbound. Inbound means the Group option is a destination group. When **Both** is selected It means the option QoS Direction of rule-based QoS Rule is both. **Time Schedule** (A Must filled setting) Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **System)** Enabling the rule Click **Enable** box to activate this rule. Click the **Save** button to save the settings
	When DiffServ Code Points is selected It means the option Resource of rule-based QoS Rule is DiffServ Code Points. In Control Function when DSCP Marking is selected It means the option Control Function of rule-based QoS Rule is DSCP marking. You must select one from the list. DSCP Marking will mark with Code Point in Packet. **QoS Direction** (A Must filled setting) When **Outbound** is selected It means the option QoS Direction of rule-based QoS Rule is outbound. Outbound means the Group option is a source group. When **Inbound** is selected It means the option QoS Direction of rule-based QoS Rule is inbound. Inbound means the Group option is a destination group. When **Both** is selected It means the option QoS Direction of rule-based QoS Rule is both.

Index skipping is used to reserve slots for new function insertion, when required.

		Time Schedule (A Must filled setting) Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **System)** Enabling the rule Click **Enable** box to activate this rule. Click the **Save** button to save the settings
Resource_2 (for Group IP settings only)	A Must filled setting	Specify resource to the QoS rule. Select **Bandwidth** is selected It means the option Resource of rule-based QoS Rule is bandwidth. In Control Function when Set MINR & MAXR is selected It means the option Control Function of rule-based QoS Rule is set MINR & MAXR. You can assign min rate, max rate and rate unit for this rule. **QoS Direction** (A Must filled setting) When **Outbound** is selected It means the option QoS Direction of rule-based QoS Rule is outbound. Outbound means the Group option is a source group. When **Inbound** is selected It means the option QoS Direction of rule-based QoS Rule is inbound. Inbound means the Group option is a destination group. When **Both** is selected It means the option QoS Direction of rule-based QoS Rule is both. **Sharing Method** (A Must filled setting) When **Individual Control** is selected, It means the option Sharing Method of rule-based QoS Rule is Individual Control. When **Group Control** is selected, It means the option Sharing Method of rule-based QoS Rule is Group Control. **Time Schedule** (A Must filled setting) Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **System)** Enabling the rule Click **Enable** box to activate this rule. Click the **Save** button to save the settings
		When Connection Sessions is selected It means the option Resource of rule-based QoS Rule is connection sessions. In Control Function when Set Session Limitation is selected It means the option Control Function of rule-based QoS Rule is set session limitation. You must fill the session number in the textbox. **QoS Direction** (A Must filled setting) When **Outbound** is selected It means the option QoS Direction of rule-based QoS Rule is outbound. Outbound means the Group option is a source group. When **Inbound** is selected It means the option QoS Direction of rule-based QoS Rule is inbound. Inbound means the Group option is a destination group. When **Both** is selected

Index skipping is used to reserve slots for new function insertion, when required.

	It means the option QoS Direction of rule-based QoS Rule is both. **Sharing Method** (A Must filled setting) When **Individual Control** is selected, It means the option Sharing Method of rule-based QoS Rule is Individual Control. When **Group Control** is selected, It means the option Sharing Method of rule-based QoS Rule is Group Control. **Time Schedule** (A Must filled setting) Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **System)** Enabling the rule Click **Enable** box to activate this rule. Click the **Save** button to save the settings
	When **Priority Queues** is selected It means the option Resource of rule-based QoS Rule is priority queues. In Control Function when Set Priority is selected It means the option Control Function of rule-based QoS Rule is set priority. You must fill the priority queue number in the textbox. Each priority have its own bandwidth. **QoS Direction** (A Must filled setting) When **Outbound** is selected It means the option QoS Direction of rule-based QoS Rule is outbound. Outbound means the Group option is a source group. When **Inbound** is selected It means the option QoS Direction of rule-based QoS Rule is inbound. Inbound means the Group option is a destination group. When **Both** is selected It means the option QoS Direction of rule-based QoS Rule is both. **Time Schedule** (A Must filled setting) Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **System)** Enabling the rule Click **Enable** box to activate this rule. Click the **Save** button to save the settings
	When DiffServ Code Points is selected It means the option Resource of rule-based QoS Rule is DiffServ Code Points. In Control Function when DSCP Marking is selected It means the option Control Function of rule-based QoS Rule is DSCP marking. You must select one from the list. DSCP Marking will mark with Code Point in Packet. **QoS Direction** (A Must filled setting) When **Outbound** is selected It means the option QoS Direction of rule-based QoS Rule is outbound. Outbound means the Group option is a source group. When **Inbound** is selected It means the option QoS Direction of rule-based QoS Rule is inbound. Inbound means the Group option is a destination group.

Index skipping is used to reserve slots for new function insertion, when required.

		When **Both** is selected It means the option QoS Direction of rule-based QoS Rule is both. **Time Schedule** (A Must filled setting) Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **System)** Enabling the rule Click **Enable** box to activate this rule. Click the **Save** button to save the settings
Resource_3 (for Group Host Name settings only)	A Must filled setting	Specify resource to the QoS rule. When **Bandwidth** is selected It means the option Resource of rule-based QoS Rule is bandwidth. In Control Function when Set MINR & MAXR is selected It means the option Control Function of rule-based QoS Rule is set MINR & MAXR. You can assign min rate, max rate and rate unit for this rule. **QoS Direction** (A Must filled setting) When **Outbound** is selected It means the option QoS Direction of rule-based QoS Rule is outbound. Outbound means the Group option is a source group. When **Inbound** is selected It means the option QoS Direction of rule-based QoS Rule is inbound. Inbound means the Group option is a destination group. When **Both** is selected It means the option QoS Direction of rule-based QoS Rule is both. **Sharing Method** (A Must filled setting) When **Individual Control** is selected, It means the option Sharing Method of rule-based QoS Rule is Individual Control. When **Group Control** is selected, It means the option Sharing Method of rule-based QoS Rule is Group Control. **Time Schedule** (A Must filled setting) Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **System)** Enabling the rule Click **Enable** box to activate this rule. Click the **Save** button to save the settings
		When Connection Sessions is selected It means the option Resource of rule-based QoS Rule is connection sessions. In Control Function when Set Session Limitation is selected It means the option Control Function of rule-based QoS Rule is set session limitation. You must fill the session number in the textbox. **QoS Direction** (A Must filled setting) When **Outbound** is selected It means the option QoS Direction of rule-based QoS Rule is outbound. Outbound means the Group option is a source group. When **Inbound** is selected

	It means the option QoS Direction of rule-based QoS Rule is inbound. Inbound means the Group option is a destination group. When **Both** is selected It means the option QoS Direction of rule-based QoS Rule is both. **Time Schedule** (A Must filled setting) Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **System)** Enabling the rule Click **Enable** box to activate this rule. Click the **Save** button to save the settings
	When **Priority Queues** is selected It means the option Resource of rule-based QoS Rule is priority queues. In Control Function when Set Priority is selected It means the option Control Function of rule-based QoS Rule is set priority. You must fill the priority queue number in the textbox. **QoS Direction** (A Must filled setting) When **Outbound** is selected It means the option QoS Direction of rule-based QoS Rule is outbound. Outbound means the Group option is a source group. When **Inbound** is selected It means the option QoS Direction of rule-based QoS Rule is inbound. Inbound means the Group option is a destination group. When **Both** is selected It means the option QoS Direction of rule-based QoS Rule is both. **Time Schedule** (A Must filled setting) Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **System)** Enabling the rule Click **Enable** box to activate this rule. Click the **Save** button to save the settings
	When DiffServ Code Points is selected It means the option Resource of rule-based QoS Rule is DiffServ Code Points. In Control Function when DSCP Marking is selected It means the option Control Function of rule-based QoS Rule is DSCP marking. You must select one from the list. DSCP Marking will mark with Code Point in Packet. **QoS Direction** (A Must filled setting) When **Outbound** is selected It means the option QoS Direction of rule-based QoS Rule is outbound. Outbound means the Group option is a source group. When **Inbound** is selected It means the option QoS Direction of rule-based QoS Rule is inbound. Inbound means the Group option is a destination group. When **Both** is selected It means the option QoS Direction of rule-based QoS Rule is both. **Time Schedule** (A Must filled setting)

Index skipping is used to reserve slots for new function insertion, when required.

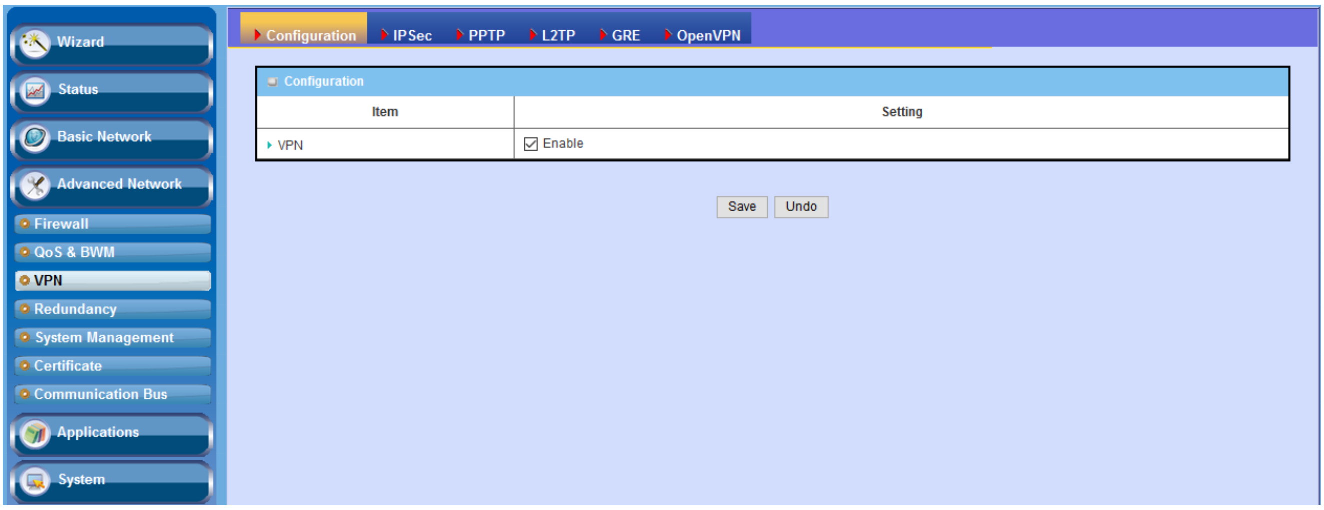
	Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **System)** Enabling the rule Click **Enable** box to activate this rule. Click the **Save** button to save the settings

5.5 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 following tunneling technologies to establish secure tunnels between multiple sites for data transferring, including IPSec, PPTP, L2TP (over IPSec) and GRE. Advanced functions include Full Tunnel, Tunnel Failover, Tunnel Load Balance, NetBIOS over IPSec, NAT Traversal and Dynamic VPN.

5.5.1 Configuration



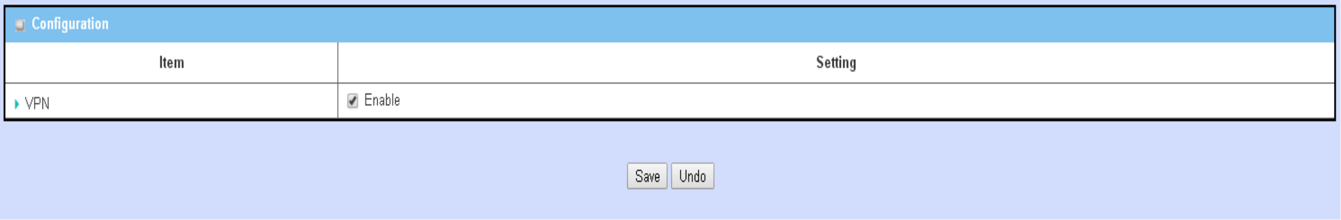
Configuration

Item	Setting
VPN	☑ Enable

VPN Configuration

Enable VPN check box will activate all VPN related functions.

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.



Configuration

Item	Setting
VPN	☑ Enable

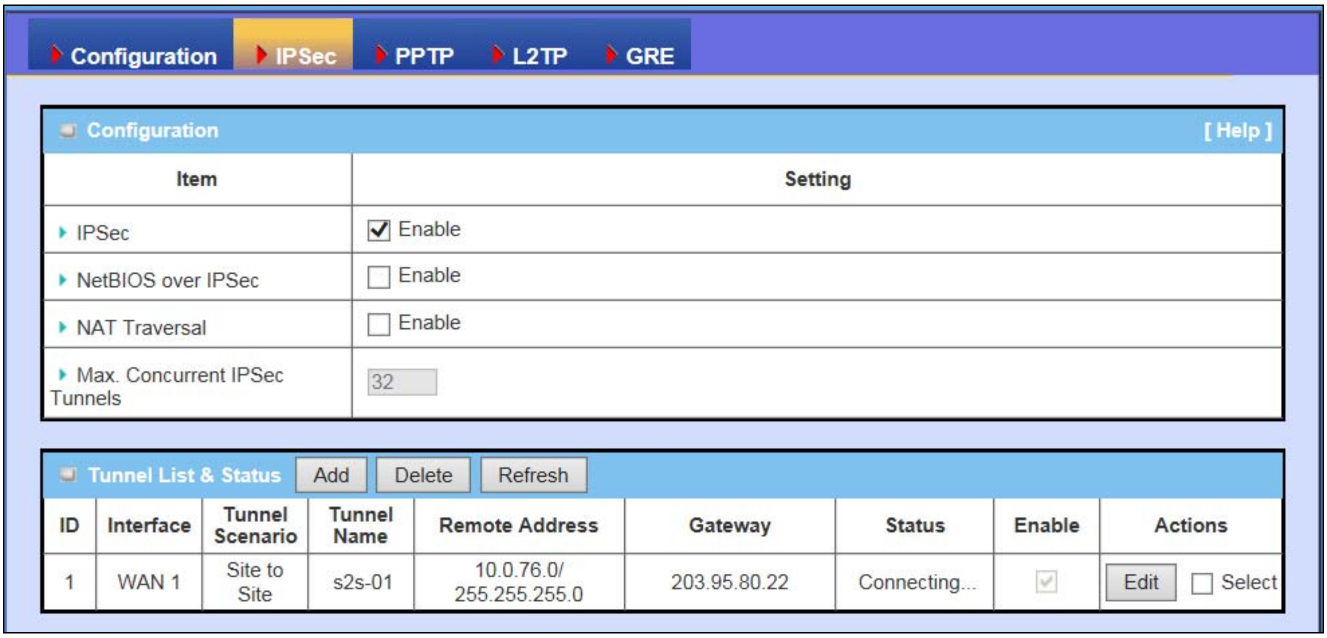
VPN Configuration		
Item	**Value setting**	**Description**
VPN	The box is unchecked by default	Check the **Enable** box to enable all VPN functions
Save	N/A	Click the **Save** button to save the settings

Index skipping is used to reserve slots for new function insertion, when required.

5.5.3 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.



Item	Setting
IPSec	☑ Enable
NetBIOS over IPSec	□ Enable
NAT Traversal	□ Enable
Max. Concurrent IPSec Tunnels	32

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

In "IPSec" page, there is the "Configuration" window to enable the IPSec for VPN function to activate network neighborhood between the Intranets of local and remote peers. It enables the VPN tunnels even the gateway is under a NAT router and specify the maximum concurrent IPSec tunnels. In addition, there is one more "Tunnel List & Status" window lists the created IPSec VPN tunnels and their connection status. To add and create a new tunnel, click on the "Add" button. There are some configuration windows for you to setup. They are "Tunnel Configuration", "Local & Remote Configuration", "Authentication", "IKE Phase", "IKE Proposal Definition", "IPSec Phase", and "IPSec Proposal Definition" windows.

Configuration

The "Configuration" window is to enable the IPSec VPN function. In addition, if you want to activate the network neighborhood communication to work between both Intranets of local and remote peers in the IPSec VPN tunnel, you can check the "NetBIOS over IPSec" box. Moreover, if your security gateway is under a NAT router and you want to create an IPSec VPN tunnel between your security gateway and remote security gateway. Your gateway must act as the initiator for the IPSec tunnel and the NAT router must pass through the IPSec packets from your security gateway to remote one. Check the "NAT Traversal" box to setup the scenario of IPSec tunnel through NAT router. At last, the "Configuration" window shows the maximum number of concurrent IPSec VPN tunnels that are running in system.

Tunnel List & Status

The Tunnel List shows the setup parameters of all IPSec VPN tunnels and their connection status, including the interface name for the tunnel endpoint, the tunnel name, the subnet of remote Intranet, the IP address of remote gateway, its connection status and the tunnel enable checkbox.

There is one "Add" button at the "Tunnel List & Status" caption can let you add and create one new IPSec VPN tunnel.

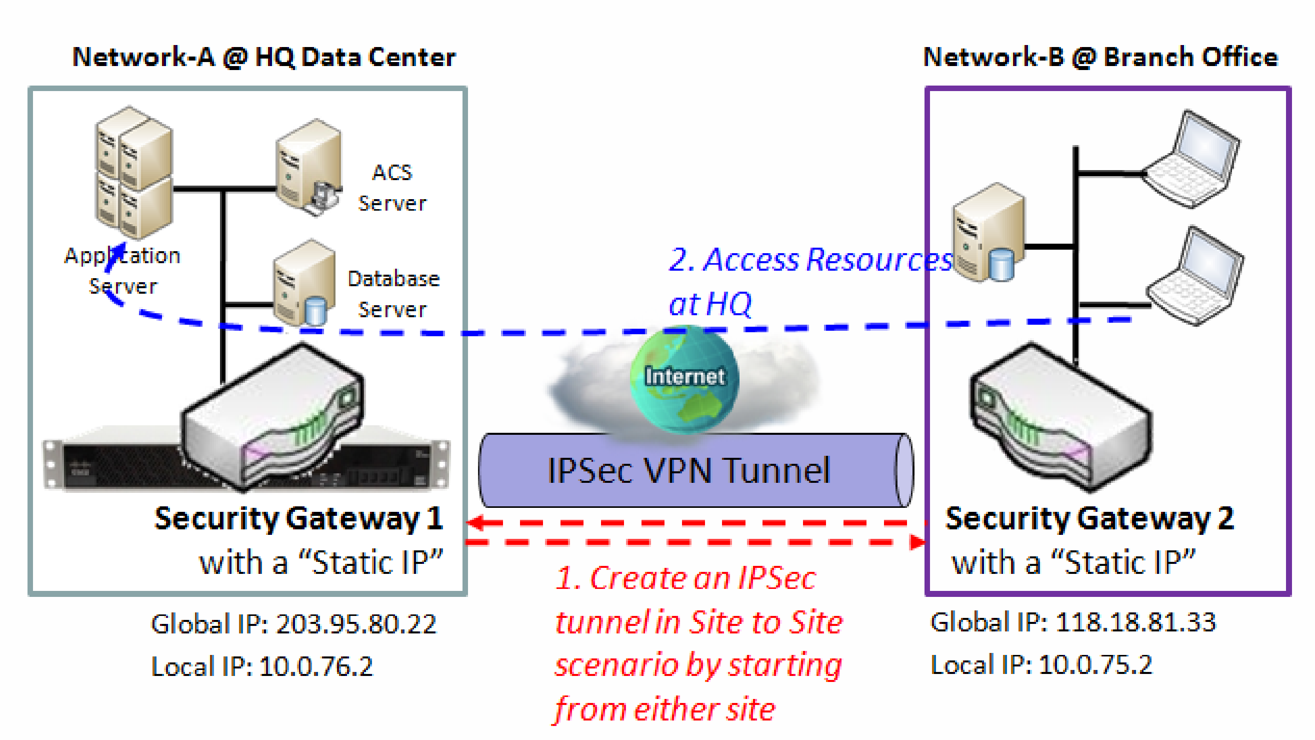
Tunnel Configuration

There are some parameters to setup the tunnel, like "Tunnel Configuration", "Local & Remote Configuration", "Authentication", "IKE Phase", "IKE Proposal Definition", "IPSec Phase" and "IPSec Proposal Definition" configuration windows.

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.

Index skipping is used to reserve slots for new function insertion, when required.

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 are 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.

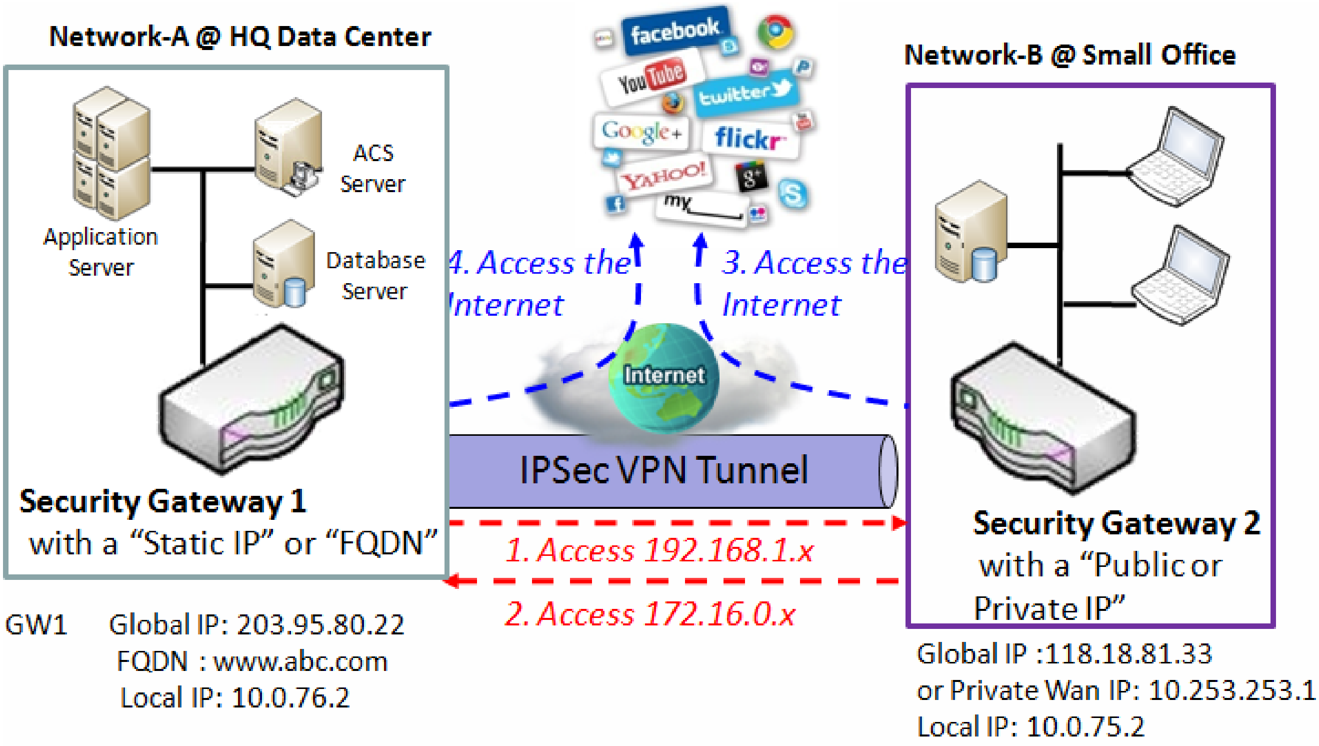
However, Network-B is in the branch office and the subnet of its Intranet is 10.0.75.0/24. The security gateway for Network-B has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN interface.

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 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.

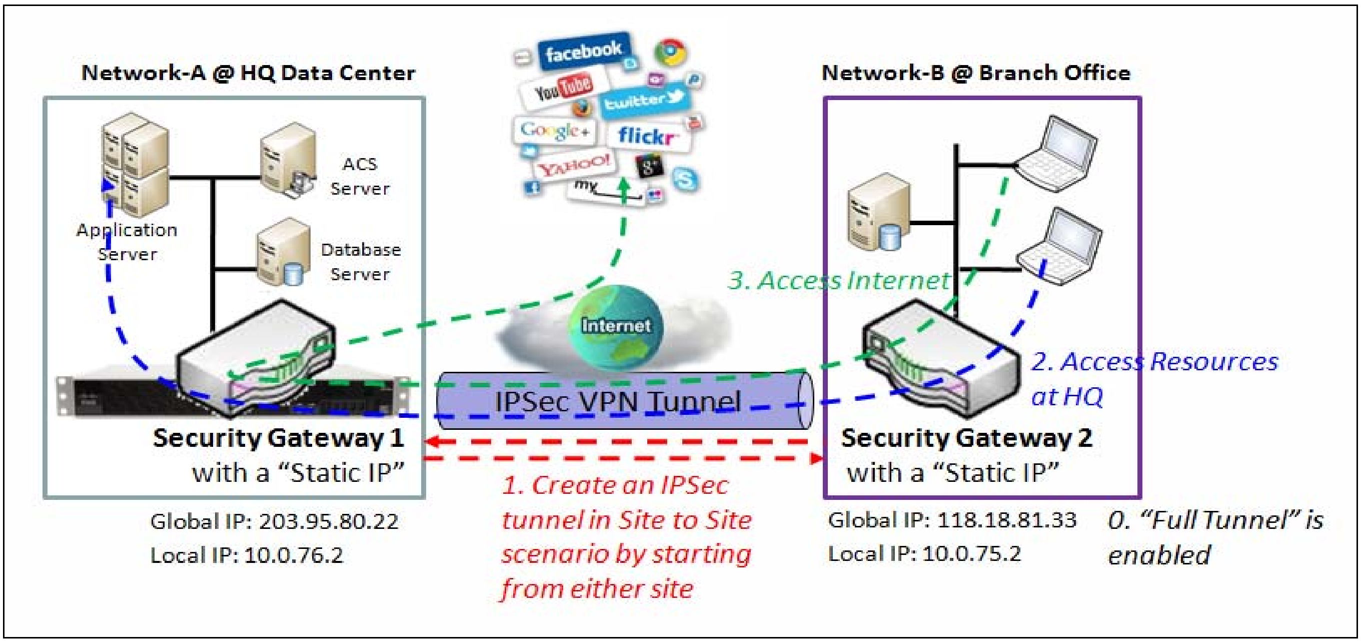
Finally, the client hosts in the Intranet of Network-B at mobile office can access the server or database resources in the Intranet of Network-A at HQ with a secured link. That means, the security gateway in headquarters supports "Dynamic VPN" function and then you, as a mobile user, can access its Intranet 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 are 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***

Index skipping is used to reserve slots for new function insertion, when required.

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.

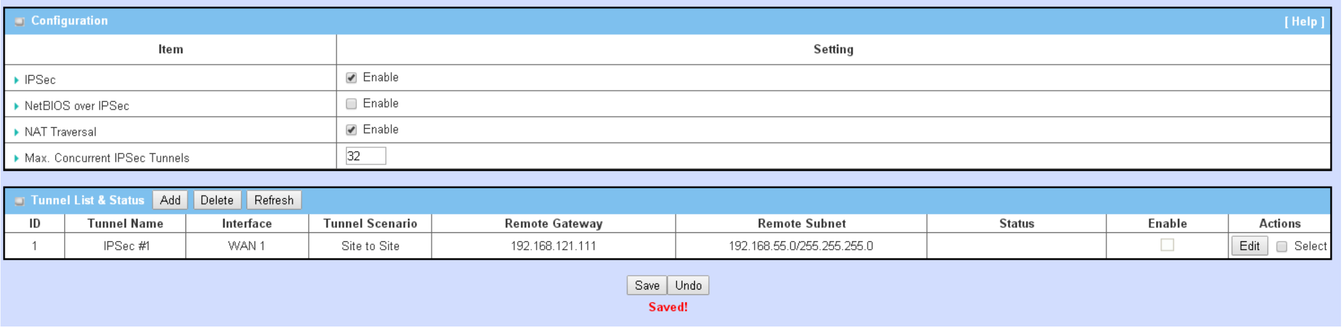
That means, the security gateway in branch office supports "Full Tunnel" feature and the client hosts behind it can access not only the server or database resources in the Intranet of Network-A at HQ, but also the Internet in a secured connection. The HQ gateway controls and secures the IP networking 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 Advanced Network > VPN > Configuration tab.

Enabling IPSec

Go to Advanced Network > VPN > IPSec tab



Configuration [Help]

Item	Setting
IPSec	☑ Enable
NetBIOS over IPSec	□ Enable
NAT Traversal	☑ Enable
Max. Concurrent IPSec Tunnels	32

Tunnel List & Status

ID	Tunnel Name	Interface	Tunnel Scenario	Remote Gateway	Remote Subnet	Status	Enable	Actions
1	IPSec #1	WAN 1	Site to Site	192.168.121.111	192.168.55.0/255.255.255.0		□	Edit □ Select

Saved!

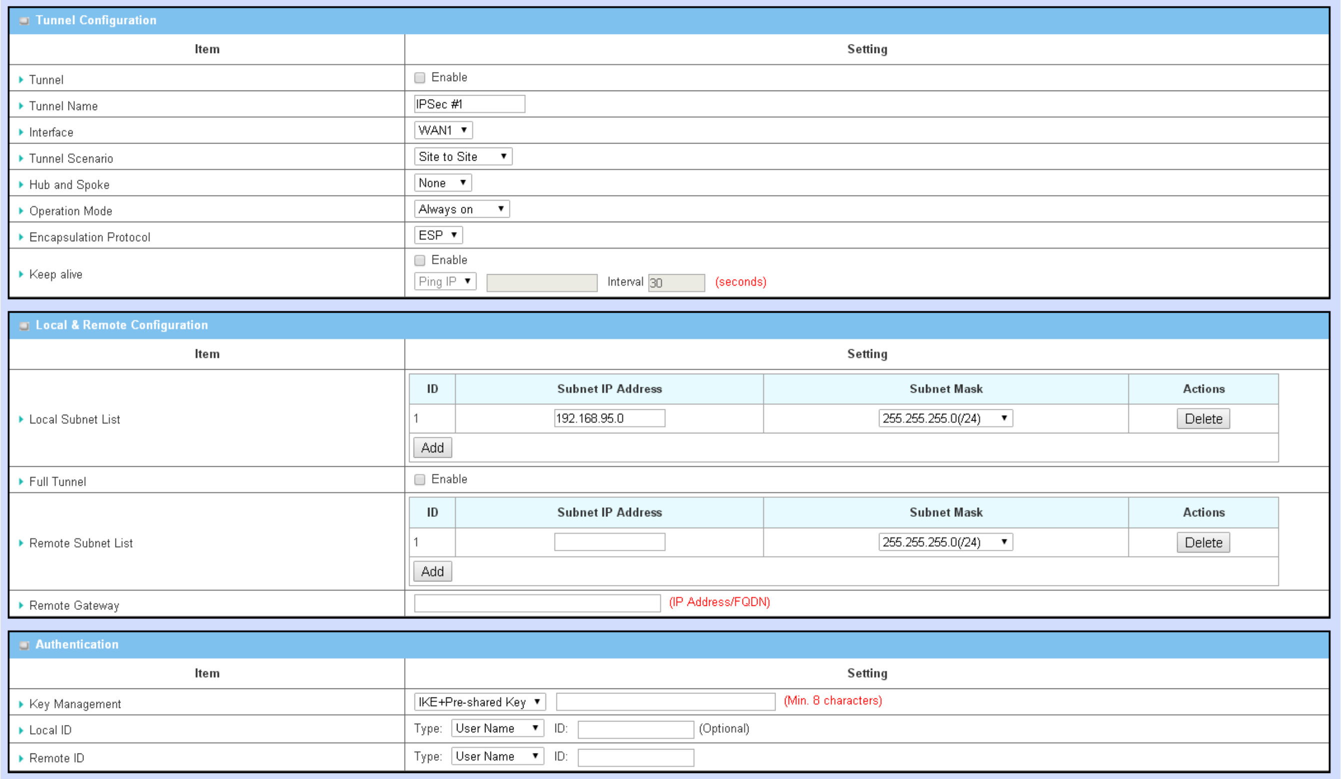
Index skipping is used to reserve slots for new function insertion, when required.

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 Value specified will limit the maximum number of simultaneous IPSec tunnel connection.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Create/Edit IPSec tunnel

The router supports up to a maximum of 32 simultaneous IPSec tunnel connections. Ensure that the IPSec enable box is checked to enable before we can setup IPSec.

When Add/Edit button is applied a series of configuration screen will appear.



Tunnel Configuration

Item	Setting
Tunnel	□ Enable
Tunnel Name	IPSec #1
Interface	WAN1 ▾
Tunnel Scenario	Site to Site ▾
Hub and Spoke	None ▾
Operation Mode	Always on ▾
Encapsulation Protocol	ESP ▾
Keep alive	□ Enable Ping IP ▾ Interval 30 (seconds)

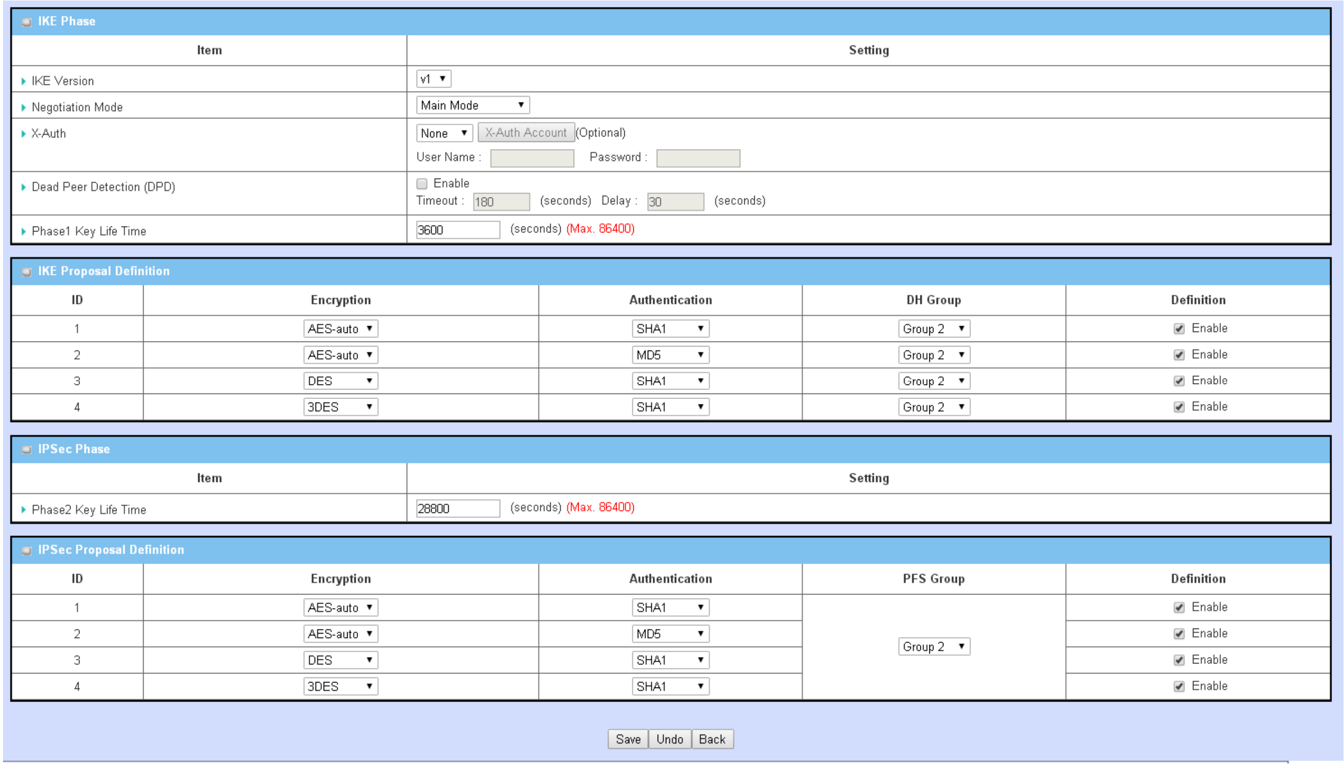
Local & Remote Configuration

Item	Setting
Local Subnet List	ID: 1, Subnet IP Address: 192.168.95.0, 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)

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:

Index skipping is used to reserve slots for new function insertion, when required.



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 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

IPSec Phase

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

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

Index skipping is used to reserve slots for new function insertion, when required.

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, Host-to-Host, or Dynamic VPN. 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 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 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 need to set a key (Min. 8 characters). **IKE+X.509** user need 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 Advanced Network> Certificate in web-based utility. **Manually** user needs to enter l key to authenticate. Manual key configuration will be explained in the Manual Key Management section located in the following next 2 pages.
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.

Index skipping is used to reserve slots for new function insertion, when required.

IKE Phase Configuration 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 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

Index skipping is used to reserve slots for new function insertion, when required.

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.

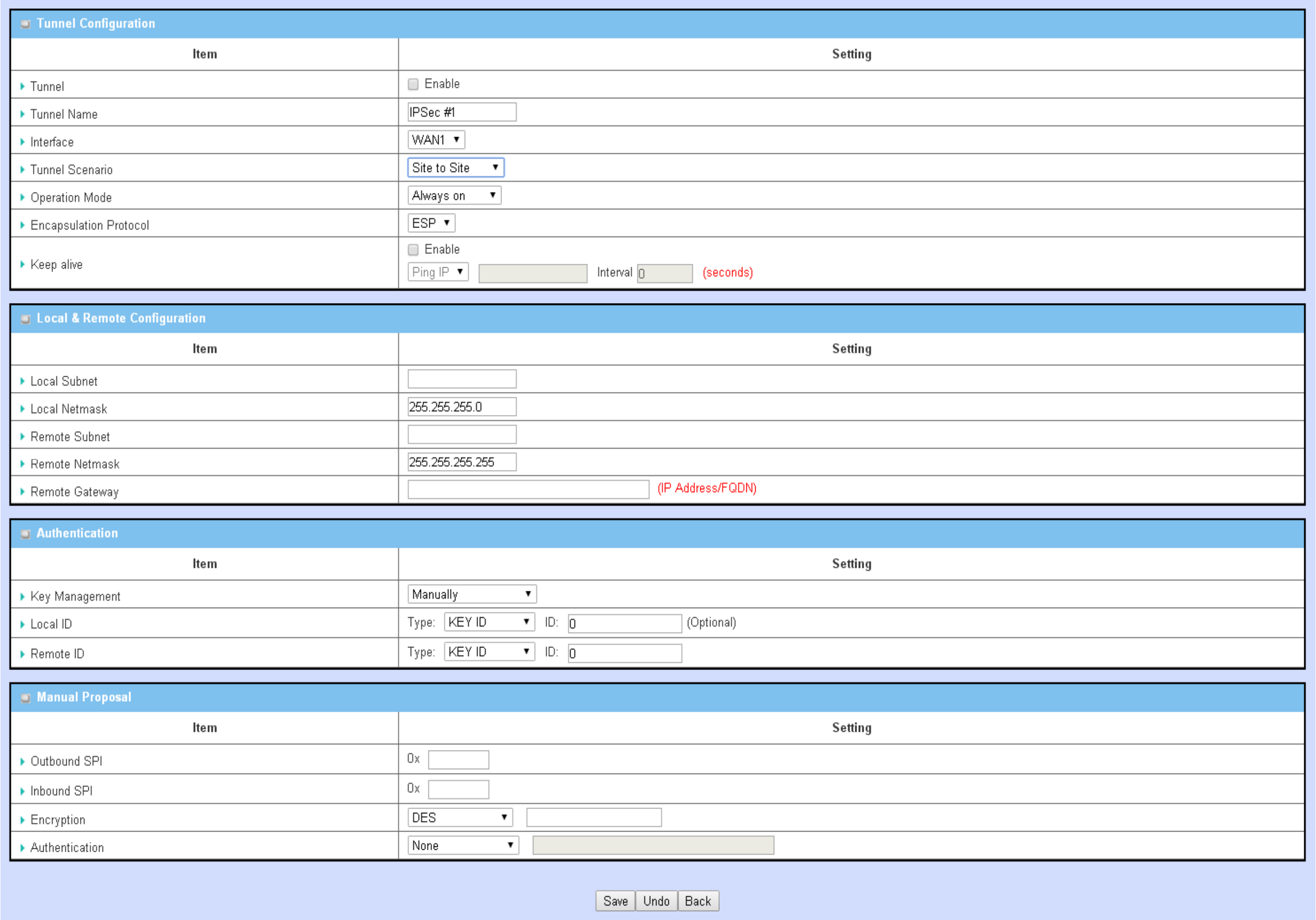
IPSec Proposal Definition Window		
Item	**Value setting**	**Description**
IPSec Proposal Definition	A Must fill setting	Specify the Encryption method None/AES-auto/AES128/AES192/AES256/DES/3DES Specify Authentication method None/MD5/SHA1/SHA2-256/SHA2-512 Specify the PFS Group None/Group1/ Group2/ Group5/ 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.

Index skipping is used to reserve slots for new function insertion, when required.

Manual Key Management

This section describes parameters available for configuring tunnel authentications manually as described in Key Management section under Authentication configuration window in the previous pages.

When Manually option is selected for Key Management described in Authentication Configuration Window, a series of configuration windows for Manual IPSec Tunnel configuration will appear. The configuration windows are the Tunnel configuration, the Local & Remote Configuration, the Authentication, the Manual Proposal. The windows may look similar to the ones below.



Tunnel Configuration

Item	Setting
Tunnel	□ Enable
Tunnel Name	IPSec #1
Interface	WAN1 ▾
Tunnel Scenario	Site to Site ▾
Operation Mode	Always on ▾
Encapsulation Protocol	ESP ▾
Keep alive	□ Enable Ping IP ▾ Interval 0 (seconds)

Local & Remote Configuration

Item	Setting
Local Subnet	
Local Netmask	255.255.255.0
Remote Subnet	
Remote Netmask	255.255.255.255
Remote Gateway	(IP Address/FQDN)

Authentication

Item	Setting
Key Management	Manually ▾
Local ID	Type: KEY ID ▾ ID: 0 (Optional)
Remote ID	Type: KEY ID ▾ ID: 0

Manual Proposal

Item	Setting
Outbound SPI	0x
Inbound SPI	0x
Encryption	DES ▾
Authentication	None ▾

Index skipping is used to reserve slots for new function insertion, when required.

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 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.
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. Define whether the IPSec tunnel is a failover tunnel function or an always on tunneling Note: If this IPSec is a failover tunneling, you will need to select the primary IPSec tunnel from which to failover to. 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	Click 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.

Index skipping is used to reserve slots for new function insertion, when required.

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

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).

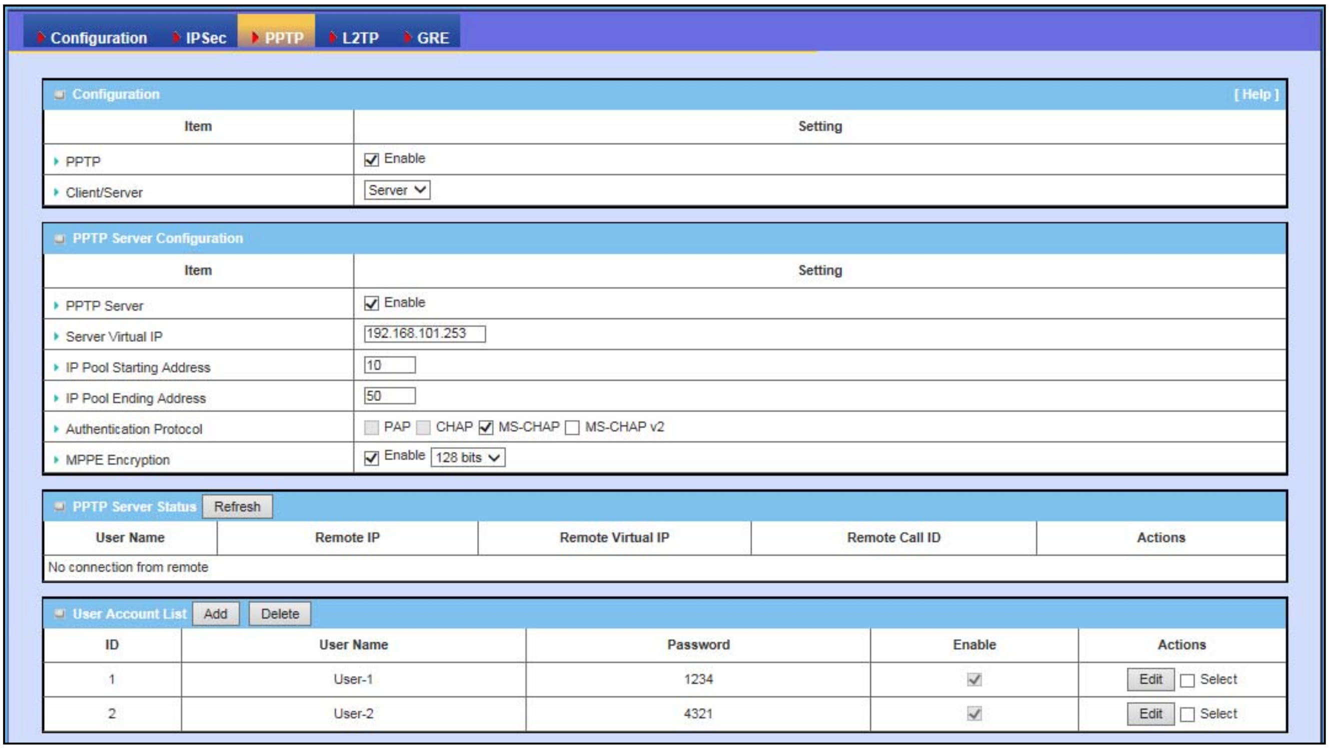
Manual Proposal Window		
Item	**Value setting**	**Description**
Outbound SPI	Hexadecimal format	Specify the Outbound SPI for this IPSec tunnel.
Inbound SPI	Hexadecimal format	Specify the Inbound SPI for this IPSec tunnel.
Encryption	1. A Must fill setting 2. Hexadecimal format	Specify the Encryption 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.

5.5.5 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.

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.



Configuration [Help]

Item	Setting
PPTP	☑ Enable
Client/Server	Server

PPTP Server Configuration

Item	Setting
PPTP Server	☑ Enable
Server Virtual IP	192.168.101.253
IP Pool Starting Address	10
IP Pool Ending Address	50
Authentication Protocol	□ PAP □ CHAP ☑ MS-CHAP □ MS-CHAP v2
MPPE Encryption	☑ Enable 128 bits

PPTP Server Status Refresh

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

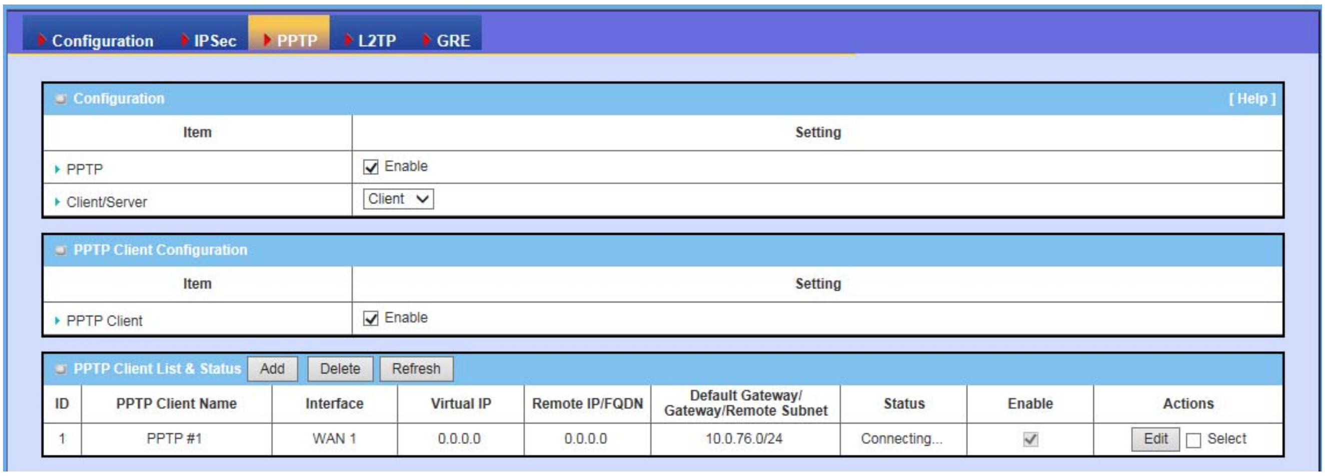
User Account List Add Delete

ID	User Name	Password	Enable	Actions
1	User-1	1234	☑	Edit □ Select
2	User-2	4321	☑	Edit □ Select

In "PPTP" page, there is the "Configuration" window to enable the PPTP VPN function. Moreover, the security gateway can play either "PPTP Server" role or "PPTP Client" role or they both at the same

Index skipping is used to reserve slots for new function insertion, when required.

time. Define and choose either one role for your router in the "Configuration" window and configure all required parameters beneath the "Configuration" window. Then configure parameters on another gateway to takes another role. Above diagram is the server role configuration and following diagram shows the client role configuration.



Configuration [Help]

Item	Setting
PPTP	☑ Enable
Client/Server	Client

PPTP Client Configuration

Item	Setting
PPTP Client	☑ Enable

PPTP Client List & Status

ID	PPTP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/ Gateway/Remote Subnet	Status	Enable	Actions
1	PPTP #1	WAN 1	0.0.0.0	0.0.0.0	10.0.76.0/24	Connecting...	☑	Edit □ Select

When you want to configure "PPTP Server" role for the security gateway, there are 4 more configuration windows: "PPTP Server Configuration", "PPTP Server Status", "User Account List" and "User Account Configuration". However, when you want to configure "PPTP Client" role for the security gateway, there are 3 more configuration windows: "PPTP Client Configuration", "PPTP Client List & Status" and "Configuration for A PPTP Client".

Configuration

The "Configuration" window is to enable the PPTP VPN function by checking the Enable box. In the "Client/Server" field of the "Configuration" window choose either "Server" or "Client". Choose Server to define the gateway as the PPTP VPN server for remote clients to initiate the connection to establish VPN tunnels. Or choose Client to create multiple PPTP VPN clients to establish VPN tunnels to remote gateways. Moreover, the security gateway operates and supports the PPTP VPN client and server simultaneously.

PPTP VPN Server Scenario

When you want the security gateway to play a PPTP server role, check the "Enable" box and choose "Server" option in the "PPTP Configuration" window. And make its related configuration in following sessions. Also refer to the above server role diagram.

PPTP Server Configuration

"PPTP Server Configuration" window can let you enable the PPTP server function, specify the virtual IP address of PPTP server, define the pool of virtual IP addresses that will assign to remote PPTP clients dialing in the security gateway, and the authentication protocol. Once you select "MS-CHAP" or

"MS-CHAP v2" for the authentication protocol, you also can specify if the PPTP server needs the MPPE encryption and its key length for the authentication process.

PPTP Server Status

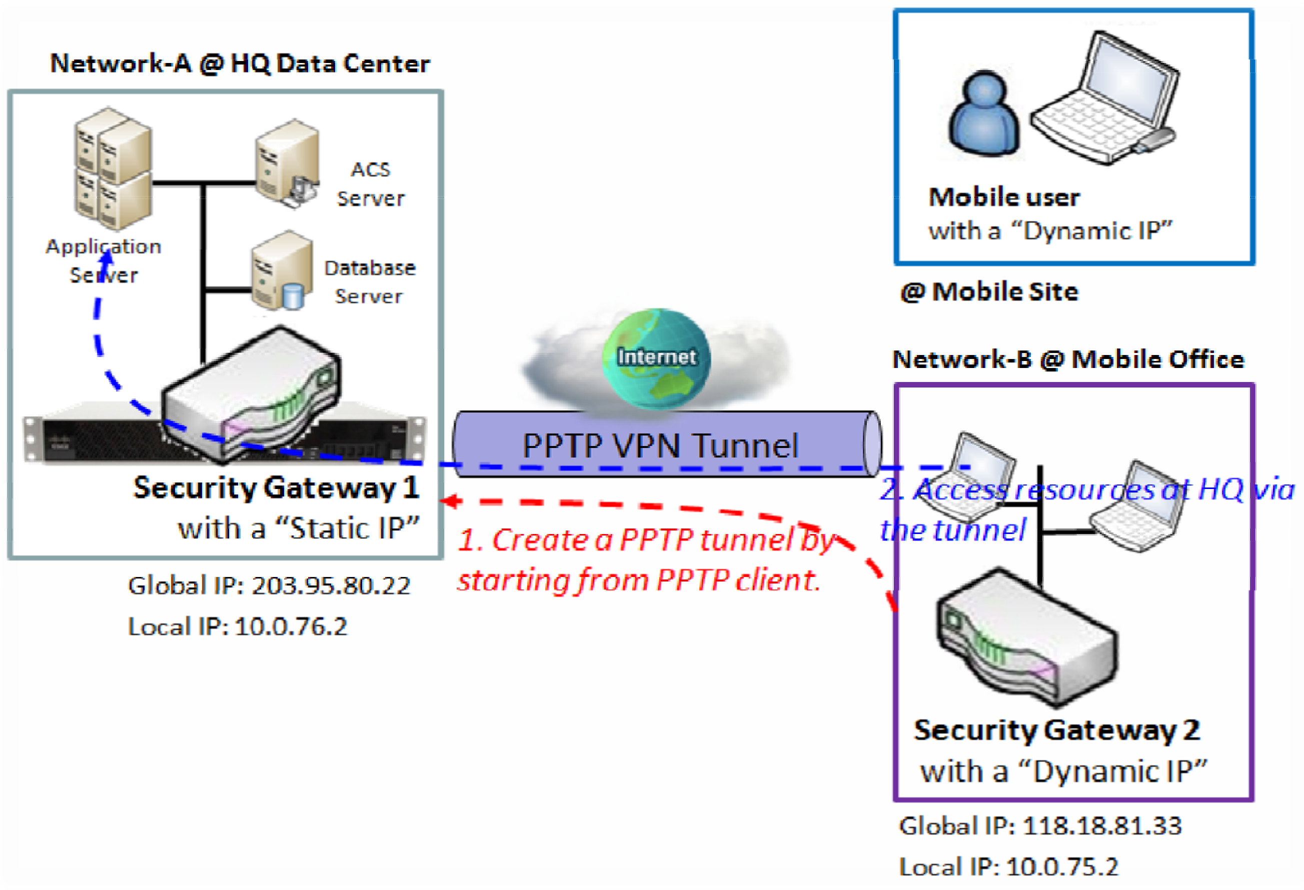
"PPTP Server Status" window shows the dialing in status to the PPTP VPN server, including the used user name, remote IP address, the obtained virtual IP address and call ID of all PPTP clients.

User Account List

"User Account List" lists your defined user accounts that can be accepted by the PPTP server.

User Account Configuration

"User Account Configuration" window can let you specify the required parameters for a PPTP client account, such as user name, password and account activation. Add one new user account by using the "Add" button and edit an existed one by using the "Edit" button. Once it is created, the user account will be appeared in the “User Account List” window.



Scenario Application Timing

Above diagram illustrates the security gateway at headquarters 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

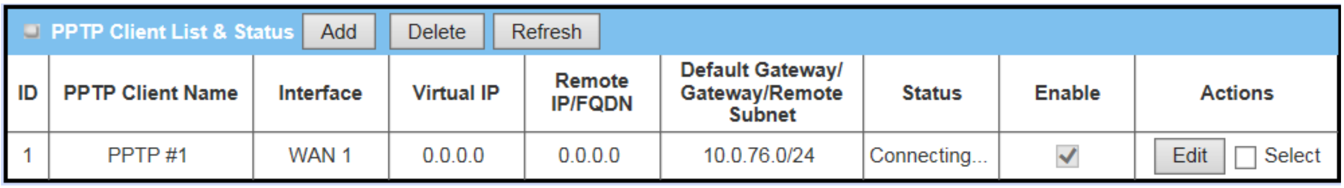
When you want the security gateway to play a PPTP client role, check the "Enable" box and choose "Client" option in the "PPTP Configuration" window. And make its related configuration in following sub-sections.

PPTP Client Configuration

"PPTP Client Configuration" window can let you enable the PPTP client function by checking the "Enable" box.

PPTP Client List & Status

"PPTP Client List & Status" window shows your defined PPTP clients and their tunnel connection status. Only some important information for all tunnels are shown in the list as following diagram.

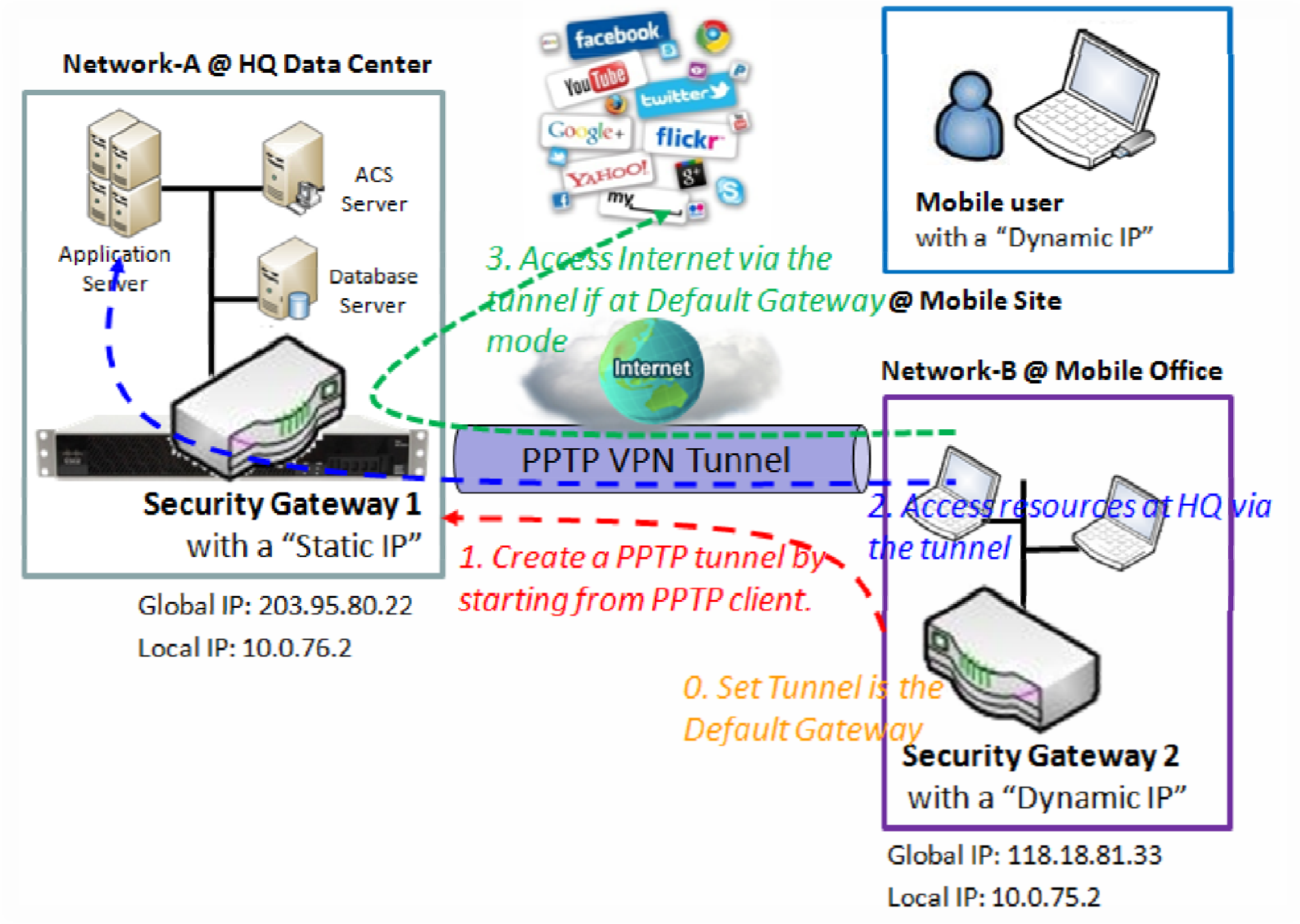


ID	PPTP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/ Gateway/Remote Subnet	Status	Enable	Actions
1	PPTP #1	WAN 1	0.0.0.0	0.0.0.0	10.0.76.0/24	Connecting...	☑	Edit ☐ Select

Configuration for A PPTP Client

"Configuration for A PPTP Client" window let you specify the required parameters for a PPTP VPN client, such as "PPTP Client Name", "Interface", "Operation Mode", "Remote IP/FQDN", "User Name", "Password", "Default Gateway/Remote Subnet", "Authentication Protocol", "MPPE Encryption", "NAT before Tunneling", "LCP Echo Type" and tunnel activation.

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.



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

Index skipping is used to reserve slots for new function insertion, when required.

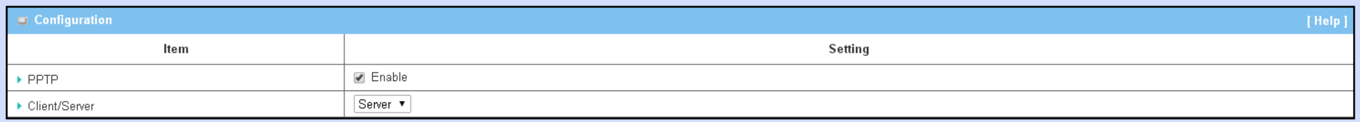
server or database resources in the Intranet of Network-A at HQ in a secured link. However, if the "Default Gateway/Remote Subnet" parameter in the Security Gateway 2 is configured to "Default Gateway", the Internet accessing of PPTP Client peer also go through the established PPTP VPN tunnel, and the Security Gateway 1 can control the accessing as same as the HQ resource accessing.

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 Advanced Network > VPN > Configuration tab.

Enabling PPTP

Go to Advanced Network > VPN > PPTP tab



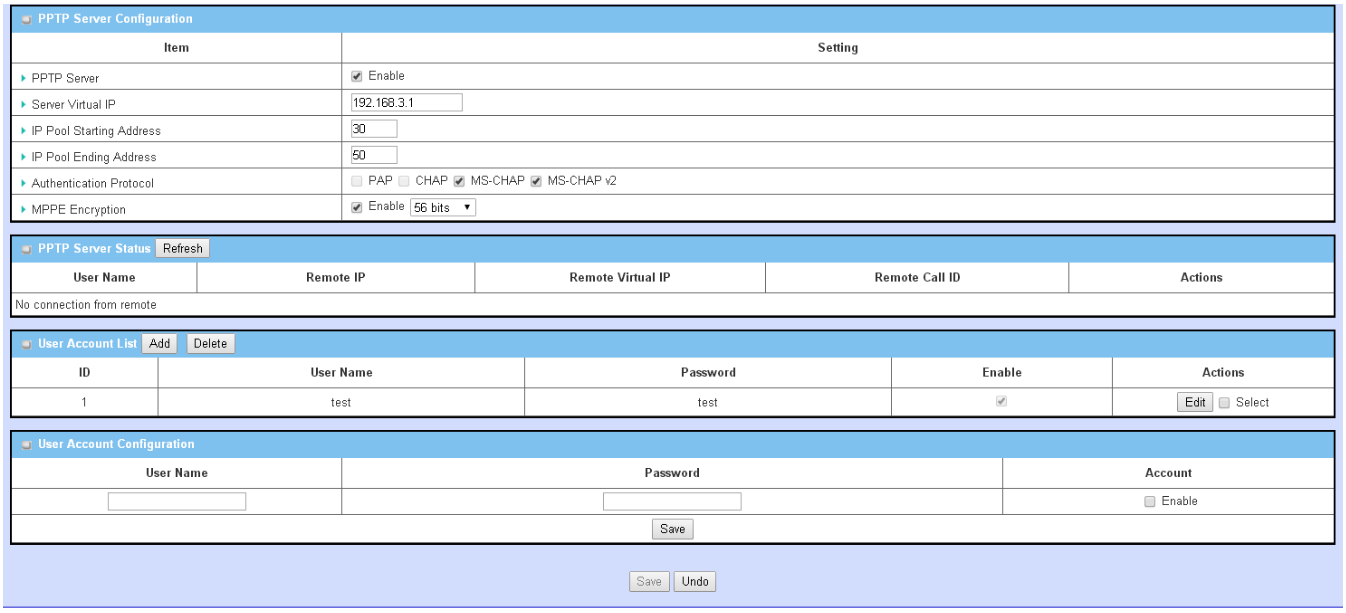
Configuration [Help]

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

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	192.168.3.1
IP Pool Starting Address	30
IP Pool Ending Address	50
Authentication Protocol	☐ PAP ☐ CHAP ☑ MS-CHAP ☑ MS-CHAP v2
MPPE Encryption	☑ Enable 56 bits ▾

PPTP Server Status

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

User Account List

ID	User Name	Password	Enable	Actions
1	test	test	☑	Edit ☐ Select

User Account Configuration

User Name	Password	Account
		☐ Enable

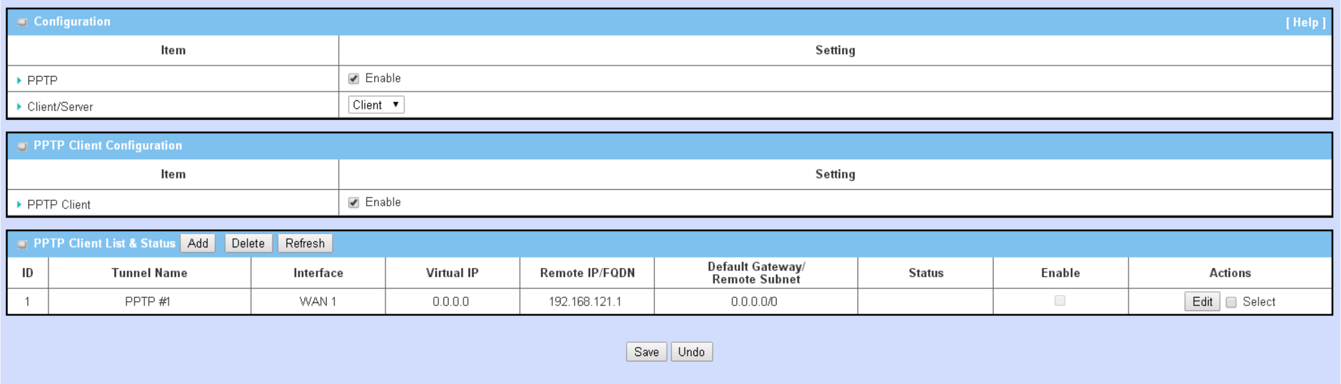
PPTP Server Configuration Window Item	Value setting	Description
PPTP Server	Unchecked by default	Check the **Enable** box to enable PPTP server role of the gateway.
Server Virtual IP	1. A Must fill setting 2. Default is 192.168.10.1	Specify the PPTP server Virtual IP address. The virtual IP address will 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 Window		
Item	**Value setting**	**Description**
PPTP Server Status	N/A	It displays the User Name, Remote IP, Remote Virtual IP, Remote Call ID of the connected PPTP clients.

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.

PPTP Client

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



Configuration [Help]

Item	Setting
PPTP	☑ Enable
Client/Server	Client ▾

PPTP Client Configuration

Item	Setting
PPTP Client	☑ Enable

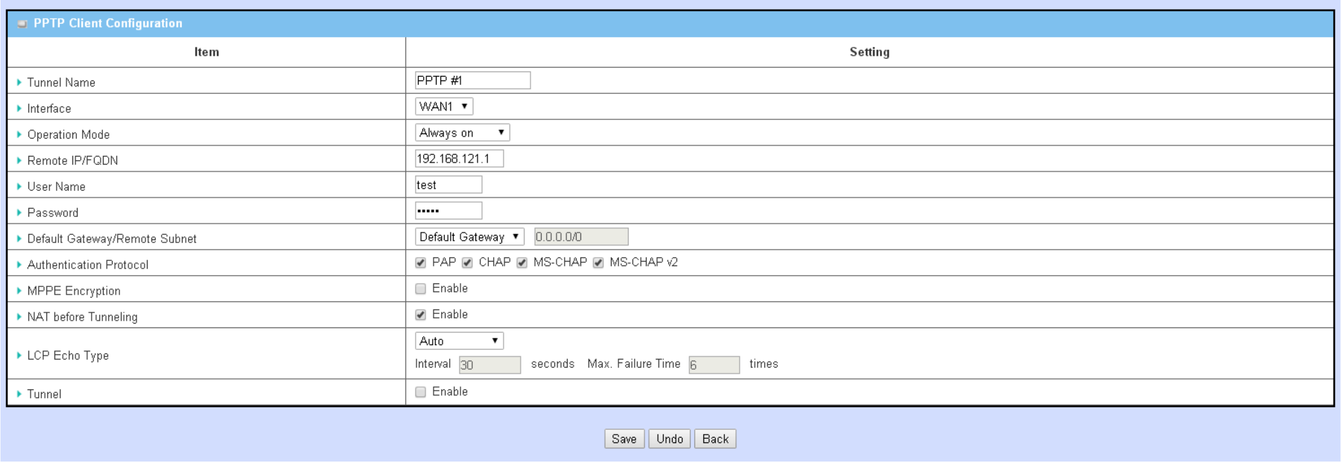
PPTP Client List & Status Add Delete Refresh

ID	Tunnel Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/ Remote Subnet	Status	Enable	Actions
1	PPTP #1	WAN 1	0.0.0.0	192.168.121.1	0.0.0.0/0		□	Edit □ Select

PPTP Client Setting Window		
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

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	192.168.121.1
User Name	test
Password	•••••
Default Gateway/Remote Subnet	Default Gateway ▾ 0.0.0.0/0
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 > 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	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

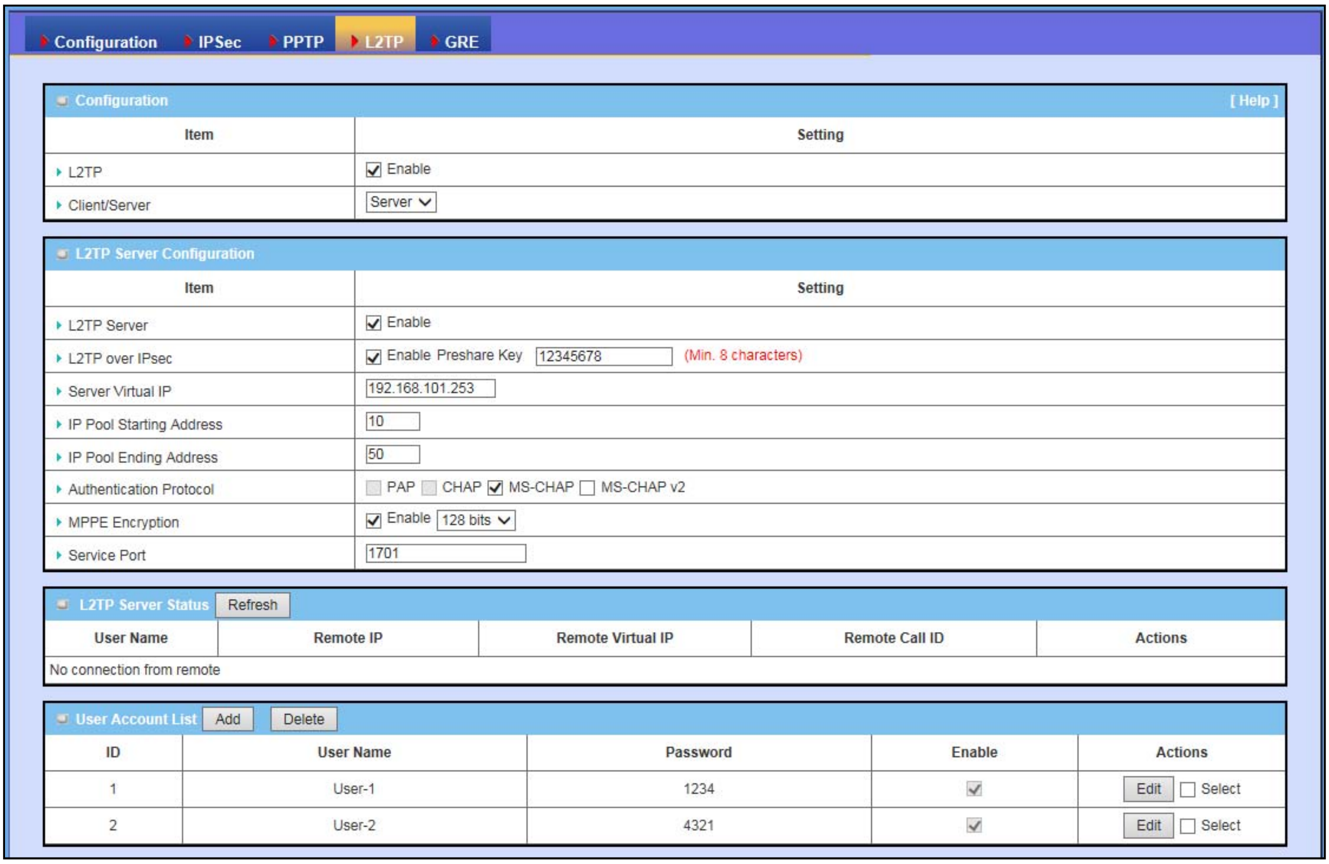
Subnet		the PPTP server then select Default Gateway, otherwise, specified a subnet and its netmask –the remote subnet, if the default gateway is not used to connect to the PPTP server. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24).
Authentication Protocol	1. A Must fill setting 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.

5.5.7 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.



Configuration

Item	Setting
L2TP	☑ Enable
Client/Server	Server

L2TP Server Configuration

Item	Setting
L2TP Server	☑ Enable
L2TP over IPsec	☑ Enable Preshare Key 12345678 (Min. 8 characters)
Server Virtual IP	192.168.101.253
IP Pool Starting Address	10
IP Pool Ending Address	50
Authentication Protocol	□ PAP □ CHAP ☑ MS-CHAP □ MS-CHAP v2
MPPE Encryption	☑ Enable 128 bits
Service Port	1701

L2TP Server Status

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

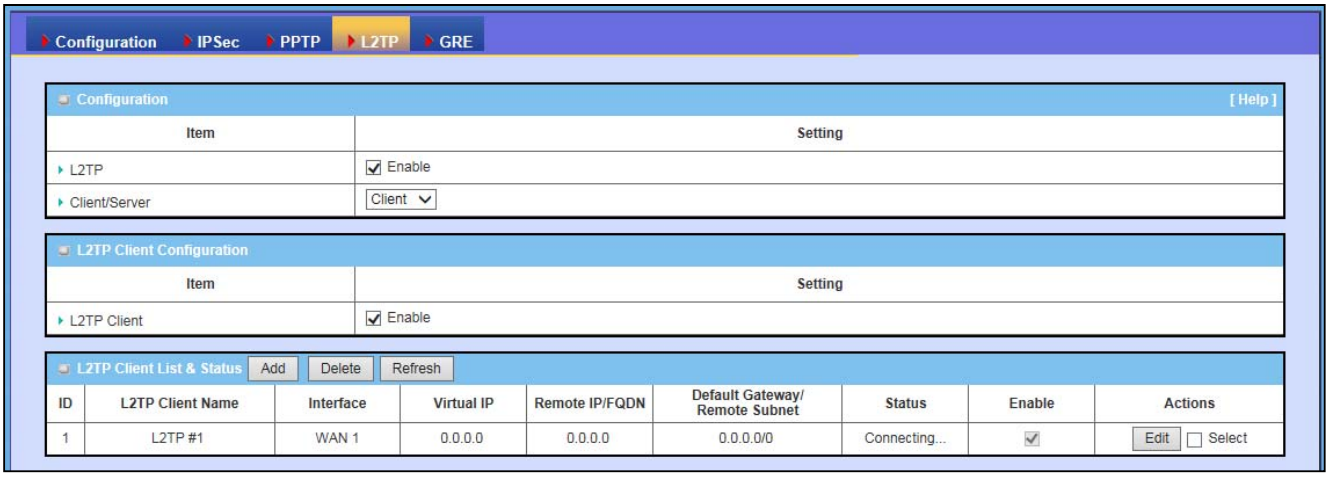
User Account List

ID	User Name	Password	Enable	Actions
1	User-1	1234	☑	Edit □ Select
2	User-2	4321	☑	Edit □ Select

In "L2TP" page, there is the "Configuration" window to enable the L2TP VPN function. The security gateway can either take a "L2TP Server" role or "L2TP Client" role or they both. Define and choose either one role for your router in the "Configuration" window and configure all required parameters

Index skipping is used to reserve slots for new function insertion, when required.

beneath the "Configuration" window. Then configure parameters on another gateway to take another role. Above diagram is the server role configuration and following diagram shows the client role configuration.



Configuration [Help]

Item	Setting
L2TP	☑ Enable
Client/Server	Client

L2TP Client Configuration

Item	Setting
L2TP Client	☑ Enable

L2TP Client List & Status

ID	L2TP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/ Remote Subnet	Status	Enable	Actions
1	L2TP #1	WAN 1	0.0.0.0	0.0.0.0	0.0.0.0/0	Connecting...	☑	Edit □ Select

When you want to configure "L2TP Server" role for the security gateway, there are 4 more configuration windows: "L2TP Server Configuration", "L2TP Server Status", "User Account List" and "User Account Configuration". However, when you want to configure "L2TP Client" role for the security gateway, there are 3 more configuration windows: "L2TP Client Configuration", "L2TP Client List & Status" and "Configuration for A L2TP Client".

Configuration

The "Configuration" window is to enable the L2TP VPN function by checking the Enable box. In the "Client/Server" field of the "Configuration" window choose either "Server" or "Client". Choose Server to define the gateway as the L2TP VPN server for remote clients to initiate the connection to establish VPN tunnels. Or choose Client to create multiple L2TP VPN clients to establish VPN tunnels to remote gateways. Moreover, the security gateway serves as the L2TP VPN client and server simultaneously.

L2TP VPN Server Scenario

When you want the security gateway to play a L2TP server role, check the "Enable" box and choose "Server" option in the "L2TP Configuration" window. And make its related configuration in following sessions. Also refer to the above server role diagram.

L2TP Server Configuration

In the "L2TP Server Configuration" window you will enable L2TP server function and decide if you want L2TP Server to support L2TP over IPSec connection and assign the IPSec authentication pre-shared key; then specify the virtual IP address of L2TP server, define the pool of virtual IP addresses that will assign to remote L2TP clients dialing in the security gateway, and the authentication protocol. Once you select "MS-CHAP" or "MS-CHAP v2" for the authentication protocol, you also can specify if

Index skipping is used to reserve slots for new function insertion, when required.

the L2TP server needs the MPPE encryption and its key length for the authentication process.

L2TP Server Status

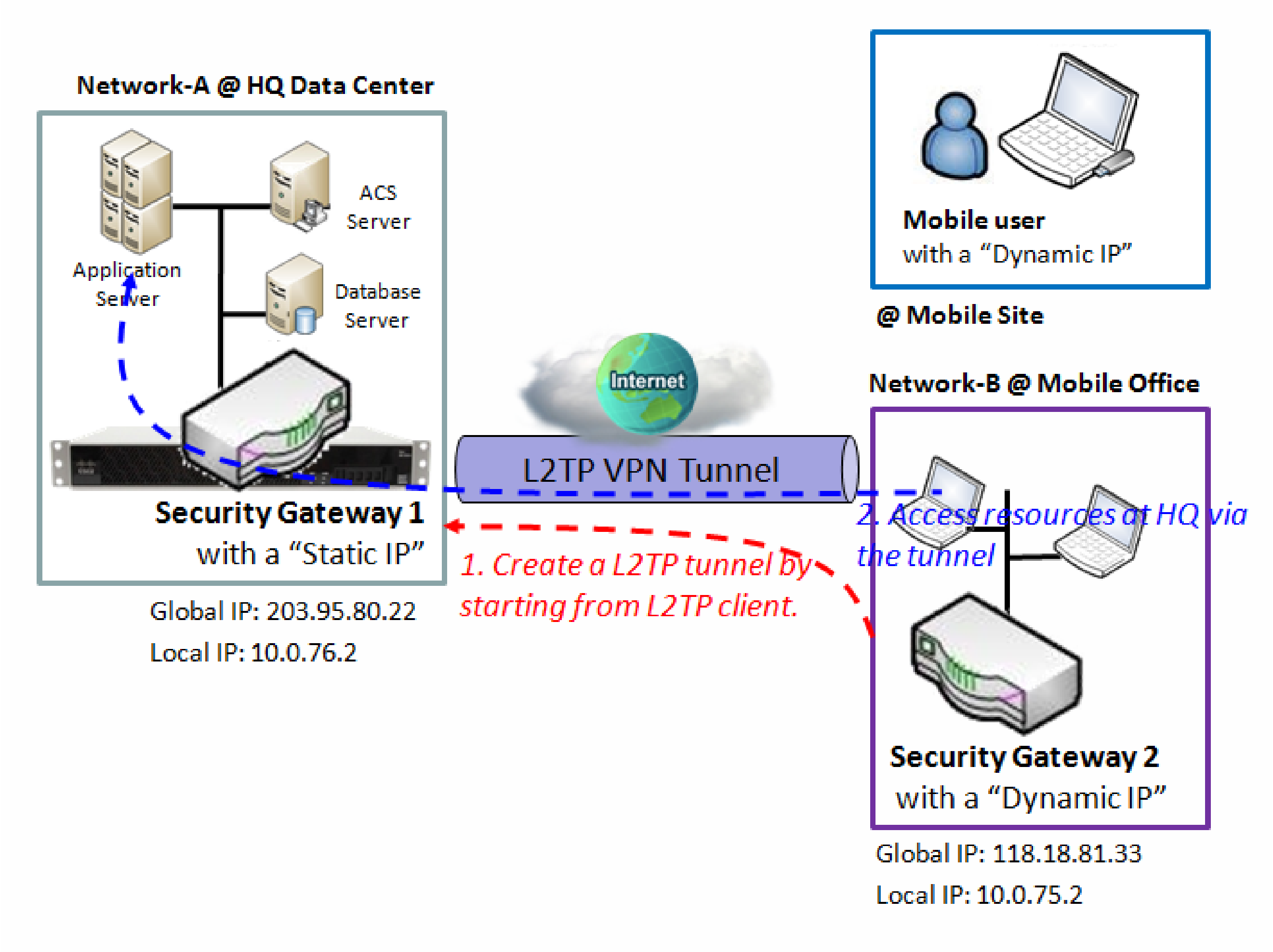
"L2TP Server Status" window shows the dialing in status to the L2TP VPN server, including the used user name, remote IP address, the obtained virtual IP address and call ID of all L2TP clients.

User Account List

"User Account List" lists your defined user accounts that can be accepted by the L2TP server.

User Account Configuration

"User Account Configuration" window can let you specify the required parameters for a L2TP client account, such as user name, password and account activation. Add one new user account by using the "Add" button and edit an existed one by using the "Edit" button.



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***

Index skipping is used to reserve slots for new function insertion, when required.

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

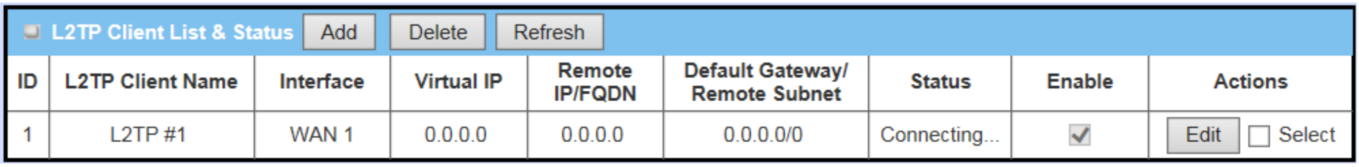
When you want the security gateway to play a L2TP client role, check the "Enable" box and choose "Client" option in the "L2TP Configuration" window. And make its related configuration in following sections.

L2TP Client Configuration

"L2TP Client Configuration" window can let you enable the L2TP client function by checking the "Enable" box.

L2TP Client List & Status

"L2TP Client List & Status" window shows your defined L2TP clients and their tunnel status. Only some important information for all tunnels are shown in the list as following diagram.

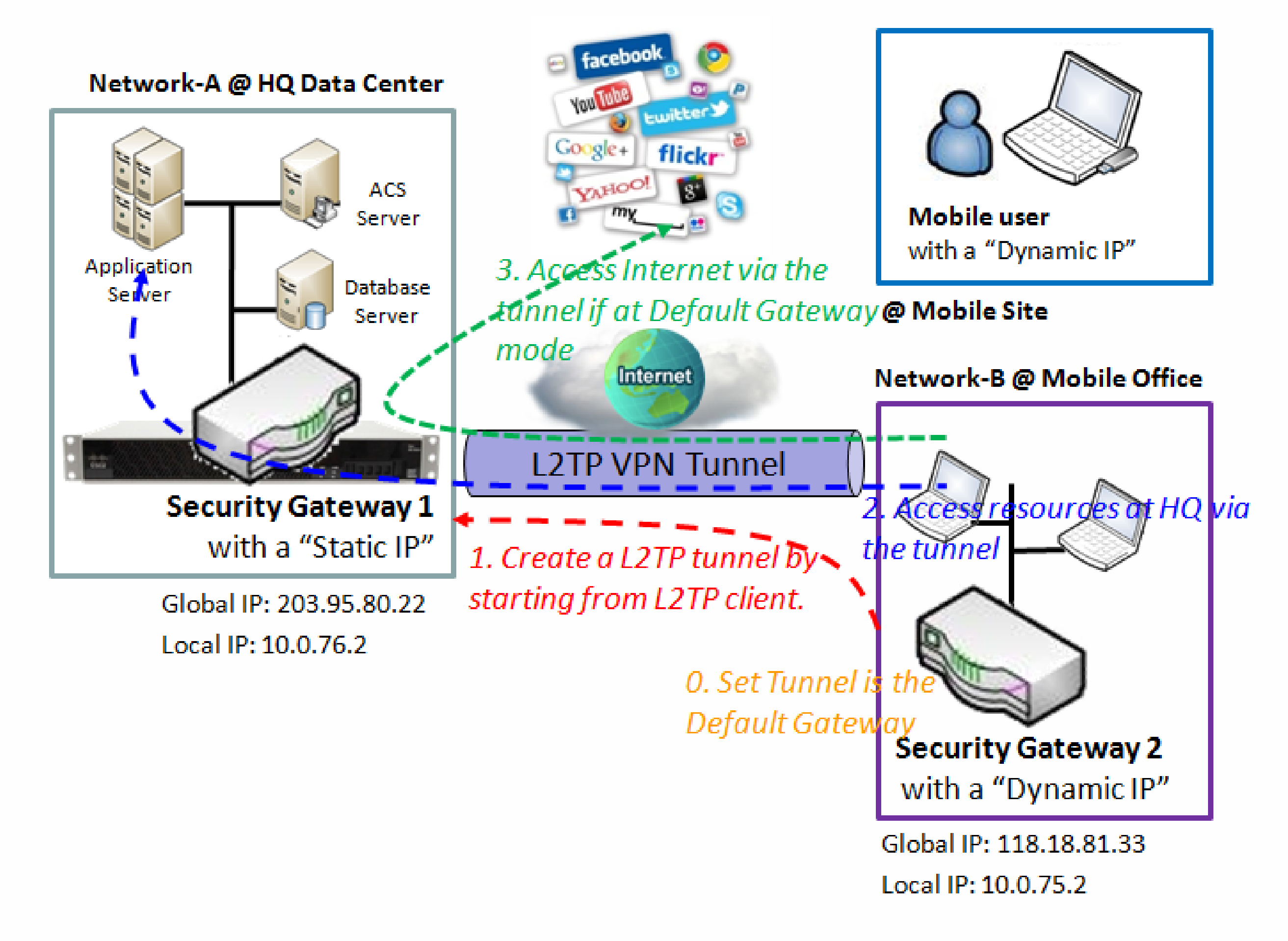


ID	L2TP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/ Remote Subnet	Status	Enable	Actions
1	L2TP #1	WAN 1	0.0.0.0	0.0.0.0	0.0.0.0/0	Connecting...	☑	Edit ☐ Select

Configuration for A L2TP Client

"Configuration for A L2TP Client" window let you specify the required parameters for a L2TP VPN client, such as "L2TP Client Name", "Interface", "Operation Mode", "L2TP over IPSec", "Remote LNS IP/FQDN", "Remote LNS Port", "User Name", "Password", "Tunneling Password", "Default Gateway/Remote Subnet", "Authentication Protocol", "MPPE Encryption", "NAT before Tunneling", "LCP Echo Type", "Service Port", and tunnel activation.

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.



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***

Index skipping is used to reserve slots for new function insertion, when required.

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.

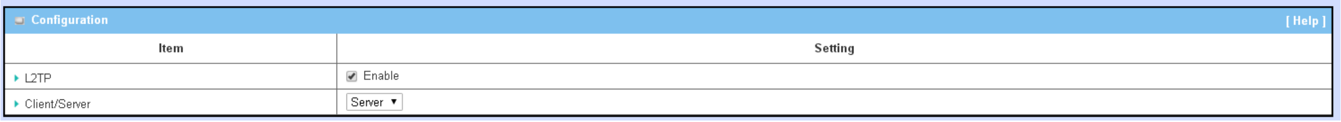
Finally, the client hosts in the Intranet of Network-B at mobile office can access the server or database resources in the Intranet of Network-A at HQ in a secured link.

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.

The L2TP allows user to configure L2TP tunnel

Ensure Configuration are enabled and saved

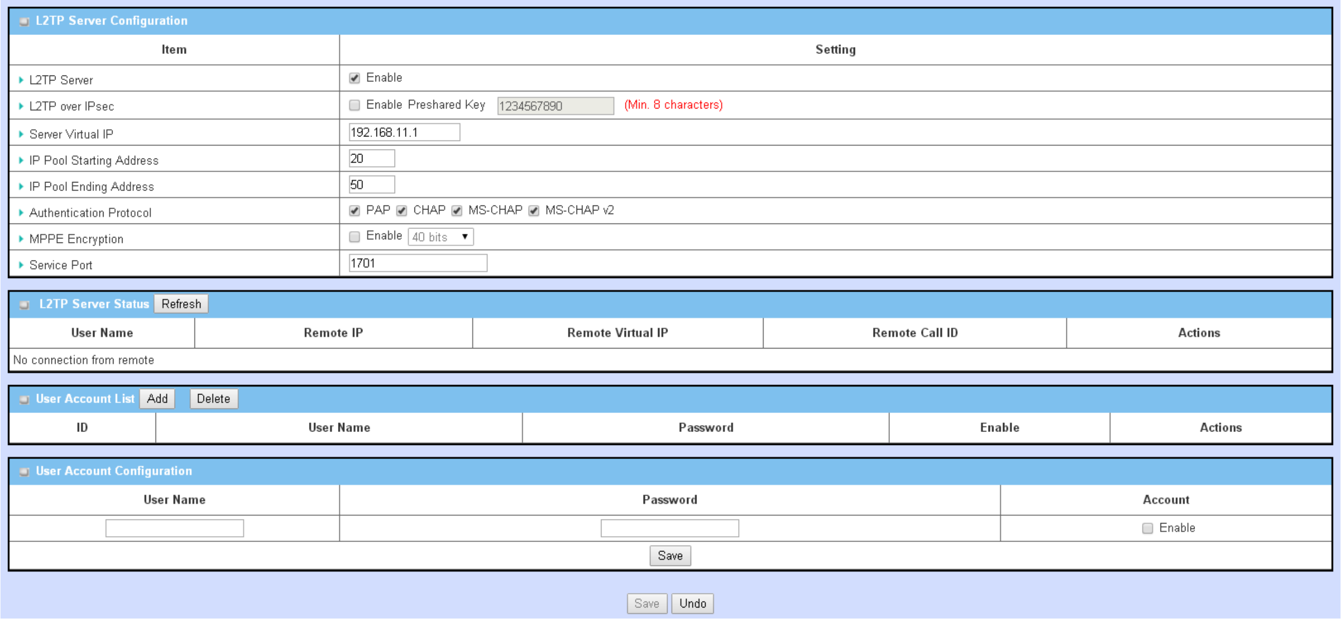
Go to Advanced Network > VPN > L2TP



Configuration [Help]

Item	Setting
L2TP	☑ Enable
Client/Server	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 1234567890 (Min. 8 characters)
Server Virtual IP	192.168.11.1
IP Pool Starting Address	20
IP Pool Ending Address	50
Authentication Protocol	☑ PAP ☑ CHAP ☑ MS-CHAP ☑ MS-CHAP v2
MPPE Encryption	☐ Enable 40 bits ▾
Service Port	1701

L2TP Server Status Refresh

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

User Account List Add Delete

ID	User Name	Password	Enable	Actions

User Account Configuration

User Name	Password	Account
		☐ Enable

Index skipping is used to reserve slots for new function insertion, when required.

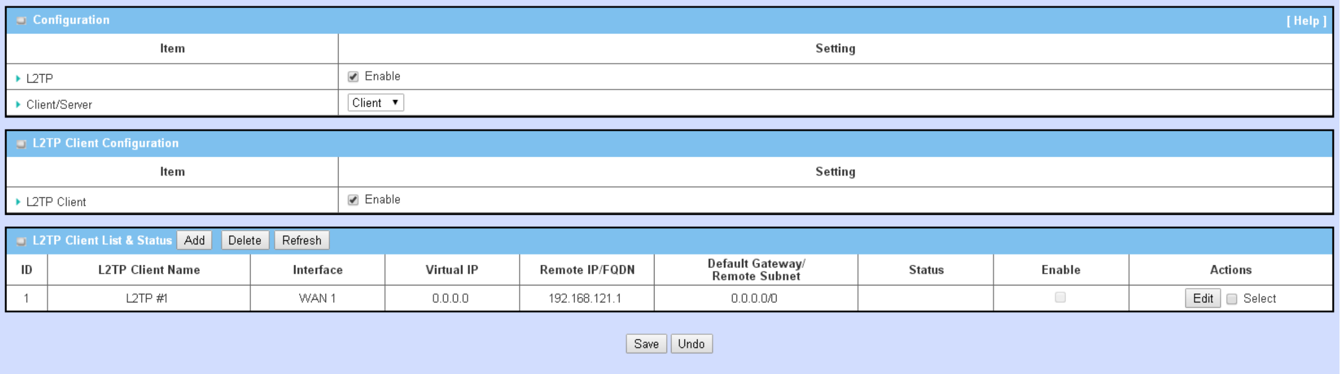
L2TP Server Configuration		
Item	**Value setting**	**Description**
L2TP	The box is unchecked by default	When click the **Enable** box It will activate L2TP functions.
Client/Server	A Must filled setting	Specify the role of **L2TP**. Selected **Server** ->Set as a L2TP server and jump to server configuration page Selected **Client** ->Set as a L2TP client and jump to client configuration page
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 as the authentication protocol which the box be click.
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 as the MPPE encryption which be choose. 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.

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.

Index skipping is used to reserve slots for new function insertion, when required.

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.

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



Configuration [Help]

Item	Setting
L2TP	☑ Enable
Client/Server	Client ▾

L2TP Client Configuration

Item	Setting
L2TP Client	☑ Enable

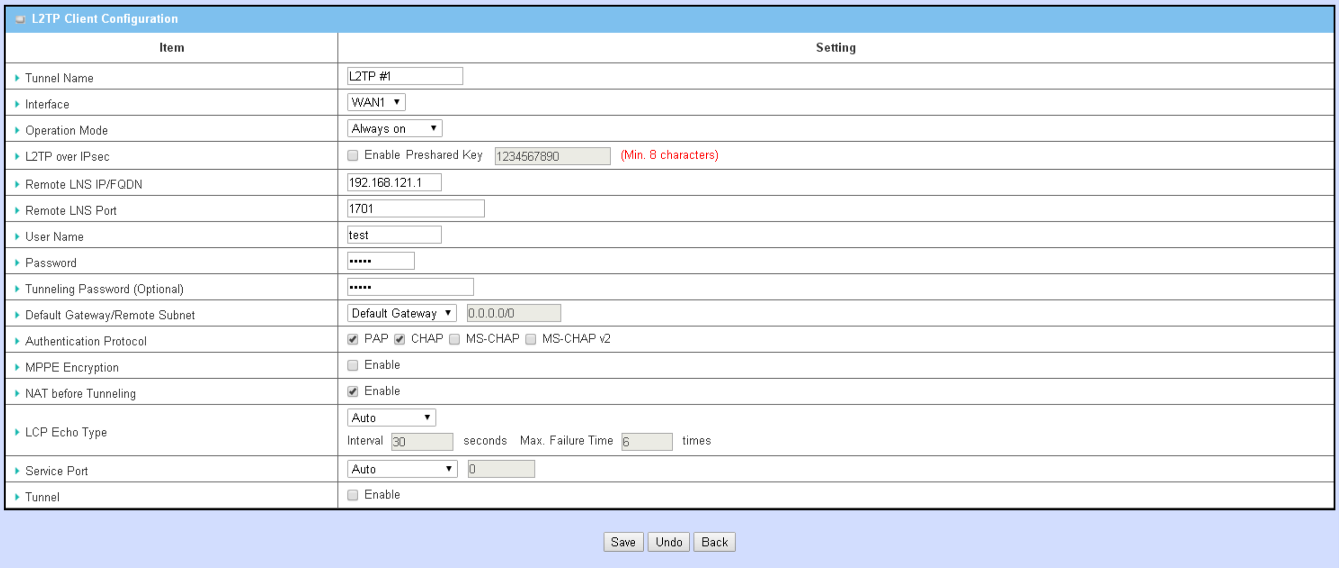
L2TP Client List & Status

ID	L2TP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/ Remote Subnet	Status	Enable	Actions
1	L2TP #1	WAN 1	0.0.0.0	192.168.121.1	0.0.0.0/0		□	Edit □ Select

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.

Index skipping is used to reserve slots for new function insertion, when required.

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 1234567890 (Min. 8 characters)
Remote LNS IP/FQDN	192.168.121.1
Remote LNS Port	1701
User Name	test
Password	•••••
Tunneling Password (Optional)	•••••
Default Gateway/Remote Subnet	Default Gateway ▾ 0.0.0.0/0
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).**
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	A Must filled setting	Specify **Authentication Protocol** for this L2TP tunnel will can be used.

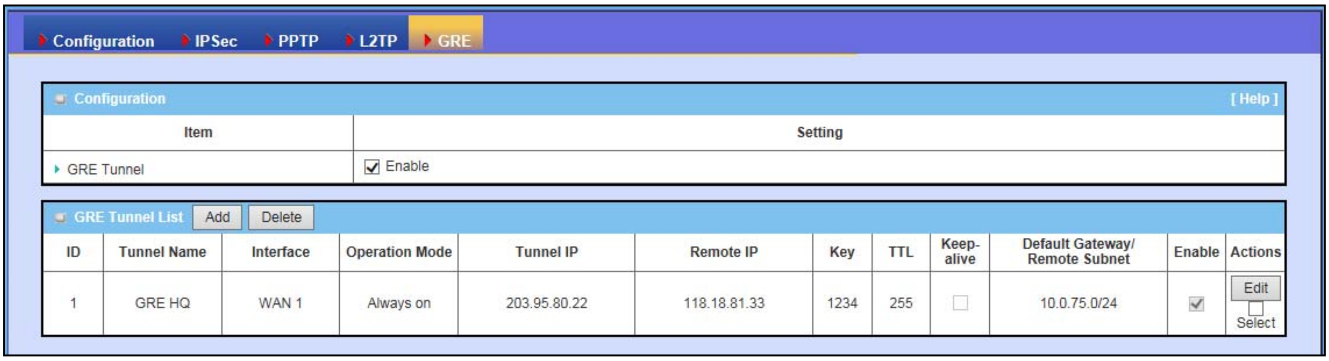
Index skipping is used to reserve slots for new function insertion, when required.

Protocol		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 availabe.
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.

5.5.9 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.



Configuration [Help]

Item	Setting
GRE Tunnel	☑ Enable

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
1	GRE HQ	WAN 1	Always on	203.95.80.22	118.18.81.33	1234	255	□	10.0.75.0/24	☑	Edit □ Select

In "GRE" page, there is a "Configuration" window to enable the GRE VPN function. In addition, the "GRE Tunnel List" window lists all your defined GRE tunnels. GRE is a peer to peer tunneling between two gateways. So, one set of parameters can be used for these both gateways to establish a GRE VPN tunnel by matching all parameters each other. Add one new GRE tunnel by using the "Add" button, and edit one existed tunnel by using the "Edit" button. At last, the "GRE Rule Configuration" window lets you specify all required parameters for a GRE tunnel.

A security gateway can be the client and server for a GRE tunnel at the same time. That is, the security gateway, configured as a client, can initiate the establishing of one GRE tunnel while taking a request for tunnel establishment from a remote GRE client security gateway, even using the same set of configuration settings.

Configuration

Index skipping is used to reserve slots for new function insertion, when required.

The "Configuration" window is to enable the GRE VPN function by checking the Enable box.

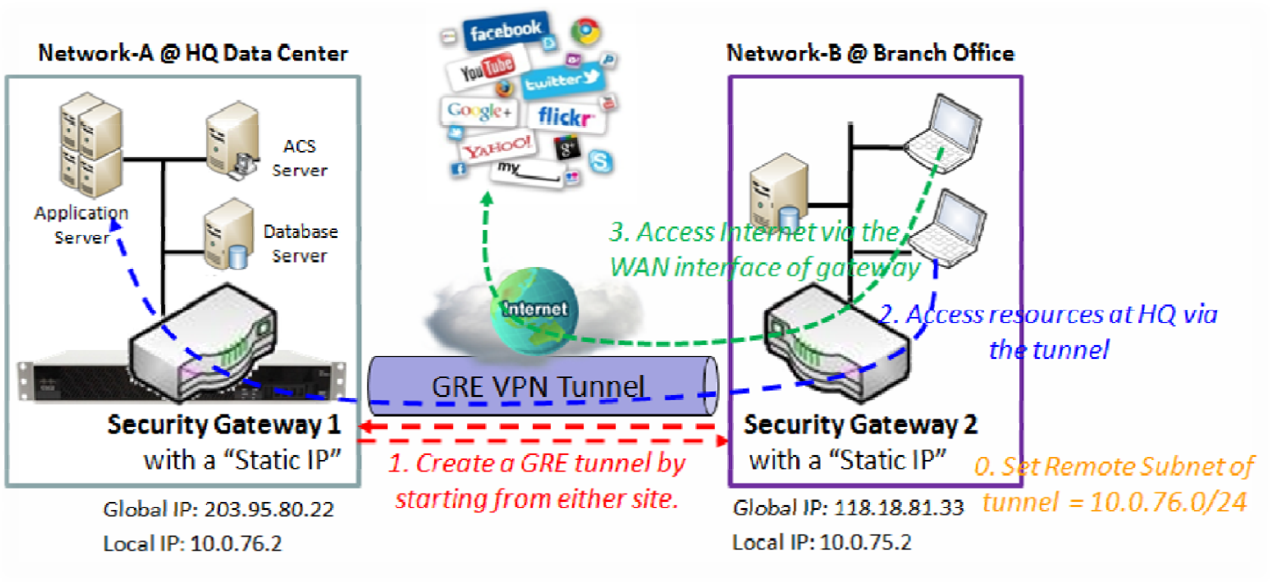
GRE Tunnel List

"GRE Tunnel List" window shows all your defined GRE tunnel profiles and parameters include Tunnel Name, Interface, Operation Mode, IP address of local peer, IP address of remote peer, Key, TTL, if keep alive or not, tunnel as the Default Gateway or specifying the remote subnet to flow through the tunnel, and tunnel activation.

GRE Rule Configuration

"GRE Rule Configuration" window can let you specify all parameters for a GRE VPN tunnel. Take a GRE tunnel between the gateway in headquarters and the one in branch office as an example fo following description.

GRE Tunnel at HQ Peer


Network-A @ HQ Data Center
ACS Server
Application 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"
Global IP: 118.18.81.33
Local IP: 10.0.75.2
0. Set Remote Subnet of tunnel = 10.0.76.0/24

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 an 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

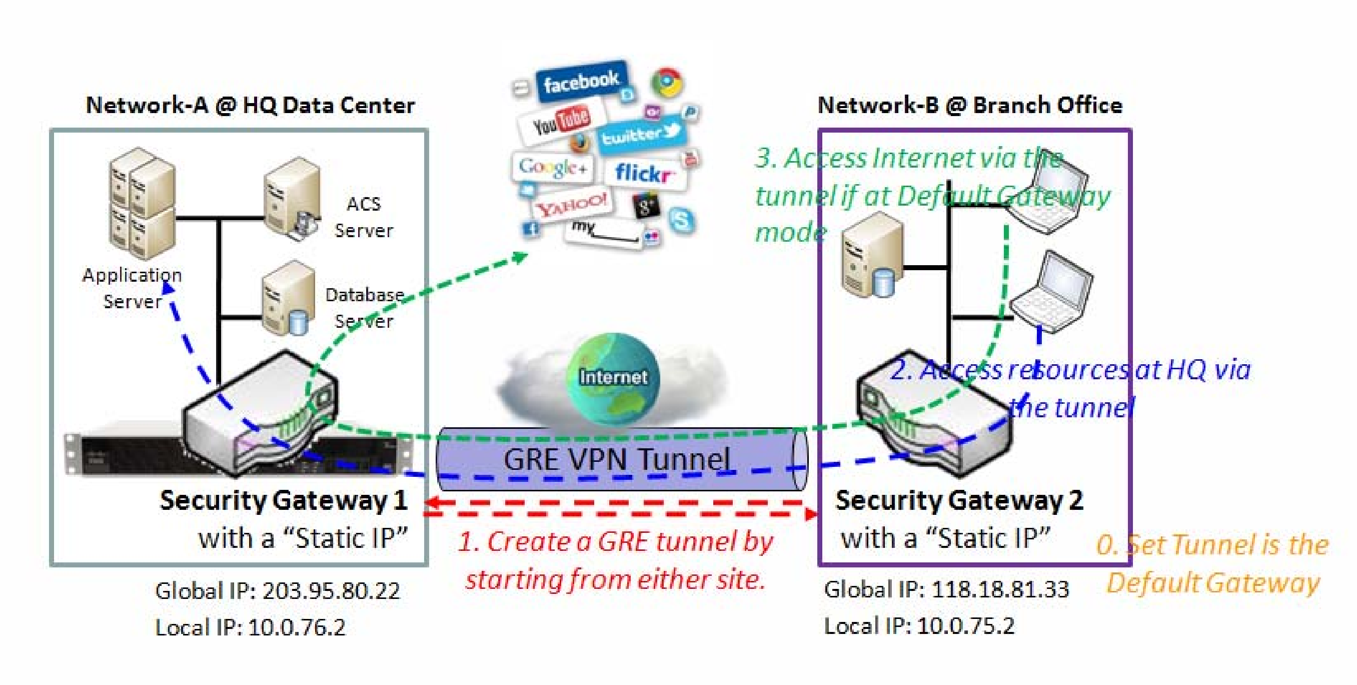
In above diagram, Network-A is in the headquarters, and the subnet of its Intranet is 10.0.76.0/24. The security gateway for Network-A has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN interface. It serves as a GRE server.

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.

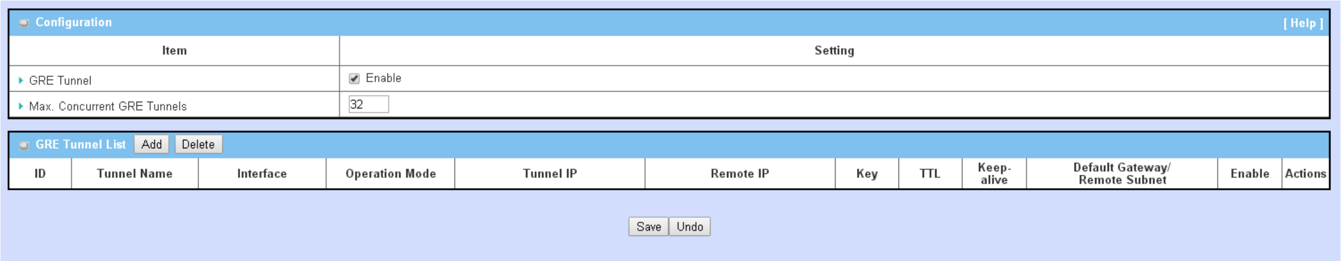
GRE Setting

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 Advanced Network > VPN > Configuration tab.

.

Enabling GRE

Go to Advanced Network > VPN > GRE tab



Configuration [Help]

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

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

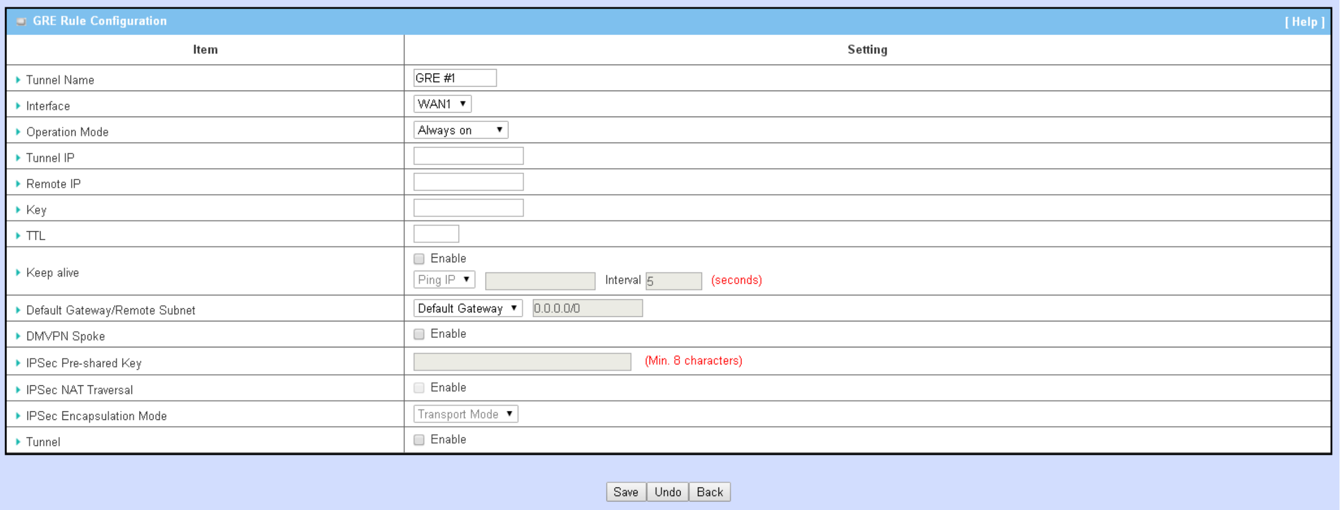
Save Undo

Enable GRE Window		
Item	**Value setting**	**Description**
GRE	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.
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

Create/Edit GRE tunnel

The router supports up to a maximum of 32 simultaneous GRE tunnel connections. Ensure that the GRE enable box is checked to enable before we can setup GRE.

When Add/Edit button is applied a series of configuration screen will appear.



GRE Rule Configuration [Help]

Item	Setting
Tunnel Name	GRE #1
Interface	WAN1 ▾
Operation Mode	Always on ▾
Tunnel IP	
Remote IP	
Key	
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 > Load Balance tab. Note: Failover and Load Balance functions are not available for Dynamic VPN specified in Tunnel Scenario.
Tunnel IP	A Must fill 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.

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. 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.
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.
GRE Pre-shared Key	1. Unchecked by default 2. Pre-shared Key 8 to 32 character length	Check Enable box to add pre-shared key for GRE tunnel connection. Enter a DMVPN spoke authentication Pre-shared Key. Note: Pre-shared Key will not be available when DMVPN Spoke is not enabled.
GRE NAT Traversal	Unchecked by default	Check Enable box to enable NAT-Traversal. Note: GRE NAT Traversal will not be available when DMVPN is not enabled.
GRE Encapsulation Mode	Unchecked by default	Specify GRE Encapsulation Mode from the dropdown box. There are Transport mode and Tunnel mode supported. Note: GRE 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.

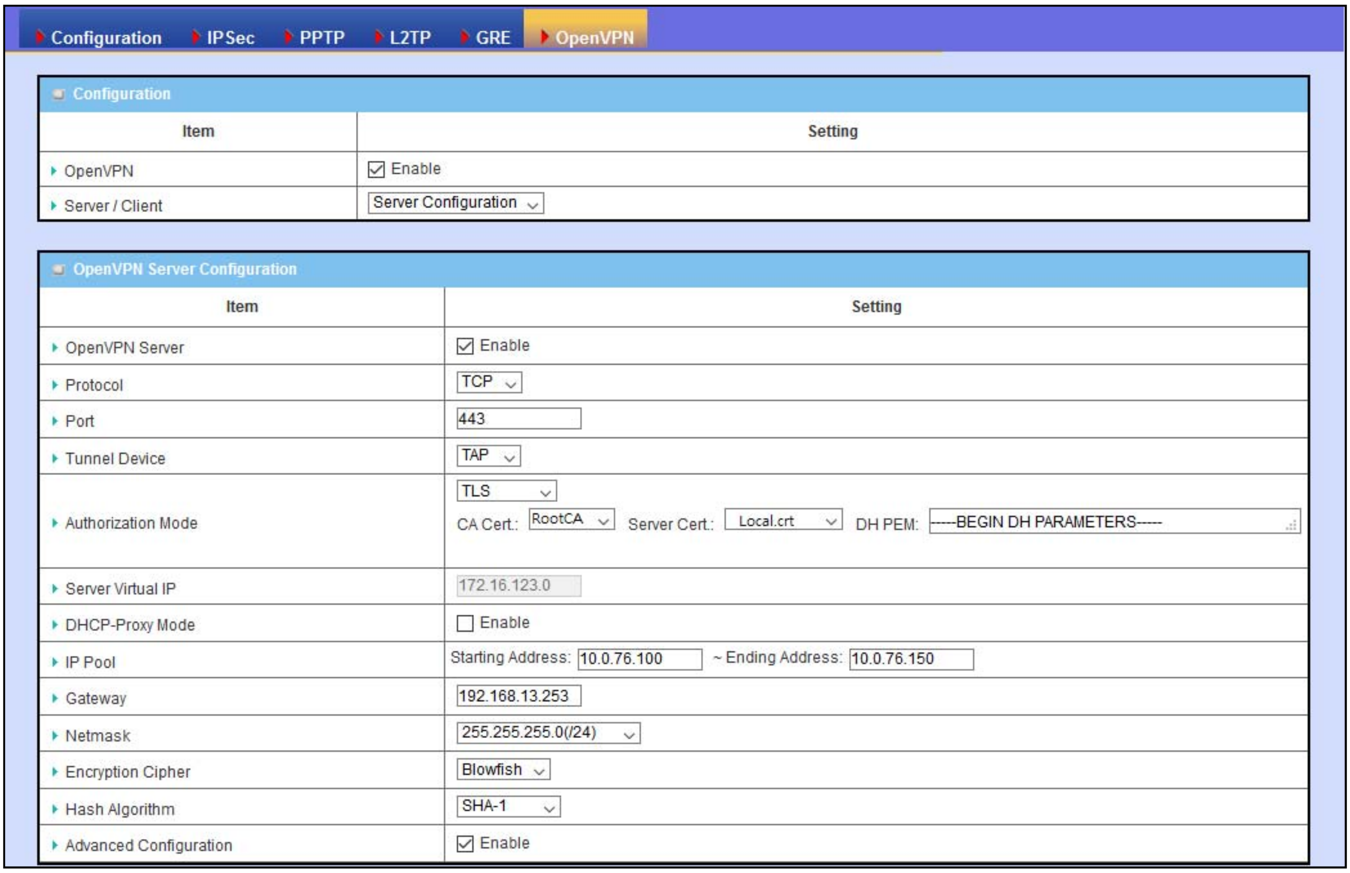
5.5.d OpenVPN

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.

Index skipping is used to reserve slots for new function insertion, when required.

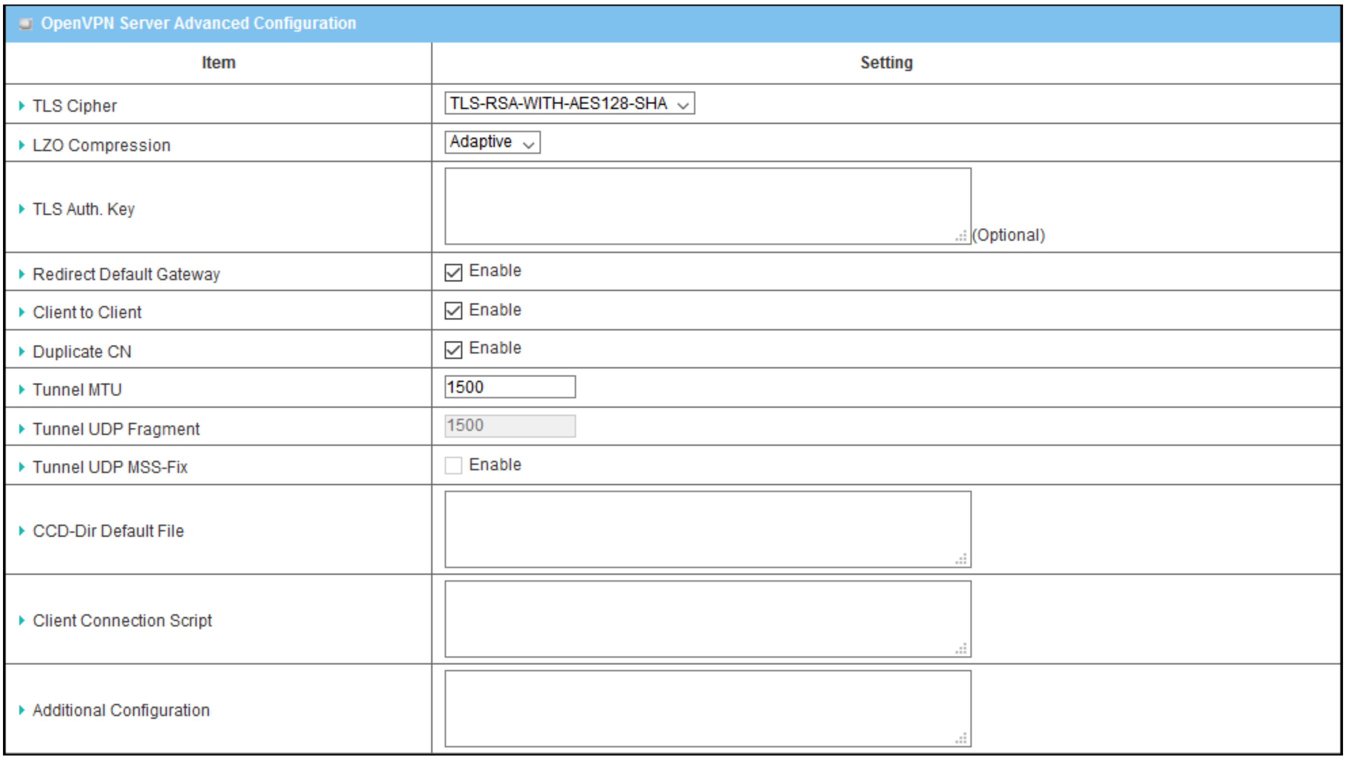


Configuration

Item	Setting
OpenVPN	☑ Enable
Server / Client	Server Configuration

OpenVPN Server Configuration

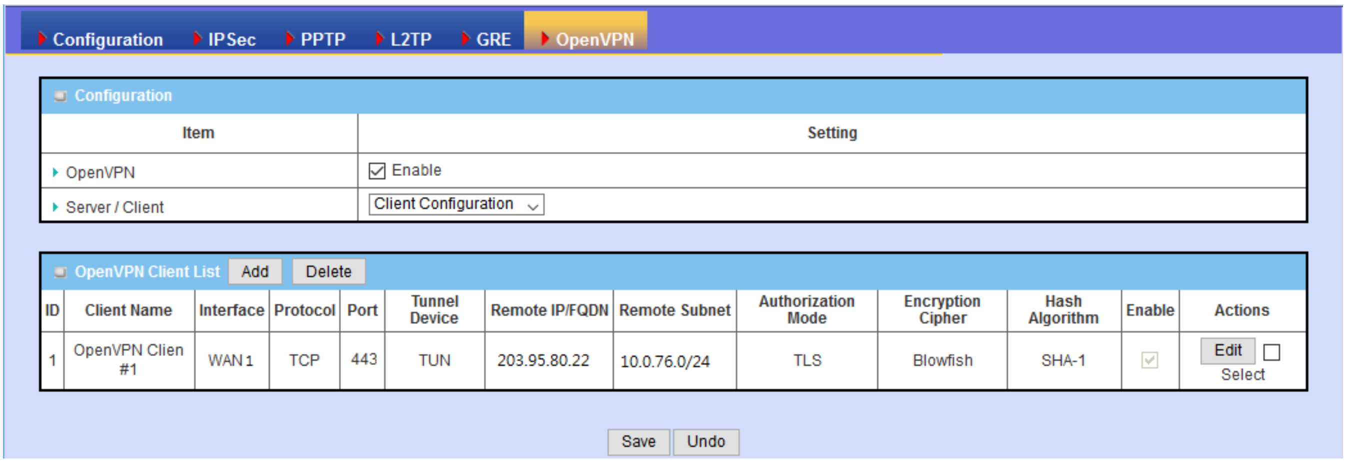
Item	Setting
OpenVPN Server	☑ Enable
Protocol	TCP
Port	443
Tunnel Device	TAP
Authorization Mode	TLS CA Cert.: RootCA Server Cert.: Local.crt DH PEM: -----BEGIN DH PARAMETERS-----
Server Virtual IP	172.16.123.0
DHCP-Proxy Mode	□ Enable
IP Pool	Starting Address: 10.0.76.100 ~ Ending Address: 10.0.76.150
Gateway	192.168.13.253
Netmask	255.255.255.0(/24)
Encryption Cipher	Blowfish
Hash Algorithm	SHA-1
Advanced Configuration	☑ Enable



OpenVPN Server Advanced Configuration

Item	Setting
TLS Cipher	TLS-RSA-WITH-AES128-SHA
LZO Compression	Adaptive
TLS Auth. Key	(Optional)
Redirect Default Gateway	☑ Enable
Client to Client	☑ Enable
Duplicate CN	☑ Enable
Tunnel MTU	1500
Tunnel UDP Fragment	1500
Tunnel UDP MSS-Fix	□ Enable
CCD-Dir Default File	
Client Connection Script	
Additional Configuration	

In "OpenVPN" page, there is the "Configuration" window to enable the OpenVPN function. The security gateway can either take "OpenVPN Server" role or "OpenVPN Client" role or they both. Define and choose either one role for your router in the "Configuration" window and configure all required parameters beneath the "Configuration" window. Then configure parameters on another gateway to take another role. Above diagram is the server role configuration and following diagram shows the client role configuration.



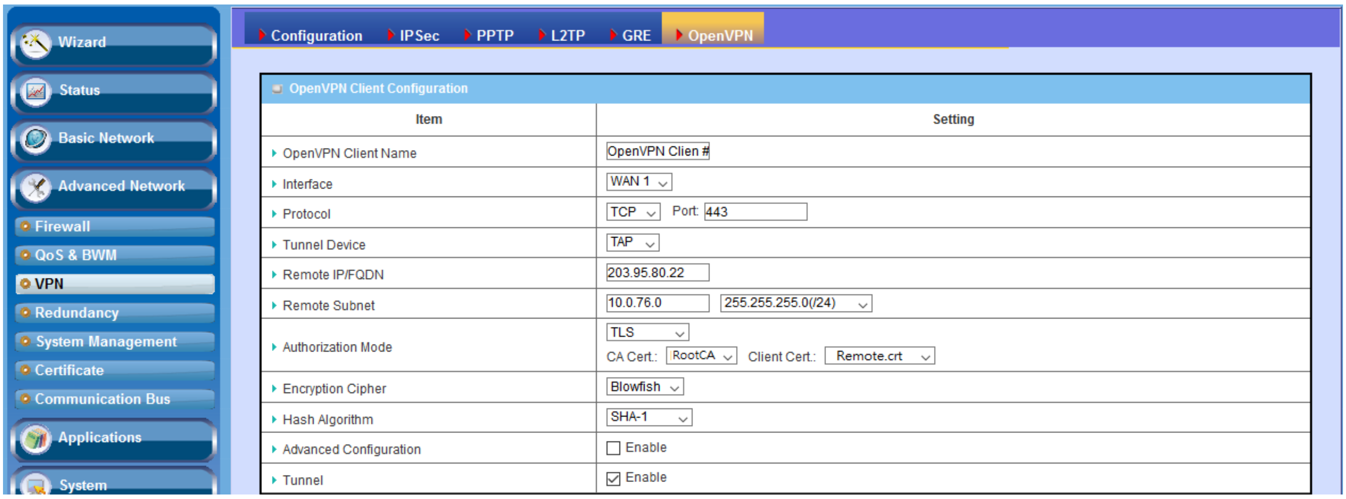
Configuration

Item	Setting
OpenVPN	☑ Enable
Server / Client	Client Configuration

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
1	OpenVPN Clien #1	WAN 1	TCP	443	TUN	203.95.80.22	10.0.76.0/24	TLS	Blowfish	SHA-1	☑	Edit □ Select

Save Undo



OpenVPN Client Configuration

Item	Setting
OpenVPN Client Name	OpenVPN Clien #
Interface	WAN 1
Protocol	TCP Port: 443
Tunnel Device	TAP
Remote IP/FQDN	203.95.80.22
Remote Subnet	10.0.76.0 255.255.255.0(/24)
Authorization Mode	TLS CA Cert.: RootCA Client Cert.: Remote.crt
Encryption Cipher	Blowfish
Hash Algorithm	SHA-1
Advanced Configuration	□ Enable
Tunnel	☑ Enable

To configure "OpenVPN Server or Client" role for the security gateway as follows:

Configuration

The "Configuration" window is to enable the OpenVPN by checking the Enable box. In the "Client/Server" field of the "Configuration" window choose either "Server" or "Client". Choose Server to define the gateway as the L2TP VPN server for remote clients to initiate the connection to establish VPN tunnels. Or choose Client to create multiple OpenVPN clients to establish VPN tunnels to remote gateways. Moreover, the security gateway serves as the OpenVPN client and server simultaneously.

OpenVPN VPN Server Scenario

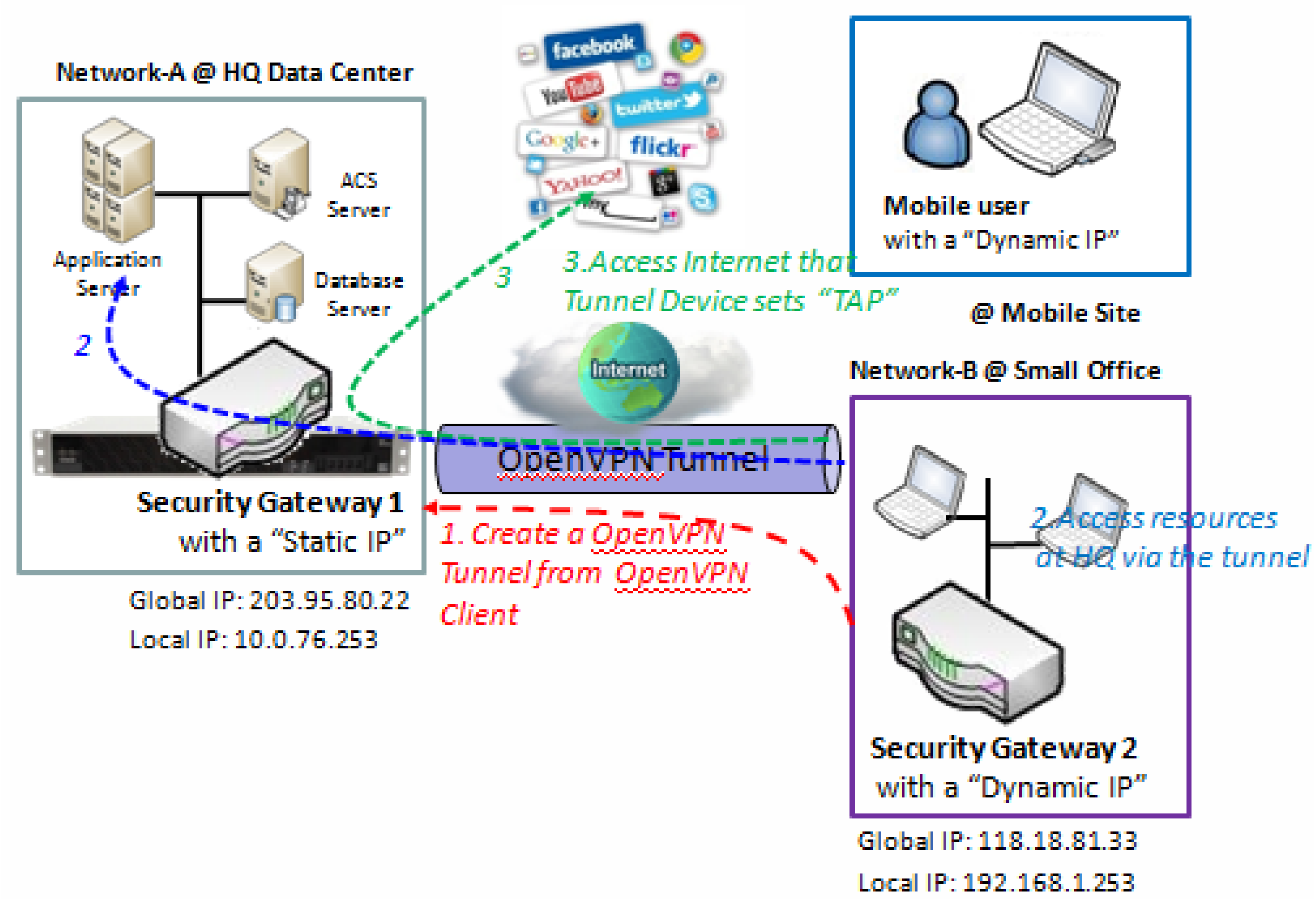
When you want the security gateway to play an OpenVPN server role, check the "Enable" box and choose "Server" option in the "OpenVPN Configuration" window. And make its related configuration in following sections. Also refer to the above server role diagram.

OpenVPN Server Configuration

In the "OpenVPN Server Configuration" window you will enable the OpenVPN server function, specify the virtual IP address of OpenVPN server, define the pool of virtual IP addresses that will assign to remote OpenVPN clients dialing in the security gateway, and the authentication protocol. Once you select "MS-CHAP" or "MS-CHAP v2" for the authentication protocol, you also can specify if the OpenVPN server needs the MPPE encryption and its key length or not for the authentication process.

OpenVPN Server Advanced Configuration

There are advanced settings available. Check the "Enable" box of Advanced Configuration.


Network-A @ HQ Data Center
Application Server
ACS Server
Database Server
2
3
3.Access Internet that Tunnel Device sets "TAP"
Internet
OpenVPN Tunnel
Security Gateway 1 with a "Static IP"
Global IP: 203.95.80.22
Local IP: 10.0.76.253
1. Create a OpenVPN Tunnel from OpenVPN Client
Mobile user with a "Dynamic IP"
@ Mobile Site
Network-B @ Small Office
2.Access resources at HQ via the tunnel
Security Gateway 2 with a "Dynamic IP"
Global IP: 118.18.81.33
Local IP: 192.168.1.253

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.

OpenVPN protocol is used for establishing an OpenVPN VPN tunnel.

Parameter Setup Example

For Network-A at HQ

Following below 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 VPN Client Scenario

When you want the security gateway to play an OpenVPN client role, check the "Enable" box and choose "Client" option in the "OpenVPN Configuration" window. And make its related configuration in following sections.

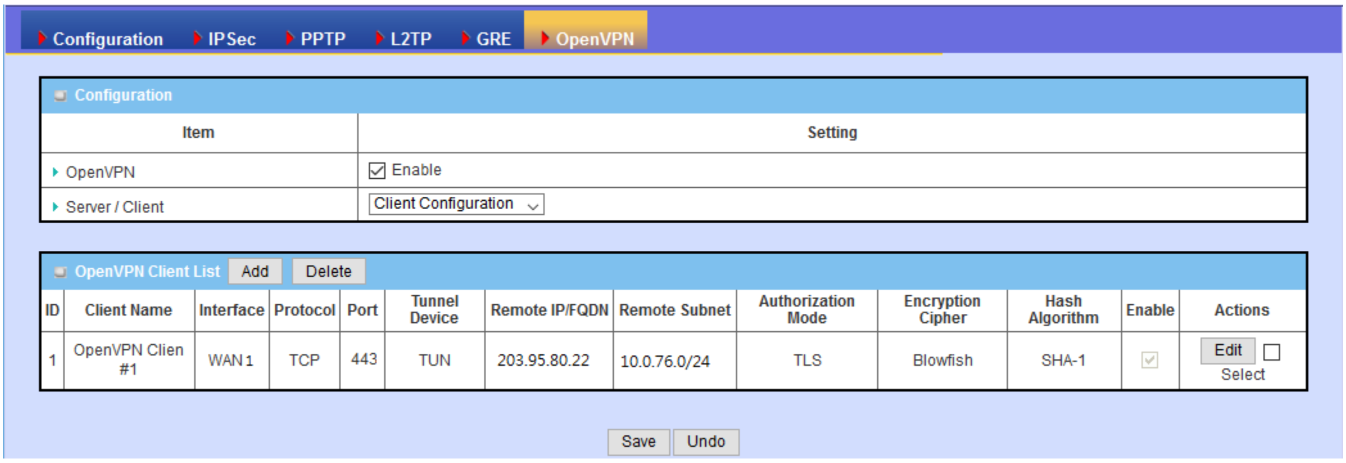
OpenVPN Client Configuration

"OpenVPN Client Configuration" window can let you enable the OpenVPN client function by checking the "Enable" box.

OpenVPN Client List

"OpenVPN Client List" window shows your defined OpenVPN clients and their tunnel status. Only some important information for all tunnels are shown in the list in following diagram.

Index skipping is used to reserve slots for new function insertion, when required.



Configuration | IPSec | PPTP | L2TP | GRE | OpenVPN

Configuration

Item	Setting
OpenVPN	☑ Enable
Server / Client	Client Configuration

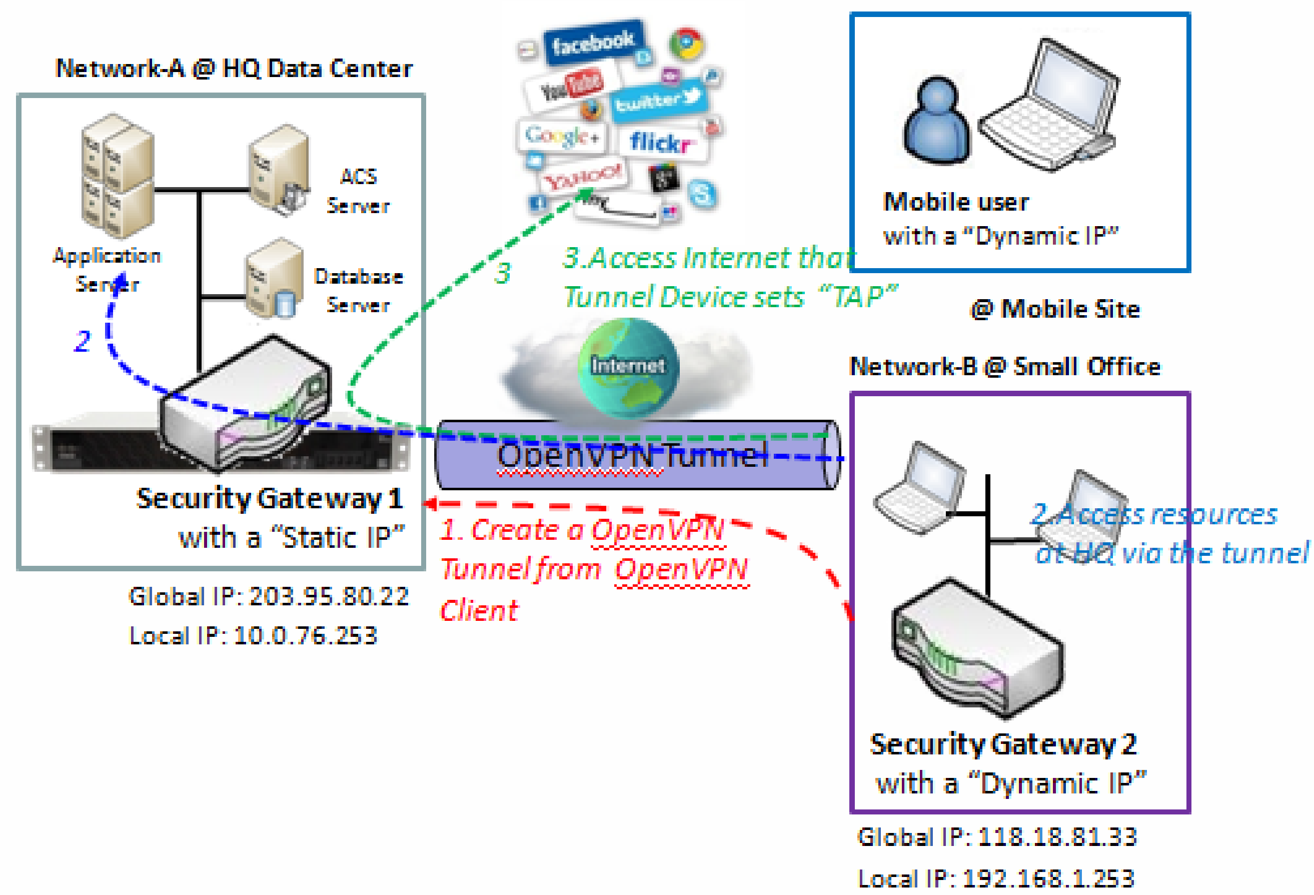
OpenVPN Client List Add Delete

ID	Client Name	Interface	Protocol	Port	Tunnel Device	Remote IP/FQDN	Remote Subnet	Authorization Mode	Encryption Cipher	Hash Algorithm	Enable	Actions
1	OpenVPN Clien #1	WAN 1	TCP	443	TUN	203.95.80.22	10.0.76.0/24	TLS	Blowfish	SHA-1	☑	Edit □ Select

Save Undo

Configuration for An OpenVPN Client

"Configuration for An OpenVPN Client" window let you specify the required parameters for an OpenVPN VPN client, such as "OpenVPN Client Name", "Interface", "Protocol", "Port", "Remote IP/FQDN", "Remote Subnet", "Authorization Mode", "Encryption Cipher", "Hash Algorithm," and tunnel activation.



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***

Index skipping is used to reserve slots for new function insertion, when required.

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.

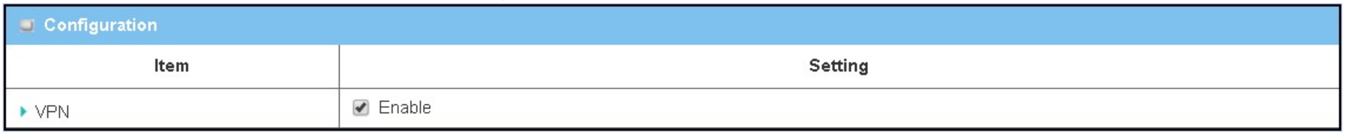
However, if the "Default Gateway/Remote Subnet" parameter in the Security Gateway 2 is configured to "Default Gateway", the Internet accessing of OpenVPN Client peer also go through the established OpenVPN VPN tunnel, and the Security Gateway 1 can control the accessing as same as the HQ resource accessing.

Open VPN Setting

T he configuration setting allows user to use OpenVPN.

Ensure VPN is enabled and saved

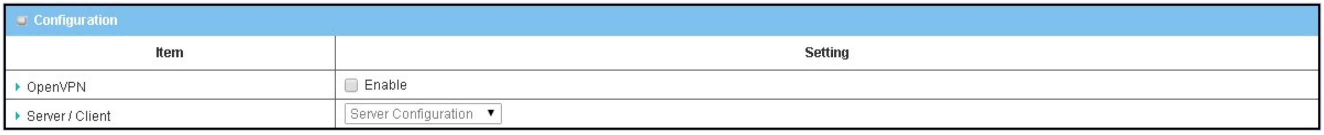
Go to Advanced Network > VPN > Configuration Tab



Configuration

Item	Setting
VPN	☑ Enable

Enable OpenVPN and select which server or client you want



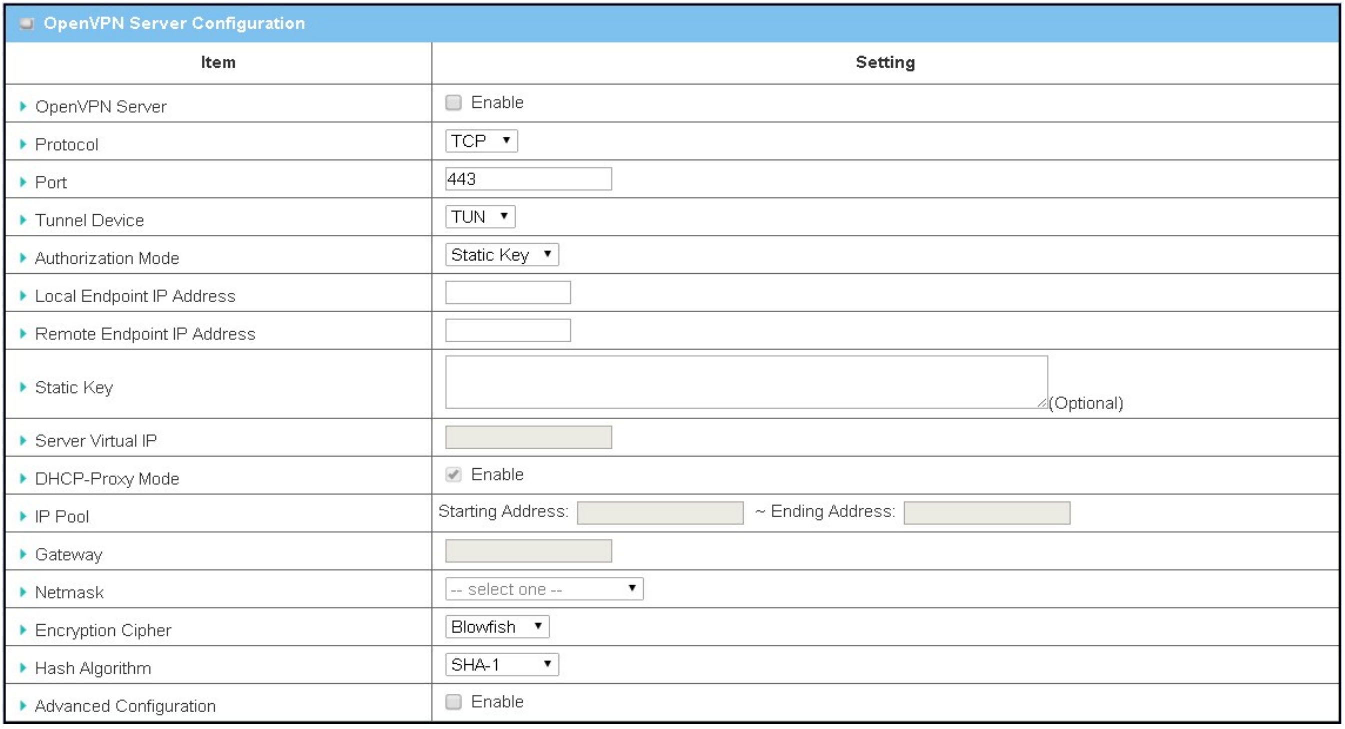
Configuration

Item	Setting
OpenVPN	□ Enable
Server / Client	Server Configuration ▾

Item	Value setting	Description
OpenVPN	The box is unchecked by default	Check the **Enable** box to activate this OpenVPN function.
Server/ Client	Server Configuration is set by default	When **Server Configuration** is selected, as the name suggest, server configuration will be display below, with **Client Configuration**, you can specifically set client configuration.

Index skipping is used to reserve slots for new function insertion, when required.

When Server Configuration is selected



OpenVPN Server Configuration

Item	Setting
OpenVPN Server	□ Enable
Protocol	TCP ▾
Port	443
Tunnel Device	TUN ▾
Authorization Mode	Static Key ▾
Local Endpoint IP Address	
Remote Endpoint IP Address	
Static Key	(Optional)
Server Virtual IP	
DHCP-Proxy Mode	☑ Enable
IP Pool	Starting Address: ~ Ending Address:
Gateway	
Netmask	-- select one -- ▾
Encryption Cipher	Blowfish ▾
Hash Algorithm	SHA-1 ▾
Advanced Configuration	□ Enable

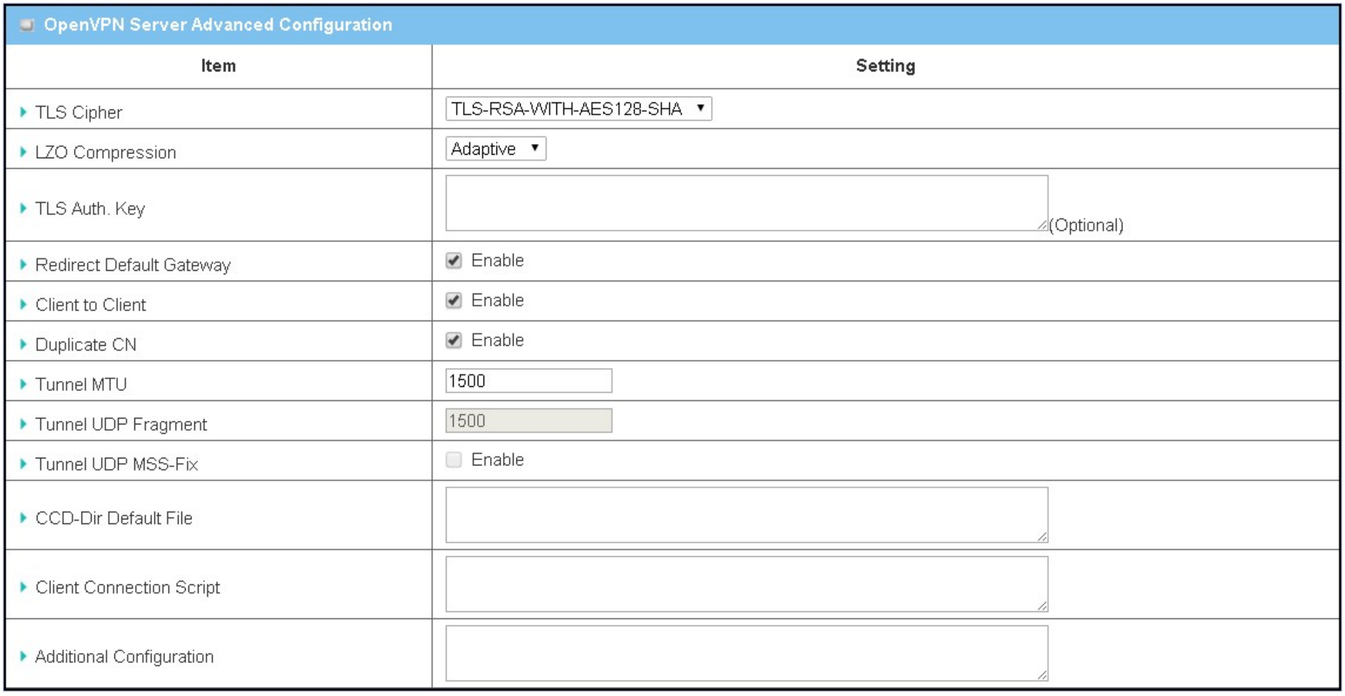
Item	Value setting	Description
OpenVPN Server	The box is unchecked by default	Click the **Enable** to activate OpenVPN Server functions.
Protocol	A Must filled setting By default **TCP** is selected.	Define the selected **Protocol** for the OpenVPN Server which to be. Select **TCP /UDP** for OpenVPN Server which to be. Select **TCP** for OpenVPN Server which to be. ->The OpenVPN will use TCP protocol, and **Port** will be set 443 automatically. Select **UDP** for OpenVPN Server which to be. -> The OpenVPN will use UDP protocol, and **Port** will be set 1194 automatically.
Port	A Must filled setting By default **443** is set.	Specify the **Port** for the OpenVPN Server to use.
Tunnel Device	A Must filled setting By default **TUN** is selected.	Specify the **Tunnel Device** for the OpenVPN Server to use. Select **TUN** for OpenVPN Server which to be. ->The OpenVPN will use TUN tunnel device. Select **TAP** for OpenVPN Server which to be. -> The OpenVPN will use TAP tunnel device.
Authorization Mode	A Must filled setting By default **Static Key** is selected.	Specify **Static Key/TLS** for the OpenVPN Server. Select **Static Key** for OpenVPN Server which to be. ->The OpenVPN will use static key authorization mode. The items **Local Endpoint IP Address**, **Remote Endpoint IP Address** and **Static Key** will be display. Select **TLS** for OpenVPN Server which to be. ->The OpenVPN will use TLS authorization mode. The items **CA Cert.**, **Server Cert.** and **DH PEM** will be display. **CA Cert.** could be generated in Certificate. Refer to

Index skipping is used to reserve slots for new function insertion, when required.

		Advanced Network > **Certificate** > **Trusted Certificates**. **Server Cert.** could be generated in Certificate. Refer to **Advanced Network** > **Certificate** > **My Certificates**. **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 be chose 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 be chose 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 be chose 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 be chose in Authorization Mode.
DHCP-Proxy Mode	A Must filled setting The box is checked by default.	Specify the DHCP-Proxy Mode. Note_1: DHCP-Proxy Mode will be available only when TAP is be chose in Tunnel Device.
IP Pool	A Must filled setting	Specify the OpenVPN server virtual **IP pool.** **Starting Address:** It will set as the starting IP which assign to OpenVPN client. **Ending Address:** It will set as the ending IP which assign to OpenVPN client. Note_1: IP Pool will be available only when TAP is be chose in Tunnel Device and DHCP-Proxy Mode is unchecked.
Gateway	A Must filled setting	Specify the OpenVPN server **Gateway** Note_1: Gateway will be available only when TAP is be chose in Tunnel Device and DHCP-Proxy Mode is unchecked.
Netmask	By default **- select one -** is selected.	Specify the OpenVPN server **Netmask.** Note_1: Netmask will be available when TAP is be chose in Tunnel Device and DHCP-Proxy Mode is unchecked. Note_2: Netmask will be available when TUN is be chose in Tunnel Device.
Encryption Cipher	By default **Blowfish** is selected.	Specify the Encryption Cipher. Selected the Blowfish/AES-256/AES-192/AES-128/None.
Hash Algorithm	By default **SHA-1** is selected.	Specify the Hash Algorithm Selected the SHA-1/MD5/MD4/SHA2-256/SHA2-512/None.
Advanced Configuration	The box is unchecked by default.	Specify the OpenVPN server **Advanced Configuration** setting. If it is checked, **Advanced Configuration** will be display below.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Index skipping is used to reserve slots for new function insertion, when required.

When select Advanced Configuration in OpenVPN Server Configuration will appear.



OpenVPN Server Advanced Configuration

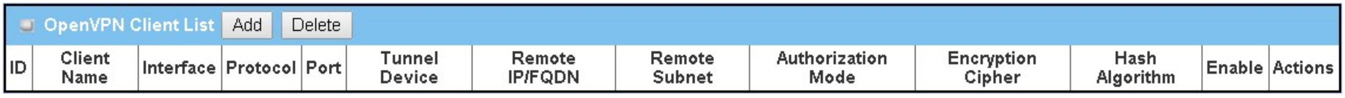
Item	Setting
TLS Cipher	TLS-RSA-WITH-AES128-SHA ▾
LZO Compression	Adaptive ▾
TLS Auth. Key	(Optional)
Redirect Default Gateway	☑ Enable
Client to Client	☑ Enable
Duplicate CN	☑ Enable
Tunnel MTU	1500
Tunnel UDP Fragment	1500
Tunnel UDP MSS-Fix	☐ Enable
CCD-Dir Default File	
Client Connection Script	
Additional Configuration	

Item	Value setting	Description
TLS Cipher	By default TLS-RSA-WITH-AES128-SHA is selected.	Specify the OpenVPN server **TLS Cipher.** Note_1: TLS Cipher will be available only when TLS is be chose in Authorization Mode.
LZO Compression	By default Adaptive is selected.	Specify the OpenVPN server **LZO Compression.**
TLS Auth. Key	String format: any text	Specify the OpenVPN server **TLS Auth. Key.** Note_1: TLS Auth. Key will be available only when TLS is be chose in Authorization Mode.
Redirect Default Gateway	The box is checked by default	Specify the OpenVPN server **Redirect Default Gateway.**
Client to Client	The box is checked by default	Specify the OpenVPN server **Client to Client.**
Duplicate CN	The box is checked by default	Specify the OpenVPN server **Duplicate CN.**
Tunnel MTU	A Must filled setting The value is 1500 by default	Specify the OpenVPN server **Tunnel MTU.**
Tunnel UDP Fragment	The value is 1500 by default	Specify the OpenVPN server **Tunnel UDP Fragment.** Note_1: Tunnel UDP Fragment will be available only when UDP is be chose in Protocol.
Tunnel UDP MSS-Fix	The box is unchecked by default.	Specify the OpenVPN server **Tunnel UDP MSS-Fix.** Note_1: Tunnel UDP MSS-Fix will be available only when UDP is be chose in Protocol.

Index skipping is used to reserve slots for new function insertion, when required.

CCD-Dir Default File	String format: any text	Specify the OpenVPN server **CCD-Dir Default File.**
Client Connection Script	String format: any text	Specify the OpenVPN server **Client Connection Script.**
Additional Configuration	String format: any text	Specify the OpenVPN server **Additional Configuration.**

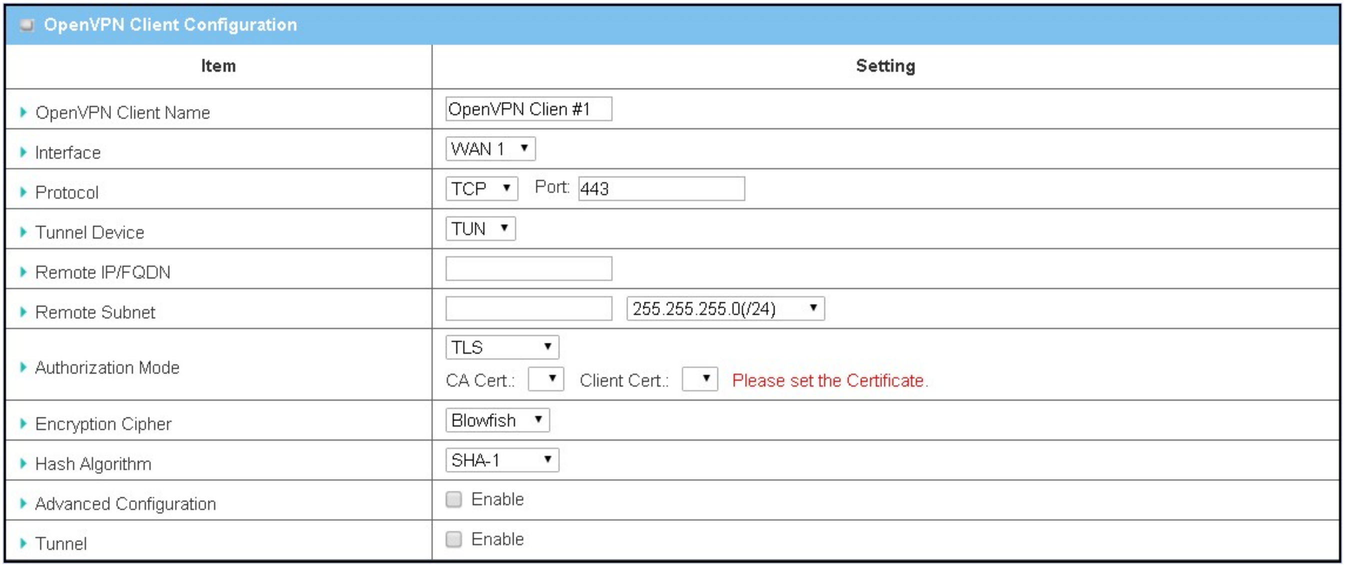
When select Client in Client/Server, a series OpenVPN Client Configuration will appear.



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 OpenVPN Client Configuration will appear.



OpenVPN Client Configuration

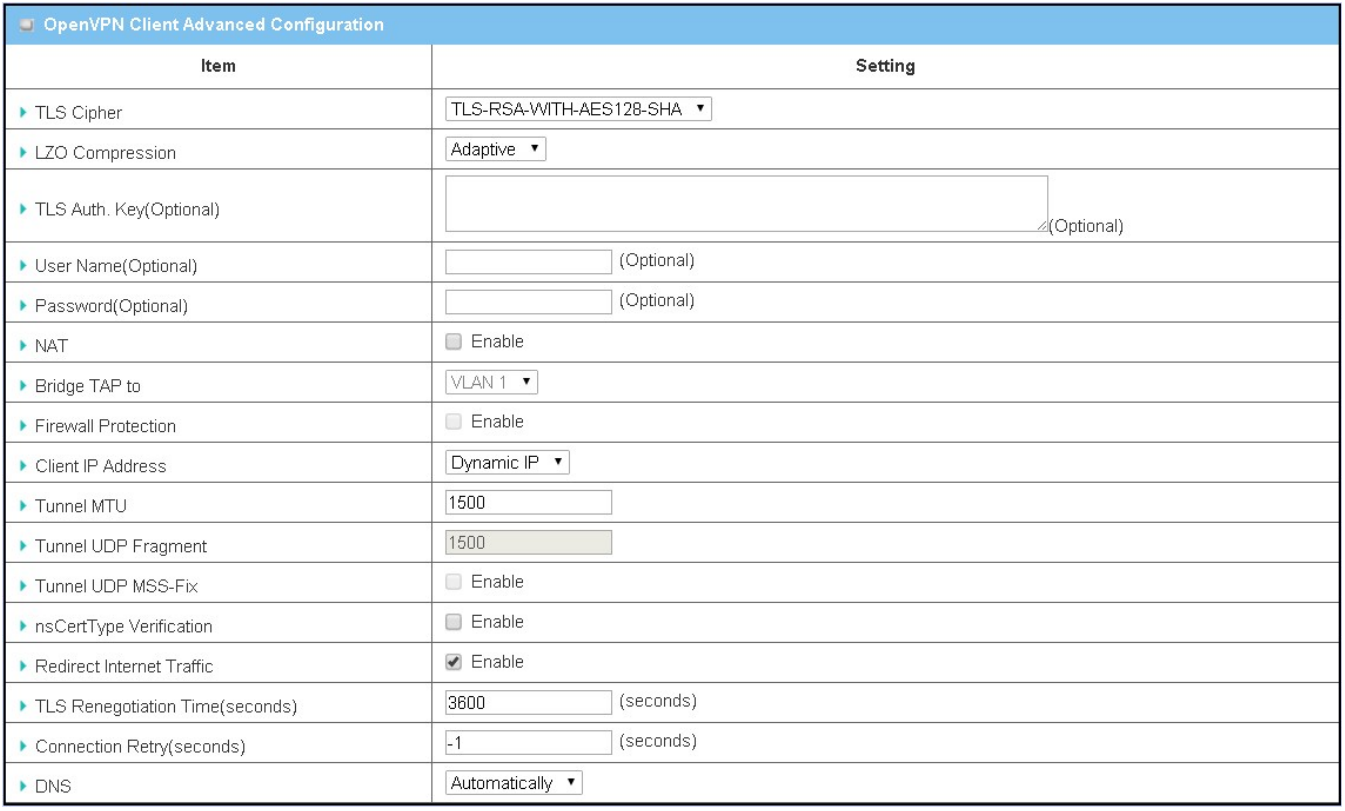
Item	Setting
OpenVPN Client Name	OpenVPN Clien #1
Interface	WAN 1 ▾
Protocol	TCP ▾ Port: 443
Tunnel Device	TUN ▾
Remote IP/FQDN	
Remote Subnet	255.255.255.0(/24) ▾
Authorization Mode	TLS ▾ CA Cert.: ▾ Client Cert.: ▾ Please set the Certificate.
Encryption Cipher	Blowfish ▾
Hash Algorithm	SHA-1 ▾
Advanced Configuration	□ Enable
Tunnel	□ Enable

Item	Value setting	Description
OpenVPN Client 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 OpenVPN Client tunnel. Select **WAN-1** for this OpenVPN Client tunnel by default.
Protocol	A Must filled setting By default **TCP** is selected.	Define the selected **Protocol** for the OpenVPN Client which to be. Select **TCP /UDP** for OpenVPN Client which to be. Select **TCP** for OpenVPN Client which to be. ->The OpenVPN will use TCP protocol, and **Port** will be set 443 automatically. Select **UDP** for OpenVPN Client which to be. -> The OpenVPN will use UDP protocol, and **Port** will be set 1194 automatically.
Port	A Must filled setting By default **443** is set.	Specify the **Port** for the OpenVPN Client to use.
Tunnel Device	A Must filled setting By default **TUN** is selected.	Specify the **Tunnel Device** for the OpenVPN Client to use. Select **TUN** for OpenVPN Client which to be. ->The OpenVPN will use TUN tunnel device.

		Select **TAP** for OpenVPN Client which to be. -> The OpenVPN will use TAP tunnel device.
Remote IP/FQDN	A Must filled setting	Specify the **Remote IP/FQDN** for this OpenVPN Client tunnel. Fill in the IP address or FQDN.
Remote Subnet	A Must filled setting	Specify **Remote Subnet** for this OpenVPN Client tunnel. Filled the remote subnet address and selected remote subnet mask.
Authorization Mode	A Must filled setting By default **TLS** is selected.	Specify **Static Key/TLS** for the OpenVPN Server. Select **Static Key** for OpenVPN Server which to be. ->The OpenVPN will use static key authorization mode. The items **Local Endpoint IP Address**, **Remote Endpoint IP Address** and **Static Key** will be display. Select **TLS** for OpenVPN Server which to be. ->The OpenVPN will use TLS authorization mode. The items **CA Cert.**, and **Client Cert.** will be display. **CA Cert.** could be generated in Certificate. Refer to **Advanced Network** > **Certificate** > **Trusted Certificates**. **Client Cert.** could be generated in Certificate. Refer to **Advanced Network** > **Certificate** > **My Certificates**.
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 be chose 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 be chose 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 be chose in Authorization Mode.
Encryption Cipher	By default **Blowfish** is selected.	Specify the Encryption Cipher. Selected the Blowfish/AES-256/AES-192/AES-128/None.
Hash Algorithm	By default **SHA-1** is selected.	Specify the Hash Algorithm. Selected the SHA-1/MD5/MD4/SHA2-256/SHA2-512/None.
Advanced Configuration	The box is unchecked by default.	Specify the OpenVPN client **Advanced Configuration** setting. If it is checked, **Advanced Configuration** will be display below.
Tunnel	The box is unchecked by default	When click Enable, it will enable this OpenVPN tunnel.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings
Back	N/A	Click the **Back** button to return the last page.

Index skipping is used to reserve slots for new function insertion, when required.

When select Advanced Configuration in OpenVPN Server Configuration will appear.



OpenVPN Client Advanced Configuration

Item	Setting
TLS Cipher	TLS-RSA-WITH-AES128-SHA ▾
LZO Compression	Adaptive ▾
TLS Auth. Key(Optional)	(Optional)
User Name(Optional)	(Optional)
Password(Optional)	(Optional)
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
nsCertType Verification	□ Enable
Redirect Internet Traffic	☑ Enable
TLS Renegotiation Time(seconds)	3600 (seconds)
Connection Retry(seconds)	-1 (seconds)
DNS	Automatically ▾

OpenVPN Client Advanced Configuration		
Item	**Value setting**	**Description**
TLS Cipher	By default TLS-RSA-WITH-AES128-SHA is selected.	Specify the OpenVPN client **TLS Cipher.** Note_1: TLS Cipher will be available only when TLS is be chose in Authorization Mode.
LZO Compression	By default Adaptive is selected.	Specify the OpenVPN client **LZO Compression.**
TLS Auth. Key (Optional)	String format: any text	Specify the OpenVPN client **TLS Auth. Key.** Note_1: TLS Auth. Key will be available only when TLS is be chose in Authorization Mode.
User Name (Optional)	String format: any text	Specify the OpenVPN client **User Name.**
Password (Optional)	String format: any text	Specify the OpenVPN client **Password.**
NAT	The box is unchecked by default.	Specify the OpenVPN client **NAT.**
Bridge TAP to	By default VLAN1 is selected	Specify the OpenVPN client **Bridge TAP to.** Note_1: Bridge TAP to will be available only when TAP is be chose in Tunnel Device and NAT is unchecked.
Firewall Protection	The box is unchecked by default.	Specify the OpenVPN client **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. Selected the Dynamic IP/Static IP Select **Static IP** for OpenVPN client which to be. -> Specify IP Address ->Fill in the IP Address. Specify Subnet Mask ->Fill in the Subnet Mask
Tunnel MTU	A Must filled setting The value is 1500 by default	Specify the OpenVPN client **Tunnel MTU.**
Tunnel UDP Fragment	The value is 1500 by default	Specify the OpenVPN client **Tunnel UDP Fragment.** Note_1: Tunnel UDP Fragment will be available only when UDP is be chose in Protocol.
Tunnel UDP MSS-Fix	The box is unchecked by default.	Specify the OpenVPN client **Tunnel UDP MSS-Fix.** Note_1: Tunnel UDP MSS-Fix will be available only when UDP is be chose in Protocol.
nsCertType Verification	The box is unchecked by default.	Specify the OpenVPN client **nsCertType Verification.**
Redirect Internet Traffic	The box is checked by default.	Specify the OpenVPN client Redirect Internet Traffic.
TLS Renegotiation Time (seconds)	The value is 3600 by default	Specify the OpenVPN client **TLS Renegotiation Time.**
Connection Retry (seconds)	The value is -1 by default	Specify the OpenVPN client **Connection Retry.** The value is -1 which represent infinite.
DNS	By default Automatically is selected	Specify the OpenVPN client **DNS.** Selected the Automatically/Manually Select **Manually** for OpenVPN client which to be. -> Specify Primary DNS ->Fill in the Primary DNS. Specify Secondary DNS ->Fill in the Secondary DNS

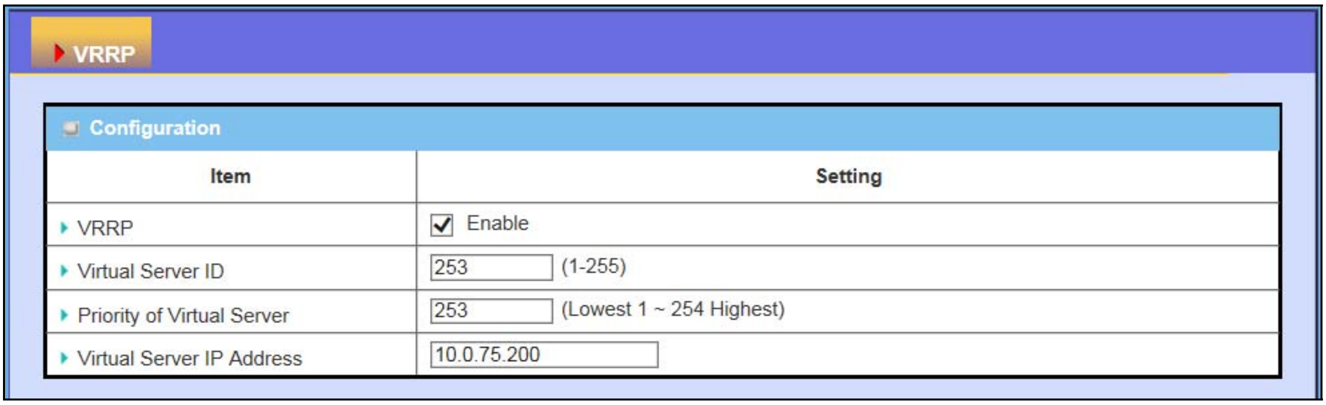
5.7 Redundancy

In engineering, redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system, usually in the form of a backup or fail-safe. In 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.

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

5.7.1 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.



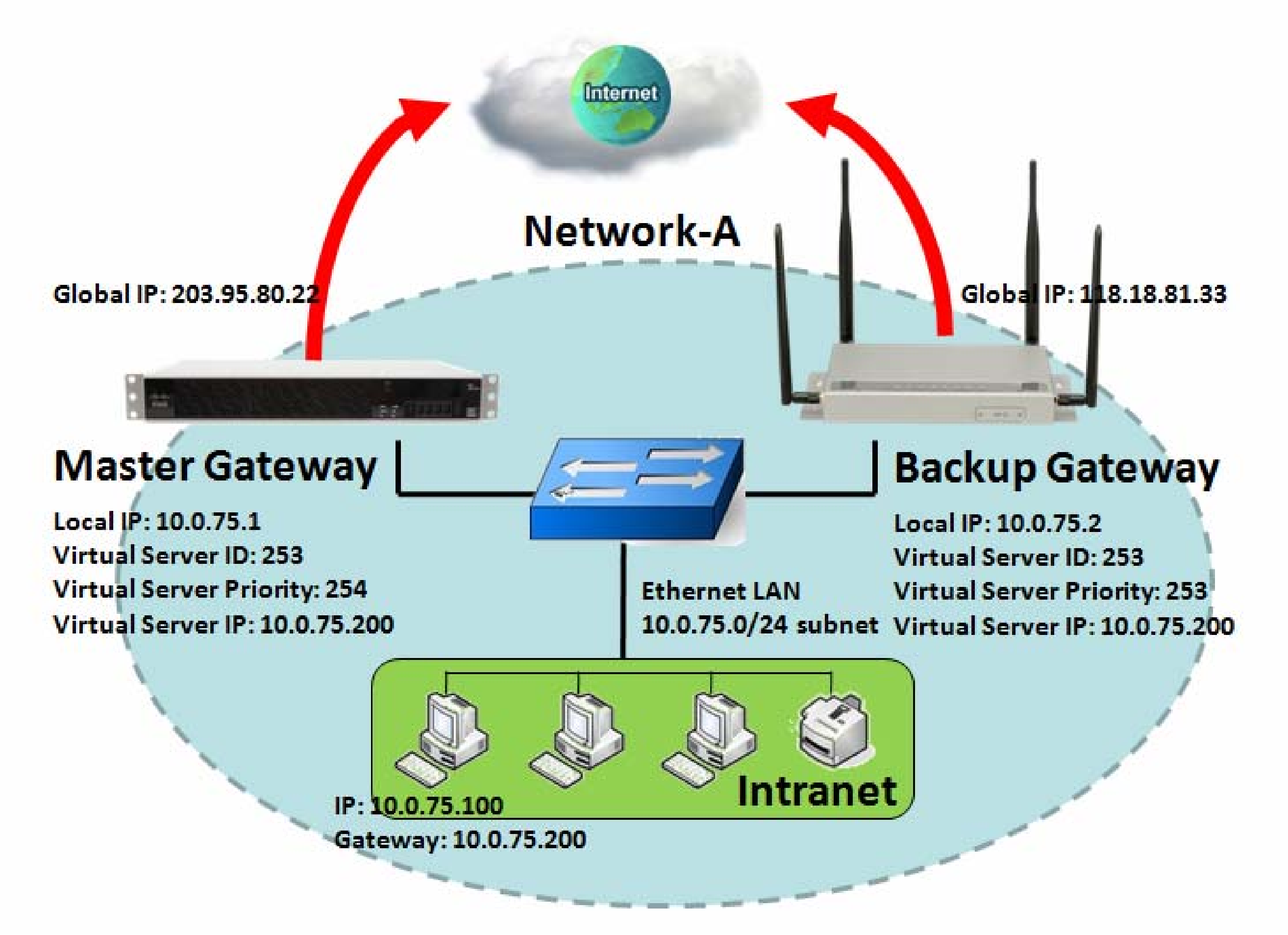
Configuration

Item	Setting
VRRP	☑ Enable
Virtual Server ID	253 (1-255)
Priority of Virtual Server	253 (Lowest 1 ~ 254 Highest)
Virtual Server IP Address	10.0.75.200

In "VRRP" page, there is only one configuration window for Redundancy function. 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.

VRRP Configuration

Check the "Enable" box to activate the VRRP function for the 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.

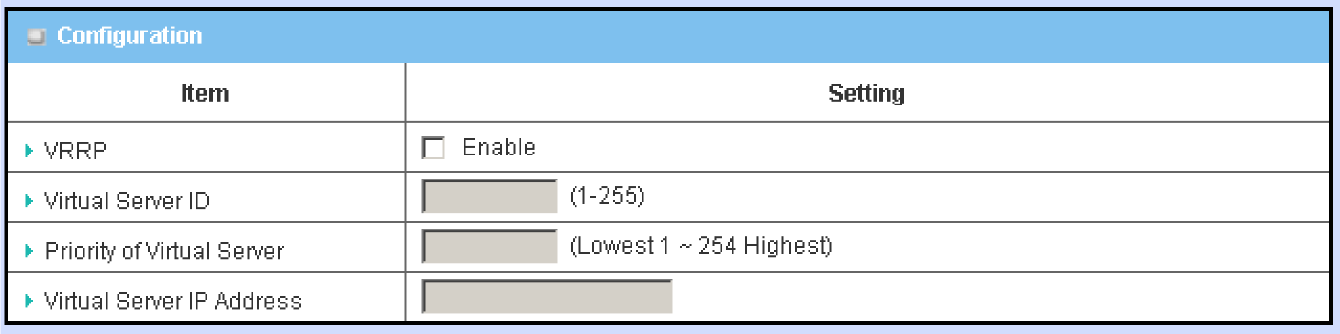
Index skipping is used to reserve slots for new function insertion, when required.

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

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

Go to Advanced 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**
Enable VRRP function	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	Define the Virtual Server ID on VRRP of the router. The value range is from 1 to 255.
Priority of Virtual Server	1. Numberic String Format 2. A Must filled setting	Define the Priority of Virtual Server on VRRP of the router. The value range is from 1 to 254.
Virtual Server IP Address	1. IPv4 Format 2. A Must filled setting	Define the Virtual Server IP Address on VRRP of the router.
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.

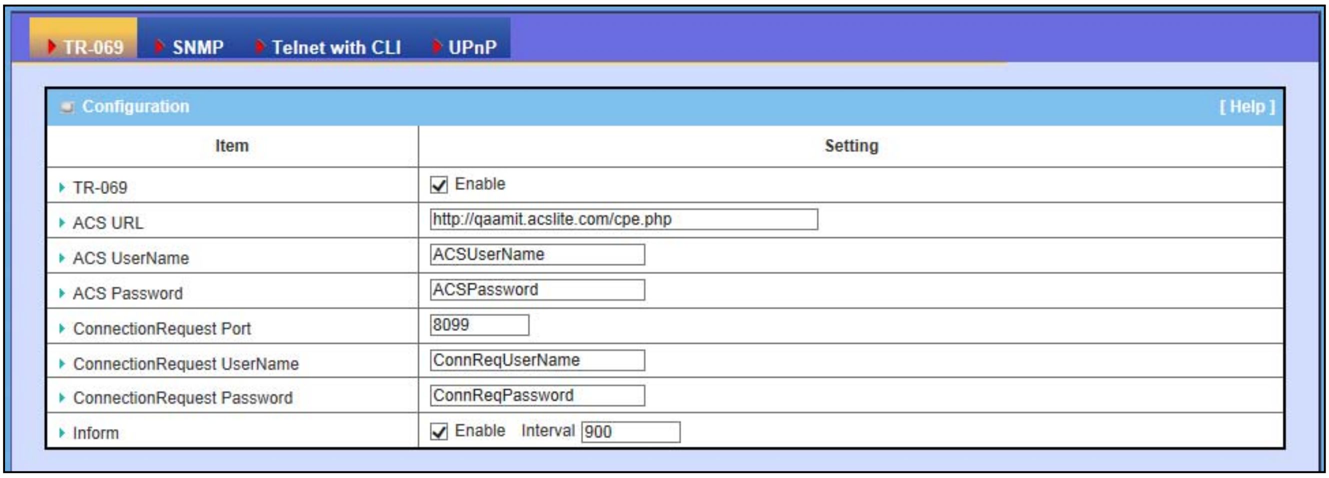
5.9 System Management

System management 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 TR-069, SNMP, Telnet with CLI and UPnP. You can setup those configurations in the "System Management" section.

5.9.1 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.



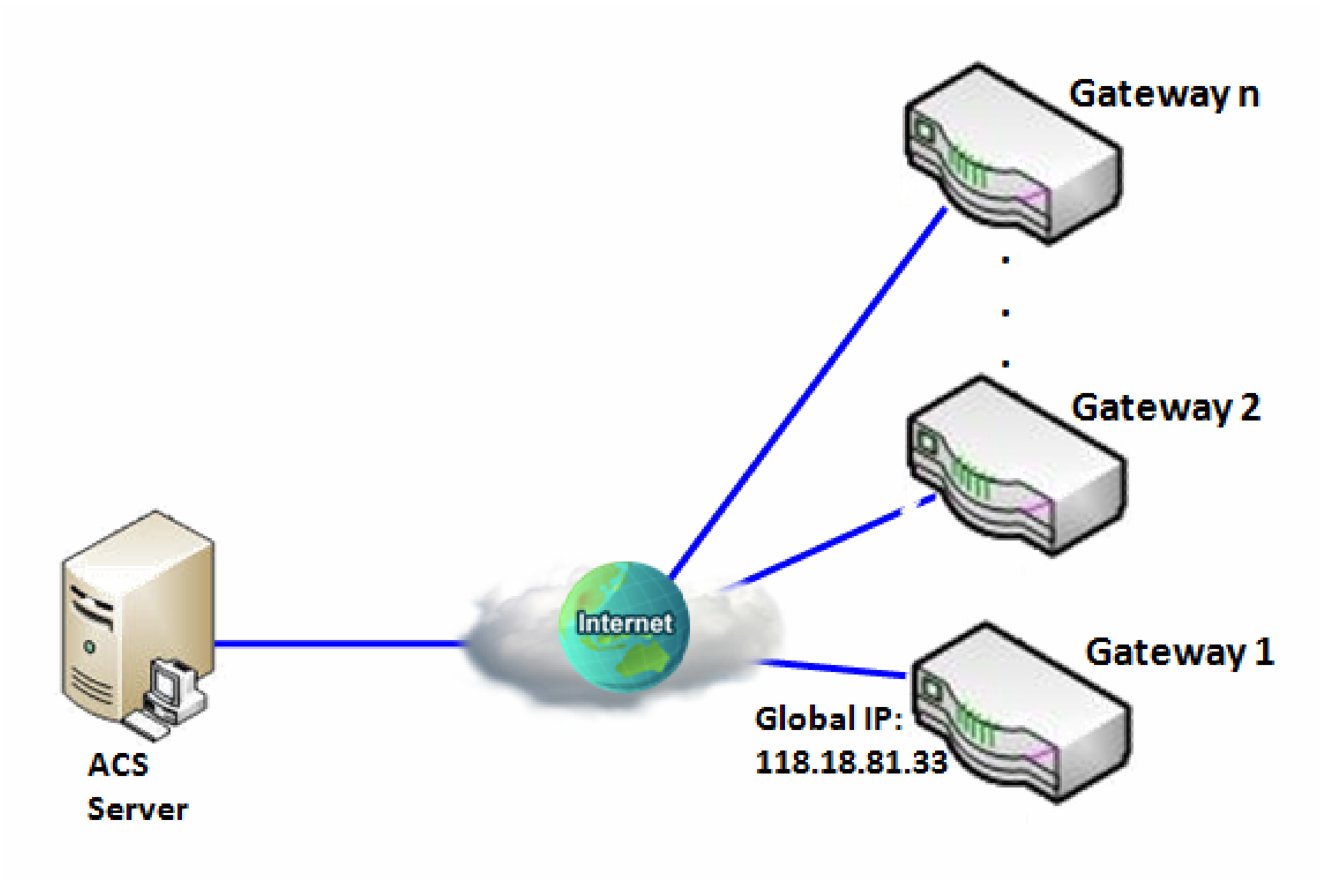
Configuration [Help]

Item	Setting
TR-069	☑ Enable
ACS URL	http://qaamit.acslite.com/cpe.php
ACS UserName	ACSUserName
ACS Password	ACSPassword
ConnectionRequest Port	8099
ConnectionRequest UserName	ConnReqUserName
ConnectionRequest Password	ConnReqPassword
Inform	☑ Enable Interval 900

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.

TR-069 Configuration

Check the "Enable" box to activate the TR-069 function for the gateway. 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.



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.

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.

Index skipping is used to reserve slots for new function insertion, when required.

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.

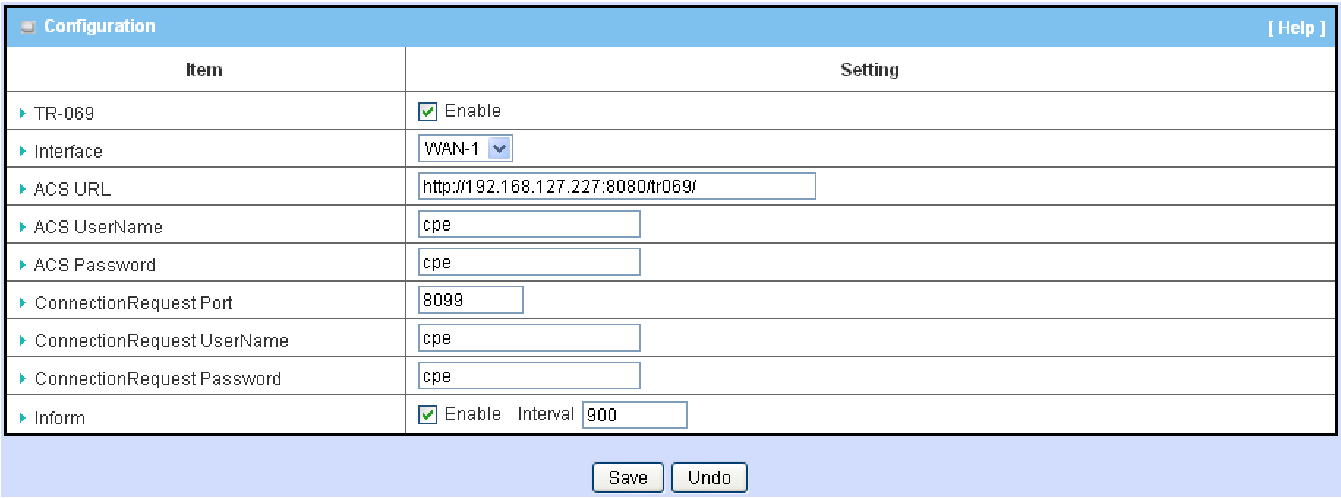
When all remote gateways have booted up, they will try to connect to the ACS server.

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.

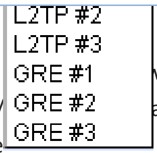
Go to Advanced Network > System Management > TR-069



Configuration [Help]

Item	Setting
TR-069	☑ Enable
Interface	WAN-1
ACS URL	http://192.168.127.227:8080/tr069/
ACS UserName	cpe
ACS Password	cpe
ConnectionRequest Port	8099
ConnectionRequest UserName	cpe
ConnectionRequest Password	cpe
Inform	☑ Enable Interval 900

Index skipping is used to reserve slots for new function insertion, when required.

TR-069		
Item	**Value setting**	**Description**
TR-069 Enable	The box is unchecked by default	Check the **Enable** box for activate TR-069
Interface	Auto is selected by default.	When you finish set basic network wan 1~wan n, you can  L2TP #2 L2TP #3 GRE #1 GRE #2 GRE #3 van n When you finish set advance network > vpn > Ipsec/pptp/ an choose Ipsec/pptp/l2tp/GRE tunnel, the interface just like
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 manu ally set
ACS Password	A Must filled setting	You can ask ACS manager provide ACS password and manually set
ConnectionRequest Port	A Must filled setting	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 Enable	The box is checked by default	When the box is checked, cpe periodic send inform to ACS
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 cpe(Client Premium Equipment) can send inform to ACS

When you finish set **ConnectionRequest Port ConnectionRequest Username ConnectionRequest Password** ,ACS can ask cpe send inform to ACS

5.9.3 SNMP

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

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

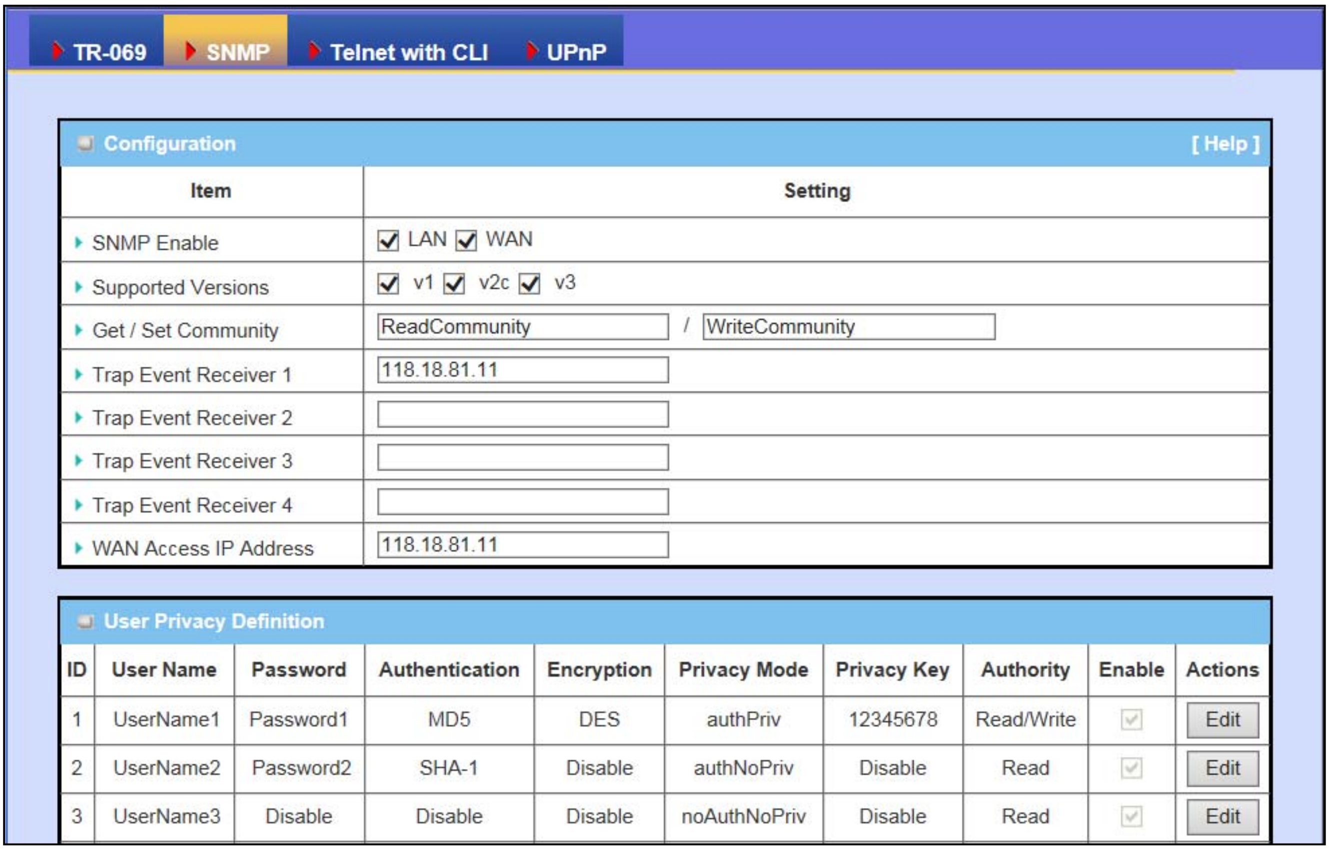
SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. These hierarchies,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

The device supports several public MIBs and one private MIB for the SNMP agent. The supported MIBs are as follow:

Supported MIBs
MIB-II (RFC 1213, Include IPv6)
IF-MIB, IP-MIB, TCP-MIB, UDP-MIB
SMIv1 and SMIv2
SNMPv2-TM and SNMPv2-MIB
AMIB (AMIT Private MIB)

In "SNMP" page, there are two configuration windows for SNMP function, including the "Configuration" window and the "User Privacy Definition" window. The "Configuration" window can let you configure the embedded SNMP agent in the gateway to run SNMP function. In addition, the "User Privacy Definition" window is for SNMPv3 only and provides 5 records of user privacy definition for user authentication and data hashing and encryption.

Index skipping is used to reserve slots for new function insertion, when required.



Configuration

Item	Setting
SNMP Enable	☑ LAN ☑ WAN
Supported Versions	☑ v1 ☑ v2c ☑ v3
Get / Set Community	ReadCommunity / WriteCommunity
Trap Event Receiver 1	118.18.81.11
Trap Event Receiver 2	
Trap Event Receiver 3	
Trap Event Receiver 4	
WAN Access IP Address	118.18.81.11

User Privacy Definition

ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	Enable	Actions
1	UserName1	Password1	MD5	DES	authPriv	12345678	Read/Write	☑	Edit
2	UserName2	Password2	SHA-1	Disable	authNoPriv	Disable	Read	☑	Edit
3	UserName3	Disable	Disable	Disable	noAuthNoPriv	Disable	Read	☑	Edit

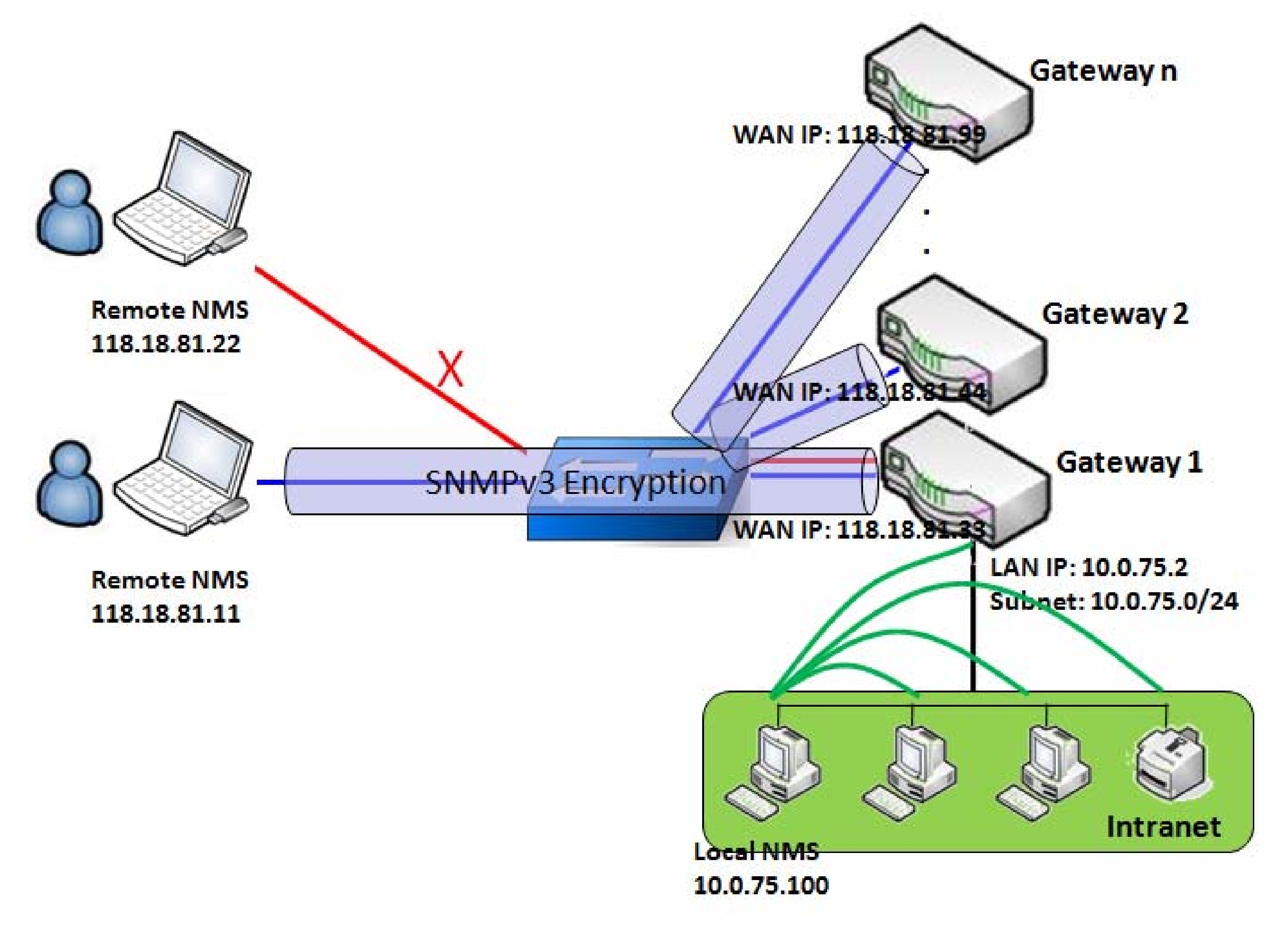
SNMP Configuration

Check the "Enable" box to activate the SNMP function for the gateway. Drive the function to work by specifying the access interfaces of SNMP protocol, the supported protocol versions, the read/write communities, the trap event receivers and the allowed IP address from outside to access the gateway by using SNMP protocol.

User Privacy Definition

However, if SNMPv3 is not listed in the supporting of the "Configuration" window, the "User Privacy Definition" window will be not used for SNMP agent in the gateway. The "User Privacy Definition" window provides 5 records of user privacy definition for user authentication and data hashing and encryption. In SNMPv3, SNMP protocol supports user privacy feature additionally. By referring to above setting diagram, there are 3 privacy modes: authPriv, authNoPriv and noAuthNoPriv. At authPriv mode, User Name and Password are used for user authentication during logging in the SNMP server. And, MD5 or SHA-1 algorithm is chosen for data hashing and DES algorithm is for data encryption. Additional Privacy Key is also used in data encryption. However, at authNoPriv mode, User Name and Password are for user authentication to login SNMP server, MD5 or SHA-1 algorithm is chosen for data hashing and there is no need of Encryption and Privacy Key. At last, at noAuthNoPriv mode, there is only User Name to be required to login the SNMP server. No matter which privacy mode is used, the authority of user can be defined to be Read-only or Read/Write both.

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

Index skipping is used to reserve slots for new function insertion, when required.

NMS and the managed devices, use SNMPv3 version of protocol.

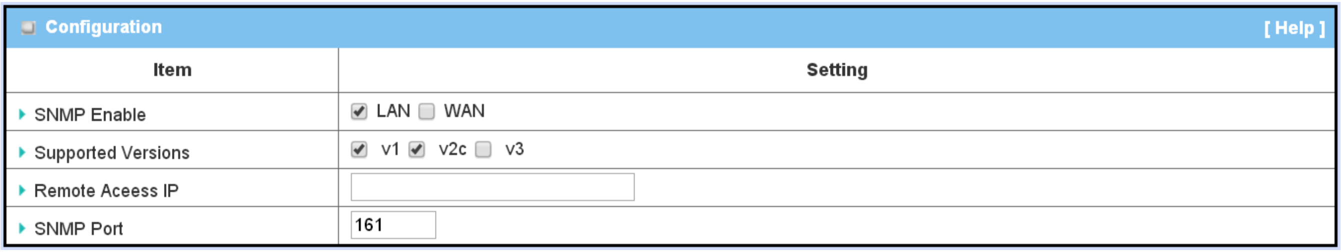
The remote NMS without privilege IP address can't manage the "Gateway 1", since "Gateway 1" allows only the NMS with privilege IP address can manage it via its WAN interface.

SNMP Setting

The SNMP allows user to configure SNMP relevant setting which includes interface, version, access control and trap receiver

Ensure Configuration are enabled and saved

Go to Advanced Network > System Management > SNMP



Configuration [Help]

Item	Setting
SNMP Enable	☑ LAN ☐ WAN
Supported Versions	☑ v1 ☑ v2c ☐ v3
Remote Aceess IP	
SNMP Port	161

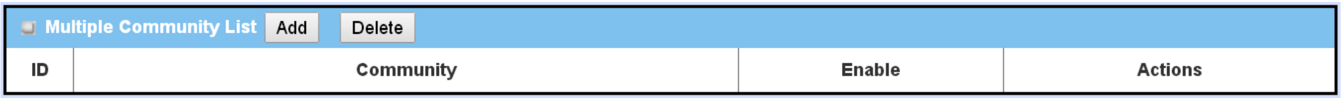
SNMP Item	Value setting	Description
SNMP Enable	1.The **LAN** box is checked by default	Select the interface for the SNMP and enable SNMP functions. When Check the **LAN** box. It will activate SNMP functions and you can access SNMP by LAN When Check the **WAN** box. It will activate SNMP functions and you can access SNMP by WAN
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 Aceess IP** for WAN. If you filled in the IP address. It means only this IP address can access SNMP by WAN. If you not filled. It means any IP address can access SNMP by WAN.
SNMP Port	1. String format: any	Specify the **SNMP Port**.

Index skipping is used to reserve slots for new function insertion, when required.

	port number 2. The default SNMP port is 161 3. A Must filled setting	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

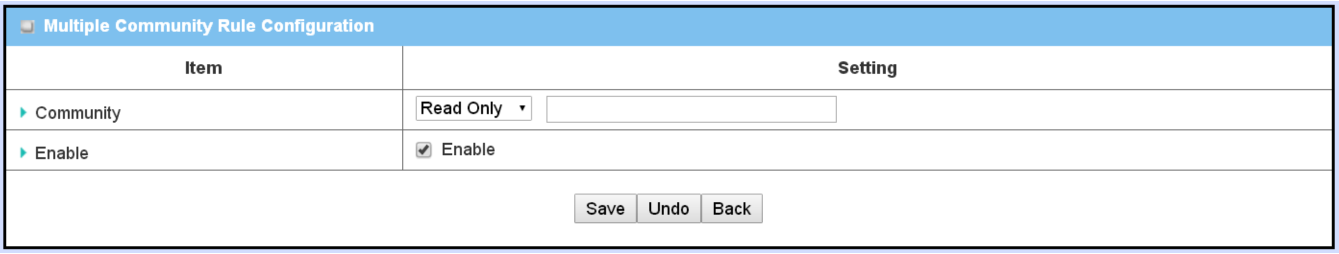
The SNMP allows you to custom your access control for version 1 and version 2 user. The router supports up to a maximum of 10 community sets.



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

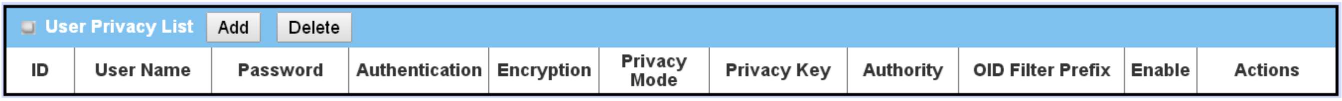
Item	Setting
Community	Read Only ▾
Enable	☑ Enable

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 Enable 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 Undo to cancel the settings.
Back	N/A	Click the Back button to return the last page.

Index skipping is used to reserve slots for new function insertion, when required.

Create/Edit User Privacy

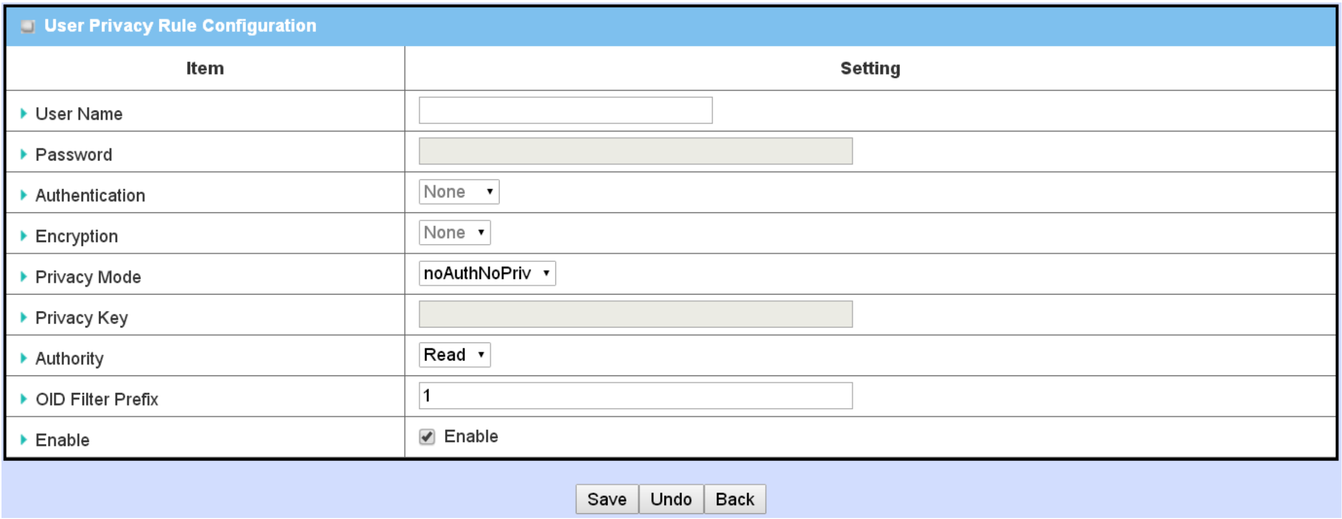
The SNMP allows you to custom your access control for version 3 user. The router supports up to a maximum of 128 User Privacy sets.



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

[Save] [Undo] [Back]

User Privacy Rule Configuration

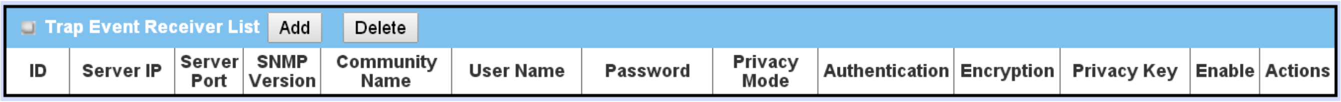
Item	Value setting	Description
User Name	1. A Must filled setting 2. String format: any text	Specify the **User Name** for this version 3 user. The maximum length of the user name is 32.
Password	1. String format: any text	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify 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**.

Index skipping is used to reserve slots for new function insertion, when required.

		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 subtree 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

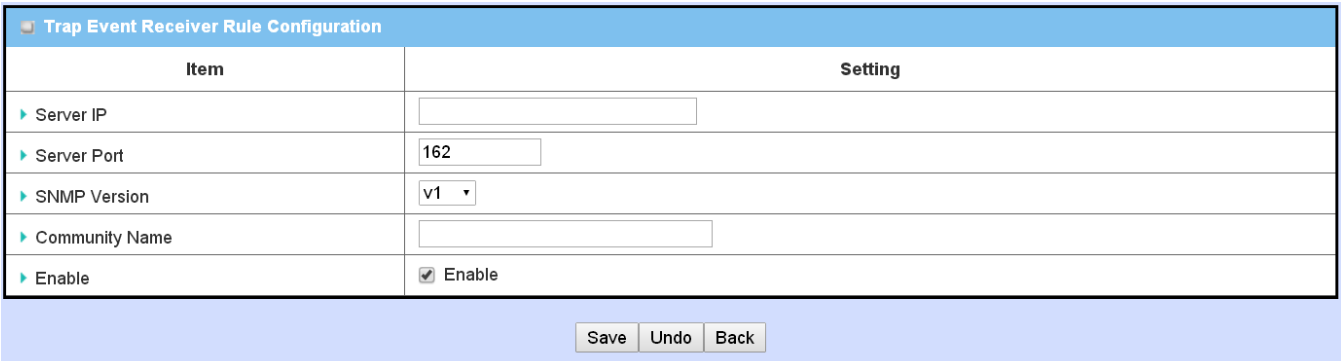
The SNMP allows you to custom your trap event receiver. The router supports up to a maximum of 4 Trap Event Receiver sets.



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.



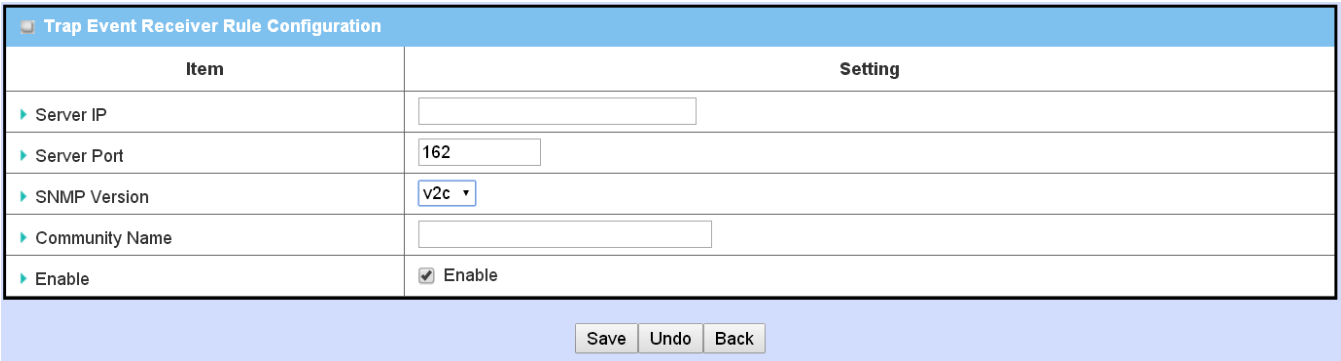
Trap Event Receiver Rule Configuration

Item	Setting
Server IP	
Server Port	162
SNMP Version	v1 ▾
Community Name	
Enable	☑ Enable

When you selected v2c. The configuration screen will provide the version 2c must filled items

Index skipping is used to reserve slots for new function insertion, when required.

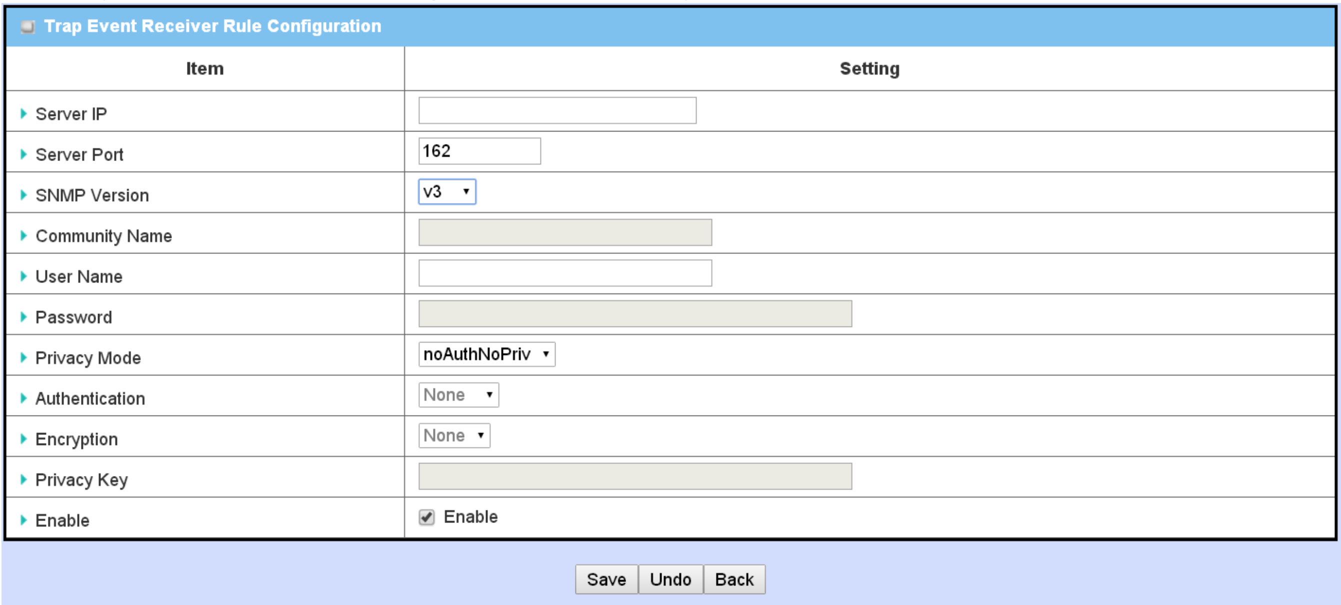
which is the same v1.



Trap Event Receiver Rule Configuration

Item	Setting
Server IP	
Server Port	162
SNMP Version	v2c ▾
Community Name	
Enable	☑ Enable

When you selected v3. The configuration screen will provide the version 3 must filled items



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

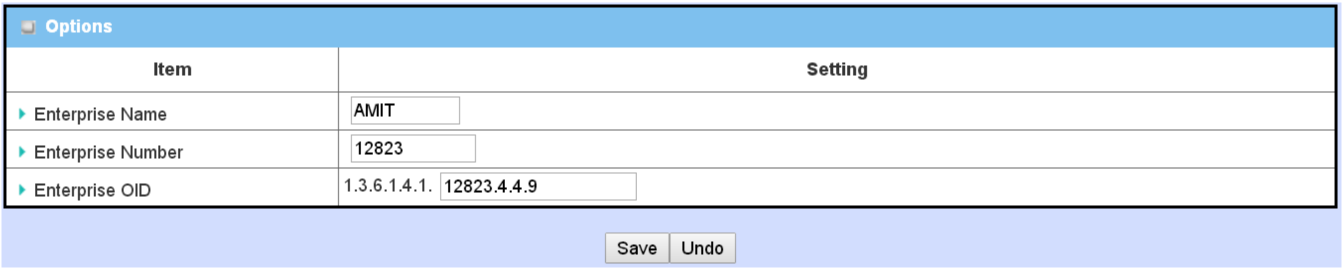
Trap Event Receiver Rule Configuration		
Item	**Value setting**	**Description**
Server IP	1. A Must filled setting 2. String format: any Ipv4 address	Specify the trap **Server IP**. The DUT will send trap to the server IP.
Server Port	1. String format: any port number 2. The default SNMP trap port is 162 3. A Must filled setting	Specify the trap **Server Port**. You can fill in any port number. But you must ensure the port number is not to be used.
SNMP Version	1. **v1** is selected by default	Select the version for the trap Selected the **v1**.

Index skipping is used to reserve slots for new function insertion, when required.

		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.

Edit Options

If you use some particular private mib, you must fill the enterprise name, number and OID.



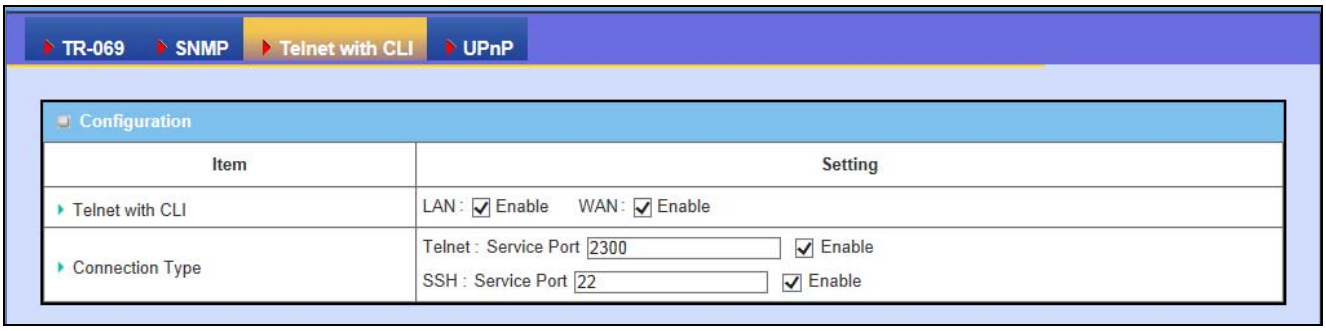
Options

Item	Setting
Enterprise Name	AMIT
Enterprise Number	12823
Enterprise OID	1.3.6.1.4.1. 12823.4.4.9

Options		
Item	**Value setting**	**Description**
Enterprise Name	1. The default value is AMIT 2. A Must filled setting 3. String format: any text	Specify the **Enterprise Name** for the particular private mib. The maximum length of the enterprise name is 10.
Enterprise Number	The default value is 12823 (AMIT Enterprise Number) 2. A Must filled setting 3. String format: any number	Specify the **Enterprise Number** for the particular private mib. The range of the enterprise number is 1-2080768.
Enterprise OID	1. The default value is 1.3.6.1.4.1.12823.4.4.9 (AMIT Enterprise OID) 2. A Must filled setting 3. String format: any legal OID	Specify the **Enterprise OID** for the particular private mib. The range of the each OID number is 1-2080768. The maximum length of the enterprise OID is 31. The seventh number must be identical with the enterprise number.
Save	N/A	Click the **Save** button to save the configuration and apply your changes to SNMP functions.
Undo	N/A	Click **Undo** to cancel the settings.

5.9.5 Telnet with CLI

A command-line interface (CLI), also known as command-line user interface, console user interface, and character user interface (CUI), 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 CLI with default service port 2300 and 22, respectively. And it also accepts commands from both LAN and WAN sides and makes corresponding responses.



Configuration

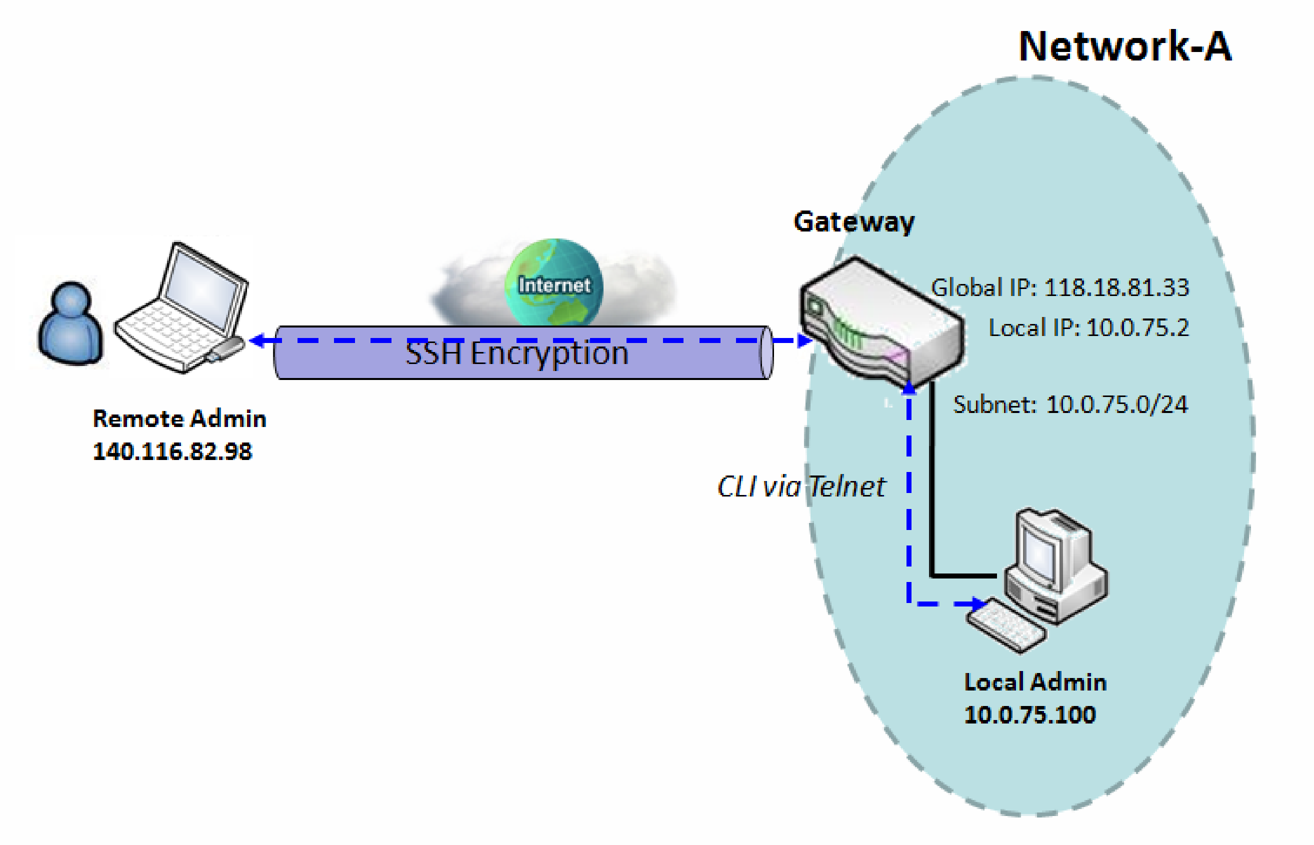
Item	Setting
Telnet with CLI	LAN : ☑ Enable WAN : ☑ Enable
Connection Type	Telnet : Service Port 2300 ☑ Enable SSH : Service Port 22 ☑ Enable

In "Telnet with CLI" page, there is only one configuration window for the "Telnet with CLI" function. The window can let you activate or deactivate the function to be made available for telnetting via LAN and WAN interfaces. You can also specify the connection type in plain text telnet or secured text ssh or both and their own service ports.

Telnet with CLI Configuration

Check the "Enable" box to activate the "Telnet with CLI" function for the LAN or WAN or both interfaces of the gateway. Choose either telnet or ssh or both for the connection type. Also change their service ports based on your requirement.

Telnet & SSH Scenario



Scenario Application Timing

When the manager 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 1 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.

Index skipping is used to reserve slots for new function insertion, when required.

Configuration Path	[Telnet with CLI]-[Configuration]
Telnet with CLI	LAN: ■ ***Enable*** WAN: ■ ***Enable***
Connection Type	Telnet: Service Port ***2300*** ■ ***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.

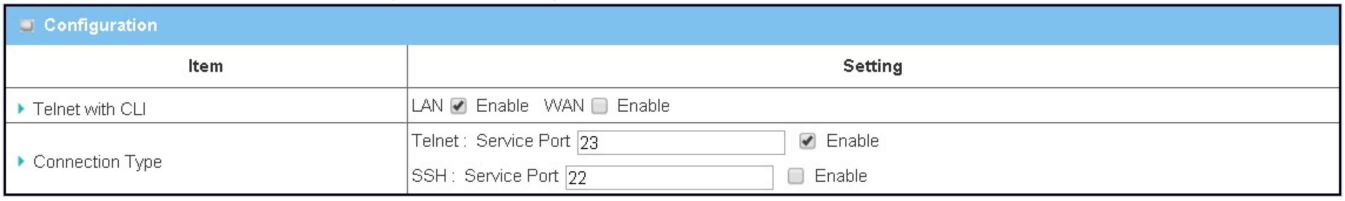
The "Local Admin" in the Intranet uses "Telnet" utility with privileged account (Usually, "root" and the same password as the one to login Web UI) to login the Gateway.

Or the "Remote Admin" in the Internet uses "SSH" utility with privileged account (Usually, "root" and the same password as the one to login Web UI) to login the Gateway.

The administrator of the gateway can control the device as like he is in front of the gateway.

The telnet with cli setting allows user to access DUT.

Go to Advanced Network > System Management > Telnet with CLI



Configuration

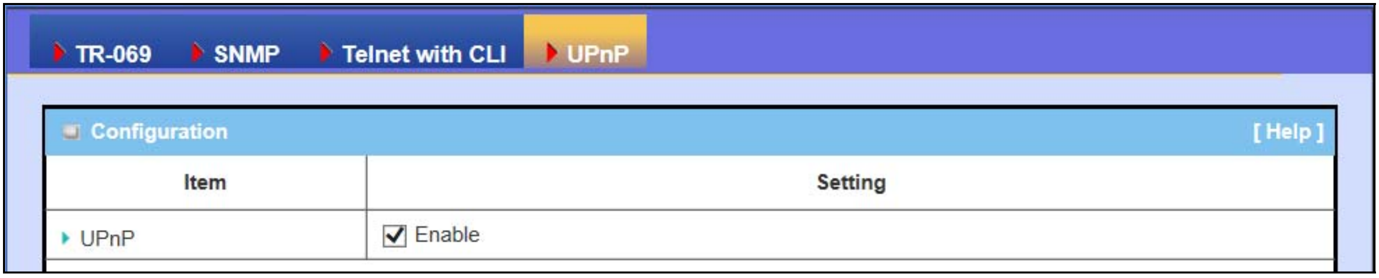
Item	Setting
Telnet with CLI	LAN ☑ Enable WAN □ Enable
Connection Type	Telnet : Service Port 23 ☑ Enable SSH : Service Port 22 □ Enable

Telnet with CLI		
Item Setting	**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 this WAN/LAN function
Connection Type	The Telnet Enable box is checked by default. By default **Service Port** is 23. The SSH Enable box is unchecked by default. By default **Service Port** is 22.	Check the Telnet **Enable** box to activate to activate telnet connect. Check the SSH **Enable** box to activate to activate telnet connect. You can set which number of **Service Port** you want to connect.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Index skipping is used to reserve slots for new function insertion, when required.

5.9.7 UPnP

UPnP Internet Gateway Device (IGD) Standardized Device Control Protocol is a NAT port mapping protocol and is supported by some NAT routers. It is a common communication protocol of automatically configuring port forwarding. Applications using peer-to-peer networks, multiplayer gaming, and remote assistance programs need a way to communicate through home and business gateways. Without IGD one has to manually configure the gateway to allow traffic through, a process which is error prone and time consuming. This device supports the UPnP Internet Gateway Device (IGD) feature, and by default, it is enabled.



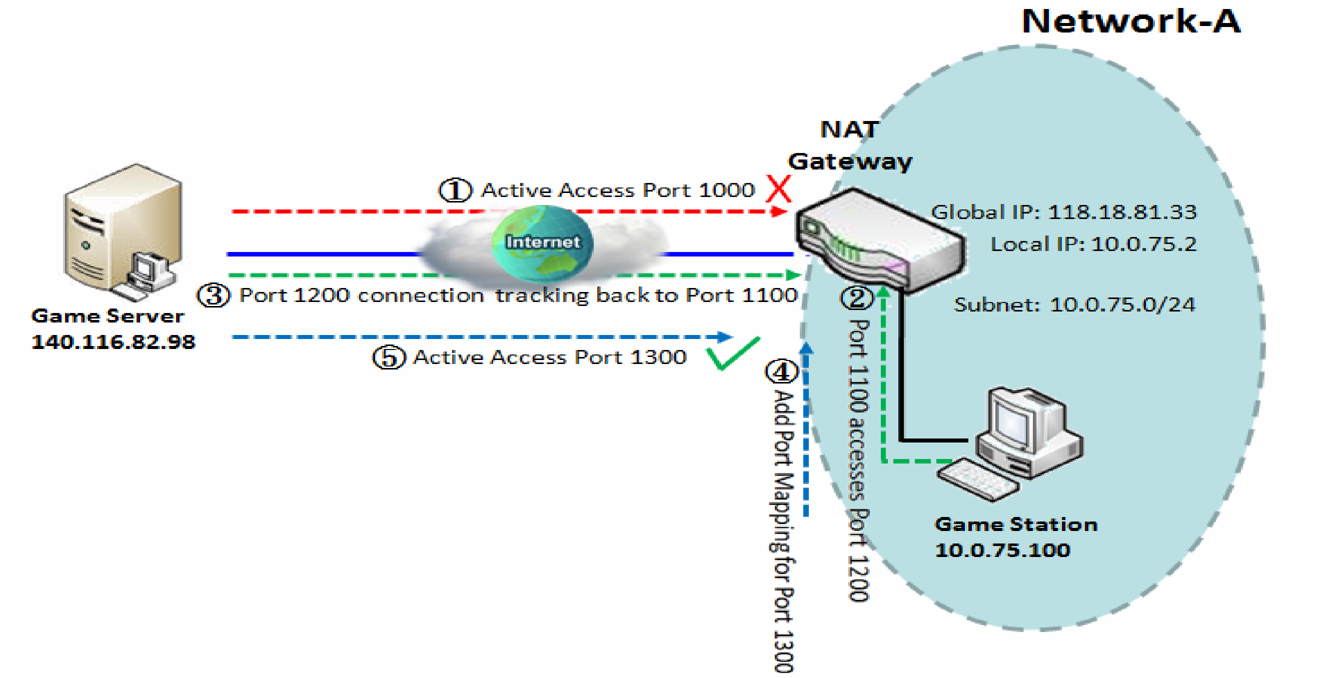
Item	Setting
UPnP	☑ Enable

In "UPnP" page, there is only one configuration window for the "UPnP" function available to you for function activation.

UPnP Configuration

Check the "Enable" box to activate the UPnP function.

UPnP Add Port Mapping Scenario


Network-A
NAT Gateway
Global IP: 118.18.81.33
Local IP: 10.0.75.2
Subnet: 10.0.75.0/24
① Active Access Port 1000 ✗
Internet
③ Port 1200 connection tracking back to Port 1100
⑤ Active Access Port 1300 ✓
② Port 1100 accesses Port 1200
④ Add Port Mapping for Port 1300
Game Server
140.116.82.98
Game Station
10.0.75.100

Scenario Application Timing

When one client host in the Intranet wants to run peer-to-peer applications, like multiplayer gaming, the NAT gateway needs the UPnP function to automatically setup or remove port mapping rules in the gateway.

Scenario Description

Usually, the active port service attempt to access the gateway from the Internet will be ignored by the gateway for security.

Normal NAT mechanism has the connection tracking feature to direct the response packets from the Internet back to the source end of request packets in the Intranet.

Once one application in the Intranet host needs an additional service port to be activated at the WAN interface of the gateway, it will ask the gateway to do that by using UPnP protocol. Then the Internet server can use the service port to contact the application for data communication.

Parameter Setup Example

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

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

Configuration Path	[UPnP]-[Configuration]
UPnP	■ ***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. It has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface.

There is one gaming station in the Intranet and a game server in the Internet. A gaming application is executed and data is communicated between the gaming station and server. The gaming application needs more service ports to be activated in the gateway, so that the gaming server can send data to the station actively via those service ports.

At first stage, the gaming server sends an active accessing for service port 1000 to the NAT Gateway, the gateway ignores it since the service port 1000 is deactivated at current stage.

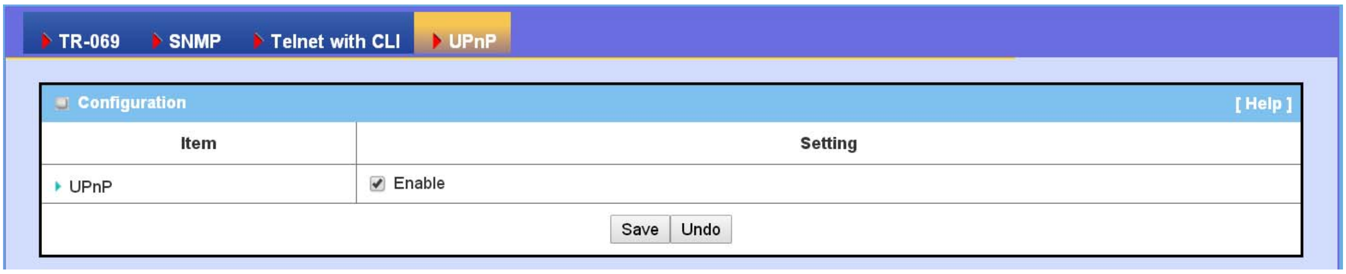
When the gaming has not be executed yet, the NAT mechanism in the gateway has its connection tracking feature to direct the response packets from the Internet back to the source end of request packets in the Intranet.

Once the gaming application in the Intranet host is executed and it needs an additional service port, like 1300, to be activated at the WAN interface of the gateway, it will ask the gateway to do that by using UPnP protocol.

Finally, the gaming server can use the service port to actively contact the application in the gaming station for data communication.

UPnP provides a set of networking protocols for networked devices to discover each other's presence and establish functional network services.

Go to Advanced Network > System Management > UPnP



Item	Setting
UPnP	☑ Enable

UPnP Configuration		
Item Name	**Value Setting**	**Description**
UPnP	Default checked	Check to enable UPnP functionality
Save	N/A	Click the **Save** button to save changes
Undo	N/A	Click the **Undo** button to revert changes

5.b 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[12].

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.

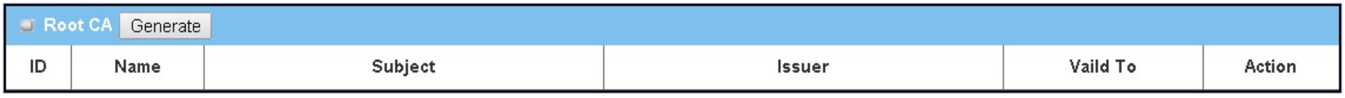
Certificates are an important component of Transport Layer Security (TLS, sometimes called by its older name SSL), where they prevent an attacker from impersonating a secure website or other server. They are also used in other important applications, such as email encryption and code signing. Here, it can be used in IPSec tunneling for user authentication.

5.b.1 Configuration

The configuration setting allows user to create Root Certificate Authority (CA) certificate and configure to set enable of SCEP.

Create root CA

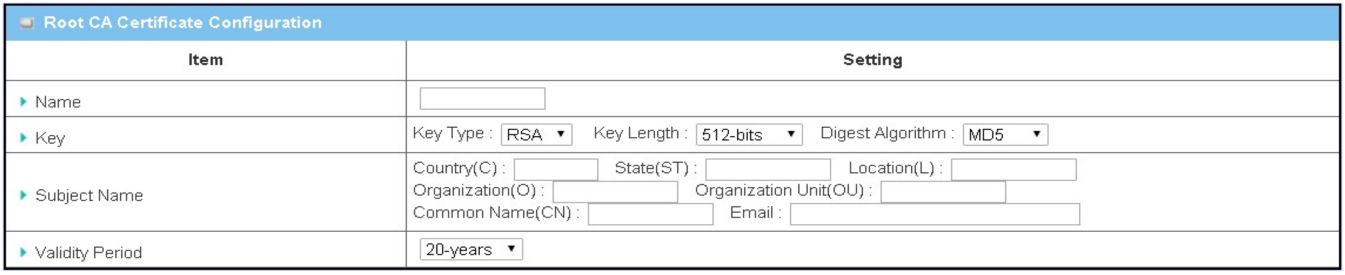
Go to Advanced Network > Certificate > Configuration



Root CA Generate

ID	Name	Subject	Issuer	Vaild To	Action

When Generate button is applied, Root CA Certificate Configuration screen will appear.



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 :

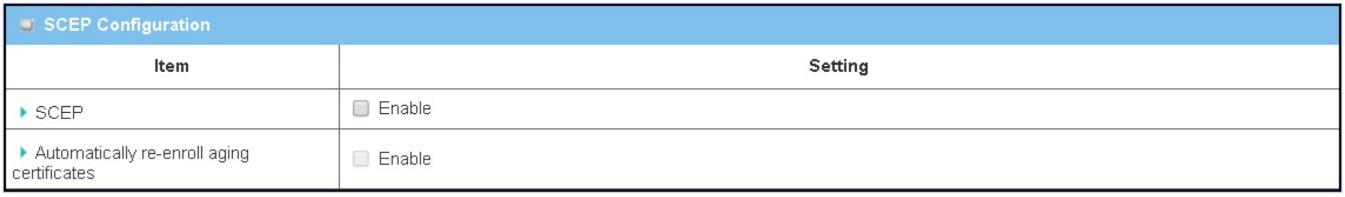
Validity Period	20-years

[12] Reference: http://en.wikipedia.org/wiki/Public_key_certificate.

Root CA Certificate Configuration		
Item	**Value setting**	**Description**
Name	1. String format can be any text 2. A Must filled setting	Enter a 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.

SCEP Configuration

Go to Advanced Network > Certificate > Configuration



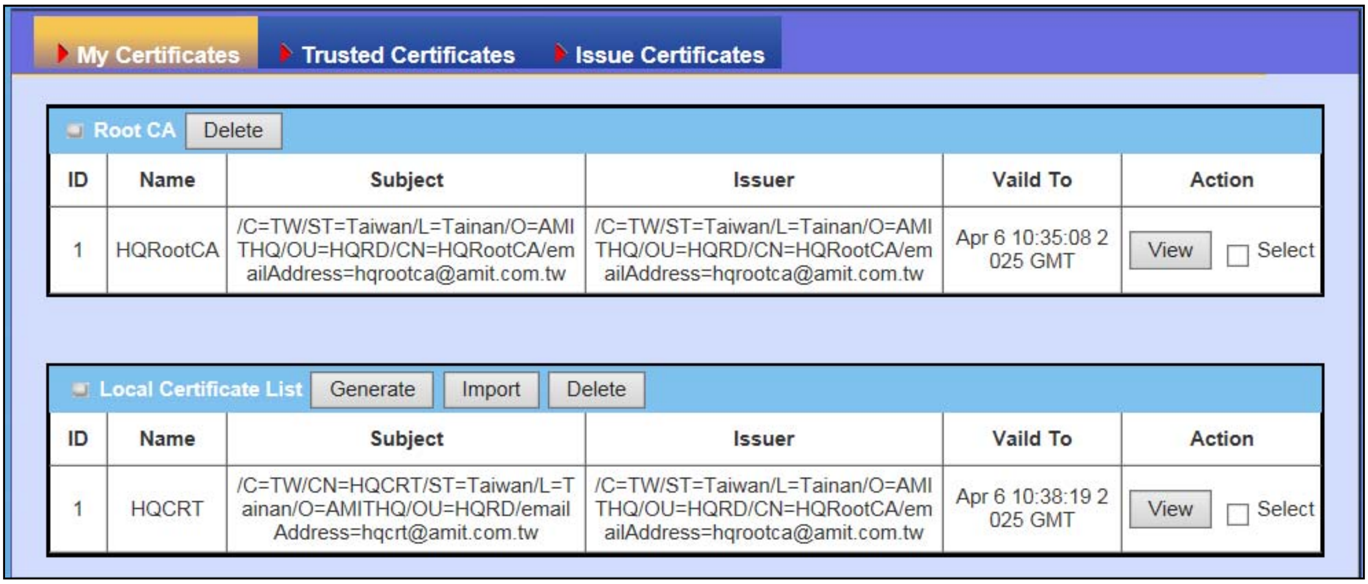
SCEP Configuration

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 Enable** is checked. 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.b.3 My Certificates

My Certificates include Root CA and Local Certificate List. Root CA is the top-most certificate of the tree, the private key of which is used to "sign" other certificates. 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.



ID	Name	Subject	Issuer	Vaild To	Action
1	HQRootCA	/C=TW/ST=Taiwan/L=Tainan/O=AMITHQ/OU=HQRD/CN=HQRootCA/emailAddress=hqrootca@amit.com.tw	/C=TW/ST=Taiwan/L=Tainan/O=AMITHQ/OU=HQRD/CN=HQRootCA/emailAddress=hqrootca@amit.com.tw	Apr 6 10:35:08 2025 GMT	View □ Select

ID	Name	Subject	Issuer	Vaild To	Action
1	HQCRT	/C=TW/CN=HQCRT/ST=Taiwan/L=Tainan/O=AMITHQ/OU=HQRD/emailAddress=hqcrt@amit.com.tw	/C=TW/ST=Taiwan/L=Tainan/O=AMITHQ/OU=HQRD/CN=HQRootCA/emailAddress=hqrootca@amit.com.tw	Apr 6 10:38:19 2025 GMT	View □ Select

In "My Certificates" page, there are four configuration windows for the "My Certificates" function. The "Root CA" window can let you generate or delete the certificate of root CA. "Root CA Configuration" window can let you fill required information necessary for generating the root CA. However, the "Local Certificate List" window shows the stored certificates or CSRs for representing the gateway. "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.

Root CA

Click on the "Generate" button and fill the required information for the Root CA certificate. There is only one Root CA certificate. Delete it by checking the Select box and clicking on the "Delete" button.

Root CA Configuration

The required information to be filled for the root CA includes the name, key, subject name and validity.

Index skipping is used to reserve slots for new function insertion, when required.

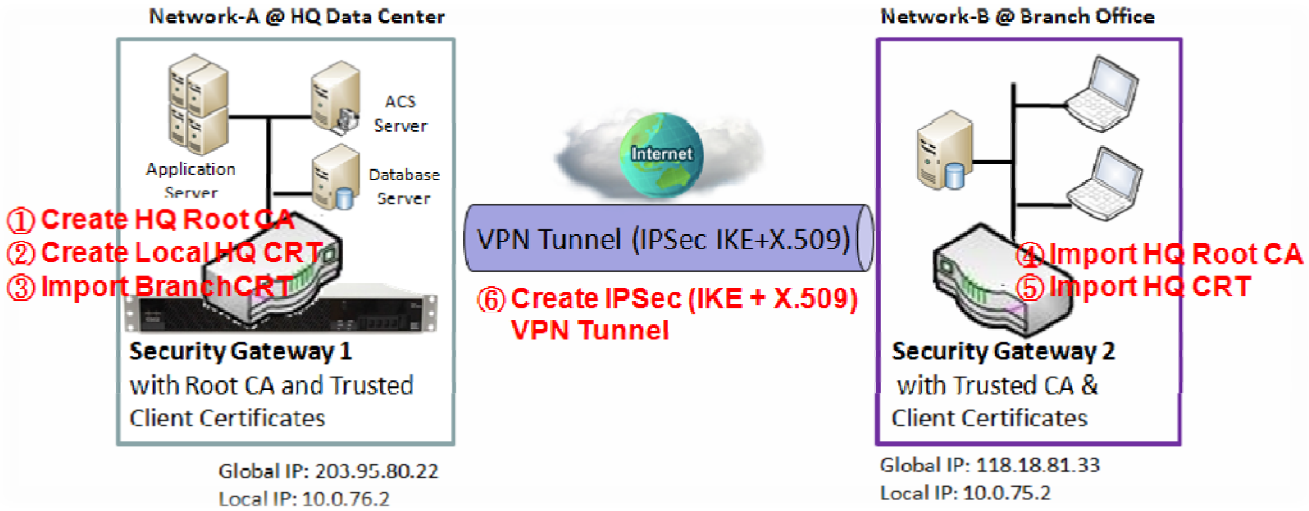
Local Certificate List

Click on the "Generate" button and fill the required information for one certificate of the gateway. There may be multiple certificates to be used for different applications to represent the gateway. You also can import certificates signed by other root CAs for the gateway. You may remove unused ones by checking the Select box of those certificates and clicking on the "Delete" button.

Local Certificate Configuration

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.

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 Certificates" 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 Certificates]-[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): ***AMITHQ*** Organization Unit(OU): ***HQRD*** Common Name(CN): ***HQRootCA*** E-mail: ***hqrootca@amit.com.tw***

Configuration Path	[My Certificates]-[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): ***AMITHQ*** Organization Unit(OU): ***HQRD*** Common Name(CN): ***HQCRT*** E-mail: ***hqcrt@amit.com.tw***

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

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

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

Remote Netmask	***255.255.255.0***
Remote Gateway	***118.18.81.33***

Configuration Path	[IPSec]-[Authentication]
Key Management	***IKE+X.509*** Local Certificate: ***HQCRT*** Remote Certificate: ***BranchCRT***
Local ID	***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 Certificates" 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 Certificates]-[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): ***AMITBranch*** Organization Unit(OU): ***BranchRD*** Common Name(CN): ***BranchCRT*** E-mail: ***branchcrt@amit.com.tw***

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

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

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

Remote Gateway	***203.95.80.22***

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

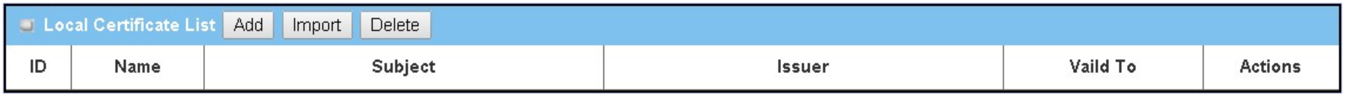
Finally, the client hosts in two subnets of 10.0.75.0/24 and 10.0.76.0/24 can communicate with each other.

Index skipping is used to reserve slots for new function insertion, when required.

The My Certificates setting allows user to create local certificate.

Create local certificate

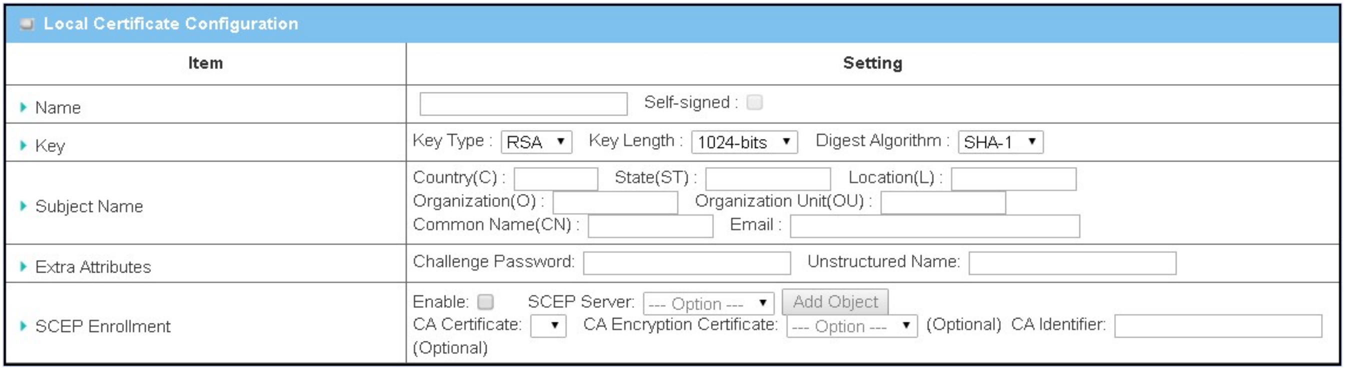
Go to Advanced Network > Certificate > My Certificates



Local Certificate List Add Import Delete

ID	Name	Subject	Issuer	Vaild To	Actions

When Add button is applied, Local Certificate Configuration screen will appear.



Local Certificate Configuration

Item	Setting
Name	Self-signed : □
Key	Key Type : RSA ▾ Key Length : 1024-bits ▾ Digest Algorithm : SHA-1 ▾

Subject Name	Country(C) : State(ST) : Location(L) :
	Organization(O) : Organization Unit(OU) :
	Common Name(CN) : Email :

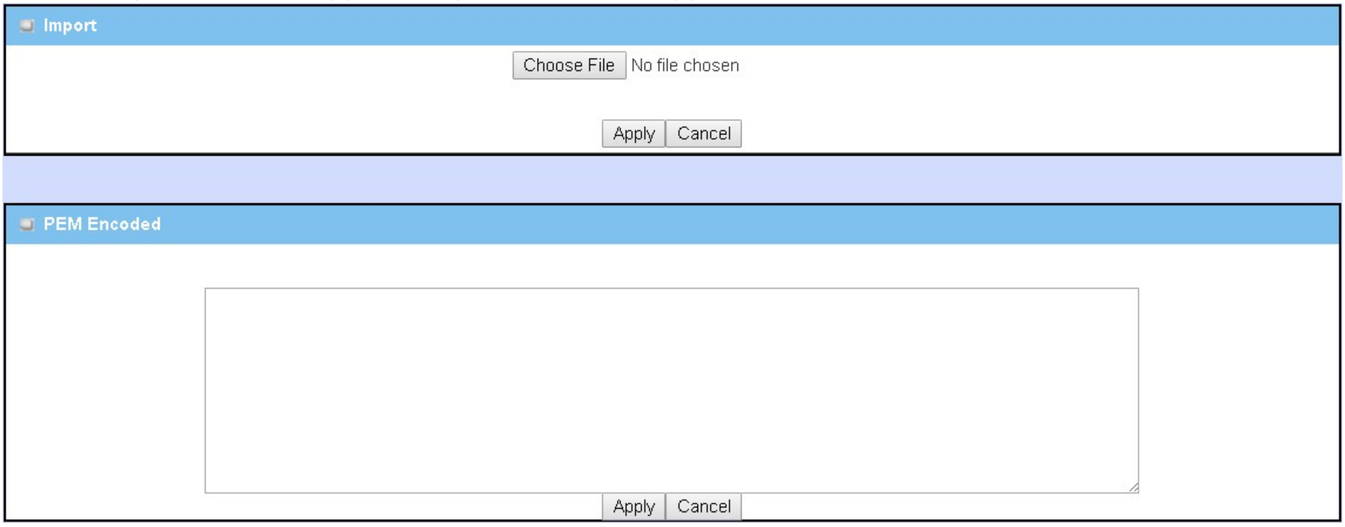
Extra Attributes	Challenge Password: Unstructured Name:
SCEP Enrollment	Enable: □ SCEP Server: --- Option --- ▾ Add Object CA Certificate: ▾ CA Encryption Certificate: --- Option --- ▾ (Optional) CA Identifier: (Optional)

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 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 setting only.
Extra Attributes	A Must filled setting	This field is to specify the extra information for generate certificate. **Challenge Password** which you can later use to request certificate revocation.

Index skipping is used to reserve slots for new function insertion, when required.

		Unstructured Name which field 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 **SCEP Server** to choice which scep server want to connect. It could be generated in External Server. Refer to **System** > **External Servers** > **External Servers**. You may click **Add Object** button to generate. Select **CA Certificate** to choice which certificate could be accepted by SCEP server for authentication. It could be generated in Trusted Certificates. Select **CA Encryption Certificate** to choice which certificate could be accepted by SCEP server for encryption data information. It could be generated in Trusted Certificates. **CA Identifier** is for SCEP server identifier which CA is used for signing certificates.

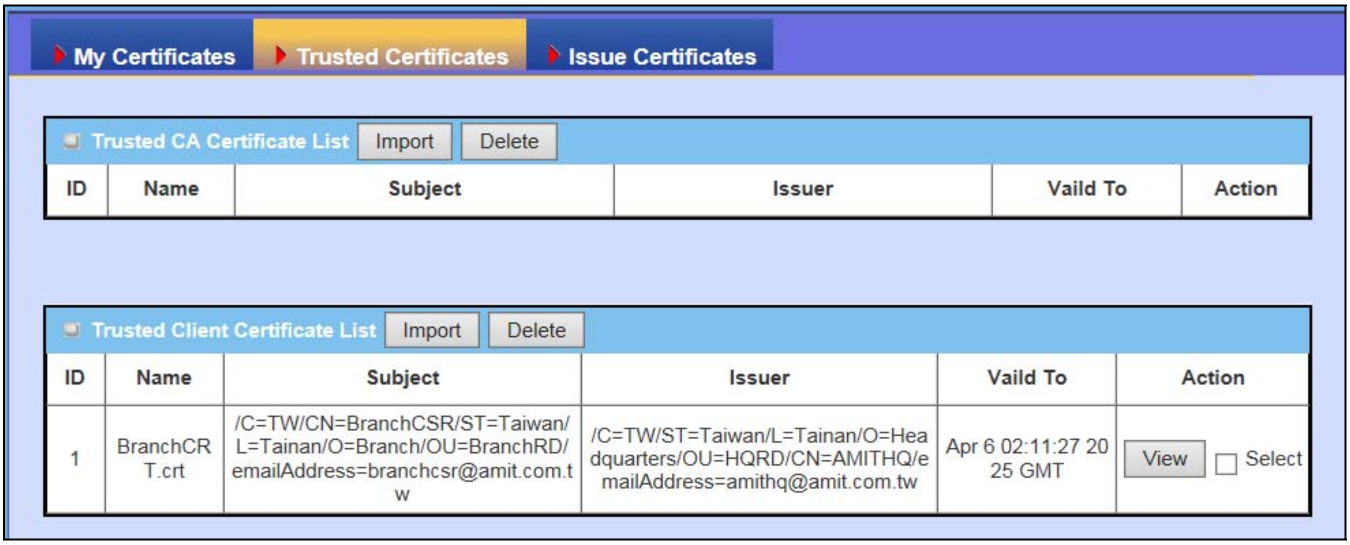
When Import button is applied, Import screen will appear.



Import		
Item	**Value setting**	**Description**
Import	A Must filled setting	It could select a certificate file from user's computer for importing to DUT.
PEM Encoded	1. String format can be any text 2. A Must filled setting	It could input the certificate pem encoded to DUT.
Apply	N/A	Click the **Apply** button to import certificate.
Cancel	N/A	When the **Cancel** button is clicked the screen will return to the My Certificates page.

5.b.5 Trusted Certificates

Trusted Certificates include Trusted CA Certificate List and Trusted Client Certificate List. The Trusted CA Certificate List places the certificates of external trusted CAs. However, the Trusted Client Certificate List places the others' certificates what you trust.



Trusted CA Certificate List Import Delete

ID	Name	Subject	Issuer	Vaild To	Action

Trusted Client Certificate List Import Delete

ID	Name	Subject	Issuer	Vaild To	Action
1	BranchCRT.crt	/C=TW/CN=BranchCSR/ST=Taiwan/L=Tainan/O=Branch/OU=BranchRD/emailAddress=branchcsr@amit.com.tw	/C=TW/ST=Taiwan/L=Tainan/O=Headquarters/OU=HQRD/CN=AMITHQ/emailAddress=amithq@amit.com.tw	Apr 6 02:11:27 2025 GMT	View □ Select

In "Trusted Certificates" page, there are six configuration windows for the "Trusted Certificates" function. The "Trusted CA Certificate List" window shows the stored certificates of trusted CAs. The "Trusted CA Certificate Import from a File" window can let you browse the file system of the management PC and select one CA certificate file to upload to the gateway for a trusted one. Another approach is the "Trusted CA Certificate Import from a PEM" window that can let you copy the contents of dedicated CA certificate and paste them in the window to be a trusted one for the gateway. Similarly, the "Trusted Client Certificate List" window, the "Trusted Client Certificate Import from a File" window and the "Trusted Client Certificate Import from a PEM" window play the same function as the ones for CA. Just substitute the CA Certificates with the Client Certificates.

Trusted CA Certificate List

Click on the "Import" button and select one CA certificate file of the management PC to upload as a trusted one. In addition, you can delete unused ones by checking the Select box of the certificates and clicking on the "Delete" button. The "View" button allows you to view the contents of the dedicated certificate and download them to the management PC by using the "Download" button.

Trusted CA Certificate Import from a File

Browse the directory and file system in the management PC to choose one CA certificate file for uploading to the gateway. Click on the "Apply" button to store it in the gateway to serve as one trusted CA certificate. Then it will be shown in the "Trusted CA Certificate List".

Trusted CA Certificate Import from a PEM

Copy the contents of one CA certificate in PEM format to this window and use "Apply" button to store it in the gateway to serve as one trusted CA certificate. It will appear in the "Trusted CA Certificate List".

Trusted Client Certificate List

Just click on the "Import" button and select one client certificate file of the management PC to upload as a trusted one. In addition, you can delete used ones by checking the Select box of those certificates and clicking on the "Delete" button. The "View" button allows you to view the contents of the dedicated certificate and download them to the management PC by using the "Download" button.

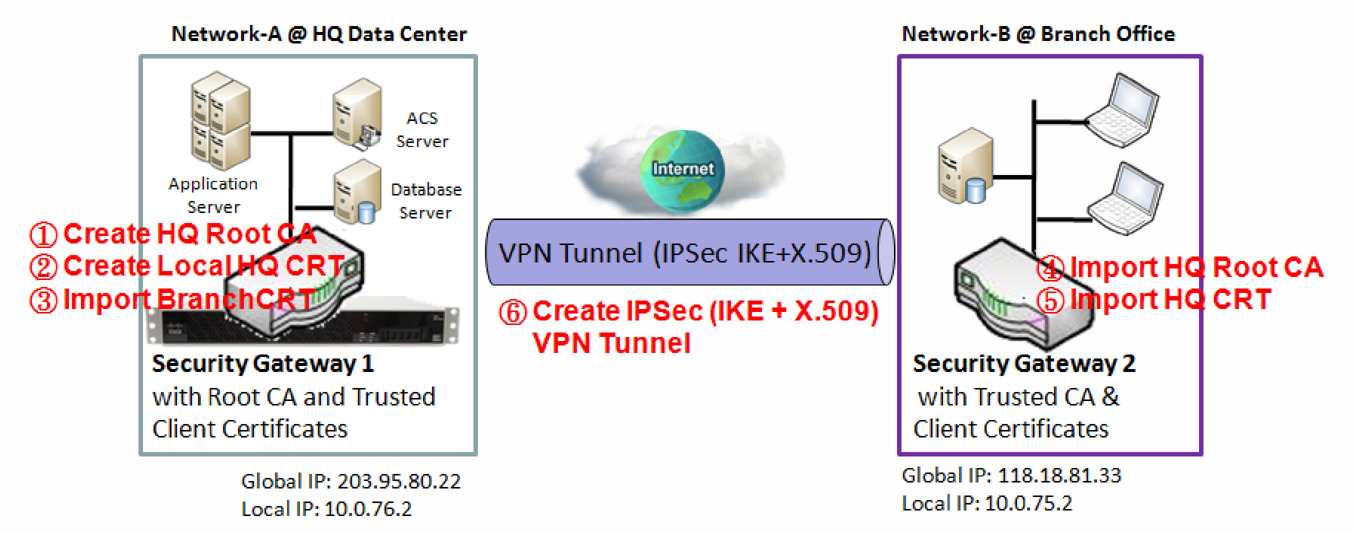
Trusted Client Certificate Import from a File

Browse the directory and file system in the management PC to choose one client certificate file for uploading to the gateway. Click on the "Apply" button to store it in the gateway to serve as one trusted client certificate. It will appear in the "Trusted Client Certificate List".

Trusted Client Certificate Import from a PEM

Copy the contents of one client certificate in PEM format to this window, and use "Apply" button to store it in the gateway to serve as one trusted client certificate. It will appear in the "Trusted Client Certificate List".

Self-signed Certificate Usage Scenario



Scenario Application Timing (same as the one described in "My Certificates" 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 Certificates" 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 Certificates" and "Issue Certificates" 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 Certificates" section)
For Network-A at HQ
Following tables list the parameter configuration as an example for the "Trusted Certificates" 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 Certificates" and "Issue Certificates" sections to complete the setup for the whole user scenario.

Configuration Path	[Trusted Certificates]-[Trusted Client Certificate List]
Command Button	***Import***

Configuration Path	[Trusted Certificates]-[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 Certificates" 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 Certificates" and "Issue Certificates" sections to complete the setup for the whole user scenario.

Configuration Path	[Trusted Certificates]-[Trusted CA Certificate List]
Command Button	***Import***

Configuration Path	[Trusted Certificates]-[Trusted CA Certificate Import from a File]
File	***HQRootCA.crt***

Index skipping is used to reserve slots for new function insertion, when required.

Configuration Path	[Trusted Certificates]-[Trusted Client Certificate List]
Command Button	*Import*

Configuration Path	[Trusted Certificates]-[Trusted Client Certificate Import from a File]
File	*HQCRT.crt*

Scenario Operation Procedure (same as the one described in "My Certificates" 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 Certificates" section of this manual.

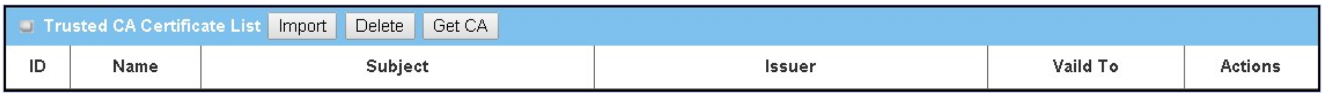
Gateway 2 can establish an IPSec VPN tunnel with "Site to Site" scenario and IKE and X.509 protocols to Gateway 1.

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

The Trusted Certificates setting allows user to import trusted certificate.

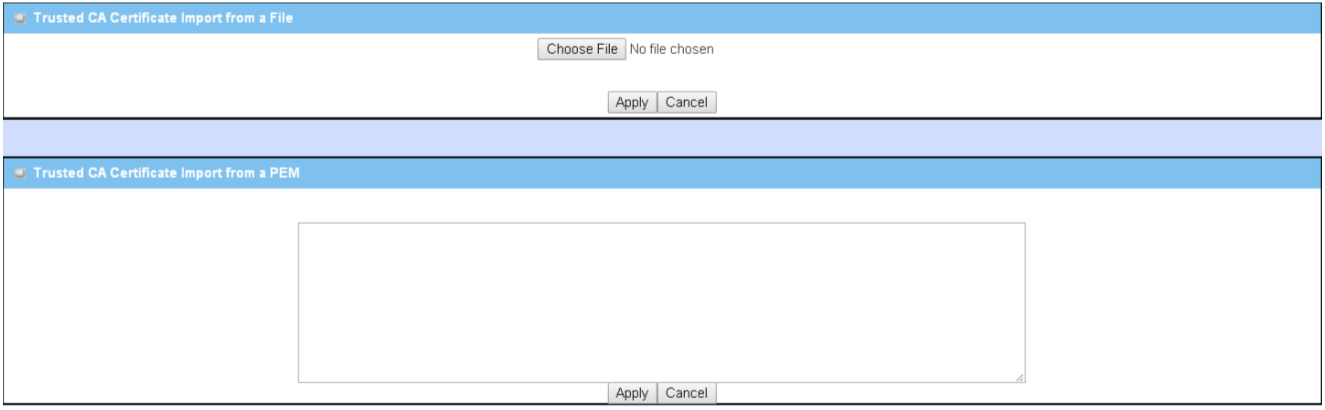
Trusted CA Certificate List

Go to Advanced Network > Certificate > Trusted Certificates



ID	Name	Subject	Issuer	Vaild To	Actions

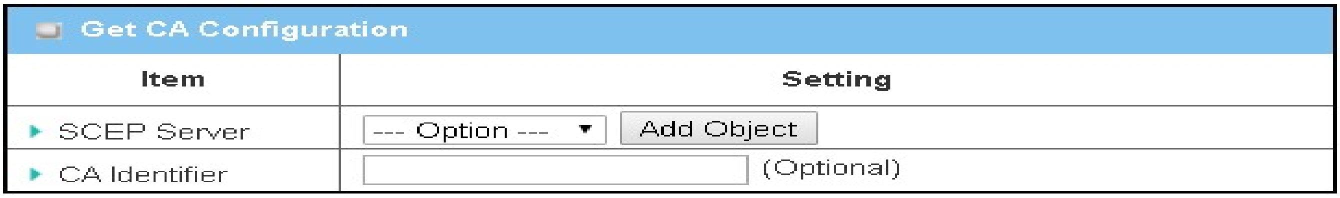
When Import button is applied, Trusted CA import screen will appear.


Trusted CA Certificate Import from a File
Choose File
No file chosen
Apply
Cancel
Trusted CA Certificate Import from a PEM
Apply
Cancel

Index skipping is used to reserve slots for new function insertion, when required.

Trusted Certificates		
Item	**Value setting**	**Description**
Import	A Must filled setting	It could select a CA certificate file from user's computer for importing to DUT.
PEM Encoded	1. String format can be any text 2. A Must filled setting	It could input the CA certificate pem encoded to DUT.
Apply	N/A	Click the **Apply** button to import certificate.
Cancel	N/A	When the **Cancel** button is clicked the screen will return to the Trusted Certificates page.

When Get CA button is applied, Trusted CA import screen will appear.
Ensure SCEP is enabled. Ref Go to Advanced Network > Certificate > Configuration



Get CA Configuration

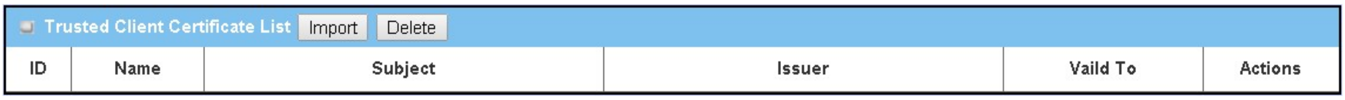
Item	Setting
SCEP Server	--- Option --- ▾ Add Object
CA Identifier	(Optional)

Get CA Configuration		
Item	**Value setting**	**Description**
SCEP Server	A Must filled setting	Select **SCEP Server** to choice which scep server want to connect. It could be generated in External Server. Refer to **System** > **External Servers** > **External Servers**. You may click **Add Object** button to generate.
CA Identifier	1. String format can be any text	**CA Identifier** is for SCEP server identifier which CA is used for signing certificates.
Save	N/A	Click **Save** to save the settings
Cancel	N/A	When the **Cancel** button is clicked the screen will return to the Trusted Certificates page.

Index skipping is used to reserve slots for new function insertion, when required.

Trusted Client Certificate List

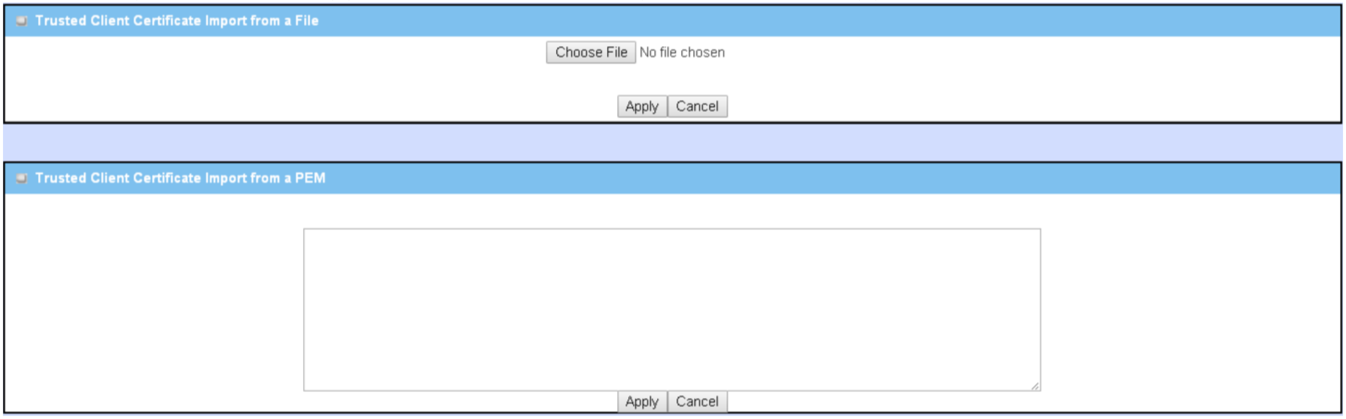
Go to Advanced Network > Certificate > Trusted Certificates



Trusted Client Certificate List

ID	Name	Subject	Issuer	Vaild To	Actions

When Import button is applied, Trusted Client import screen will appear.



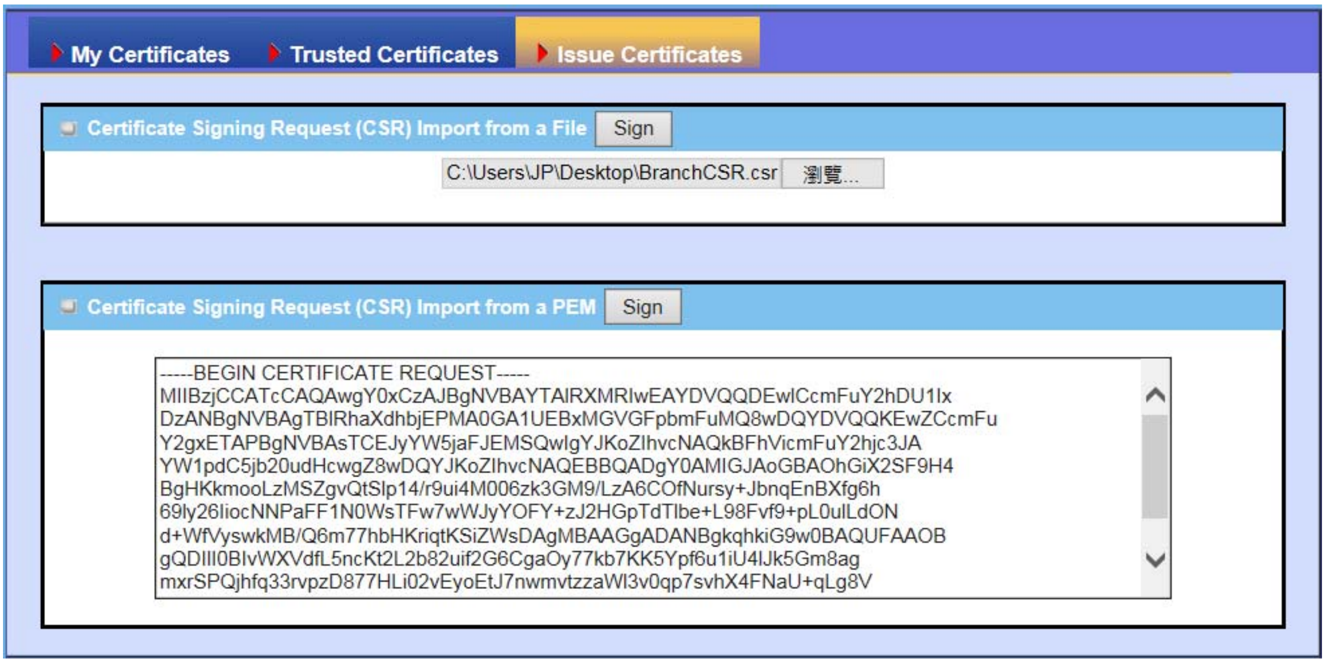
Trusted Client Certificate Import from a File

Trusted Client Certificate Import from a PEM

Trusted Client Certificate List		
Item	**Value setting**	**Description**
Import	A Must filled setting	It could select a certificate file from user's computer for importing to DUT.
PEM Encoded	1. String format can be any text 2. A Must filled setting	It could input the certificate pem encoded to DUT.
Apply	N/A	Click the **Apply** button to import certificate.
Cancel	N/A	When the **Cancel** button is clicked the screen will return to the Trusted Certificates page.

5.b.7 Issue Certificates

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.


My Certificates
Trusted Certificates
Issue Certificates
Certificate Signing Request (CSR) Import from a File
Sign
瀏覽...
Certificate Signing Request (CSR) Import from a PEM
Sign

C:\Users\JP\Desktop\BranchCSR.csr

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBzjCCATcCAQAwgY0xCzAJBgNVBAYTAlRXMRIwEAYDVQQDEwlCcmFuY2hDU1Ix
DzANBgNVBAgTBlRhaXdhbjEPMA0GA1UEBxMGVGFpbmFuMQ8wDQYDVQQKEwZCcmFu
Y2gxETAPBgNVBAsTCEJyYW5jaFJEMSQwIgYJKoZIhvcNAQkBFhVicmFuY2hjc3JA
YW1pdC5jb20udHcwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOhGiX2SF9H4
BgHKkmooLzMSZgvQtSlp14/r9ui4M006zk3GM9/LzA6COfNursy+JbnqEnBXfg6h
69ly26liocNNPaFF1N0WsTFw7wWJyYOFY+zJ2HGpTdTlbe+L98Fvf9+pL0ulLdON
d+WfVyswkMB/Q6m77hbHKriqtKSiZWsDAgMBAAGgADANBgkqhkiG9w0BAQUFAAOB
gQDIlI0BIvWXVdfL5ncKt2L2b82uif2G6CgaOy77kb7KK5Ypf6u1iU4lJk5Gm8ag
mxrSPQjhfq33rvpzD877HLi02vEyoEtJ7nwmvtzzaWl3v0qp7svhX4FNaU+qLg8V
```

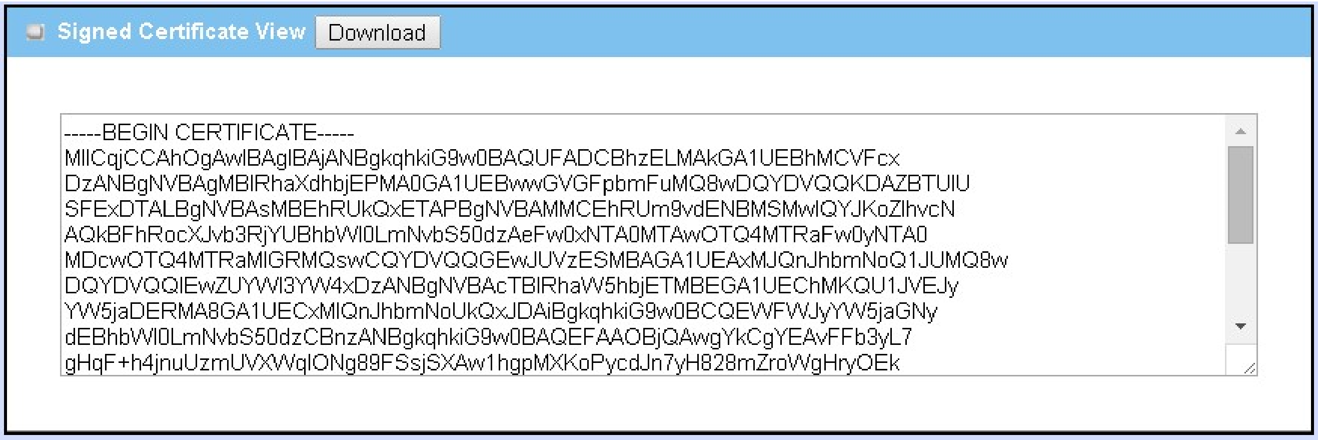
In "Issue Certificates" page, there are three configuration windows for the "Issue Certificates" function. The "Certificate Signing Request (CSR) Import from a File" window let you browse the directories and file list of the managing PC to choose a CSR file and import it as the certificate signing request. The gateway will generates the certificate based on the dedicated CSR by clicking on the "Sign" button in the window. Certainly, only the gateway be the root CA and it can sign the requests to certify. Another approach to import a CSR to the gateway for signing is to copy the PEM-formatted CSR contents and paste them directly into the blank space in the "Certificate Signing Request (CSR) Import from a PEM" window. The gateway will generates the certificate based on the pasted CSR contents by clicking on the "Sign" button. A successful signing will show the "Signed Certificate View" window to display the resulted certificate contents. And you can download the certification to a file in the managing PC.

Certificate Signing Request (CSR) Import from a File

Only the gateway plays the root CA role can sign CSRs and certify certificates for others. In this window, you can browse the directory architecture and file system in the managing PC to choose one CSR file for uploading unsigned certificates to the gateway. Click on the "Sign" button to generate corresponding certificate based on the imported CSR. The "Signed Certificate View" window will display the resulted certificate contents, and you can download the certification to a file in the managing PC by clicking on the "Download" button. The default name of the saved certification file is "issued.crt". You need to change to a preferred file name.

Certificate Signing Request (CSR) Import from a PEM

Copy the contents of one CSR in PEM format to this window, and use "Sign" button to generate corresponding certificate based on the pasted CSR contents. The "Signed Certificate View" window will display the resulted certificate contents, and you can download the certification to a file in the managing PC by clicking on the "Download" button. The default name of the saved certification file is "issued.crt". You need to change to a preferred file name.



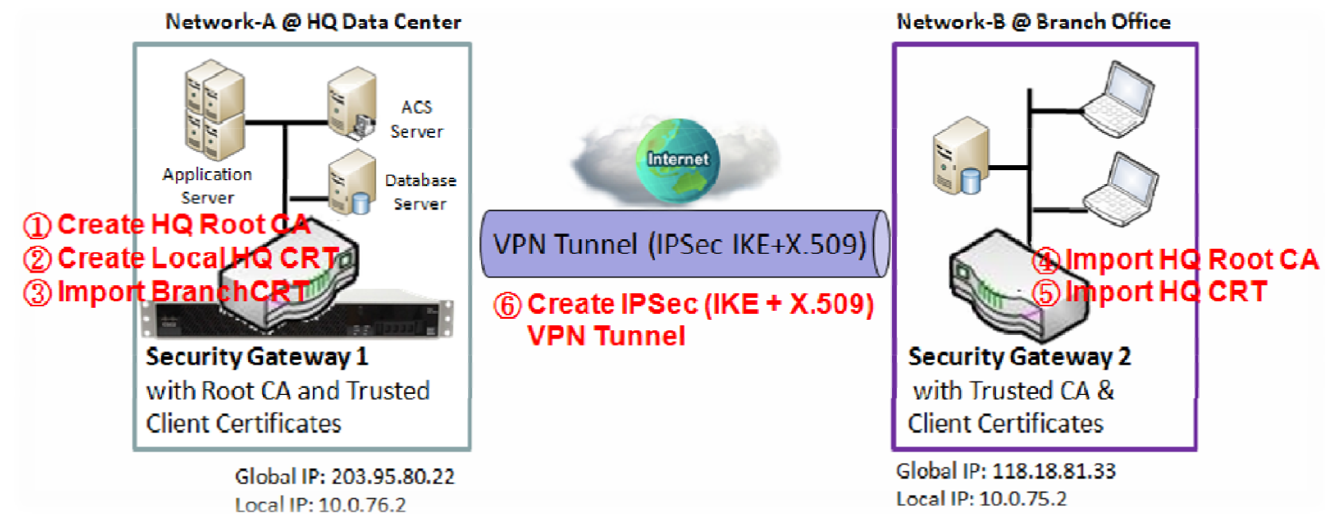
```
-----BEGIN CERTIFICATE-----
MIICqjCCAhOgAwIBAgIBAjANBgkqhkiG9w0BAQUFADCBhzELMAkGA1UEBhMCVFcx
DzANBgNVBAgMBlRhaXdhbjEPMA0GA1UEBwwGVGFpbmFuMQ8wDQYDVQQKDAZBTUlU
SFExDTALBgNVBAsMBEhRUkQxETAPBgNVBAMMCEhRUm9vdENBMSMwIQYJKoZIhvcN
AQkBFhRocXJvb3RjYUBhbWl0LmNvbS50dzAeFw0xNTA0MTAwOTQ4MTRaFw0yNTA0
MDcwOTQ4MTRaMIGRMQswCQYDVQQGEwJUVzESMBAGA1UEAxMJQnJhbmNoQ1JUMQ8w
DQYDVQQIEwZUYWl3YW4xDzANBgNVBAcTBlRhaW5hbjETMBEGA1UEChMKQU1JVEJy
YW5jaDERMA8GA1UECxMIQnJhbmNoUkQxJDAiBgkqhkiG9w0BCQEWFWJyYW5jaGNy
dEBhbWl0LmNvbS50dzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAvFFb3yL7
gHqF+h4jnuUzmUVXWqlONg89FSsjSXAw1hgpMXKoPycdJn7yH828mZroWgHryOEk
```

Singed Certificate View

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.

Index skipping is used to reserve slots for new function insertion, when required.

Self-signed Certificate Usage Scenario



Scenario Application Timing (same as the one described in "My Certificates" 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 Certificates" 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 Certificates" and "Trusted Certificates" 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 Certificates" section)
For Network-A at HQ
Following tables list the parameter configuration as an example for the "Issue Certificates" 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 Certificates" and "Trusted Certificates" sections to complete the setup for whole user scenario.

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

Configuration Path	[Issue Certificates]-[Signed Certificate View]
Command Button	***Download*** (default name is "issued.crt")

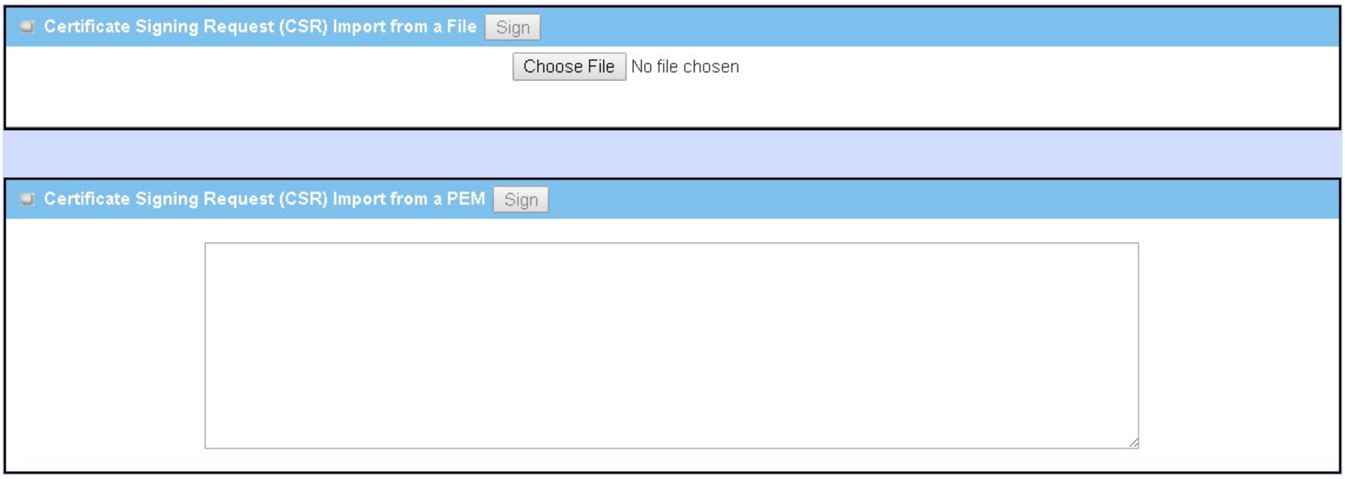
Scenario Operation Procedure (same as the one described in "My Certificates" section)
In above diagram, the "Gateway 1" is the gateway of Network-A in headquarters and the subnet of its Intranet is 10.0.76.0/24. It has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN-1 interface. 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.

The Issued Certificates setting allows user to import Certificate Signing Request (CSR) to be signed by root CA.

Index skipping is used to reserve slots for new function insertion, when required.

Issued Certificate

Go to Advanced Network > Certificate > Issued Certificates


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	It could select a certificate signing request file from user's computer for importing to DUT.
Certificate Signing Request (CSR) Import from a PEM	1. String format can be any text 2. A Must filled setting	It could input the certificate signing request pem encoded to DUT.
Sign	N/A	When root CA is exist, click the **Sign** button to be signed by root CA

Chapter 7 Applications

7.1 Mobile Application

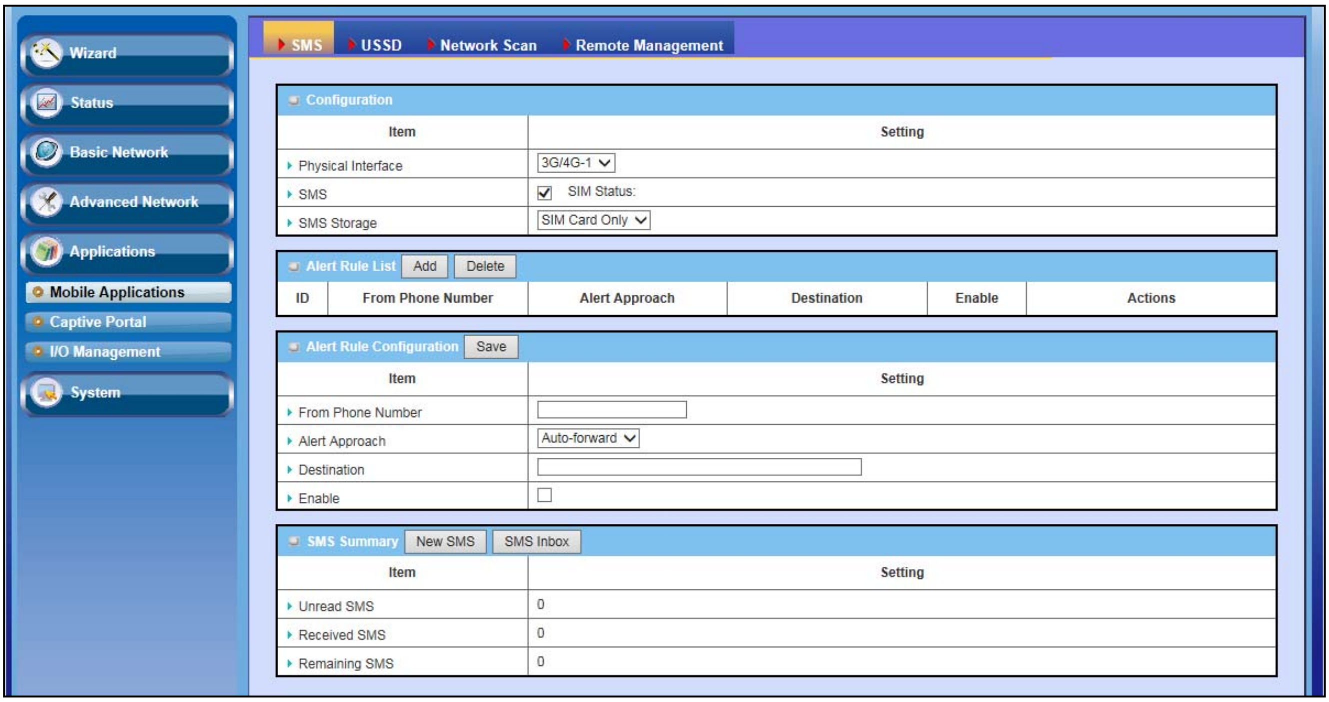
Whether there is the mobile application existed in your purchased gateway depends on its product category. In Mobile Application section, the device supports SMS Management, USSD Management, Network Scan and SMS-based Remote Management. You can setup these four aspects of mobile applications by using embedded 3G/LTE module in the device.

7.1.1 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. [13]

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.[1]

Index skipping is used to reserve slots for new function insertion, when required.



Configuration

Item	Setting
Physical Interface	3G/4G-1
SMS	☑ SIM Status:
SMS Storage	SIM Card Only

Alert Rule List [Add] [Delete]

ID	From Phone Number	Alert Approach	Destination	Enable	Actions

Alert Rule Configuration [Save]

Item	Setting
From Phone Number	
Alert Approach	Auto-forward
Destination	
Enable	□

SMS Summary [New SMS] [SMS Inbox]

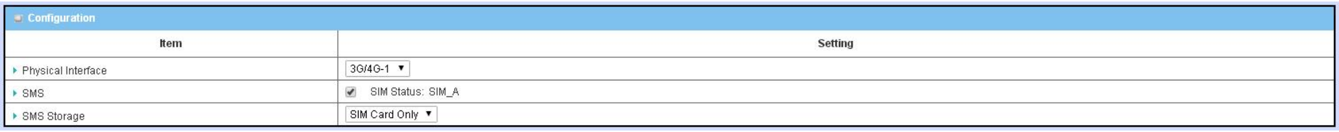
Item	Setting
Unread SMS	0
Received SMS	0
Remaining SMS	0

In "SMS" page, there are four windows for the SMS function. The "Configuration" window can let you specify which 3G/4G module (physical interface) is used for the SMS function, and system will show which SIM card in the module is the current used one. In addition, the supported media to store SMS messages in the gateway now has only "SIM Card Only" option. The second window is the "Alter Rule List" and it shows all your defined altering rules for SMS messages, like auto-forwarding messages to another mobile phone set, message forwarding by email and message forwarding by syslog. By using the third window, "Alter Rule Configuration", you can define an altering rule for SMS messages. At last, the "SMS Summary" window displays information such as the numbers of unread SMS messages, total received SMS messages and SMS messages in free space. Moreover, a "New SMS" button can let you compose and send a new SMS message. The "SMS Inbox" button can let you check all received SMS messages.

The SMS function allow user to send SMS, read and delete SMS from SIM Card.

Configuration setting

Go to **Application** > **Mobile Application** > **SMS**



Configuration

Item	Setting
Physical Interface	3G/4G-1 ▼
SMS	☑ SIM Status: SIM_A
SMS Storage	SIM Card Only ▼

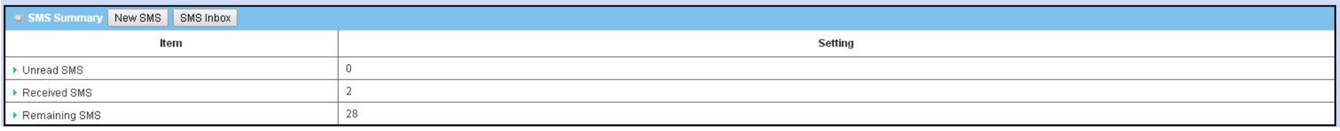
Configuration		
Item	**Value setting**	**Description**
Physical Interface	The box is 3G/4G-1 by default	Choose the **3G/4G-1** or **3G/4G-2** to change setting of cellular module1 or cellular module2.

Index skipping is used to reserve slots for new function insertion, when required.

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

SMS Summary

Show **Unread SMS**, **Received SMS**, **Remaining SMS**, and edit SMS context to send, read SMS from SIM card.

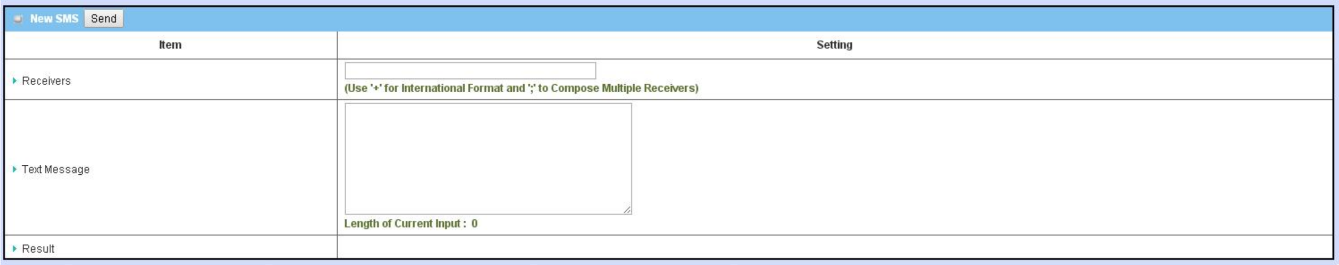


Item	Setting
Unread SMS	0
Received SMS	2
Remaining SMS	28

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

User can set the SMS setting from this screen.



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

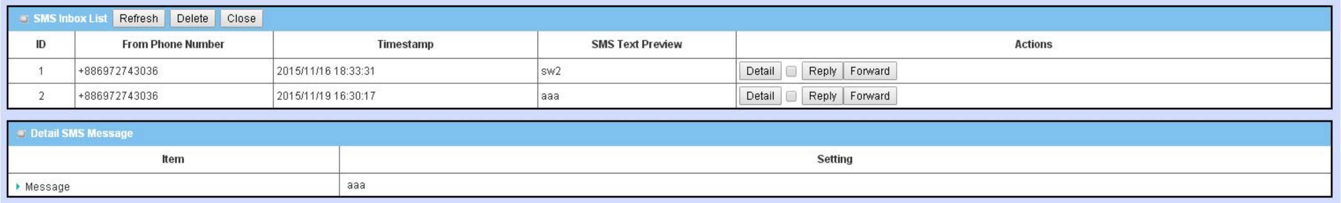
New SMS		
Item	**Value setting**	**Description**
Receivers	N/A	Write the receivers to send SMS. User need to add the semicolon and compose multiple receivers that can group send SMS.

Index skipping is used to reserve slots for new function insertion, when required.

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**. If send SMS fail, **Result** will show **Send Failed**.
Send	N/A	Click **Send** button, SMS will send.

SMS Inbox List

User can read or delete SMS, reply SMS or forward SMS from this screen.



ID	From Phone Number	Timestamp	SMS Text Preview	Actions
1	+886972743036	2015/11/16 18:33:31	sw2	Detail □ Reply Forward
2	+886972743036	2015/11/19 16:30:17	aaa	Detail □ Reply Forward

Detail SMS Message

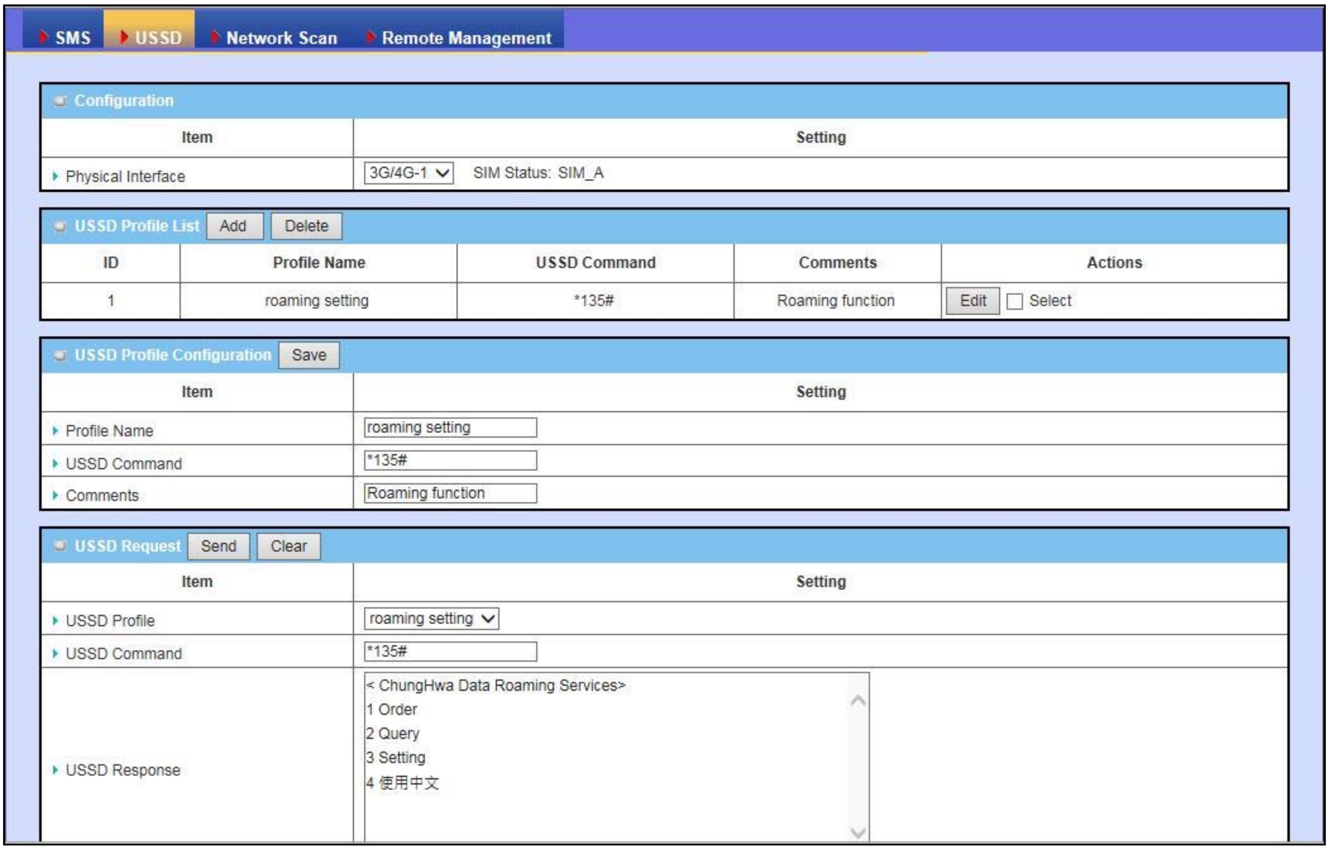
Item	Setting
Message	aaa

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.
Action	The box is unchecked by default	User can check the box, then click **Delete** button to delete SMS. User click Reply/Forward button to reply/forward SMS. User click Detail button to read the SMS detail, and Detail SMS Message screen appears.
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.

7.1.3 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. [14]

An USSD messageis 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.[1]



Configuration

Item	Setting
Physical Interface	3G/4G-1 SIM Status: SIM_A

USSD Profile List Add Delete

ID	Profile Name	USSD Command	Comments	Actions
1	roaming setting	*135#	Roaming function	Edit □ Select

USSD Profile Configuration Save

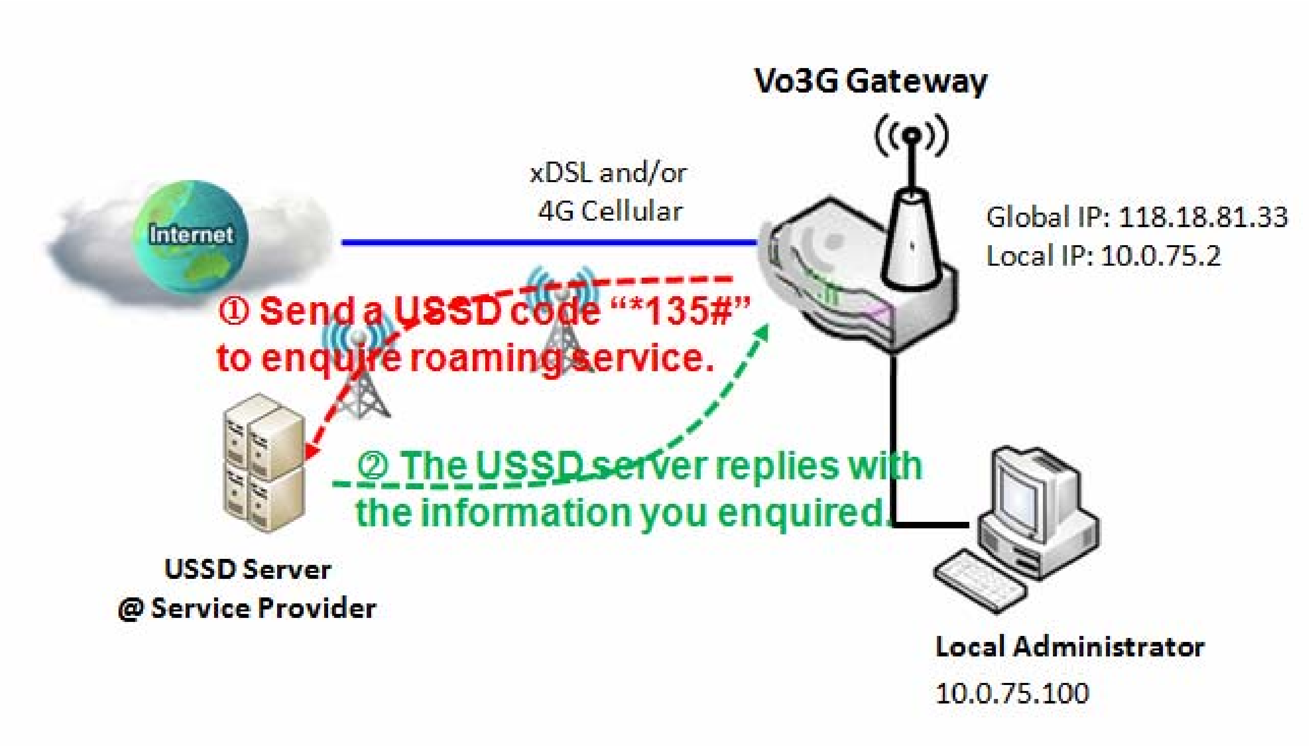
Item	Setting
Profile Name	roaming setting
USSD Command	*135#
Comments	Roaming function

USSD Request Send Clear

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 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 voice 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

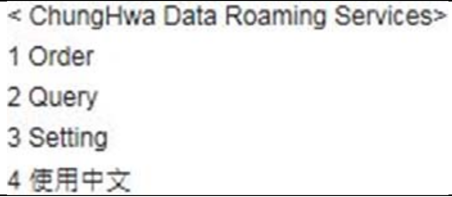
Following tables list the parameter configuration as an example for "USSD" function, as shown in above diagram.

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

Index skipping is used to reserve slots for new function insertion, when required.

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.

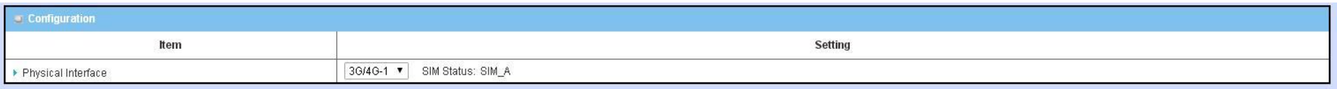
First, administrator selects one 3G/4G module as the physical interface of the USSD session. And then, he defines an USSD profile named as "roaming setting" with command "*135#" for further use.

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 recevied 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 avaliable services from ISP via USSD sessions.

The USSD function allow user to send USSD to ISP, then ISP will provide some service for user.

Configuration setting

Go to Application > Mobile Application > USSD



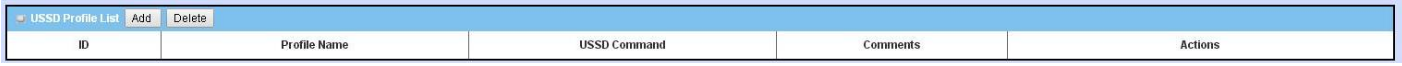
Configuration

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 the **3G/4G-1** or **3G/4G-2** to change setting of cellular module1 or cellular module2.
SIM Status	N/A	Depend on currently SIM status.

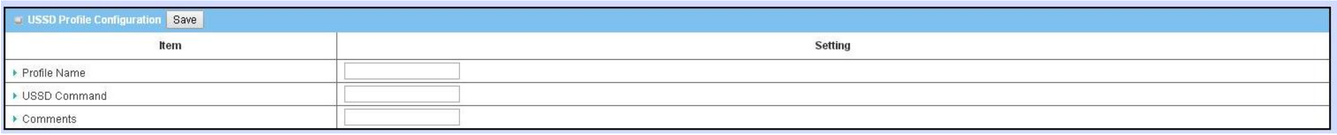
USSD Profile List setting

The USSD allows you to custom your profile. The router supports up to a maximum of 35 USSD profile list.



ID	Profile Name	USSD Command	Comments	Actions

When Add button is applied USSD Profile List Configuration screen will appear.



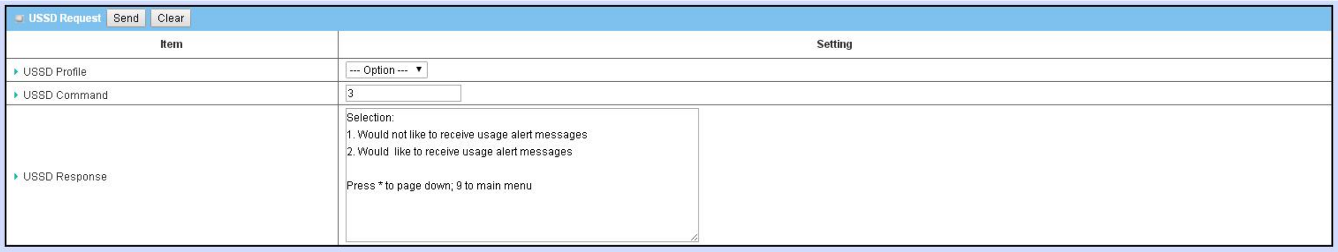
Item	Setting
Profile Name	
USSD Command	
Comments	

USSD Profile List		
Item	**Value setting**	**Description**
Profile Name	N/A	The **Profile Name** that user can key in.
USSD Command	N/A	The **USSD command** that user can key in.
Comments	N/A	The **Comments** is this profile comment.

USSD Request

When send the USSD command, the USSD Response screen will appear.

When click the Clear button, the USSD Response will disappear.



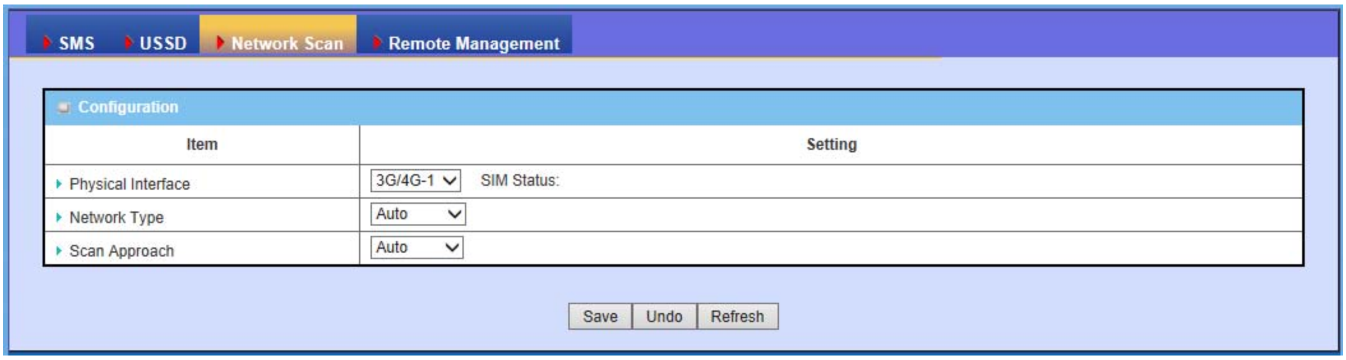
Item	Setting
USSD Profile	--- Option ---
USSD Command	3
USSD Response	Selection: 1. Would not like to receive usage alert messages 2. Would like to receive usage alert messages Press * to page down; 9 to main menu

USSD Request		
Item	**Value setting**	**Description**
USSD Profile	N/A	User can select the **USSD Profile**, then USSD Command will change by USSD Profile.
USSD Command	N/A	**USSD Command** can be key in by User or change when User select USSD Profile.
USSD Response	N/A	When send the USSD command, the **USSD Response** screen will appear, User can see the service or receive the service SMS.

Index skipping is used to reserve slots for new function insertion, when required.

7.1.5 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 by manual, 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.



Configuration

Item	Setting
Physical Interface	3G/4G-1 SIM Status:
Network Type	Auto
Scan Approach	Auto

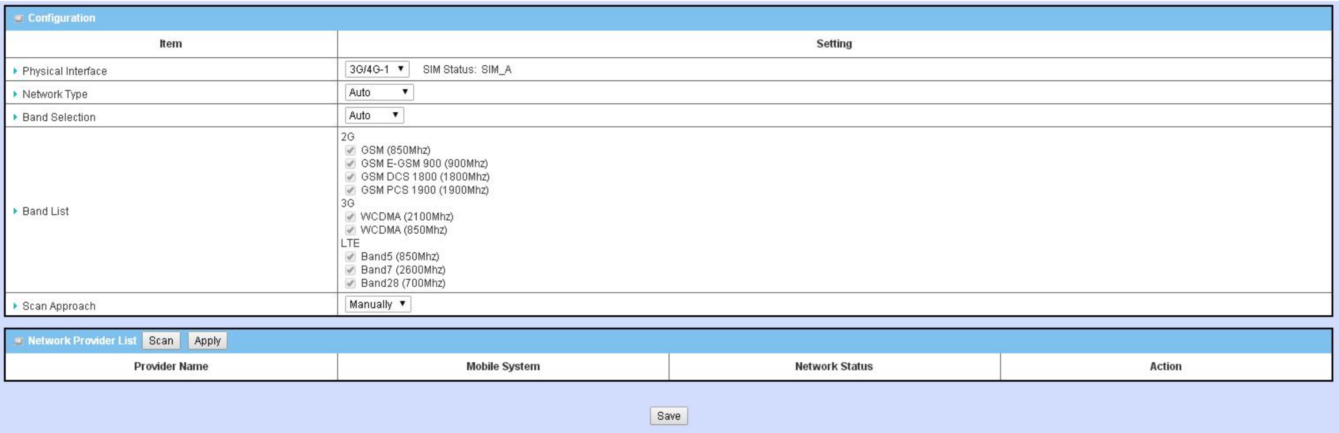
In "Network Scan" page, there are two windows for the Network Scan function. The "Configuration" window can let you select which 3G/4G module (physical interface) is used to perform Network Scan, and system will show the current used SIM card in the module. You can configure each 3G/4G WAN interface 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 "Scan Approach" is Manually 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.

The Network Scan function allow user to set band, network type or specific ISP to register.

Configuration setting

Go to **Application** > **Mobile Application** > **Network Scan**

Index skipping is used to reserve slots for new function insertion, when required.



Configuration

Item	Setting
Physical Interface	3G/4G-1 ▼ SIM Status: SIM_A
Network Type	Auto ▼
Band Selection	Auto ▼
Band List	2G ☑ GSM (850Mhz) ☑ GSM E-GSM 900 (900Mhz) ☑ GSM DCS 1800 (1800Mhz) ☑ GSM PCS 1900 (1900Mhz) 3G ☑ WCDMA (2100Mhz) ☑ WCDMA (850Mhz) LTE ☑ Band5 (850Mhz) ☑ Band7 (2600Mhz) ☑ Band28 (700Mhz)
Scan Approach	Manually ▼

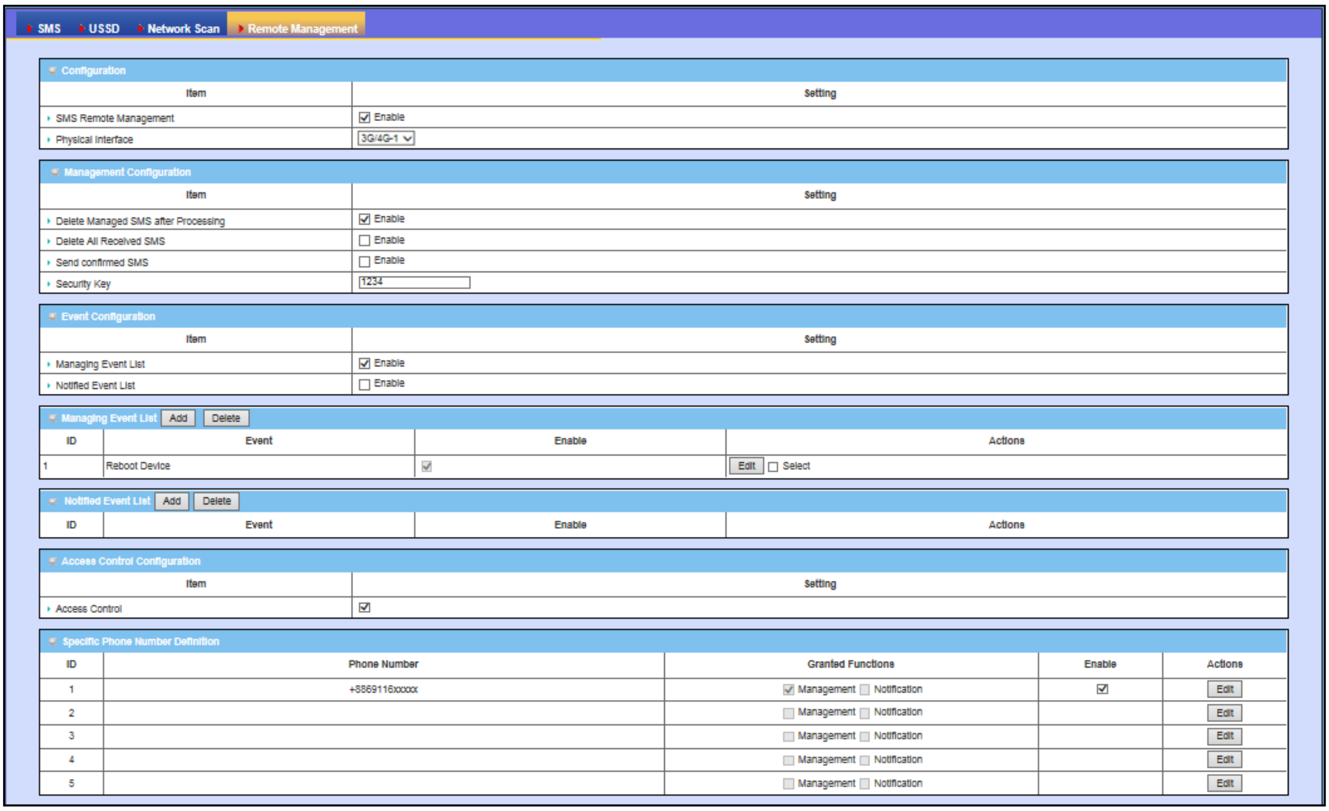
Network Provider List

Provider Name	Mobile System	Network Status	Action

Configuration		
Item	**Value setting**	**Description**
Physical Interface	The box is 3G/4G-1 by default	Choose the **3G/4G-1** or **3G/4G-2** to change setting of cellular module1 or cellular module2.
SIM Status	N/A	Depend on currently SIM status.
Network Type	The box is Auto 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	The box is Auto by default	When **Auto** selected, **Band List** all box checked, and user can't select any option. User need to select the **Manual** option, then allow to change the **Band List** setting.
Band List	All box is checked by default	The **Band List's** options depend on module, and user need to select option at least one for all network type.
Scan Approach	The box is Auto by default	When **Auto** selected, cellular module register automatically. If the **Manually** selected, Network Provider List will shown. when **Manually** is selected in the dropdown list for **Scan Approach**, a network provider list screen appears. Press **Scan** button to scan for the nearest base stations. Select preferred base stations then click **Apply** button to apply settings. **Network Provider List:** When user click **Scan** button, it will be find the provider list nearby. When user select the one of provider list, click **Apply** button to apply it. **Provider Name:** Find the provider near by. **Mobile System:** Find the provider near by. **Network Status:** If this provider and mobile system register currently, It will show **Current**. If it can be register that show **Available**. If it can't register that show **Forbidden**. **Action:** The box is unchecked by default. User can check the box, then click Apply button to apply this provider and mobile system.
Save	N/A	Click **Save** to save the settings

7.1.7 SMS Management

"SMS-based Remote Management" function can let administrator manage the gateway device remotely by using text SMS (Short Message Service) application in the mobile system. Users can send managing SMS messages to this gateway to perform necessary actions, such as to get WAN status, to connect / disconnect / reconnect WAN connection or to reboot the system. In addition, gateway can also send SMS notification messages automatically to users for alert events. Moreover, only the assigned person with connection key can link with the gateway via the SMS system. Administrator can further limit the assigned person by specifying phone numbers to allow communicate with the gateway via the SMS system. Only these phones can SMS control the gateway. Furthermore, the SMS messages can be removed after being processed by the system to clear up the memory to receive more other managing SMS messages in the future. The administrator can also select the kinds of managing and notification events.



Configuration

Item	Setting
SMS Remote Management	☑ Enable
Physical Interface	3G/4G-1

Management Configuration

Item	Setting
Delete Managed SMS after Processing	☑ Enable
Delete All Received SMS	□ Enable
Send confirmed SMS	□ Enable
Security Key	1234

Event Configuration

Item	Setting
Managing Event List	☑ Enable
Notified Event List	□ Enable

Managing Event List Add Delete

ID	Event	Enable	Actions
1	Reboot Device	☑	Edit □ Select

Notified Event List Add Delete

ID	Event	Enable	Actions

Access Control Configuration

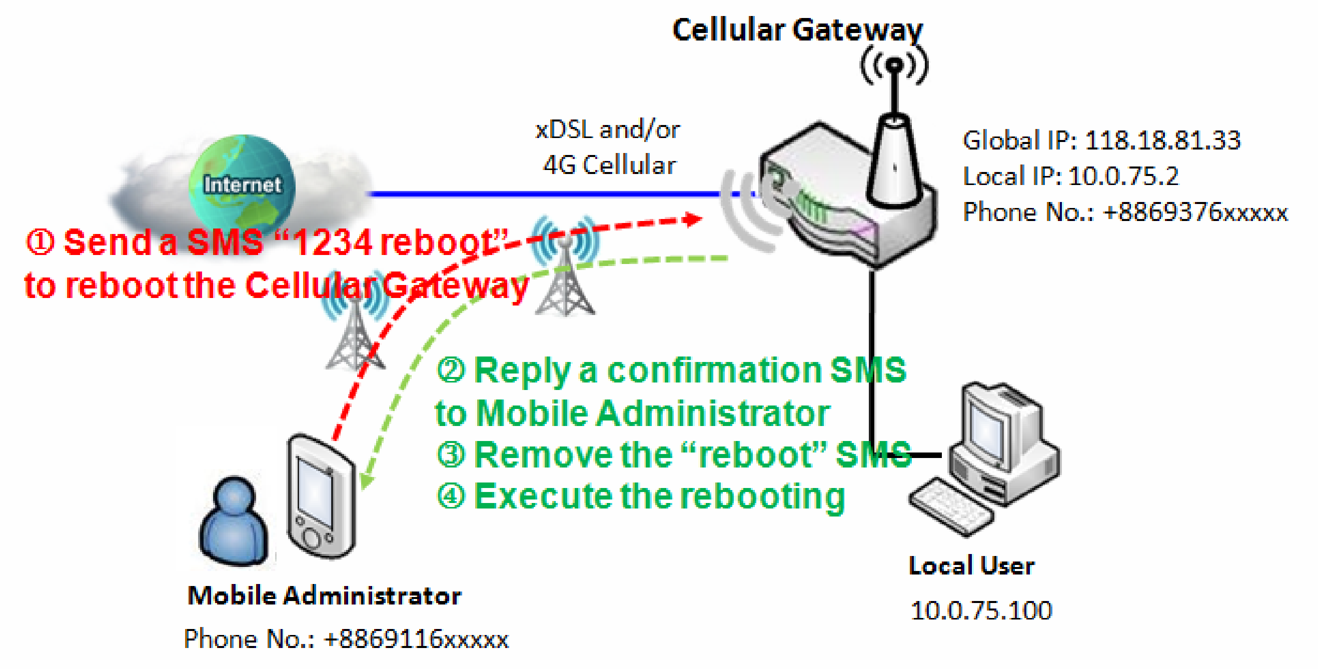
Item	Setting
Access Control	☑

Specific Phone Number Definition

ID	Phone Number	Granted Functions	Enable	Actions
1	+8869116xxxxx	☑ Management □ Notification	☑	Edit
2		□ Management □ Notification		Edit
3		□ Management □ Notification		Edit
4		□ Management □ Notification		Edit
5		□ Management □ Notification		Edit

In "Remote Management" page, there are seven windows for the SMS-based Remote Management function. The "Configuration" window can let you enable the remote management function and specify which 3G/4G interface is the one to carry out the function. The second window is "Management Configuration", administrator can indicate to delete the read SMS for management or others. He also can indicate if the gateway wants to make a reply SMS after processing one managing SMS message. Moreover, he can specify the security key for validating the incoming SMS messages. The third window is "Event Configuration" window, administrator can indicate if the gateway would like to receive the managing events and if the gateway will issue alerting SMS messages upon events happened. In the "Managing Event List" and "Notified Event List" windows, there are managing events and notified events to be selected to enable gateway to execute corresponding actions and make responses once selected events happened. At last, the sixth window is "Access Control Configuration" window. Administrator can enable the access control here to specify only some defined phone numbers can communicate with the gateway via the SMS system. In the "Specific Phone Number Definition" window, for each phone number administrator can further specify the SMS messaging access control. From which phone number the gateway will receive the management SMS messages or to which phone the gateway can issue the notification SMS messages.

A SMS-based Remote Management Scenario



Scenario Application Timing

When the administrator wants to uses a SMS message to drive his remote cellular gateway to make an action and to receive a response when done, the scenario is adequate for the application. Following example is the reboot request to the cellular gateway.

Scenario Description

The mobile administrator sends a reboot SMS with a prefix code of security key to the cellular gateway.

The cellular gateway replies with a confirmation SMS and then tries to reboot itself.

Parameter Setup Example

Following tables list the parameter configuration as an example for "SMS-based Remote Management" function, as shown in above diagram.

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

Configuration Path	[Remote Management]-[Configuration]
SMS Remote Management	■ *Enable*
Physical Interface	*3G/4G-1*

Configuration Path	[Remote Management]-[Management Configuration]
Delete Managed SMS after Processing	■ *Enable*
Send Confirmed SMS	■ *Enable*
Security Key	*1234*

Configuration Path	[Remote Management]-[Event Configuration]
Managing Event List	■ *Enable*

Configuration Path	[Remote Management]-[Managing Event List]
ID	1
Event	*Reboot Device*
Enable	■

Configuration Path	[Remote Management]-[Access Control Configuration]
Access Control	■ *Enable*

Configuration Path	[Remote Management]-[Specific Phone Number Definition]
ID	1
Phone Number	*+8869116xxxxx*
Granted Functions	■ *Management* □ *Notification*
Enable	■

Scenario Operation Procedure

In above diagram, the "Cellular Gateway" is configured with SMS-based Remote Management enabled, the security key and one dedicated phone number (+8869116xxxxx) to manage the gateway remotely for "Reboot Device" managing event.

First, the mobile administrator with a mobile phone set (phone number: +8869116xxxxx) sends a reboot SMS with a prefix code of security key ("1234" here) to the cellular gateway (phone number: +8869376xxxxx).

The cellular gateway receives that SMS message, check the phone number that message comes from, check the security key, reply a confirmation SMS to the sender, deletes the SMS message in the queue and tries to reboot itself.

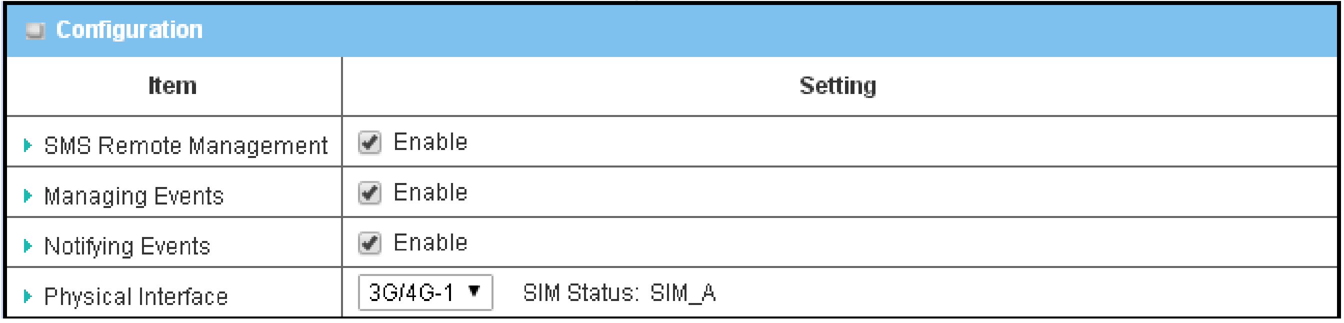
Index skipping is used to reserve slots for new function insertion, when required.

SMS Management Setting

SMS management is the application that allows administrator to remotely managing the gateway via issuing some Managing Event SMS, or got the instant alerts from the remote gateway with notifying event SMS.

Enabling SMS Management

Go to **Applications** > **Mobile Application** > **SMS Management Tab**



Configuration

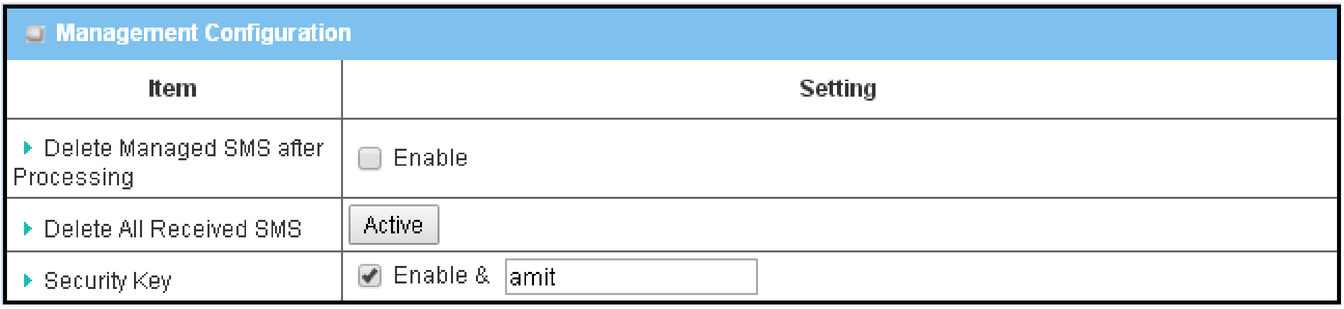
Item	Setting
SMS Remote Management	☑ Enable
Managing Events	☑ Enable
Notifying Events	☑ Enable
Physical Interface	3G/4G-1 ▼ SIM Status: SIM_A

Configuration Item	Value setting	*Description*
SMS Remote Management	The box is unchecked by default	Check the **Enable** box to activate SMS Remote Management function
Managing Events	The box is unchecked by default	Check the **Enable** box to activate Managing Events function
Notifying Events	The box is unchecked by default	Check the **Enable** box to activate Notifying Events function
Physical Interface	The box is 3G/4G-1 by default	Choose the **3G/4G-**1 or **3G/4G-2** to change setting of cellular module1 or cellular module2.
SIM Status	N/A	Depend on currently SIM status.
Save	NA	Click the Save button to save the configuration

Index skipping is used to reserve slots for new function insertion, when required.

Management Configuration Definition

SMS setting about managing events



Management Configuration

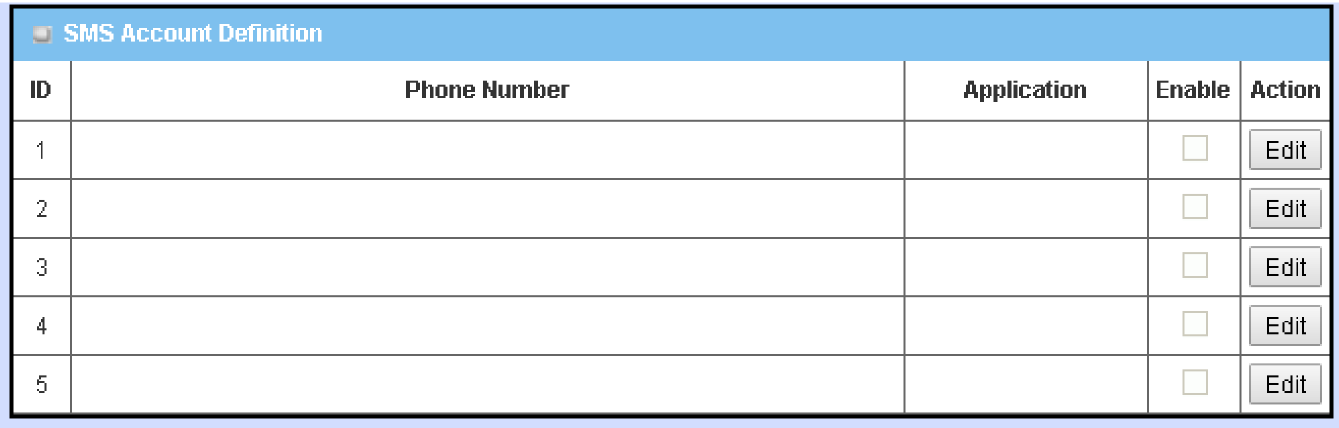
Item	Setting
Delete Managed SMS after Processing	□ Enable
Delete All Received SMS	Active
Security Key	☑ Enable & amit

Management Configuration		
Item	**Value setting**	**Description**
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.
Delete All Received SMS	N/A	Press the **Active** button to delete all the received SMS.
Security Key	The box is unchecked by default	Click the **Enable** box to enable the security key for validating the received SMS. Once the function is enabled, you have to enter the security key behind the checkbox. The received managing events SMS must have the designated security key as an initial identifier, then corresponding handlers will become effective for further processing.
Save	NA	Click the Save button to save the configuration

Index skipping is used to reserve slots for new function insertion, when required.

SMS Account Definition

Setup your SMS Account. It supports up to a maximum of 5 accounts. You can click the **Edit** button for each ID to edit the account.



SMS Account Definition

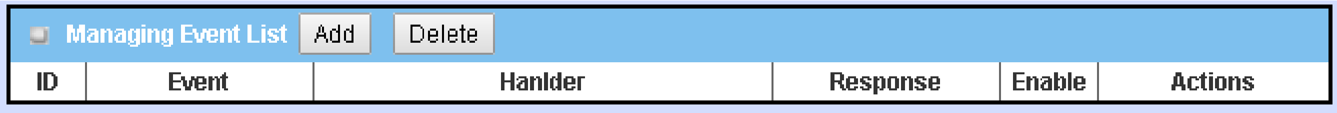
ID	Phone Number	Application	Enable	Action
1			□	Edit
2			□	Edit
3			□	Edit
4			□	Edit
5			□	Edit

SMS Account Definition		
Item	**Value setting**	**Description**
Phone Number	1. Mobile telephone numbers format 2. A Must filled setting	Specify the phone number that will issuing the SMS as the account identifier.
Application	A Must filled setting	Specify the application type. It could be **Managing Events, Notifying Events, 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.

Index skipping is used to reserve slots for new function insertion, when required.

Create/Edit Managing Events Rules

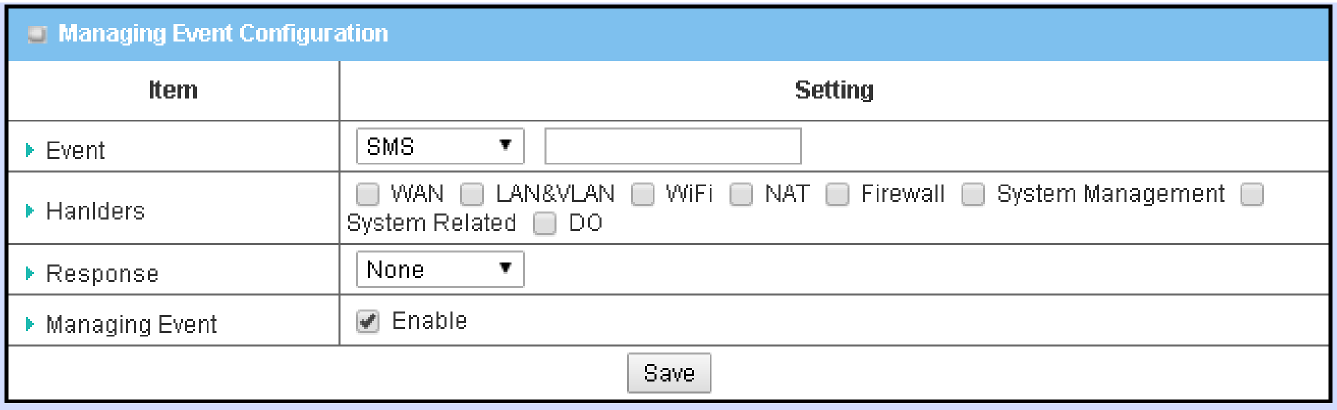
Setup your Managing Event rules. It supports up to a maximum of 128 rules.



Managing Event List

ID	Event	Hanlder	Response	Enable	Actions

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



Managing Event Configuration

Item	Setting
Event	SMS ▼
Hanlders	□ WAN □ LAN&VLAN □ WiFi □ NAT □ Firewall □ System Management □ System Related □ DO
Response	None ▼
Managing Event	☑ Enable

Managing Event Configuration		
Item	**Value setting**	**Description**
Event	**SMS** (or **SNMP Trap**) by default	Specify the Event type (**SMS**, **SNMP Trap**, **DI**, or **Modbus**) and event code. Select **SMS** and fill the message in the textbox to specify SMS Event; Select **SNMP Trap** and fill the message in the textbox to specify SNMP Trap Event; Select **DI** and select profile from Digital Input (DI) Profile List to specify DI Event; Select **Modbus** and select profile from Modbus Definition to specify Modbus Event.
Handlers	All box is unchecked by default.	Specify the related Handlers for the managing event. Select **Power** Checkbox and select the handlers you want to specify Power Handlers; Select **WAN** Checkbox and select the handlers you want to specify WAN Handlers ; Select **LAN&VLAN** Checkbox and select the handlers you want to specify LAN&VLAN Handlers; Select **WiFi** Checkbox and select the handlers you want to specify WiFi Handlers; Select **NAT** Checkbox and select the handlers you want to specify NAT Handlers; Select **Firewall** Checkbox and select the handlers you want to specify Firewall Handlers; Select **System Management** Checkbox and select the handlers you want to specify System Management Handlers; Select **System Related** Checkbox and select the handlers you want to specify System Related Handlers; Select **DO** Checkbox and select the profile from Digital Output (DO) Profile List to specify DO Handlers.

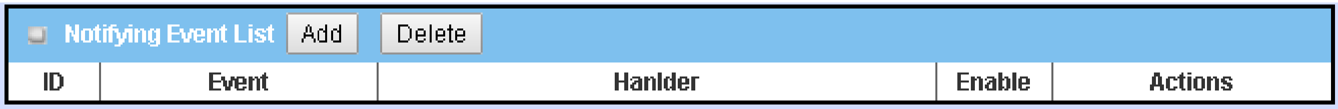
Index skipping is used to reserve slots for new function insertion, when required.

Response	**None** by default	Specify the Response to be taken for the managing event. Select **None** to specify no response; Select **DO** and select profile from Digital Output (DO) Profile List to specify the DO Response; Select **SMS** to specify the SMS Response; Select **SNMP Trap** to specify the SNMP Trap Response; Select **Modbus** and select profile from Modbus Definition to specify the Modbus Response.
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

Index skipping is used to reserve slots for new function insertion, when required.

Create/Edit Notifying Events Rules

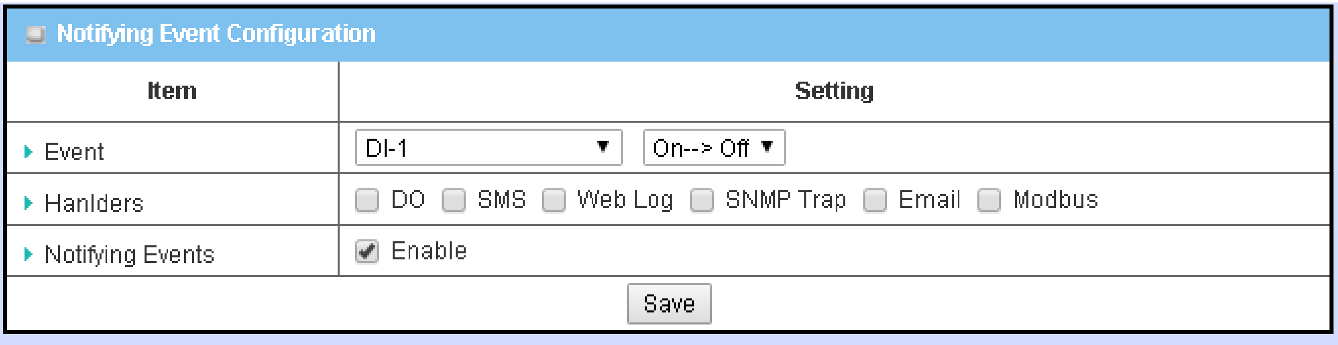
Setup your Notifying Event rules. It supports up to a maximum of 128 rules.



Notifying Event List

ID	Event	Hanlder	Enable	Actions

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



Notifying Event Configuration

Item	Setting
Event	DI-1 ▼ On--> Off ▼
Hanlders	□ DO □ SMS □ Web Log □ SNMP Trap □ Email □ Modbus
Notifying Events	☑ Enable

Notifying Event Configuration		
Item	**Value setting**	**Description**
Event	**DI-1** (or **WAN**) by default	Specify the Event type and event condition. Select **DI-1** and select the event condition to specify DI-1 Event; Select **Power-1** and select the event condition to specify Power-1 Event; Select **WAN** and select the event condition to specify WAN Event; Select **LAN&VLAN** and select the event condition to specify LAN&VLAN Event; Select **WiFi** and select the event condition to specify WiFi Event; Select **Client&Server&Proxy** and select the event condition to specify Client&Server&Proxy Event; Select **System Related** and the event condition to specify System Related Event.
Handlers	All box is unchecked by default.	Specify the Handlers to take reaction when the event is triggered. Select **DO** Checkbox and select the profile from Digital Output (DO) Profile List to specify DO Handlers; Select **SMS** to specify the SMS Handler; Select **Web Log** and select/unselect the Enable Checkbox to specify the Web Log Handler; Select **SNMP Trap** to specify the SNMP Trap Handler; Select **Email** and select the profile from Email Definition to specify the Email Handler; Select **Modbus** and select profile from Modbus Definition to specify the Modbus Handler.
Notifying Events Enable	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

7.5 Captive Portal

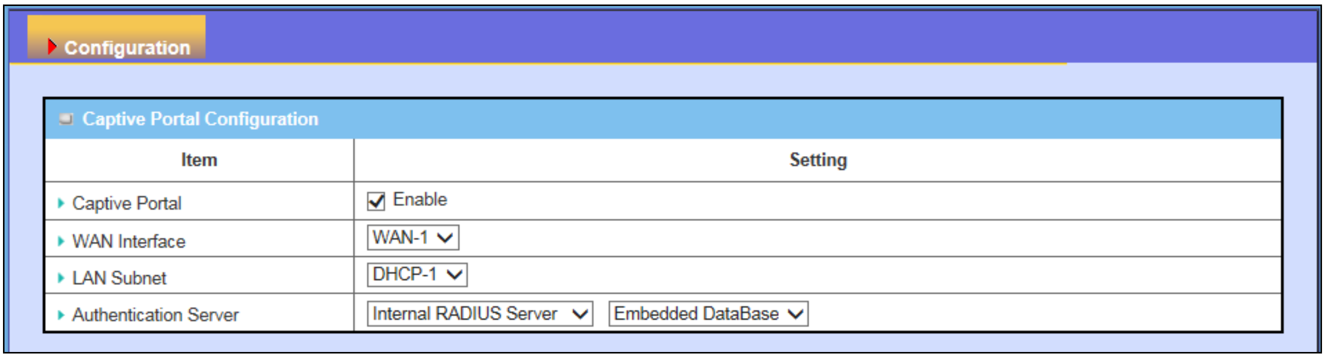
A captive portal is a portal web page that is displayed before a user can browse Internet. The portal is often used to present a login page. This is done by intercepting most packets, regardless of address or port, until the user opens a browser and tries to access the web. At that time the browser is redirected to a web page which may require authentication and/or payment, or simply display an acceptable use policy and require the user to agree. Captive portals are used at many Wi-Fi hotspot services, and can be used to control wired access (e.g. apartment houses, hotel rooms, business centers, "open" Ethernet jacks) as well.[15]

Since the login page itself must be presented to the client, either that login page is locally stored in the gateway, or the web server hosting that page must be "whitelisted" via a walled garden to bypass the authentication process. Depending on the feature set of the gateway, multiple web servers can be whitelisted (say for iframes or links within the login page). In addition to whitelisting the URLs of web hosts, some gateways can whitelist TCP ports. The MAC address of attached clients can also be set to bypass the login process. This technique has occasionally been referred to as UAM (Universal Access Method) in implementations and standards forums.[1]

The gateway supports the Captive Portal function to ask guests or passengers to pass the authentication process before they can surf the Internet via the gateway. There are two approaches, including internal captive portal and external captive portal. For external captive portal, you must specify external RADIUS (Remote Authentication Dial In User Service) server and external UAM (Universal Access Method) server. In contrast, for internal captive portal, you will only select “Internal RADIUS Server” option for user authentication. The user account database can be an embedded database, an external AD database or an external LDAP database. However, the UAM server is not necessary for this case and that the captive portal Web site is embedded in the device.

7.5.1 Configuration

Administrator of gateway can enable the Captive Portal function and configure the device to be the internal captive portable or the external captive portal for the function. But please be noted that there is only selected AMIT gateway models support external captive portal function.



Captive Portal Configuration

Item	Setting
Captive Portal	☑ Enable
WAN Interface	WAN-1
LAN Subnet	DHCP-1
Authentication Server	Internal RADIUS Server Embedded DataBase

[15] http://en.wikipedia.org/wiki/Captive_portal

In "Configuration" page, there is only one window for the Captive Portal function. The "Captive Portal Configuration" window can let you enable the function, specify which WAN interface for user authentication, which VLAN group of client hosts must pass the user authentication before Internet surfing and choose the internal captive portal or the external captive portal.

External Captive Portal

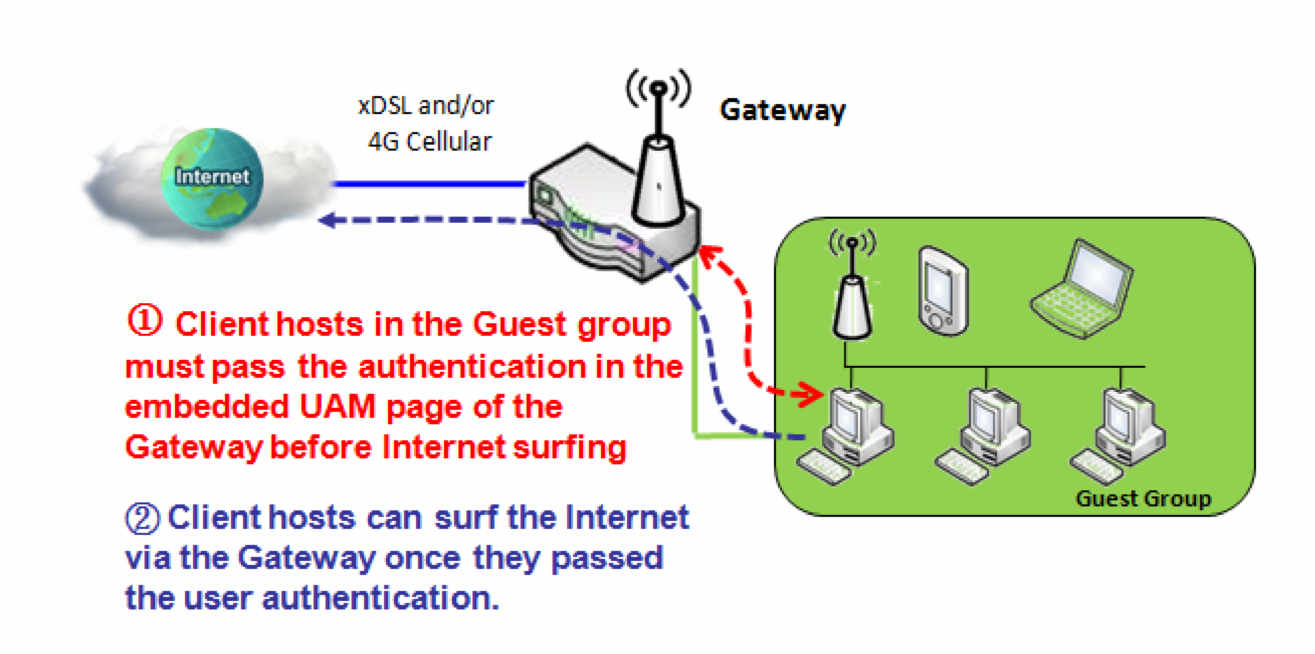
Before enabling the external Captive Portal function, please go to **[System]-[External Servers]** to setup external server objects, like RADIUS server and UAM server. Then return to configure Captive Portal function back in this page to specific WAN Interface, select external Authentication Server and UAM Server from the pre-defined external server object list.

Internal Captive Portal

Before enabling internal Captive Portal function, please go to **[System]-[External Servers]** to define some external server objects, like LDAP server or AD server if necessary. Then return to configure Captive Portal function back in this page to specific WAN Interface, select “Internal RADIUS Server” option for user authentication and specify its user database to be the embedded one, an external LDAP server or an external AD server from the pre-defined external server object list.

NOTE: All Internet Packets will be forwarded to Captive Portal Web site of the gateway when Captive portal feature is enabled. Please make sure that at least one user account is created.

Internal Captive Portal Scenario


xDSL and/or
4G Cellular
Gateway
Internet
① Client hosts in the Guest group must pass the authentication in the embedded UAM page of the Gateway before Internet surfing
② Client hosts can surf the Internet via the Gateway once they passed the user authentication.
Guest Group

Scenario Application Timing

When your purchased gateway has the "Captive Portal" function and the administrator wants to ask specific users to execute an authentication process before their Internet surfing via the gateway. The Captive Portal function in the gateway includes the internal one and the administrator of gateway can create user accounts for users in the [System]-[User Management] for user authentication. Then the scenario is adequate to be adopted in the situation.

Scenario Description

Client hosts in the Guest group must pass the authentication process in the embedded UAM page of the Gateway before Internet surfing.

Client hosts can access the Internet via the Gateway once they passed the user authentication.

Parameter Setup Example

Following tables list the parameter configuration as an example for "Internal Captive Portal" function, as shown in above diagram.

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

Configuration Path	[DHCP Server]-[DHCP Server Configuration]
DHCP Server Name	***DHCP 2***
LAN IP Address	***10.0.76.2***
Subnet Mask	***255.255.255.0 (/24)***
IP Pool	***10.0.76.100 ~ 10.0.76.200***
Server	■ ***Enable***

Configuration Path	[VLAN]-[Configuration]
VLAN Type	***Port-based***

Configuration Path	[VLAN]-[Port-based VLAN List]
Port	***Port-4***
NAT/Bridge	***NAT***
DHCP Server	***DHCP 2***

Configuration Path	[User Profile]-[User List Configuration]
User Name	***GuestAccount***
Password	***GuestPassword***
User Level	***Guest***
Lease Time	***10000*** (seconds)
Idle Timeout	***60*** (seconds)
Profile	■ ***Enable***

Configuration Path	[Configuration]-[Captive Portal Configuration]
Captive Portal	■ *Enable*
WAN Interface	*WAN-1*
LAN Subnet	*DHCP-2*
Authentication Server	*Internal RADIUS Server Embedded Database*

Scenario Operation Procedure

In above diagram, the "Gateway" serves as the gateway integrating with internal captive portal function and an embedded user account database. There are two VLAN groups in its Intranet. The first one is VLAN-1 and the IP address of the virtual LAN interface is 10.0.75.2. There is one DHCP server, DHCP-1, acting for the VLAN-1 group, and it is adequate for the Staff group of users. The Staff can surf the Internet normally without user authentication. But, the second VLAN group is VLAN-2 and the IP address of the virtual LAN interface is 10.0.76.2. There is another DHCP server, DHCP-2, acting for the VLAN-2 group, and it is for the Guest group of users. The Guest can surf the Internet only when they can pass the authentication process in the embedded UAM web page.

One client host under the Guest group wants to surf the Internet by using its browser.

The gateway checks out that the Internet surfing request comes from the Guest group and the client host in the Guest group hasn't been authenticated by the gateway. So, the gateway redirects the request to the UAM web page and asks the user to input correct account and password.

Once the user authentication process completes successfully, the gateway redirects the web page to the requested one. Furthermore, the gateway also records the MAC address of guest client host and allows its incoming Internet access requests.

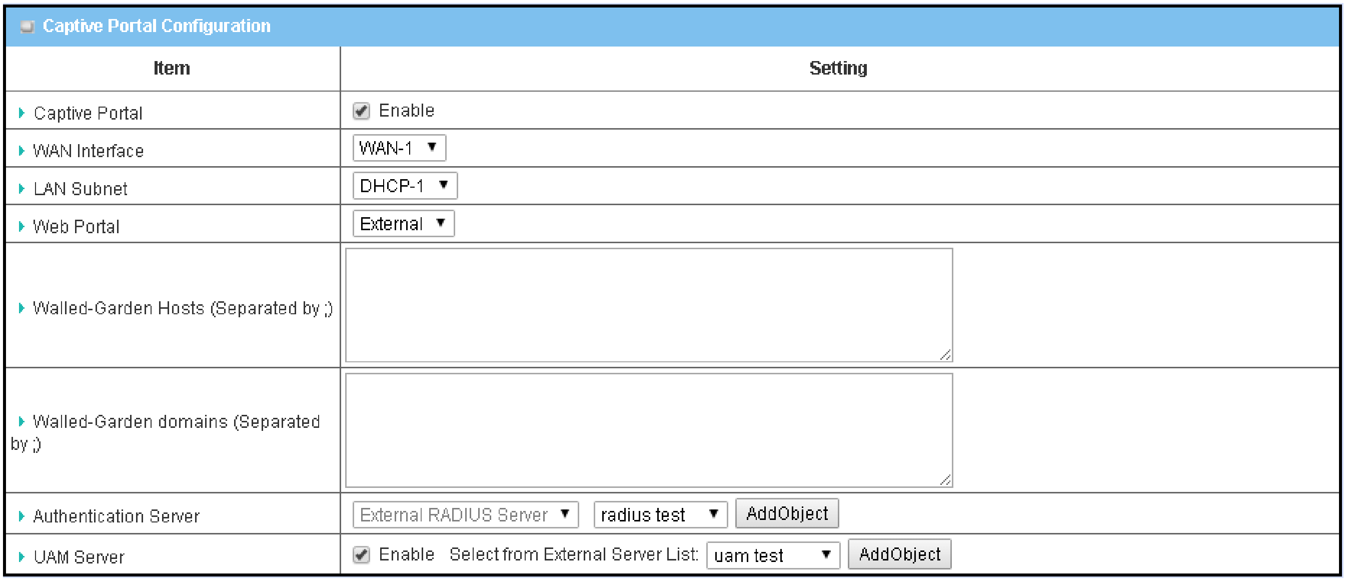
Each account has its own lease time and it will not be reused for authentication once the lease time has run out. The client host with that account will be rejected to surf the Internet.

However, there is a timeout setting for each account. When the client host with that account has been idle at the Internet surfing for a while that reaches the timeout setting, the gateway will re-authenticate the client host for further Internet connection.

The Captive Portal will direct user to a login page when user try to access the Internet.

Ensure Captive Portal are enabled and saved
Go to Applications > Captive Portal > Configuration Tab

Index skipping is used to reserve slots for new function insertion, when required.



Captive Portal Configuration

Item	Setting
Captive Portal	☑ Enable
WAN Interface	WAN-1 ▼
LAN Subnet	DHCP-1 ▼
Web Portal	External ▼
Walled-Garden Hosts (Separated by ;)	
Walled-Garden domains (Separated by ;)	
Authentication Server	External RADIUS Server ▼ radius test ▼ AddObject
UAM Server	☑ Enable Select from External Server List: uam test ▼ AddObject

Captive Portal Item Setting	Value setting	Description
Captive Portal	The box is unchecked by default	When Check the **Enable** box It will activate Captive Portal functions.
WAN Interface	A Must filled setting	This field is to specify the WAN interface of captive portal. Select **WAN-1** it means when WAN-1 interface gets its IP, the captive portal is loading. Other WAN interface options can be added by enable WAN interface in **Basic Network > WAN > Physical Interface**.
LAN Subnet	A Must filled setting	This field is to specify the LAN subnet of captive portal. When **DHCP-1** is selected, means if user connect to the physical port which the DHCP-1 server binds, user will be directed to a login page when access the Internet. Other DHCP server options can be added in **Basic Network > Client/Server/Proxy > DHCP Server**. When user create a new DHCP server, it must binds physical port if this DHCP server used in Captive Portal.
Web Portal	A Must filled setting	This field is to specify the internal or external authentication server. Not all machines with internal options, some machine only have external options. When External is selected, there is no Customize login page and user must specify Uam Server and Authentication Server. When **Internal** is selected, user just need to specify **Authentication Server** and login page can be edited in **Customize login page.**
Customize login page	N/A	The **Download Default CSS and Logo** button can download the default CSS file and Logo of login page of internal authentication server. The **Download Current CSS and Logo** button can download the current CSS file and Logo of login page of internal authentication server. User can edit the CSS file or Logo downloaded from above buttons and upload them by **Upload CSS and Logo files** button.
Walled-Garden	Optional setting	The host IPs and domain names filled in this field can be accessed directly without

Hosts(Separated by;)		direct to login page.
Walled-Garden domains(Separated by;)	Optional setting	The domain names filled in this field can be accessed directly without direct to login page.
Authentication Server	A Must filled setting	This field is to specify the authentication server. If Web Portal is internal, there are three servers you can choose. When **Embedded DataBase** is selected, the login IDs and passwords are created in **System > User Management > User Profile tab** When **External LDAP** is selected, the login IDs and passwords are from external LDAP server. When **External AD** is selected, the login IDs and passwords are from external AD server. If Web Portal is external, user need to specify external radius server. The external LDAP, AD server or external radius server can be added by pressing **AddObject** button directly or added in **System > External Servers > External Servers tab.**
Uam Server	A Must filled setting	This field is to specify the uam server. If Web Portal is external, user need to specify and enable uam server. The uam server can be added by pressing **AddObject** button directly or added in **System > External Servers > External Servers tab.** Note: UAM Server is available when **External** in Web Portal dropdown box is selected.
Save	N/A	Click the **Save** button to save the settings.
Refresh	N/A	Click the **Refresh** button to refresh the page.

Chapter 9 System

9.1 System Related

9.1.1 System Related

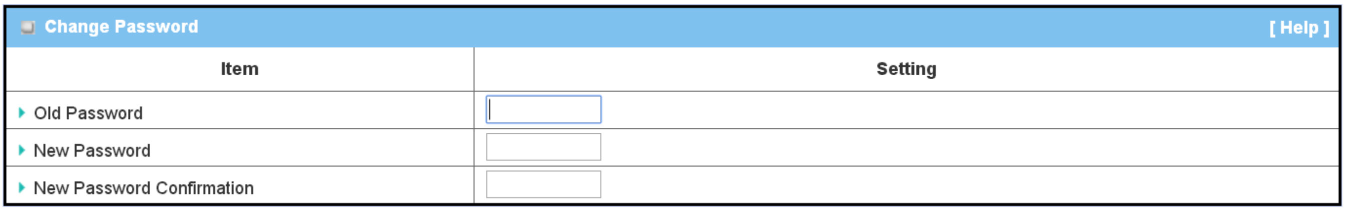
System Related allows the network administrator to manage system, settings such as web-based utility access password change, advanced system & network tools, system firmware upgrades, Email alert and system log.

Go to System > System Related tab

Change Password

Change password screen allows network administrator to change the web-based utility login password to access gateway.

Go to System > System Related > Change Password tab



Change Password [Help]

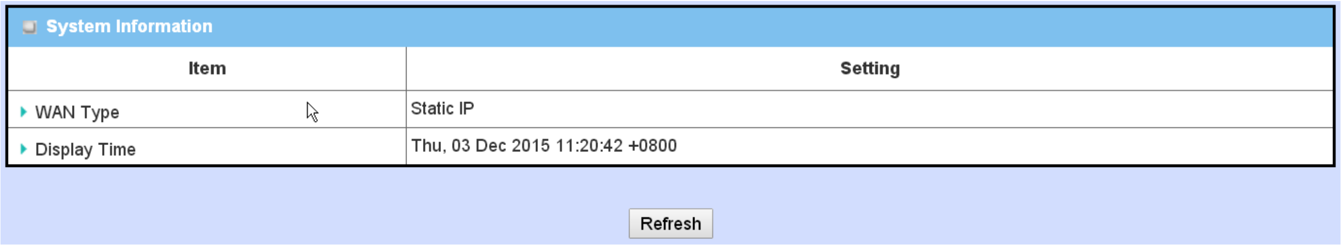
Item	Setting
Old Password	
New Password	
New Password Confirmation	

Change Password Item	Value Setting	Description
Old Password	String: any text	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

System Information

System Information screen gives network administrator a quick look up on the type of WAN connection is currently 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 System > System Related > System Information tab



System Information

Item	Setting
WAN Type	Static IP
Display Time	Thu, 03 Dec 2015 11:20:42 +0800

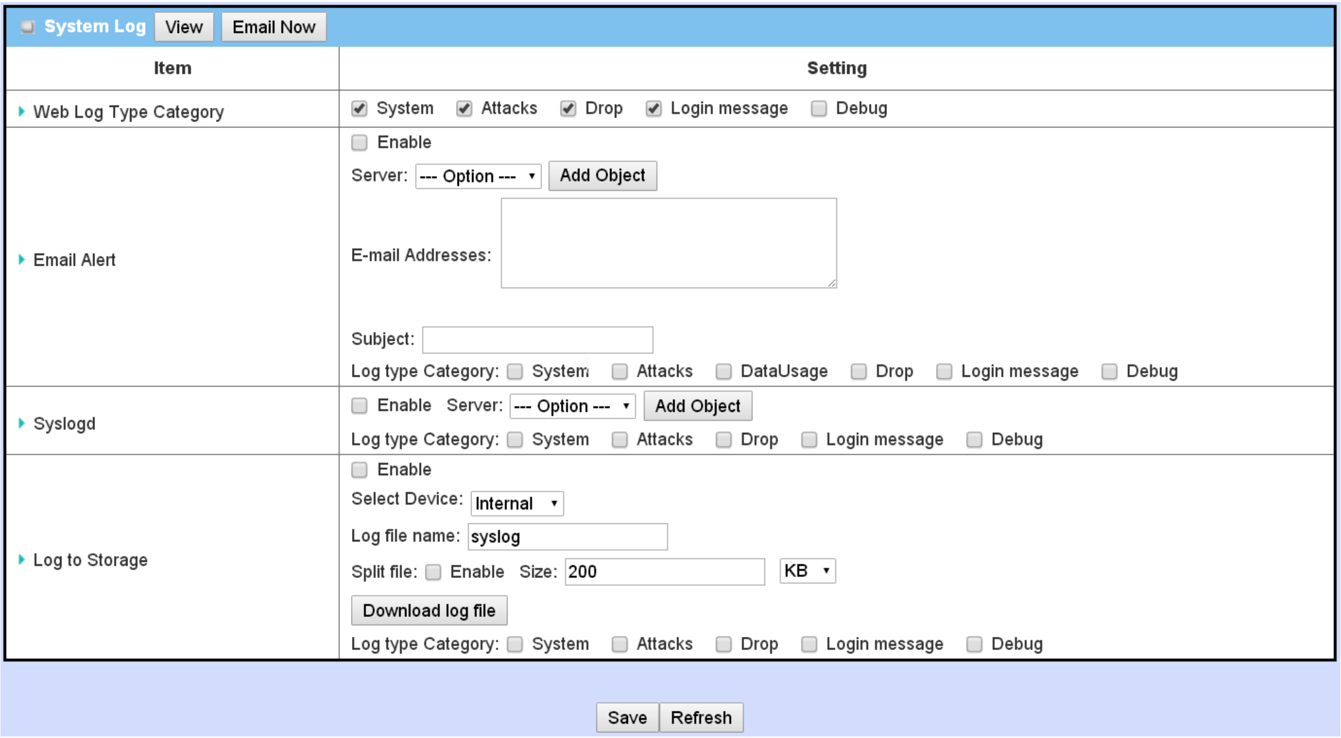
System Information		
Item	**Value Setting**	**Description**
WAN Type	N/A	It displays WAN Type of WAN-1 Interface Internet connection configured.
Display Time	N/A	It displays current system time.

Index skipping is used to reserve slots for new function insertion, when required.

System Status

System Status screen contains various event log tools facilitating network administrator to perform local event logging and remote reporting.

Go to System > System Related > System Status tab



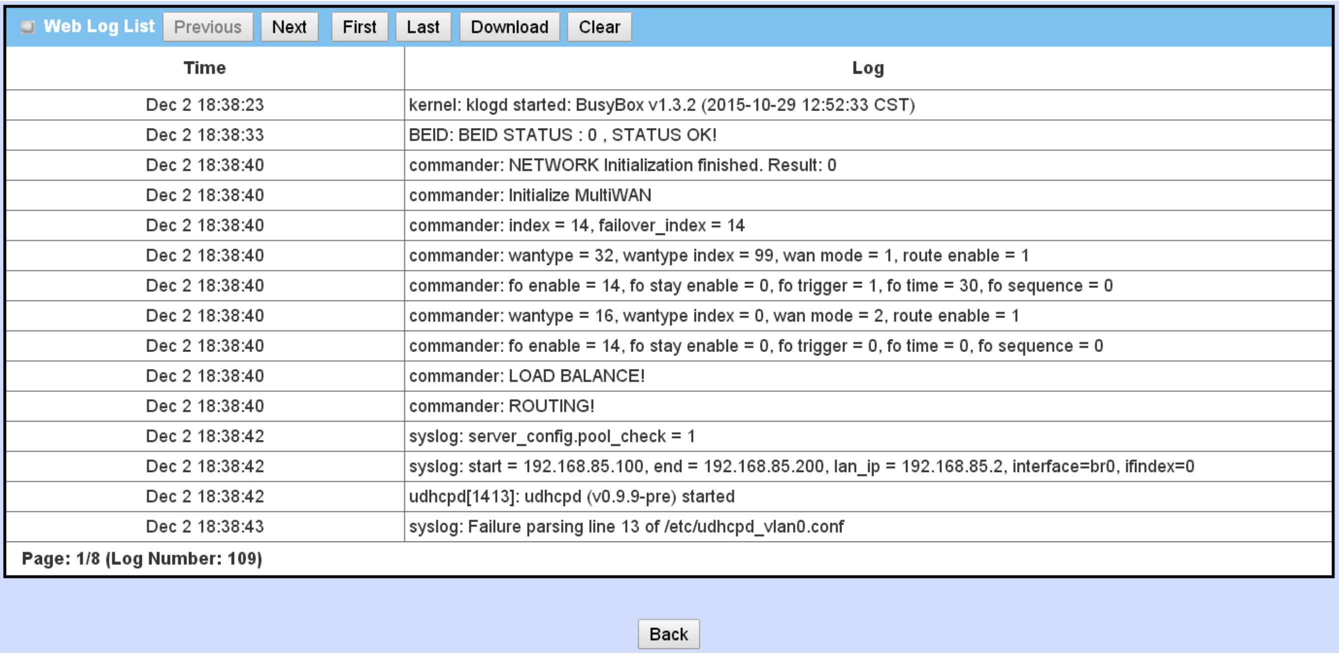
Item	Setting
Web Log Type Category	☑ System ☑ Attacks ☑ Drop ☑ Login message □ Debug
Email Alert	□ Enable Server: --- Option --- Add Object E-mail Addresses: Subject: Log type Category: □ System □ Attacks □ DataUsage □ Drop □ Login message □ Debug
Syslogd	□ Enable Server: --- Option --- Add Object Log 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 Emails for analysis.

View & Email Log History

Item	Value setting	Description
View button	N/A	Click on the **View** button to view Log History in Web Log List Window.
Email Now button	N/A	Click on the **Email Now** button to send Log History via email instantly.
Save	N/A	Click **Save** button to save the settings.
Refresh	N/A	Click the **Refresh** button to refresh the page.



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)

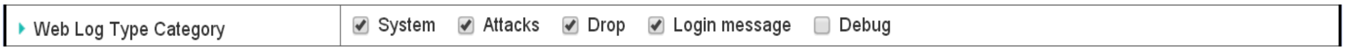
Web Log List Window

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 event 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.

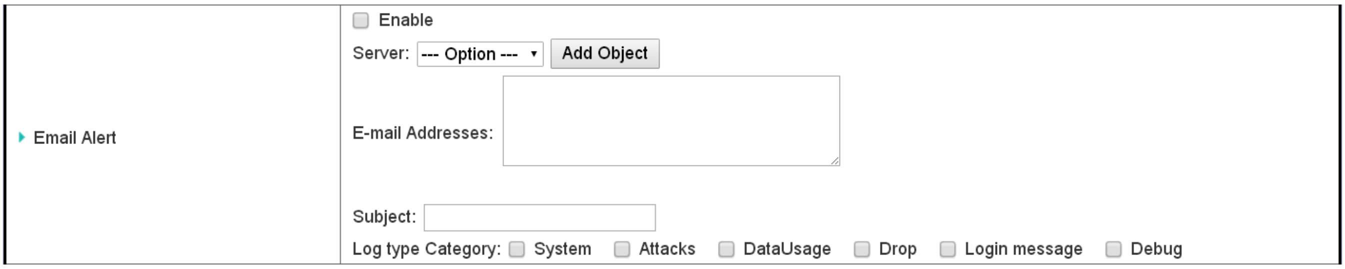


Web Log Type Category	☑ System ☑ Attacks ☑ Drop ☑ Login message □ Debug

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

Email Alert

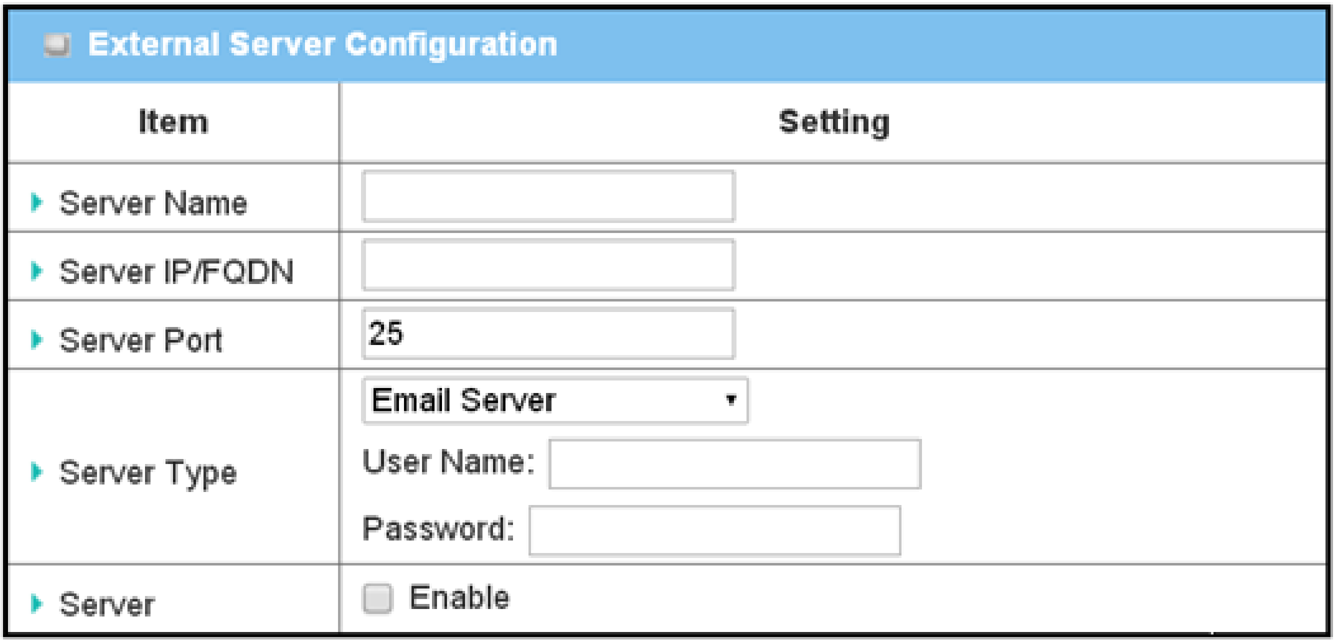
Email Alert screen allows network administrator to select the type of event to log and be sent to the destined Email account.



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

Email Alert Setting Window		
Item	**Value Setting**	**Description**
Enable	Default unchecked	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, press Add Object button to create an outgoing Email server.
E-mail address	String : email format	Enter the recipient's Email account. Separate Email accounts with comma ',' or semicolon ' ;' Enter the Email account 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 event to log and be sent to the destined Email account. Available events are System, Attacks, Data Usage, Drop, Login message, and Debug.

Email Alert Button Description		
Item	**Value setting**	**Description**
Add Object Button	N/A	Click on the Add Object button, a popup window will appear. Add an outgoing Email server. You may also add an outgoing Email server from External Servers under System (System > External Server > External Server tab).

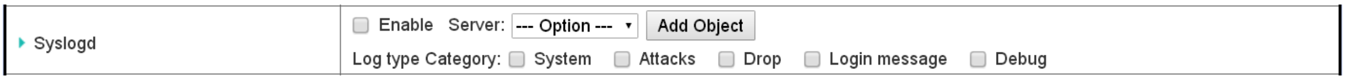


External Server Configuration

Item	Setting
Server Name	
Server IP/FQDN	
Server Port	25
Server Type	Email Server ▾ User Name: Password:
Server	□ Enable

Syslogd

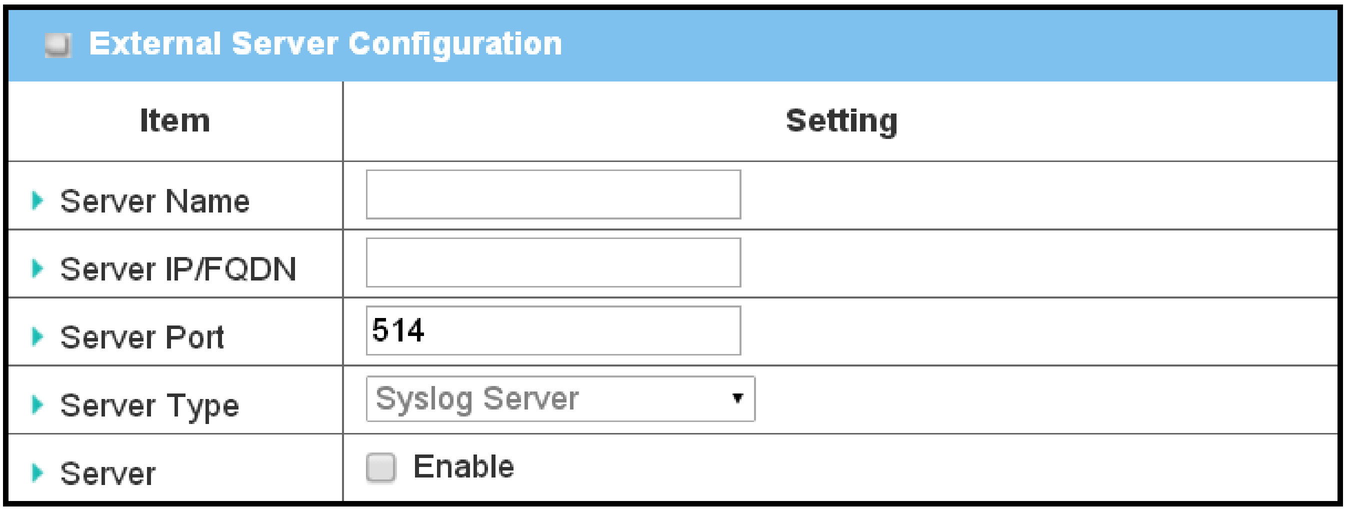
Syslogd screen allows network administrator to select the type of event to log and be sent to the destined Syslog server.



Syslogd	□ Enable Server: --- Option --- ▾ Add Object Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug

Syslogd Setting Window		
Item	**Value Setting**	**Description**
Enable	Default unchecked	Check Enable box to enable sending event logs to syslog server
Server	Select from menu	Select one syslog server from the Server dropdown box to sent event log to. If none has been available, press Add Object button to create a syslog server.
Log type category	Default unchecked	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.

Syslogd Button Description		
Item	**Value setting**	**Description**
Add Object Button	N/A	Click on the Add Object button, a popup window will appear. Add a syslog server. You may also add a syslog server from External Servers under System (System > External Server > External Server tab).



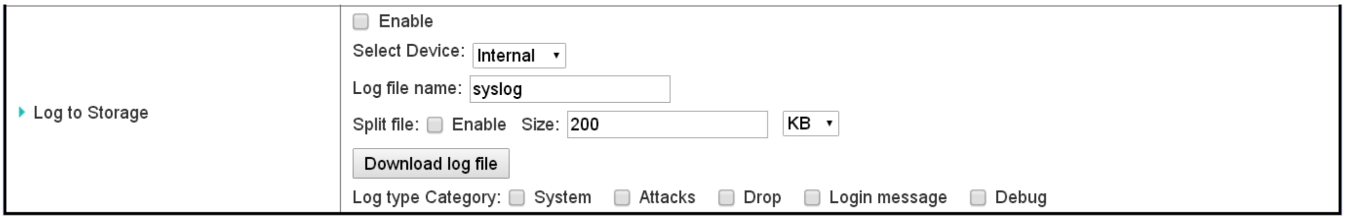
External Server Configuration

Item	Setting
Server Name	
Server IP/FQDN	
Server Port	514
Server Type	Syslog Server ▾
Server	□ Enable

Index skipping is used to reserve slots for new function insertion, when required.

Log to Storage

Log to Storage screen allows network administrator to select the type of event 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	Default unchecked	Check to enable sending log to storage
Select Device	Internal is selected by default	Select internal or external storage
Log file name	Default unchecked	Set file name to save logs in storage
Split file Enable	Default unchecked	Check to enable split file whenever log file reaching size set in the following filed
Split file Size	Default 200 KB	Set file size to split log file
Log type category	Default unchecked	Check which type of logs to send: System, Attacks, Drop, Login message, Debug

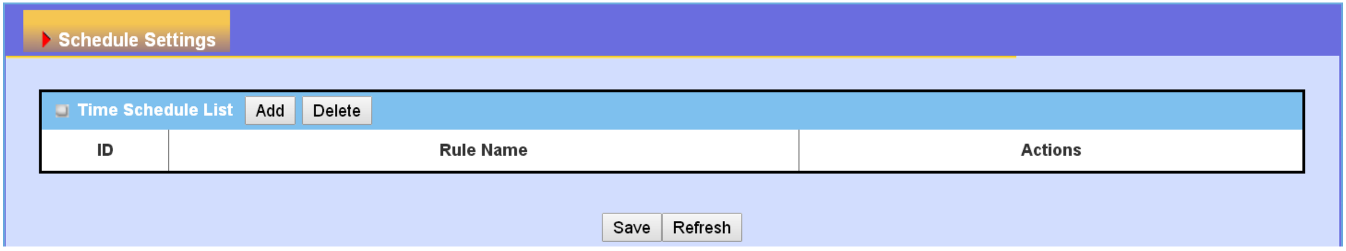
Log to Storage Button Description		
Item	**Value setting**	**Description**
Download log file	N/A	Click the **Download log file** button to download log files so far

Index skipping is used to reserve slots for new function insertion, when required.

9.3 Scheduling

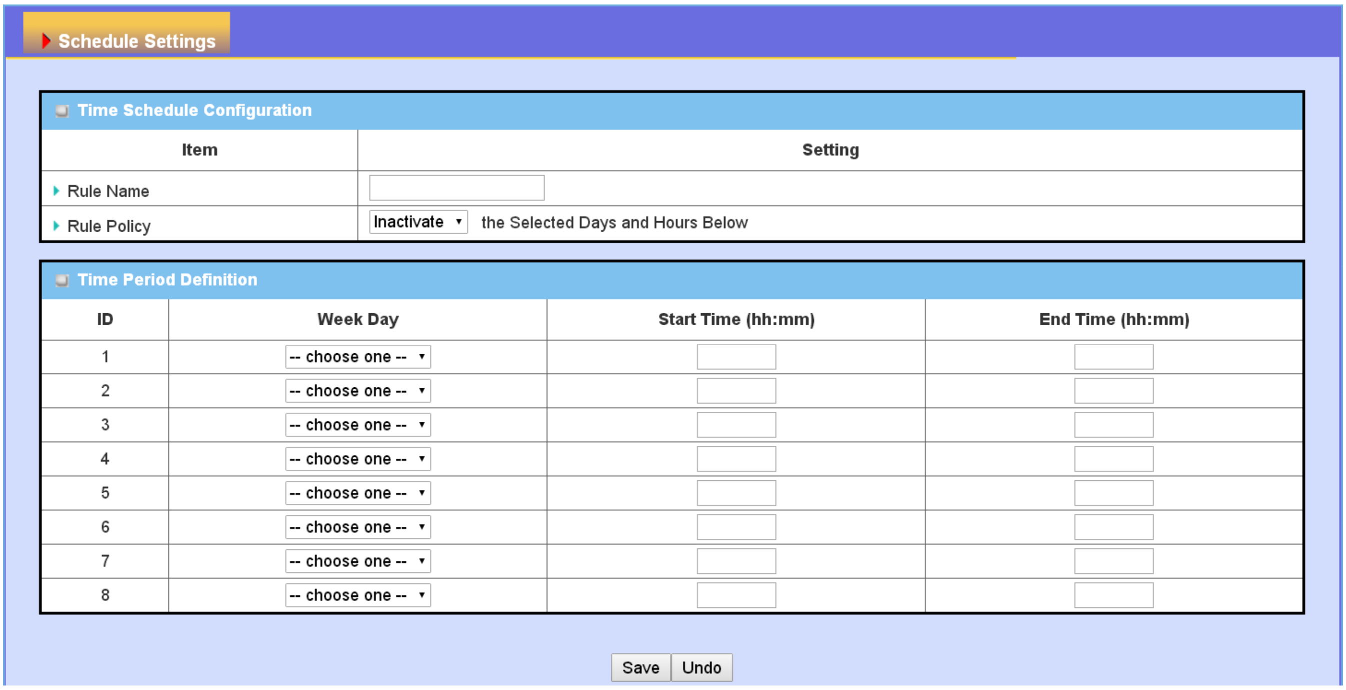
Scheduling provides ability of adding/deleting time schedule rules, which can be applied to other functionality.

Go to System > Scheduling > Schedule Settings



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)
Save	N/A	Click the **Save** button to save changes
Refresh	N/A	Click the **Refresh** button to refresh current page



Item	Setting
Rule Name	
Rule Policy	Inactivate the Selected Days and Hours Below

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 --		

Index skipping is used to reserve slots for new function insertion, when required.

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

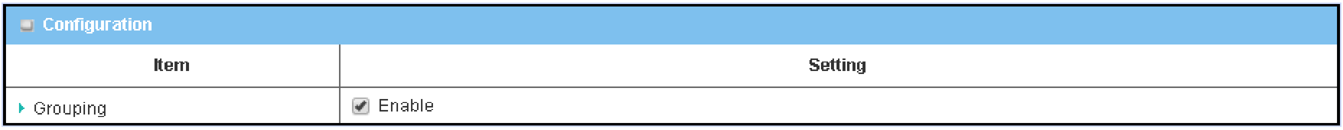
Time Period Definition		
Item	**Value Setting**	**Description**
Week Day	Select from menu	Select everyday or one of weekday
Start Time	Time format (hh :mm)	Start time in selected weekday
End Time	Time format (hh :mm)	End time in selected weekday

Button description		
Item	**Value setting**	**Description**
Save	NA	Click the **Save** button to save changes
Undo	NA	Click the **Undo** button to revert changes

9.7 Grouping

The Grouping allow user to make group for some services.

Ensure Grouping are enabled and saved
Go to System > Grouping > Configuration Tab



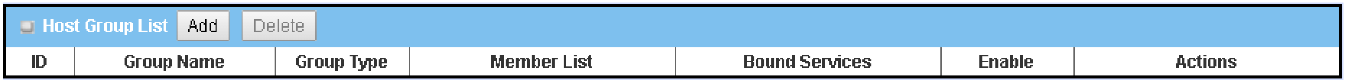
Configuration

Item	Setting
Grouping	☑ Enable

Currently support three kinds of group: Host Grouping, File Extension Grouping and L7 Application Grouping.

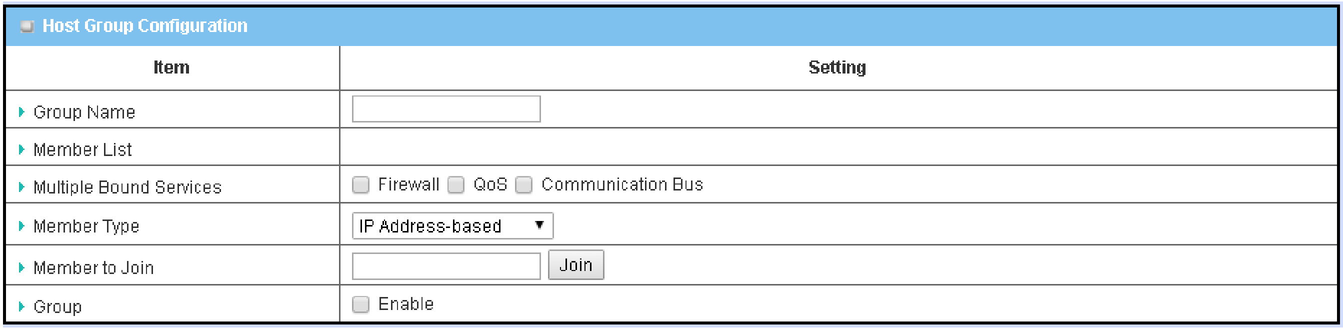
Host Grouping

Go to System > Grouping > Host Grouping Tab



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

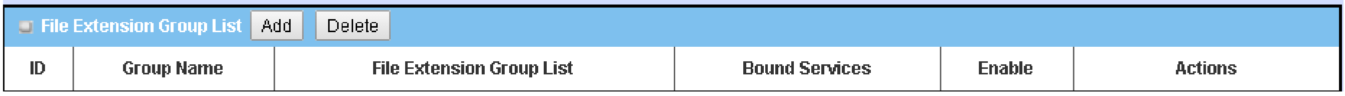
Host Group Configuration		
Item	**Value setting**	**Description**
Group Name	1. String format can be any text 2. A Must filled setting	Enter a group rule name. Enter a name that is easy for you to understand.
Member List	NA	This field is shown members contained in group.
Multiple Bound Services	The boxes are unchecked by default	Binding the services that group can be applied. If user enable the **Firewall**, the produced group can be used in firewall service. Same as by enable **Qos** and **Communication Bus**.
Member Type	A Must filled setting 2.	Define the member type of group. When **IP Address-based** is selected, only IP address can be added in **Member to Join.**

Index skipping is used to reserve slots for new function insertion, when required.

		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 member to the group in this field. Key the member in the blank and press the **Join** button to add. Each time can be add only one member.
Group	The box is unchecked by default	Enable the group that can be used in bound service.

File Extension Grouping

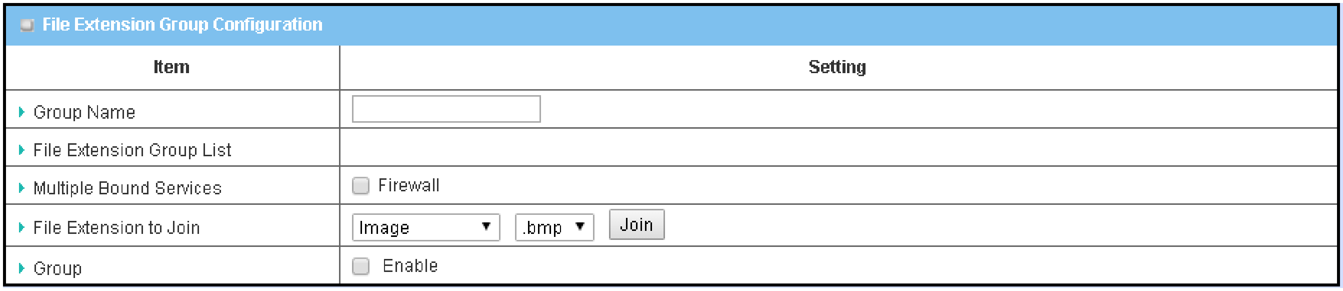
Go to System > Grouping > File Extension Grouping Tab



File Extension Group List

ID	Group Name	File Extension Group List	Bound Services	Enable	Actions

When Add button is applied File Extension Group Configuration screen will appear.



File Extension Group Configuration

Item	Setting
Group Name	
File Extension Group List	
Multiple Bound Services	□ Firewall
File Extension to Join	Image ▼ .bmp ▼ Join
Group	□ Enable

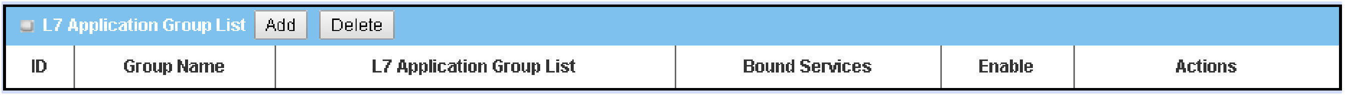
File Extension Group Configuration		
Item	**Value setting**	**Description**
Group Name	1. String format can be any text 2. A Must filled setting	Enter a group rule name. Enter a name that is easy for you to understand.
File Extension Group List	N/A	This field is shown members contained in group.
Multiple Bound Services	The boxes are unchecked by default	Binding the services that group can be applied. If user enable the **Firewall**, the produced group can be used in firewall service.
File Extension to Join	A Must filled setting	Define the member type of group. There are six member types can be selected. When **Image** is selected, there are total eleven file extension names about image can be added. Include .bmp, .gif, .jpeg, .jpg, .jpg2, .jp2, .pcx, .pig, .png, .tif and .tiff. When **Video** is selected, there are total twelve file extension names

Index skipping is used to reserve slots for new function insertion, when required.

		about video can be added. Include .asf, .avi, .mov, .mpeg, .mpg, .mp4, .rm, .wmv, .3gp, .3gpp, .3gpp2 and .3g2. When **Audio** is selected, there are total eleven file extension names about audio can be added. Include .aac, .au, .mp3, .m4a, .m4p, .ogg, .ra, .ram, .vox, .wav and .wma. When **Java** is selected, there are total ten file extension names about java can be added. Include .class, .jad, .jar, .jav, .java, .jcm, .js, .jse, .jsp and .jtk. When **Compression** is selected, there are total ten file extension names about compression can be added. Include .ace, .ari, .bzip2, .bz2, .cab, .gz, .gzip, .rar, .sit and .zip. When **Execution** is selected, there are total eight file extension names about execution can be added. Include .bas, .bat, .com, .exe, .inf, .pif, .reg, .scr.
Group	The box is unchecked by default	Enable the group that can be used in bound service.

L7 Application Grouping

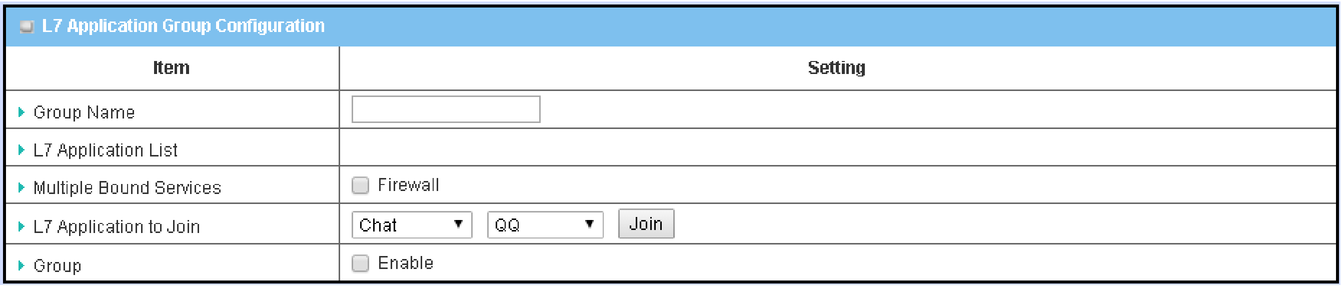
Go to System > Grouping > L7 Application Grouping Tab



L7 Application Group List Add Delete

ID	Group Name	L7 Application Group List	Bound Services	Enable	Actions

When Add button is applied L7 Application Group Configuration screen will appear.



L7 Application Group Configuration

Item	Setting
Group Name	
L7 Application List	
Multiple Bound Services	□ Firewall
L7 Application to Join	Chat ▼ QQ ▼ Join
Group	□ Enable

L7 Application Group Configuration		
Item	**Value setting**	**Description**
Group Name	1. String format can be any text 2. A Must filled setting	Enter a group rule name. Enter a name that is easy for you to understand.
L7 Application List	N/A	This field is shown members contained in group.

Index skipping is used to reserve slots for new function insertion, when required.

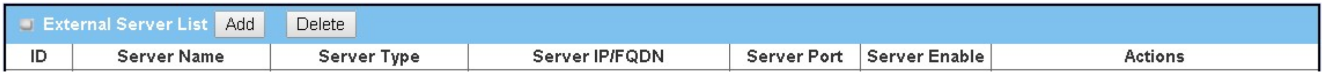
Multiple Bound Services	The boxes are unchecked by default	Binding the services that group can be applied. If user enable the **Firewall**, the produced group can be used in firewall service.
L7 Application to Join	A Must filled setting	Define the member type of group. There are four member types can be selected. When **Chat** is selected, there are total four Chat application can be added. Include QQ, Skype, Facebook, Aliww. When **P2P** is selected, there are total seven P2P application can be added. Include BT, eDonkey, eMule, Shareaza, HTTP. Multiple Thread Download, Thunder, Baofeng. When **Proxy** is selected, there are three proxy application can be added. Include HTTP Proxy, SOCKS 4 and 5 Proxy. When **Streaming** is selected, there are total five streaming application can be added. Include MMS, RTSP, PPLive, PPStream and Qvod.
Group	The box is unchecked by default	Enable the group that can be used in bound service.

9.9 External Servers

The External Servers setting allows user to add external server.

Create external server

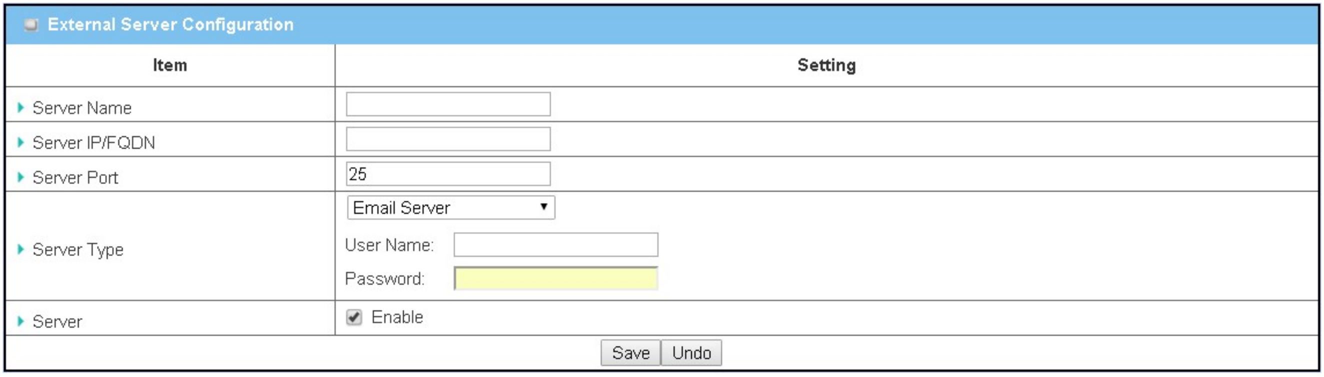
Go to System > External Servers > External Servers



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 IP/FQDN	
Server Port	25
Server Type	Email Server ▾ User Name: Password:
Server	☑ Enable

Save Undo

Index skipping is used to reserve slots for new function insertion, when required.

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 server to the Server Type. **Email Server** (A Must filled setting) When **Email Server** is selected, it means the option External Servers is set email server. **Server Port** will be set 25 by default. **User Name** (String format: any text) **Password** (String format: any text) Then check **Enable** box to add this server. **Syslog Server** (A Must filled setting) When **Syslog Server** is selected, it means the option External Servers is set Syslog Server. **Server Port** will be set 514 by default. Then check **Enable** box to add this server. **RADIUS Server** (A Must filled setting) When **RADIUS Server** is selected, it means the option External Servers is set RADIUS Server. **Server Port** will be set 1812 by default. **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. Then check **Enable** box to add this server.

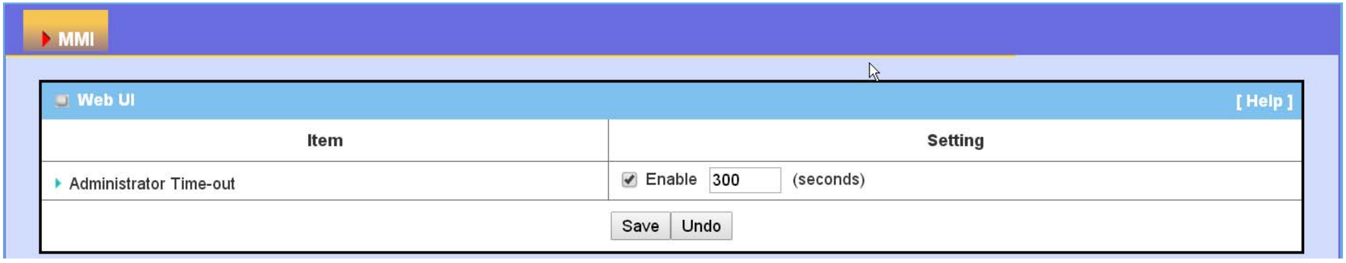
		Active Directory Server (A Must filled setting) When **Active Directory Server** is selected, it means the option External Servers is set Active Directory Server. **Server Port** will be set 389 by default. **Domain** (String format: any text) Then check **Enable** box to add this server. **LDAP Server** (A Must filled setting) When **LDAP Server** is selected, it means the option External Servers is set LDAP Server. **Server Port** will be set 389 by default. **Base DN** (String format: any text) **Identity** (String format: any text) **Password** (String format: any text) Then check **Enable** box to add this server. **UAM Server** (A Must filled setting) When **UAM Server** is selected, it means the option External Servers is set UAM Server. **Server Port** will be set 80 by default. **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) Then check **Enable** box to add this server. **TACACS+ Server** (A Must filled setting) When **TACACS+ Server** is selected, it means the option External Servers is set TACACS+ Server. **Server Port** will be set 49 by default. **Shared Key** (String format: any text) **Session Timeout** (String format: any number) The values must be between 1 and 60. Then check **Enable** box to add this server. **SCEP Server** (A Must filled setting) When **SCEP Server** is selected, it means the option External Servers is set SCEP Server. **Server Port** will be set 80 by default. **Path** (String format: any text, By default **cgi-bin** is filled) **Application** (String format: any text, By default **pkiclient.exe** is filled) Then check **Enable** box to add this server.
Server	The box is checked by default	When click Enable, it will enable this External Server.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings
Refresh	N/A	Click the **Refresh** button to refresh the external server list.

Index skipping is used to reserve slots for new function insertion, when required.

9.b MMI

This is the gateway's web-based utility access which allows administrator to access the gateway for management. The gateway's web-based utility automatically logs out the administrator when the idle time has elapsed. The setting allows administrator to enable automatic logout and set the logout idle time. When the Time-out is disabled the system will not logout the administrator automatically.

Go to System > MMI > Web UI tab



Item	Setting
Administrator Time-out	☑ Enable 300 (seconds)

Web UI		
Item	**Value Setting**	**Description**
Administrator Time-out Enable	Default checked	Enable auto logout when maximum idle time elapsed.
Administrator Time-out	300s is set by default	Set maximum user idle time
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings