LTE Industrial Router

ICR-1601

CONFIGURATION MANUAL

ADVANTECH

Used Symbols

Danger – Information regarding user safety or potential damage to the router.

Attention – Problems that can arise in specific situations.

Information, notice – Useful tips or information of special interest.

Example – Example of function, command or script.

Advantech B+B SmartWorx s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Document No. MAN-0040-EN, revision from February 12, 2019. Released in the Czech Republic.

Contents

1. Introduction

Cellular router ICR-1601 is designed for wireless communication in the mobile networks that make use of traditional cellular technologies. The primary purpose of this router is its use in the newest Category 4 (Cat.4) services on the cellular LTE network.

LTE Category 4 (Cat.4) is the next step in 4G LTE device capability. Cat.4 rated ICR-1601 routers are capable of achieving better typical speeds in 4G coverage areas where the network is enabled with 20 MHz of contiguous spectrum. The peak downlink data rate for a Category 4 is approximately 150 Mbps. Also in the uplink, LTE Category 4 provides a peak data rate of 50 Mbps.

Below is the list of the main router's features:

- ***Compact design:*** Built-in LTE and configurable Ethernet WAN/LAN can provide Ethernet machine easy connection to internet/intranet by LTE or high reliable fail-over wired/LTE connection.
- **Dual SIM:** Embedded 3G/4G with configurable dual-SIM achieve location free multi-ISP fail-over requirement.
- ***Versatile Cellular:*** Preferred service selection can simplify uplink setting; toolkit function of data usage can control budget; configurable SMS command is useful and efficient for remote administration.
- ***Complete Network***: Built-in NAT/Port Forward/Routing/IPv6 are compatible to existing IP network.
- ***Highly Security:*** Various VPN protocol & scenario can setup secure intranet; built-in Firewall prevents malicious attacks; ACL & Authentication by MAC /User enhances secure access.
- ***Flexible Administration:*** Web UI is used for basic setting; programmable CLI and Command Script are used for advanced configuration; system can be managed by NMS based on TR-069.
- ***Smart Event Handing:*** Mechanism to manage action for pre-defined events by administrator. Events can be triggered or notified based on System/Interface status change, SMS, SNMP trap, or e-mail.

1.1 Basic HW Information

As a standard, the ICR-1601 router is equipped with two Fast Ethernet 10/100 Mbps interfaces, two readers for SIM cards and reader for MicroSD card (log storage). The router can be equipped with WiFi module or with GPS module. This router is supplied in a metal bracket casing. For more detail see *User Manual for ICR-1601* [2].

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

1.2 Installation & Maintenance Notice

1.2.1 System Requirements

Network Requirements	• A fast Ethernet RJ45 cable • 3G/4G cellular service subscription • IEEE 802.11b/g/n wireless client • 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

1.2.2 Warnings

- Only use the power adapter that comes with the package. Using a different voltage rating power adaptor is dangerous and may damage the product.

- Do not open or repair the case yourself. If the product is too hot, turn off the power immediately and have it repaired at a qualified service center.

- Place the product on a stable surface and avoid using this product and all accessories outdoors.

1.2.3 Hot Surface Caution

- The surface temperature for the metallic enclosure can be very high!

- Especially after operating for a long time, installed at a closed cabinet without air conditioning support, or in a high ambient temperature space.

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

1.3 Access to the Web Configuration

❗ **Attention!** Wireless transmissions work only when you activate the SIM card for data traffic and insert it into the router. Remove the power source before inserting the SIM card.

You may use the web interface to monitor, configure and manage the router. To do so, enter the router's IP address in your browser. The default address is http://192.168.1.1[1]. Please note that the DHCP server is enabled by default.

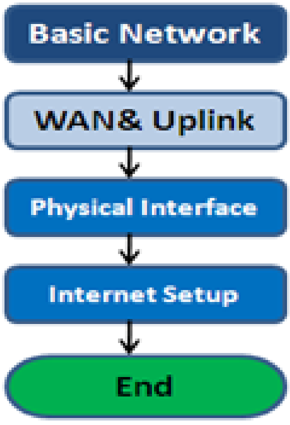
When you see the login page, enter the user name and password and then click *Login* button. The default username is "**admin**". The default password is "**admin**". Change the default password as soon as possible!

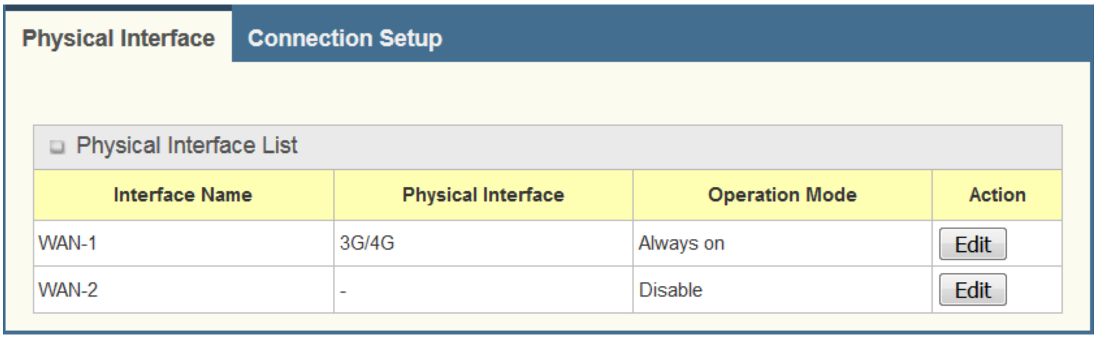
❗ For increased security of the network connected to the router, change the default router password.

[1] The default LAN IP address of this gateway is 192.168.1.1. If you change it, you need to login by using the new IP address.

2. Basic Network

2.1 WAN & Uplink



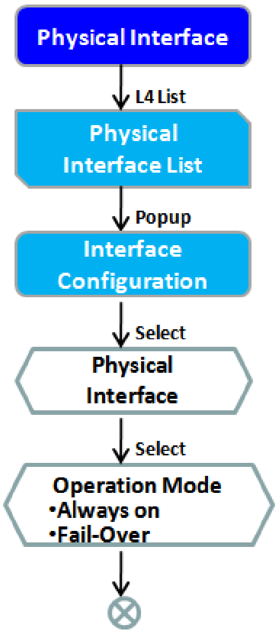


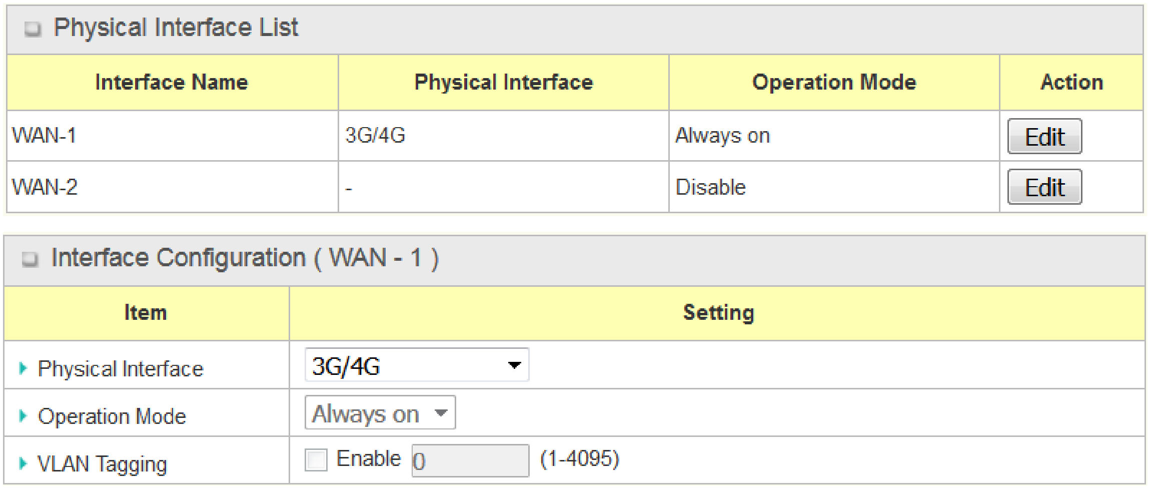
Physical Interface List

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

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

2.1.1 Physical Interface





Physical Interface List

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

Interface Configuration (WAN - 1)

Item	Setting
Physical Interface	3G/4G
Operation Mode	Always on
VLAN Tagging	□ Enable 0 (1-4095)

ICR-1601 routers are usually equipped with various WAN interfacess to support different WAN connection scenario for requirement. You can configure the WAN interface one by one to get proper internet connection setup. **Refer to the product specification for the available WAN interfaces in the product you purchased.**

The first step to configure one WAN interface is to specify which kind of connection media 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:

- **Ethernet WAN:** The router has one RJ45 WAN port that can be configured to be WAN connections. You can directly connect to external DSL modem or setup behind a firewall device.
- **3G/4G WAN:** The router has one built-in 3G/4G cellular as WAN connection. For each cellular WAN, there are 1 or 2 SIM cards to be inserted for special failover function.

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

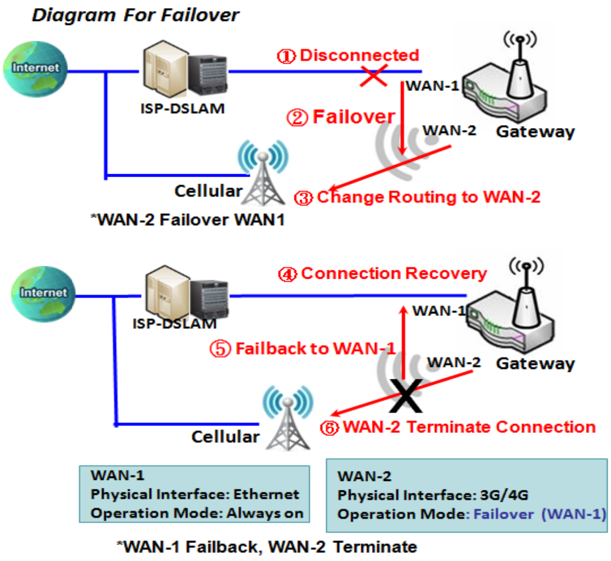
- **WiFi Uplink WAN**: For the product with WiFi Uplink function, one WiFi module can be configured to be WAN connections. For the WiFi module with Uplink function activated, you can further create some uplink profiles for ease of connecting to an uplink network.

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. When two or more WAN are established at "Always on" mode, outgoing data will through these WAN connections.

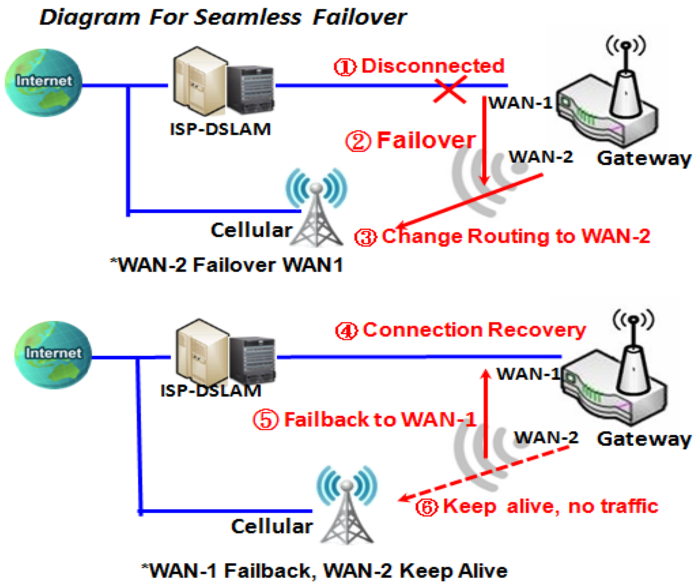
Failover:



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.

As shown in the diagram, WAN-2 is backup WAN for WAN-1. WAN-1 serves as the primary connection with operation mode "Always on". WAN-2 won’t be activated until WAN-1 disconnected. When WAN-1 connection is recovered back with a connection, it will take over data traffic again. At that time, WAN-2 connection will be terminated.

Seamless Failover:



In addition, there is a "Seamless" option for Failover operation mode. When seamless option is activated by checking on the "Seamless" box in configuration window, both the primary connection and the failover connection are started up after system rebooting. But only the primary connection executes the data transfer, while the failover one just keeps 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.

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

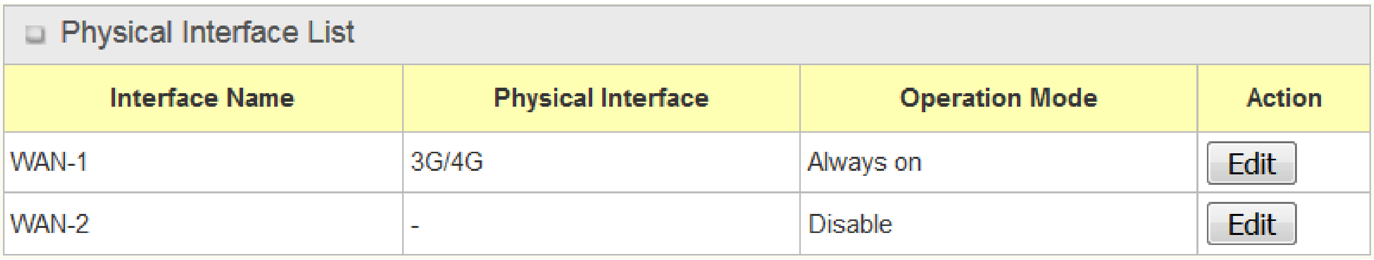
VLAN Tagging

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

Physical Interface Setting

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

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

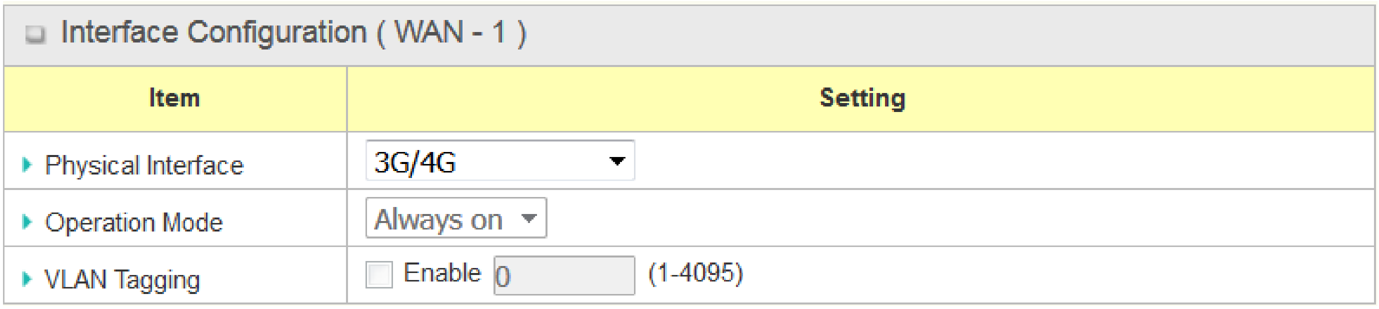


Physical Interface List

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

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

Interface Configuration:



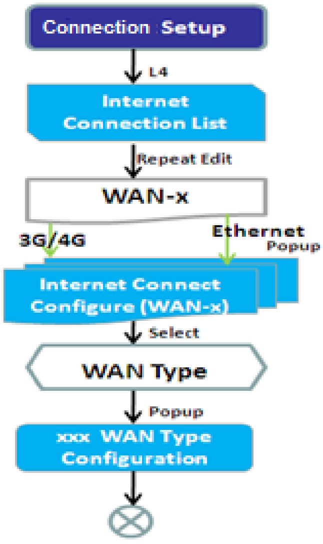
Interface Configuration (WAN - 1)

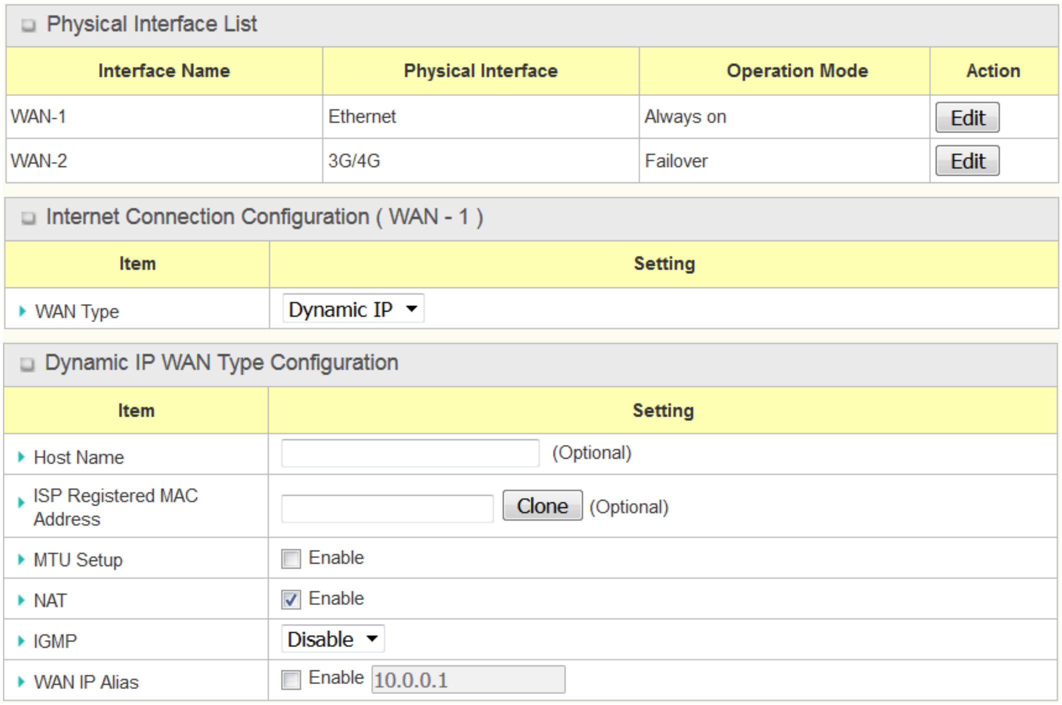
Item	Setting
Physical Interface	3G/4G ▾
Operation Mode	Always on ▾
VLAN Tagging	□ Enable 0 (1-4095)

Interface Configuration

Item	Value setting	Description
Physical Interface	1. A Must fill setting 2. WAN-1 is the primary interface and is factory set to Always on.	Select one expected interface from the available interface dropdown list. It can be **3G/4G**, **Ethernet** or **WiFi Module**. Depending on the router model, **Disable** and **Failover** options will be available only to multiple WAN routers. WAN-2 ~ WAN-4 interfaces are only available to multiple WAN router.
Operation Mode	A Must fill setting	Define the operation mode of the interface. Select **Always on** to make this WAN always active. Select **Disable** to disable this WAN interface. Select **Failover** to make this WAN a Failover WAN when the primary or the secondary WAN link failed. Then select the primary or the existed secondary WAN interface to switch Failover from. (Note: for WAN-1, only **Always on** option is available.)
VLAN Tagging	Optional setting	Check **Enable** box to enter tag value provided by your ISP. Otherwise uncheck the box. ***Value Range***: 1 ~ 4095. Note: This feature is NOT available for 3G/4G WAN connection.

2.1.2 Connection Setup





Physical Interface List

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

Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	Dynamic IP

Dynamic IP WAN Type Configuration

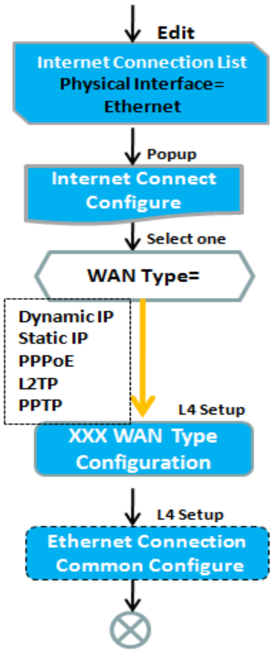
Item	Setting
Host Name	(Optional)
ISP Registered MAC Address	Clone (Optional)
MTU Setup	□ Enable
NAT	☑ Enable
IGMP	Disable
WAN IP Alias	□ Enable 10.0.0.1

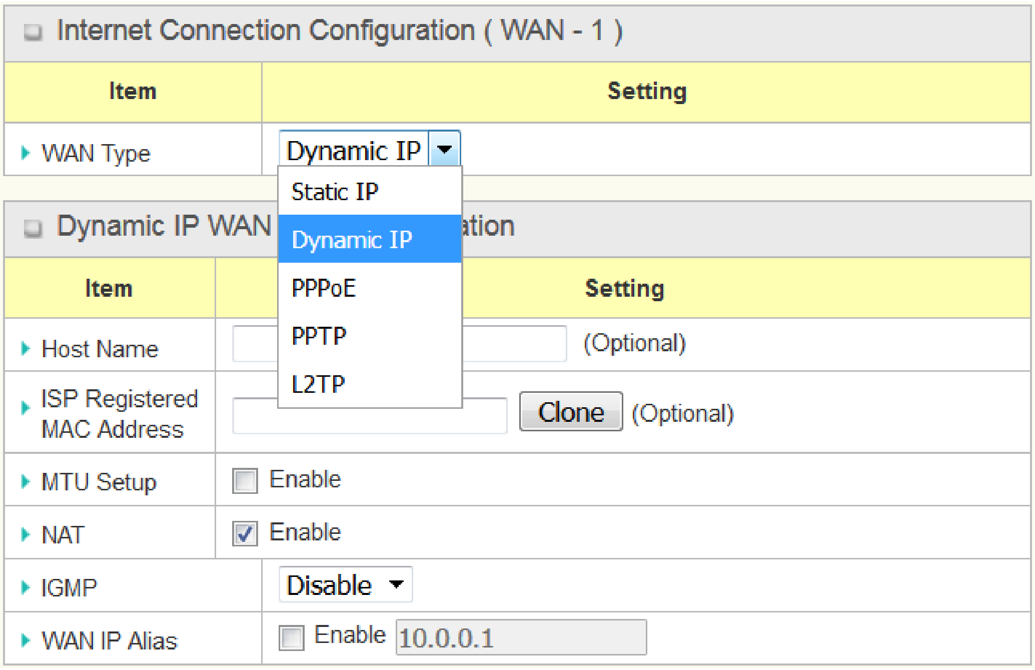
After specifying the physical interface for each WAN connection, administrator must configure their connection profile to meet the dial in process of ISP, so that all client hosts in the Intranet of the router can access the Internet.

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

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

Internet Connection List - Ethernet WAN





Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	Dynamic IP ▾

Static IP
Dynamic IP
PPPoE
PPTP
L2TP

Dynamic IP WAN ation

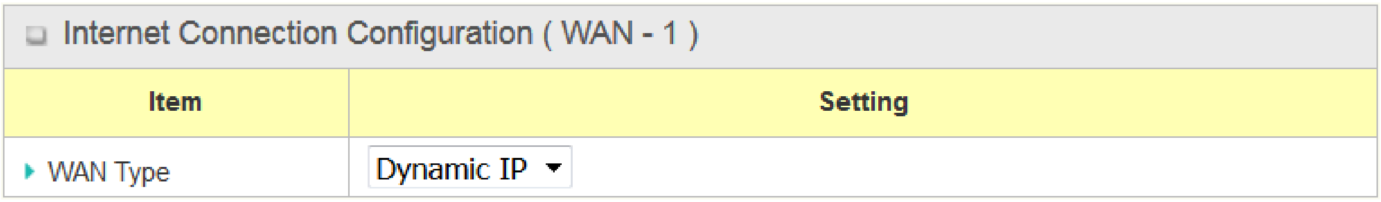
Item	Setting
Host Name	(Optional)
ISP Registered MAC Address	Clone (Optional)
MTU Setup	□ Enable
NAT	☑ Enable
IGMP	Disable ▾
WAN IP Alias	□ Enable 10.0.0.1

WAN Type for Ethernet Interface:

Ethernet is the most common WAN and uplink interface for ICR-1601 routers. Usually it is connected with xDSL or cable modem for you to setup the WAN connection. There are various WAN types to connect with ISP:

- **Static IP:** Select this option if ISP provides a fixed IP to you when you subscribe the service. Usually is more expensive but very important for cooperate requirement.
- **Dynamic IP:** The assigned IP address for the WAN by a DHCP server is different every time. It is cheaper and usually for consumer use.
- **PPP over Ethernet:** As known as PPPoE. This WAN type is widely used for ADSL connection. IP is usually different for every dial up.
- **PPTP:** This WAN type is popular in some countries, like Russia.
- **L2TP :** This WAN type is popular in some countries, like Israel.

Configure Ethernet WAN Setting



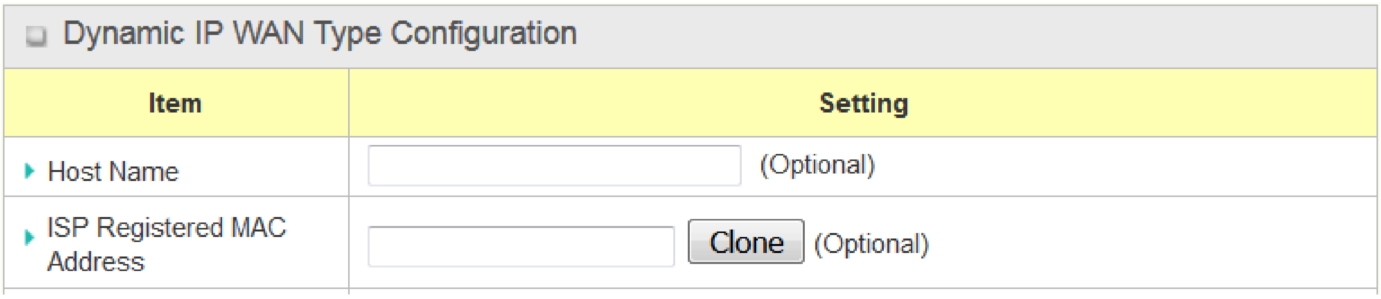
Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	Dynamic IP

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

WAN Type = Dynamic IP

When you select it, "Dynamic IP WAN Type Configuration" will appear. Items and setting is explained below.



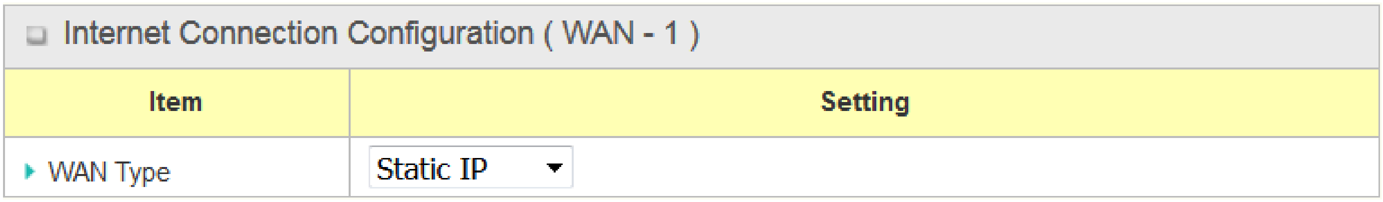
Dynamic IP WAN Type Configuration

Item	Setting
Host Name	(Optional)
ISP Registered MAC Address	Clone (Optional)

Dynamic IP WAN Type Configuration

Item	Value setting	Description
Host Name	An optional setting	Enter the host name provided by your 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.

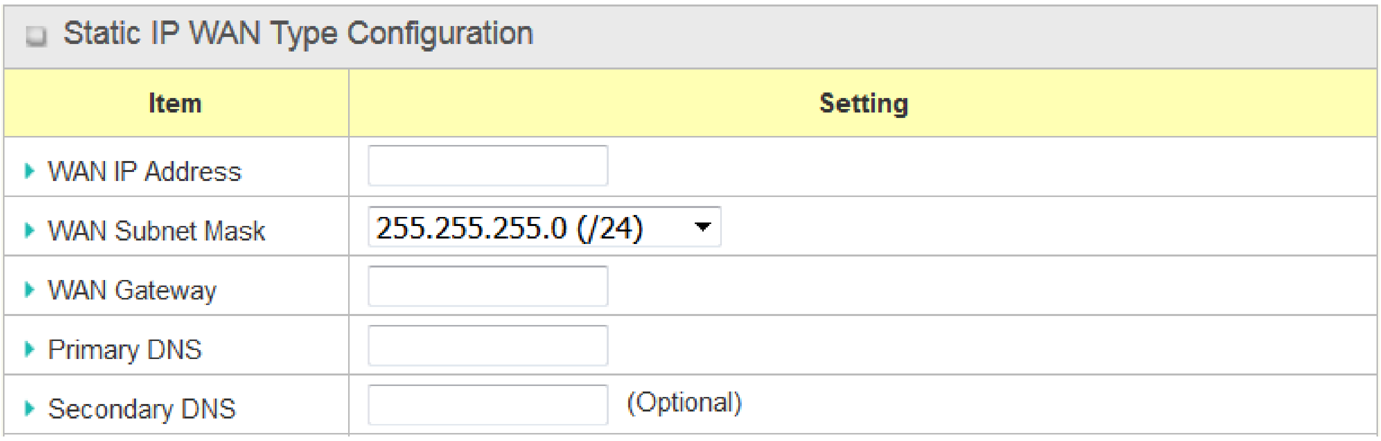
WAN Type = Static IP



Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	Static IP

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

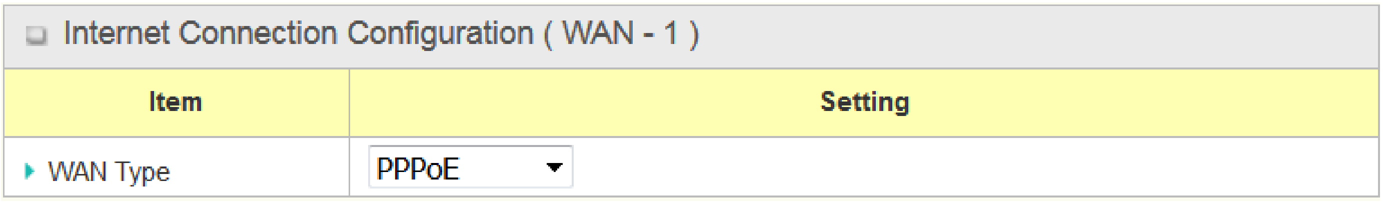


Static IP WAN Type Configuration

Item	Setting
WAN IP Address	
WAN Subnet Mask	255.255.255.0 (/24)
WAN Gateway	
Primary DNS	
Secondary DNS	(Optional)

Static IP WAN Type Configuration		
Item	**Value setting**	**Description**
WAN IP Address	A Must filled setting	Enter the WAN IP address given by your Service Provider
WAN Subnet Mask	A Must filled setting	Enter the WAN subnet mask given by your Service Provider
WAN Gateway	A Must filled setting	Enter the WAN gateway IP address given by your Service Provider
Primary DNS	A Must filled setting	Enter the primary WAN DNS IP address given by your Service Provider
Secondary DNS	An optional setting	Enter the secondary WAN DNS IP address given by your Service Provider

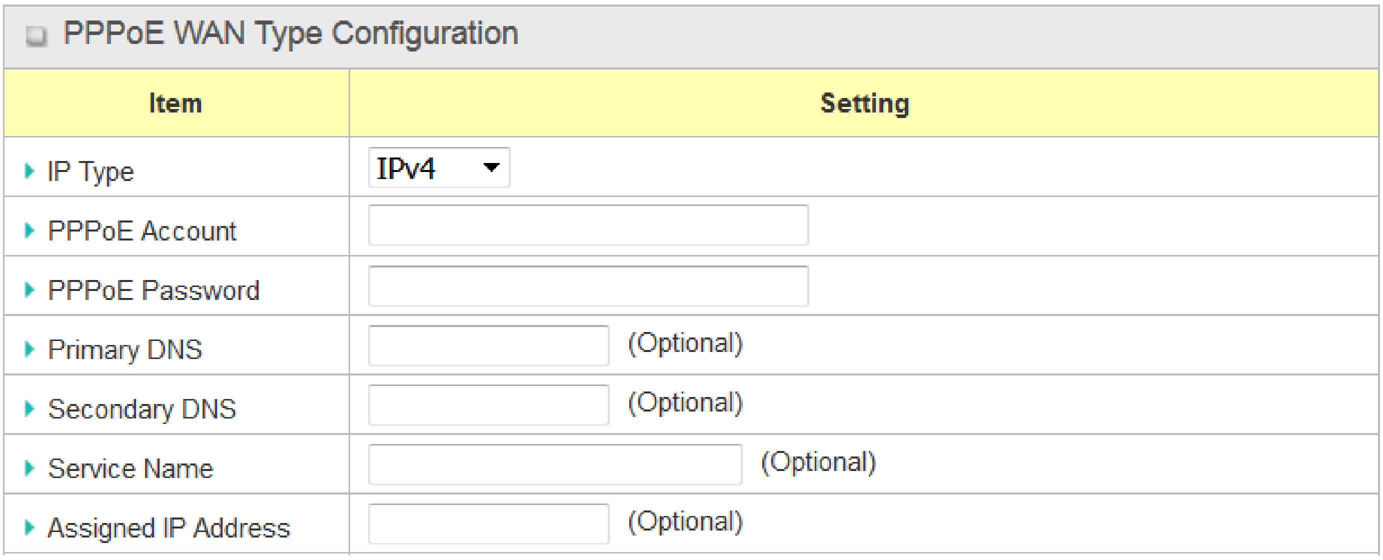
WAN Type = PPPoE



Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	PPPoE

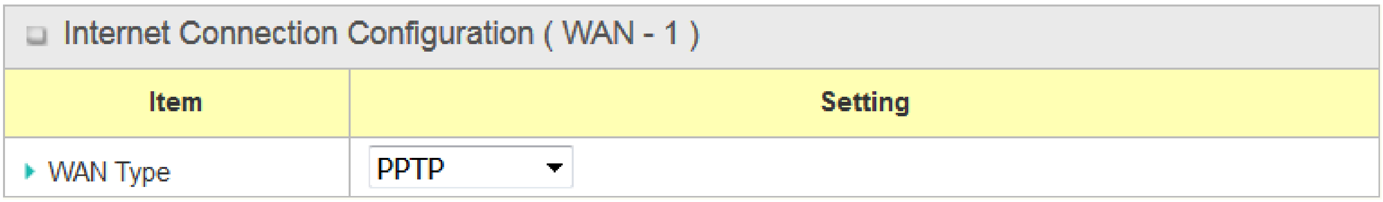
When you select it, "PPPoE WAN Type Configuration" will appear. Items and setting is explained below.



PPPoE WAN Type Configuration

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

PPPoE WAN Type Configuration		
Item	**Value setting**	**Description**
PPPoE Account	A Must filled setting	Enter the PPPoE User Name provided by your Service Provider.
PPPoE Password	A Must filled setting	Enter the PPPoE password provided by your Service Provider.
Primary DNS	An optional setting	Enter the IP address of Primary DNS server.
Secondary DNS	An optional setting	Enter the IP address of Secondary DNS server.
Service Name	An optional setting	Enter the service name if your ISP requires it
Assigned IP Address	An optional setting	Enter the IP address assigned by your Service Provider.

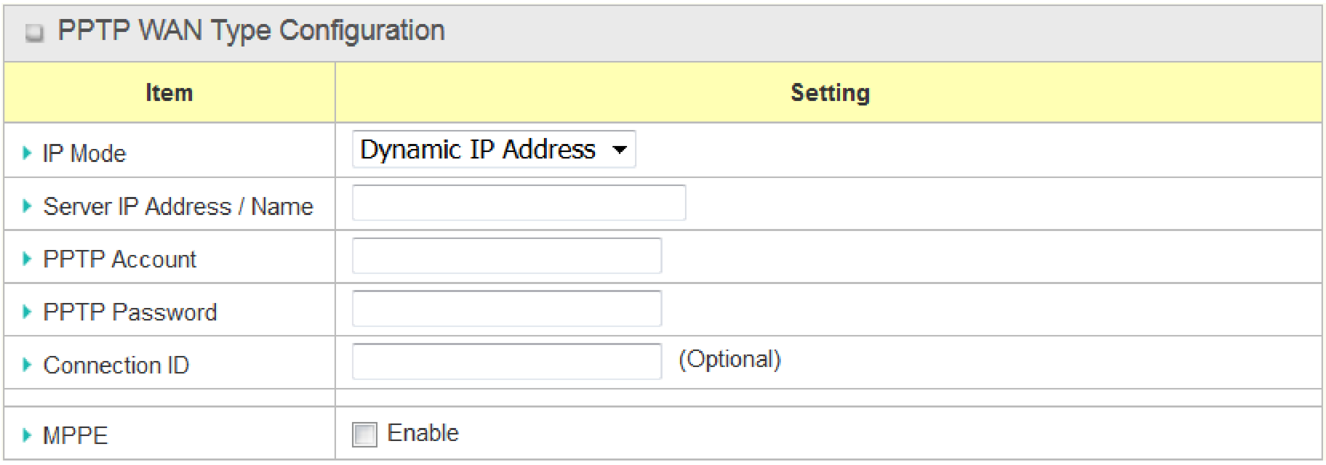


Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	PPTP

WAN Type = PPTP

When you select it, "PPTP WAN Type Configuration" will appear. Items and setting is explained below.



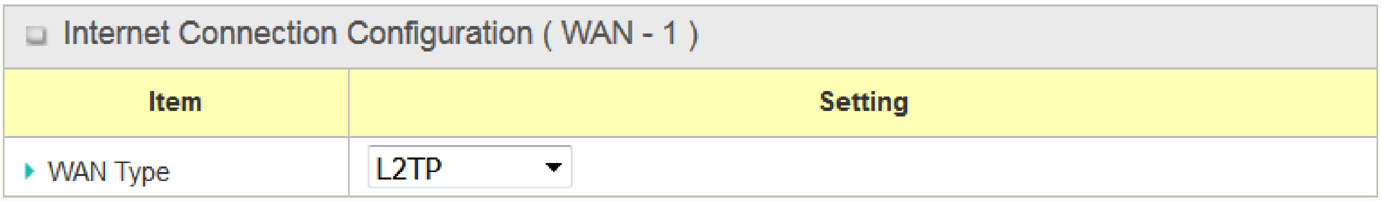
PPTP WAN Type Configuration

Item	Setting
IP Mode	Dynamic IP Address
Server IP Address / Name	
PPTP Account	
PPTP Password	
Connection ID	(Optional)
MPPE	□ Enable

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

Connection ID	An optional setting	Enter a name to identify the PPTP connection.
MPPE	An optional setting	Select **Enable** to enable MPPE **(**Microsoft Point-to-Point Encryption) security for PPTP connection.

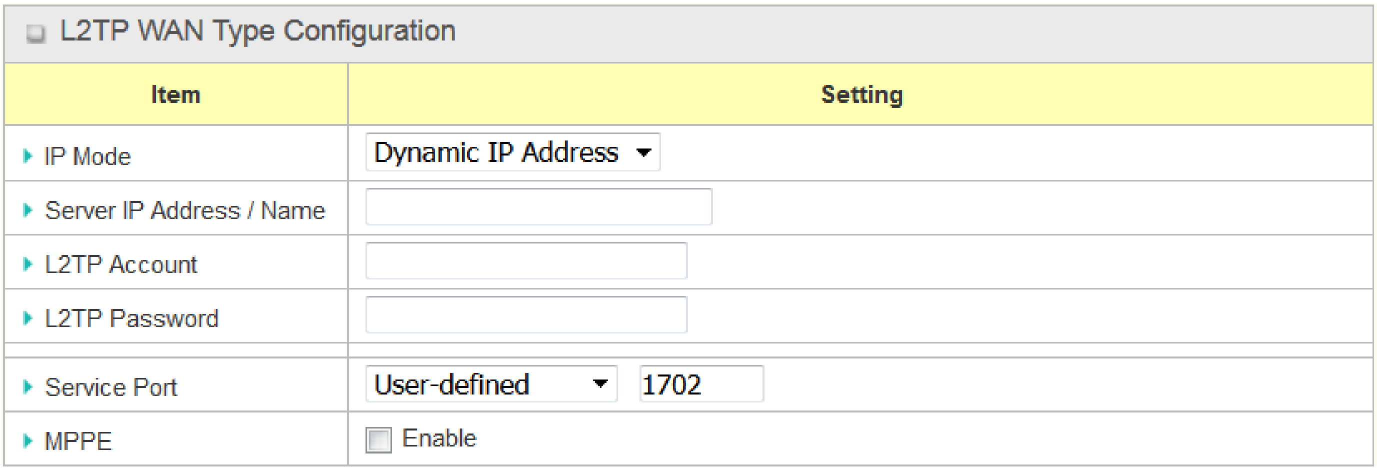
WAN Type = L2TP



Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	L2TP ▾

When you select it, "L2TP WAN Type Configuration" will appear. Items and setting is explained below**.**



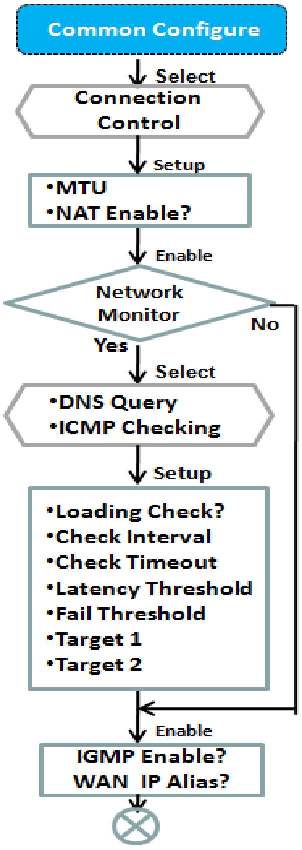
L2TP WAN Type Configuration

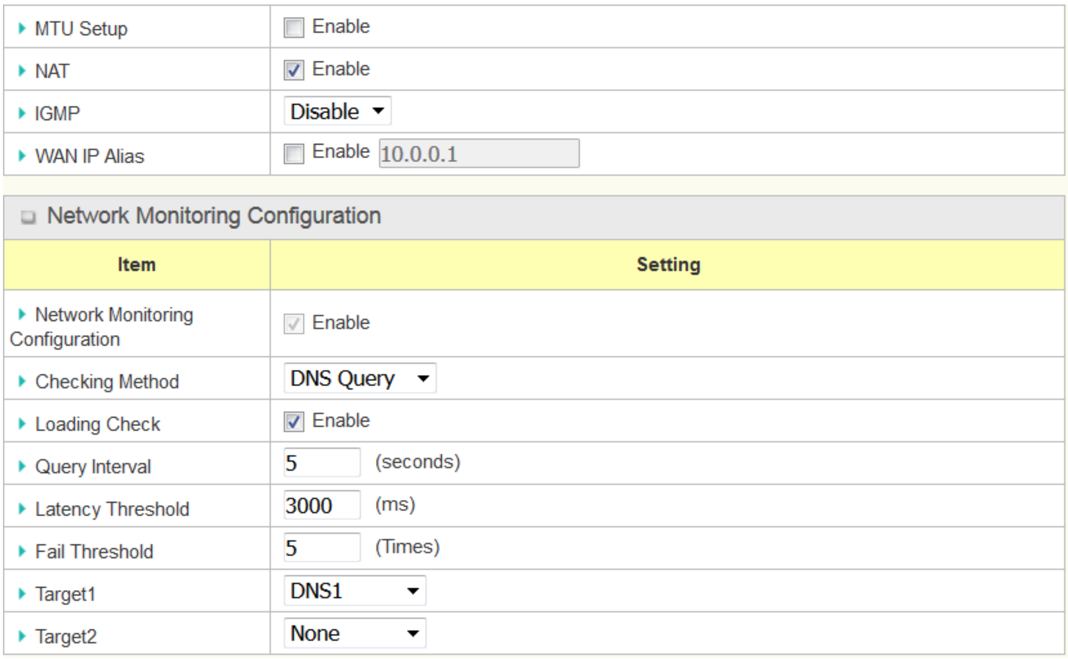
Item	Setting
IP Mode	Dynamic IP Address ▾
Server IP Address / Name	
L2TP Account	
L2TP Password	
Service Port	User-defined ▾ 1702
MPPE	□ Enable

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

Service Port	A Must filled setting	Enter the service port that the Internet service. There are three options can be selected : ● **Auto:** Port will be automatically assigned. ● **1701 (For Cisco)**: Set service port to port 1701 to connect to CISCO server. ● **User-defined**: enter a service port provided by your Service Provider.
MPPE	An optional setting	Select **Enable** to enable MPPE (Microsoft Point-to-Point Encryption) security for PPTP connection.

Ethernet Connection Common Configuration





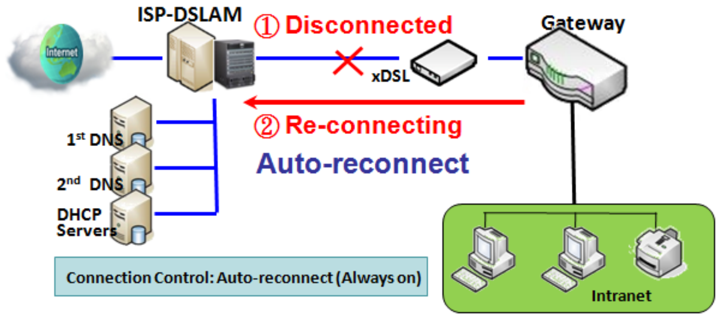
MTU Setup	□ Enable
NAT	☑ Enable
IGMP	Disable ▾
WAN IP Alias	□ Enable 10.0.0.1

Network Monitoring Configuration

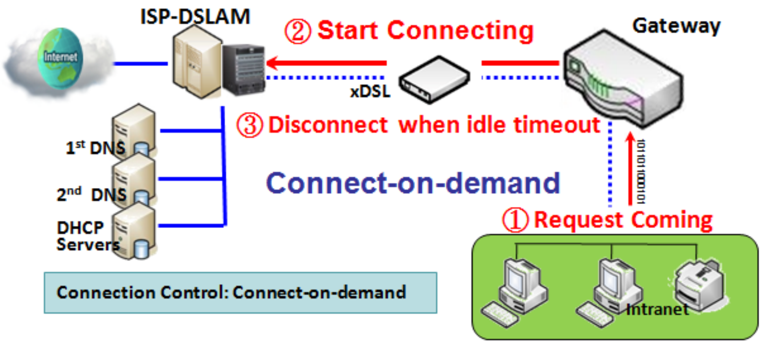
Item	Setting
Network Monitoring Configuration	☑ Enable
Checking Method	DNS Query ▾
Loading Check	☑ Enable
Query Interval	5 (seconds)
Latency Threshold	3000 (ms)
Fail Threshold	5 (Times)
Target1	DNS1 ▾
Target2	None ▾

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

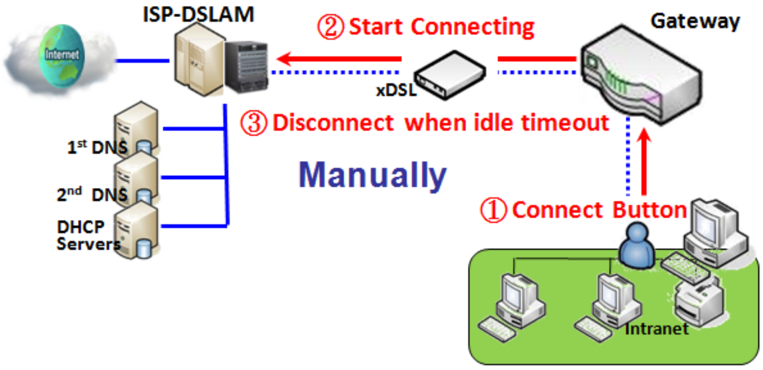
Connection Control



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



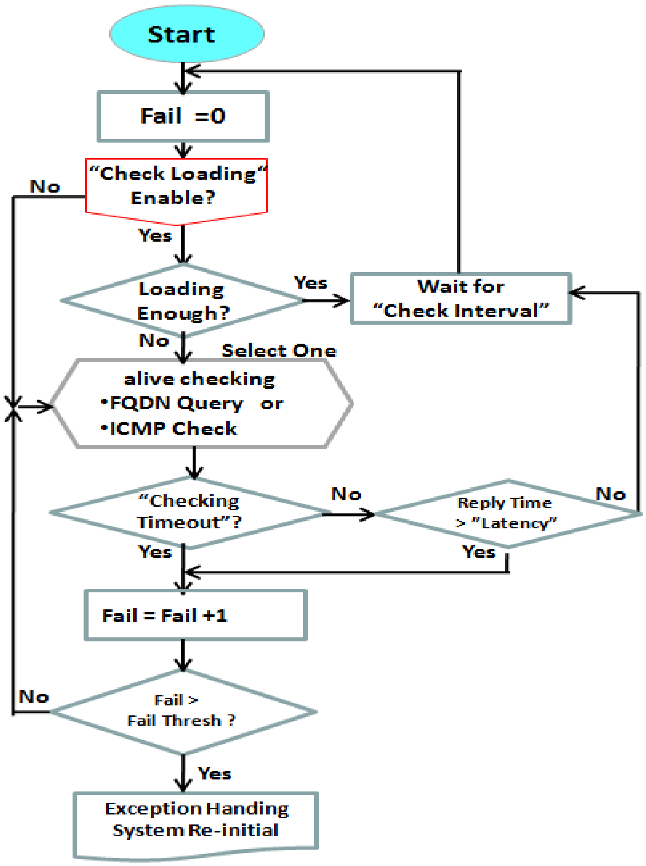
Connect-on-demand: This gateway won't start to establish Internet connection until local data is going to be sent to WAN side. After normal data transferring between LAN and WAN sides, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time.



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

Please 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)".

Network Monitoring



It is necessary to monitor connection status continuous. To do it, "ICMP Check" and "FQDN Query" are used to check. When there is traffic of connection, checking packet will waste bandwidth. Response time of replied packets may also increase. To avoid "Network Monitoring" work abnormally, enabling "Checking Loading" option will stop connection check when there is traffic. It will wait for another "Check Interval" and then check loading again.

When you do "Network Monitoring", if reply time longer than "Latency" or even no response longer than "Checking Timeout", "Fail" count will be increased. If it is continuous and "Fail" count is more than "Fail Threshold", gateway will do exception handing process and re-initial this connection again. Otherwise, network monitoring process will be start again.

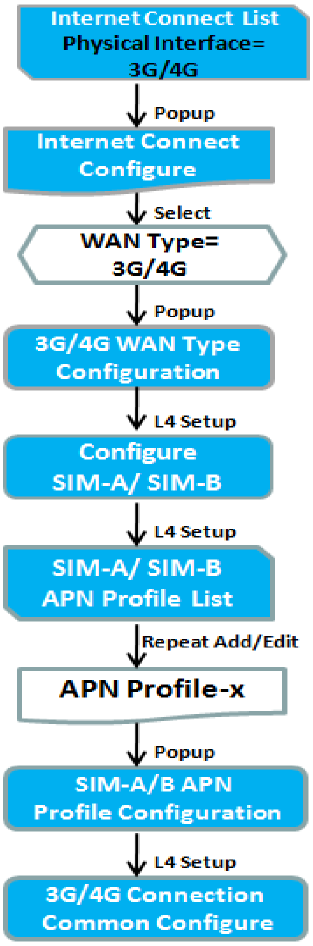
Set up "Ethernet Common Configuration"

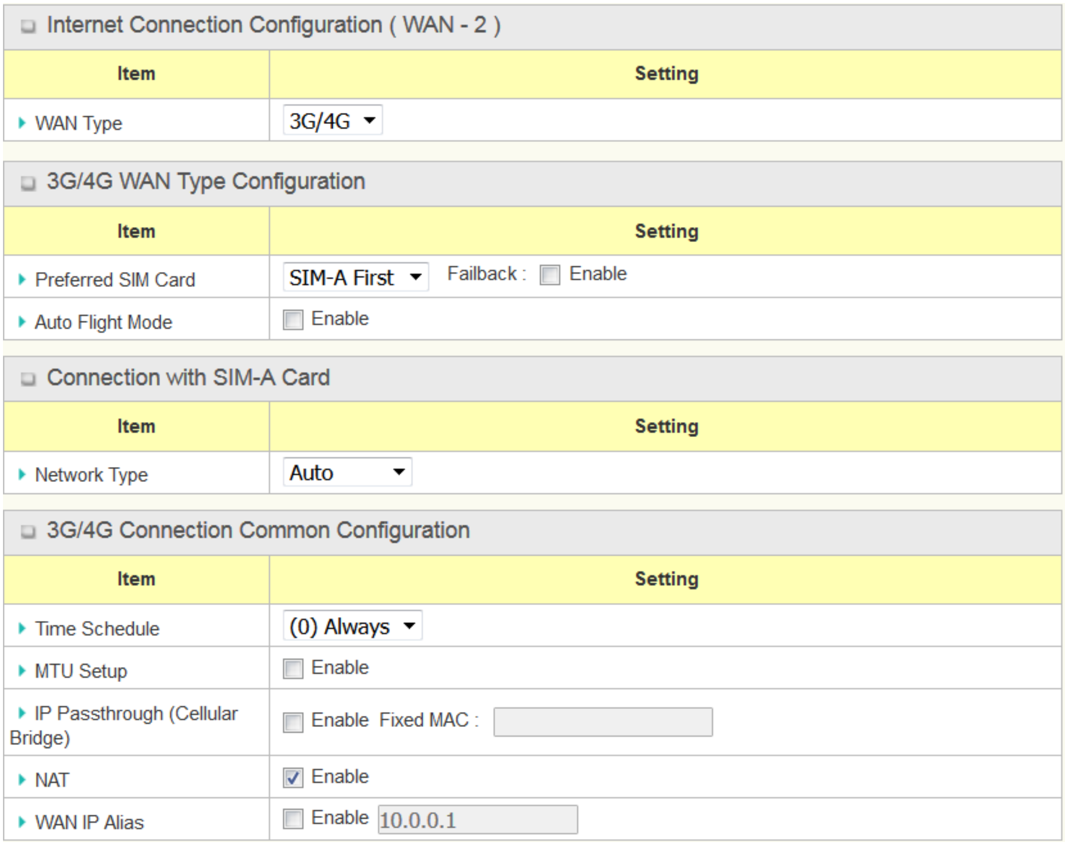
Ethernet WAN Common Configuration		
Item	**Value setting**	**Description**
Connection Control	A Must filled setting	There are three connection modes. • **Auto-reconnect** enables the router to always keep the Internet connection on. • **Connect-on-demand** enables the router to automatically re-establish Internet connection as soon as user attempts to access the Internet. Internet connection will be disconnected when it has been inactive for a specified idle time. • **Connect Manually** allows user to connect to Internet manually**.** Internet connection will be inactive after it has been inactive for specified idle time.
Maximum Idle Time	1. An Optional setting 2. By default **600** seconds is filled-in	Specify the maximum Idle time setting to disconnect the internet connection when the connection idle timed out. ***Value Range***: 300 ~ 86400. **Note**: This field is available only when **Connect-on-demand** or **Connect Manually** is selected as the connection control scheme.

MTU Setup	1. An Optional setting 2. **Uncheck** by default	Check the Enable box to enable the MTU (Maximum Transmission Unit) limit, and specify the **MTU** for the 3G/4G connection. **MTU** refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. ***Value Range***: 1200 ~ 1500.
MTU Setup	1. A Must filled setting 2. **Auto** (value zero) is set by default 3. Manual set range 1200~1500	**MTU** refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. When set to **Auto** (value '0'), the router selects the best MTU for best Internet connection performance.
NAT	1. An optional setting 2. NAT is enabled by default	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
Network Monitoring	1. An optional setting 2. Enabled by default	When the Network Monitoring feature is enabled, the gateway will use DNS Query or ICMP to periodically check Internet connection –connected or disconnected. ● Choose either **DNS Query** or **ICMP Checking** to detect WAN link. With **DNS Query,** the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. With **ICMP Checking,** the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2. ● **Loading Check** Enable Loading Check allows the router to ignore unreturned DNS Queries or ICMP requests when WAN bandwidth is fully occupied. This is to prevent false link-down status. ● **Check Interval** defines the transmitting interval between two DNS Query or ICMP checking packets. ● **Check Timeout** defines the timeout of each DNS query/ICMP. ● **Latency Threshold** defines the tolerance threshold of responding time. ● **Fail Threshold** specifies the detected disconnection before the router recognize the WAN link down status. Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged. ● **Target1** (**DNS1** set by default**)** specifies the first target of sending DNS query/ICMP request. ■ **DNS1**: set the primary DNS to be the target. ■ **DNS2**: set the secondary DNS to be the target. ■ **Gateway**: set the Current gateway to be the target. ■ **Other Host**: enter an IP address to be the target. ● **Target2** (**None** set by default**)** specifies the second target of sending DNS query/ICMP request. ■ **None**: to disable **Target2.** ■ **DNS1**: set the primary DNS to be the target. ■ **DNS2**: set the secondary DNS to be the target. ■ **Gateway**: set the Current gateway to be the target. ■ **Other Host**: enter an IP address to be the target.
IGMP	1. A Must filled setting 2. Disable is set by default	Enable IGMP (Internet Group Management Protocol) would enable the router to listen to IGMP packets to discover which interfaces are connected to which device. The router uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.

WAN IP Alias	1. An optional setting 2. **Uncheck** by default	Enable **WAN IP Alias** then enter the IP address provided by your service provider. **WAN IP Alias** is used by the device router and is treated as a second set of WAN IP to provide dual WAN IP address to your LAN network.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

Internet Connection – 3G/4G WAN


Internet Connect List
Physical Interface= 3G/4G
Popup
Internet Connect Configure
Select
WAN Type= 3G/4G
Popup
3G/4G WAN Type Configuration
L4 Setup
Configure SIM-A/ SIM-B
L4 Setup
SIM-A/ SIM-B APN Profile List
Repeat Add/Edit
APN Profile-x
Popup
SIM-A/B APN Profile Configuration
L4 Setup
3G/4G Connection Common Configure



Internet Connection Configuration (WAN - 2)

Item	Setting
WAN Type	3G/4G

3G/4G WAN Type Configuration

Item	Setting
Preferred SIM Card	SIM-A First Failback : □ Enable
Auto Flight Mode	□ Enable

Connection with SIM-A Card

Item	Setting
Network Type	Auto

3G/4G Connection Common Configuration

Item	Setting
Time Schedule	(0) Always
MTU Setup	□ Enable
IP Passthrough (Cellular Bridge)	□ Enable Fixed MAC :
NAT	☑ Enable
WAN IP Alias	□ Enable 10.0.0.1

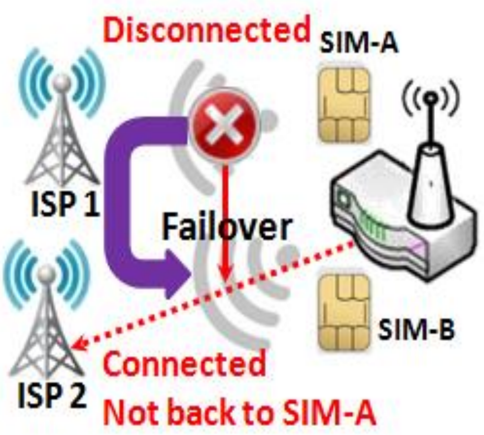
Preferred SIM Card – Dual SIM Fail Over

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

SIM-A/SIM-B only

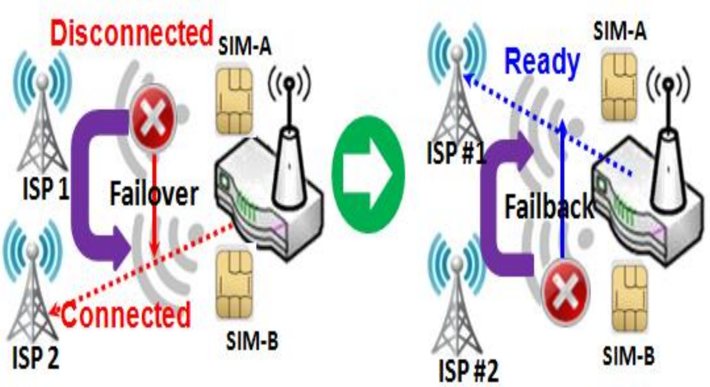
When “SIM-A Only” or “SIM-B Only” is used, the specified SIM slot card is the only one to be used for negotiation parameters between gateway device and cellular ISP.

SIM-A / SIM-B first without enable Failback



By default, “SIM-A First” scenario is used to connect to cellular ISP for data transfer. In the case of “SIM-A First” or “SIM-B First” scenario, the gateway will try to connect to the Internet by using SIM-A or SIM-B card first. And when the connection is broken, the gateway will switch to use the other SIM card 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.

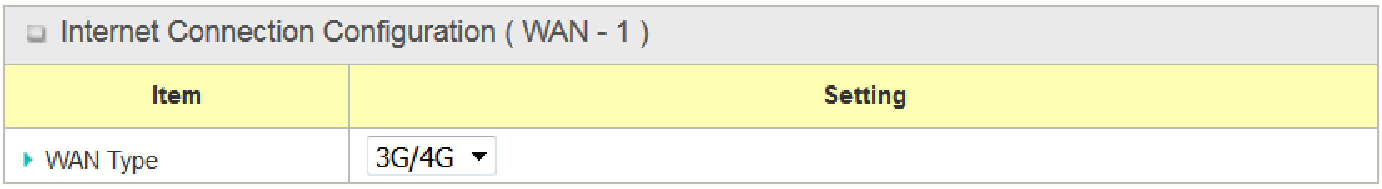
SIM-A / SIM-B first with Failback enable



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

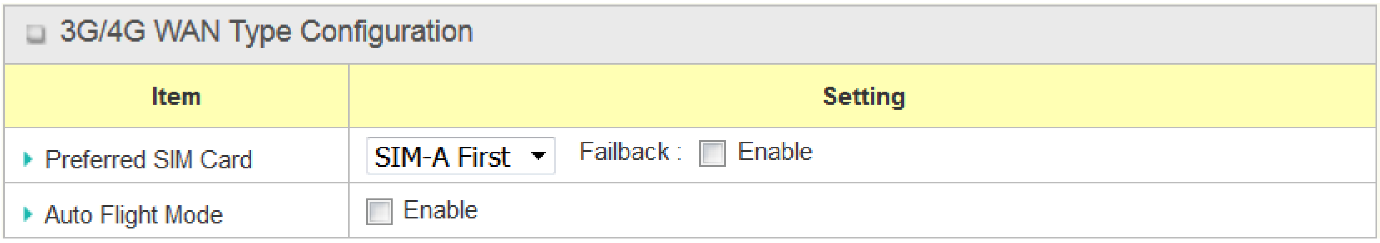
Configure 3G/4G WAN Setting

When **Edit** button is applied, **Internet Connection Configuration**, and **3G/4G WAN Configuration** screens will appear.



Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	3G/4G ▾



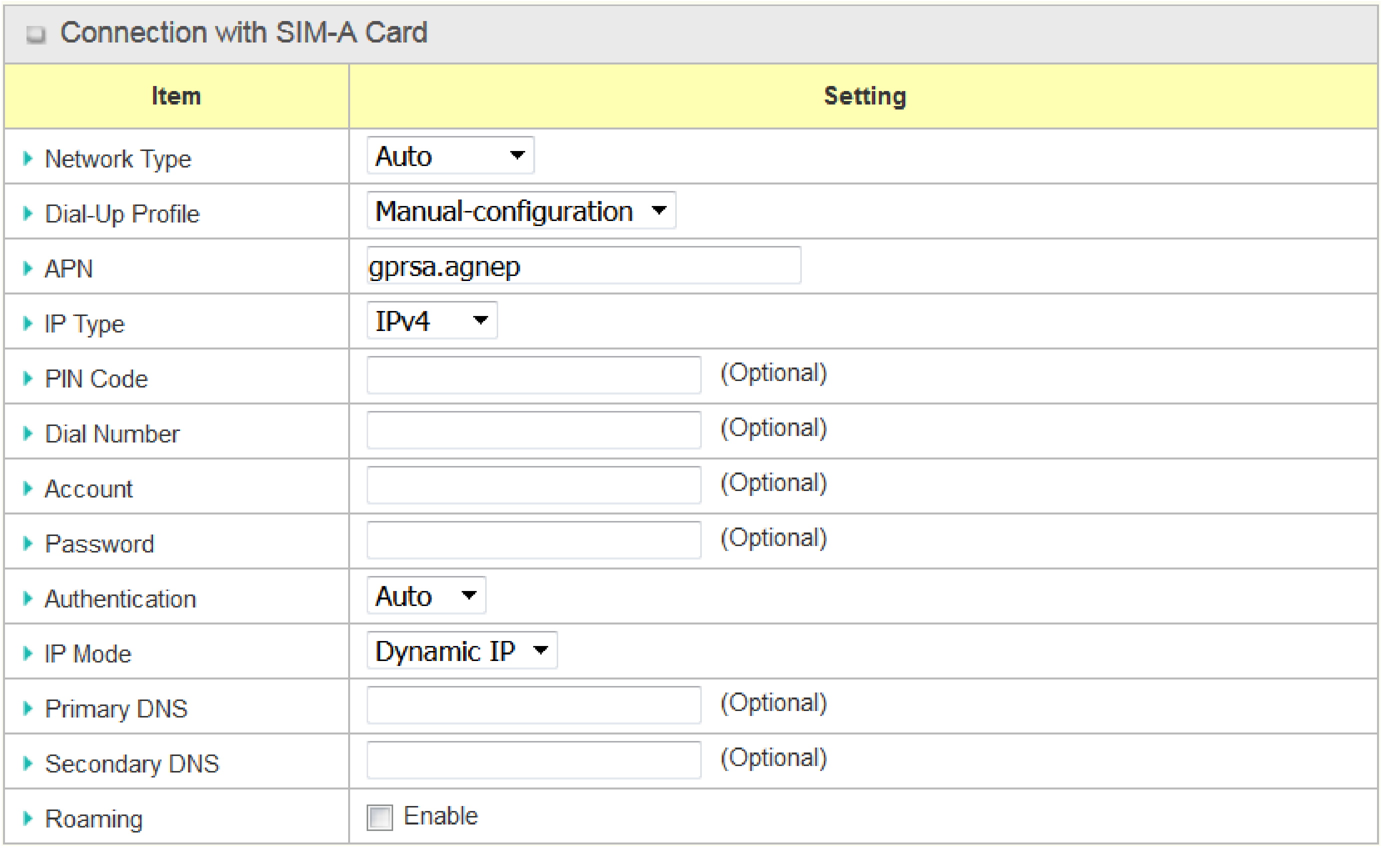
3G/4G WAN Type Configuration

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

3G/4G Connection Configuration		
Item	**Value setting**	**Description**
WAN Type	1. A Must filled setting 2. **3G/4G** is set by default.	From the dropdown box, select Internet connection method for 3G/4G WAN Connection. Only **3G/4G** is available.
Preferred SIM Card	1. A Must filled setting 2. By default **SIM-A First** is selected 3. **Failback** is unchecked by default	Choose which SIM card you want to use for the connection. When **SIM-A First** or **SIM-B First** is selected, it means the connection is built first by using SIM A/SIM B. And if the connection is failed, it will change to the other SIM card and try to dial again, until the connection is up. When **SIM-A only** or **SIM-B only** is selected, it will try to dial up only using the SIM card you selected. When **Failback** is checked, it means if the connection is dialed-up not using the main SIM you selected, it will failback to the main SIM and try to establish the connection periodically. **Note_1**: For the product with single SIM design, only **SIM-A Only** option is available. **Note_2**: **Failback** is available only when **SIM-A First** or **SIM-B First** is selected.
Auto Flight Mode	The box is unchecked by default	Check the **Enable** box to activate the function. By default, if you disabled the **Auto Flight Mode**, the cellular module will always occupy a physical channel with cellular tower. It can get data connection instantly, and receive managing SMS all the time on required. If you enabled the **Auto Flight Mode**, the gateway will pop up a message *“Flight mode will cause cellular function to be malfunctioned, when the data session is offline.”,* and it will make the cellular module into flight mode and disconnected with cellular tower physically. In, addition, whenever the cellular module is going to be used for data connection to backup the failed primary connection, the cellular module will be active to connect with cellular tower and get the data connection for use, It takes few more seconds. **Note**: Keep it unchecked unless your cellular ISP asked the connected gateway to enable the Auto Flight Mode.

Configure SIM-A / SIM-B Card

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



Connection with SIM-A Card

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

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

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

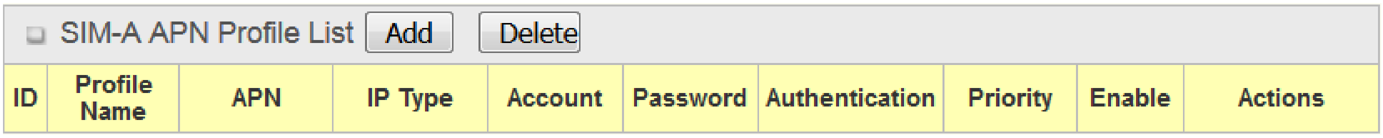
Connection with SIM-A/-B Card		
Item	**Value setting**	**Description**
Network Type	1. A Must filled setting 2. By default **Auto** is selected	Select **Auto** to register a network automatically, regardless of the network type. Select **2G Only** to register the 2G network only. Select **2G Prefer** to register the 2G network first if it is available. Select **3G only** to register the 3G network only. Select **3G Prefer** to register the 3G network first if it is available. Select **LTE only** to register the LTE network only. **Note**: Options may be different due to the specification of the module.

Dial-Up Profile	1. A Must filled setting 2. By default **Manual-configuration** is selected	Specify the type of dial-up profile for your 3G/4G network. It can be **Manual-configuration**, **APN Profile List**, or **Auto-detection**. Select **Manual-configuration** to set **APN** (Access Point Name), **Dial Number**, **Account**, and **Password** to what your carrier provides. Select **APN Profile List** to set more than one profile to dial up in turn, until the connection is established. It will pop up a new filed, please go to **Basic Network > WAN & Uplink > Internet Setup > SIM-A APN Profile List** for details. Select **Auto-detection** to automatically bring out all configurations needed while dialing-up, by comparing the IMSI of the SIM card to the record listed in the manufacturer's database. **Note_1:** You are highly recommended to select the **Manual** or **APN Profile List** to specify the network for your subscription. Your ISP always provides such network settings for the subscribers. **Note_2:** If you select **Auto-detection,** it is likely to connect to improper network, or failed to find a valid APN for your ISP.
APN	1. A Must filled setting 2. String format : any text	Enter the **APN** you want to use to establish the connection. This is a must-filled setting if you selected **Manual-configuration** as dial-up profile scheme.
IP Type	1. A Must filled setting 2. By default **IPv4** is selected	Specify the IP type of the network service provided by your 3G/4G network. It can be **IPv4**, **IPv6**, or **IPv4/6**.
PIN code	1. An Optional setting 2. String format : integer	Enter the PIN (Personal Identification Number) code if it needs to unlock your SIM card.
Dial Number, Account, Password	1. An Optional setting 2. String format : any text	Enter the optional **Dial Number**, **Account**, and **Password** settings if your ISP provided such settings to you. Note: These settings are only displayed when Manual-configuration is selected.
Authentication	1. A Must filled setting 2. By default **Auto** is selected	Select **PAP** (Password Authentication Protocol) and use such protocol to be authenticated with the carrier's server. Select **CHAP** (Challenge Handshake Authentication Protocol) and use such protocol to be authenticated with the carrier's server. When **Auto** is selected, it means it will authenticate with the server either **PAP** or **CHAP**.
IP Mode	1. A Must filled setting 2. By default **Dynamic IP** is selected	When **Dynamic IP** is selected, it means it will get all IP configurations from the carrier's server and set to the device directly. If you have specific application provided by the carrier, and want to set IP configurations on your own, you can switch to **Static IP** mode and fill in all parameters that required, such as IP address, subnet mask and gateway. **Note**: **IP Subnet Mask** is a must filled setting, and make sure you have the right configuration. Otherwise, the connection may get issues.
Primary DNS	1. An Optional setting 2. String format : IP address (IPv4 type)	Enter the IP address to change the primary DNS (Domain Name Server) setting. If it is not filled-in, the server address is given by the carrier while dialing-up.
Secondary DNS	1. An Optional setting 2. String format : IP address (IPv4 type)	Enter the IP address to change the secondary DNS (Domain Name Server) setting. If it is not filled-in, the server address is given by the carrier while dialing-up.

Roaming	The box is unchecked by default	Check the box to establish the connection even the registration status is roaming, not in home network. **Note**: It may cost additional charges if the connection is under roaming.

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

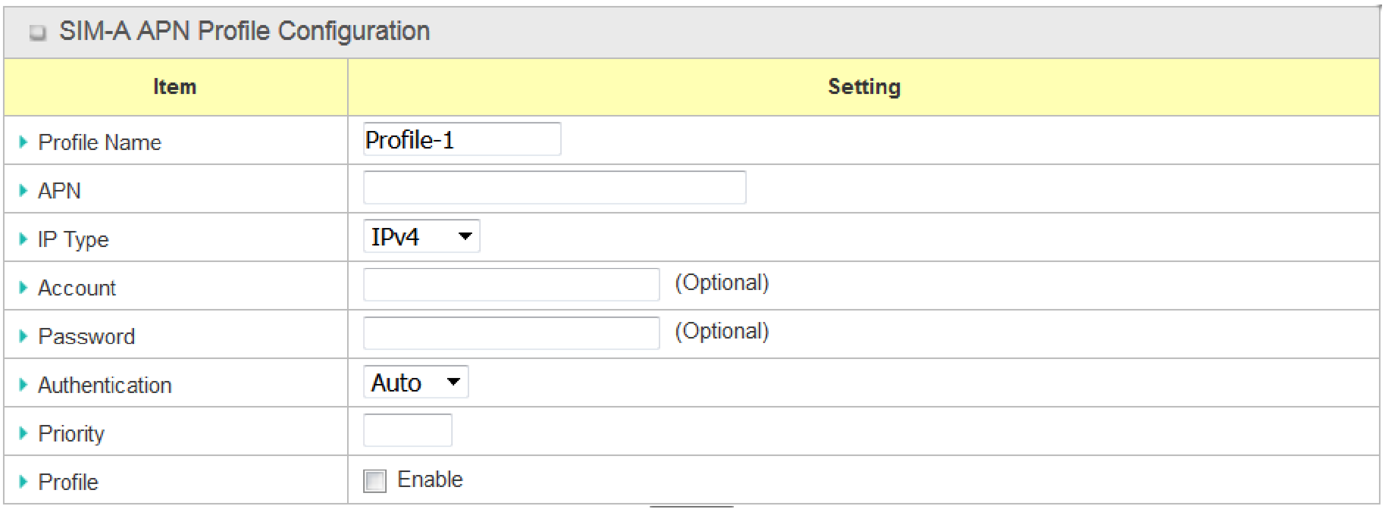
You can add a new APN profile for the connection, or modify the content of the APN profile you added. It is available only when you select **Dial-Up Profile** as **APN Profile List**.



SIM-A APN Profile List [Add] [Delete]

ID	Profile Name	APN	IP Type	Account	Password	Authentication	Priority	Enable	Actions

List all the APN profile you created, easily for you to check and modify. It is available only when you select **Dial-Up Profile** as **APN Profile List**. When **Add** button is applied, an **APN Profile Configuration** screen will appear.



SIM-A APN Profile Configuration

Item	Setting
Profile Name	Profile-1
APN	
IP Type	IPv4 ▾
Account	(Optional)
Password	(Optional)
Authentication	Auto ▾
Priority	
Profile	□ Enable

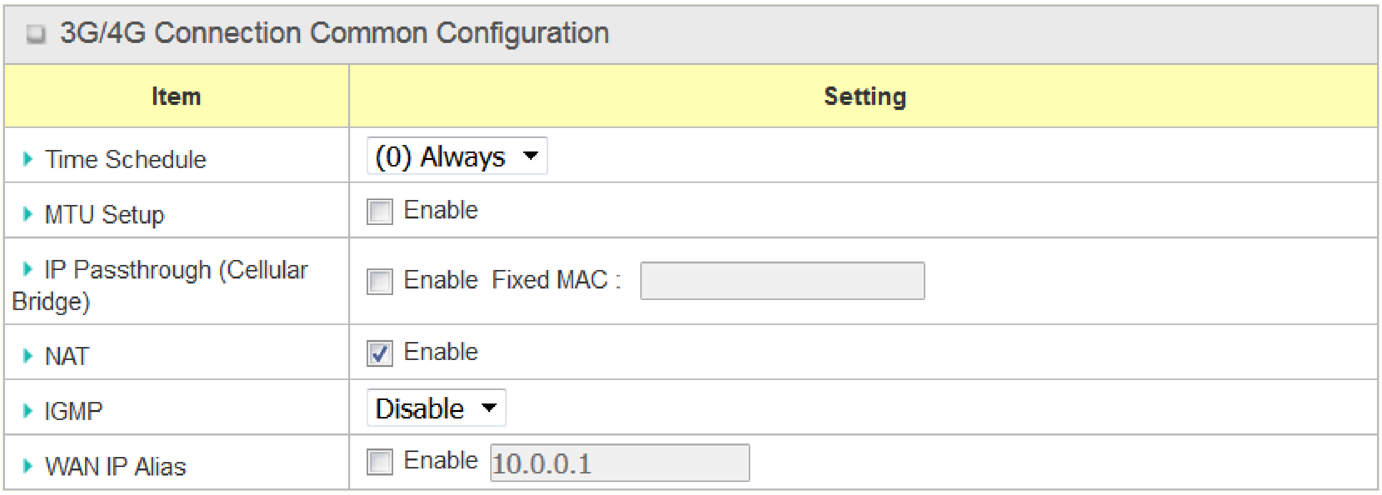
SIM-A/-B APN Profile Configuration

Item	Value setting	Description
Profile Name	1. By default **Profile-x** is listed 2. String format : any text	Enter the profile name you want to describe for this profile.
APN	String format : any text	Enter the **APN** you want to use to establish the connection.
IP Type	1. A Must filled setting 2. By default **IPv4** is selected	Specify the IP type of the network service provided by your 3G/4G network. It can be **IPv4**, **IPv6**, or **IPv4/6**.
Account	String format : any text	Enter the **Account** you want to use for the authentication. ***Value Range***: 0 ~ 53 characters.
Password	String format : any text	Enter the **Password** you want to use for the authentication.

Authentication	1. A Must filled setting 2. By default **Auto** is selected	Select the Authentication method for the 3G/4G connection. It can be **Auto**, **PAP**, **CHAP**, or **None**.
Priority	1. A Must filled setting 2. String format : integer	Enter the value for the dialing-up order. The valid value is from 1 to 16. It will start to dial up with the profile that assigned with the smallest number. ***Value Range***: 1 ~ 16.
Profile	The box is checked by default	Check the box to enable this profile. Uncheck the box to disable this profile in dialing-up action.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	N/A	When the **Back** button is clicked, the screen will return to the previous page.

Setup 3G/4G Connection Common Configuration

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

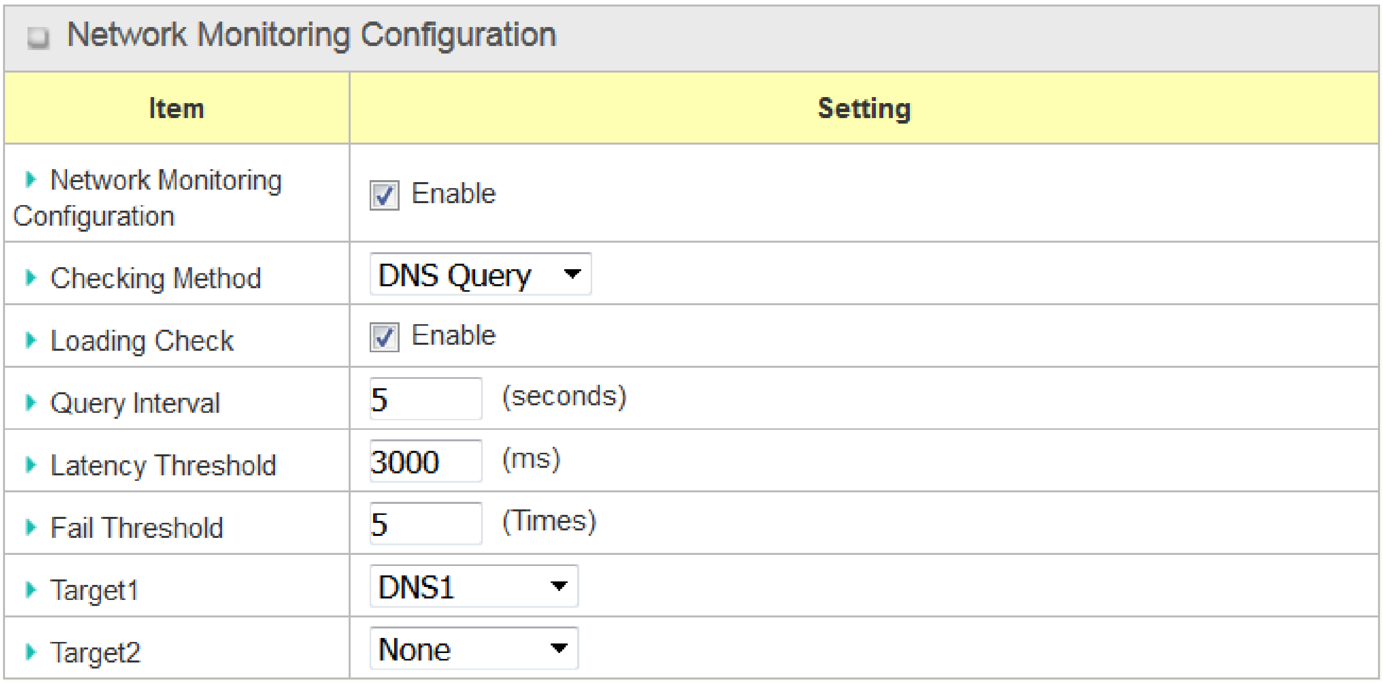


3G/4G Connection Common Configuration

Item	Setting
Time Schedule	(0) Always
MTU Setup	□ Enable
IP Passthrough (Cellular Bridge)	□ Enable Fixed MAC :
NAT	☑ Enable
IGMP	Disable
WAN IP Alias	□ Enable 10.0.0.1

3G/4G Connection Common Configuration		
Item	**Value setting**	**Description**
Connection Control	By default **Auto-reconnect** is selected	When **Auto-reconnect** is selected, it means it will try to keep the Internet connection on all the time whenever the physical link is connected. When **Connect-on-demand** is selected, it means the Internet connection will be established only when detecting data traffic. When **Connect Manually** is selected, it means you need to click the **Connect** button to dial up the connection manually. Please go to **Status > Basic Network > WAN & Uplink** tab for details. **Note**: If the WAN interface serves as the primary one for another WAN interface in Failover role(and vice versa), the Connection Control parameter will not be available on both WANs as the system must set it to “Auto-reconnect”
Maximum Idle Time	1. An Optional setting 2. By default **600** seconds is filled-in	Specify the maximum Idle time setting to disconnect the internet connection when the connection idle timed out. ***Value Range***: 300 ~ 86400.

		Note: This field is available only when **Connect-on-demand** or **Connect Manually** is selected as the connection control scheme.
Time Schedule	1. A Must filled setting 2. By default **(0) Always** is selected	When **(0) Always** is selected, it means this WAN is under operation all the time. Once you have set other schedule rules, there will be other options to select. Please go to **Object Definition > Scheduling** for details.
MTU Setup	1. An Optional setting 2. **Uncheck** by default	Check the Enable box to enable the MTU (Maximum Transmission Unit) limit, and specify the **MTU** for the 3G/4G connection. **MTU** refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. ***Value Range***: 1200 ~ 1500.
IP Pass-through (Cellular Bridge)	1. The box is unchecked by default 2. String format for **Fixed MAC**: MAC address, e.g. 00:50:18:aa:bb:cc	When **Enable** box is checked, it means the device will directly assign the WAN IP to the first connected local LAN client. However, when an optional **Fixed MAC** is filled-in a non-zero value, it means only the client with this MAC address can get the WAN IP address. **Note**: When the **IP Pass-through** is on, **NAT** and **WAN IP Alias** will be unavailable until the function is disabled again.
NAT	**Check** by default	Uncheck the box to disable **NAT** (Network Address Translation) function.
IGMP	By default **Disable** is selected	Select **Auto** to enable **IGMP** function. Check the **Enable** box to enable **IGMP Proxy**.
WAN IP Alias	1. Unchecked by default 2. String format: IP address (IPv4 type)	Check the box to enable **WAN IP Alias**, and fill in the IP address you want to assign.



Network Monitoring Configuration

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

Network Monitoring Configuration		
Item	**Value setting**	**Description**
Network Monitoring Configuration	1. An optional setting 2. Box is checked by default	Check the **Enable** box to activate the network monitoring function.
Checking Method	1. An Optional setting 2. **DNS Query** is set by default	Choose either **DNS Query** or **ICMP Checking** to detect WAN link. With **DNS Query**, the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. With **ICMP Checking**, the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2.
Loading Check	1. An optional setting 2. Box is checked by default	Check the **Enable** box to activate the loading check function. Enable Loading Check allows the gateway to ignore unreturned DNS queries or ICMP requests when WAN bandwidth is fully occupied. This is to prevent false link-down status.
Query Interval	1. A Must filled setting 2. By default **3** seconds is filled-in	**Query Interval** defines the transmitting interval between two DNS Query or ICMP checking packets.
Latency Threshold	1. A Must filled setting 2. By default **3000** ms is filled-in	**Latency Threshold** defines the tolerance threshold of responding time.
Fail Threshold	1. A Must filled setting 2. By default **10** times is filled-in	**Fail Threshold** specifies the detected disconnection before the router recognize the WAN link down status. Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged.
Target 1	1. An Optional filled setting 2. **DNS1** is selected by default	**Target1** specifies the first target of sending DNS query/ICMP request. **DNS1**: set the primary DNS to be the target. **DNS2**: set the secondary DNS to be the target. **Gateway**: set the Current gateway to be the target. **Other Host**: enter an IP address to be the target.
Target 2	1. An Optional filled setting 2. **None** is selected by default	**Target1** specifies the second target of sending DNS query/ICMP request. **None:** no second target is required. **DNS1**: set the primary DNS to be the target. **DNS2**: set the secondary DNS to be the target. **Gateway**: set the Current gateway to be the target. **Other Host**: enter an IP address to be the target.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

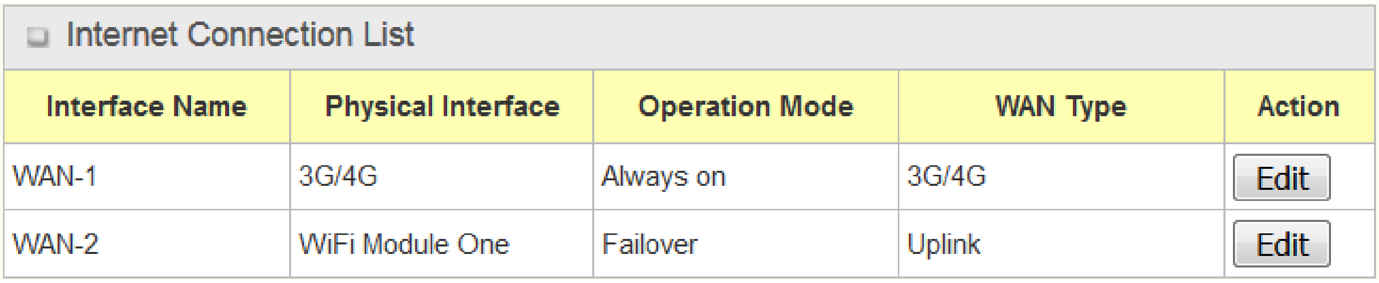
Internet Connection – WiFi Uplink WAN

If the device connects to Internet through WiFi Uplink, this section will help you to complete WiFi Uplink connection setup.

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

WiFi Uplink interface: The Uplink network is a wireless network, and the gateway can connect to the Uplink network through WiFi connection.

If you have the access permission to a certain wireless network, you can setup a WiFi Uplink connection by using the router device. This router can support 802.11n/g/b data connection, and it can connect to a wireless network (access point) under the regular infrastructure mode.

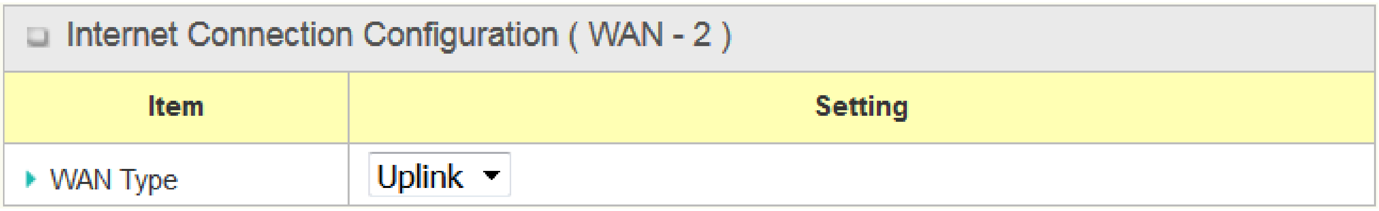


Internet Connection List

Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	3G/4G	Always on	3G/4G	Edit
WAN-2	WiFi Module One	Failover	Uplink	Edit

Configure WiFi Uplink Setting

When **Edit** button is applied, **Internet Connection Configuration** screen will appear. WAN-2 interface is used in this example.

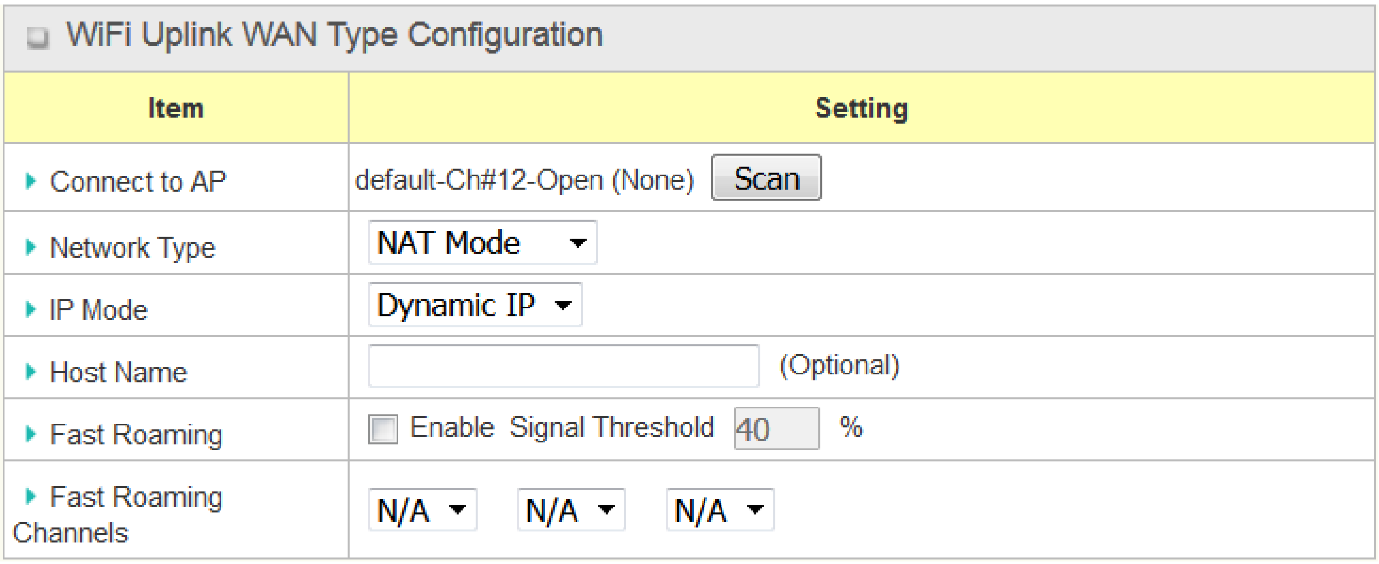


Internet Connection Configuration (WAN - 2)

Item	Setting
WAN Type	Uplink

Internet Connection Configuration		
Item	**Value setting**	**Description**
WAN Type	1. A Must filled setting. 2. **Uplink** is selected by default.	From the dropdown box, select Internet connection method for WiFi Uplink Connection. Only **Uplink** is available.

WiFi Uplink



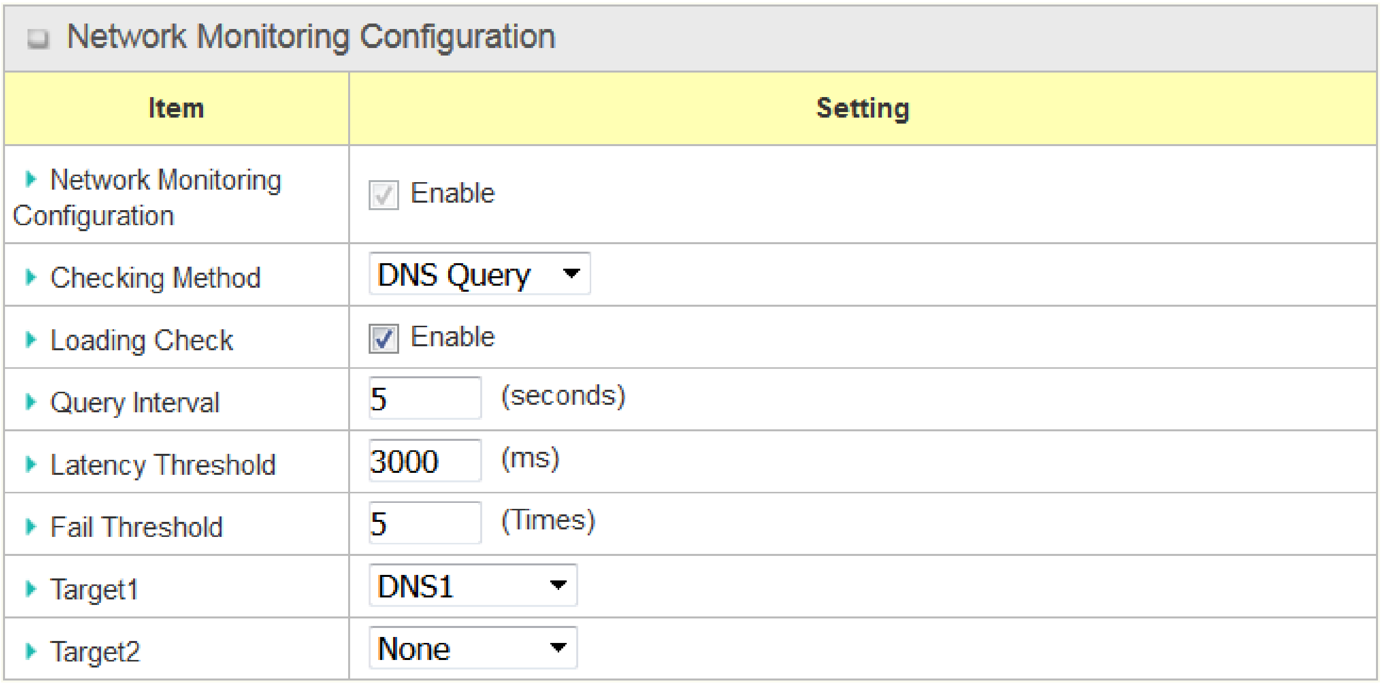
WiFi Uplink WAN Type Configuration

Item	Setting
Connect to AP	default-Ch#12-Open (None) Scan
Network Type	NAT Mode ▾
IP Mode	Dynamic IP ▾
Host Name	(Optional)
Fast Roaming	□ Enable Signal Threshold 40 %
Fast Roaming Channels	N/A ▾ N/A ▾ N/A ▾

WiFi Uplink WAN Type Configuration

Item	Value setting	Description
Connect to AP	N/A	Display the information of AP for connecting. You can Click the **Scan** button and select an AP for the uplink network. Besides, you can also create uplink profile(s) for ease of connecting to an available Uplink network. Refer to **Basic Network > WiFi > Uplink Profile** tab.
Network Type	1. A Must filled setting **2. NAT Mode** is selected by default.	Select the expected network type for the WiFi Uplink connection. It can be **NAT Mode**, **Bridge Mode**, or **NAT Disable**. When **NAT Mode** is selected, the NAT function is activated on the Wireless Uplink connection; When **Bridge Mode** is selected, the bridge function is activated on the Wireless Uplink connection; The supporting of bridge mode depends on the product specification, if the purchased device doesn't support the bridge mode, it will be greyed out from selection. When **NAT Disable** is selected, the NAT function is deactivated on the Wireless Uplink connection, and it can function as a router with manually configured routing setting.
IP Mode	1. A Must filled setting **2. Dynamic IP** is selected by default.	Specify the IP mode for the wireless uplink Interface. It can be **Dynamic IP** or **Static IP**. When **Dynamic IP** is selected, the device will request a IP from the Uplink Network as the IP for the uplink interface ; When **Static IP** is selected, you have to manually configure the IP address settings for the uplink interface. The settings include IP address, subnet mask, gateway, and primary/secondary DNS.
Host Name	An Optional setting	Specify the Host Name.
Fast Roaming	1. An Optional setting **2. Unchecked** is selected by default.	Click the **Enable** checkbox to activate the fast roaming function. In addition, you can also specify a threshold value for changing from one AP to another near-by AP. The default threshold value is 40%. ***Value Range***: 30 ~ 60%.
Fast Roaming Channels	An Optional setting	Select up to three fast roaming WiFi channels.

Network Monitoring



Network Monitoring Configuration

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

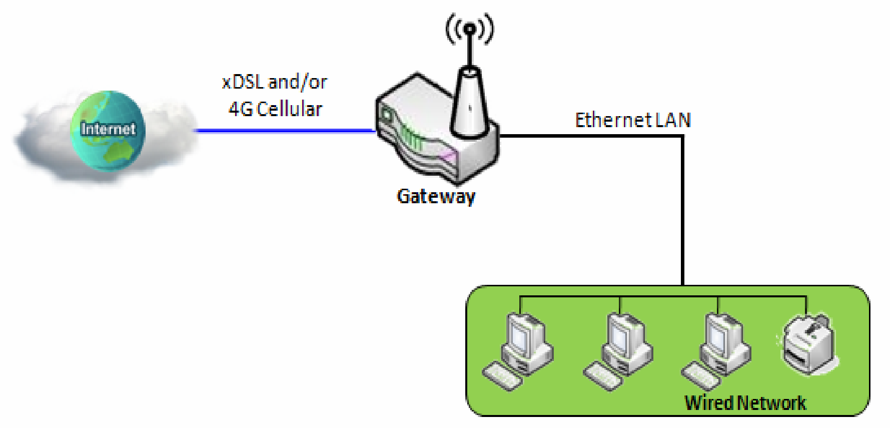
Network Monitoring Configuration		
Item	**Value setting**	**Description**
Network Monitoring Configuration	1. An Optional setting 2. The box is **checked** by default.	Click the **Enable** checkbox to activate the function.
Checking Method	1. An Optional setting 2. **DNS Query** is selected by default.	Choose either **DNS Query** or **ICMP Checking** method and specify a Query/Check Interval to detect WAN link. With such configuration, the gateway will use DNS Query or ICMP Checking to periodically check Internet connection –connected or disconnected.
Load Checking	1. An optional setting 2. Enabled by default.	Click the **Enable** checkbox to activate the function. Enable Loading Check allows the gateway to ignore unreturned DNS Queries or ICMP requests when WAN bandwidth is fully occupied. This is to prevent false link-down status. **Latency Threshold** defines the tolerance threshold of responding time. **Fail Threshold** specifies the detected disconnection before the router recognize the WAN link down status. Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged.
Query Interval	1. An Optional setting 2. **5 seconds** is selected by default.	Specify a time interval as the DNS **Query Interval**. **Query Interval** defines the transmitting interval between two DNS Query or ICMP checking packets. With **DNS Query,** the system checks the connection by sending DNS Query packets to the destination specified in Target 1 and Target 2. ***Value Range***: 2 ~ 14400.

Check Interval	1. An Optional setting 2. **5 seconds** is selected by default.	Specify a time interval as the ICMP **Checking Interval**. **Query Interval** defines the transmitting interval between two DNS Query or ICMP checking packets. With **ICMP Checking,** the system will check connection by sending ICMP request packets to the destination specified in Target 1 and Target 2. ***Value Range***: 2 ~ 14400.
Latency Threshold	1. An Optional setting 2. **3000 ms** is selected by default.	Specify a time interval as the **Latency Threshold**. **Latency Threshold** defines the tolerance threshold of responding time.
Fail Threshold	1. An Optional setting 2. **5 times** is selected by default.	Enter a number of detecting disconnection times to be the threshold before disconnection is acknowledged. **Fail Threshold** specifies the detected disconnection before the router recognize the WAN link down status. ***Value Range***: 1 ~ 10.
Target 1	1. An Optional setting 2. **DNS1** is selected by default.	**Target1** (**DNS1** set by default**)** specifies the first target of sending DNS query/ICMP request. ■ **DNS1**: set the primary DNS to be the target. ■ **DNS2**: set the secondary DNS to be the target. ■ **Gateway**: set the Current gateway to be the target. ■ **Other Host**: enter an IP address to be the target.
Target 2	1. An Optional setting 2. **None** is selected by default.	**Target2** (**None** set by default**)** specifies the second target of sending DNS query/ICMP request. ■ **None**: to disable **Target2.** ■ **DNS1**: set the primary DNS to be the target. ■ **DNS2**: set the secondary DNS to be the target. ■ **Gateway**: set the Current gateway to be the target. ■ **Other Host**: enter an IP address to be the target.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

2.2 LAN & VLAN

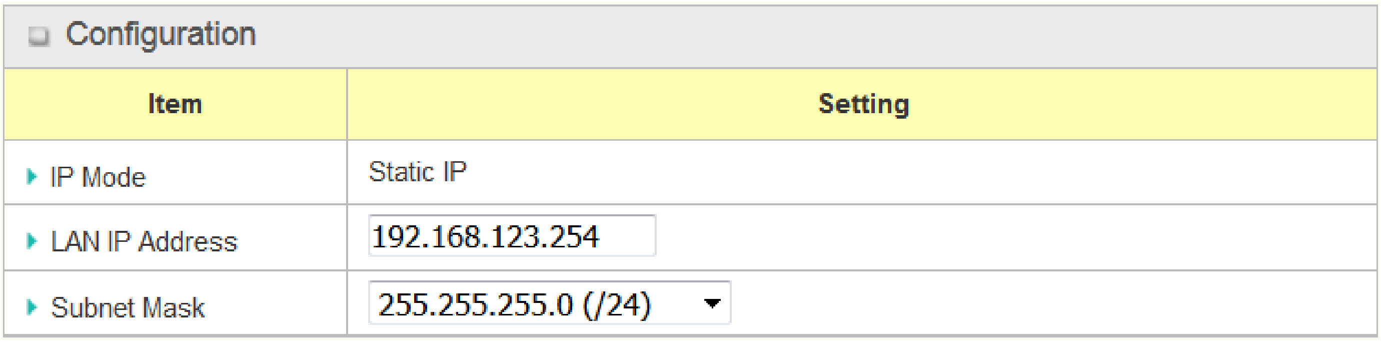
This section provides the configuration of LAN and VLAN. VLAN is an optional feature, and it depends on the product specification of the purchased gateway.

2.2.1 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 inter-connects computers.

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



Configuration

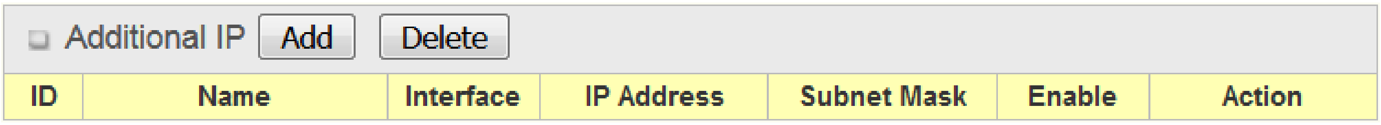
Item	Setting
IP Mode	Static IP
LAN IP Address	192.168.123.254
Subnet Mask	255.255.255.0 (/24) ▾

Configuration		
Item	**Value setting**	**Description**
IP Mode	N/A	It shows the LAN IP mode for the router according the related configuration. **Static IP**: If there is at least one WAN interface activated, the LAN IP mode is fixed in Static IP mode. **Dynamic IP**: If all the available WAN interfaces are disabled, the LAN IP mode can be Dynamic IP mode.
LAN IP Address	1. A Must filled setting **2.** 192.168.1.1 **is set by default**	Enter the local IP address of this device. The network device(s) on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary. **Note**: *It's also the IP address of web UI. If you change it, you need to type new IP address in the browser to see web UI.*

Subnet Mask	1. A Must filled setting 2. **255.255.255.0 (/24)** is set by default	Select the subnet mask for this gateway from the dropdown list. Subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0 (/24), and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway, so there are maximum 253 clients allowed in LAN network. ***Value Range***: 255.0.0.0 (/8) ~ 255.255.255.252 (/30).
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.

Create / Edit Additional IP

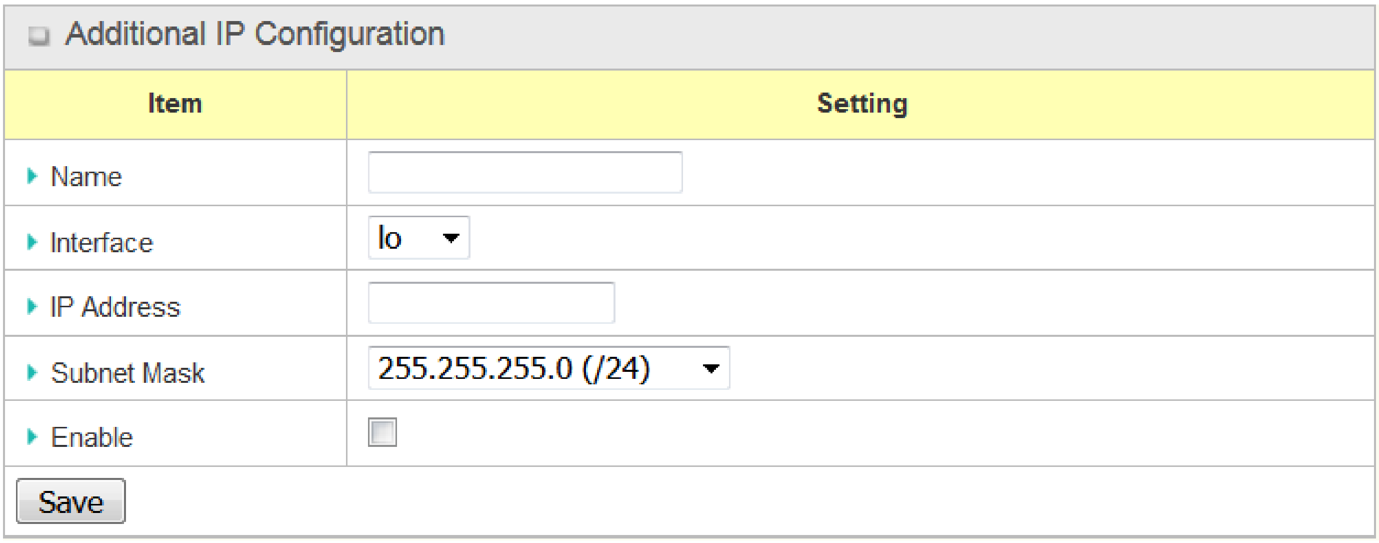
This router provides the LAN IP alias function for some special management consideration. You can add additional LAN IP for this router, and access to this router with the additional IP.



Additional IP Add Delete

ID	Name	Interface	IP Address	Subnet Mask	Enable	Action

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



Additional IP Configuration

Item	Setting
Name	
Interface	lo
IP Address	
Subnet Mask	255.255.255.0 (/24)
Enable	□

Save

Configuration		
Item	**Value setting**	**Description**
Name	1. An Optional Setting	Enter the name for the alias IP address.
Interface	1. A Must filled setting 2. **lo** is set by default	Specify the Interface type. It can be **lo** or **br0**.
IP Address	1. An Optional setting **2.** 192.168.1.1 **is set by default**	Enter the addition IP address for this device.

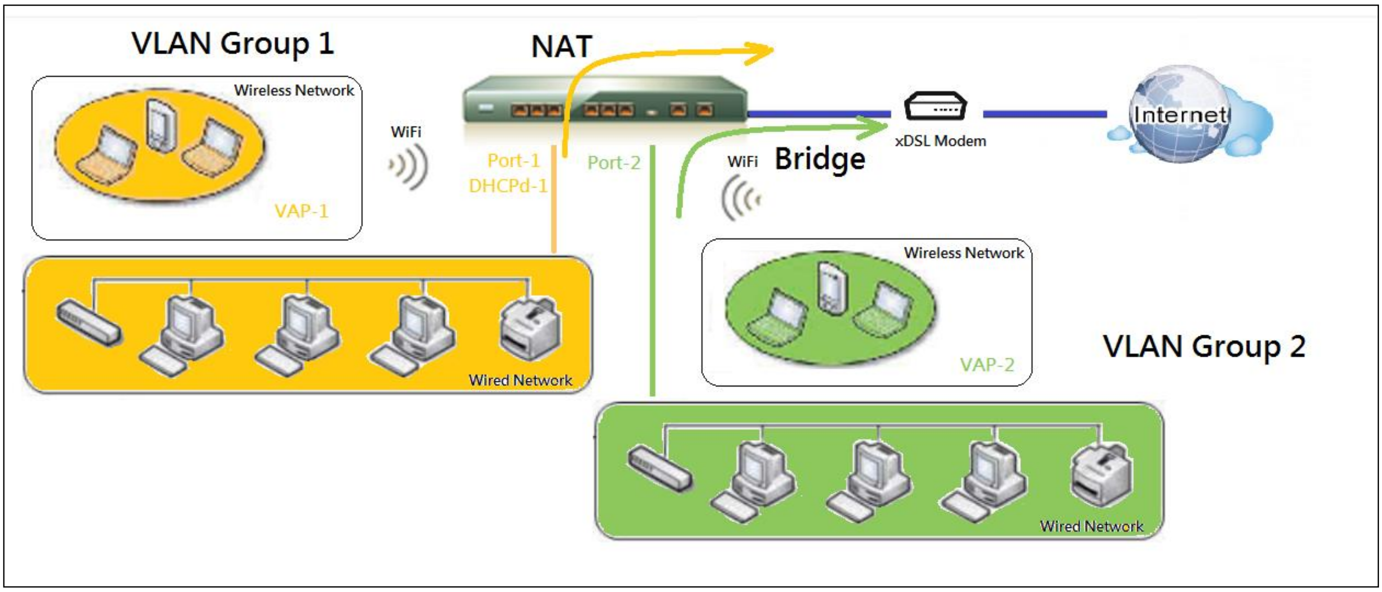
Subnet Mask	1. A Must filled setting 2. **255.255.255.0 (/24)** is set by default	Select the subnet mask for this gateway from the dropdown list. Subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0 (/24), and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway, so there are maximum 253 clients allowed in LAN network. ***Value Range*:** 255.0.0.0 (/8) ~ 255.255.255.255 (/32).
Save	NA	Click the **Save** button to save the configuration

2.2.2 VLAN

VLAN (Virtual LAN) is a logical network under a certain switch or router device to group client hosts with a specific VLAN ID. This gateway supports both Port-based VLAN and Tag-based VLAN. These functions allow you to divide local network into different “virtual LANs”. It is common requirement for some application scenario. For example, there are various departments within SMB. All client hosts in the same department should own common access privilege and QoS property. You can assign departments either by port-based VLAN or tag-based VLAN as a group, and then configure it by your plan. In some cases, ISP may need router to support “VLAN tag” for certain kinds of services (e.g. IPTV). You can group all devices required this service as one tag-based VLAN.

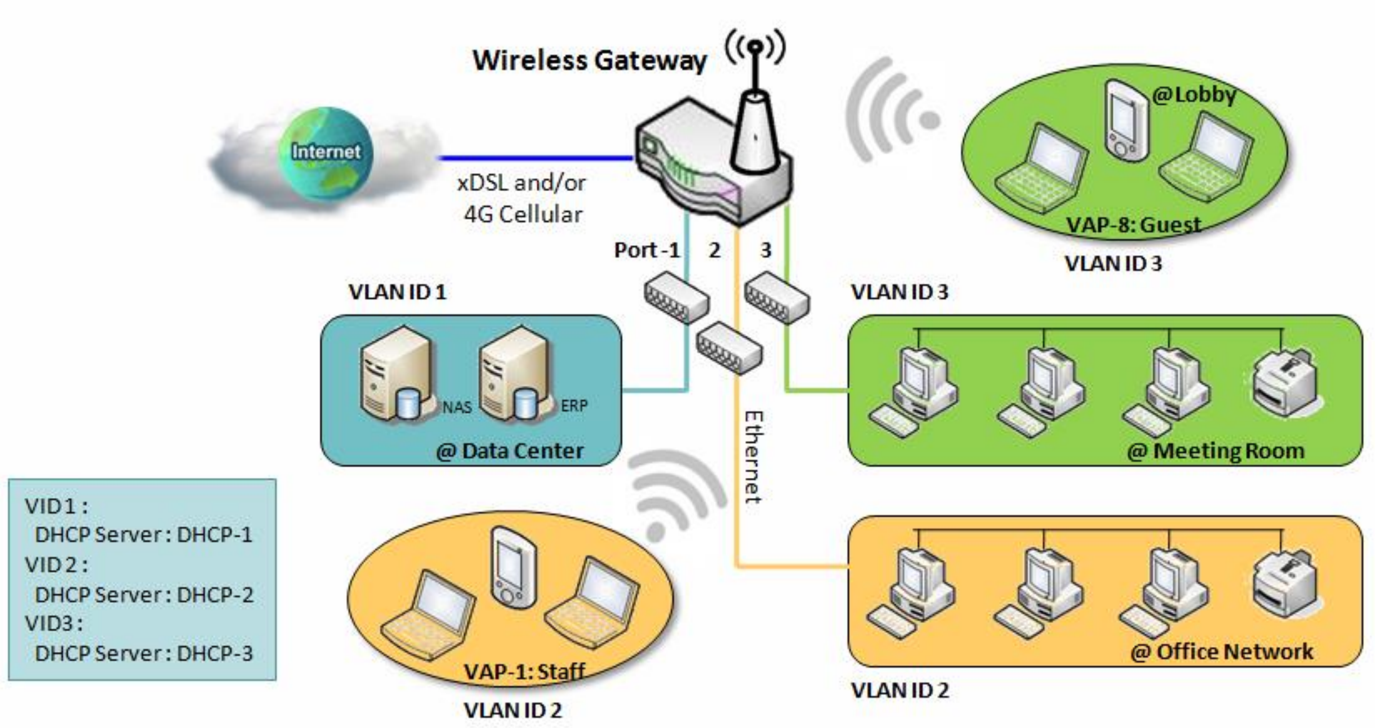
➢ Port-based VLAN

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



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

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

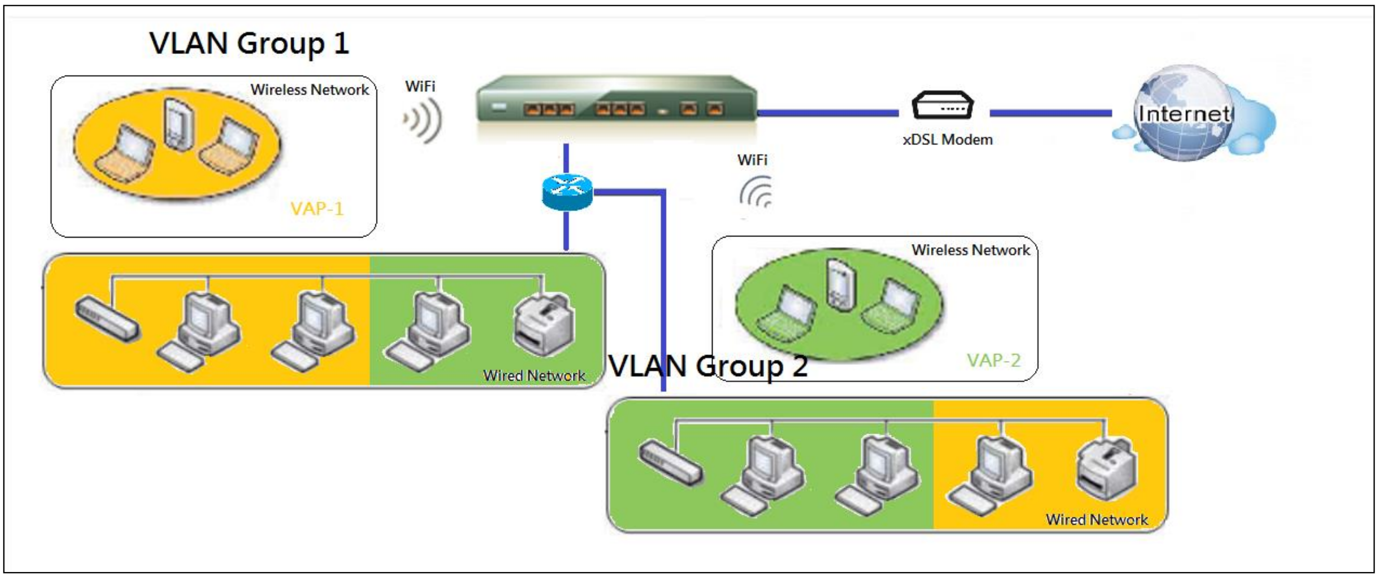


Above is the general case for 3 Ethernet LAN ports in the gateway. But if the device just has one Ethernet LAN port, there will be only one VLAN group for the device. Under such situation, it still supports both the NAT and Bridge mode for the Port-based VLAN configuration.

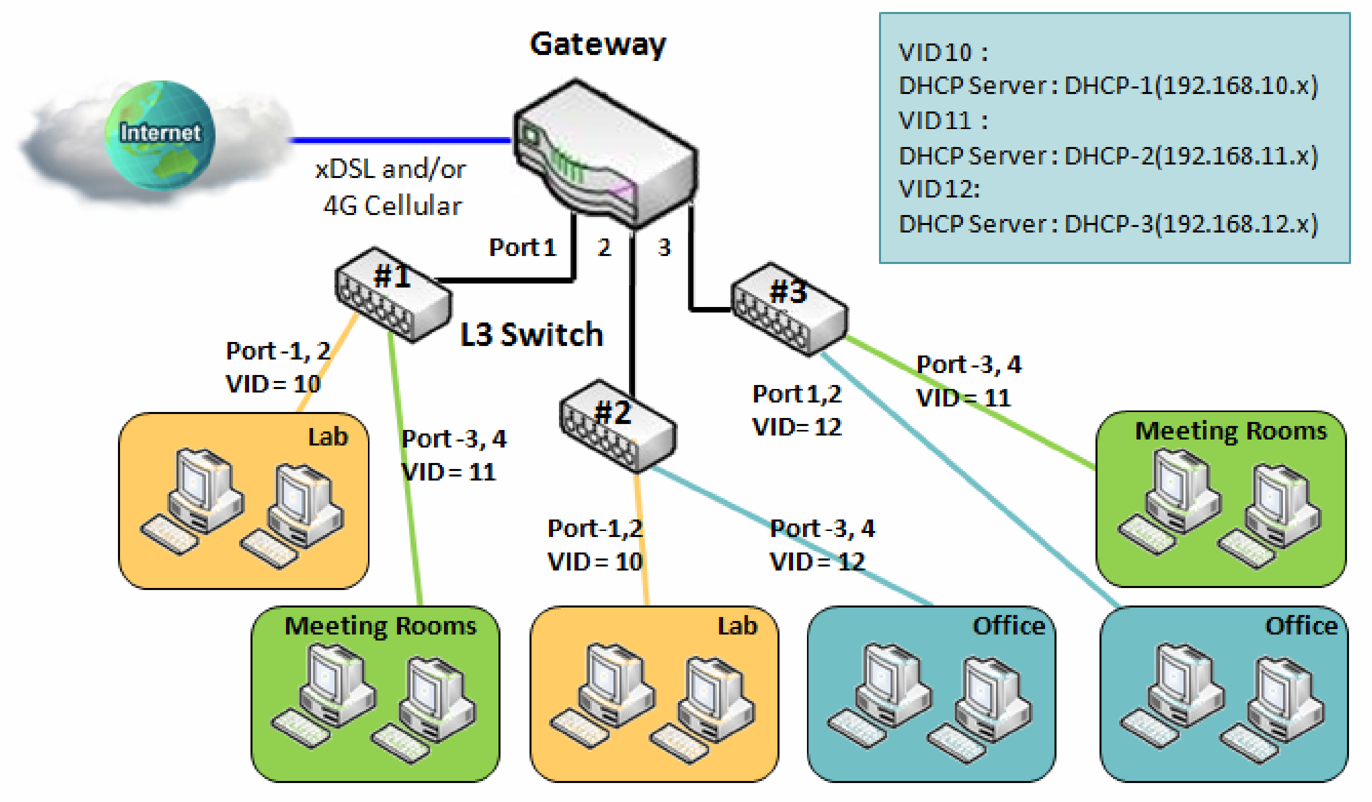
➢ Tag-based VLAN

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

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



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

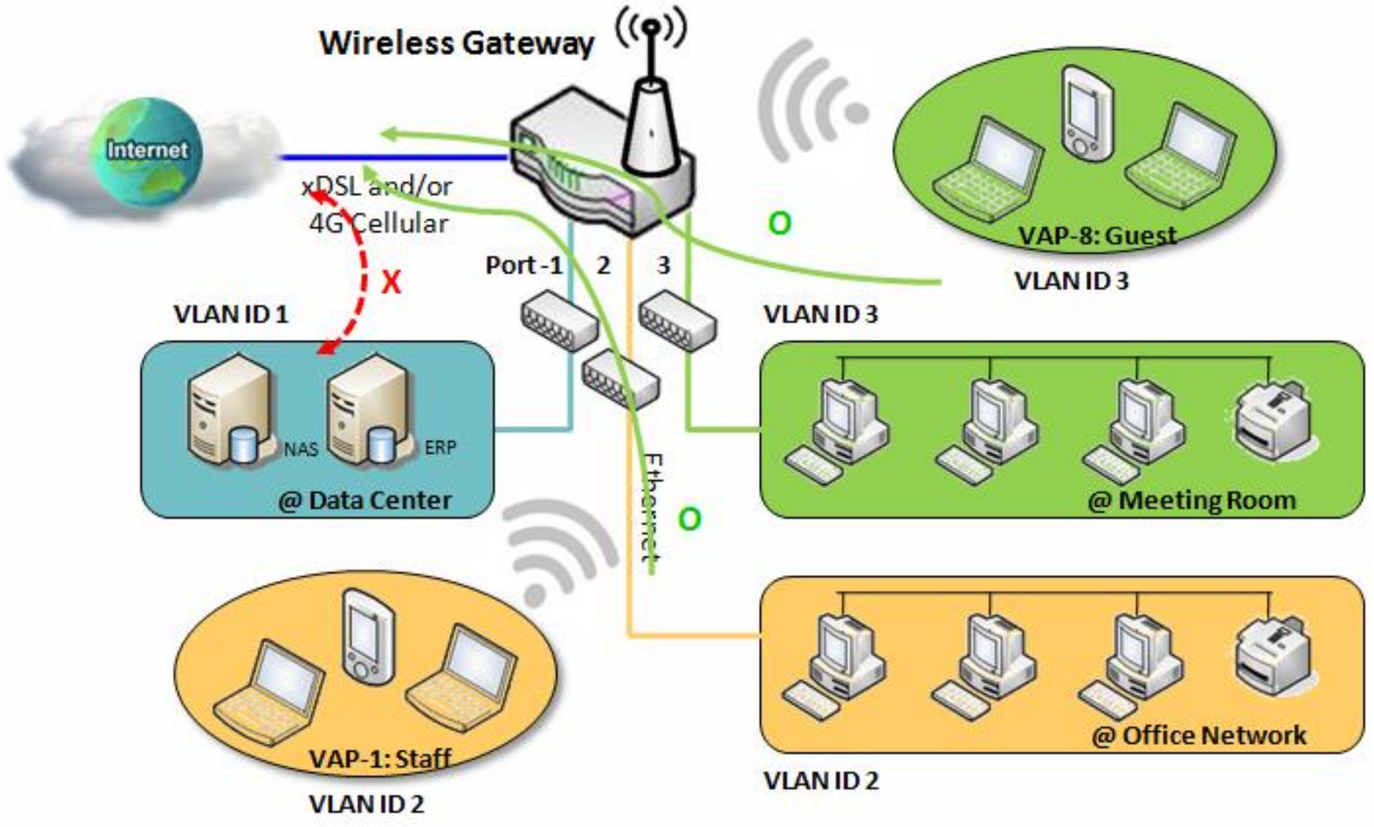


➢ VLAN Groups Access Control

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

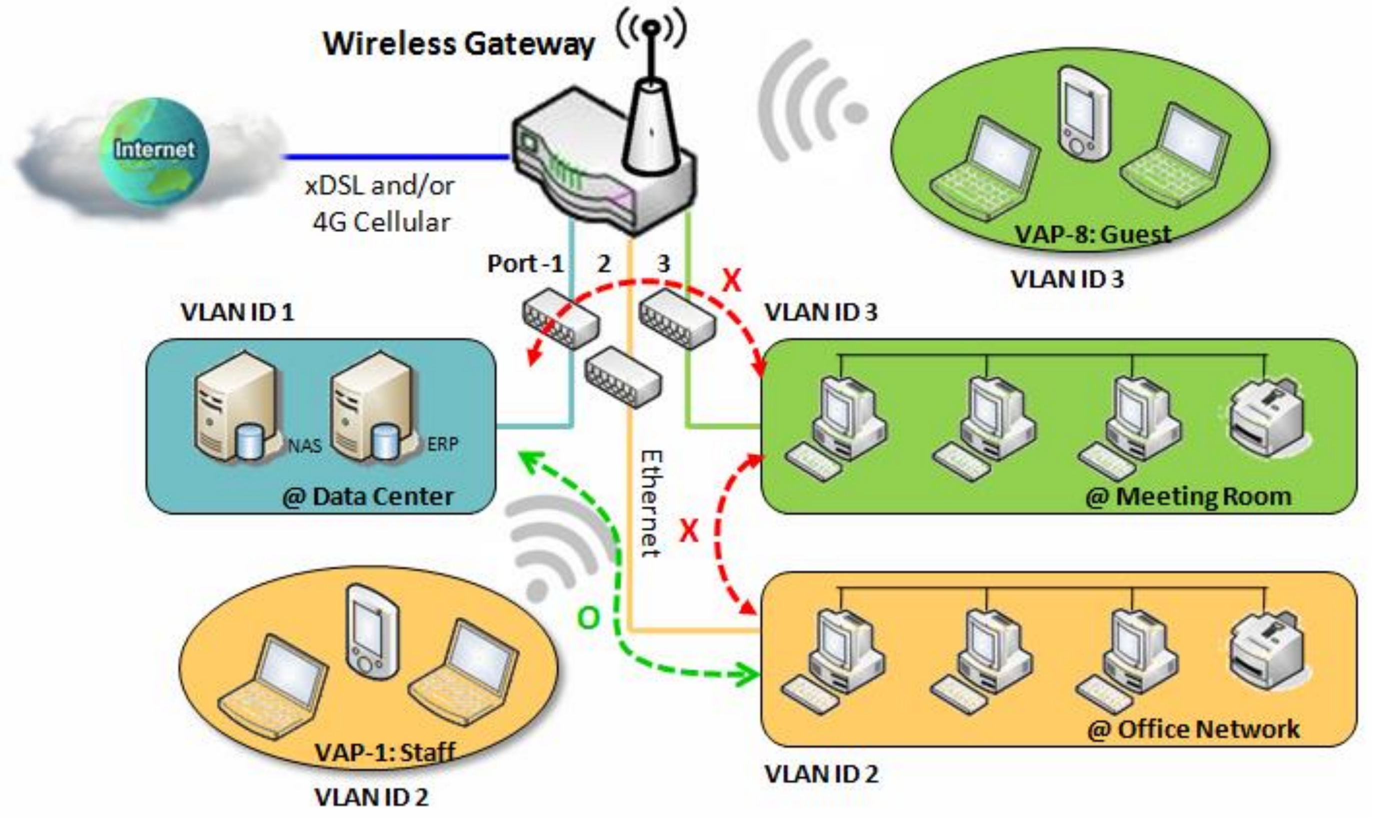
VLAN Group Internet Access

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



Inter VLAN Group Routing

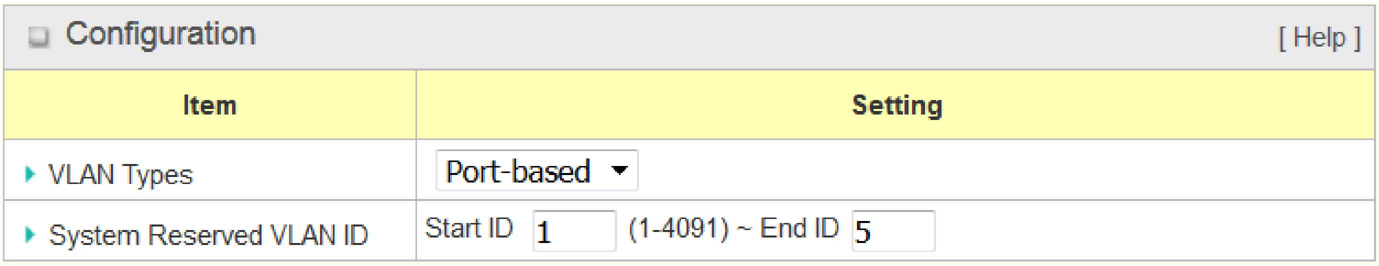
In Port-based tagging, administrator can specify member hosts of one VLAN group to be able to communicate with the ones of another VLAN group or not. This is a communication pair, and one VLAN group can join many communication pairs. But communication pair doesn't have the transitive property. That is,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



VLAN Setting

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

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



Configuration [Help]

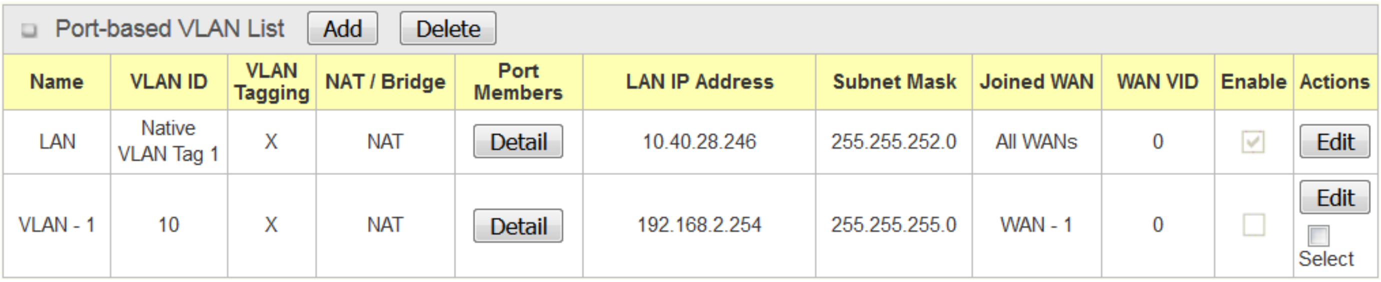
Item	Setting
VLAN Types	Port-based ▾
System Reserved VLAN ID	Start ID 1 (1-4091) ~ End ID 5

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

System Reserved VLAN ID	A Must filled setting	Define the **Start ID** for the VLAN and the **End ID** will be automatically counted as Start ID + 4. ***Value Range***: 1 ~ 4091
Save	NA	Click the **Save** button to save the configuration

Port-based VLAN – Create/Edit VLAN Rules

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

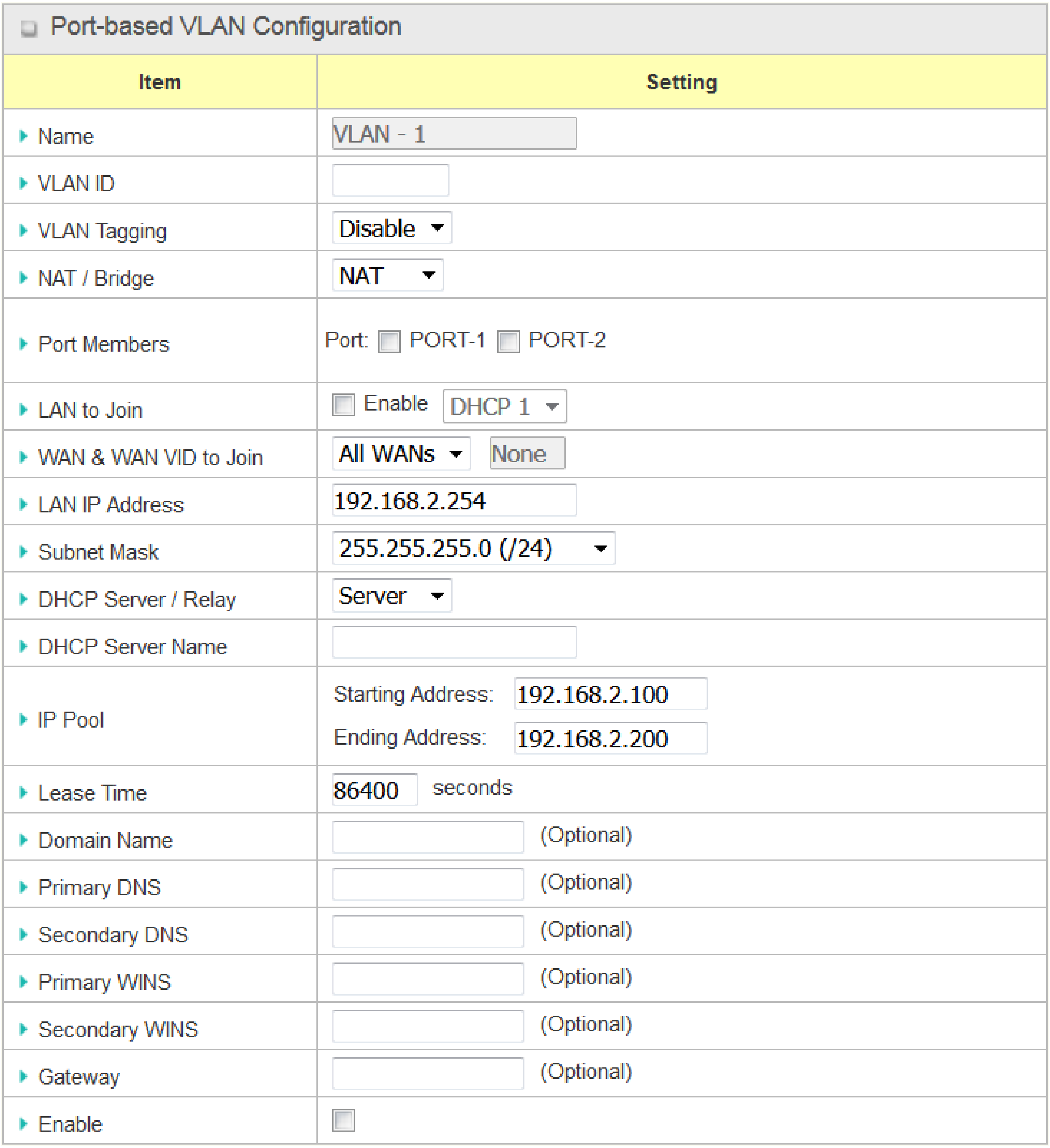


Port-based VLAN List Add Delete

Name	VLAN ID	VLAN Tagging	NAT / Bridge	Port Members	LAN IP Address	Subnet Mask	Joined WAN	WAN VID	Enable	Actions
LAN	Native VLAN Tag 1	X	NAT	Detail	10.40.28.246	255.255.252.0	All WANs	0	☑	Edit
VLAN - 1	10	X	NAT	Detail	192.168.2.254	255.255.255.0	WAN - 1	0	☐	Edit ☐ Select

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

Port-based VLAN - Configuration



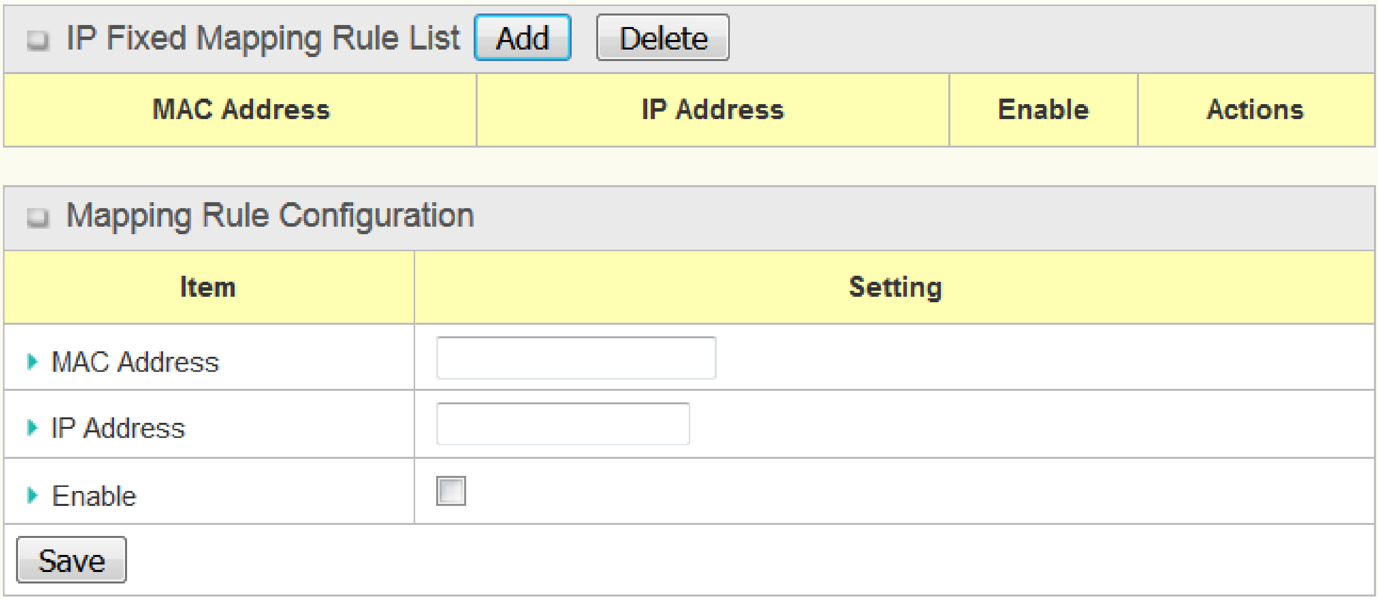
Port-based VLAN Configuration

Item	Setting
Name	VLAN - 1
VLAN ID	
VLAN Tagging	Disable
NAT / Bridge	NAT
Port Members	Port: □ PORT-1 □ PORT-2
LAN to Join	□ Enable DHCP 1
WAN & WAN VID to Join	All WANs None
LAN IP Address	192.168.2.254
Subnet Mask	255.255.255.0 (/24)
DHCP Server / Relay	Server
DHCP Server Name	
IP Pool	Starting Address: 192.168.2.100 Ending Address: 192.168.2.200
Lease Time	86400 seconds
Domain Name	(Optional)
Primary DNS	(Optional)
Secondary DNS	(Optional)
Primary WINS	(Optional)
Secondary WINS	(Optional)
Gateway	(Optional)
Enable	□

Port-based VLAN Configuration		
Item	**Value setting**	**Description**
Name	1. A Must filled setting 2. String format: already have default texts	Define the **Name** of this rule. It has a default text and cannot be modified.
VLAN ID	A Must filled setting	Define the VLAN ID number, range is 1~4094.
VLAN Tagging	**Disable** is selected by default.	The rule is activated according to **VLAN ID** and **Port Members** configuration when **Enable** is selected. The rule is activated according **Port Members** configuration when **Disable** is selected.
NAT / Bridge	**NAT** is selected by default.	Select **NAT** mode or **Bridge** mode for the rule.
Port Members	These box is unchecked by default.	Select which LAN port(s) and VAP(s) that you want to add to the rule. Note: The available member list can be different for the purchased product.
LAN to Join	1. An Optional Setting 2. The box is unchecked by default.	Select the LAN to join.
WAN & WAN VID to Join	**All WANs** is selected by default.	Select which **WAN** or **All WANs** that allow accessing Internet. Note: If Bridge mode is selected, you need to select a WAN and enter a VID.
LAN IP Address	A Must filled setting	Assign an **IP Address** for the DHCP Server that the rule used, this IP address is a gateway IP.
Subnet Mask	**255.255.255.0(/24)** is selected by default.	Select a **Subnet Mask** for the DHCP Server.
DHCP Server /Relay	**Server** is selected by default.	Define the **DHCP Server** type. There are three types you can select: **Server**, **Relay**, and **Disable**. **Relay**: Select **Relay** to enable DHCP Relay function for the VLAN group, and you only need to fill the **DHCP Server IP Address** field. **Server**: Select **Server** to enable DHCP Server function for the VLAN group, and you need to specify the DHCP Server settings. **Disable**: Select **Disable** to disable the DHCP Server function for the VLAN group.
DHCP Server IP Address (for DHCP **Relay** only)	A Must filled setting	If you select **Relay** type of DHCP Server, assign a **DHCP Server IP Address** that the gateway will relay the DHCP requests to the assigned DHCP server.
DHCP Server Name	A Must filled setting	Define name of the DHCP Server for the specified VLAN group.
IP Pool	A Must filled setting	Define the IP Pool range. There are **Starting Address** and **Ending Address** fields. If a client requests an IP address from this DHCP Server, it will assign an IP address in the range of **IP pool**.
Lease Time	A Must filled setting	Define a period of time for an IP Address that the DHCP Server leases to a new device. By default, the **lease time** is 86400 seconds.
Domain Name	String format can be any text	The Domain Name of this DHCP Server. ***Value Range***: 0 ~ 31 characters.
Primary DNS	IPv4 format	The Primary DNS of this DHCP Server.
Secondary DNS	IPv4 format	The Secondary DNS of this DHCP Server.
Primary WINS	IPv4 format	The Primary WINS of this DHCP Server.
Secondary WINS	IPv4 format	The Secondary WINS of this DHCP Server.
Gateway	IPv4 format	The Gateway of this DHCP Server.

Enable	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore what you just configured back to the previous setting.

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



IP Fixed Mapping Rule List [Add] [Delete]

MAC Address	IP Address	Enable	Actions

Mapping Rule Configuration

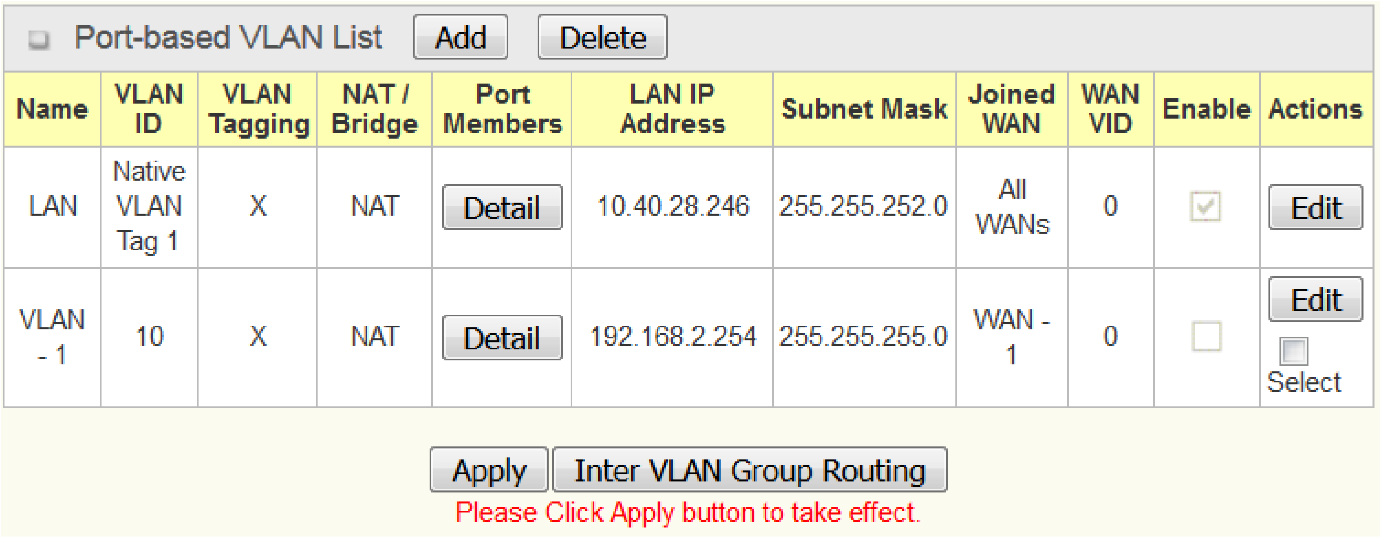
Item	Setting
MAC Address	
IP Address	
Enable	□

[Save]

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

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

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



Port-based VLAN List Add Delete

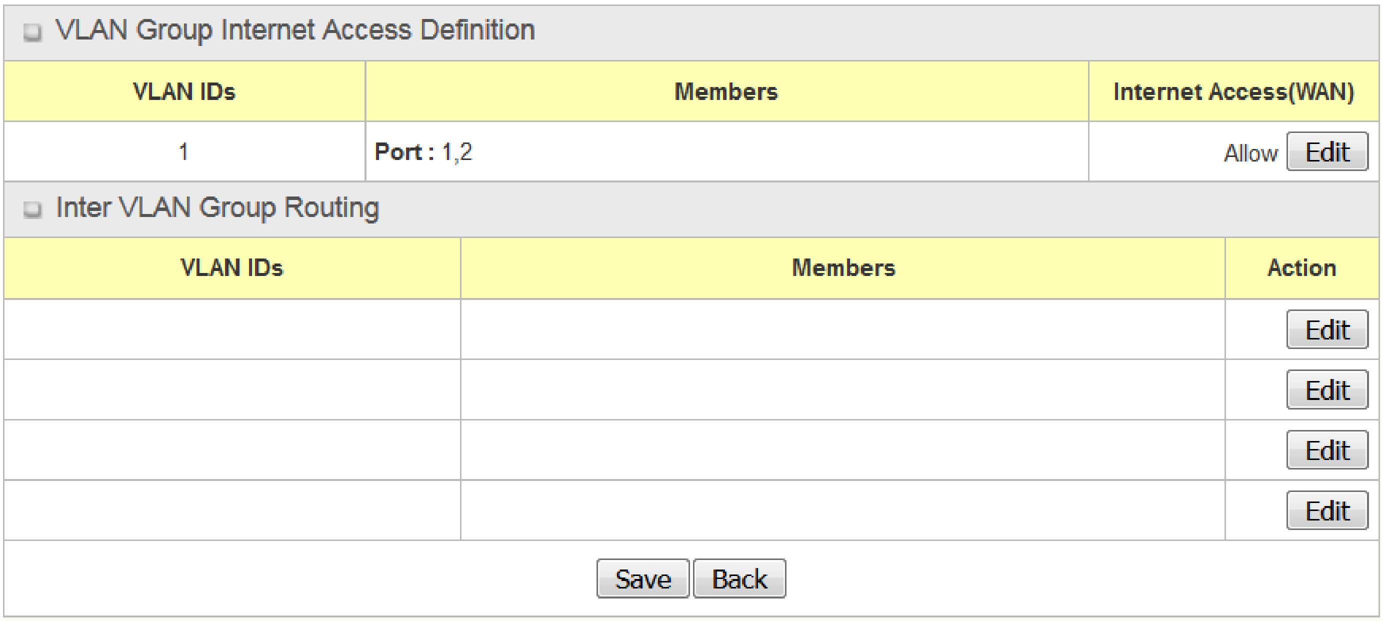
Name	VLAN ID	VLAN Tagging	NAT / Bridge	Port Members	LAN IP Address	Subnet Mask	Joined WAN	WAN VID	Enable	Actions
LAN	Native VLAN Tag 1	X	NAT	Detail	10.40.28.246	255.255.252.0	All WANs	0	☑	Edit
VLAN - 1	10	X	NAT	Detail	192.168.2.254	255.255.255.0	WAN - 1	0	☐	Edit ☐ Select

Apply | Inter VLAN Group Routing

Please Click Apply button to take effect.

Port-based VLAN – Inter VLAN Group Routing

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



VLAN Group Internet Access Definition

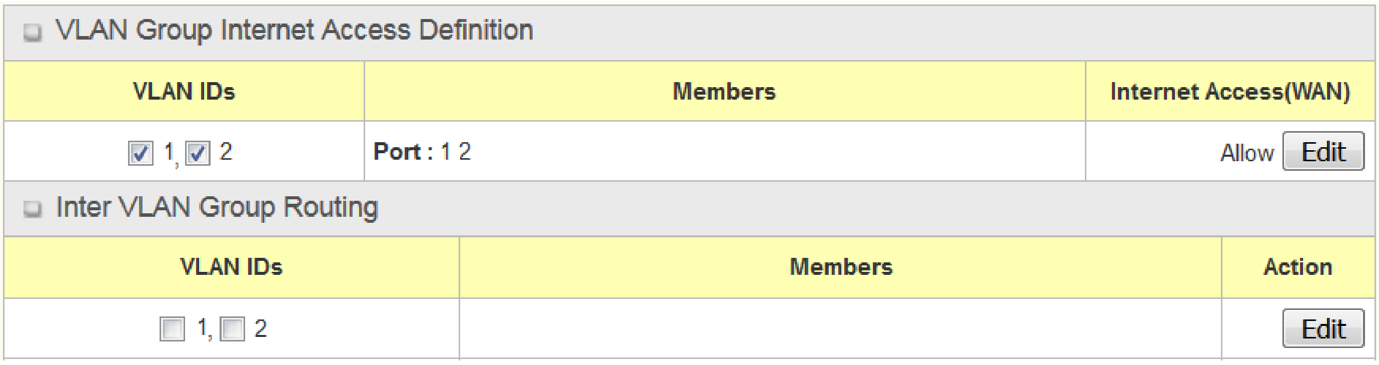
VLAN IDs	Members	Internet Access(WAN)
1	**Port :** 1,2	Allow Edit

Inter VLAN Group Routing

VLAN IDs	Members	Action
		Edit
		Edit
		Edit
		Edit

Save | Back

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



VLAN Group Internet Access Definition

VLAN IDs	Members	Internet Access(WAN)
☑ 1, ☑ 2	**Port :** 1 2	Allow Edit

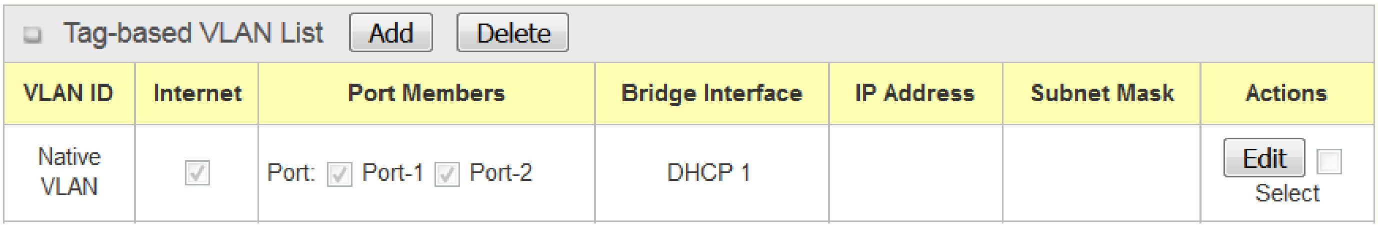
Inter VLAN Group Routing

VLAN IDs	Members	Action
□ 1, □ 2		Edit

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

Tag-based VLAN – Create/Edit VLAN Rules

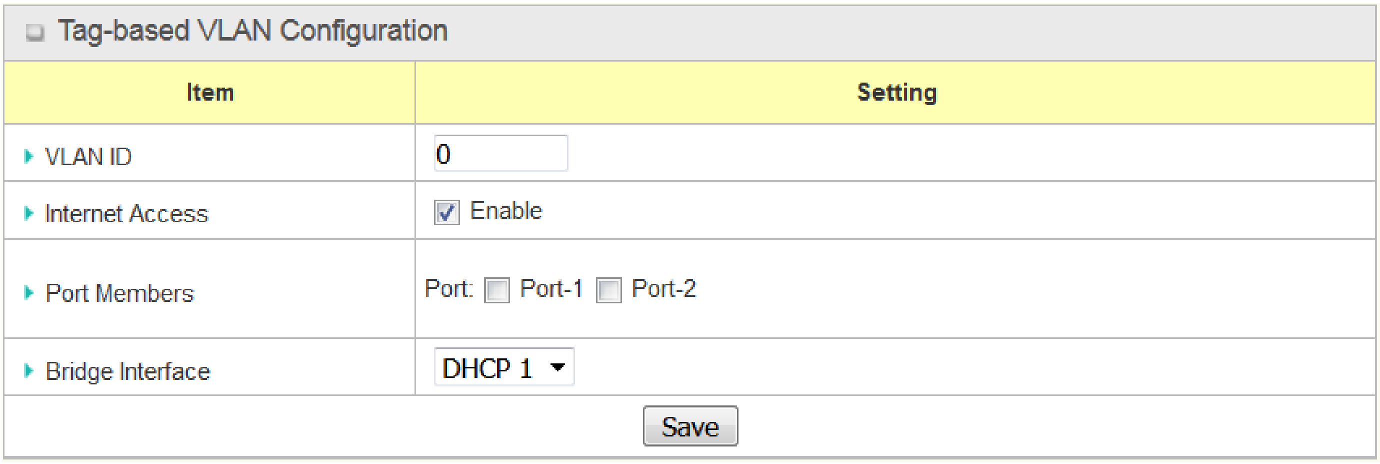
The **Tag-based VLAN** allows you to customize each LAN port according to VLAN ID. There is a default rule shows the configuration of all LAN ports and all VAPs. Also, if your device has a DMZ port, you will see DMZ configuration, too. The router supports up to a maximum of 128 tag-based VLAN rule sets.



Tag-based VLAN List Add Delete

VLAN ID	Internet	Port Members	Bridge Interface	IP Address	Subnet Mask	Actions
Native VLAN	☑	Port: ☑ Port-1 ☑ Port-2	DHCP 1			Edit □ Select

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



Tag-based VLAN Configuration

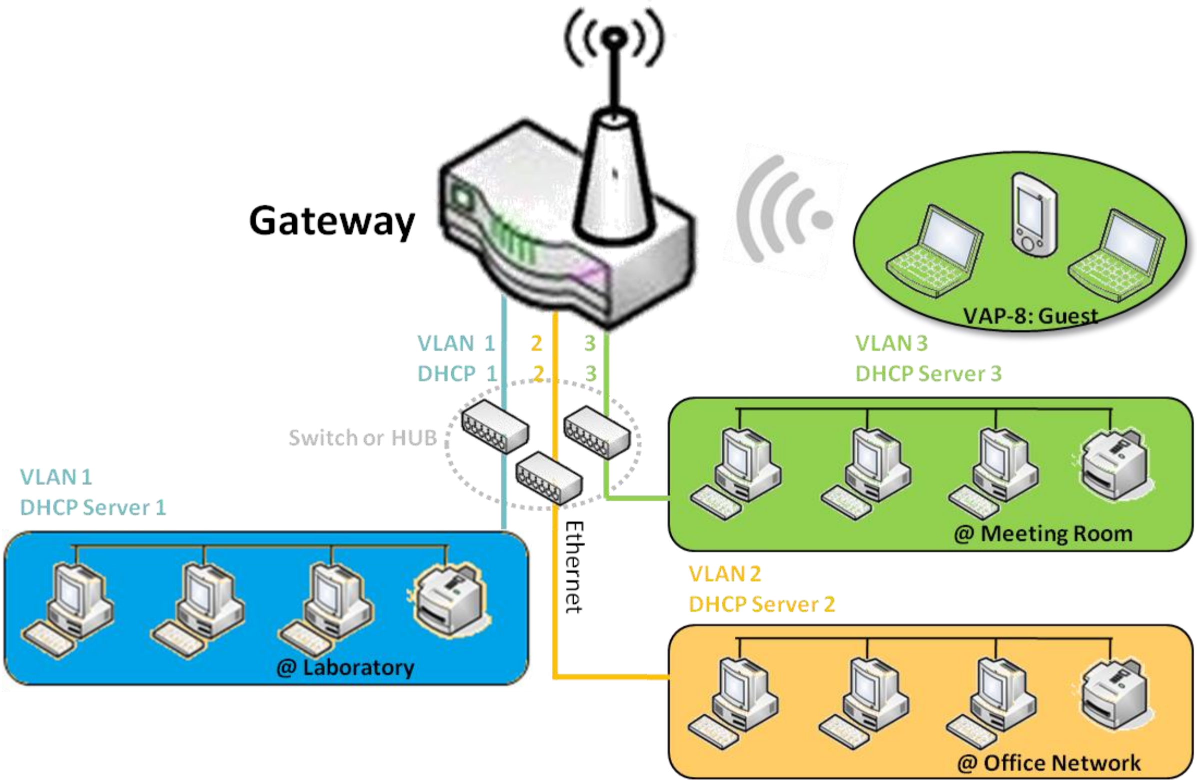
Item	Setting
VLAN ID	0
Internet Access	☑ Enable
Port Members	Port: □ Port-1 □ Port-2
Bridge Interface	DHCP 1

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

2.2.3 DHCP Server

➢ DHCP Server

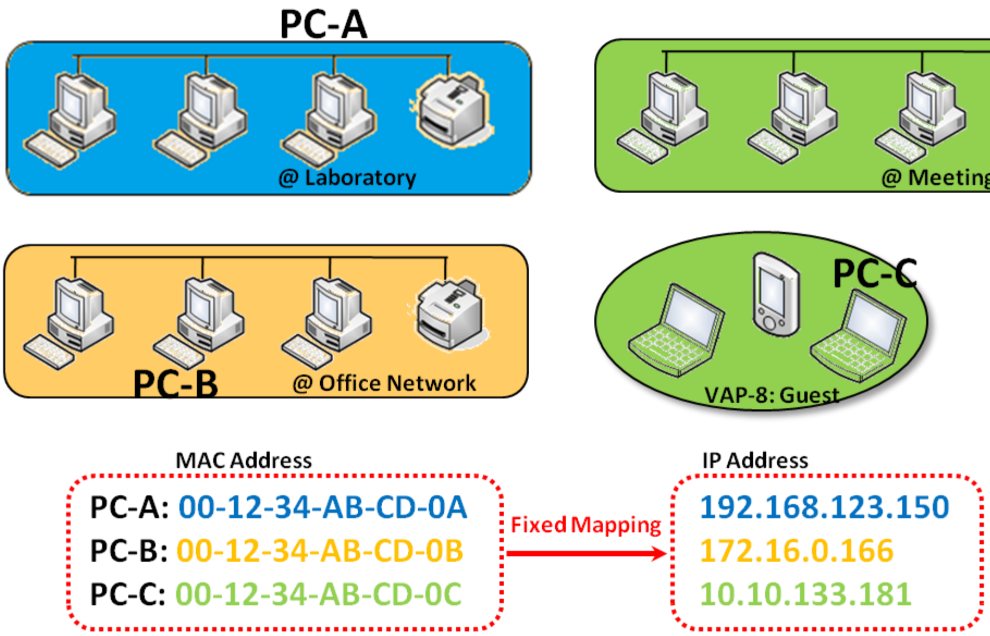
The gateway supports up to 4 DHCP servers to fulfill the DHCP requests from different VLAN groups (please refer to VLAN section for getting more usage details). And there is one default setting for whose LAN IP Address is the same one of router LAN interface, with its default Subnet Mask setting as "255.255.255.0",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



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

➢ Fixed Mapping

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



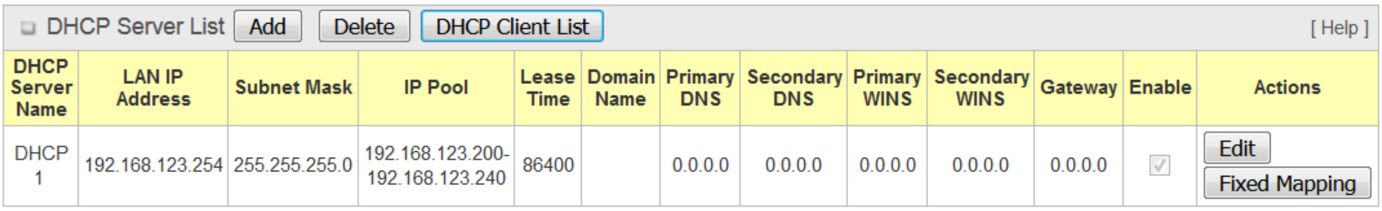
DHCP Server Setting

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

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

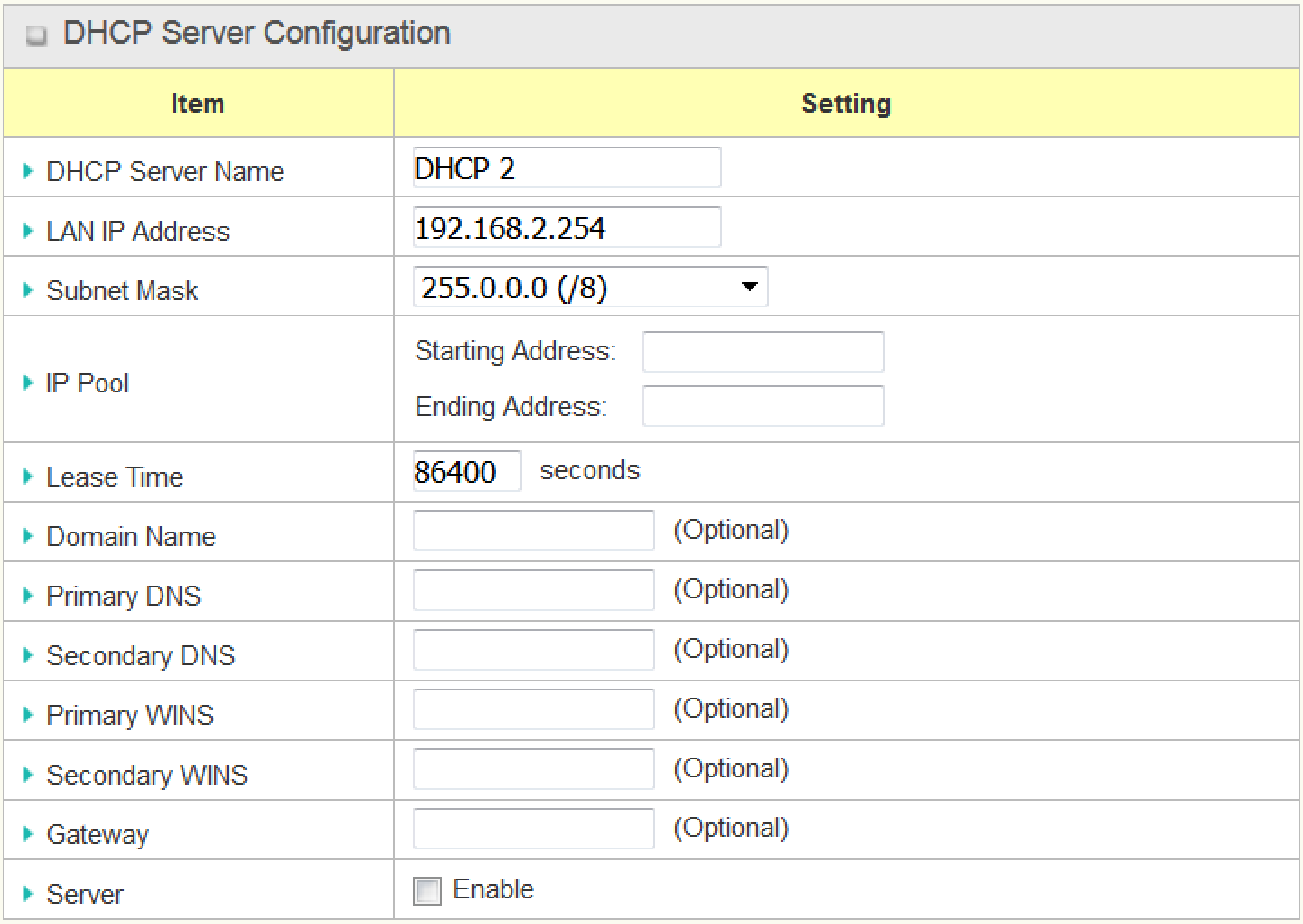
Create / Edit DHCP Server Policy

The router allows you to custom your DHCP Server Policy. If multiple LAN ports are available, you can define one policy for each LAN (or VLAN group), and it supports up to a maximum of 4 policy sets.



DHCP Server 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	192.168.123.254	255.255.255.0	192.168.123.200- 192.168.123.240	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	255.0.0.0 (/8)
IP Pool	Starting Address: Ending Address:
Lease Time	86400 seconds
Domain Name	(Optional)
Primary DNS	(Optional)
Secondary DNS	(Optional)
Primary WINS	(Optional)
Secondary WINS	(Optional)
Gateway	(Optional)
Server	□ Enable

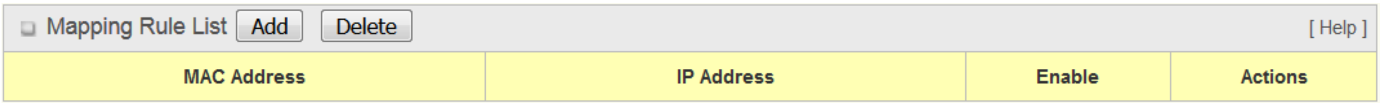
DHCP Server Configuration

Item	Value setting	Description
DHCP Server Name	1. String format can be any text 2. A Must filled setting	Enter a DHCP Server name. Enter a name that is easy for you to understand.
LAN IP Address	1. IPv4 format. 2. A Must filled setting	The LAN IP Address of this DHCP Server.
Subnet Mask	255.0.0.0 (/8) is set by default	The Subnet Mask of this DHCP Server.
IP Pool	1. IPv4 format. 2. A Must filled setting	The IP Pool of this DHCP Server. It composed of Starting Address entered in this field and Ending Address entered in this field.
Lease Time	1. Numeric string format. 2. A Must filled setting	The Lease Time of this DHCP Server. ***Value Range***: 300 ~ 604800 seconds.
Domain Name	String format can be any text	The Domain Name of this DHCP Server.
Primary DNS	IPv4 format	The Primary DNS of this DHCP Server.
Secondary DNS	IPv4 format	The Secondary DNS of this DHCP Server.
Primary WINS	IPv4 format	The Primary WINS of this DHCP Server.

Secondary WINS	IPv4 format	The Secondary WINS of this DHCP Server.
Gateway	IPv4 format	The Gateway of this DHCP Server.
Server	The box is unchecked by default.	Click **Enable** box to activate this DHCP Server.
Save	N/A	Click the **Save** button to save the configuration
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	N/A	When the **Back** button is clicked the screen will return to the DHCP Server Configuration page.

Create / Edit Mapping Rule List on DHCP Server

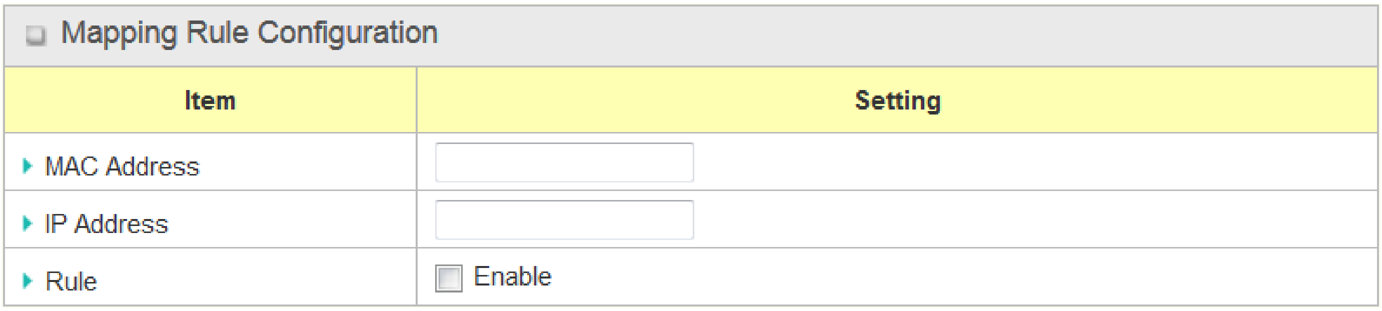
The router allows you to custom your Mapping Rule List on DHCP Server. It supports up to a maximum of 64 rule sets. When **Fix Mapping** button is applied, the **Mapping Rule List** screen will appear.



Mapping Rule List Add Delete [Help]

MAC Address	IP Address	Enable	Actions

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



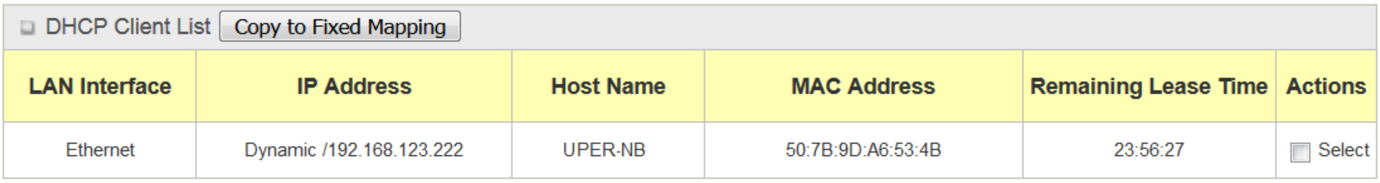
Mapping Rule Configuration

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

View / Copy DHCP Client List

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



DHCP Client List [Copy to Fixed Mapping]

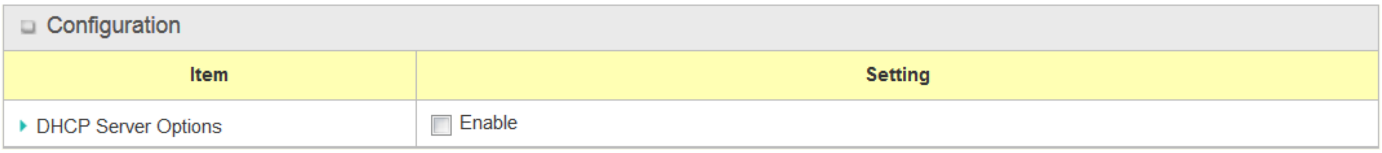
LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time	Actions
Ethernet	Dynamic /192.168.123.222	UPER-NB	50:7B:9D:A6:53:4B	23:56:27	□ Select

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

Enable / Disable DHCP Server Options

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

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

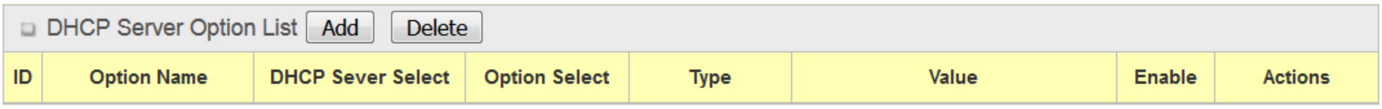


Configuration

Item	Setting
DHCP Server Options	□ Enable

Create / Edit DHCP Server Options

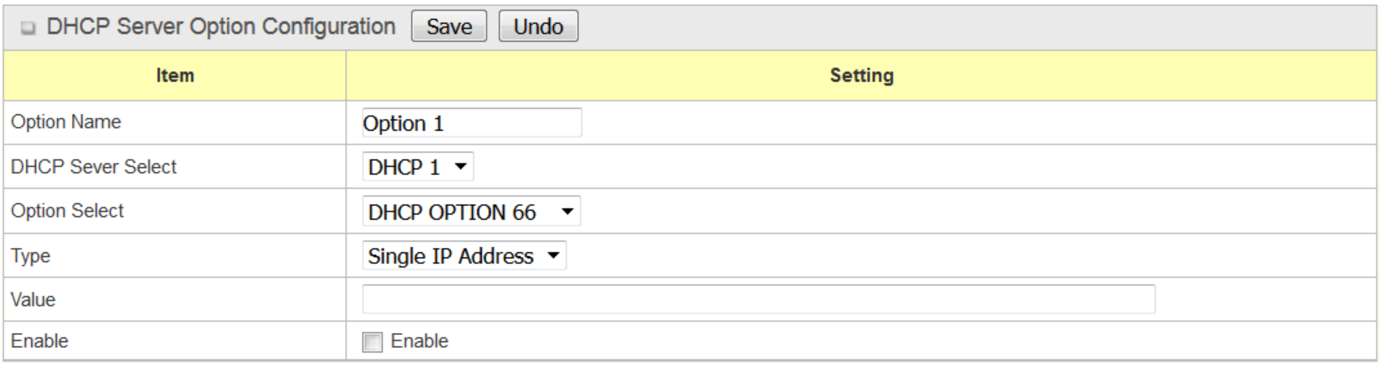
The router supports up to a maximum of 99 option settings.



DHCP Server Option List [Add] [Delete]

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

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



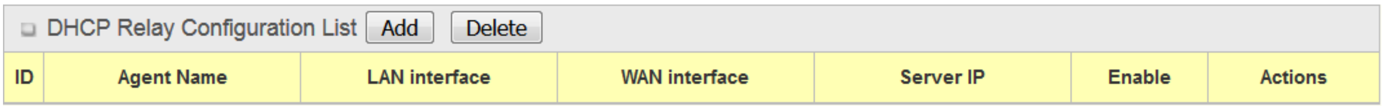
DHCP Server Option Configuration [Save] [Undo]

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

<table>
<tr><th colspan="5">DHCP Server Option Configuration</th></tr>
<tr><th>Item</th><th>Value setting</th><th colspan="3">Description</th></tr>
<tr><td><b>Option Name</b></td><td>1. String format can be any text
2. A Must filled setting.</td><td colspan="3">Enter a DHCP Server Option name. Enter a name that is easy for you to understand.</td></tr>
<tr><td><b>DHCP Server Select</b></td><td>Dropdown list of all available DHCP servers.</td><td colspan="3">Choose the DHCP server this option should apply to.</td></tr>
<tr><td><b>Option Select</b></td><td>1. A Must filled setting.
2. <b>Option 66</b> is selected by default.</td><td colspan="3">Choose the specific option from the dropdown list. It can be <b>Option 66</b>, <b>Option 72</b>, <b>Option 144</b>, <b>Option 42</b>, <b>Option 150</b>, <b>or Option 160</b>.
<b>Option 42</b> for ntp server;
<b>Option 66</b> for tftp;
<b>Option 72</b> for www;
<b>Option 144</b> for url;</td></tr>
<tr><td rowspan="10"><b>Type</b></td><td rowspan="10">Dropdown list of DHCP server option value’s type</td><td colspan="3">Each different options has different value types.</td></tr>
<tr><td rowspan="2">66</td><td colspan="2">Single IP Address</td></tr>
<tr><td colspan="2">Single FQDN</td></tr>
<tr><td>72</td><td colspan="2">IP Addresses List, separated by “,”</td></tr>
<tr><td>114</td><td colspan="2">Single URL</td></tr>
<tr><td>42</td><td colspan="2">IP Addresses List, separated by “,”</td></tr>
<tr><td>150</td><td colspan="2">IP Addresses List, separated by “,”</td></tr>
<tr><td rowspan="2">160</td><td colspan="2">Single IP Address</td></tr>
<tr><td colspan="2">Single FQDN</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="6"><b>Value</b></td><td rowspan="6">1. IPv4 format
2. FQDN format
3. IP list
4. URL format
5. A Must filled setting</td><td colspan="3">Should conform to Type :</td></tr>
<tr><td></td><td>Type</td><td>Value</td></tr>
<tr><td rowspan="2">66</td><td>Single IP Address</td><td>IPv4 format</td></tr>
<tr><td>Single FQDN</td><td>FQDN format</td></tr>
<tr><td>72</td><td>IP Addresses List, separated by “,”</td><td>IPv4 format, separated by “,”</td></tr>
<tr><td>114</td><td>Single URL</td><td>URL format</td></tr>
<tr><td><b>Enable</b></td><td>The box is unchecked by default.</td><td colspan="3">Click <b>Enable</b> box to activate this setting.</td></tr>
<tr><td><b>Save</b></td><td><i>NA</i></td><td colspan="3">Click the <b>Save</b> button to save the setting.</td></tr>
<tr><td><b>Undo</b></td><td><i>NA</i></td><td colspan="3">When the <b>Undo</b> button is clicked the screen will return back with nothing changed.</td></tr>
</table>

Create / Edit DHCP Relay

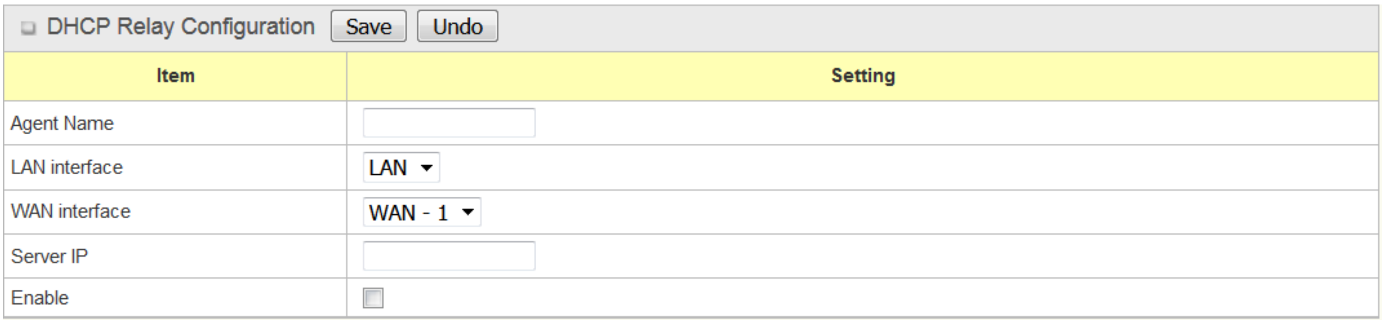
The router supports up to a maximum of 6 DHCP Relay configurations.



DHCP Relay Configuration List Add Delete

ID	Agent Name	LAN interface	WAN interface	Server IP	Enable	Actions

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



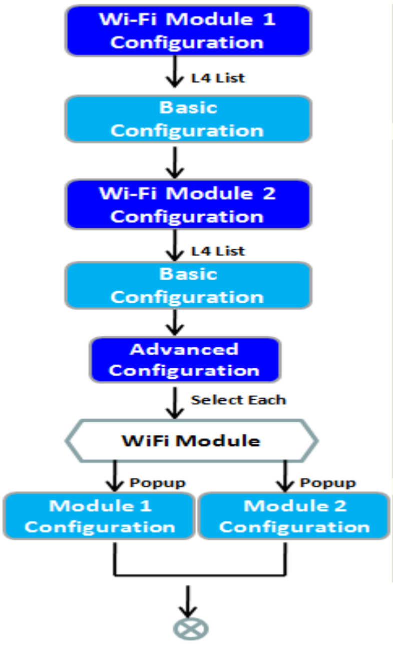
DHCP Relay Configuration Save Undo

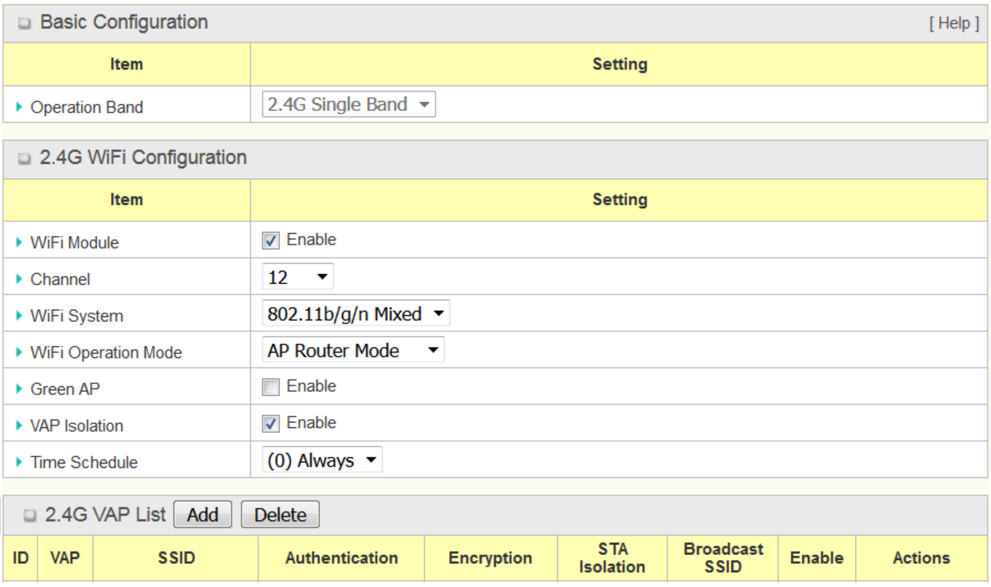
Item	Setting
Agent Name	
LAN interface	LAN ▾
WAN interface	WAN - 1 ▾
Server IP	
Enable	□

DHCP Relay Configuration

Item	Value setting	Description
Agent Name	1. String format can be any text 2. A Must filled setting.	Enter a DHCP Relay name. Enter a name that is easy for you to understand. ***Value Range***: 1~64 characters.
LAN Interface	1. A Must filled setting. 2. **LAN** is selected by default.	Choose a LAN Interface for the dropdown list to apply with the DHCP Relay function.
WAN Interface	1. A Must filled setting. 2. **WAN-1** is selected by default.	Choose a WAN Interface for the dropdown list to apply with the DHCP Relay function. It can be the available WAN interface(s), and L2TP connection.
Server IP	1. A Must filled setting. 2. **null** by default.	Assign a **DHCP Server IP Address** that the gateway will relay the DHCP requests to the assigned DHCP server via specified WAN interface.
Enable	The box is unchecked by default.	Click **Enable** box to activate this setting.
Save	*NA*	Click the **Save** button to save the setting.
Undo	*NA*	When the **Undo** button is clicked the screen will return back with nothing changed.

2.3 WiFi





Basic Configuration [Help]

Item	Setting
Operation Band	2.4G Single Band

2.4G WiFi Configuration

Item	Setting
WiFi Module	☑ Enable
Channel	12
WiFi System	802.11b/g/n Mixed
WiFi Operation Mode	AP Router Mode
Green AP	□ Enable
VAP Isolation	☑ Enable
Time Schedule	(0) Always

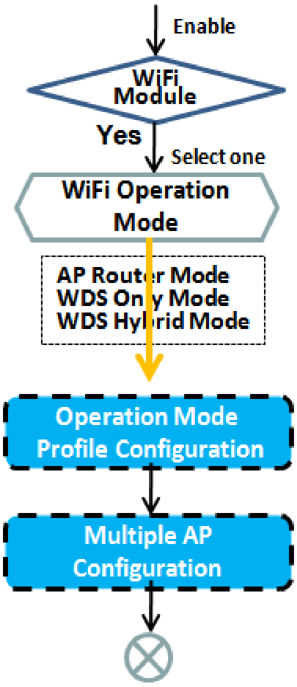
2.4G VAP List Add Delete

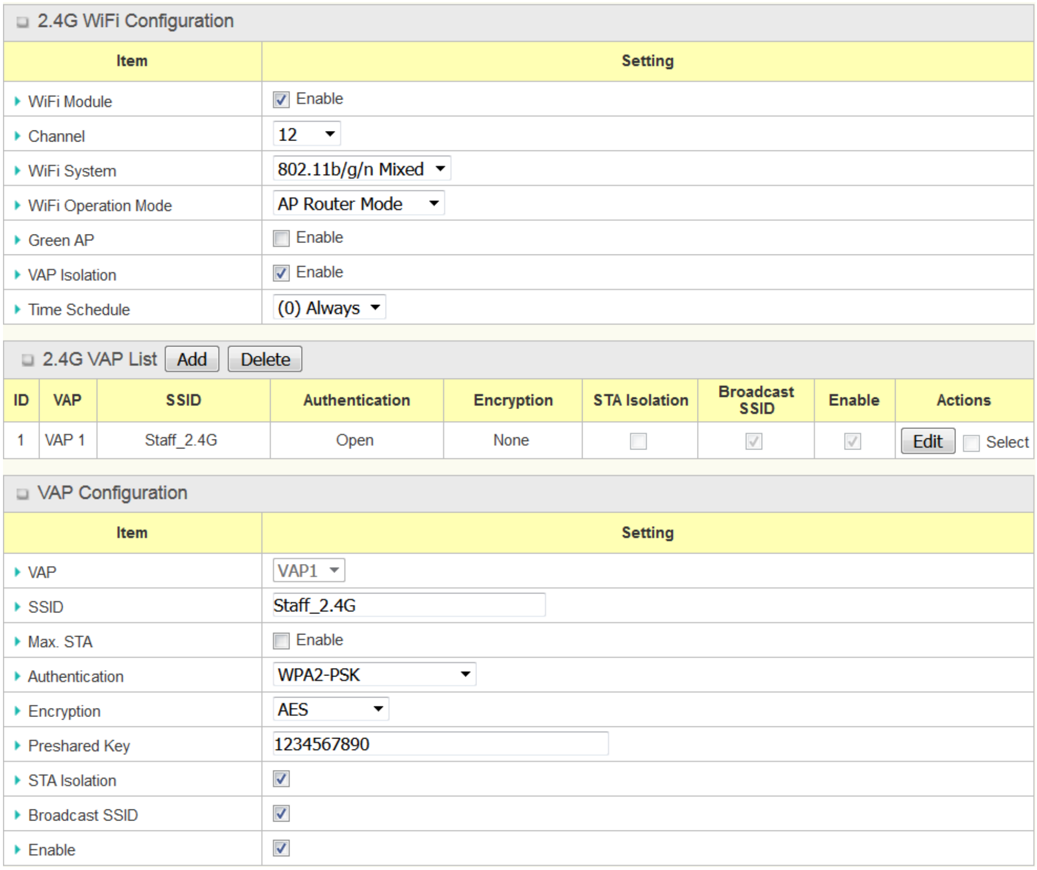
ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions

The router provides WiFi interface for mobile devices or BYOD devices to connect for Internet/Intranet accessing. WiFi function is usually modularized design in a router, and there can be single or dual modules within a router. The WiFi system in the router complies with IEEE 802.11n/11g/11b standard in 2.4GHz single band. There are several wireless operation modes provided by this device. They are: "**AP Router Mode**", "**WDS Only Mode**", and "**WDS Hybrid Mode**". You can choose the expected mode from the wireless operation mode list.

There are some sub-sections for you to configure the WiFi function, including "Basic Configuration" and "Advanced Configuration". In Basic Configuration section, you have to finish almost all the settings for using the WiFi function. And the Advanced Configuration section provides more parameters for advanced user to fine tune the connectivity performance for the WiFi function.

2.3.1 WiFi Configuration





2.4G WiFi Configuration

Item	Setting
WiFi Module	☑ Enable
Channel	12
WiFi System	802.11b/g/n Mixed
WiFi Operation Mode	AP Router Mode
Green AP	□ Enable
VAP Isolation	☑ Enable
Time Schedule	(0) Always

2.4G VAP List Add Delete

ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	Staff_2.4G	Open	None	□	☑	☑	Edit □ Select

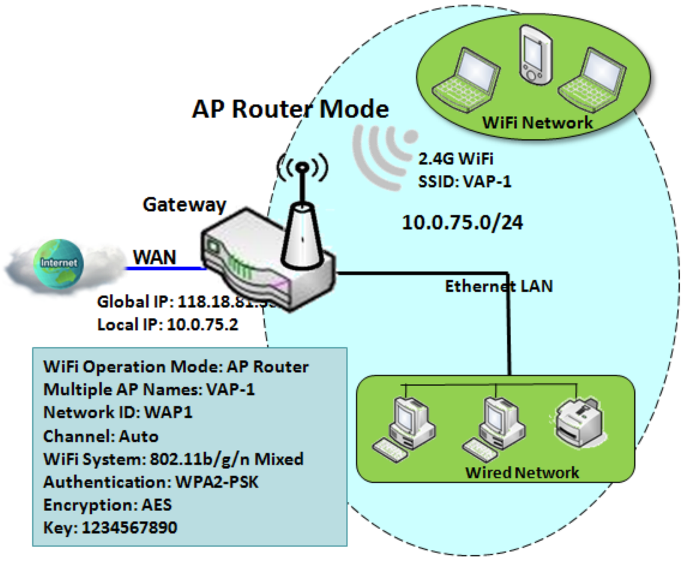
VAP Configuration

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

Due to optional module(s) and frequency band, you need to setup module one by one. For each module, you need to specify the operation mode, and then setup the virtual APs for wireless access.

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

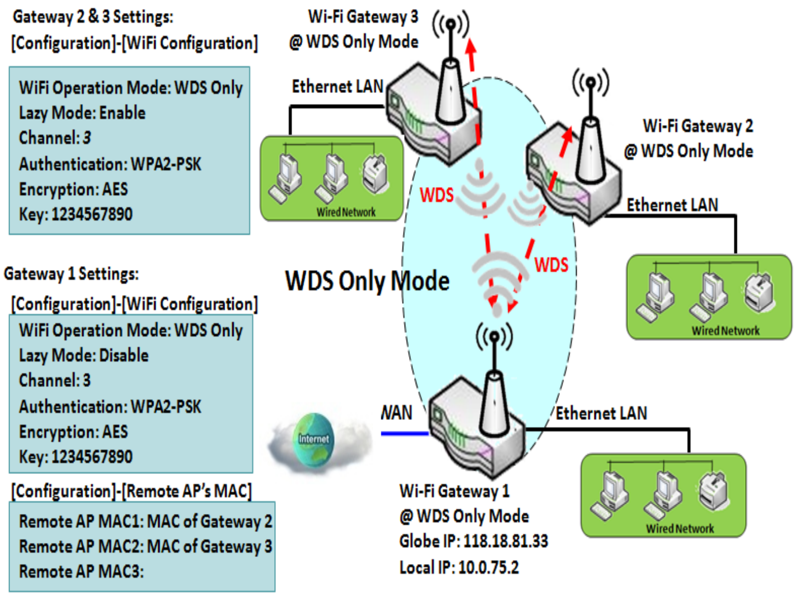
AP Router Mode



WiFi Operation Mode: AP Router
Multiple AP Names: VAP-1
Network ID: WAP1
Channel: Auto
WiFi System: 802.11b/g/n Mixed
Authentication: WPA2-PSK
Encryption: AES
Key: 1234567890

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

WDS Only Mode



Gateway 2 & 3 Settings:
[Configuration]-[WiFi Configuration]

WiFi Operation Mode: WDS Only
Lazy Mode: Enable
Channel: 3
Authentication: WPA2-PSK
Encryption: AES
Key: 1234567890

Gateway 1 Settings:
[Configuration]-[WiFi Configuration]

WiFi Operation Mode: WDS Only
Lazy Mode: Disable
Channel: 3
Authentication: WPA2-PSK
Encryption: AES
Key: 1234567890

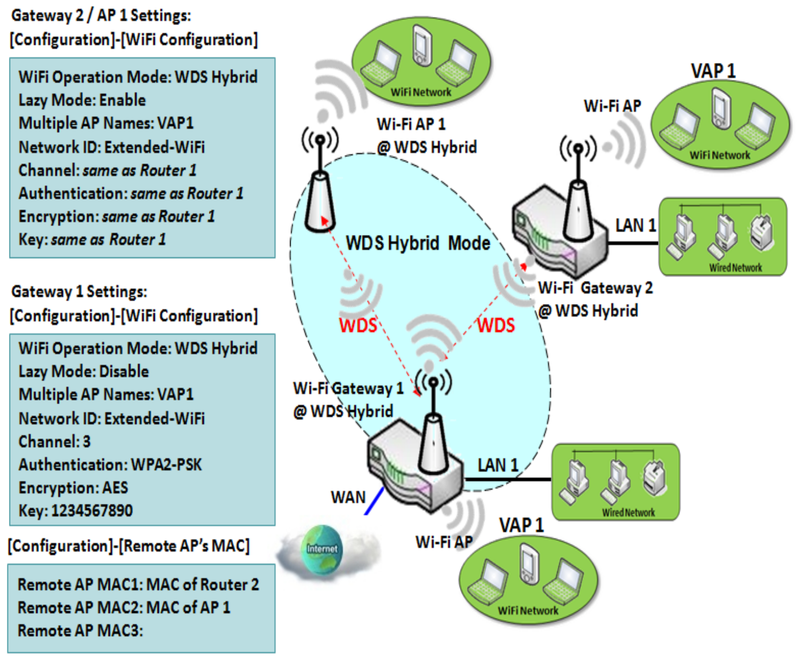
[Configuration]-[Remote AP's MAC]

Remote AP MAC1: MAC of Gateway 2
Remote AP MAC2: MAC of Gateway 3
Remote AP MAC3:

WDS (Wireless Distributed System) Only mode drives a WiFi gateway to be a bridge for its wired Intranet and a repeater to extend distance. You can use multiple WiFi gateways as a WiFi repeater chain with all gateways setup as "WDS Only" mode. All gateways can communicate with each other through WiFi. All wired client hosts within each gateway can also communicate each other in the scenario. Only one gateway within repeater chain can be DHCP server to provide IP for all wired client hosts of every gateway which being disabled DHCP server. This router can be NAT router to provide internet access.

The diagram illustrates that there are two wireless gateways 2, 3 running at "WDS Only" mode. They both use channel 3 to link to local Gateway 1 through WDS. Both gateways connected by WDS need to setup the remote AP MAC for each other. All client hosts under gateway 2, 3 can request IP address from the DHCP server at gateway 1. Besides, wireless Gateway 1 also execute the NAT mechanism for all client hosts Internet accessing.

WDS Hybrid Mode



Gateway 2 / AP 1 Settings:
[Configuration]-[WiFi Configuration]

WiFi Operation Mode: WDS Hybrid
Lazy Mode: Enable
Multiple AP Names: VAP1
Network ID: Extended-WiFi
Channel: *same as Router 1*
Authentication: *same as Router 1*
Encryption: *same as Router 1*
Key: *same as Router 1*

Gateway 1 Settings:
[Configuration]-[WiFi Configuration]

WiFi Operation Mode: WDS Hybrid
Lazy Mode: Disable
Multiple AP Names: VAP1
Network ID: Extended-WiFi
Channel: 3
Authentication: WPA2-PSK
Encryption: AES
Key: 1234567890

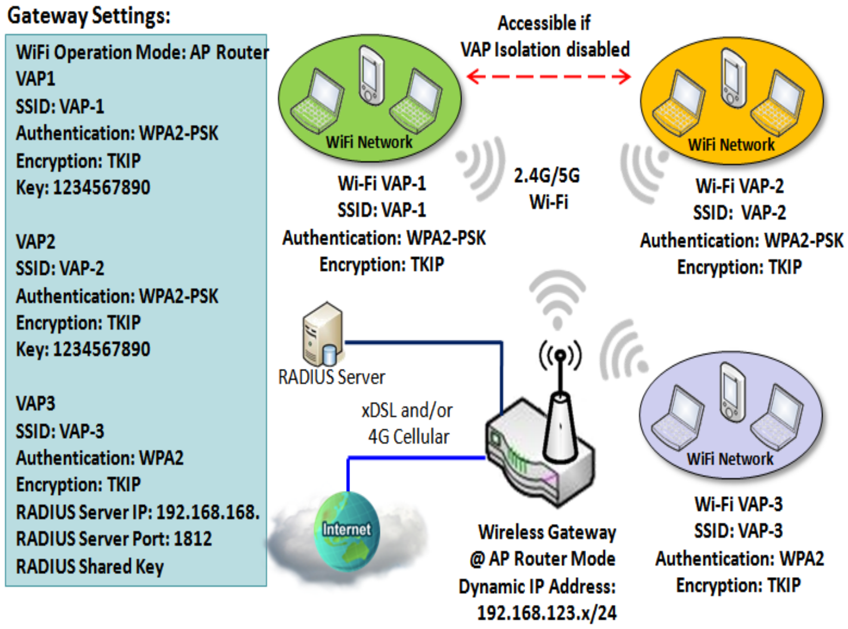
[Configuration]-[Remote AP's MAC]

Remote AP MAC1: MAC of Router 2
Remote AP MAC2: MAC of AP 1
Remote AP MAC3:

WDS hybrid mode includes both WDS and AP Router mode. WDS Hybrid mode can act as an access point for its WiFi Intranet and a WiFi bridge for its wired and WiFi Intranets at the same time. Users can thus use the features to build up a large wireless network in a large space like airports, hotels or campus.

The diagram illustrates Gateway 1, Gateway 2 and AP 1 connected by WDS. Each gateway has access point function for WiFi client access. Gateway 1 has DHCP server to assign IP to each client hosts. All gateways and AP are under WDS hybrid mode. To setup WDS hybrid mode, it need to fill all configuration items similar to that of AP-router and WDS modes.

Multiple VAPs



Gateway Settings:

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

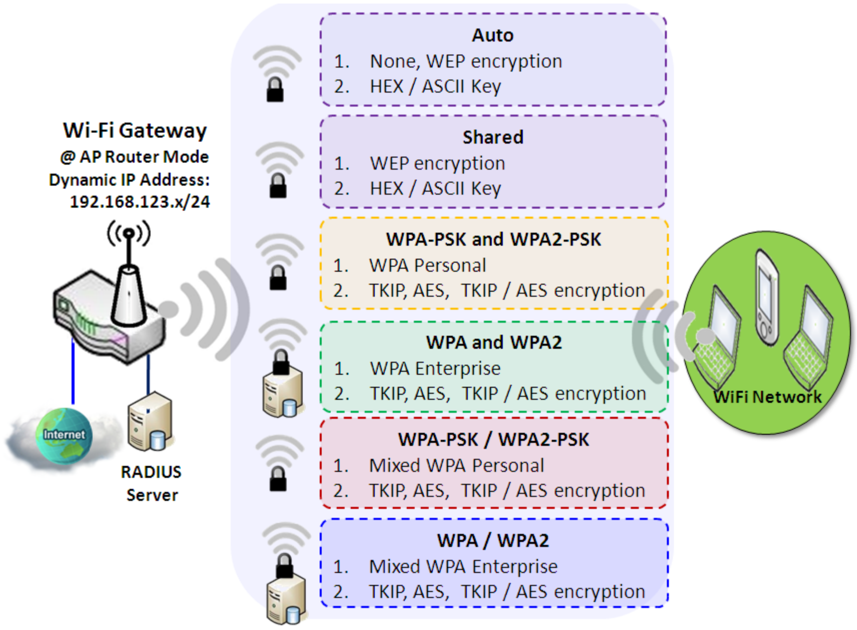
VAP2
SSID: VAP-2
Authentication: WPA2-PSK
Encryption: TKIP
Key: 1234567890

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

VAP (Virtual Access Point) is function to partition wireless network into multiple broadcast domains. It can simulate multiple APs in one physical AP. This wireless gateway supports up to 2 VAPs. For each VAP, you need to setup SSID, authentication and encryption to control Wi-Fi client access.

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

Wi-Fi Security – Authentication & Encryption



Wi-Fi security provides complete authentication and encryption mechanisms to enhance the data security while your data is transferred wirelessly over the air. The wireless gateway supports Shared, WPA-PSK / WPA2-PSK and WPA / WPA2 authentication. You can select one authentication scheme to validate the wireless clients while they are connecting to the AP. As to the data encryption, the router supports WEP, TKIP and AES. The selected encryption algorithm will be applied to the data while the wireless connection is established.

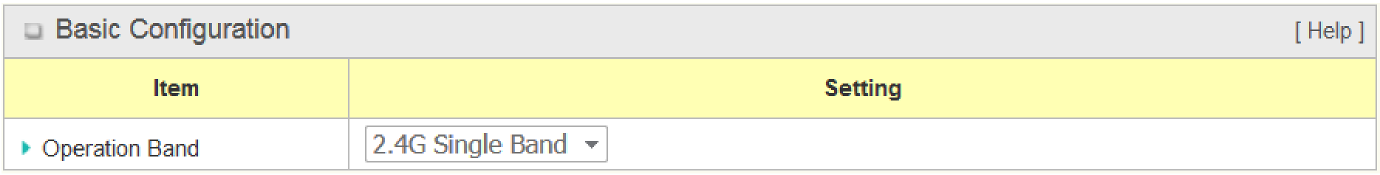
WiFi Configuration Setting

The WiFi configuration allows user to configure 2.4GHz WiFi settings.

Go to **Basic Network > WiFi > WiFi Module One** Tab.

If the gateway is equipped with two WiFi modules, there will be another **WiFi Module Two**. You can do the similar configurations on both WiFi modules.

Basic Configuration

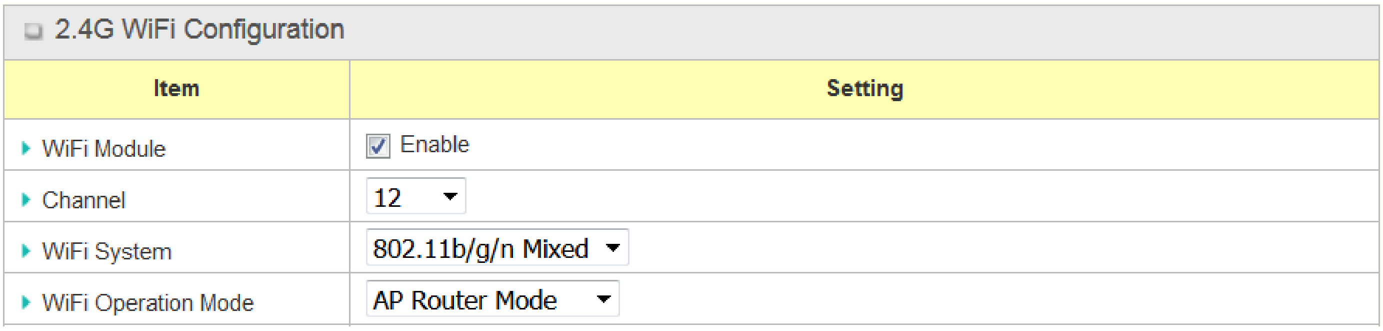


Basic Configuration [Help]

Item	Setting
Operation Band	2.4G Single Band ▾

Basic Configuration		
Item	**Value setting**	**Description**
Operation Band	A Must filled setting	Specify the intended operation band for the WiFi module. Basically, this setting is fixed and cannot be changed once the module is integrated into the product. However, there is some module with selectable band for user to choose according to his network environment. Under such situation, you can specify which operation band is suitable for the application.

Configure WiFi Setting



2.4G WiFi Configuration

Item	Setting
WiFi Module	☑ Enable
Channel	12
WiFi System	802.11b/g/n Mixed
WiFi Operation Mode	AP Router Mode

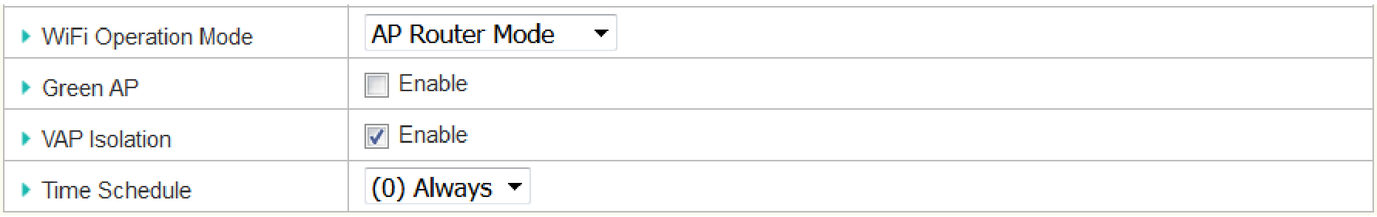
Configuring Wi-Fi Settings

Item	Value setting	Description
WiFi Module	The box is checked by default	Check the **Enable** box to activate Wi-Fi function.
Channel	1. A Must filled setting. 2. **Auto** is selected be default.	Select a radio channel for the VAP. Each channel is corresponding to different radio band. The permissible channels depend on the **Regulatory Domain**. There are two available options when **Auto** is selected: ● **By AP Numbers** The channel will be selected according to AP numbers (The less, the better). ● **By Less Interference** The channel will be selected according to interference. (The lower, the better).
WiFi System	A Must filled setting	Specify the preferred WiFi System. The dropdown list of **WiFi system** is based on **IEEE 802.11** standard. ● **2.4G WiFi** can select b, g and n only or mixed with each other.
WiFi Operation Mode		Specify the **WiFi Operation Mode** according to your application. Go to the following table for **AP Router Mode**, **WDS Only Mode**, and **WDS Hybrid Mode** settings. Note: The available operation modes depend on the product specification.

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

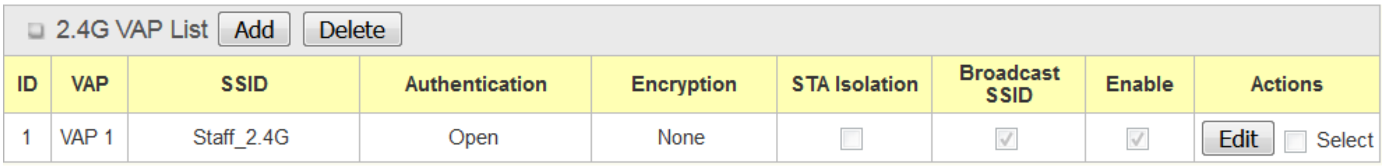
AP Router Mode & VAPs Configuration

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



WiFi Operation Mode	AP Router Mode
Green AP	□ Enable
VAP Isolation	☑ Enable
Time Schedule	(0) Always

AP Router Mode		
Item	**Value setting**	**Description**
Green AP	The box is unchecked by default.	Check the **Enable** box to activate **Green AP** function.
VAP Isolation	The box is checked by default.	Check the **Enable** box to activate this function. By default, the box is checked; it means that stations which associated to different VAPs cannot communicate with each other.
Time Schedule	A Must filled setting	Apply a specific **Time Schedule** to this rule; otherwise leave it as **(0) Always**. If the dropdown list is empty ensure **Time Schedule** is pre-configured. Refer to **Object Definition** > **Scheduling > Configuration** tab.



ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	Staff_2.4G	Open	None	□	☑	☑	Edit □ Select

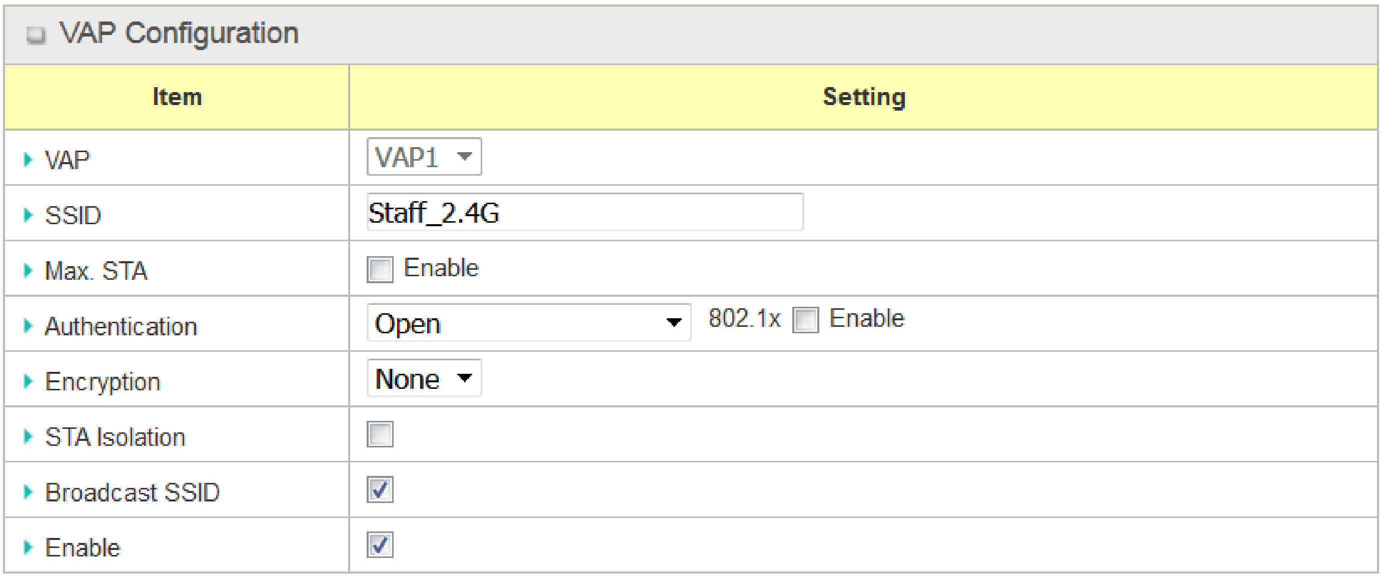
By default, VAP 1 is enabled and security key is required to connect to the gateway wirelessly to enhance the security level and prevent unexpected access of un-authorized devices.

The default WiFi key is printed on both the device label and the Security Card. It is created randomly and differs from devices. So, you can connected to the VAP1 (SSID: Staff_2.4G) with the provided key.

However, it is strongly recommended that you have to change the security key to easy-to-remember one by clicking the Edit button.

Click **Add** / **Edit** button in the VAP List screen to create or edit the settings for a VAP. A VAP Configuration screen will appear.

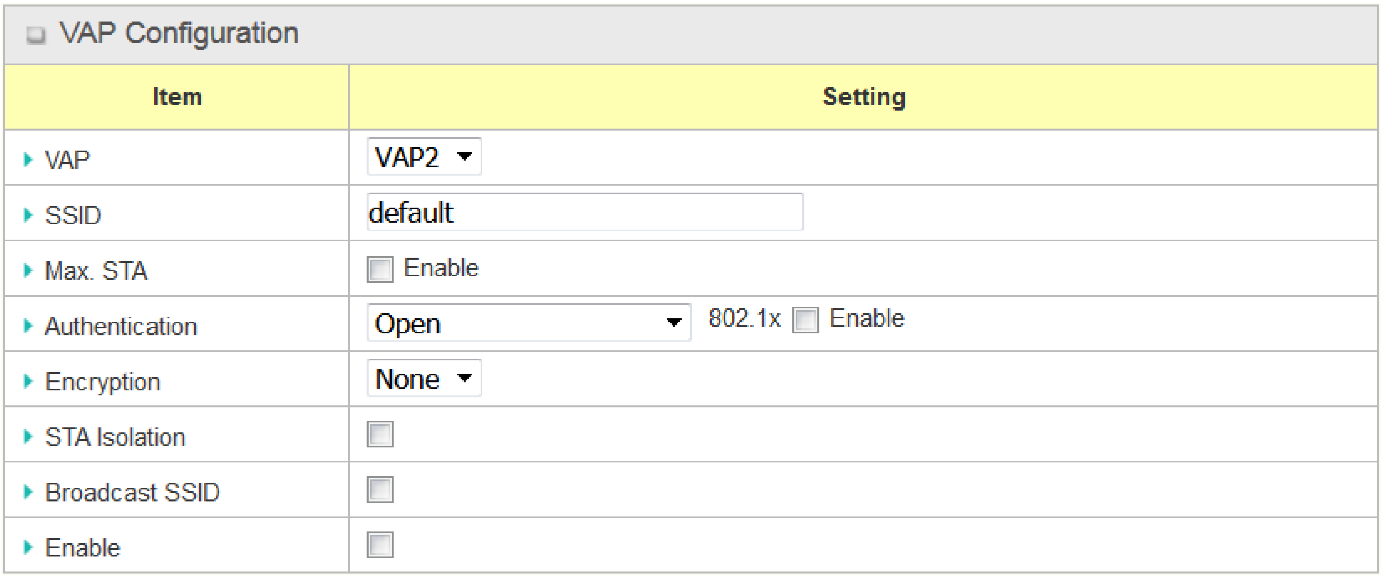
For VAP 1:



VAP Configuration

Item	Setting
VAP	VAP1
SSID	Staff_2.4G
Max. STA	□ Enable
Authentication	Open 802.1x □ Enable
Encryption	None
STA Isolation	□
Broadcast SSID	☑
Enable	☑

For others:



VAP Configuration

Item	Setting
VAP	VAP2
SSID	default
Max. STA	□ Enable
Authentication	Open 802.1x □ Enable
Encryption	None
STA Isolation	□
Broadcast SSID	□
Enable	□

VAP Configuration

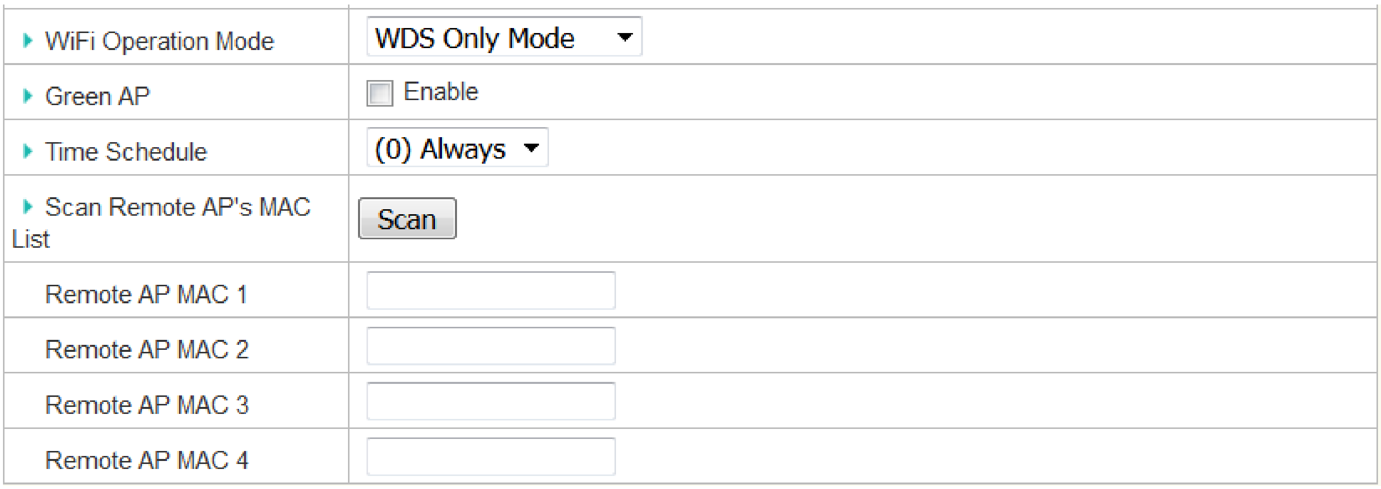
Item	Value setting	Description
SSID	1. String format : Any text	Enter the SSID for the VAP, and decide whether to broadcast the SSID or not. The **SSID** is used for identifying from another AP, and client stations will associate with AP according to SSID.
Max. STA	The box is unchecked by default.	Check this box and enter a limitation to limit the maximum number of client station. The box is unchecked by default. It means no special limitation on the number of connected STAs.
Authentication	1. A Must filled setting 2. VAP1: **WPA2-PSK** is selected be default; Others: **Open** is selected be default.	For security, there are several authentication methods supported. Client stations should provide the key when associate with this device.
		When **Open** is selected The check box named **802.1x** shows up next to the dropdown list. ● **802.1x** (The box is unchecked by default) When **802.1x** is enabled, it means the client stations will be authenticated by RADIUS server. **RADIUS Server IP** (The default IP is 0.0.0.0) **RADIUS Server Port** (The default value is 1812) **RADIUS Shared Key**
		When **Shared** is selected The pre-shared WEP key should be set for authenticating.
		When **Auto** is selected The device will select **Open** or **Shared** by requesting of client automatically. The check box named **802.1x** shows up next to the dropdown list. ● **802.1x** (The box is unchecked by default) When **802.1x** is enabled, it means the client stations will be authenticated by RADIUS server. **RADIUS Server IP** (The default IP is 0.0.0.0) **RADIUS Server Port** (The default value is 1812) **RADIUS Shared Key**

		When **WPA** or **WPA2** is selected They are implementation of IEEE 802.11i. **WPA** only had implemented part of IEEE 802.11i, but owns the better **compatibility**. **WPA2** had fully implemented 802.11i standard, and owns the highest **security**. ● **RADIUS Server** The client stations will be authenticated by RADIUS server. **RADIUS Server IP** (The default IP is 0.0.0.0) **RADIUS Server Port** (The default value is 1812) **RADIUS Shared Key**
		When **WPA** / **WPA2** is selected It owns the same setting as **WPA** or **WPA2**. The client stations can associate with this device via **WPA** or **WPA2**.
		When **WPA-PSK** or **WPA2-PSK** is selected It owns the same encryption system as WPA or WPA2. The authentication uses pre-shared key instead of RADIUS server.
		When **WPA-PSK** / **WPA2-PSK** is selected It owns the same setting as **WPA-PSK** or **WPA2-PSK**. The client stations can associate with this device via **WPA-PSK** or **WPA2-PSK**.
Encryption	1. A Must filled setting. 2. VAP1: **AES** is selected be default; Others: **None** is selected be default.	Select a suitable encryption method and enter the required key(s). The available method in the dropdown list depends on the Authentication you selected. **None** It means that the device is open system without encrypting. **WEP** Up to 4 WEP keys can be set, and you have to select one as current key. The key type can set to **HEX** or **ASCII**. If **HEX** is selected, the key should consist of (0 to 9) and (A to F). If **ASCII** is selected, the key should consist of ASCII table. **TKIP** TKIP was proposed instead of WEP without upgrading hardware. Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters. **AES** The newest encryption system in WiFi, it also designed for the fast 802.11n high bitrates schemes. Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters. You are recommended to use **AES** encryption instead of any others for security. **TKIP / AES** **TKIP / AES** mixed mode. It means that the client stations can associate with this device via **TKIP** or **AES**. Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters.
STA Isolation	VAP1: The box is checked by default; Others: unchecked by default.	Check the **Enable** box to activate this function. By default, the box is checked; it means that stations which associated to the same VAP cannot communicate with each other.
Broadcast SSID	VAP1: The box is checked by default; Others: unchecked by default.	Check the **Enable** box to activate this function. If the broadcast SSID option is enabled, it means the SSID will be broadcasted, and the stations can associate with this device by scanning SSID.
Enable	VAP1: The box is checked by default; Others: unchecked by default.	Check the **Enable** box to activate this VAP.

Save	N/A	Click the **Save** button to save the current configuration.
Undo	N/A	Click the **Undo** button to restore configuration to previous setting before saving.
Apply	N/A	Click the **Apply** button to apply the saved configuration.

WDS Only Mode

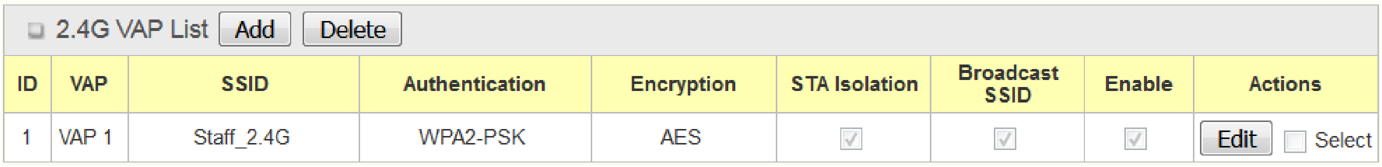
For the WDS Only mode, the device only bridges the connected wired clients to another WDS-enabled WiFi device which the device associated with. That is, it also means the no wireless clients stat can connect to this device while WDS Only Mode is selected.



WiFi Operation Mode	WDS Only Mode ▾
Green AP	□ Enable
Time Schedule	(0) Always ▾
Scan Remote AP's MAC List	Scan
Remote AP MAC 1	
Remote AP MAC 2	
Remote AP MAC 3	
Remote AP MAC 4	

WDS Only Mode

Item	Value setting	Description
Green AP	The box is unchecked by default.	Check the **Enable** box to activate **Green AP** function.
Time Schedule	A Must filled setting	Apply a specific **Time Schedule** to this rule; otherwise leave it as **(0) Always**. If the dropdown list is empty ensure **Time Schedule** is pre-configured. Refer to **Object Definition** > **Scheduling > Configuration** tab.
Scan Remote AP's MAC List	N/A	Press the **Scan** button to scan the spatial AP information, and then select one from the AP list, the MAC of selected AP will be auto filled in the following Remote AP MAC table.
Remote AP MAC 1~4	A Must filled setting	Enter the remote AP's MAC manually, or via auto-scan approach, The device will bridge the traffic to the remote AP when associated successfully.



2.4G VAP List Add Delete

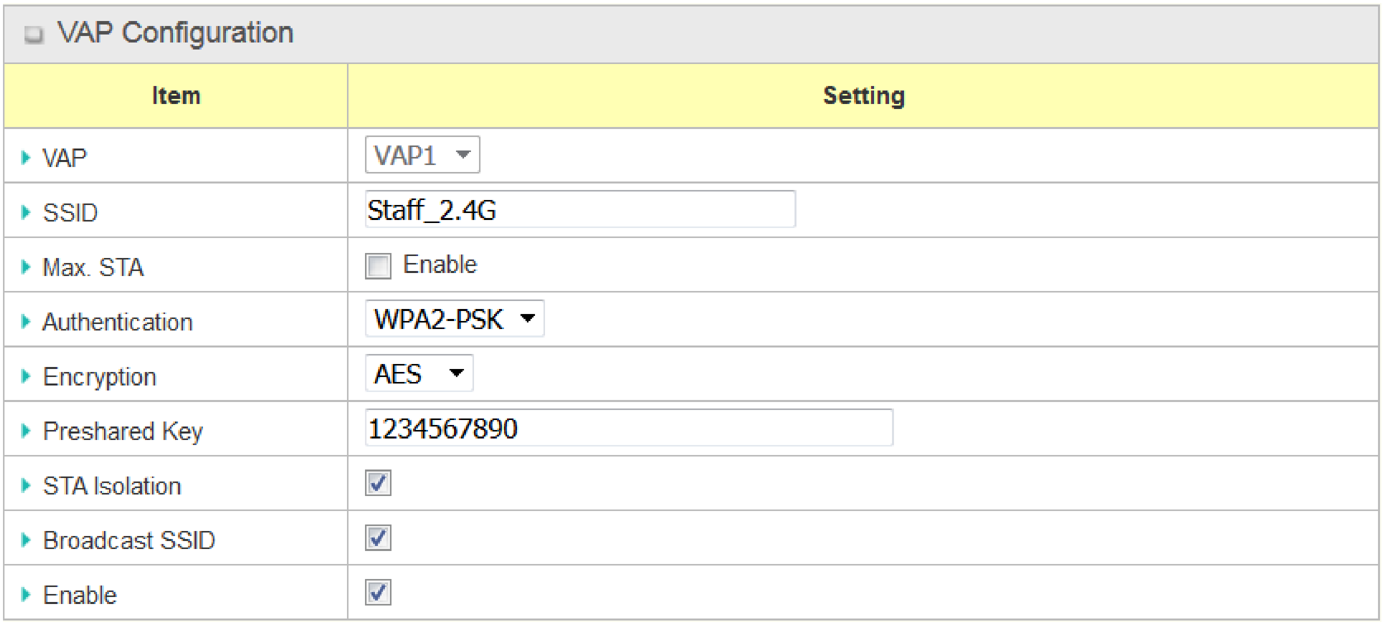
ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	Staff_2.4G	WPA2-PSK	AES	☑	☑	☑	Edit □ Select

By default, VAP 1 is enabled and security key is required to connect to the gateway wirelessly to enhance the security level and prevent unexpected access of un-authorized devices.

The default WiFi key is printed on both the device label and the Security Card. It is created randomly and differs from devices. So, you can connected to the VAP1 (SSID: Staff_2.4G) with the provided key.

However, it is strongly recommended that you have to change the security key to an easy-to-remember one by clicking the Edit button.

Under **WDS Only** mode, only VAP1 is available for further specifying the required authentication and Encryption settings. Click **Edit** button in the VAP List screen and a VAP Configuration screen will appear for you to configure the required settings



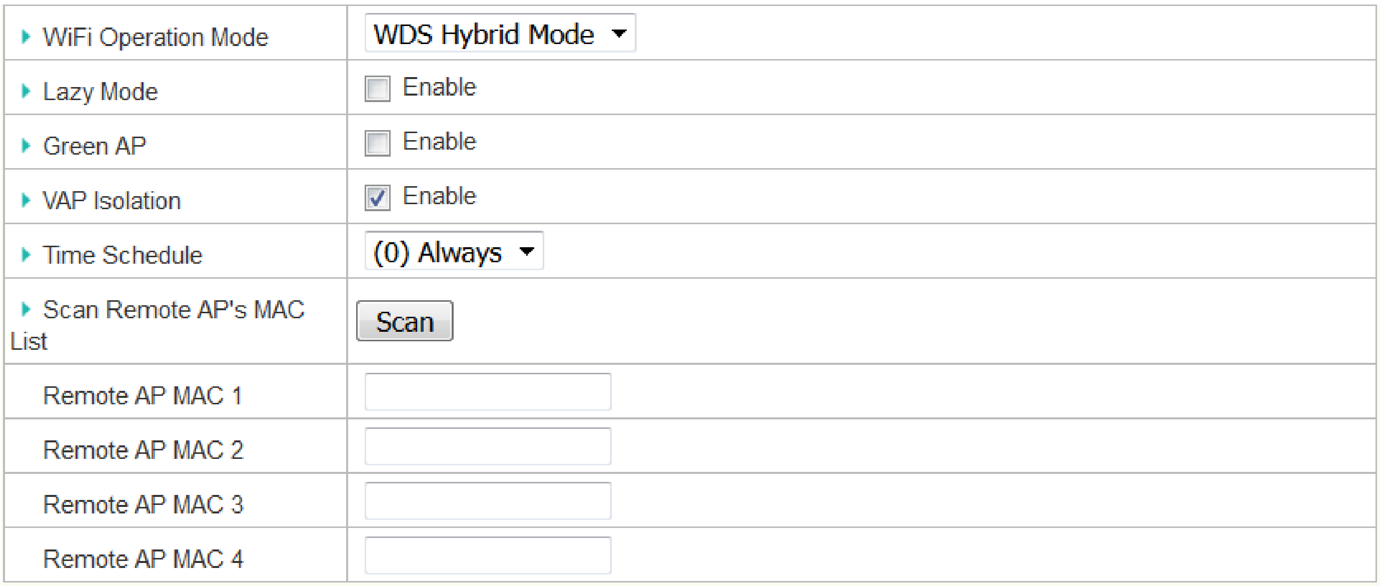
VAP Configuration

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

For the detail description about VAP configuration, please refer to the description stated in AP-Router section.

WDS Hybrid Mode

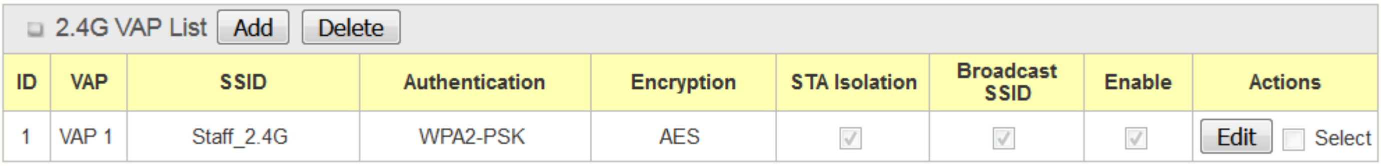
For the WDS Hybrid mode, the device bridges all the wired **LAN** and **WLAN** clients to another WDS or WDS hybrid enabled WiFi devices which the device associated with.



WiFi Operation Mode	WDS Hybrid Mode
Lazy Mode	□ Enable
Green AP	□ Enable
VAP Isolation	☑ Enable
Time Schedule	(0) Always
Scan Remote AP's MAC List	Scan
Remote AP MAC 1	
Remote AP MAC 2	
Remote AP MAC 3	
Remote AP MAC 4	

WDS Hybrid Mode

Item	Value setting	Description
Lazy Mode	The box is checked by default.	Check the **Enable** box to activate this function. With the function been enabled, the device can auto-learn WDS peers without manually entering other AP's MAC address. But at least one of the APs has to fill remote AP MAC addresses.
Green AP	The box is unchecked by default.	Check the **Enable** box to activate **Green AP** function.
VAP Isolation	The box is checked by default.	Check the **Enable** box to activate this function. By default, the box is checked; it means that stations which associated to different VAPs cannot communicate with each other.
Time Schedule	A Must filled setting	Apply a specific **Time Schedule** to this rule; otherwise leave it as **(0) Always**. If the dropdown list is empty ensure **Time Schedule** is pre-configured. Refer to **Object Definition** > **Scheduling > Configuration** tab.
Scan Remote AP's MAC List	Available when Lazy Mode disabled.	Press the **Scan** button to scan the spatial AP information, and then select one from the AP list, the MAC of selected AP will be auto filled in the following Remote AP MAC table.
Remote AP MAC 1~4	Available when Lazy Mode disabled.	Enter the remote AP's MAC manually, or via auto-scan approach, The device will bridge the traffic to the remote AP when associated successfully.



2.4G VAP List Add Delete

ID	VAP	SSID	Authentication	Encryption	STA Isolation	Broadcast SSID	Enable	Actions
1	VAP 1	Staff_2.4G	WPA2-PSK	AES	☑	☑	☑	Edit □ Select

By default, VAP 1 is enabled and security key is required to connect to the gateway wirelessly to enhance the security level and prevent unexpected access of un-authorized devices.

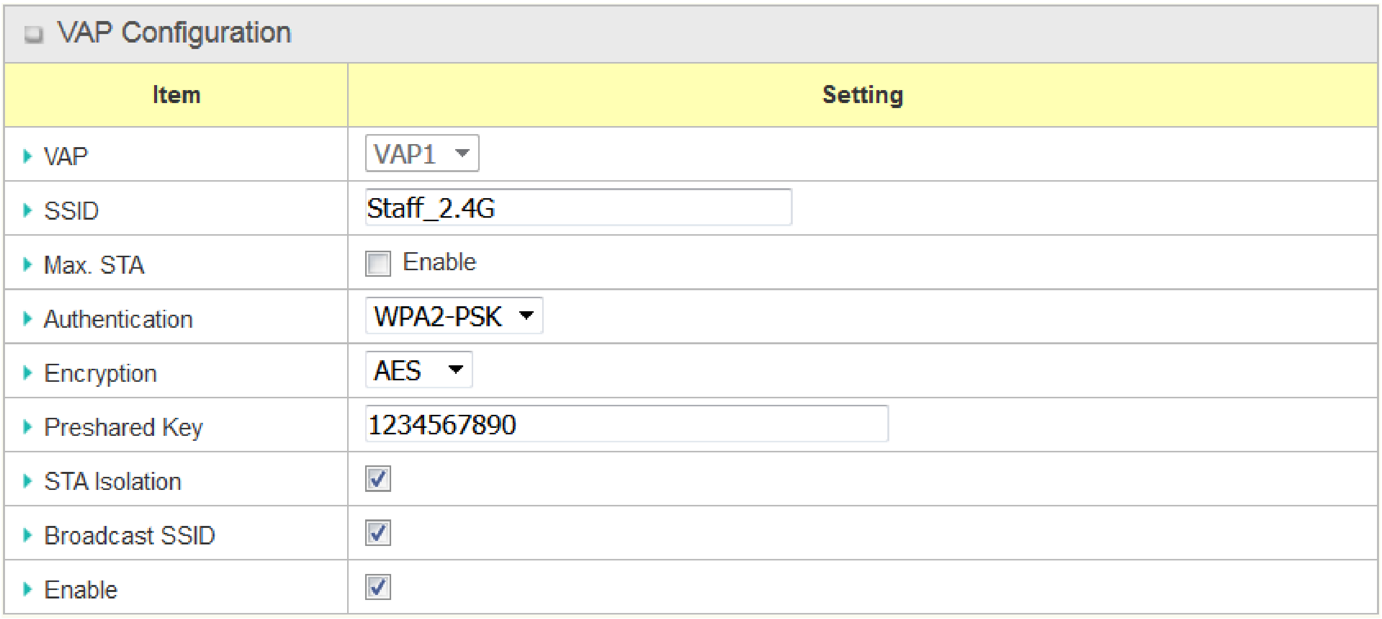
The default WiFi key is printed on both the device label and the Security Card. It is created randomly and differs from devices. So, you can connected to the VAP1 (SSID: Staff_2.4G) with the provided key.

However, it is strongly recommended that you have to change the security key to an easy-to-remember one by clicking the Edit button.

Under **WDS Hybrid** mode, the VAP function is available and you can further specifying the required VAP settings for connecting with wireless client devices.

Click **Add** / **Edit** button in the VAP List screen to create or edit the settings for a VAP. A VAP Configuration screen will appear.

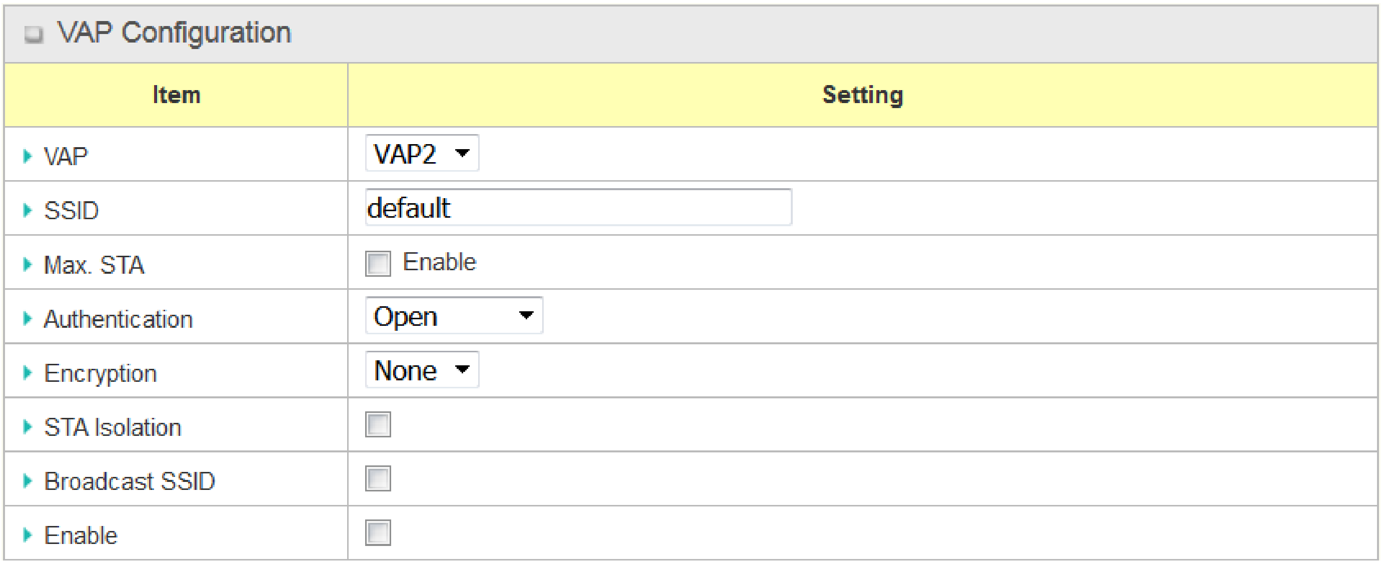
For VAP 1:



VAP Configuration

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

For others:



VAP Configuration

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

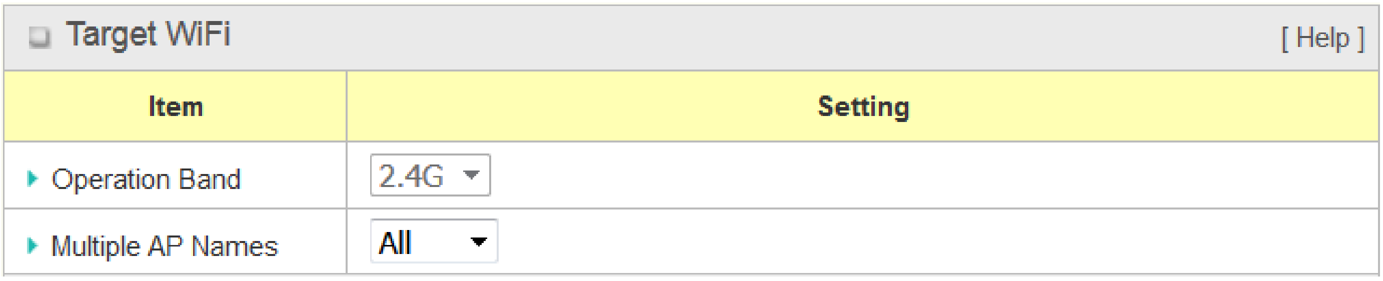
For the detail description about VAP configuration, please refer to the description stated in AP-Router section.

2.3.2 Wireless Client List

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

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

Select Target WiFi



Target WiFi [Help]

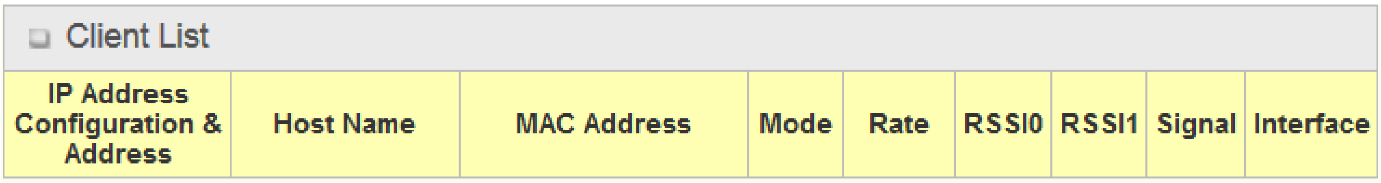
Item	Setting
Operation Band	2.4G
Multiple AP Names	All

Target Configuration		
Item	**Value setting**	**Description**
Operation Band	A Must filled setting.	Specify the intended operation band for the WiFi module. Basically, this setting is fixed and cannot be changed once the module is integrated into the product. However, there is some module with selectable band for user to choose according to his network environment. Under such situation, you can specify which operation band is suitable for the application.

Multiple AP Names	1. A Must filled setting. 2. **All** is selected by default.	Specify the VAP to show the associated clients information in the following Client List. By default, All VAP is selected.

Show Client List

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



Client List

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

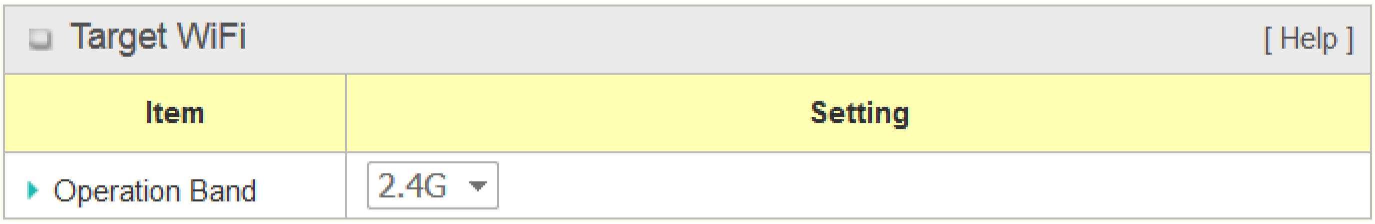
Target Configuration Item	Value setting	Description
IP Address Configuration & Address	N/A	It shows the Client's IP address and the deriving method. **Dynamic** means the IP address is derived from a DHCP server. **Static** means the IP address is a fixed one that is self-filled by client.
Host Name	N/A	It shows the host name of client.
MAC Address	N/A	It shows the MAC address of client.
Mode	N/A	It shows what kind of **Wi-Fi system** the client used to associate with this device.
Rate	N/A	It shows the **data rate** between client and this device.
RSSI0, RSSI1	N/A	It shows the RX sensitivity (RSSI) value for each radio path.
Signal	N/A	The **signal strength** between client and this device.
Interface	N/A	It shows the VAP ID that the client associated with.
Refresh	N/A	Click the **Refresh** button to update the Client List immediately.

2.3.3 Advanced Configuration

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

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

Select Target WiFi

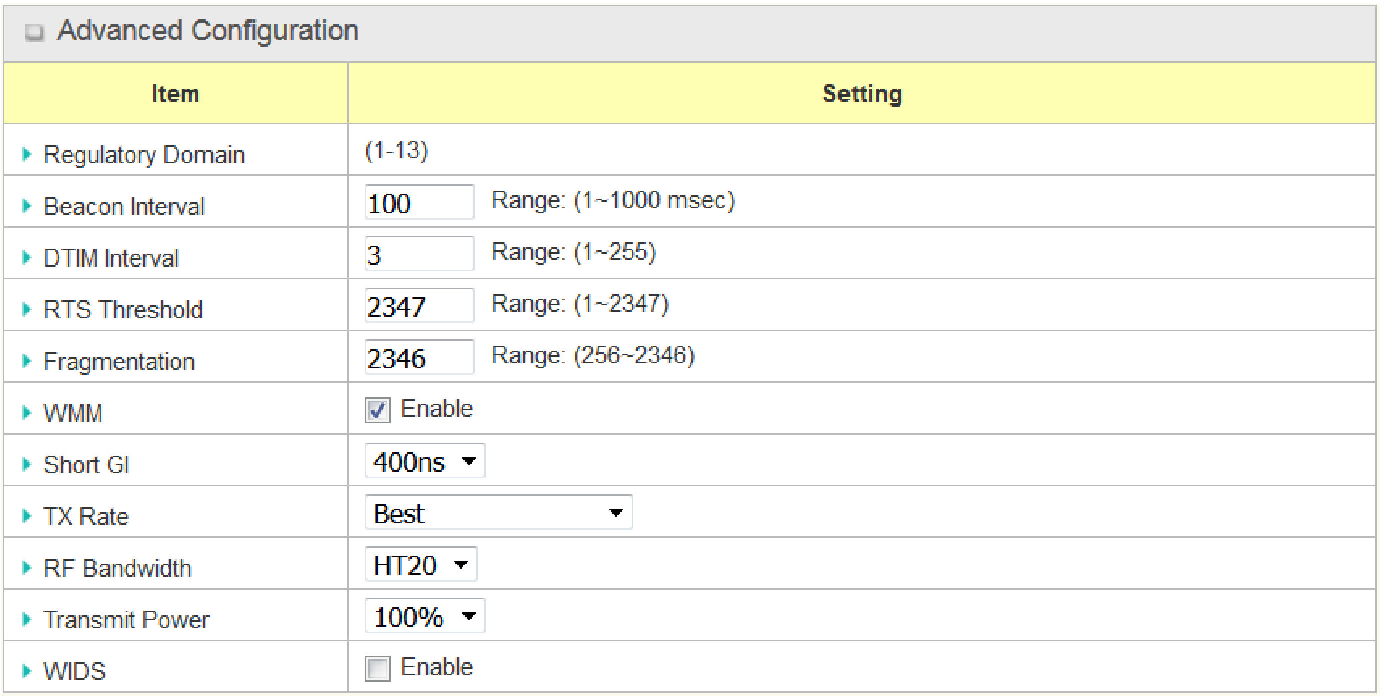


Target WiFi

Item	Setting
Operation Band	2.4G

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

Setup Advanced Configuration



Advanced Configuration

Item	Setting
Regulatory Domain	(1-13)
Beacon Interval	100 Range: (1~1000 msec)
DTIM Interval	3 Range: (1~255)
RTS Threshold	2347 Range: (1~2347)
Fragmentation	2346 Range: (256~2346)
WMM	☑ Enable
Short GI	400ns
TX Rate	Best
RF Bandwidth	HT20
Transmit Power	100%
WIDS	□ Enable

Advanced Configuration		
Item	**Value setting**	**Description**
Regulatory Domain	The default setting is according to where the product sale to	It limits the available radio channel of this device. The permissible channels depend on the **Regulatory Domain**.
Beacon Interval	100	It shows the time interval between each beacon packet broadcasted. The beacon packet contains **SSID**, **Channel ID** and **Security setting**.
DTIM Interval	3	A **DTIM (Delivery Traffic Indication Message)** is a countdown informing clients of the next window for listening to broadcast message. When the device has buffered broadcast message for associated client, it sends the next DTIM with a DTIM value.
RTS Threshold	2347	**RTS (Request to send) Threshold** means when the packet size is over the setting value, then active **RTS** technique. RTS/CTS is a **collision avoidance** technique. It means RTS **never** activated when the threshold is set to **2347**.
Fragmentation	2346	Wireless frames can be divided into smaller units (fragments) to **improve performance** in the presence of RF interference at the limits of RF coverage.
WMM	The box is checked by default	**WMM (Wi-Fi Multimedia)** can help control **latency** and **jitter** when transmitting **multimedia content** over a wireless connection.

Short GI	By default **400ns** is selected	**Short GI (Guard Interval)** is defined to set the sending interval between each packet. Note that lower **Short GI** could **increase** not only the **transition rate** but also **error rate**.
TX Rate	By default **Best** is selected	It means the **data transition rate**. When **Best** is selected, the device will choose a proper **data rat**e according to **signal strength**.
RF Bandwidth	By default **Auto** is selected	The setting of RF bandwidth limits the maximum data rate.
Transmit Power	By default **100%** is selected	Normally the wireless transmitter operates at 100% power. By setting the **transmit power** to control the Wi-Fi **coverage**.
WIDS	The box is unchecked by default	The WIDS (Wireless Intrusion Detection System) will analyze all packets and make a statistic table in WiFi status. Go to **Status** > **Basic Network** > **WiFi** tab for detailed WIDS status.
Save	N/A	Click the **Save** button to save the current configuration.
Undo	N/A	Click the **Undo** button to restore configuration to previous setting before saving.

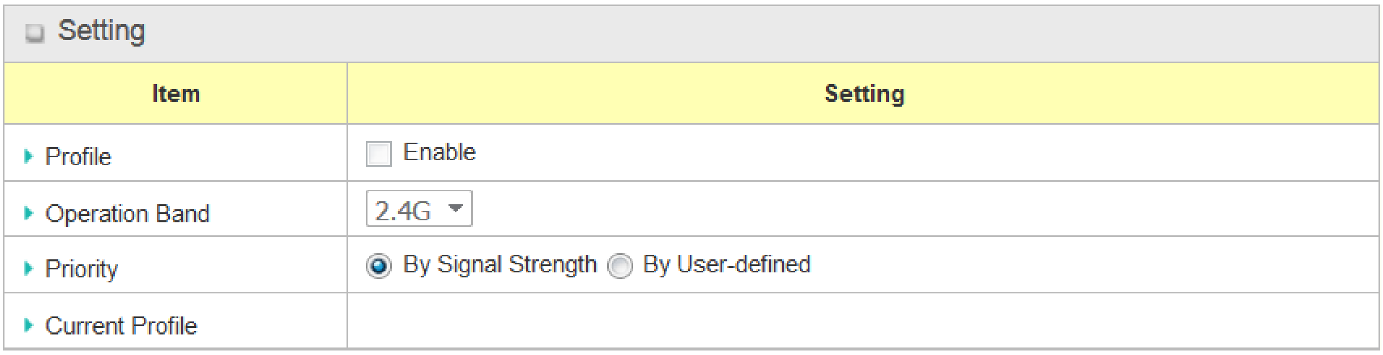
2.3.4 Uplink Profile

This device provides WiFi Uplink function for connecting to a wireless access point just like connected to a wired WAN or cellular WAN connection. It can operate as a NAT gateway and link the devices wirelessly to the uplink network or hosts.

To connect to the wireless access point, user has to enable the wireless Uplink function for a certain WiFi Module (refer to **Basic Network > WAN & Uplink > Physical Interface**, **Internet Setup** tabs) first, and then configure the Uplink profile(s) for the access point to be connected to in the **Uplink Profile** page.

Go to **Basic Network > WiFi > Uplink Profile** tab for configuring the Uplink Profile page.

Uplink Profile Setting



Setting

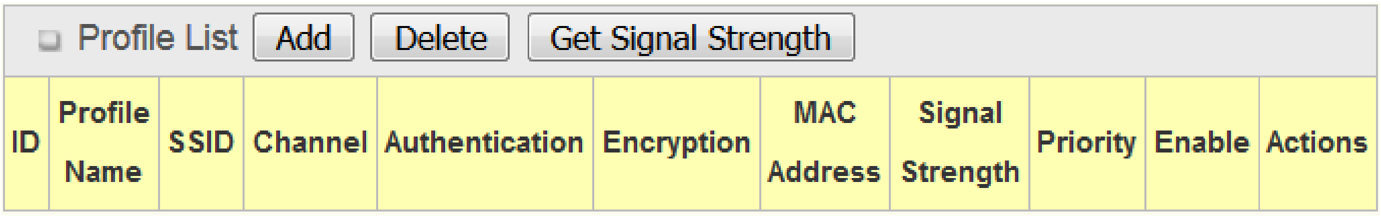
Item	Setting
Profile	□ Enable
Operation Band	2.4G
Priority	● By Signal Strength ○ By User-defined
Current Profile	

Setting		
Item	**Value setting**	**Description**
Profile	1. A Must filled setting. 2. **Unchecked** by default.	Check the **Enable** box to activate the profile function. It is available only when the selected WiFi module is configured at WiFi Uplink mode.
Module Select	A Must filled setting.	Select the WiFi module to check or configure the expected uplink profile(s). For those single WiFi module products, this option is hidden.

Operation Band	A Must filled setting.	Specify the intended operation band for the WiFi module. Basically, this setting is fixed and cannot be changed once the module is integrated into the router product. However, there are some module with selectable band for user to choose according to his network environment. Under such situation, you can specify which operation band is suitable for the application.
Priority	1. A Must filled setting. 2. **By Signal Strength** is selected by default.	Specify the network selection methodology for connection to an available wireless uplink network. It can be **By Signal Strength** or **By User-defined** priority. When **By Signal Strength** is selected, the router will try to connect to the available uplink network whose wireless signal strength is the strongest. When **By User-defined** is selected, the router will try to connect to the available uplink network whose priority is the highest (1 is the highest priority, and 16 is the lowest priority).

Note: to apply the defined Uplink profile(s) for the router to find a best fit profile for connecting to a certain uplink network, user has to **Enable** the Profile auto-connect function (Refer to **Basic Network > WiFi > (Module 1/ Module 2) WiFi Configuration** tab.

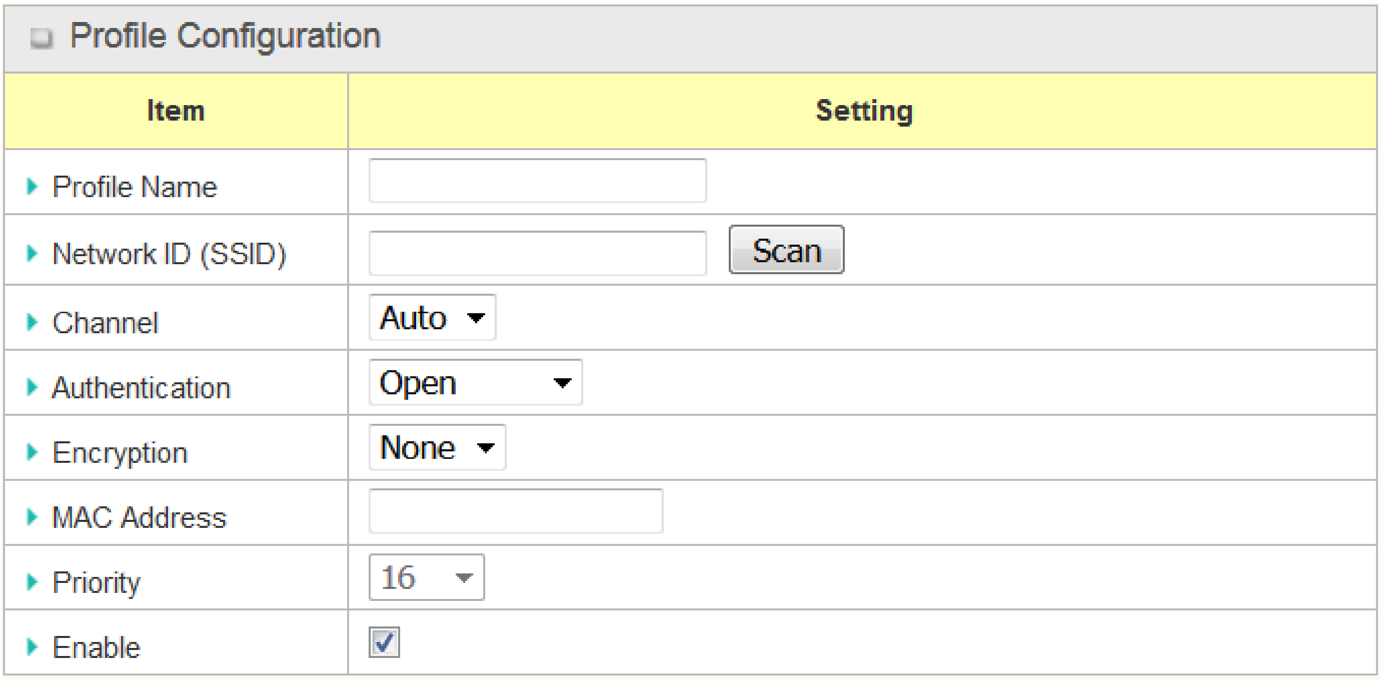
Create/Edit Uplink Profile



ID	Profile Name	SSID	Channel	Authentication	Encryption	MAC Address	Signal Strength	Priority	Enable	Actions

The Profile List shows the settings for the created uplink profiles. The information includes Profile Name, SSID, Channel, Authentication, Encryption, MAC Address, Signal Strength, Priority, and Enable.

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



Profile Configuration

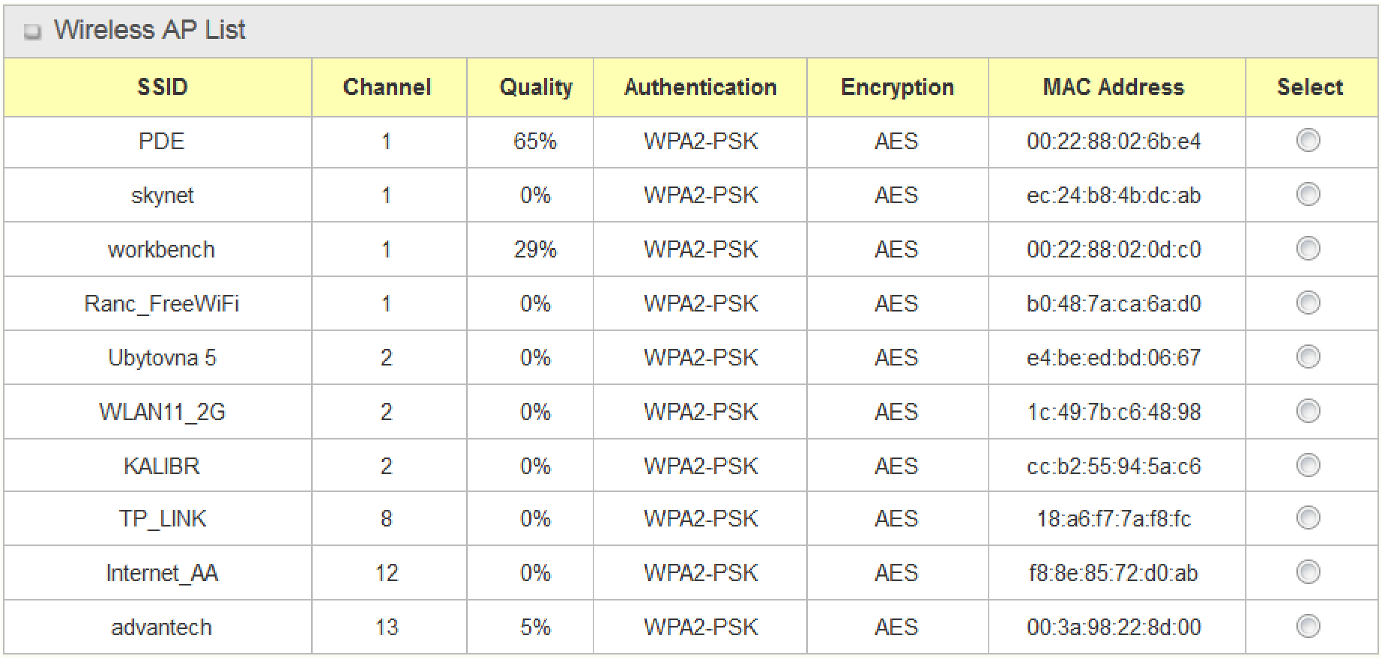
Item	Setting
Profile Name	
Network ID (SSID)	Scan
Channel	Auto
Authentication	Open
Encryption	None
MAC Address	
Priority	16
Enable	☑

Profile Configuration		
Item	**Value setting**	**Description**
Profile Name	1. String format can be any text 2. A Must filled setting	Enter a profile name for the uplink network specified below. It is a name that is easy for you to understand. ***Value Range*:** 1 ~ 64 characters.
Network ID (SSID)	1. String format : Any text 2. The box is checked by default.	Enter the SSID for the VAP, and decide whether to broadcast the SSID or not. The **SSID** is used for identifying from another AP, and client stations will associate with AP according to SSID. If the broadcast SSID option is enabled, it means the SSID will be broadcasted, and the stations can associate with this device by scanning SSID.
Channel	1. A Must filled setting. 2. **Auto** is selected by default.	Select a radio channel for the VAP. Each channel is corresponding to different radio band. The permissible channels depend on the **Regulatory Domain**. There are two available options when **Auto** is selected: ● **By AP Numbers** The channel will be selected according to AP numbers (The less, the better). ● **By Less Interference** The channel will be selected according to interference. (The lower, the better).
Authentication	1. A Must filled setting 2. **Open** is selected by default.	Specify the authentication method for connecting with the uplink network. It can be **Open**, **Shared**, **WPA-SPK**, or **WPA2-PSK**. When **Open** is selected, the pre-shared WEP key could be set for authentication; When **Shared** is selected, the pre-shared WEP key should be set for authentication; When **WPA-PSK** or **WPA2-PSK** is selected, The TKIP or AES pre-shared key should be set for authentication;

Encryption	1. A Must filled setting. 2. **None** is selected by default.	Select a suitable encryption method and enter the required key(s). The available method in the dropdown list depends on the Authentication you selected. **None** It means that the device is open system without encrypting. **WEP** Up to 4 WEP keys can be set, and you have to select one as current key. The key type can set to **HEX** or **ASCII**. If **HEX** is selected, the key should consist of (0 to 9) and (A to F). If **ASCII** is selected, the key should consist of ASCII table. **TKIP** TKIP was proposed instead of WEP without upgrading hardware. Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters. **AES** The newest encryption system in WiFi, it also designed for the fast 802.11n high bitrates schemes. Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters. You are recommended to use **AES** encryption instead of any others for security.
MAC Address	1. MAC Address string Format 2. A Must fill setting	Specify the **MAC Address** of the access point (with the Network ID) to be connected to.
Priority	1. An Optional filled setting. 2. **16** is set by default.	Specify a priority setting for the uplink profile when the **By User-defined** methodology is selected. The priority value can be 1 ~ 16. 1 is the highest priority, and 16 is the lowest priority).
Enable	The box is checked by default.	Click the **Enable** box to activate this profile.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	N/A	When the **Back** button is clicked, the screen will return to the Profile List page.

Instead of manually enter the information for the uplink network, you can also click the **Scan** button to get the available wireless networks around the device, and select one as the uplink network.

When the **Scan** button is applied, **Wireless AP List** will appear after few seconds.



Wireless AP List

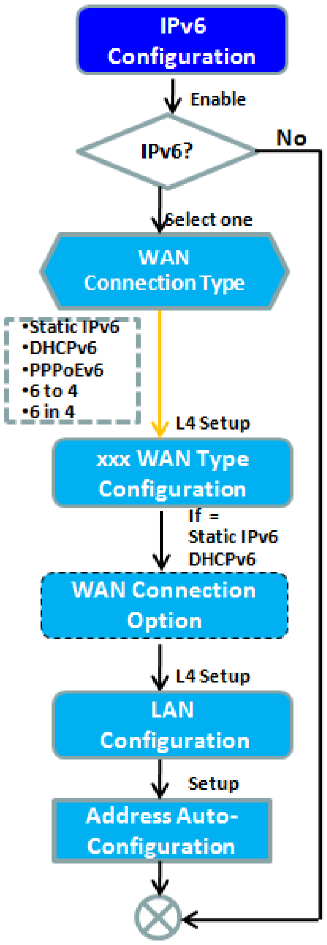
SSID	Channel	Quality	Authentication	Encryption	MAC Address	Select
PDE	1	65%	WPA2-PSK	AES	00:22:88:02:6b:e4	○
skynet	1	0%	WPA2-PSK	AES	ec:24:b8:4b:dc:ab	○
workbench	1	29%	WPA2-PSK	AES	00:22:88:02:0d:c0	○
Ranc_FreeWiFi	1	0%	WPA2-PSK	AES	b0:48:7a:ca:6a:d0	○
Ubytovna 5	2	0%	WPA2-PSK	AES	e4:be:ed:bd:06:67	○
WLAN11_2G	2	0%	WPA2-PSK	AES	1c:49:7b:c6:48:98	○
KALIBR	2	0%	WPA2-PSK	AES	cc:b2:55:94:5a:c6	○
TP_LINK	8	0%	WPA2-PSK	AES	18:a6:f7:7a:f8:fc	○
Internet_AA	12	0%	WPA2-PSK	AES	f8:8e:85:72:d0:ab	○
advantech	13	5%	WPA2-PSK	AES	00:3a:98:22:8d:00	○

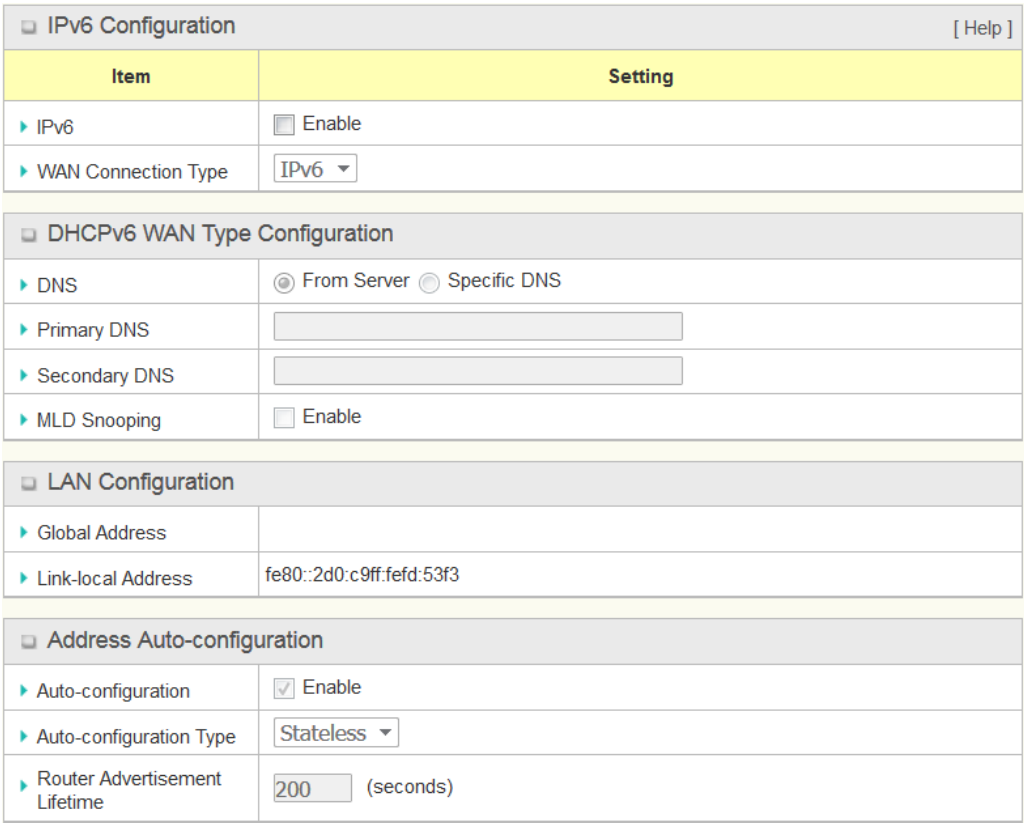
Once you selected an AP from the AP list, the channel, SSID, Authentication, Encryption, and MAC address will be automatically filled into the profile, you just have to enter a key for the uplink connection, if required.

2.4 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.

2.4.1 IPv6 Configuration





IPv6 Configuration [Help]

Item	Setting
IPv6	□ Enable
WAN Connection Type	IPv6 ▾

DHCPv6 WAN Type Configuration

DNS	● From Server ○ Specific DNS
Primary DNS	
Secondary DNS	
MLD Snooping	□ Enable

LAN Configuration

Global Address	
Link-local Address	fe80::2d0:c9ff:fefd:53f3

Address Auto-configuration

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

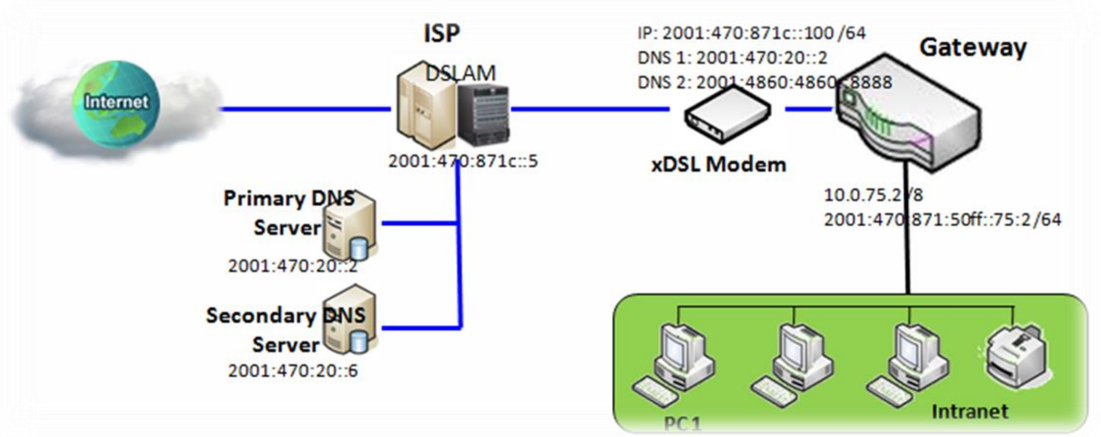
The **IPv6 Configuration** setting allows user to set the IPv6 connection type to access the IPv6 network. This router supports various types of IPv6 connection, including **Static IPv6**, **DHCPv6**, and **PPPoEv6**

Note: For the products just having 3G/4G WAN interface, only **IPv6** is supported. Please contact your ISP for the IPv6 supports before you proceed with IPv6 setup.

IPv6 WAN Connection Type

Static IPv6

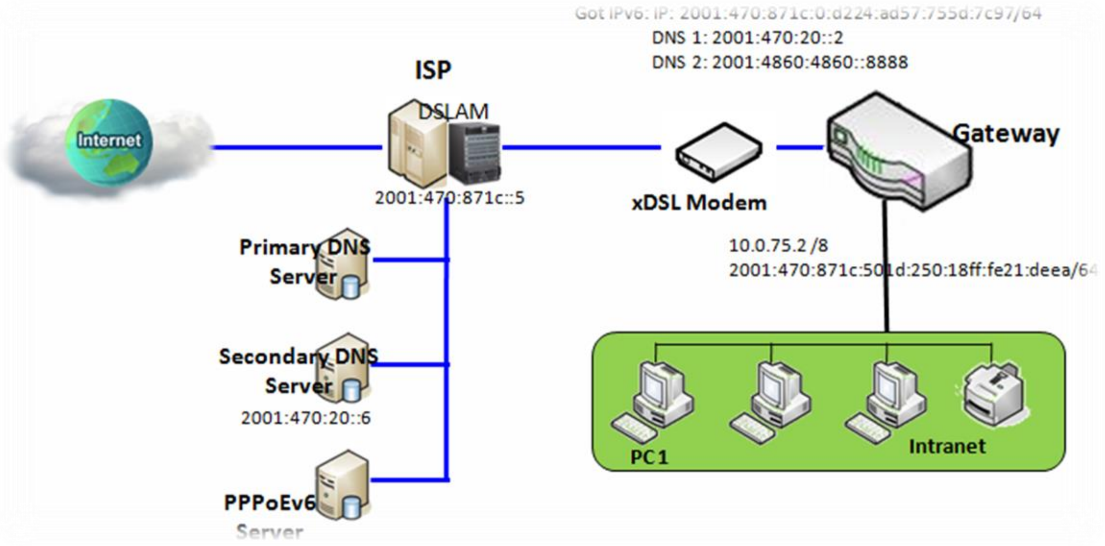
Static IPv6 does the same function as static IPv4. The static IPv6 provides manual setting of IPv6 address, IPv6 default router address, and IPv6 DNS.



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

DHCPv6

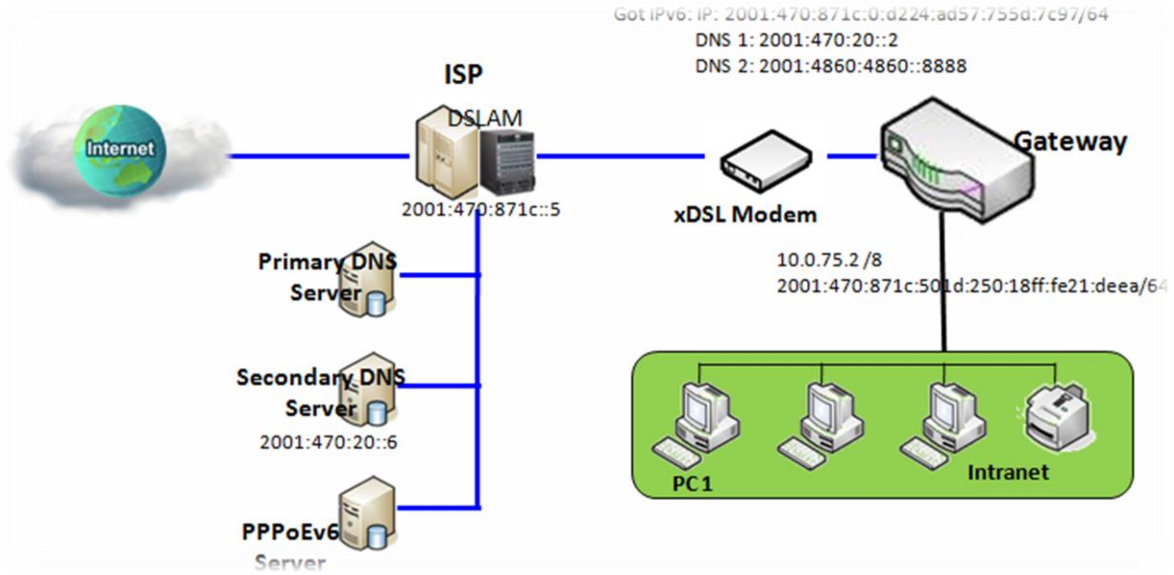
DHCP in IPv6 does the same function as DHCP in IPv4. The DHCP server sends IP address, DNS server addresses and other possible data to the DHCP client to configure automatically. The server also sends a lease time of the address and time to re-contact the server for IPv6 address renewal. The client has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



Above diagram depicts DHCP IPv6 IP addressing, the DHCPv6 server on the ISP side assigns IPv6 address, IPv6 default router 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.

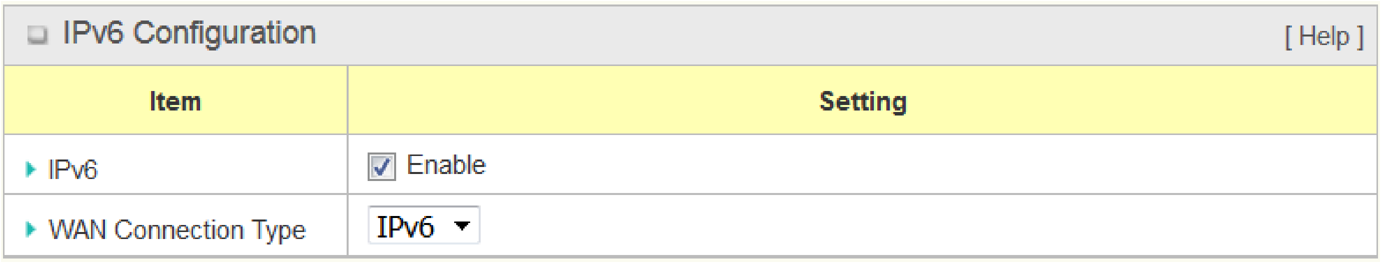


The diagram above depicts the IPv6 addressing through PPPoE, PPPoEv6 server (DSLAM) on the ISP side provides IPv6 configuration upon receiving PPPoEv6 client request. When PPPoEv6 server gets client request and successfully authenticates it, the server sends IP address, DNS server addresses and other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

IPv6 Configuration Setting

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

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

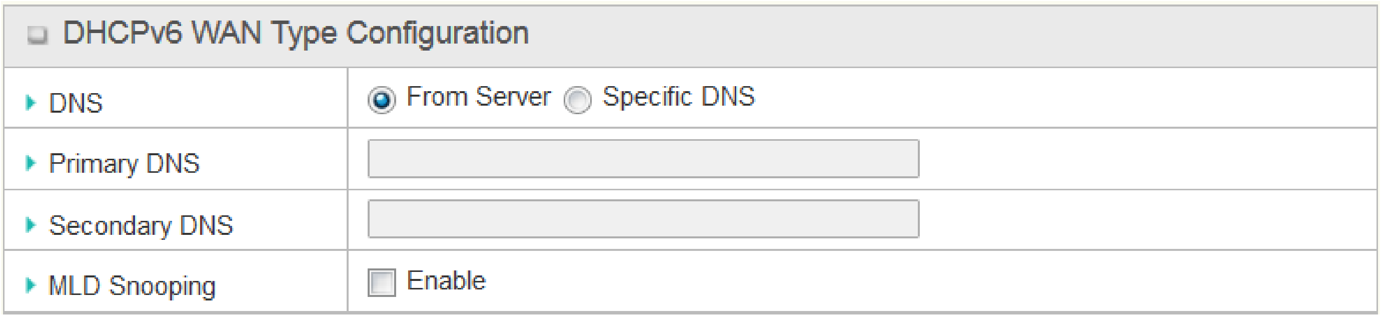


IPv6 Configuration [Help]

Item	Setting
IPv6	☑ Enable
WAN Connection Type	IPv6 ▾

IPv6 Configuration		
Item	**Value setting**	**Description**
IPv6	The box is unchecked by default,	Check the **Enable** box to activate the IPv6 function.
WAN Connection Type	1. Only can be selected when IPv6 Enable 2. A Must filled setting	Define the selected IPv6 WAN Connection Type to establish the IPv6 connectivity. For this product only **IPv6** is supported.

DHCPv6 WAN Type Configuration

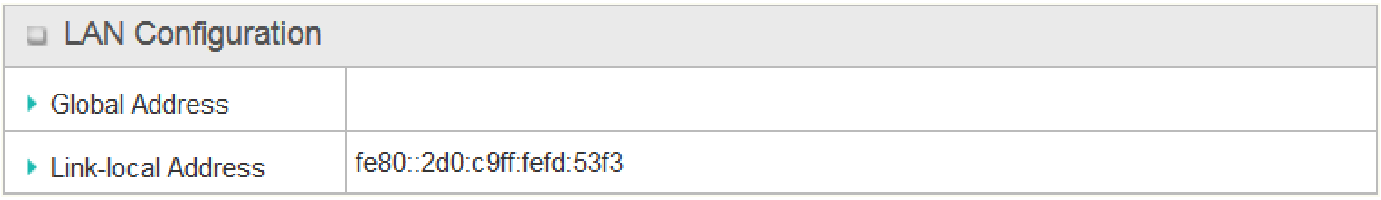


DHCPv6 WAN Type Configuration

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	Cannot modified by default	Enter the WAN **primary DNS Server**.
Secondary DNS	Cannot modified by default	Enter the WAN **secondary DNS Server**.
MLD	The box is unchecked by default	Enable/Disable the MLD Snooping function

LAN Configuration



LAN Configuration

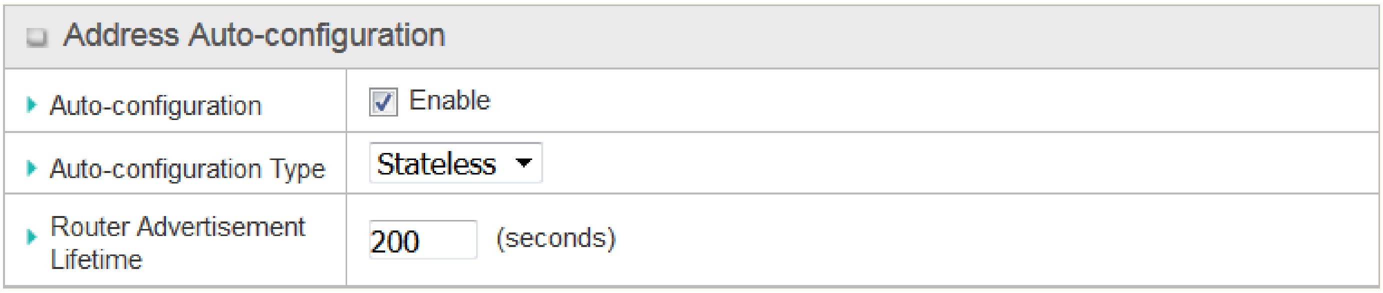
Global Address	
Link-local Address	fe80::2d0:c9ff:fefd:53f3

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

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

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

Address Auto-configuration



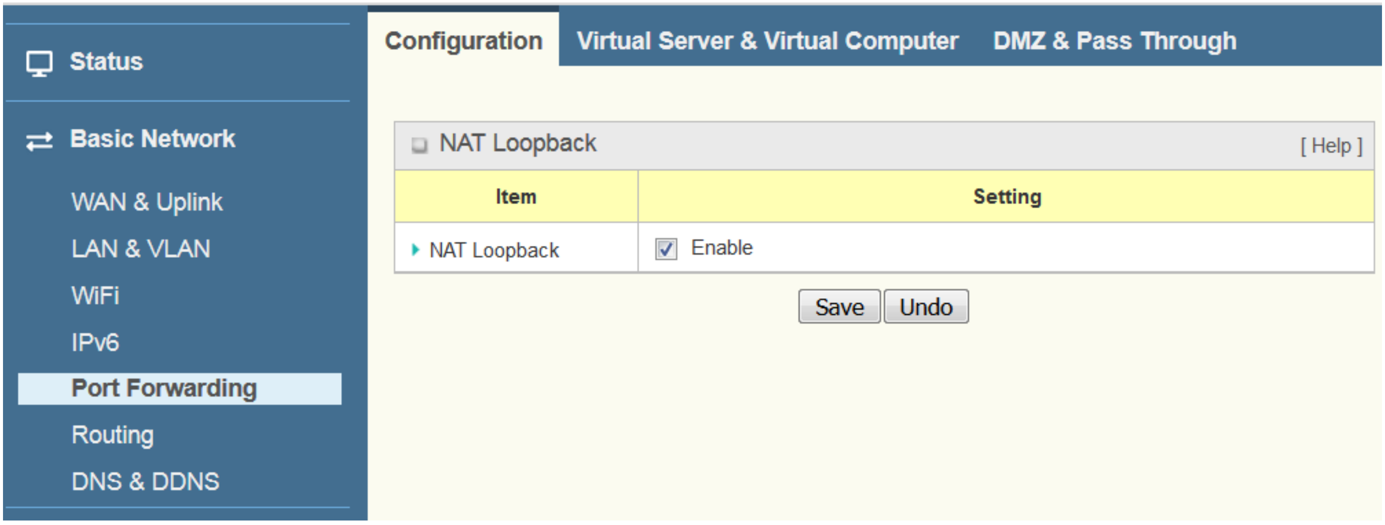
Address Auto-configuration

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

Address Auto-configuration		
Item	**Value setting**	**Description**
Auto-configuration	The box is unchecked by default	Check to enable the Auto configuration feature.
Auto-configuration Type	1. Only can be selected when **Auto-configuration** enabled 2. Stateless is selected by default	Define the selected IPv6 WAN Connection Type to establish the IPv6 connectivity. Select **Stateless** to manage the Local Area Network to be SLAAC + RDNSS **Router Advertisement Lifetime** (A Must filled setting): Enter the Router Advertisement Lifetime (in seconds). 200 is set by default. *Value Range*: 0 ~ 65535.

2.5 Port Forwarding

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



NAT Loopback

Item	Setting
NAT Loopback	☑ Enable

Usually all local hosts or servers behind corporate router are protected by NAT firewall. NAT firewall will filter out unrecognized packets to protect your Intranet. So, all local hosts are invisible to the outside world. Port forwarding or port mapping is function that redirects a communication request from one address and port number combination to assigned one. This technique is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the router (external network), by remapping the destination IP address and port number

There are several optional Port Forwarding related functions in this router. They are Virtual Server, Virtual Computer, IP Translation, Special AP & ALG, DMZ and Pass Through, etc. The available functions might be different for the purchased model.

2.5.1 Configuration

NAT Loopback

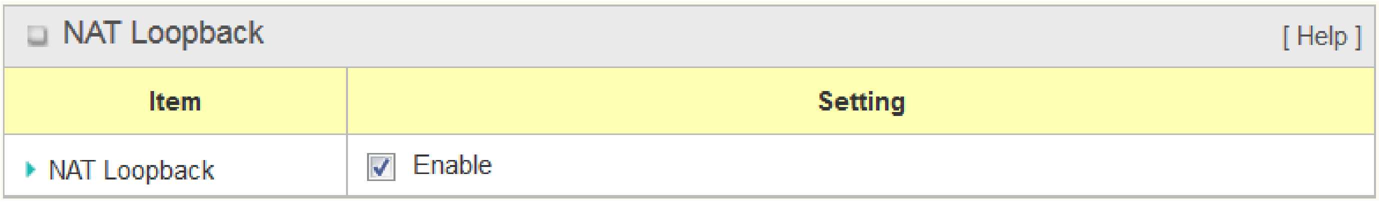
This feature allows you to access the WAN global IP address from your inside NAT local network. It is useful when you run a server inside your network. For example, if you set a mail server at LAN side, your local devices can access this mail server through router's global IP address when enable NAT 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.

Configuration Setting

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

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

Enable NAT Loopback

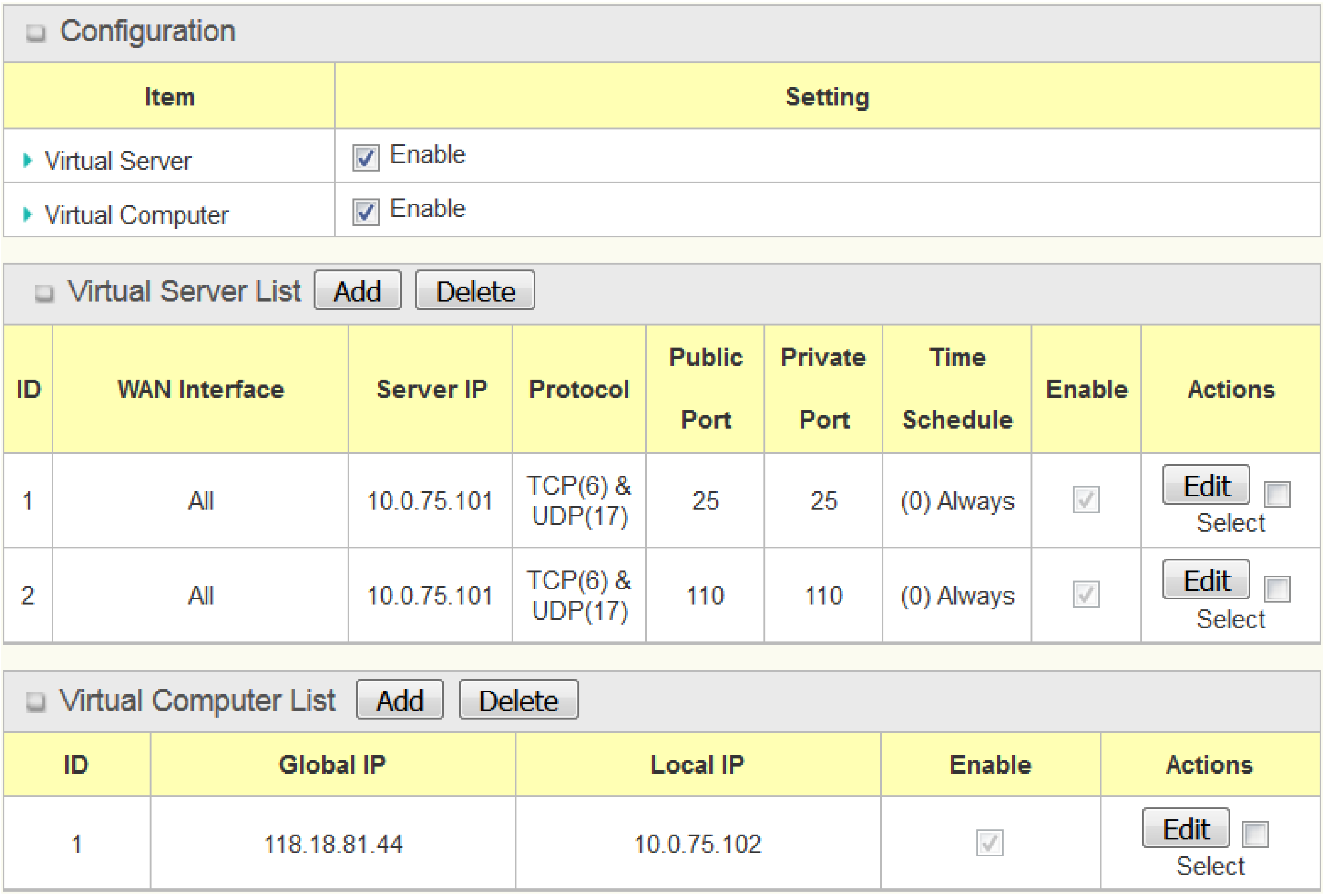


NAT Loopback [Help]

Item	Setting
NAT Loopback	☑ Enable

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

2.5.2 Virtual Server & Virtual Computer



Configuration

Item	Setting
Virtual Server	☑ Enable
Virtual Computer	☑ Enable

Virtual Server List

ID	WAN Interface	Server IP	Protocol	Public Port	Private Port	Time Schedule	Enable	Actions
1	All	10.0.75.101	TCP(6) & UDP(17)	25	25	(0) Always	☑	Edit □ Select
2	All	10.0.75.101	TCP(6) & UDP(17)	110	110	(0) Always	☑	Edit □ Select

Virtual Computer List

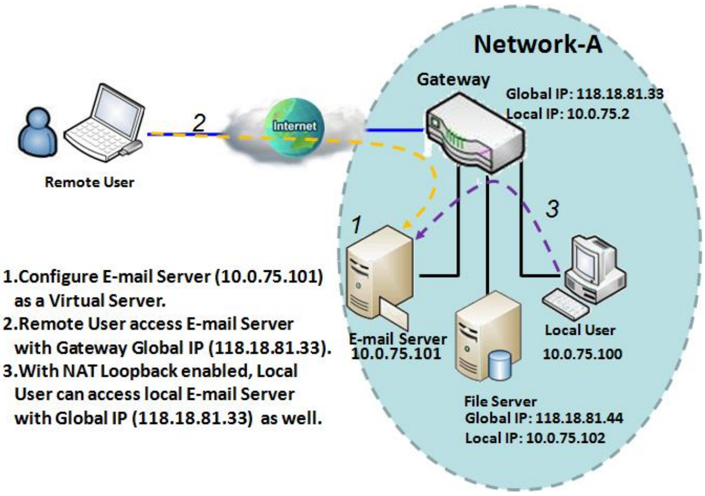
ID	Global IP	Local IP	Enable	Actions
1	118.18.81.44	10.0.75.102	☑	Edit □ Select

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

It is necessary for cooperate staffs who travel outside and want to access various servers behind office router. You can set up those servers by using "Virtual Server" feature. After trip, if want to access those servers from LAN side by global IP, without change original setting, NAT Loopback can achieve it.

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

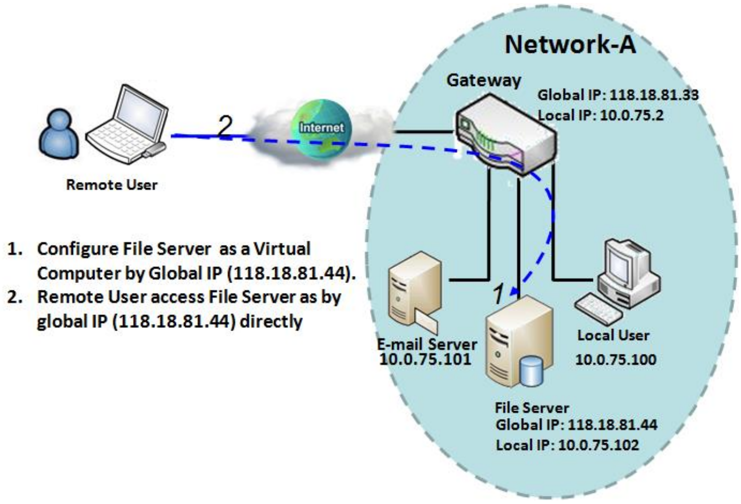
Virtual Server & NAT Loopback


Network-A
Gateway
Global IP: 118.18.81.33
Local IP: 10.0.75.2
2
Internet
Remote User
1
3
1.Configure E-mail Server (10.0.75.101) as a Virtual Server.
2.Remote User access E-mail Server with Gateway Global IP (118.18.81.33).
3.With NAT Loopback enabled, Local User can access local E-mail Server with Global IP (118.18.81.33) as well.
E-mail Server
10.0.75.101
Local User
10.0.75.100
File Server
Global IP: 118.18.81.44
Local IP: 10.0.75.102

"Virtual Server" allows you to access 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. As shown in example, an E-mail virtual server is defined 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 with the gateway's global IP 118.18.81.33 from its WAN side. But the real E-mail server is located at LAN side and the gateway is the port forwarder for E-mail service.

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

Virtual Computer

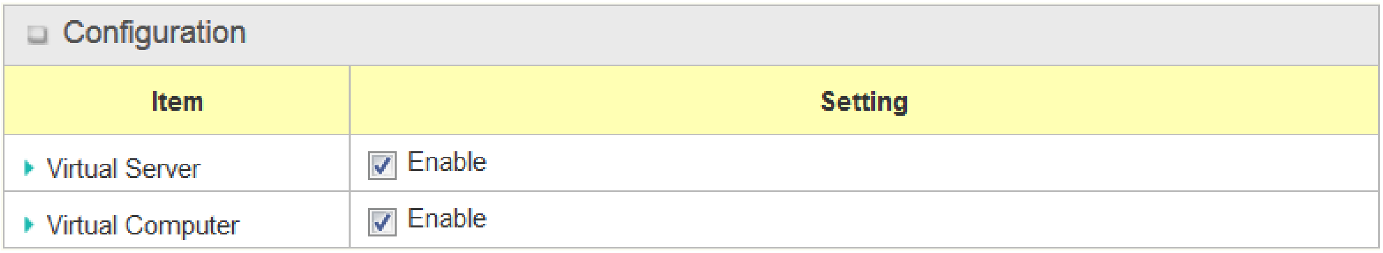


"Virtual Computer" allows you to assign LAN hosts to global IP addresses, so that they can be visible to outside world. While so, they are also protected by the gateway firewall as being client hosts in the Intranet. For example, if you set a FTP file server at LAN side with local IP address 10.0.75.102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

Virtual Server & Virtual Computer Setting

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

Enable Virtual Server and Virtual Computer



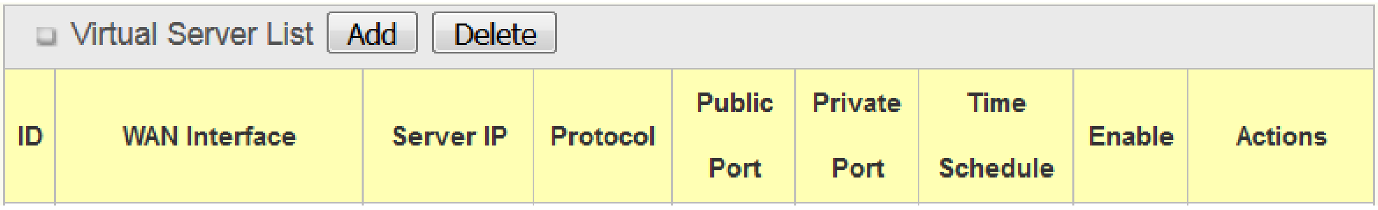
Configuration

Item	Setting
Virtual Server	☑ Enable
Virtual Computer	☑ Enable

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

Create / Edit Virtual Server

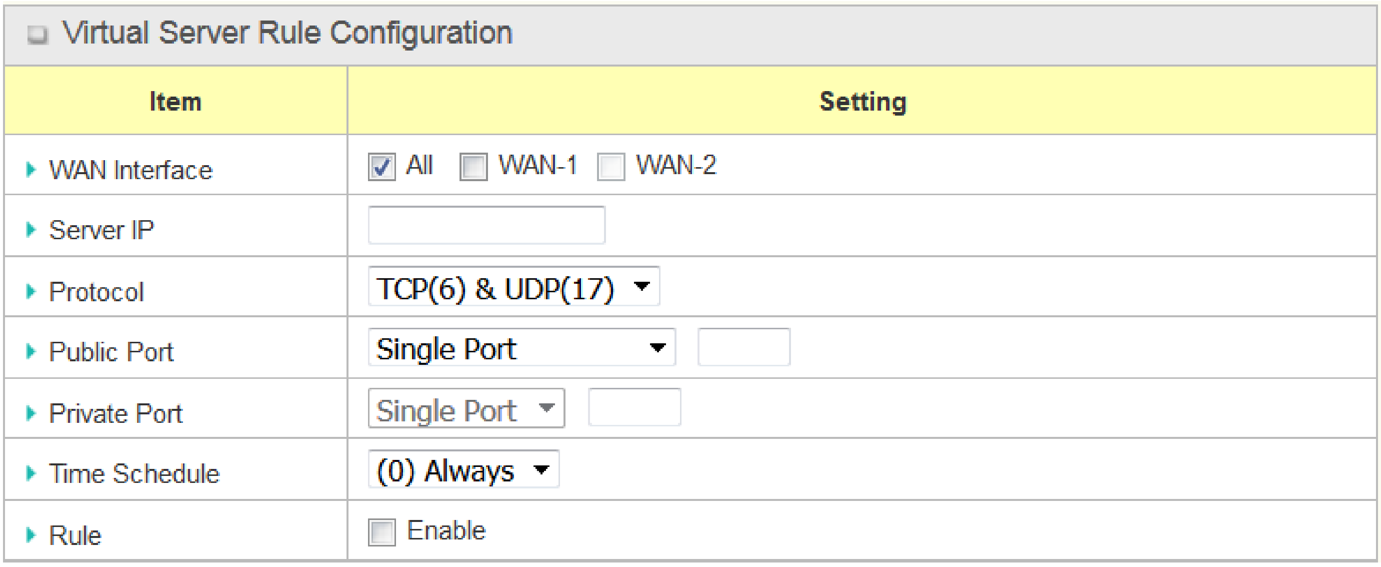
The router allows you to custom your Virtual Server rules. It supports up to a maximum of 20 rule-based Virtual Server sets.



Virtual Server List Add Delete

ID	WAN Interface	Server IP	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

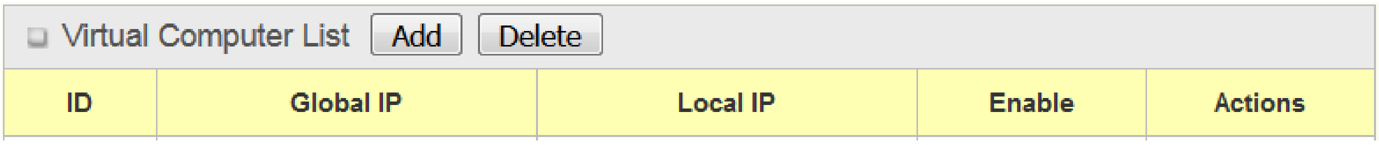
Item	Setting
WAN Interface	☑ All ☐ WAN-1 ☐ WAN-2
Server IP	
Protocol	TCP(6) & UDP(17)
Public Port	Single Port
Private Port	Single Port
Time Schedule	(0) Always
Rule	☐ Enable

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 interface. It can be selected **WAN-x** box when **WAN-x** enabled. **Note**: The available check boxes (**WAN-1** ~ **WAN-4**) depend on the number of WAN interfaces for the product.
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 **Public Port** **Private Port**	A Must filled setting	When **"ICMPv4"** is selected It means the option "Protocol" of packet filter rule is ICMPv4. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **Object Definition)** Then check **Enable** box to enable this rule.
		When **"TCP"** is selected It means the option "Protocol" of packet filter rule is TCP. **Public Port** selected a predefined port from **Well-known Service**, and **Private Port** is the same with **Public Port** number. **Public Port** is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number. **Public Port** is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**. *Value Range*: 1 ~ 65535 for Public Port, Private Port.

		When **"UDP"** is selected It means the option "Protocol" of packet filter rule is UDP. **Public Port** selected a predefined port from **Well-known Service**, and **Private Port** is the same with **Public Port** number. **Public Port** is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number. **Public Port** is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**. *Value Range*: 1 ~ 65535 for Public Port, Private Port.
		When **"TCP & UDP"** is selected It means the option "Protocol" of packet filter rule is TCP and UDP. **Public Port** selected a predefined port from **Well-known Service**, and **Private Port** is the same with **Public Port** number. **Public Port** is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number. **Public Port** is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**. *Value Range*: 1 ~ 65535 for Public Port, Private Port.
		When **"GRE"** is selected It means the option "Protocol" of packet filter rule is GRE.
		When **"ESP"** is selected It means the option "Protocol" of packet filter rule is ESP.
		When **"SCTP"** is selected It means the option "Protocol" of packet filter rule is SCTP.
		When **"User-defined"** is selected It means the option "Protocol" of packet filter rule is User-defined. For **Protocol Number**, enter a port number.
Time Schedule	1. An optional filled setting 2. **(0)Always** Is selected by default.	Apply Time Schedule to this rule; otherwise leave it as (0)Always. (refer to Scheduling setting under Object Definition)
Rule	1. An optional filled setting 2. The box is unchecked by default.	Check the Enable box to activate the rule.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the settings.
Back	N/A	When the **Back** button is clicked the screen will return to previous page.

Create / Edit Virtual Computer

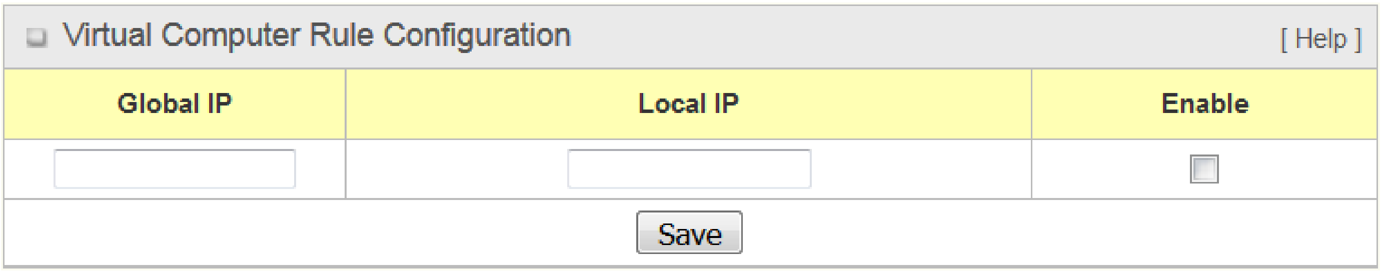
The router allows you to custom your Virtual Computer rules. It supports up to a maximum of 20 rule-based Virtual Computer sets.



Virtual Computer List

ID	Global IP	Local IP	Enable	Actions

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



Virtual Computer Rule Configuration

Global IP	Local IP	Enable
		□

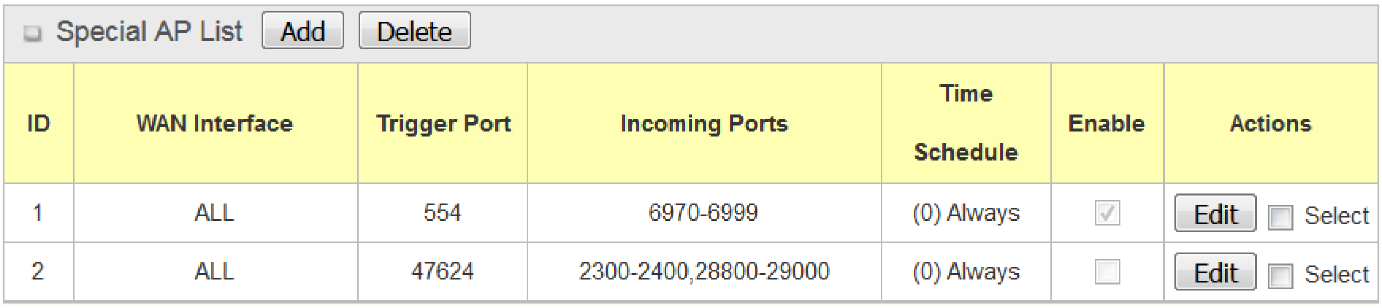
Virtual Computer Rule Configuration		
Item	**Value setting**	**Description**
Global IP	A Must filled setting	This field is to specify the IP address of the WAN IP.
Local IP	A Must filled setting	This field is to specify the IP address of the LAN IP.
Enable	N/A	Then check **Enable** box to enable this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

2.5.3 Special AP & ALG

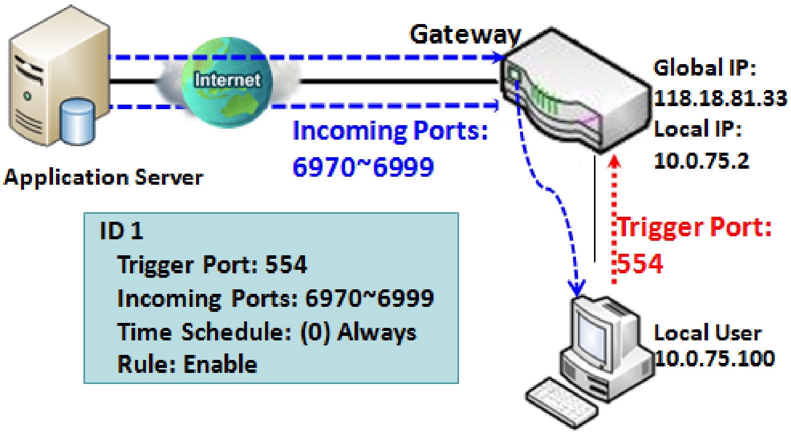
As a NAT gateway, it doesn't allow an active connection request from outside world. All this kind of requests will be ignored by the NAT gateway. But at the client hosts in the Intranet, users may use applications that need more service ports to be allowed for passing through the NAT gateway. The "Special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

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.

Special AP



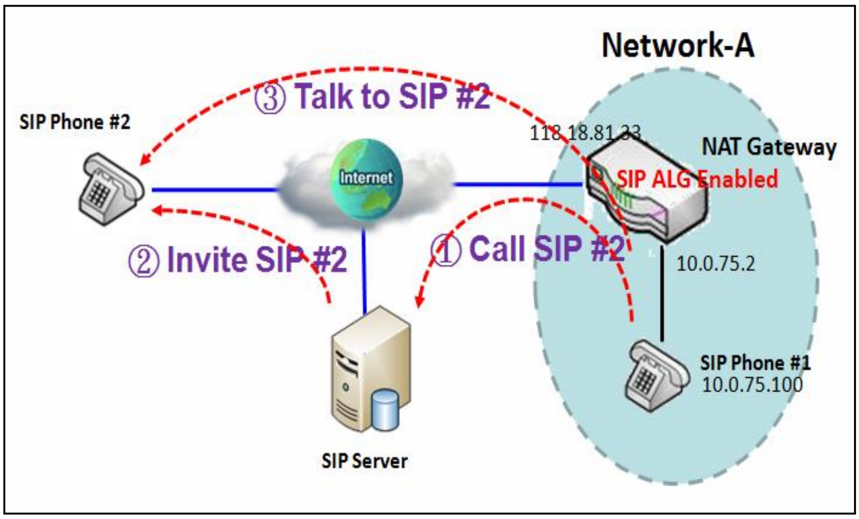
ID	WAN Interface	Trigger Port	Incoming Ports	Time Schedule	Enable	Actions
1	ALL	554	6970-6999	(0) Always	☑	Edit □ Select
2	ALL	47624	2300-2400,28800-29000	(0) Always	□	Edit □ Select



The Special AP feature allows you to request the gateway open a pre-defined service ports for incoming packets to pass through once the trigger port is activated by local hosts. As shown in the diagram, special AP rule define port **554** as trigger port and **6970~6999** as incoming ports. With such setting, local user at host 10.0.75.100 can enjoy the music by using Quick Time application, whose media server is located in the Internet. When you open application, it will activate Trigger Port and then incoming data packet from remote application server will pass through incoming port 6970~6999.

SIP ALG

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.



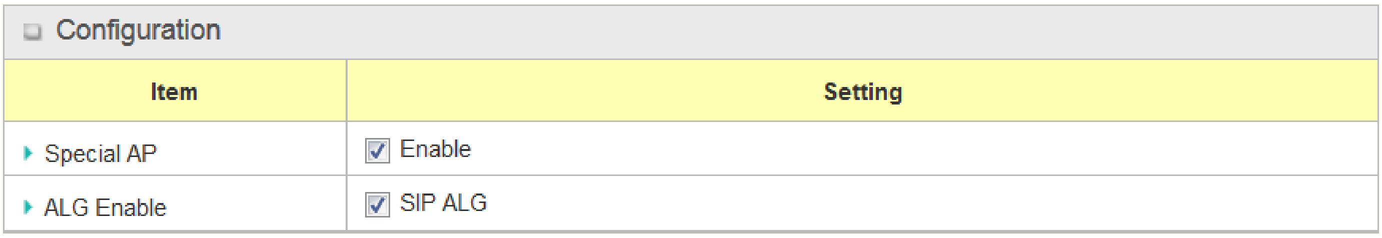
As shown in the diagram, the calling starts from the SIP Phone #1 to the SIP server via the NAT gateway. Then the SIP server invites the SIP Phone #2 and finally, the SIP Phone #1 talks to the SIP Phone #2. But for the NAT gateway, SIP Phone #2 is an unknown host, so the active access from the Phone #2 will be treated as unexpected traffic and will be blocked out. With the SIP ALG function enabled, the NAT gateway will monitor the control traffic for the SIP calls, and recognized the traffic from SIP Phone #2 is part of the connection sessions with SIP Phone #1.

Special AP & ALG Setting

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

The Special AP setting allows some applications require multiple connections. The ALG setting allows user to Support some SIP ALG, like STUN.

Enable Special AP & ALG



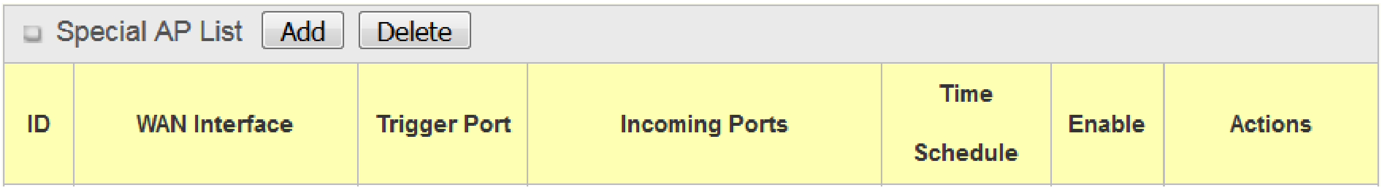
Configuration

Item	Setting
Special AP	☑ Enable
ALG Enable	☑ SIP ALG

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

Create / Edit Special AP Rule

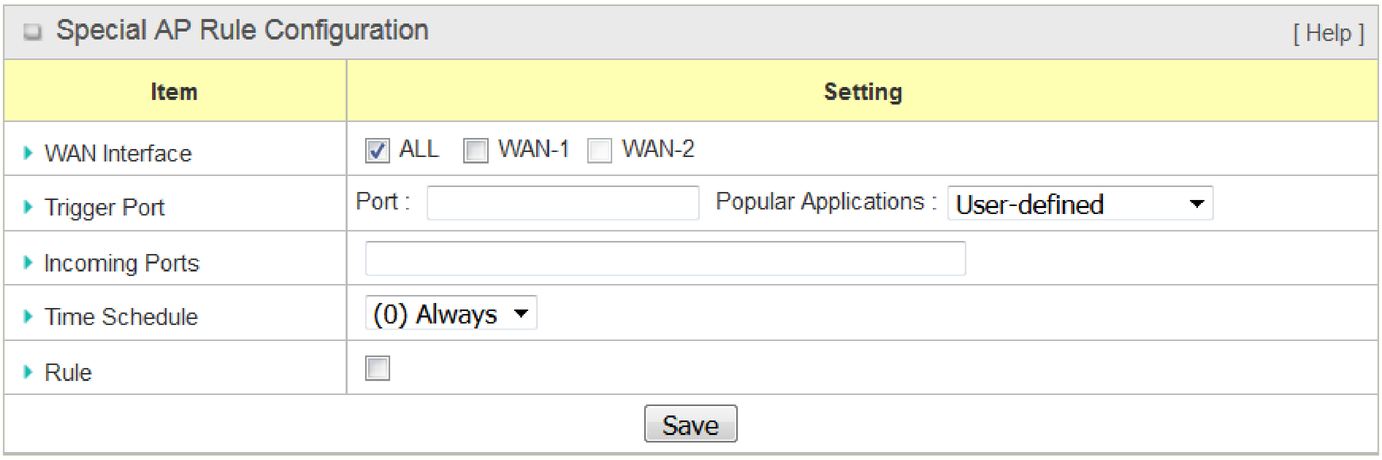
The gateway allows you to custom your Special AP rules. It supports up to a maximum of 8 rule-based Special AP sets.



Special AP List [Add] [Delete]

ID	WAN Interface	Trigger Port	Incoming Ports	Time Schedule	Enable	Actions

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



Special AP Rule Configuration [Help]

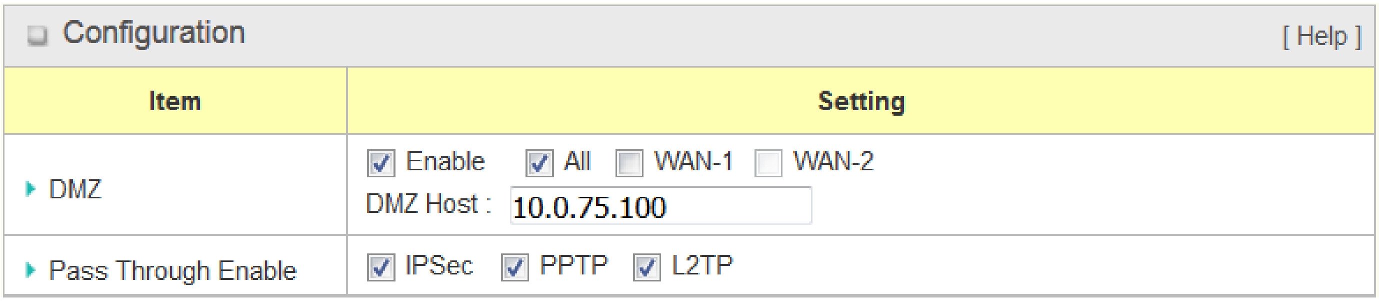
Item	Setting
WAN Interface	☑ ALL ☐ WAN-1 ☐ WAN-2
Trigger Port	Port : ____ Popular Applications : User-defined
Incoming Ports	____
Time Schedule	(0) Always
Rule	☐

[Save]

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

2.5.4 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 router 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.

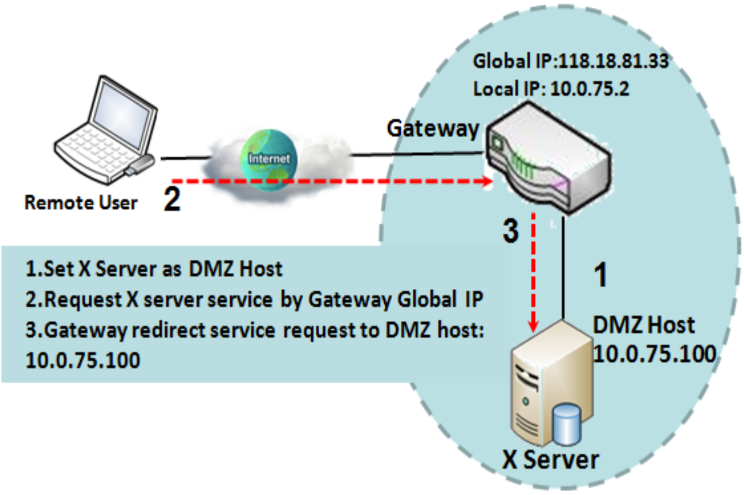


Configuration [Help]

Item	Setting
DMZ	☑ Enable ☑ All □ WAN-1 □ WAN-2 DMZ Host : 10.0.75.100
Pass Through Enable	☑ IPSec ☑ PPTP ☑ L2TP

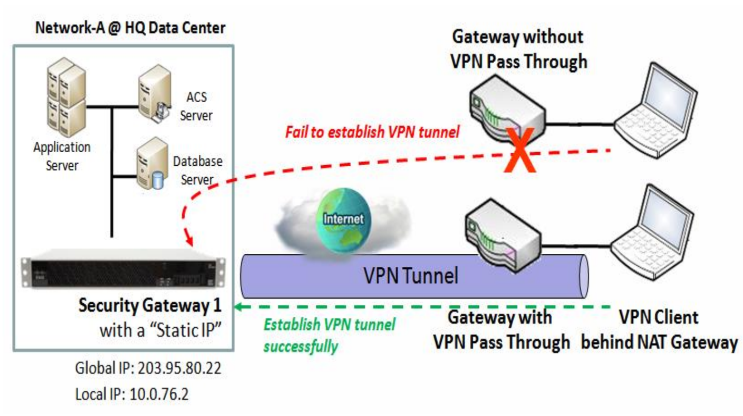
The DMZ function allows you to ask the router pass through all normal packets to the DMZ host behind the NAT router only when these packets are not expected to receive by applications in the router or by other client hosts in the Intranet. Certainly, the DMZ host is also protected by the router firewall.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

DMZ Scenario


Global IP:118.18.81.33
Local IP: 10.0.75.2
Gateway
Internet
Remote User
2
3
1
DMZ Host
10.0.75.100
X Server
1.Set X Server as DMZ Host
2.Request X server service by Gateway Global IP
3.Gateway redirect service request to DMZ host: 10.0.75.100

When the network administrator wants to set up some service daemons in a host behind NAT gateway to allow remote users request for services from server actively, you just have to configure this host as DMZ Host. As shown in the diagram, there is an X server installed as DMZ host, whose IP address is 10.0.75.100. Then, remote user can request services from X server just as it is provided by the gateway whose global IP address is 118.18.81.33. The gateway will forward those packets, not belonging to any configured virtual server or applications, directly to the DMZ host.

VPN Pass through Scenario



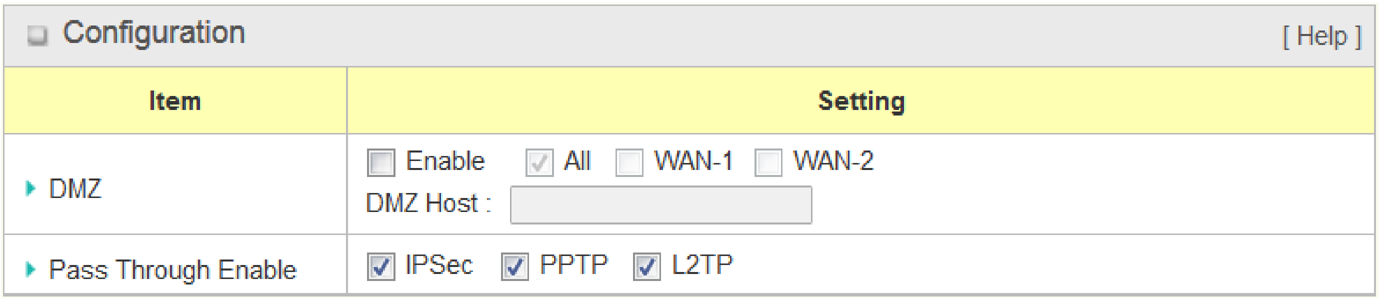
Since VPN traffic is different from that of TCP or UDP connection, it will be blocked by NAT gateway. To support the pass through function for the VPN connections initiating from VPN clients behind NAT gateway, the gateway must implement some kind of VPN pass through function for such application. The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

DMZ & Pass Through Setting

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

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

Enable DMZ and Pass Through



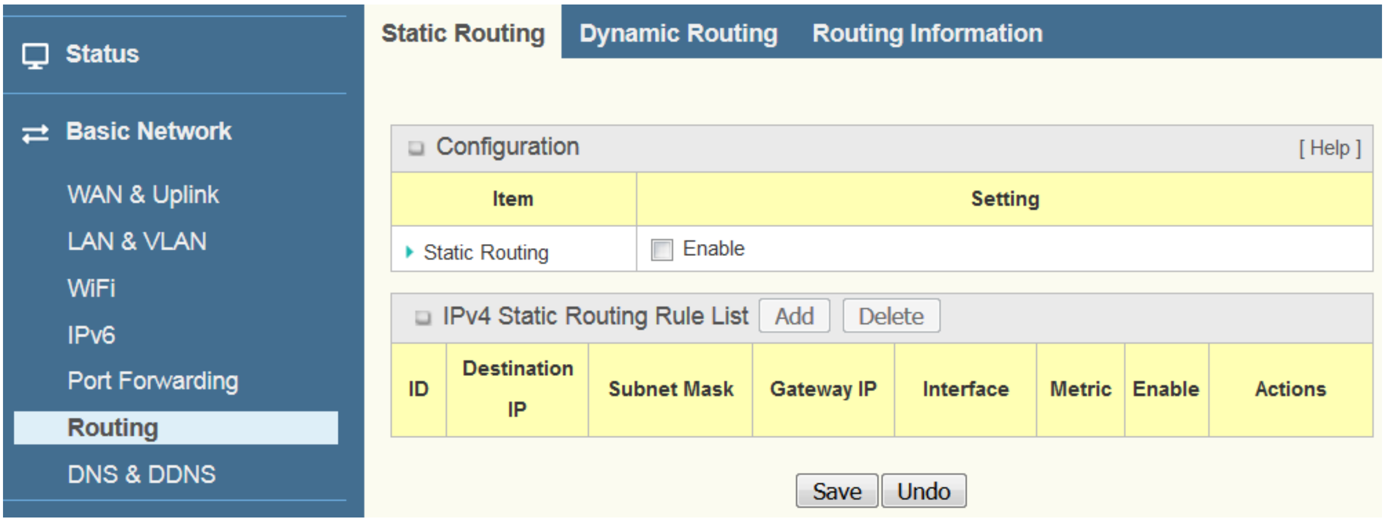
Configuration [Help]

Item	Setting
DMZ	□ Enable ☑ All □ WAN-1 □ WAN-2 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 the DMZ function Define the selected interface to be the packet-entering interface of the router, and fill in the IP address of Host LAN IP in **DMZ Host** field. 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. **Note**: The available check boxes (**WAN-1** ~ **WAN-4**) depend on the number of WAN interfaces for the product.

Pass Through Enable	The boxes are checked by default	Check the box to enable the pass through function for the **IPSec**, **PPTP**, and **L2TP**. With the pass through function enabled, the VPN hosts behind the router still can connect to remote VPN servers.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click the **Undo** button to cancel the settings

2.6 Routing



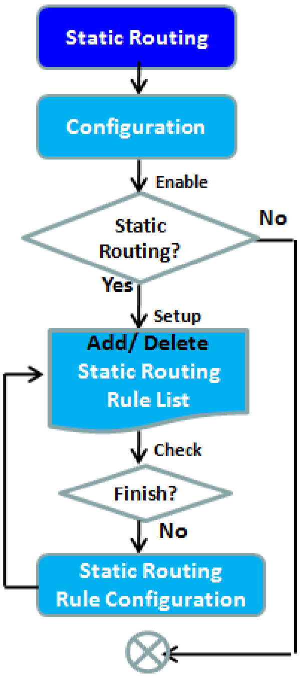
Item	Setting
Static Routing	□ Enable

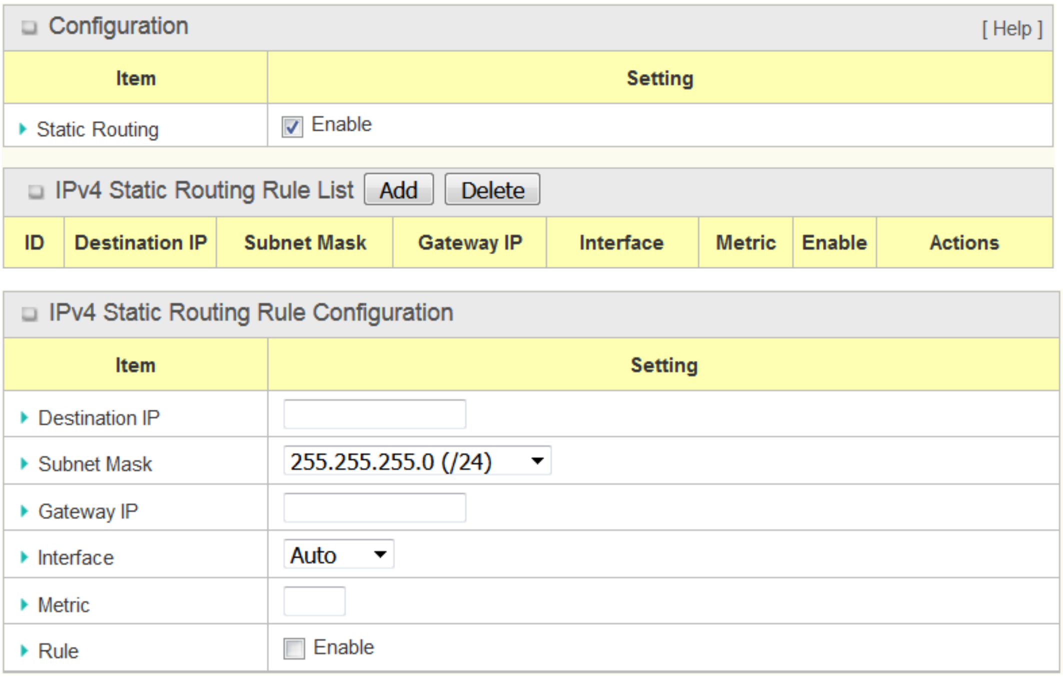
ID	Destination IP	Subnet Mask	Gateway IP	Interface	Metric	Enable	Actions

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. In addition, the router also built in one advanced configurable routing software Quagga for more complex routing applications, you can configure it if required via Telnet CLI.

2.6.1 Static Routing





Configuration [Help]

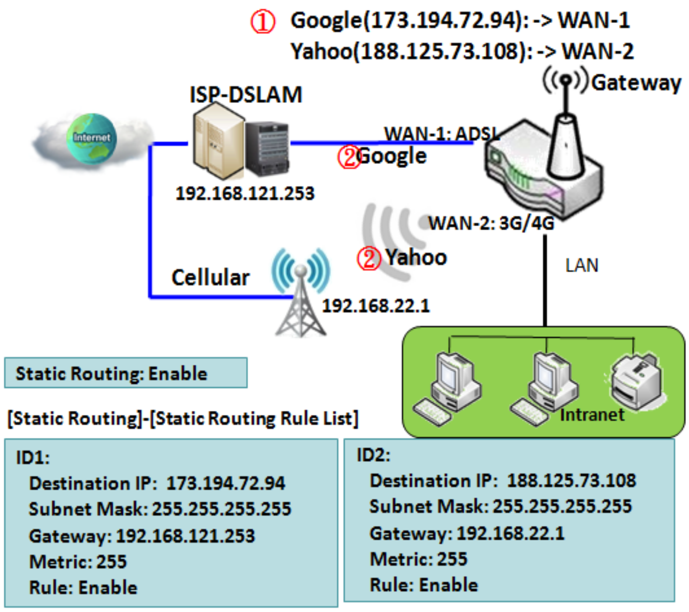
Item	Setting
Static Routing	☑ Enable

IPv4 Static Routing Rule List [Add] [Delete]

ID	Destination IP	Subnet Mask	Gateway IP	Interface	Metric	Enable	Actions

IPv4 Static Routing Rule Configuration

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



Static Routing: Enable

[Static Routing]-[Static Routing Rule List]

ID1:
Destination IP: 173.194.72.94
Subnet Mask: 255.255.255.255
Gateway: 192.168.121.253
Metric: 255
Rule: Enable

ID2:
Destination IP: 188.125.73.108
Subnet Mask: 255.255.255.255
Gateway: 192.168.22.1
Metric: 255
Rule: Enable

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

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

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

Static Routing Setting

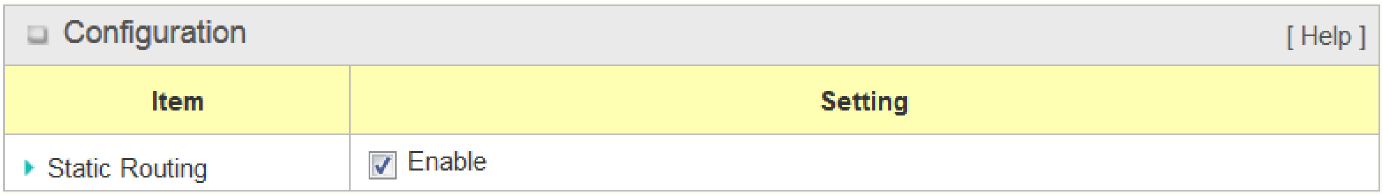
Go to **Basic Network** > **Routing** > **Static Routing** Tab.

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

Enable Static Routing

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



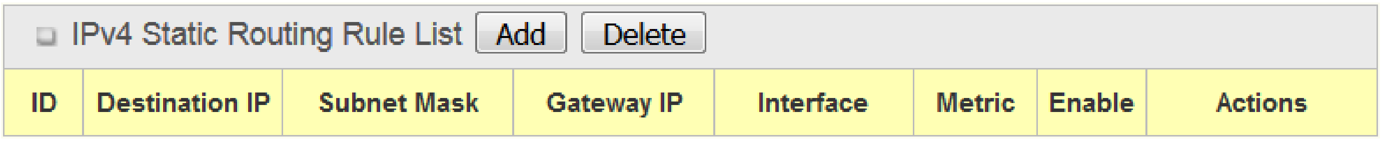
Configuration [Help]

Item	Setting
Static Routing	☑ Enable

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

Create / Edit Static Routing Rules

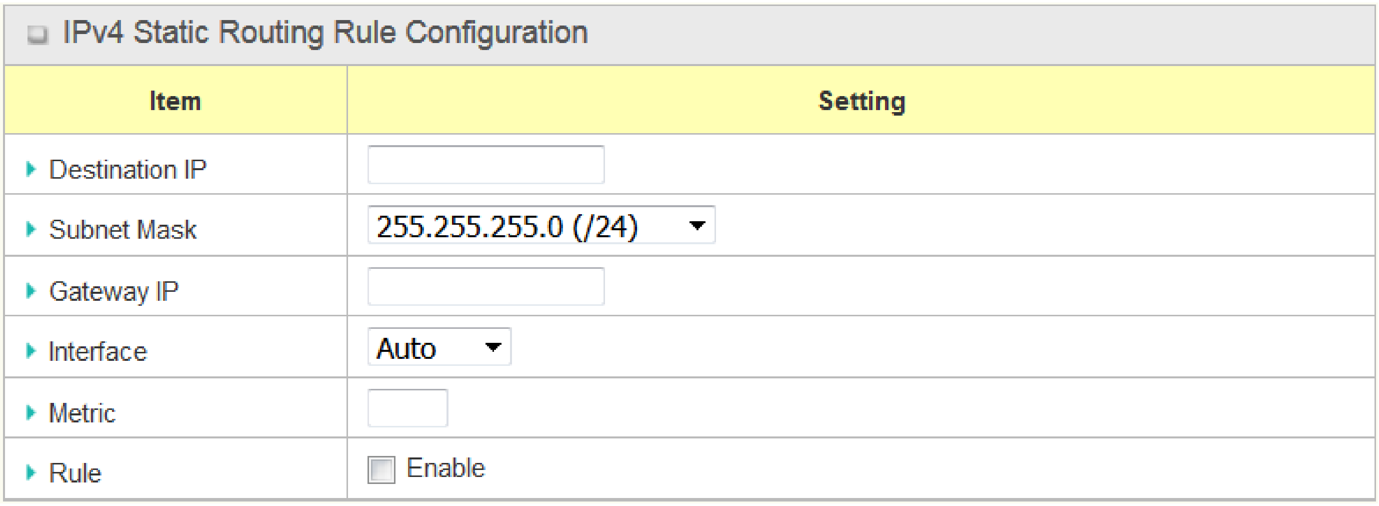
The Static Routing Rule List shows the setup parameters of all static routing rule entries. To configure a static routing rule, you must specify related parameters including the destination IP address and subnet mask of dedicated host/server or subnet, the IP address of peer gateway, the metric and the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



IPv4 Static Routing Rule List

ID	Destination IP	Subnet Mask	Gateway IP	Interface	Metric	Enable	Actions

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

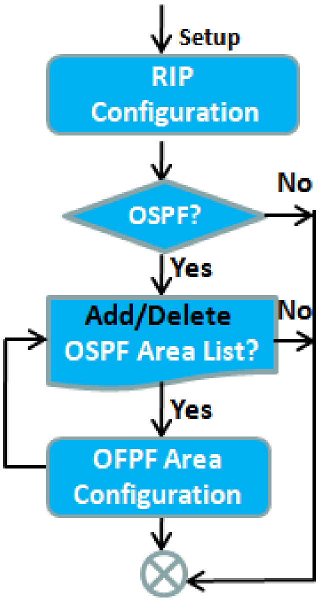


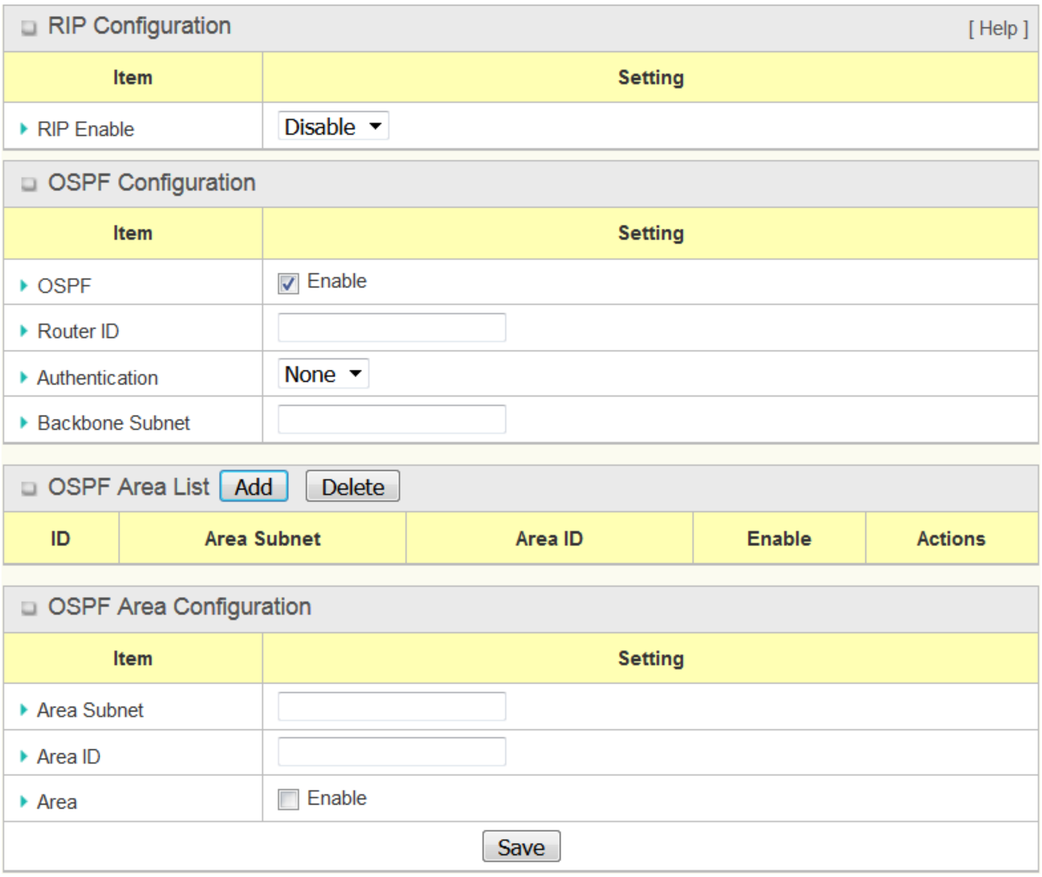
IPv4 Static Routing Rule Configuration

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

IPv4 Static Routing		
Item	**Value setting**	**Description**
Destination IP	1. IPv4 Format 2. A Must filled setting	Specify the Destination IP of this static routing rule.
Subnet Mask	255.255.255.0 (/24) is set by default	Specify the Subnet Mask of this static routing rule.
Gateway IP	1. IPv4 Format 2. A Must filled setting	Specify the Gateway IP of this static routing rule.
Interface	Auto is set by default	Select the Interface of this static routing rule. It can be **Auto**, or the available WAN / LAN interfaces.
Metric	1. Numeric String Format 2. A Must filled setting	The Metric of this static routing rule. *Value Range*: 0 ~ 255.
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.
Back	NA	When the **Back** button is clicked the screen will return to the Static Routing Configuration page.

2.6.2 Dynamic Routing




RIP Configuration [Help]

Item	Setting
RIP Enable	Disable ▾

OSPF Configuration

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

OSPF Area List

ID	Area Subnet	Area ID	Enable	Actions

OSPF Area Configuration

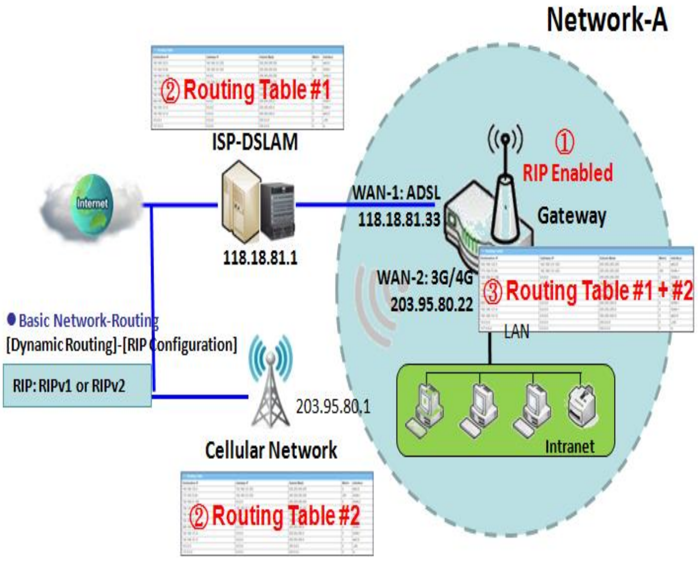
Item	Setting
Area Subnet	
Area ID	
Area	□ Enable

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

This router supports dynamic routing protocols, including RIPv1/RIPv2 (Routing Information Protocol), and OSPF (Open Shortest Path First), 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.

The supported dynamic routing protocols are described as follows:

RIP Scenario

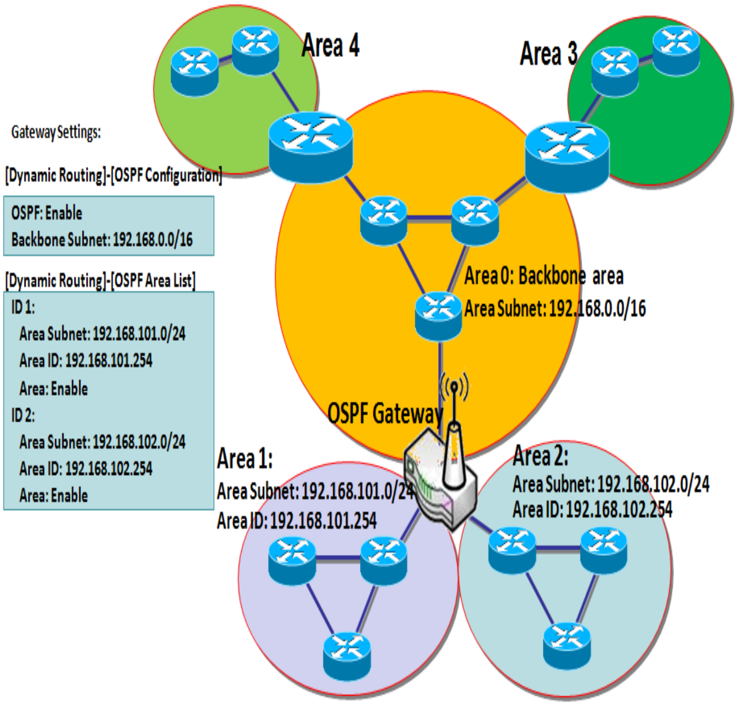


● Basic Network-Routing
[Dynamic Routing]-[RIP Configuration]

RIP: RIPv1 or RIPv2

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

OSPF Scenario



Gateway Settings:

[Dynamic Routing]-[OSPF Configuration]

OSPF: Enable
Backbone Subnet: 192.168.0.0/16

[Dynamic Routing]-[OSPF Area List]

ID 1:
Area Subnet: 192.168.101.0/24
Area ID: 192.168.101.254
Area: Enable
ID 2:
Area Subnet: 192.168.102.0/24
Area ID: 192.168.102.254
Area: Enable

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

Network administrator can deploy OSPF gateway in large enterprise network to get its routing table from the enterprise backbone, and forward routing information to other routers, which are no linked to the enterprise backbone. Usually, an OSPF network is subdivided into routing areas to simplify administration and optimize traffic and resource utilization.

As shown in the diagram, OSPF gateway gathers routing information from the backbone gateways in area 0, and will forward its routing information to the routers in area 1 and area 2 which are not in the backbone.

Dynamic Routing Setting

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

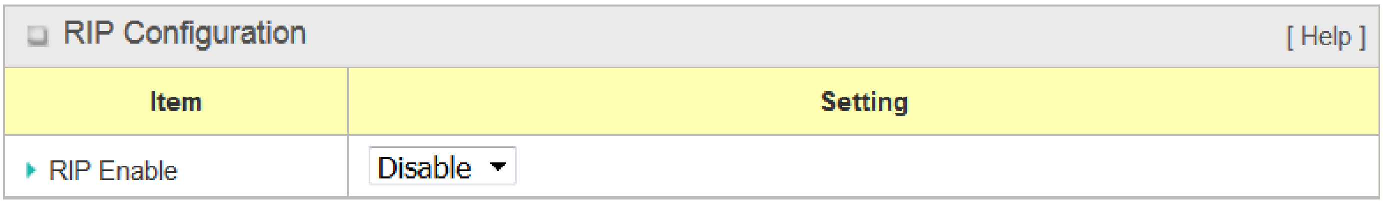
The dynamic routing setting allows user to customize RIP, and OSPF protocols through the router based on their office setting.

In the "Dynamic Routing" page, there are several configuration windows for dynamic routing feature. They are the "RIP Configuration" window, "OSPF Configuration" window, "OSPF Area List", and "OSPF Area Configuration" window. RIP, and OSPF 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.

RIP Configuration

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



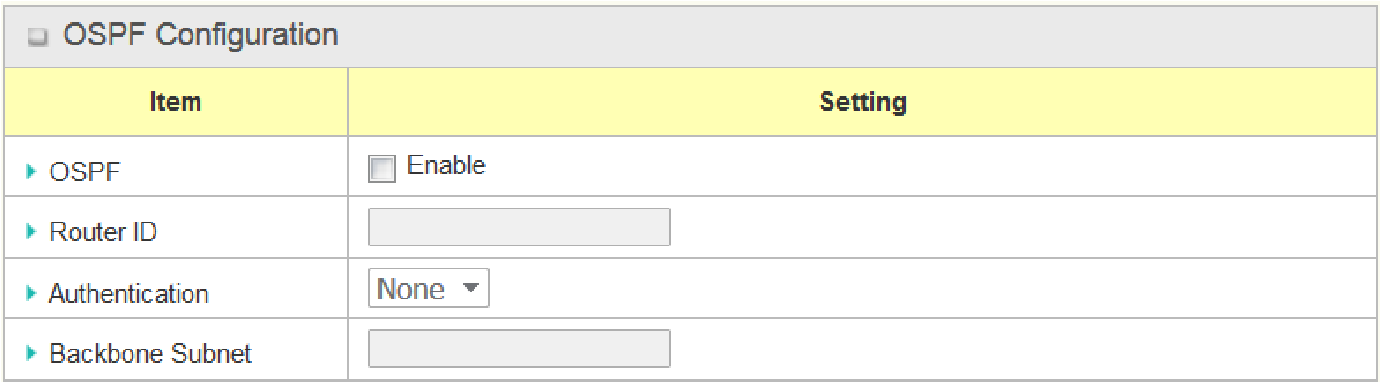
RIP Configuration [Help]

Item	Setting
RIP Enable	Disable

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

OSPF Configuration

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



OSPF Configuration

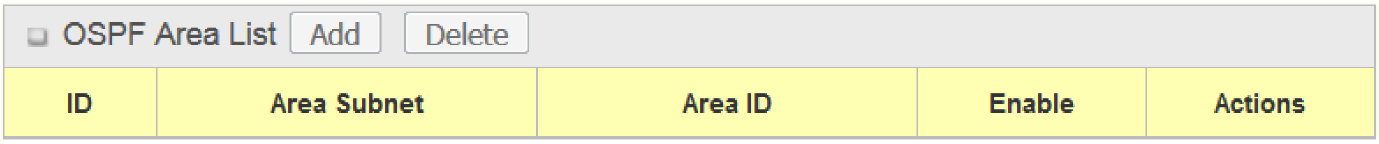
Item	Setting
OSPF	□ Enable
Router ID	
Authentication	None
Backbone Subnet	

OSPF Configuration

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

Create / Edit OSPF Area Rules

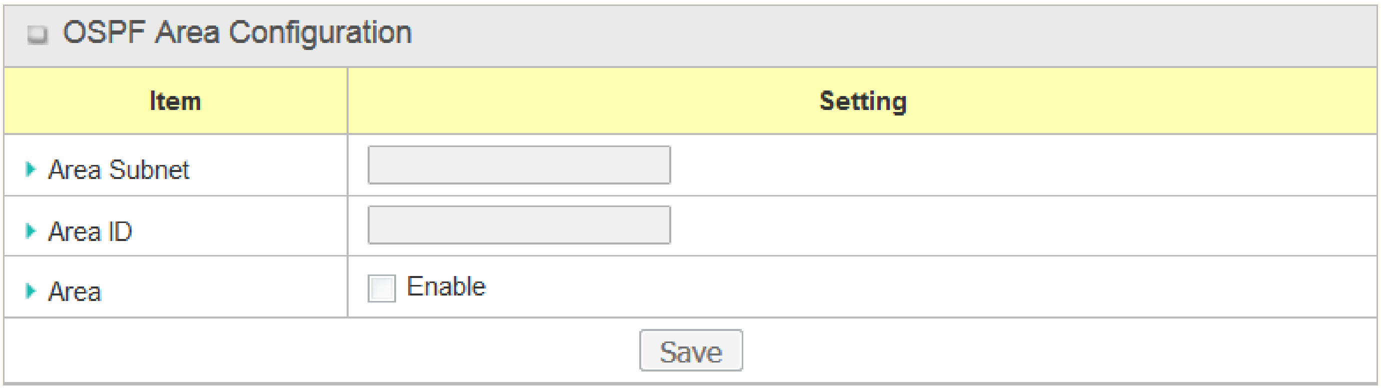
The router allows you to custom your OSPF Area List rules. It supports up to a maximum of 32 rule sets.



OSPF Area List Add Delete

ID	Area Subnet	Area ID	Enable	Actions

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



OSPF Area Configuration

Item	Setting
Area Subnet	
Area ID	
Area	□ Enable

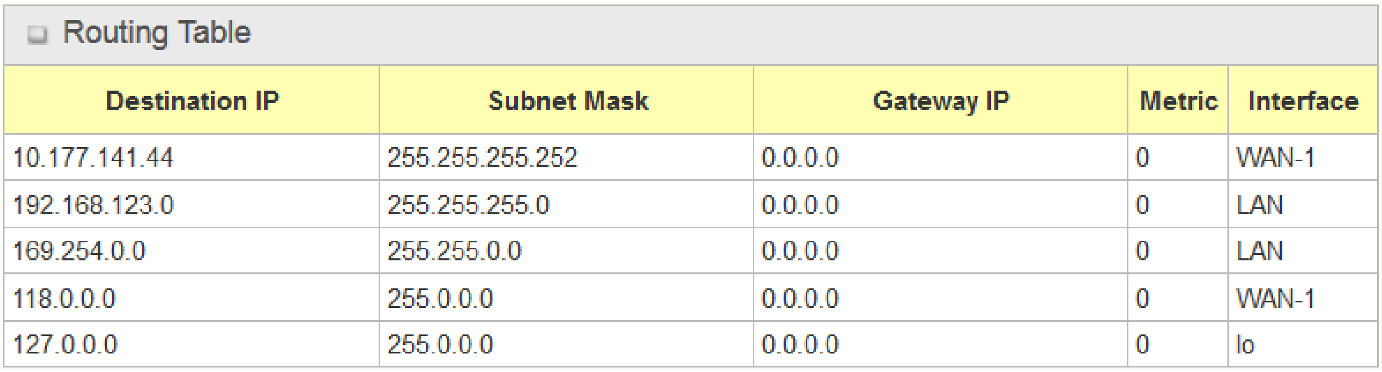
Save

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

2.6.3 Routing Information

The routing information allows user to view the routing table and policy routing information.

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



Routing Table

Destination IP	Subnet Mask	Gateway IP	Metric	Interface
10.177.141.44	255.255.255.252	0.0.0.0	0	WAN-1
192.168.123.0	255.255.255.0	0.0.0.0	0	LAN
169.254.0.0	255.255.0.0	0.0.0.0	0	LAN
118.0.0.0	255.0.0.0	0.0.0.0	0	WAN-1
127.0.0.0	255.0.0.0	0.0.0.0	0	lo

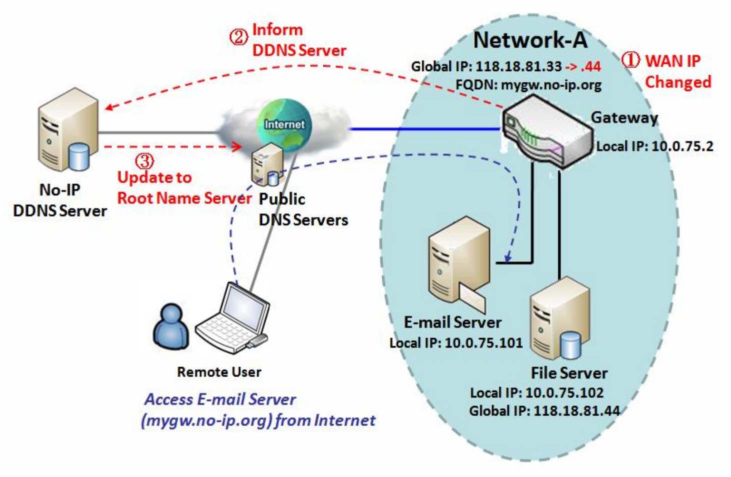
Routing Table		
Item	**Value setting**	**Description**
Destination IP	N/A	Routing record of Destination IP. IPv4 Format.
Subnet Mask	N/A	Routing record of Subnet Mask. IPv4 Format.
Gateway IP	N/A	Routing record of Gateway IP. IPv4 Format.
Metric	N/A	Routing record of Metric. Numeric String Format.
Interface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

2.7 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[1].

2.7.1 DNS & DDNS Configuration

Dynamic DNS



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

The Dynamic DNS service allows the gateway to alias a public dynamic IP address to a static domain name, allowing the gateway to be more easily accessed from various locations on the Internet. As shown in the diagram, user registered a domain name to a third-party DDNS service provider (NO-IP) to use DDNS function. Once the IP address of designated WAN interface has changed, the dynamic DNS agent in the gateway will inform the DDNS server with the new IP address. The server automatically re-maps your domain name with the changed IP address. So, other hosts or remote users in the Internet world are able to link to your gateway by using your domain name regardless of the changing global IP address.

[1] http://en.wikipedia.org/wiki/Domain_Name_System, http://en.wikipedia.org/wiki/Dynamic_DNS

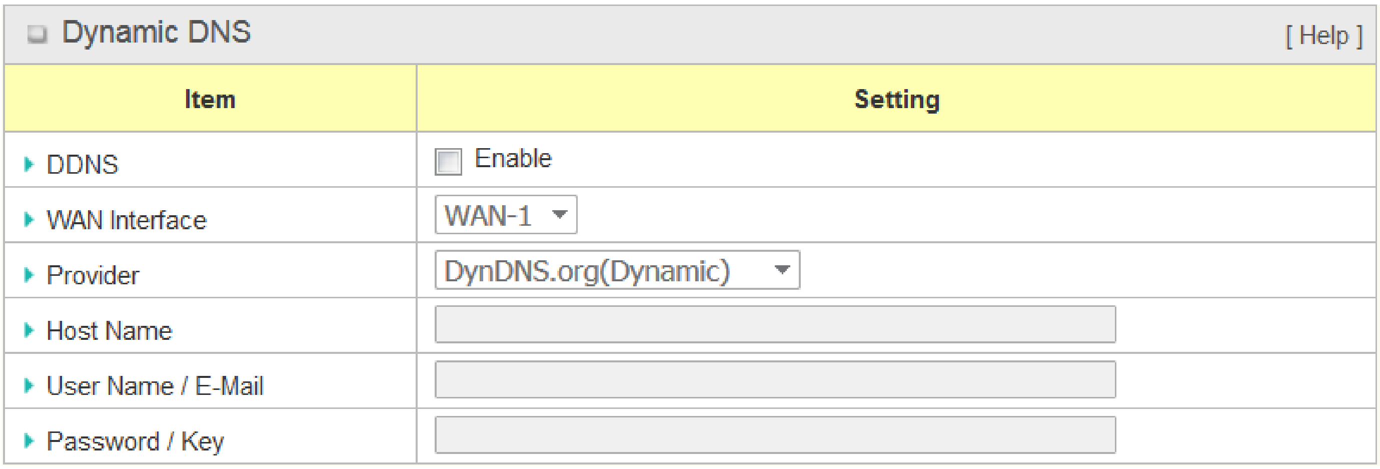
DNS & DDNS Setting

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

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

Setup Dynamic DNS

The router allows you to custom your Dynamic DNS settings.



Dynamic DNS [Help]

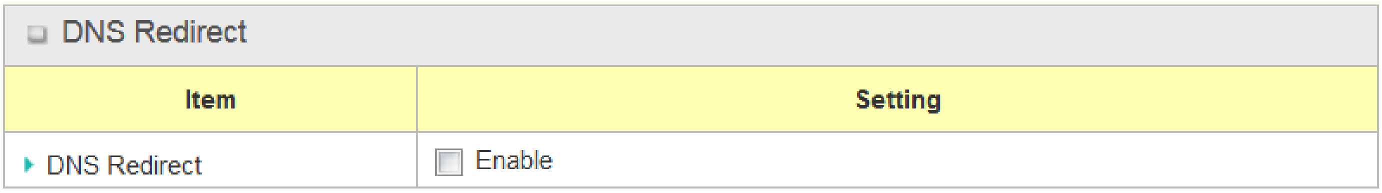
Item	Setting
DDNS	□ Enable
WAN Interface	WAN-1
Provider	DynDNS.org(Dynamic)
Host Name	
User Name / E-Mail	
Password / Key	

DDNS (Dynamic DNS) Configuration

Item	Value setting	Description
DDNS	The box is unchecked by default	Check the **Enable** box to activate this function.
WAN Interface	WAN 1 is set by default	Select the WAN Interface IP Address of the router.
Provider	**DynDNS.org (Dynamic)** is set by default	Select your DDNS provider of Dynamic DNS. It can be **DynDNS.org(Dynamic)**, **DynDNS.org(Custom)**, **NO-IP.com**, etc...
Host Name	1. String format can be any text 2. A Must filled setting	Your registered host name of Dynamic DNS. ***Value Range***: 0 ~ 63 characters.
User Name / E-Mail	1. String format can be any text 2. A Must filled setting	Enter your User name or E-mail address of Dynamic DNS.
Password / Key	1. String format can be any text 2. A Must filled setting	Enter your Password or Key of Dynamic DNS.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Setup DNS Redirect

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

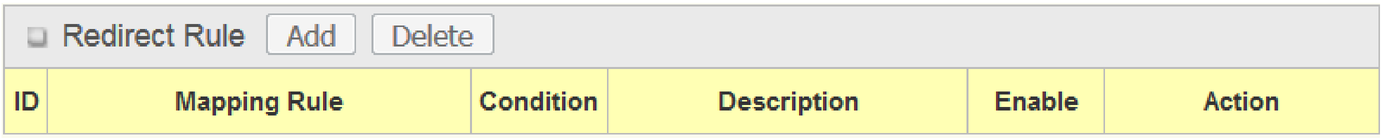


DNS Redirect

Item	Setting
DNS Redirect	□ Enable

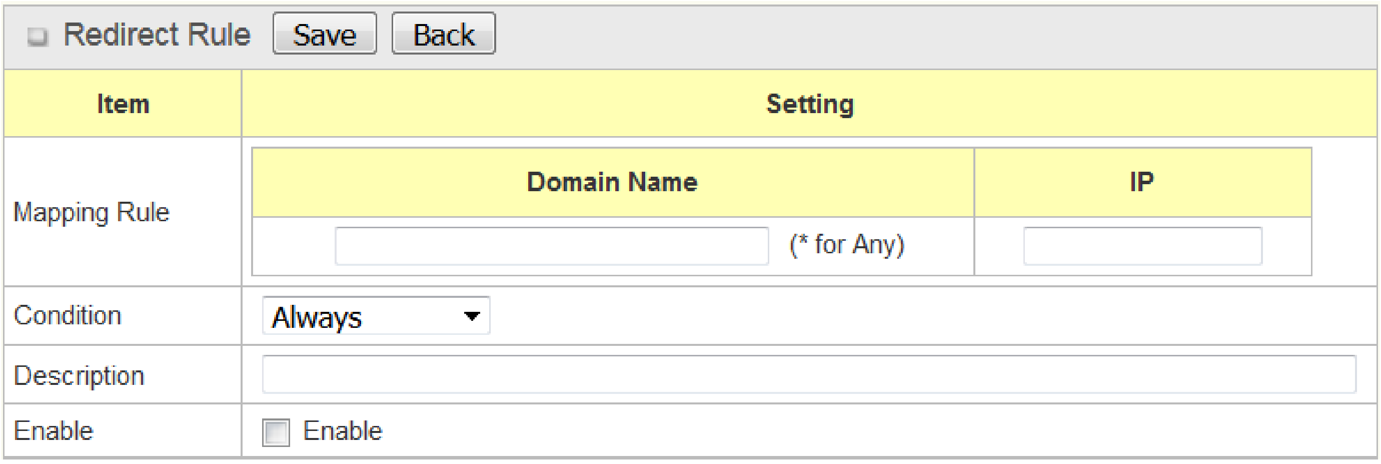
DNS Redirect Configuration		
Item	**Value setting**	**Description**
DNS Redirect	The box is unchecked by default	Check the **Enable** box to activate this function.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

If you enabled the DNS Redirect function, you have to further specify the redirect rules. According to the rules, the router can redirect the traffic that matched the DNS to corresponding pre-defined IP address.



ID	Mapping Rule	Condition	Description	Enable	Action

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



Item	Setting
Mapping Rule	Domain Name: (* for Any) IP:
Condition	Always
Description	
Enable	□ Enable

Redirect Rule Configuration		
Item	**Value setting**	**Description**
Domain Name	1. String format can be any text 2. A Must filled setting	Enter a domain name to be redirect. The traffic to specified domain name will be redirect to the following IP address. ***Value Range***: at least 1 character is required; '*' for any.
IP	1. IPv4 format 2. A Must filled setting	Enter an IP Address as the target for the DNS redirect.
Condition	1. A Must filled setting **2. Always is selected by default.**	Specify when the DNS redirect action can be applied. It can be **Always**, or **WAN Block**. **Always:** The DNS redirect function can be applied to the matched DNS all the time. **WAN Block:** The DNS redirect function can be applied to the matched DNS only when the WAN connection is disconnected, or un-reachable.
Description	1. String format can be any text 2. A Must filled setting	Enter a brief description for this rule. ***Value Range***: 0 ~ 63 characters.
Enable	The box is unchecked by default	Click the **Enable** button to activate this rule.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

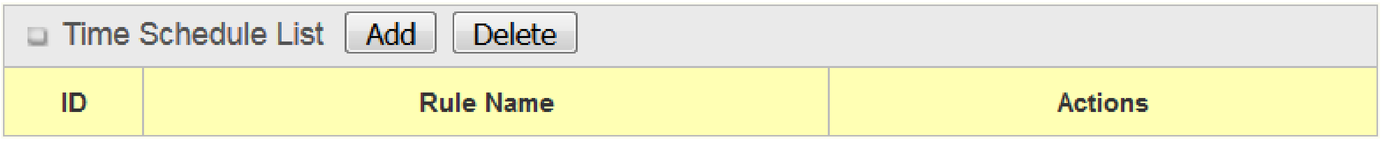
3. Object Definition

3.1 Scheduling

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

3.1.1 Scheduling Configuration

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

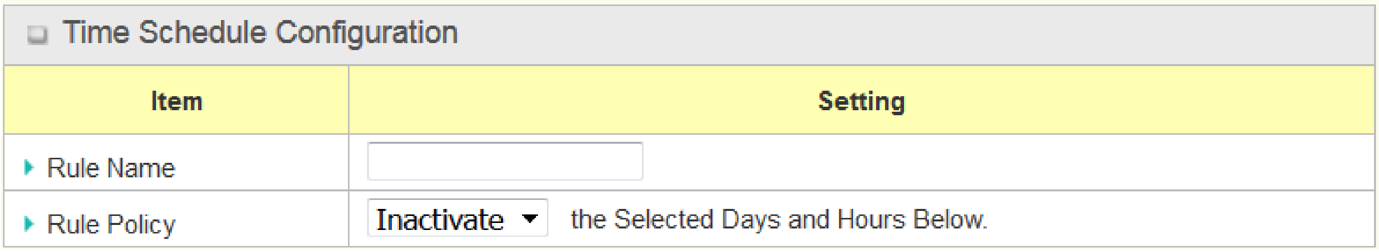


Time Schedule List Add Delete

ID	Rule Name	Actions

Button description		
Item	**Value setting**	**Description**
Add	N/A	Click the **Add** button to configure time schedule rule
Delete	N/A	Click the **Delete** button to delete selected rule(s)

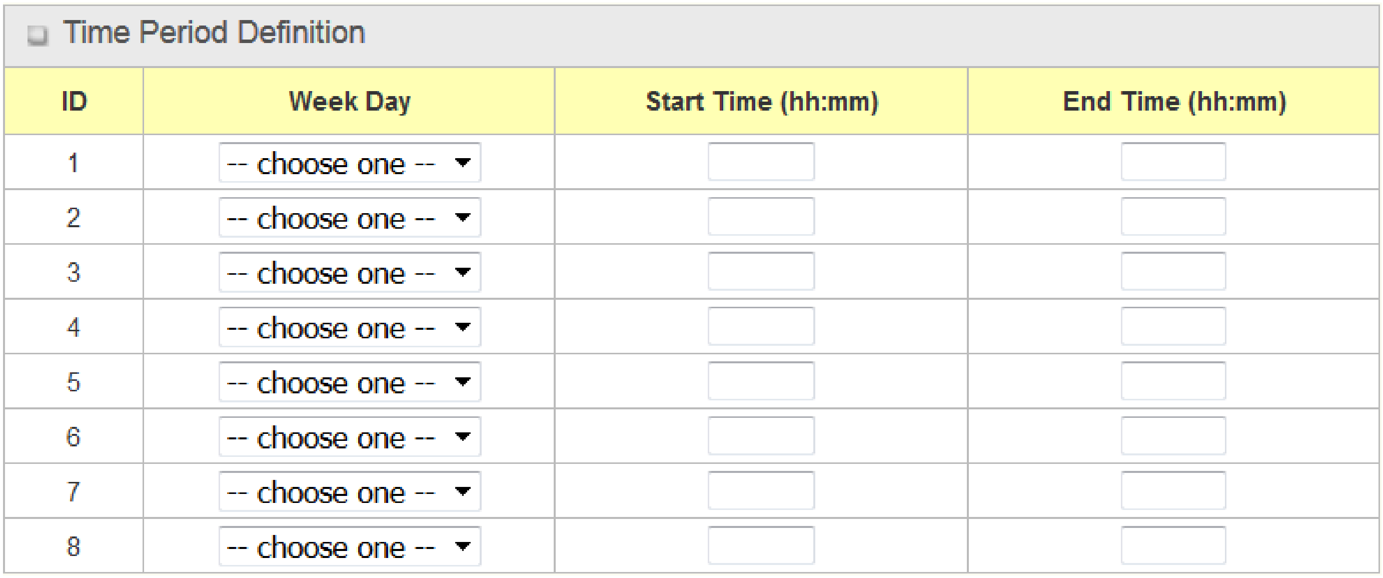
When **Add** button is applied, Time Schedule Configuration and Time Period Definition screens will appear.



Time Schedule Configuration

Item	Setting
Rule Name	
Rule Policy	Inactivate ▾ the Selected Days and Hours Below.

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



Time Period Definition

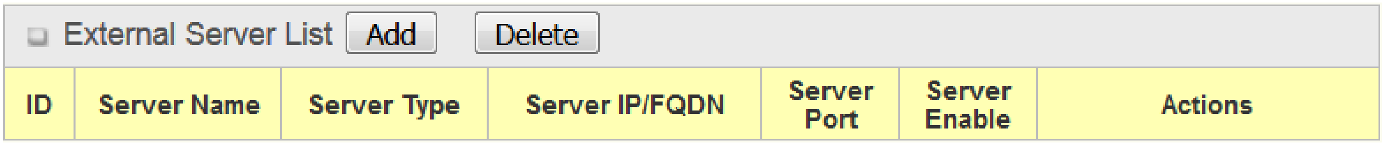
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one --		
2	-- choose one --		
3	-- choose one --		
4	-- choose one --		
5	-- choose one --		
6	-- choose one --		
7	-- choose one --		
8	-- choose one --		

Time Period Definition		
Item	**Value Setting**	**Description**
Week Day	Select from menu	Select everyday or one of weekday
Start Time	Time format (hh:mm)	Start time in selected weekday
End Time	Time format (hh:mm)	End time in selected weekday
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 time schedule list.

3.2 External Server

Go to **Object Definition > External Server > External Server** tab.

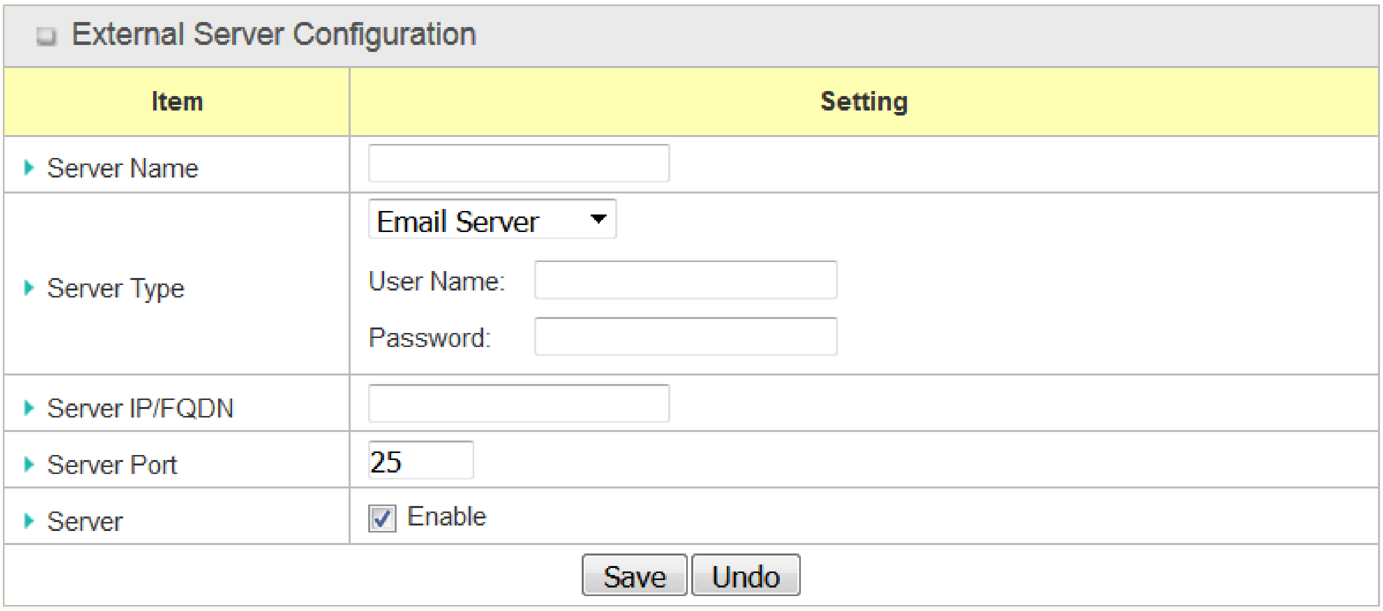
The External Server setting allows user to add external server.



External Server List Add Delete

ID	Server Name	Server Type	Server IP/FQDN	Server Port	Server Enable	Actions

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



External Server Configuration

Item	Setting
Server Name	
Server Type	Email Server User Name: Password:
Server IP/FQDN	
Server Port	25
Server	☑ Enable

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 Type	A Must filled setting	Specify the Server Type of the external server, and enter the required settings for the accessing the server.
		Email Server (A Must filled setting) : When **Email Server** is selected, **User Name**, and **Password** are also required. **User Name** (String format: any text) **Password** (String format: any text)
		Syslog Server
		RADIUS Server (A Must filled setting) : When **RADIUS Server** is selected, the following settings are also required. 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 15. 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 15.
Server IP/FQDN	A Must filled setting	Specify the IP address or FQDN used for the external server.
Server Port	A Must filled setting	Specify the Port used for the external server. If you selected a certain server type, the default server port number will be set. For **Email Server** 25 will be set by default; For **Syslog Server**, port 514 will be set by default; For **RADIUS Server**, port 1812 will be set by default; ***Value Range***: 1 ~ 65535.
Account Port	1. A Must filled setting **2. 1813 is set by default**	Specify the accounting port used if you selected external RADIUS server. ***Value Range***: 1 ~ 65535.
Server	The box is checked by default	Click **Enable to** activate 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.

3.3 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[1].

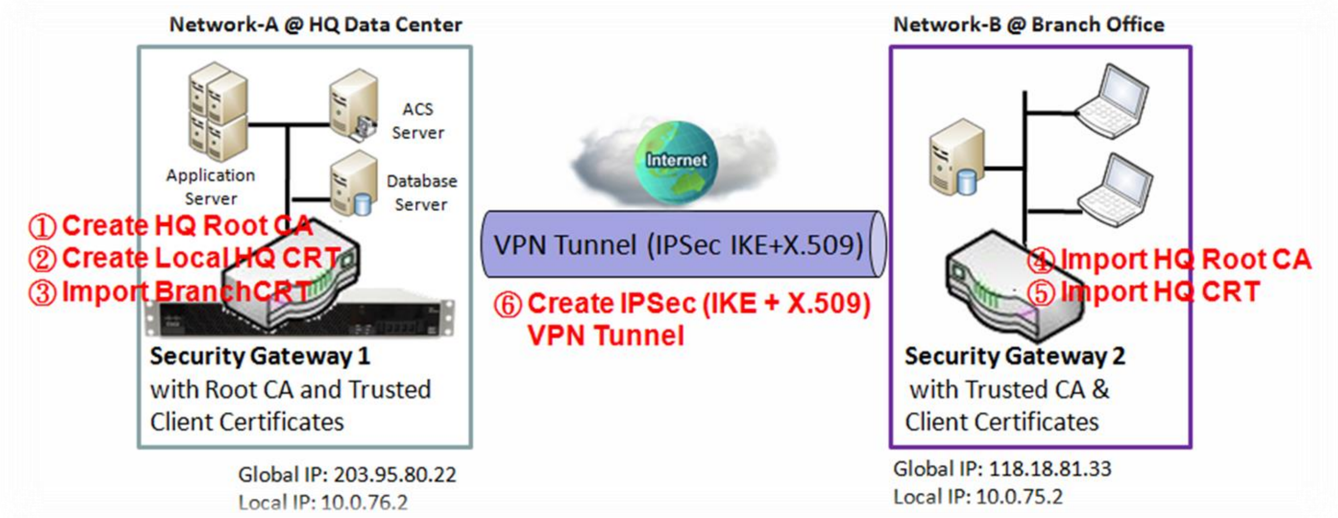
In a typical public-key infrastructure (PKI) scheme, the signer is a certificate authority (CA), usually a company such as VeriSign which charges customers to issue certificates for them. In a web of trust scheme, the signer is either the key's owner (a self-signed certificate) or other users ("endorsements") 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.

3.3.1 My Certificate

My Certificate includes a Local Certificate List. Local Certificate List shows all generated certificates by the root CA for the router. 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 router.

Self-signed Certificate Usage Scenario



Scenario Application Timing

- When the enterprise router 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

[1] http://en.wikipedia.org/wiki/Public_key_certificate

can sign Certificate Signing Requests (CSR) to form corresponding certificates for others.

- These certificates can be used for two remote peers to make sure their identity during establishing a VPN tunnel.

Scenario Description

- Gateway 1 generates the root CA and a local certificate (HQCRT) signed by itself. Import a trusted certificate (BranchCRT) –a BranchCSR certificate of Gateway 2 signed by root CA of Gateway 1.
- Gateway 2 creates a CSR (BranchCSR) to let the root CA of the Gateway 1 sign it to be the BranchCRT certificate. Import the certificate into the Gateway 2 as a local certificate. In addition, also import the certificates of the root CA of the Gateway 1 into the Gateway 2 as the trusted ones. (Please also refer to following two sub-sections.)
- Establish an IPSec VPN tunnel with IKE and X.509 protocols by starting from either peer, so that all client hosts in these both subnets can communicate with each other.

Parameter Setup Example

For Network-A at HQ

- Following tables list the parameter configuration as an example for the "My Certificate" function used in the user authentication of IPSec VPN tunnel establishing, as shown in above diagram.
- The configuration example must be combined with the ones in following two sections to complete the whole user scenario.
- Use default value for those parameters that are not mentioned in the tables.

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

Configuration Path	[My Certificate]-[Local Certificate Configuration]
Name	***HQCRT*** Self-signed: ■
Key	Key Type: ***RSA*** Key Length: ***1024-bits***
Subject Name	Country(C): ***TW*** State(ST): ***Taiwan*** Location(L): ***Tainan*** Organization(O): ***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 Certificate" function used in the user authentication of IPSec VPN tunnel establishing, as shown in above diagram.
- The configuration example must be combined with the ones in following two sections to complete the whole user scenario.
- Use default value for those parameters that are not mentioned in the tables.

Configuration Path	[My Certificate]-[Local Certificate Configuration]
Name	***BranchCRT*** Self-signed: □
Key	Key Type: ***RSA*** Key Length: ***1024-bits***
Subject Name	Country(C): ***TW*** State(ST): ***Taiwan*** Location(L): ***Tainan*** Organization(O): ***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

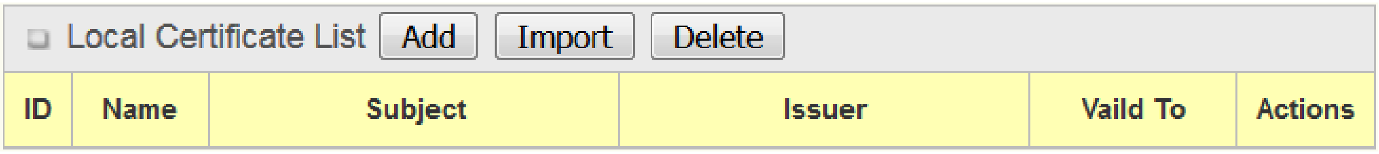
- In above diagram, "Gateway 1" is the gateway of Network-A in headquarters and the subnet of its Intranet is 10.0.76.0/24. It has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN-1 interface. "Gateway 2" is the gateway of Network-B in branch office and the subnet of its Intranet 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.

My Certificate Setting

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

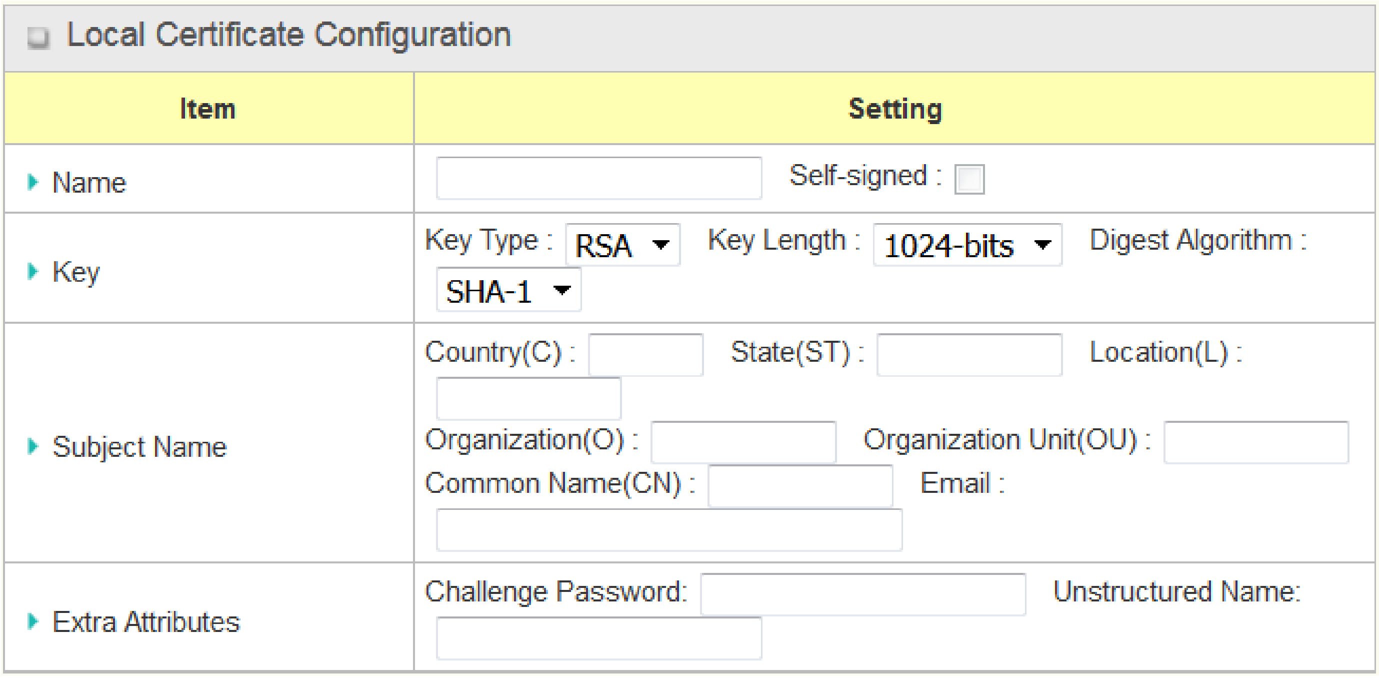
The My Certificate setting allows user to create local certificates. In "My Certificate" page, there are two configuration windows for the "My Certificate" function. The "Local Certificate List" window shows the stored certificates or CSRs for representing the gateway. The "Local Certificate Configuration" window can let you fill required information necessary for corresponding certificate to be generated by itself, or corresponding CSR to be signed by other CAs.

Create Local Certificate



ID	Name	Subject	Issuer	Vaild To	Actions

When **Add** button is applied, **Local Certificate Configuration** screen will appear. The required information to be filled for the certificate or CSR includes the name, key and subject name. It is a certificate if the "Self-signed" box is checked; otherwise, it is a CSR.



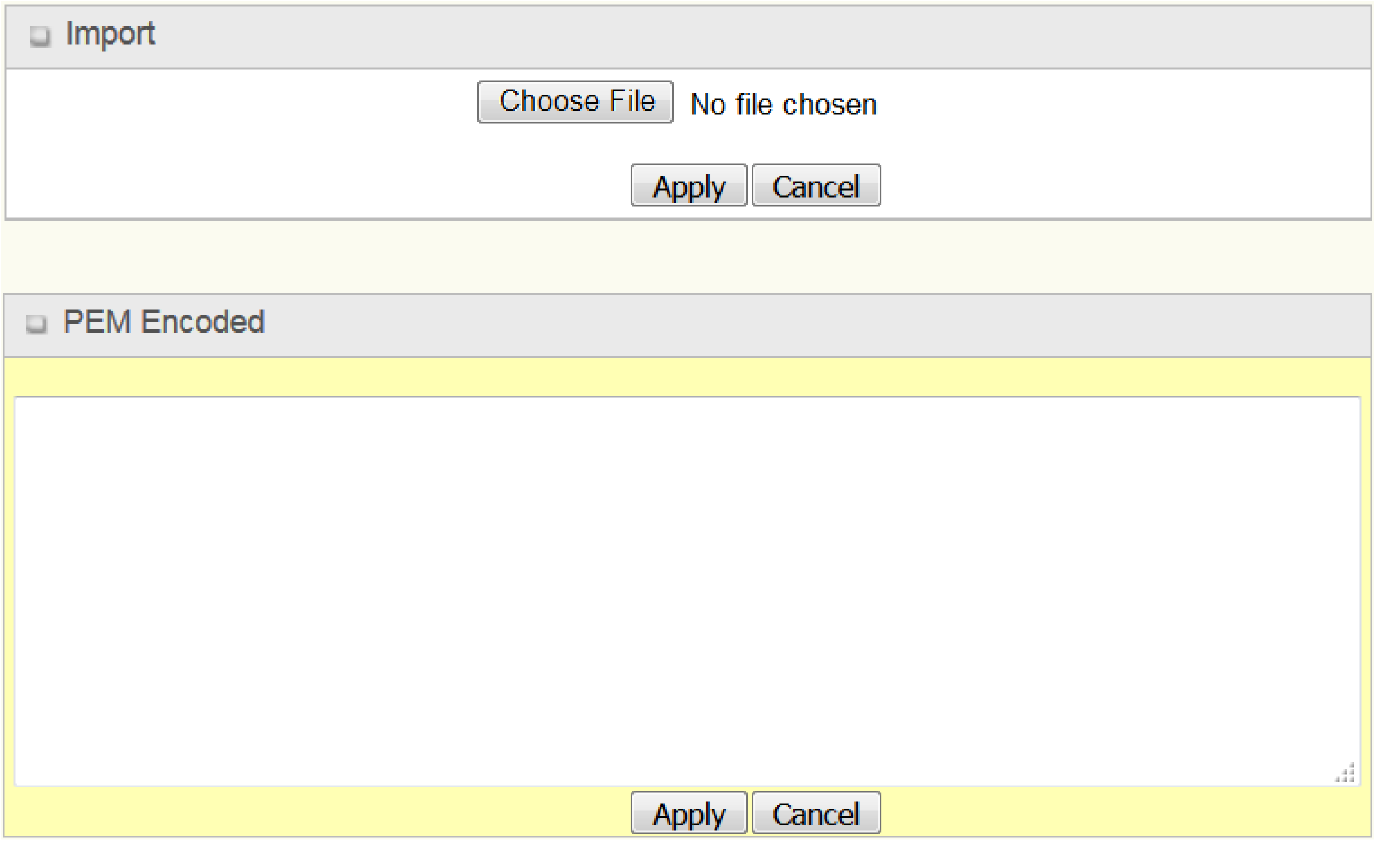
Item	Setting
Name	Self-signed : □
Key	Key Type : RSA Key Length : 1024-bits Digest Algorithm : SHA-1

Subject Name	Country(C) :
	State(ST) :
	Location(L) :
	Organization(O) :
	Organization Unit(OU) :
	Common Name(CN) :
	Email :

Extra Attributes	Challenge Password: Unstructured Name:

Local Certificate Configuration		
Item	**Value setting**	**Description**
Name	1. String format can be any text 2. A Must filled setting	Enter a certificate name. It will be a certificate file name If **Self-signed** is checked, it will be signed by root CA. If **Self-signed** is not checked, it will generate a certificate signing request (CSR).
Key	A Must filled setting	This field is to specify the key attributes of certificate. **Key Type** to set public-key cryptosystems. Currently, only RSA is supported. **Key Length** to set the length in bits of the key used in a cryptographic algorithm. It can be 512/768/1024/1536/2048. **Digest Algorithm** to set identifier in the signature algorithm identifier of certificates. It can be MD5/SHA-1.
Subject Name	A Must filled setting	This field is to specify the information of certificate. **Country(C)** is the two-letter ISO code for the country where your organization is located. **State(ST)** is the state where your organization is located. **Location(L)** is the location where your organization is located. **Organization(O)** is the name of your organization. **Organization Unit(OU)** is the name of your organization unit. **Common Name(CN)** is the name of your organization. **Email** is the email of your organization. It has to be email address setting only.
Extra Attributes	A Must filled setting	This field is to specify the extra information for generating a certificate. **Challenge Password** for the password you can use to request certificate revocation in the future. **Unstructured Name** for additional information.
Save	N/A	Click the **Save** button to save the configuration.
Back	N/A	When the **Back** button is clicked, the screen will return to previous page.

When **Import** button is applied, an Import screen will appear. You can import a certificate from an existed certificate file, or directly paste a PEM encoded string as the certificate.

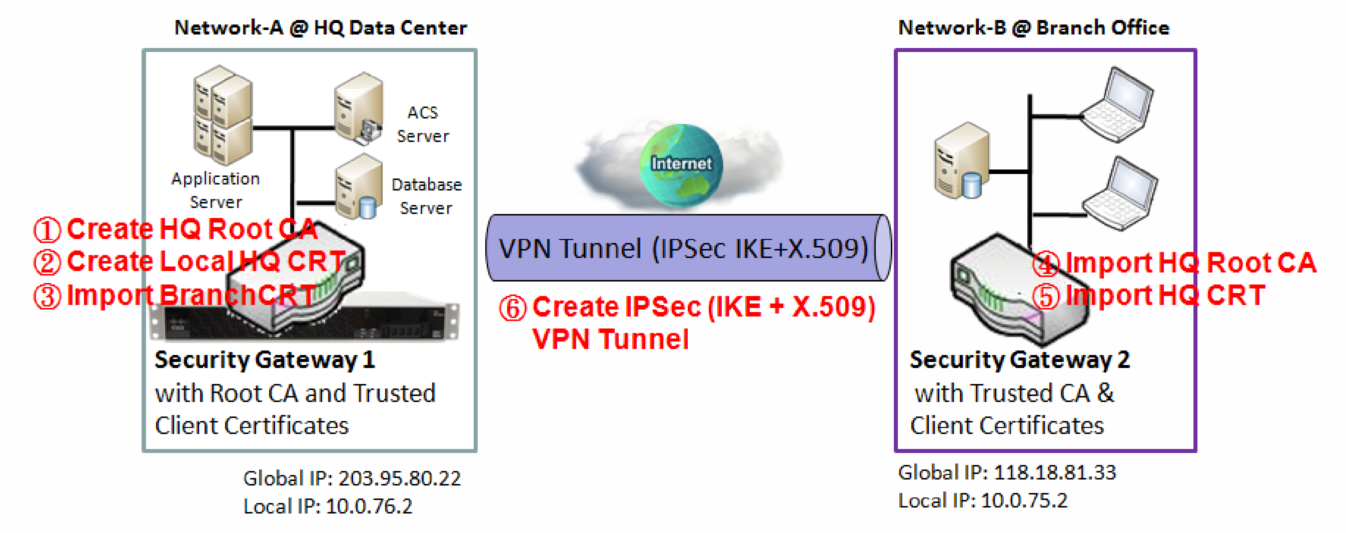


Import		
Item	**Value setting**	**Description**
Import	A Must filled setting	Select a certificate file from user's computer, and click the **Apply** button to import the specified certificate file to the router.
PEM Encoded	1. String format can be any text 2. A Must filled setting	This is an alternative approach to import a certificate. You can directly fill in (Copy and Paste) the PEM encoded certificate string, and click the **Apply** button to import the specified certificate to the router.
Apply	N/A	Click the **Apply** button to import the certificate.
Cancel	N/A	Click the **Cancel** button to discard the import operation and the screen will return to the My Certificates page.

3.3.2 Trusted Certificate

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

Self-signed Certificate Usage Scenario



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

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

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

- Gateway 1 generates the root CA and a local certificate (HQCRT) signed by itself. Import a trusted certificate (BranchCRT) –a BranchCSR certificate of Gateway 2 signed by root CA of Gateway 1.
- Gateway 2 creates a CSR (BranchCSR) to let the root CA of the Gateway 1 sign it to be the BranchCRT certificate. Import the certificate into the Gateway 2 as a local certificate. In addition, also imports the certificates of the root CA of Gateway 1 into the Gateway 2 as the trusted ones. (Please also refer to "My Certificate" and "Issue Certificate" sections).
- Establish an IPSec VPN tunnel with IKE and X.509 protocols by starting from either peer, so that all client hosts in these both subnets can communicate with each other.

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

For Network-A at HQ

- Following tables list the parameter configuration as an example for the "Trusted Certificate" function used in the user authentication of IPSec VPN tunnel establishing, as shown in above diagram.
- The configuration example must be combined with the ones in "My Certificate" and "Issue Certificate" sections to complete the setup for the whole user scenario.

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate List]
Command Button	*Import*

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate Import from a File]
File	*BranchCRT.crt*

For Network-B at Branch Office

- Following tables list the parameter configuration as an example for the "Trusted Certificate" function used in the user authentication of IPSec VPN tunnel establishing, as shown in above diagram.
- The configuration example must be combined with the ones in "My Certificate" and "Issued Certificate" sections to complete the setup for the whole user scenario.

Configuration Path	[Trusted Certificate]-[Trusted CA Certificate List]
Command Button	***Import***

Configuration Path	[Trusted Certificate]-[Trusted CA Certificate Import from a File]
File	***HQRootCA.crt***

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate List]
Command Button	***Import***

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate Import from a File]
File	***HQCRT.crt***

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

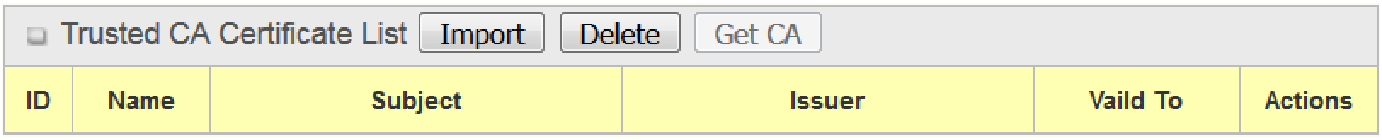
- In above diagram, the "Gateway 1" is the gateway of Network-A in headquarters and the subnet of its Intranet is 10.0.76.0/24. It has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN-1 interface. The "Gateway 2" is the gateway of Network-B in branch office and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. They both serve as the NAT security gateways.
- In Gateway 2 import the certificates of the root CA and HQCRT that were generated and signed by Gateway 1 into the "Trusted CA Certificate List" and "Trusted Client Certificate List" of Gateway 2.
- Import the obtained BranchCRT certificate (the derived BranchCSR certificate after Gateway 1’s root CA signature) into the "Trusted Client Certificate List" of the Gateway 1 and the "Local Certificate List" of the Gateway 2. For more details, refer to the Network-B operation procedure in "My Certificate" section of this manual.
- Gateway 2 can establish an IPSec VPN tunnel with "Site to Site" scenario and IKE and X.509 protocols to Gateway 1.
- Finally, the client hosts in two subnets of 10.0.75.0/24 and 10.0.76.0/24 can communicate with each other.

Trusted Certificate Setting

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

The Trusted Certificate setting allows user to import trusted certificates and keys.

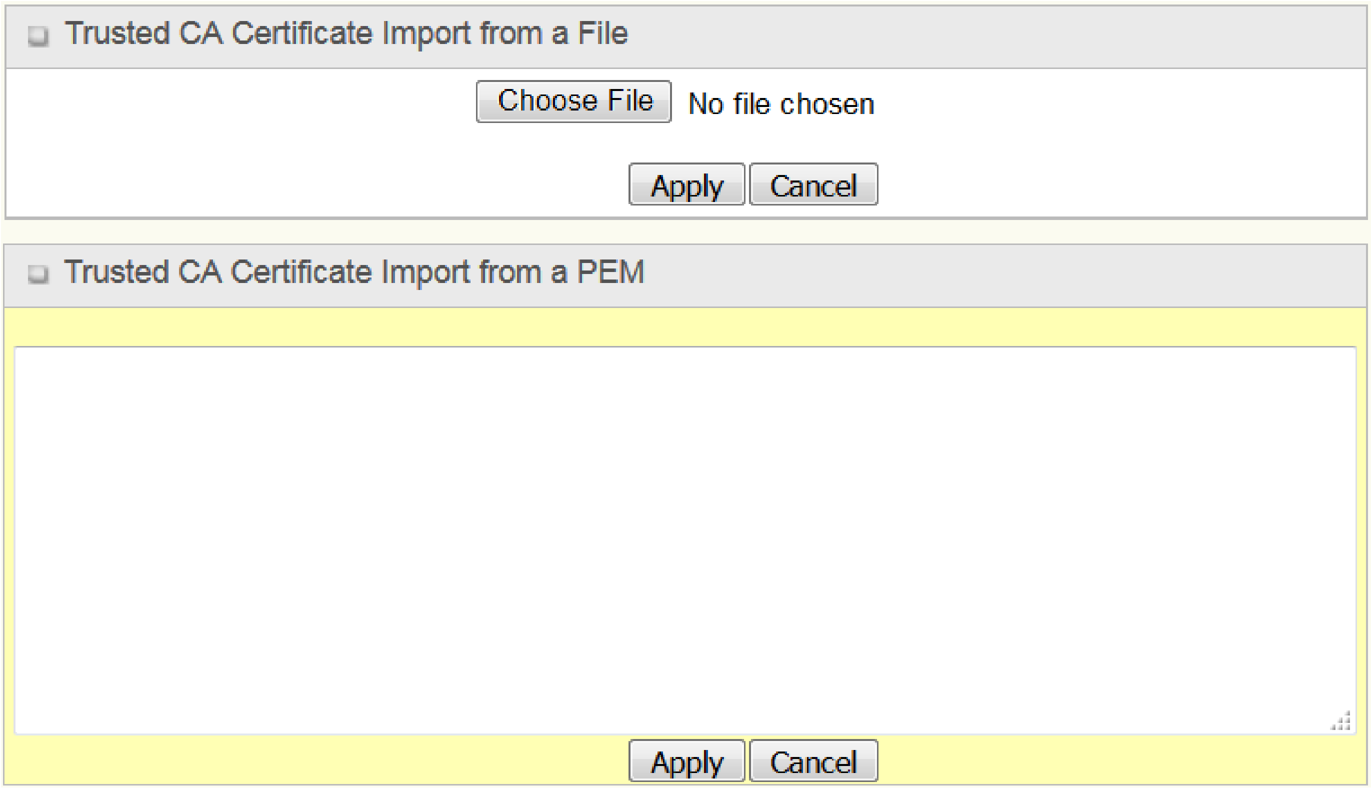
Import Trusted CA Certificate



Trusted CA Certificate List

ID	Name	Subject	Issuer	Vaild To	Actions

When **Import** button is applied, a **Trusted CA import** screen will appear. You can import a Trusted CA certificate from an existed certificate file, or directly paste a PEM encoded string as the certificate.



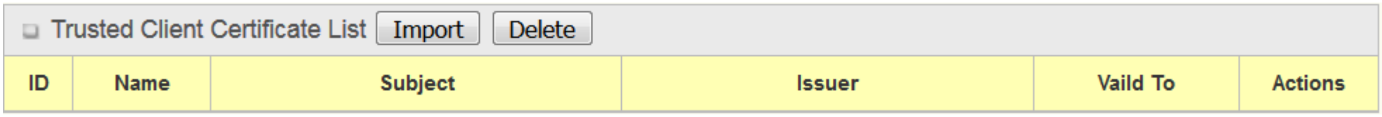
Trusted CA Certificate Import from a File

No file chosen

Trusted CA Certificate Import from a PEM

Trusted CA Certificate List		
Item	**Value setting**	**Description**
Import from a File	A Must filled setting	Select a CA certificate file from user's computer, and click the **Apply** button to import the specified CA certificate file to the router.
Import from a PEM	1. String format can be any text 2. A Must filled setting	This is an alternative approach to import a CA certificate. You can directly fill in (Copy and Paste) the PEM encoded CA certificate string, and click the **Apply** button to import the specified CA certificate to the router.
Apply	N/A	Click the **Apply** button to import the certificate.
Cancel	N/A	Click the **Cancel** button to discard the import operation and the screen will return to the Trusted Certificates page.

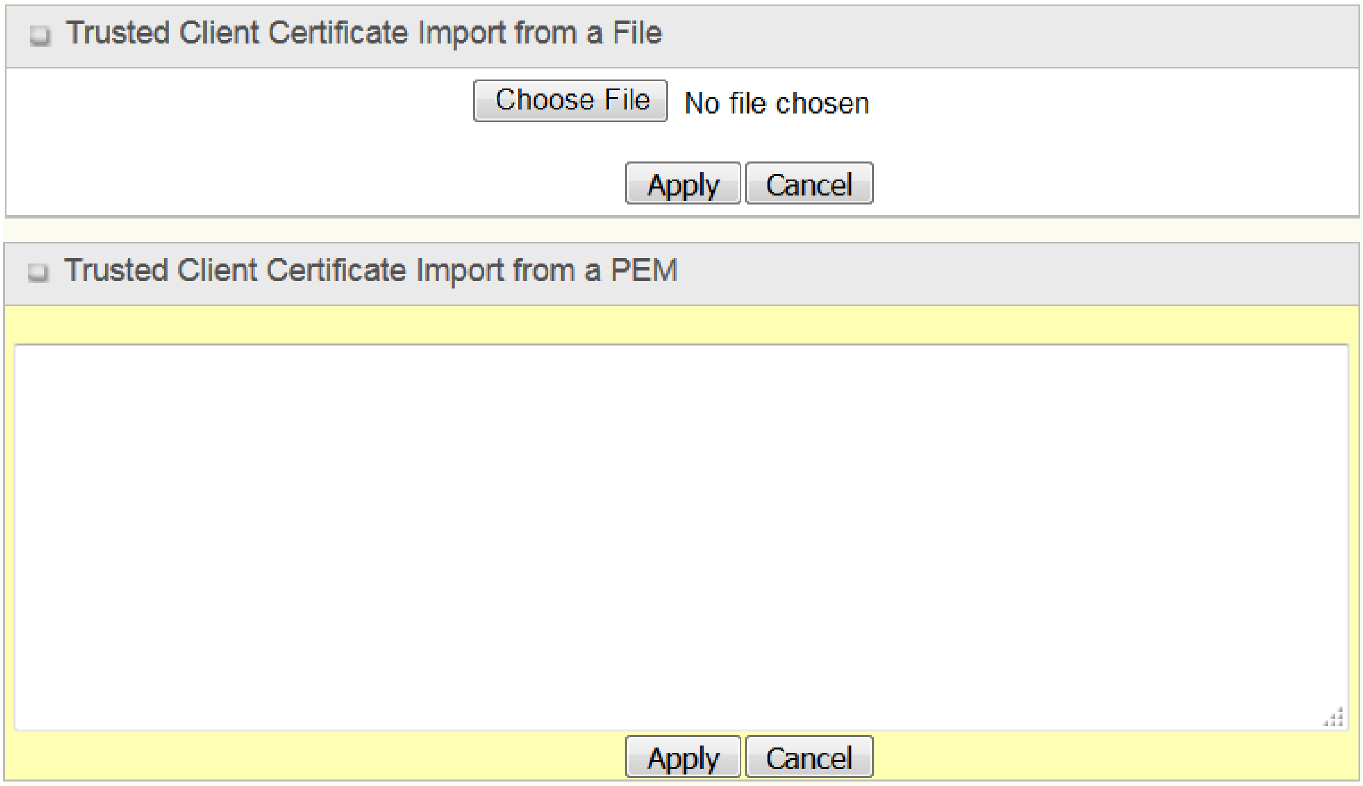
Import Trusted Client Certificate



Trusted Client Certificate List

ID	Name	Subject	Issuer	Vaild To	Actions

When **Import** button is applied, a **Trusted Client Certificate Import** screen will appear. You can import a Trusted Client Certificate from an existed certificate file, or directly paste a PEM encoded string as the certificate.

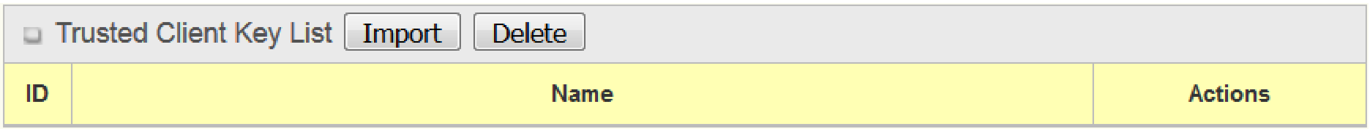


Trusted Client Certificate Import from a File

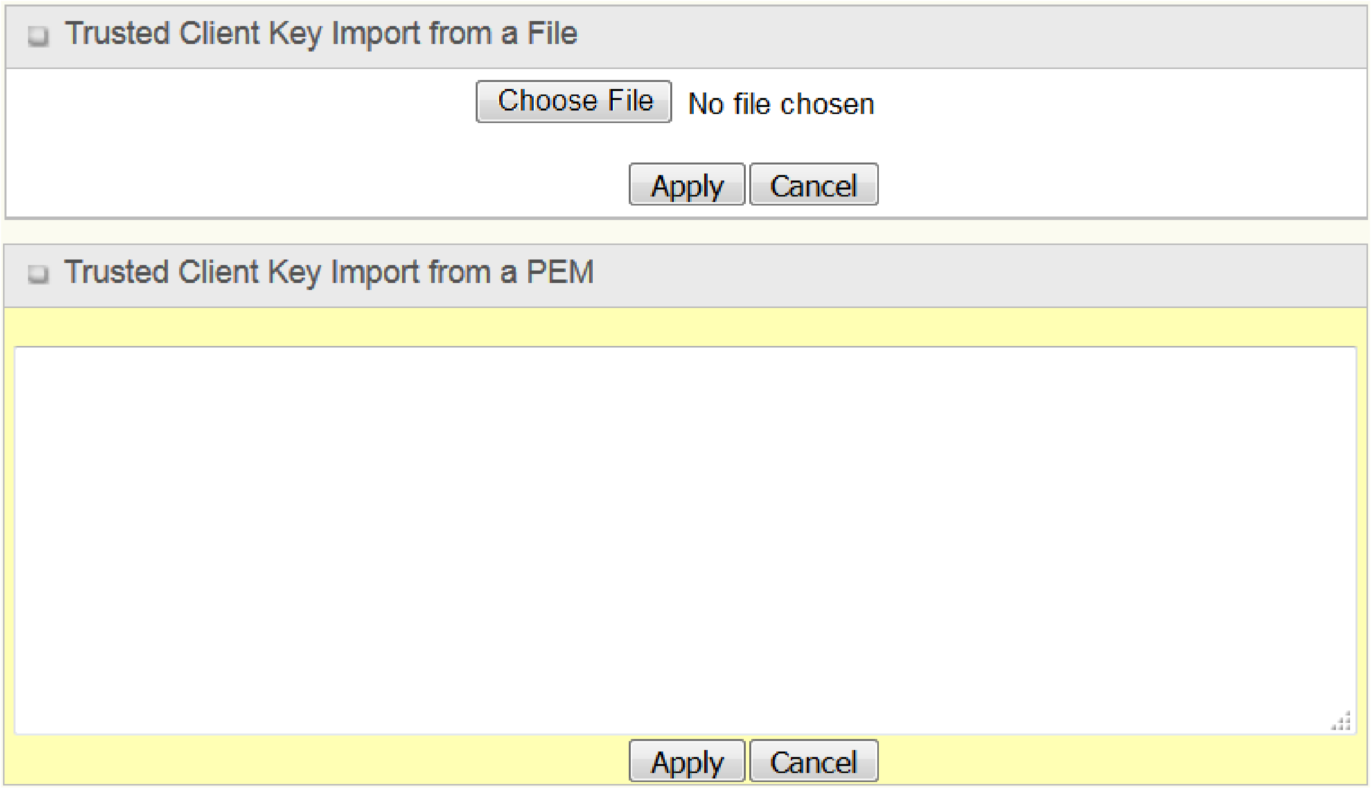
Trusted Client Certificate Import from a PEM

Trusted Client Certificate List		
Item	**Value setting**	**Description**
Import from a File	A Must filled setting	Select a certificate file from user's computer, and click the **Apply** button to import the specified certificate file to the router.
Import from a PEM	1. String format can be any text 2. A Must filled setting	This is an alternative approach to import a certificate. You can directly fill in (Copy and Paste) the PEM encoded certificate string, and click the **Apply** button to import the specified certificate to the router.
Apply	N/A	Click the **Apply** button to import certificate.
Cancel	N/A	Click the **Cancel** button to discard the import operation and the screen will return to the Trusted Certificates page.

Import Trusted Client Key



When **Import** button is applied, a **Trusted Client Key Import** screen will appear. You can import a Trusted Client Key from an existed file, or directly paste a PEM encoded string as the key.

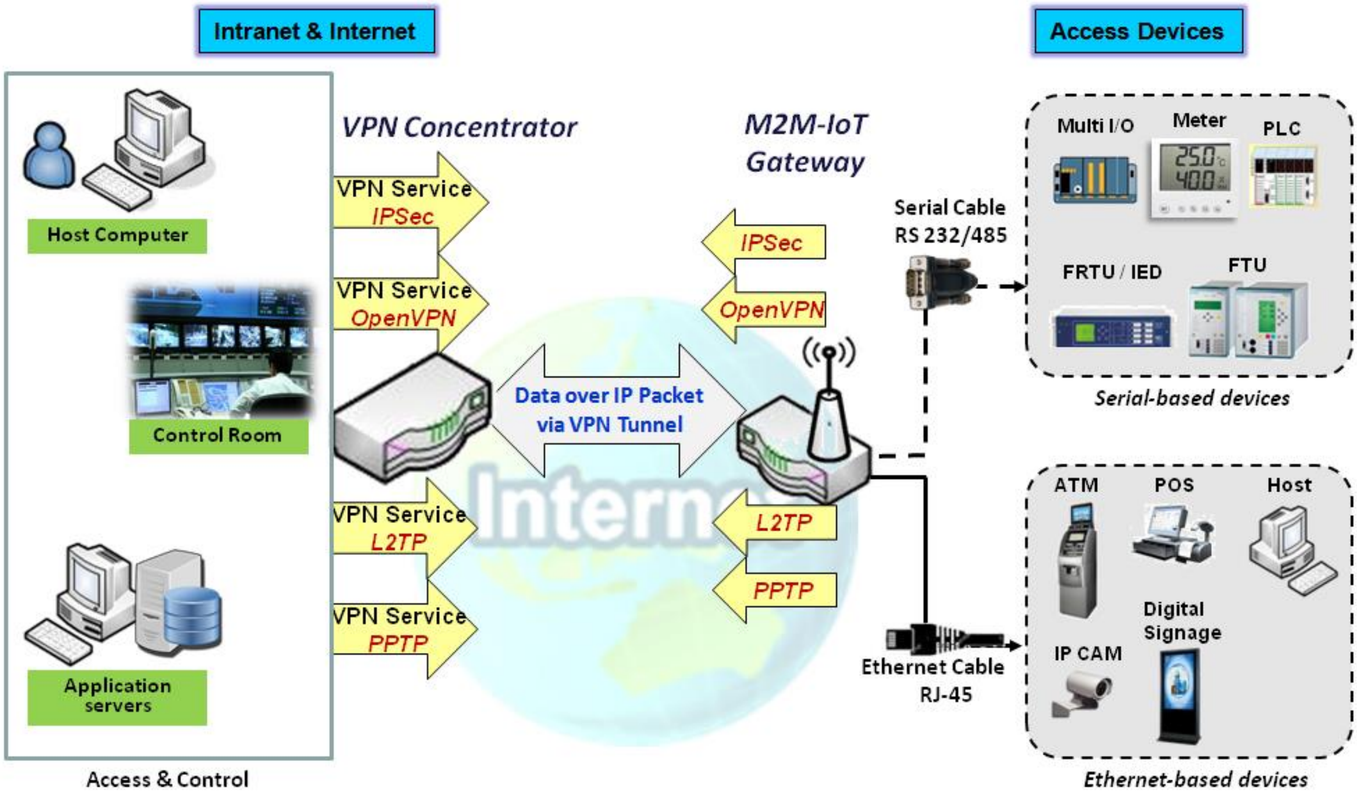

Trusted Client Key Import from a File
Choose File
No file chosen
Apply
Cancel
Trusted Client Key Import from a PEM
Apply
Cancel

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

4. Security

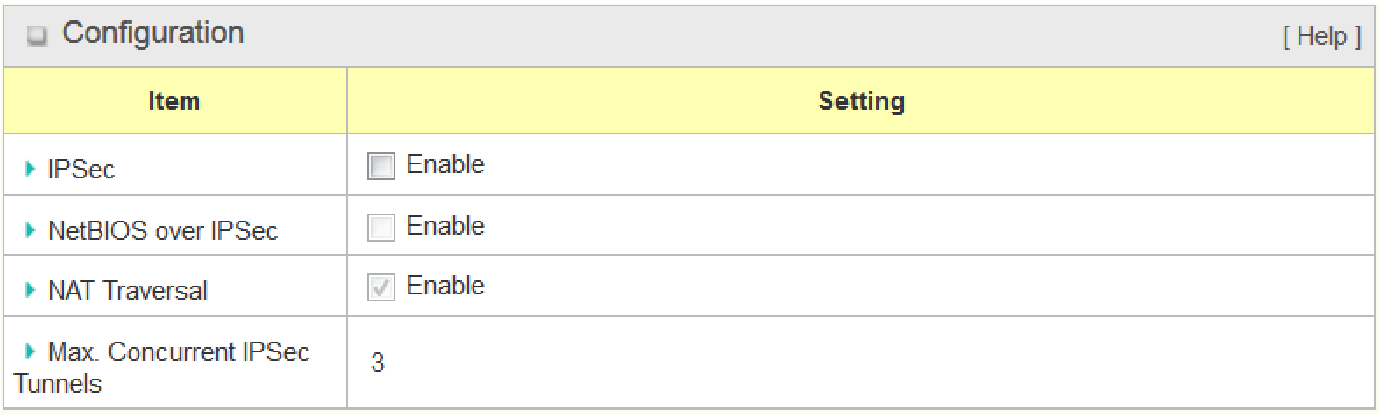
4.1 VPN

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The tunnel technology supports data confidentiality, data origin authentication and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.



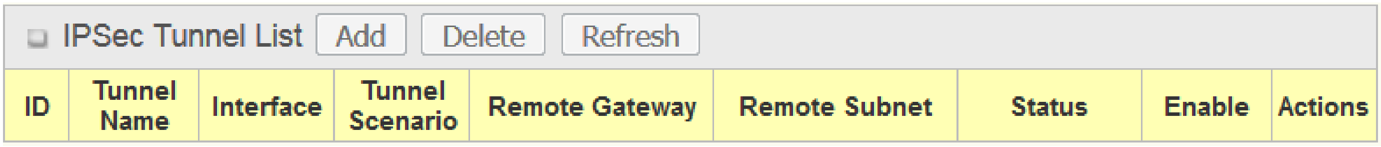
The product series supports different tunneling technologies to establish secure tunnels between multiple sites for data transferring, such as IPSec, OpenVPN, L2TP (over IPSec), PPTP and GRE. Besides, some advanced functions, like Full Tunnel, Tunnel Failover, NetBIOS over IPSec, NAT Traversal are also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

4.1.1 IPSec



Configuration [Help]

Item	Setting
IPSec	□ Enable
NetBIOS over IPSec	□ Enable
NAT Traversal	☑ Enable
Max. Concurrent IPSec Tunnels	3



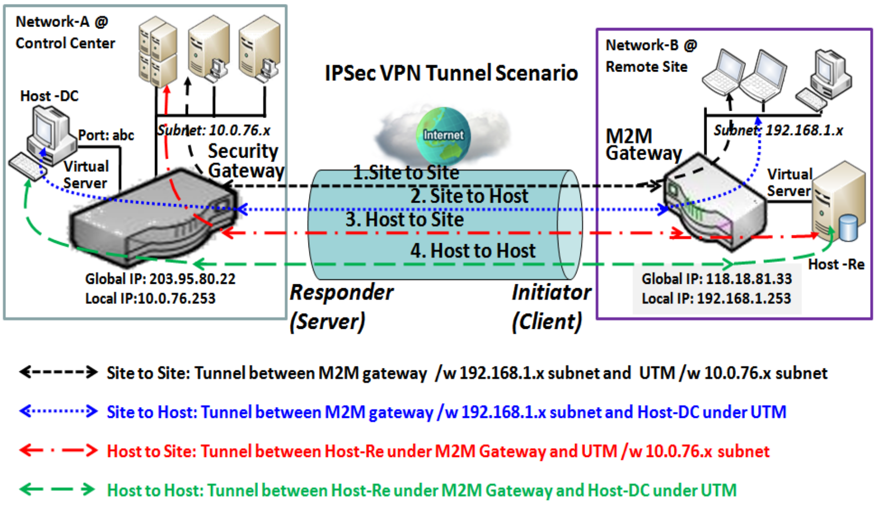
IPSec Tunnel List Add Delete Refresh

ID	Tunnel Name	Interface	Tunnel Scenario	Remote Gateway	Remote Subnet	Status	Enable	Actions

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

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

IPSec Tunnel Scenarios



<-----> Site to Site: Tunnel between M2M gateway /w 192.168.1.x subnet and UTM /w 10.0.76.x subnet

<·······> Site to Host: Tunnel between M2M gateway /w 192.168.1.x subnet and Host-DC under UTM

<-·-> Host to Site: Tunnel between Host-Re under M2M Gateway and UTM /w 10.0.76.x subnet

<— —> Host to Host: Tunnel between Host-Re under M2M Gateway and Host-DC under UTM

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

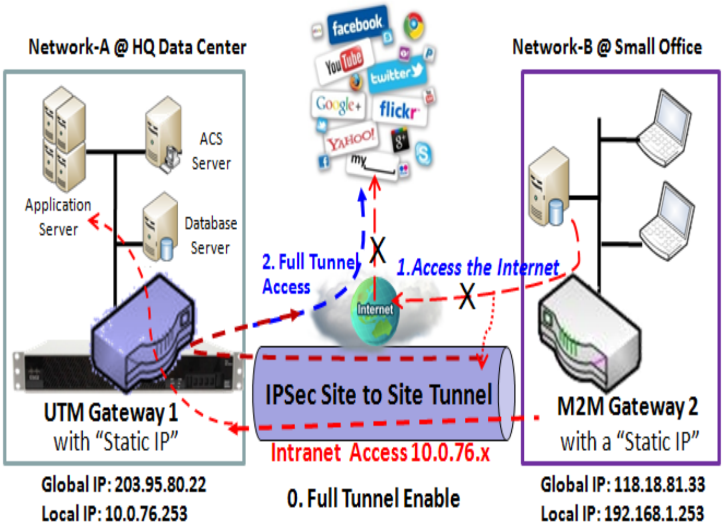
Site to Site: You need to setup remote gateway IP and subnet of both gateways. After the IPSec tunnel established, hosts behind both gateways can communication each other through the tunnel.

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

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

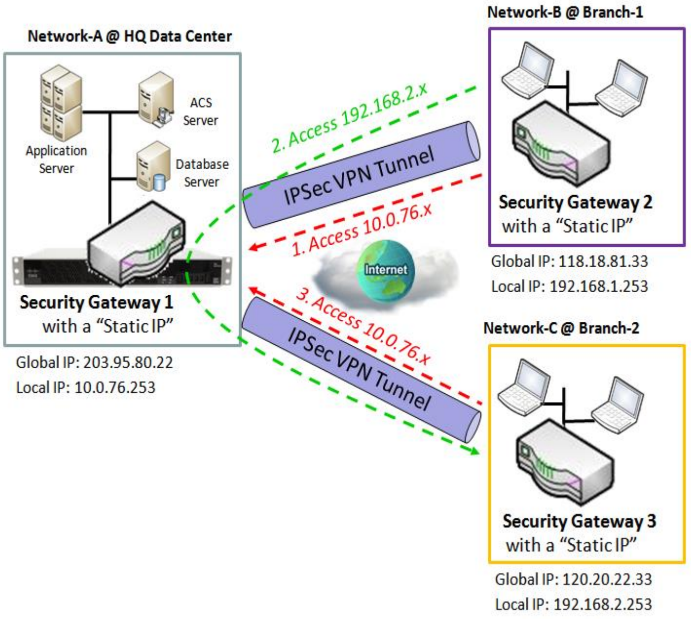
Host to Host: Host to Host is a special configuration for building a VPN tunnel between two single hosts.

Site to Site with "Full Tunnel" enabled



In "Site to Site" scenario, client hosts in remote site can access the enterprise resources in the Intranet of HQ gateway via an established IPSec tunnel, as described above. However, Internet access originates from remote site still go through its regular WAN connection. If you want all packets from remote site to be routed via this IPSec tunnel, including HQ server access and Internet access, you can just enable the "Full Tunnel" setting. As a result, every time users surfs web or searching data on Internet, checking personal emails, or HQ server access, all traffics will go through the secure IPSec tunnel and route by the Security Gateway in control center.

Site to Site with "Hub and Spoke" mechanism



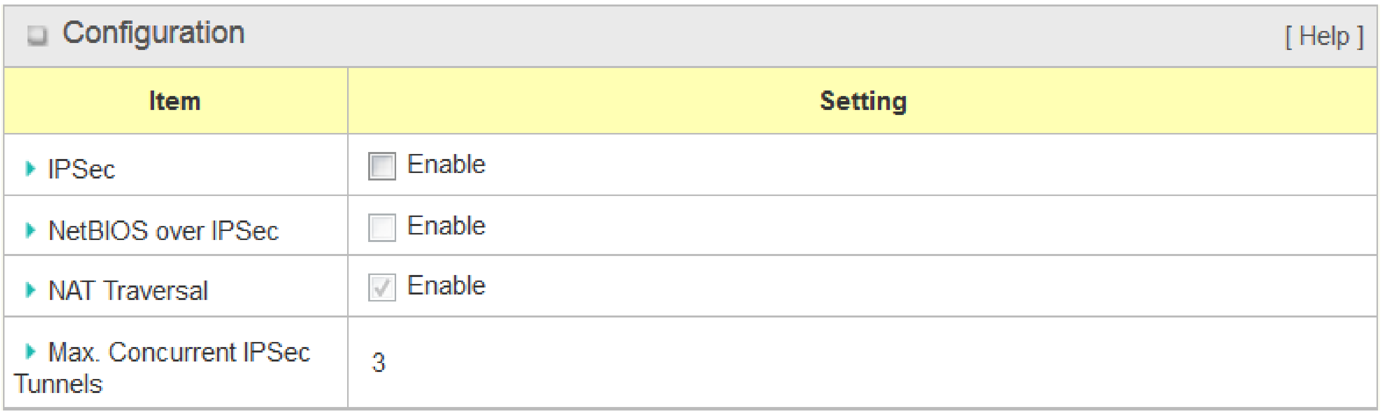
For a control center to manage the secure Intranet among all its remote sites, there is a simple configuration, called **Hub and Spoke**, for the whole VPN network. A Hub and Spoke VPN Network is set up in organizations with centralized control center over all its remote sites, like shops or offices. The control center acts as the Hub role and the remote shops or Offices act as Spokes. All VPN tunnels from a remote sites terminate at this Hub, which acts as a concentrator. Site-to-site connections between spokes do not exist. Traffic originating from one spoke and destined for another spoke has to go via the Hub. Under such configuration, you don't need to maintain VPN tunnels between each two remote clients.

IPSec Setting

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

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

Enable IPSec



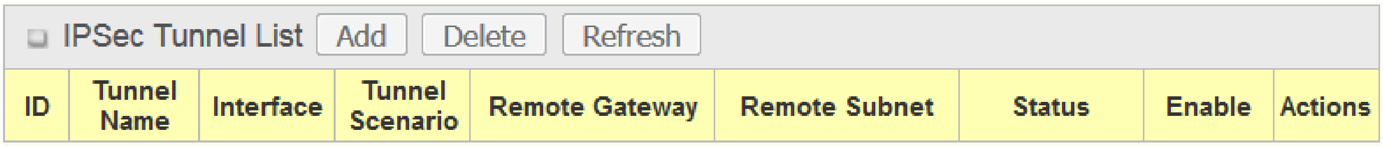
Configuration

Item	Setting
IPSec	□ Enable
NetBIOS over IPSec	□ Enable
NAT Traversal	☑ Enable
Max. Concurrent IPSec Tunnels	3

Configuration 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	Checked by default	Click the **Enable** box to enable NAT Traversal function.
Max. Concurrent IPSec Tunnels	Depends on Product specification.	The specified value will limit the maximum number of simultaneous IPSec tunnel connection. The default value can be different for the purchased model.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Create/Edit IPSec tunnel

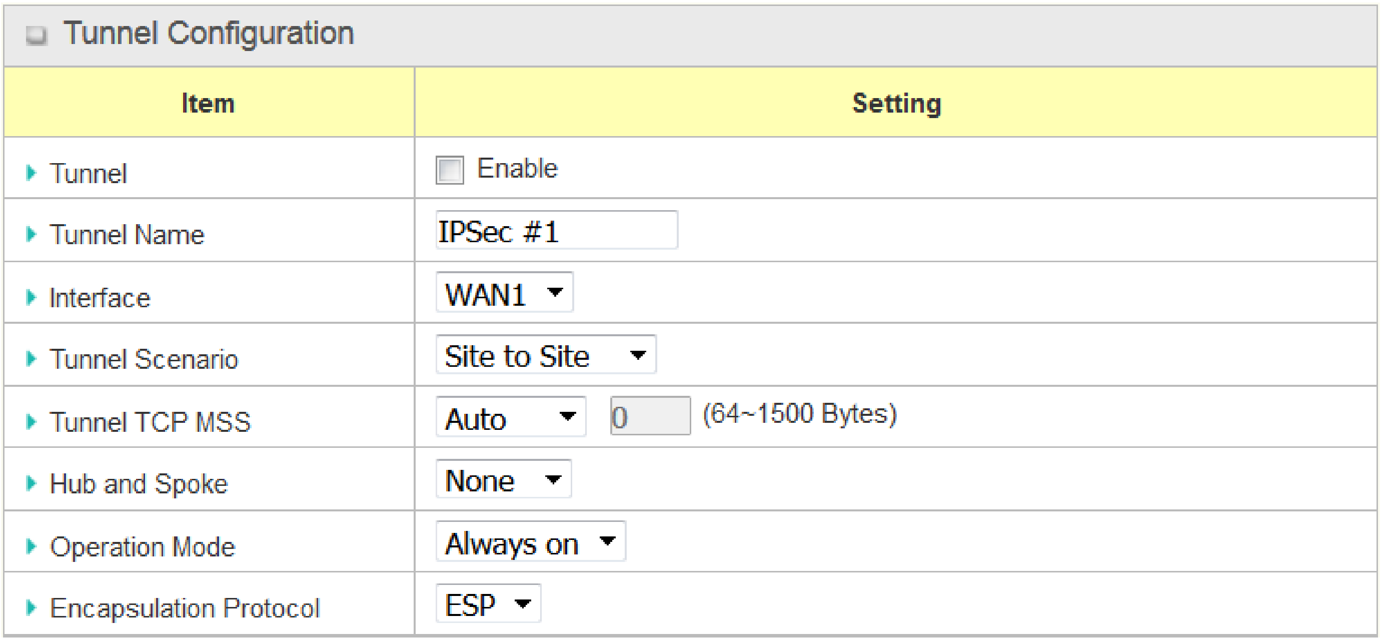
Ensure that the IPSec enable box is checked to enable before further configuring the IPSec tunnel settings.



IPSec Tunnel List

ID	Tunnel Name	Interface	Tunnel Scenario	Remote Gateway	Remote Subnet	Status	Enable	Actions

When **Add/Edit** button is applied, a series of configuration screens will appear. They are Tunnel Configuration, Local & Remote Configuration, Authentication, IKE Phase, IKE Proposal Definition, IPSec Phase, and IPSec Proposal Definition. You have to configure the tunnel details for both local and remote VPN devices.

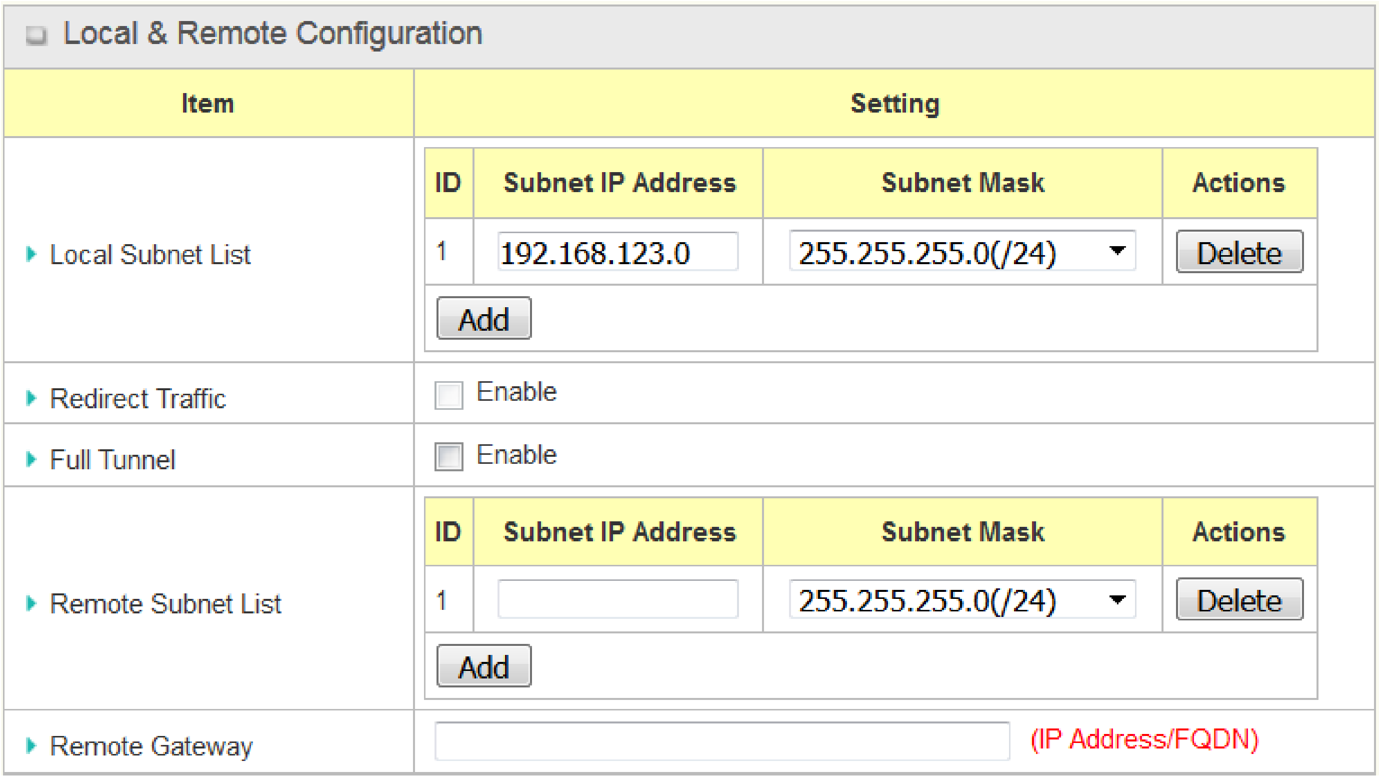


Tunnel Configuration

Item	Setting
Tunnel	□ Enable
Tunnel Name	IPSec #1
Interface	WAN1
Tunnel Scenario	Site to Site
Tunnel TCP MSS	Auto 0 (64~1500 Bytes)
Hub and Spoke	None
Operation Mode	Always on
Encapsulation Protocol	ESP

Tunnel Configuration Window		
Item	**Value setting**	**Description**
Tunnel	Unchecked by default	Check the **Enable** box to activate the 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. ***Value Range***: 1 ~ 19 characters.
Interface	1. A Must fill setting 2. **WAN 1** is selected by default	Select the interface on which IPSec tunnel is to be established. It can be the available WAN and LAN interfaces.
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**. If LAN interface is selected, only **Host-to-Host** scenario is available. 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.
Tunnel TCP MSS	1. An optional setting 2. **Auto** is set by default	Select from the dropdown box to define the size of Tunnel TCP MSS. Select **Auto**, and all devices will adjust this parameter automatically. Select **Manual, and** specify an expected value for Tunnel TCP MSS. ***Value Range***: 64 ~ 1500 bytes.
Hub and Spoke	1. An optional setting 2. **None** is set by default	Select from the dropdown box to setup your router 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.

Operation Mode	1. A Must fill setting 2. **Always on** is selected by default	Define operation mode for the IPSec Tunnel. It can be **Always On**, or **Failover**. If this tunnel is set as a failover tunnel, you need to further select a primary tunnel from which to failover to. Note: **Failover** mode is not available for the gateway with single WAN.
Encapsulation Protocol	1. A Must fill setting 2. **ESP** is selected by default	Select the Encapsulation Protocol from the dropdown box for this IPSec tunnel. Available encapsulations are **ESP** and **AH**.



Local & Remote Configuration

Item	Setting
Local Subnet List	
Redirect Traffic	☐ Enable
Full Tunnel	☐ Enable
Remote Subnet List	
Remote Gateway	(IP Address/FQDN)

Local Subnet List

ID	Subnet IP Address	Subnet Mask	Actions
1	192.168.123.0	255.255.255.0(/24) ▾	Delete

Add

Remote Subnet List

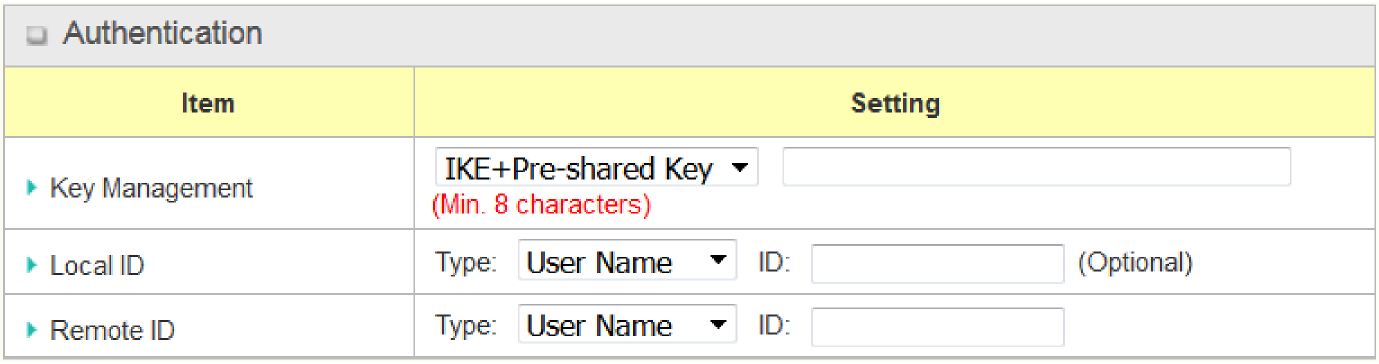
ID	Subnet IP Address	Subnet Mask	Actions
1		255.255.255.0(/24) ▾	Delete

Add

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 Host-to-Site or Host-to-Host option in Tunnel Scenario is selected, Local Subnet will not be available. Note_2: When Hub and Spoke option in Hub and Spoke is selected, there will be only one subnet available.
Redirect Traffic	Unchecked by default	Click **Enable** box to activate the Redirect Traffic function. Note: Redirect Traffic is available only for Host-to-Site specified in Tunnel Scenario. By default, it is disabled, so it can prevent the un-expected and dangerous access to the peer subnet. If you enable such function, all the network devices behind the VPN host (actually, it is an NAT router) can access to the peer subnet with the host IP.

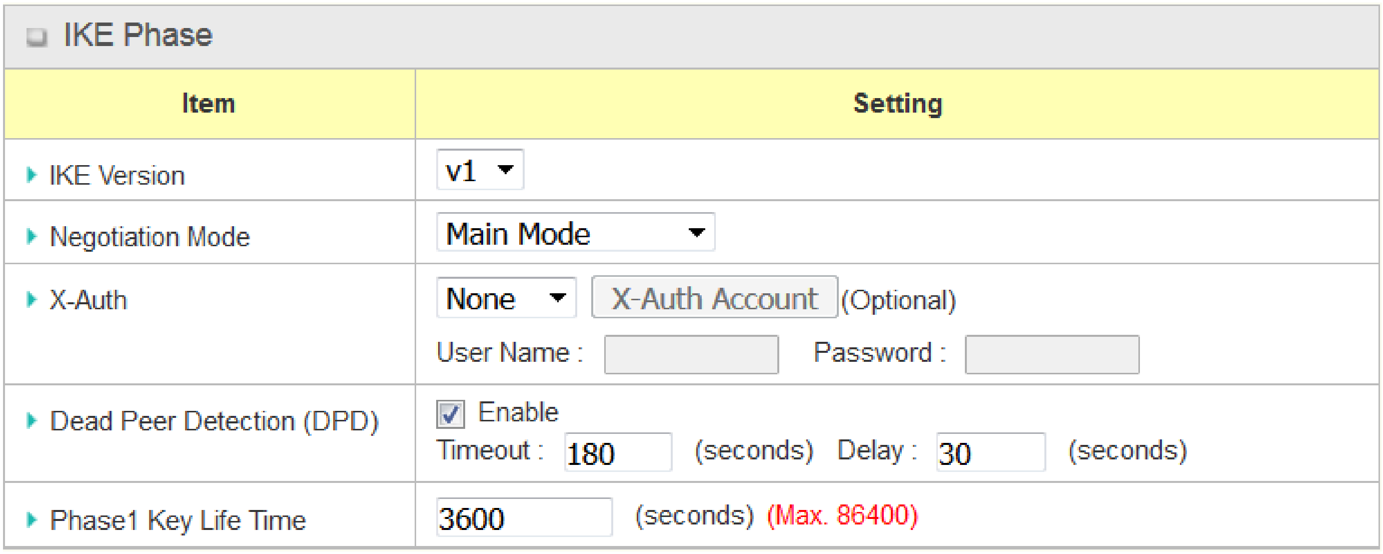
Full Tunnel	Unchecked by default	Click **Enable** box to enable Full Tunnel. Note: Full tunnel is available only for Site-to-Site specified in Tunnel Scenario.
Remote Subnet List	A Must fill setting	Specify the Remote Subnet IP address and Subnet Mask. Click the Add or Delete button to add or delete Remote Subnet setting.
Remote Gateway	1. A Must fill setting. 2. Format can be a ipv4 address or FQDN	Specify the Remote Gateway.



Authentication

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

Authentication Configuration Window		
Item	**Value setting**	**Description**
Key Management	1. A Must fill setting 2. Pre-shared Key 8 to 32 characters.	Select Key Management from the dropdown box for this IPSec tunnel. **IKE + Pre-shared Key:** user needs to set a key (8 ~ 32 characters). **IKE+X.509:** user needs Certificate to authenticate. IKE+X.509 will be available only when Certificate has been configured properly. Refer to Certificate section of this manual and also **Object Definition > Certificate** in web-based utility. **Manually:** user needs to enter key ID to authenticate. Manual key configuration will be explained in the following Manual Key Management section.
Local ID	An optional setting	Specify the Local ID for this IPSec tunnel to authenticate. Select **User Name** for Local ID and enter the username. The username may include but can't be all numbers. Select **FQDN** for Local ID and enter the FQDN. Select **User@FQDN** for Local ID and enter the User@FQDN. Select **Key ID** for Local ID and enter the Key ID (English alphabet or number).
Remote ID	An optional setting	Specify the Remote ID for this IPSec tunnel to authenticate. Select **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).

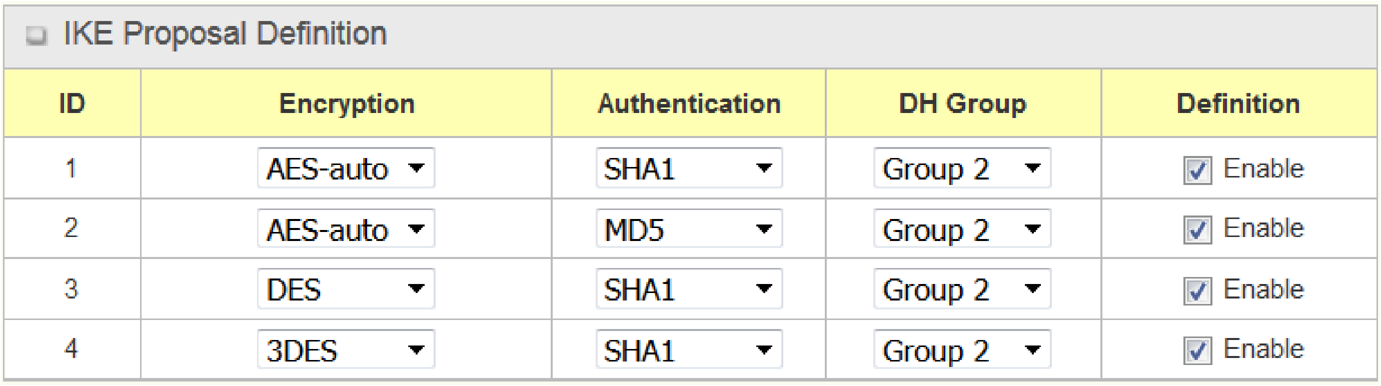


IKE Phase

Item	Setting
IKE Version	v1
Negotiation Mode	Main Mode
X-Auth	None X-Auth Account (Optional) User Name : Password :
Dead Peer Detection (DPD)	☑ Enable Timeout : 180 (seconds) Delay : 30 (seconds)
Phase1 Key Life Time	3600 (seconds) (Max. 86400)

IKE Phase Window

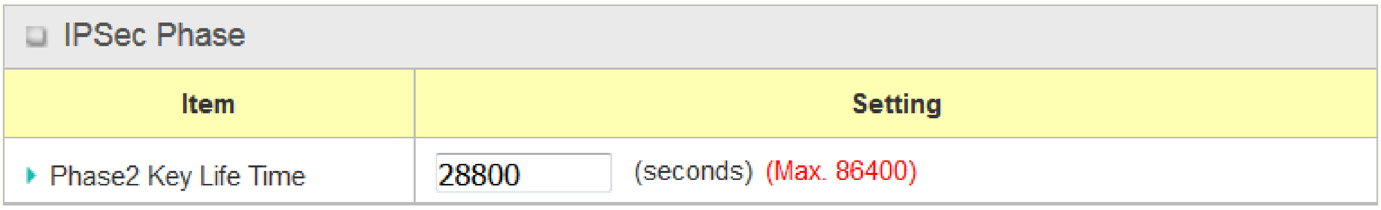
Item	Value setting	Description
IKE Version	1. A must fill setting 2. v1 is selected by default	Specify the IKE version for this IPSec tunnel. Select v1 or v2 Note: IKE versions will not be available when AH option in Encapsulation Protocol is selected.
Negotiation Mode	Main Mode is set by default	Specify 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 an X-Auth client. Enter User name and Password to be authenticated by the X-Auth server gateway.
Dead Peer Detection (DPD)	1. Checked by default 2. Default Timeout 180s and Delay 30s	Click **Enable** box to enable **DPD** function. Specify the **Timeout** and **Delay** time in seconds. ***Value Range***: 0 ~ 999 seconds for **Timeout** and **Delay**.
Phase1 Key Life Time	1. A Must fill setting 2. Default 3600s 3. Max. 86400s	Specify the Phase1 Key Life Time. ***Value Range***: 30 ~ 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

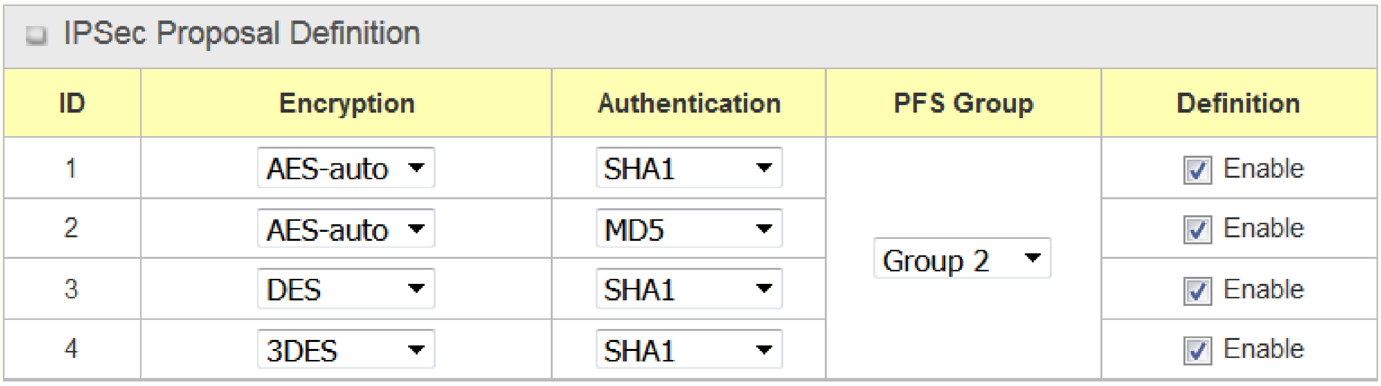
IKE Proposal Definition Window		
Item	**Value setting**	**Description**
IKE Proposal Definition	A Must fill setting	Specify the Phase 1 Encryption method. It can be DES / 3DES / AES-auto / AES-128 / AES-192 / AES-256. Specify the Authentication method. It can be None / MD5 / SHA1 / SHA2-256. Specify the DH Group. It can be None / Group1 / Group2 / Group5 / Group14 / Group15 / Group16 / Group17 / Group18. Check Enable box to enable this setting



IPSec Phase

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

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



IPSec Proposal Definition

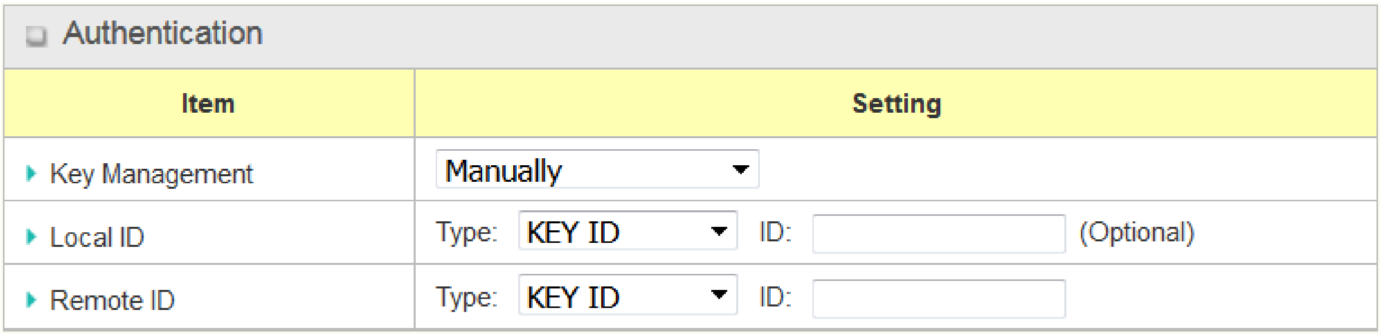
ID	Encryption	Authentication	PFS Group	Definition
1	AES-auto	SHA1	Group 2	☑ Enable
2	AES-auto	MD5		☑ Enable
3	DES	SHA1		☑ Enable
4	3DES	SHA1		☑ Enable

IPSec Proposal Definition Window

Item	Value setting	Description
IPSec Proposal Definition	A Must fill setting	Specify the Encryption method. It can be None / DES / 3DES / AES-auto / AES-128 / AES-192 / AES-256. Note: None is available only when Encapsulation Protocol is set as **AH**; it is not available for **ESP** Encapsulation. Specify the Authentication method. It can be None / MD5 / SHA1 / SHA2-256. Note: None and SHA2-256 are available only when Encapsulation Protocol is set as **ESP**; they are not available for **AH** Encapsulation. Specify the PFS Group. It can be 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** to cancel the settings
Back	N/A	Click **Back** to return to the previous page.

Manual Key Management

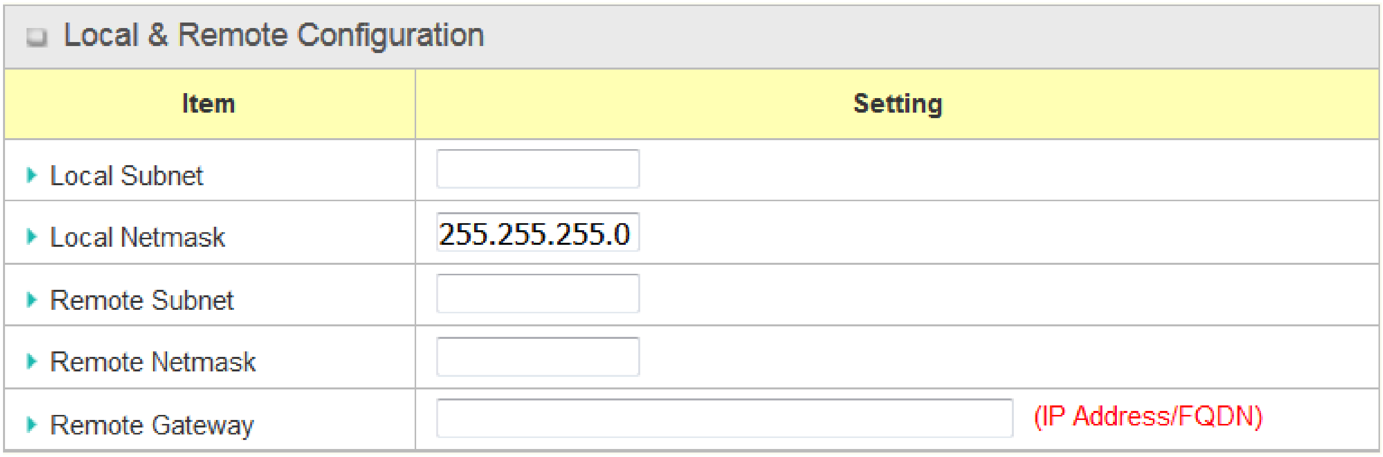
When the Manually option is selected for Key Management as described in Authentication Configuration Window, a series of configuration windows for Manual IPSec Tunnel configuration will appear. The configuration windows are the Local & Remote Configuration, the Authentication, and the Manual Proposal.



Authentication

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

Authentication 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.
Local ID	An optional setting	Specify the **Local ID** for this IPSec tunnel to authenticate. Select the **Key ID** for Local ID and enter the Key ID (English alphabet or number).
Remote ID	An optional setting	Specify the **Remote ID** for this IPSec tunnel to authenticate. Select **Key ID** for Remote ID and enter the Key ID (English alphabet or number).

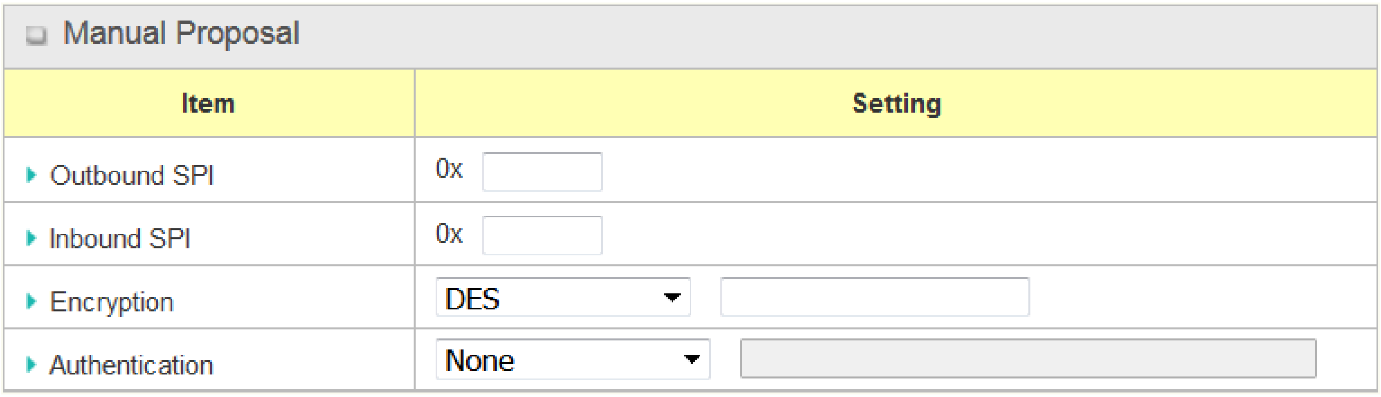


Local & Remote Configuration

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

Local & Remote Configuration Window		
Item	**Value setting**	**Description**
Local Subnet	A Must fill setting	Specify the Local Subnet IP address and Subnet Mask.
Local Netmask	A Must fill setting	Specify the Local Subnet Mask.
Remote Subnet	A Must fill setting	Specify the Remote Subnet IP address
Remote Netmask	A Must fill setting	Specify the Remote Subnet Mask.
Remote Gateway	1. A Must fill setting 2. An IPv4 address or FQDN format	Specify the Remote Gateway. The Remote Gateway

Under the Manually Key Management authentication configuration, only one subnet is supported for both Local and Remote IPSec peer.



Manual Proposal

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

Manual Proposal Window		
Item	**Value setting**	**Description**
Outbound SPI	Hexadecimal format	Specify the Outbound SPI for this IPSec tunnel. *Value Range*: 0 ~ FFFF.
Inbound SPI	Hexadecimal format	Specify the Inbound SPI for this IPSec tunnel. *Value Range*: 0 ~ FFFF.
Encryption	1. A Must fill setting 2. Hexadecimal format	Specify the Encryption Method and Encryption key. Available encryption methods are DES/3DES/AES-128/AES-192/AES-256. The key length for DES is 16, 3DES is 48, AES-128 is 32, AES-192 is 48, and AES-256 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. The key length for MD5 is 32, SHA1 is 40, and 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** to cancel the settings
Back	N/A	Click **Back** to return to the previous page.

4.1.2 OpenVPN

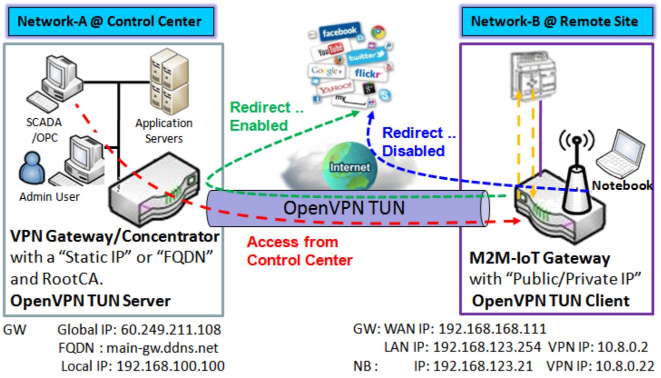
OpenVPN is an application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable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

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

OpenVPN Tunneling is a Client and Server based tunneling technology. The OpenVPN Server must have a Static IP or a FQDN, and maintain a Client list. The OpenVPN Client may be a mobile user or mobile site with public IP or private IP, and requesting the OpenVPN tunnel connection. The product can only behave as an OpenVPN Client role for an OpenVPN tunnel connection.

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

OpenVPN TUN Scenario

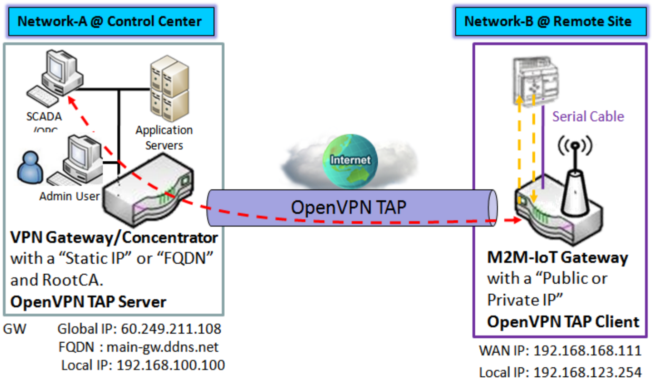

Network-A @ Control Center
Network-B @ Remote Site
SCADA /OPC
Application Servers
Admin User
Redirect .. Enabled
Redirect .. Disabled
Internet
OpenVPN TUN
Notebook
VPN Gateway/Concentrator with a "Static IP" or "FQDN" and RootCA.
OpenVPN TUN Server
Access from Control Center
M2M-IoT Gateway with "Public/Private IP"
OpenVPN TUN Client
GW Global IP: 60.249.211.108
FQDN : main-gw.ddns.net
Local IP: 192.168.100.100
GW: WAN IP: 192.168.168.111
LAN IP: 192.168.123.254 VPN IP: 10.8.0.2
NB : IP: 192.168.123.21 VPN IP: 10.8.0.22

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

The term "TUN" mode is referred to routing mode and operates with layer 3 packets. In routing mode, the VPN client is given an IP address on a different subnet than the local LAN under the OpenVPN server. This virtual subnet is created for connecting to any remote VPN computers. In routing mode, the OpenVPN server creates a "TUN" interface with its own IP address pool which is different to the local LAN. Remote hosts that dial-in will get an IP address inside the virtual network and will have access only to the server where OpenVPN resides. If you want to offer remote access to a VPN server from client(s), and inhibit the access to remote LAN resources under VPN server, OpenVPN TUN mode is the simplest solution.

As shown in the diagram, the M2M-IoT Gateway is configured as an OpenVPN TUN Client, and connects to an OpenVPN UN Server. Once the OpenVPN TUN connection is established, the connected TUN client will be assigned a virtual IP (10.8.0.2) which is belong to a virtual subnet that is different to the local subnet in Control Center. With such connection, the local networked devices will get a virtual IP 10.8.0.x if its traffic goes through the OpenVPN TUN connection when Redirect Internet Traffic settings is enabled; Besides, the SCADA Server in Control Center can access remote attached serial device(s) with the virtual IP address (10.8.0.2).

OpenVPN TAP Scenario



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

The term "TAP" is referred to bridge mode and operates with layer 2 packets. In bridge mode, the VPN client is given an IP address on the same subnet as the LAN resided under the OpenVPN server. Under such configuration, the OpenVPN client can directly access to the resources in LAN. If you want to offer remote access to the entire remote LAN for VPN client(s), you have to setup OpenVPN in "TAP" bridge mode.

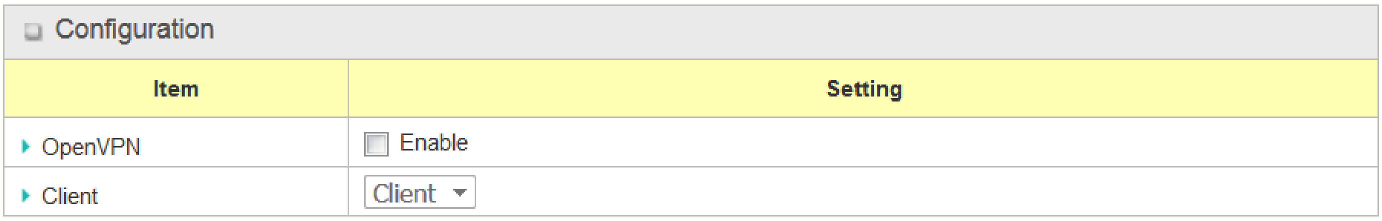
As shown in the diagram, the M2M-IoT Gateway is configured as an OpenVPN TAP Client, and connects to an OpenVPN TAP Server. Once the OpenVPN TAP connection is established, the connected TAP client will be assigned a virtual IP (192.168.100.210) which is the same subnet as that of local subnet in Control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

Open VPN Setting

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

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

Enable OpenVPN



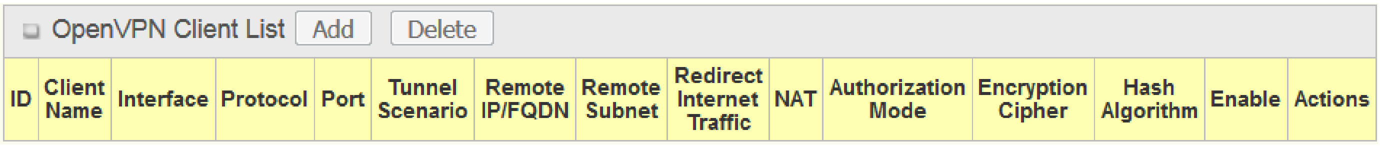
Configuration

Item	Setting
OpenVPN	□ Enable
Client	Client ▾

Configuration		
Item	**Value setting**	**Description**
OpenVPN	The box is unchecked by default	Check the **Enable** box to activate the OpenVPN function.
Client	**Client** is selected by default.	Only **Client** is available, you can specify the client settings in another client configuration window.

As an OpenVPN Client

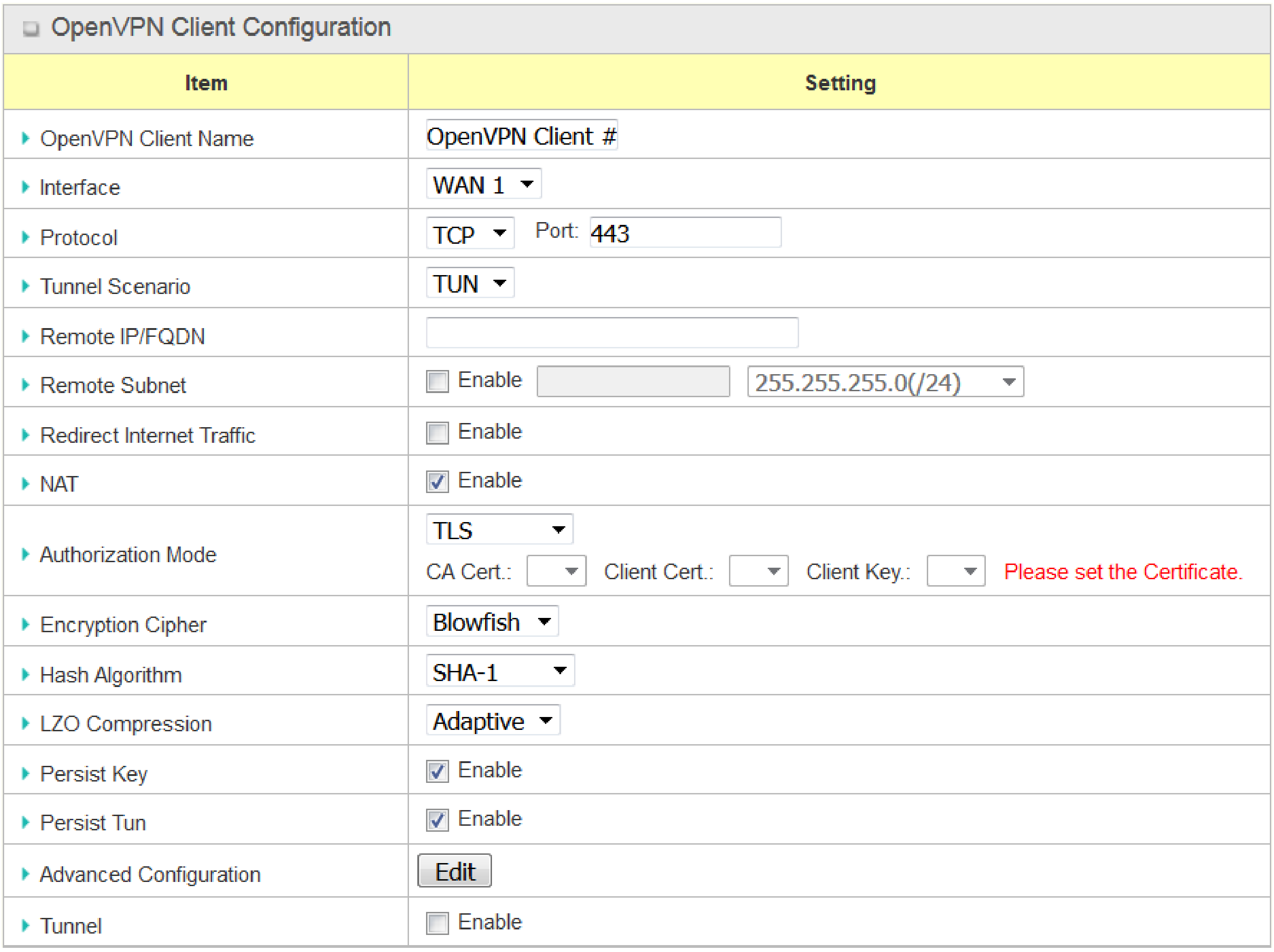
If **Client** is selected, an OpenVPN Client List screen will appear.



OpenVPN Client List Add Delete

ID	Client Name	Interface	Protocol	Port	Tunnel Scenario	Remote IP/FQDN	Remote Subnet	Redirect Internet Traffic	NAT	Authorization Mode	Encryption Cipher	Hash Algorithm	Enable	Actions

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



OpenVPN Client Configuration

Item	Setting
OpenVPN Client Name	OpenVPN Client #
Interface	WAN 1 ▾
Protocol	TCP ▾ Port: 443
Tunnel Scenario	TUN ▾
Remote IP/FQDN	
Remote Subnet	□ Enable 255.255.255.0(/24) ▾
Redirect Internet Traffic	□ Enable
NAT	☑ Enable
Authorization Mode	TLS ▾ CA Cert.: ▾ Client Cert.: ▾ Client Key.: ▾ Please set the Certificate.
Encryption Cipher	Blowfish ▾
Hash Algorithm	SHA-1 ▾
LZO Compression	Adaptive ▾
Persist Key	☑ Enable
Persist Tun	☑ Enable
Advanced Configuration	Edit
Tunnel	□ Enable

OpenVPN Client Configuration

Item	Value setting	Description
OpenVPN Client Name	A Must filled setting	The **OpenVPN Client Name** will be used to identify the client in the tunnel list. ***Value Range***: 1 ~ 32 characters.
Interface	1. A Must filled setting 2. By default **WAN-1** is selected.	Define the physical interface to be used for this OpenVPN Client tunnel.
Protocol	1. A Must filled setting 2. By default **TCP** is selected.	Define the **Protocol** for the OpenVPN Client. • Select **TCP** ->The OpenVPN will use TCP protocol, and **Port** will be set as 443 automatically. • Select **UDP** -> The OpenVPN will use UDP protocol, and **Port** will be set as 1194 automatically.
Port	1. A Must filled setting 2. By default **443** is set.	Specify the **Port** for the OpenVPN Client to use. ***Value Range***: 1 ~ 65535.

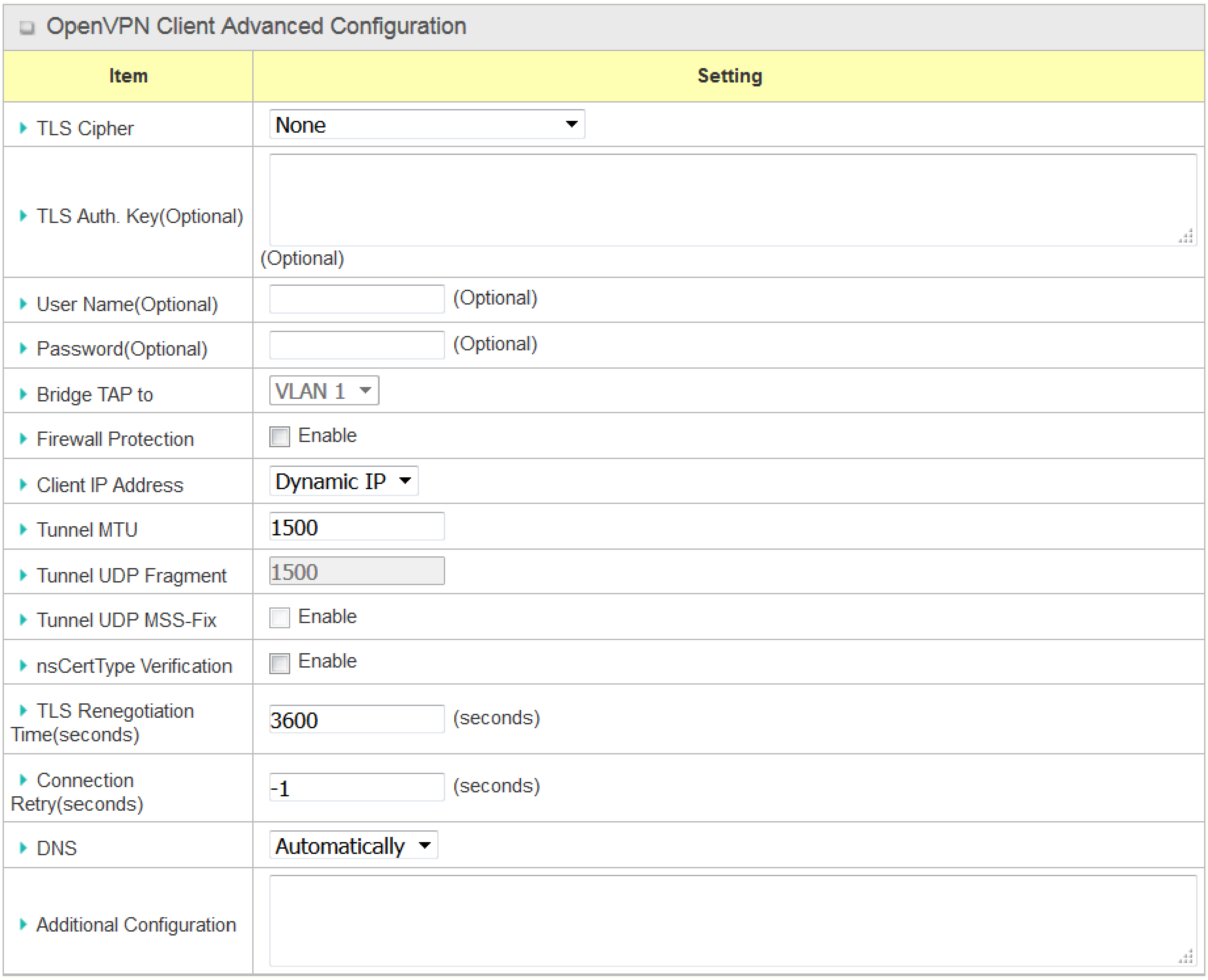
Tunnel Scenario	1. A Must filled setting 2. By default **TUN** is selected.	Specify the type of **Tunnel Scenario** for the OpenVPN Client to use. It can be **TUN** for TUN tunnel scenario, or **TAP** for TAP tunnel scenario.
Remote IP/FQDN	A Must filled setting	Specify the **Remote IP/FQDN** of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the IP address or FQDN.
Remote Subnet	1. An Optional setting. 2. The box is unchecked by default.	Check the **Enable** box to activate remote subnet function, and specify **Remote Subnet** of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the remote subnet address and remote subnet mask.
Redirect Internet Traffic	1. An Optional setting. 2. The box is unchecked by default.	Check the **Enable** box to activate the **Redirect Internet Traffic** function.
NAT	1. An Optional setting. 2. The box is unchecked by default.	Check the **Enable** box to activate the **NAT** function.
Authorization Mode	1. A Must filled setting 2. By default **TLS** is selected.	Specify the authorization mode for the OpenVPN Server. • **TLS** ->The OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Client Cert.** and **Client Key** will be displayed. **CA Cert.** could be selected in Trusted CA Certificate List. Refer to **Object Definition** > **Certificate** > **Trusted Certificate**. **Client Cert.** could be selected in Local Certificate List. Refer to **Object Definition** > **Certificate** > **My Certificate**. **Client Key** could be selected in Trusted Client key List. Refer to **Object Definition** > **Certificate** > **Trusted Certificate**. • **Static Key** ->The OpenVPN will use static key authorization mode, and the following items **Local Endpoint IP Address**, **Remote Endpoint IP Address** and **Static Key** will be displayed.
Local Endpoint IP Address	A Must filled setting	Specify the virtual **Local Endpoint IP Address** of this OpenVPN gateway. ***Value Range*****:** The IP format is 10.8.0.x, the range of x is 1~254. Note: Local Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Remote Endpoint IP Address	A Must filled setting	Specify the virtual **Remote Endpoint IP Address** of the peer OpenVPN gateway. ***Value Range*****:** The IP format is 10.8.0.x, the range of x is 1~254. Note: Remote Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Static Key	A Must filled setting	Specify the **Static Key**. Note: Static Key will be available only when Static Key is chosen in Authorization Mode.
Encryption Cipher	By default **Blowfish** is selected.	Specify the **Encryption Cipher.** It can be **Blowfish/AES-256/AES-192/AES-128/None.**

Hash Algorithm	By default **SHA-1** is selected.	Specify the **Hash Algorithm.** It can be **SHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable.**
LZO Compression	By default **Adaptive** is selected.	Specify the **LZO Compression** scheme. It can be **Adaptive/YES/NO/Default.**
Persis Key	1. An Optional setting. 2. The box is checked by default.	Check the **Enable** box to activate the **Persis Key** function.
Persis Tun	1. An Optional setting. 2. The box is checked by default.	Check the **Enable** box to activate the **Persis Tun** function.
Advanced Configuration	N/A	Click the **Edit** button to specify the **Advanced Configuration** setting for the OpenVPN server. If the button is clicked, **Advanced Configuration** will be displayed below.
Tunnel	The box is unchecked by default	Check the **Enable** box to activate this OpenVPN tunnel.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **Undo** to cancel the changes.
Back	N/A	Click **Back** to return to last page.

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

OpenVPN Advanced Client Configuration		
Item	**Value setting**	**Description**
TLS Cipher	1. A Must filled setting. 2. **TLS-RSA-WITH-AES128-SHA** is selected by default	Specify the **TLS Cipher** from the dropdown list. It can be **None / TLS-RSA-WITH-RC4-MD5 / TLS-RSA-WITH-AES128-SHA / TLS-RSA-WITH-AES256-SHA / TLS-DHE-DSS-AES128-SHA / TLS-DHE-DSS-AES256-SHA.** Note: TLS Cipher will be available only when TLS is chosen in Authorization Mode.
TLS Auth. Key	1. An Optional setting. 2. String format: any text	Specify the **TLS Auth. Key** for connecting to an OpenVPN server, if the server required it. Note: TLS Auth. Key will be available only when TLS is chosen in Authorization Mode.
User Name	An Optional setting.	Enter the **User account** for connecting to an OpenVPN server, if the server required it. Note: User Name will be available only when TLS is chosen in Authorization Mode.
Password	An Optional setting.	Enter the **Password** for connecting to an OpenVPN server, if the server required it. Note: User Name will be available only when TLS is chosen in Authorization Mode.
Bridge TAP to	By default **VLAN 1** is selected	Specify the setting of "**Bridge TAP to**" to bridge the TAP interface to a certain local network interface or VLAN. Note: Bridge TAP to will be available only when TAP is chosen in Tunnel Scenario and NAT is unchecked.
Firewall Protection	The box is unchecked by default.	Check the box to activate the **Firewall Protection** function. Note: Firewall Protection will be available only when NAT is enabled.
Client IP Address	By default **Dynamic IP** is selected	Specify the virtual IP Address for the OpenVPN Client. It can be **Dynamic IP/Static IP.**
Tunnel MTU	1.A Must filled setting 2.The value is 1500 by default	Specify the value of **Tunnel MTU.** ***Value Range***: 0 ~ 1500.
Tunnel UDP Fragment	The value is 1500 by default	Specify the value of **Tunnel UDP Fragment.** ***Value Range***: 0 ~ 1500. Note: Tunnel UDP Fragment will be available only when UDP is chosen in Protocol.
Tunnel UDP MSS-Fix	The box is unchecked by default.	Check the **Enable** box to activate the **Tunnel UDP MSS-Fix** function. Note: Tunnel UDP MSS-Fix will be available only when UDP is chosen in Protocol.
nsCerType Verification	The box is unchecked by default.	Check the **Enable** box to activate the **nsCerType Verification** function. Note: nsCerType Verification will be available only when TLS is chosen in Authorization Mode.
TLS Renegotiation Time (seconds)	The value is 3600 by default	Specify the time interval of **TLS Renegotiation Time.** ***Value Range***: -1 ~ 86400.
Connection Retry(seconds)	The value is -1 by default	Specify the time interval of **Connection Retry.** The default -1 means that it is no need to execute connection retry. ***Value Range***: -1 ~ 86400, and -1 means no retry is required.

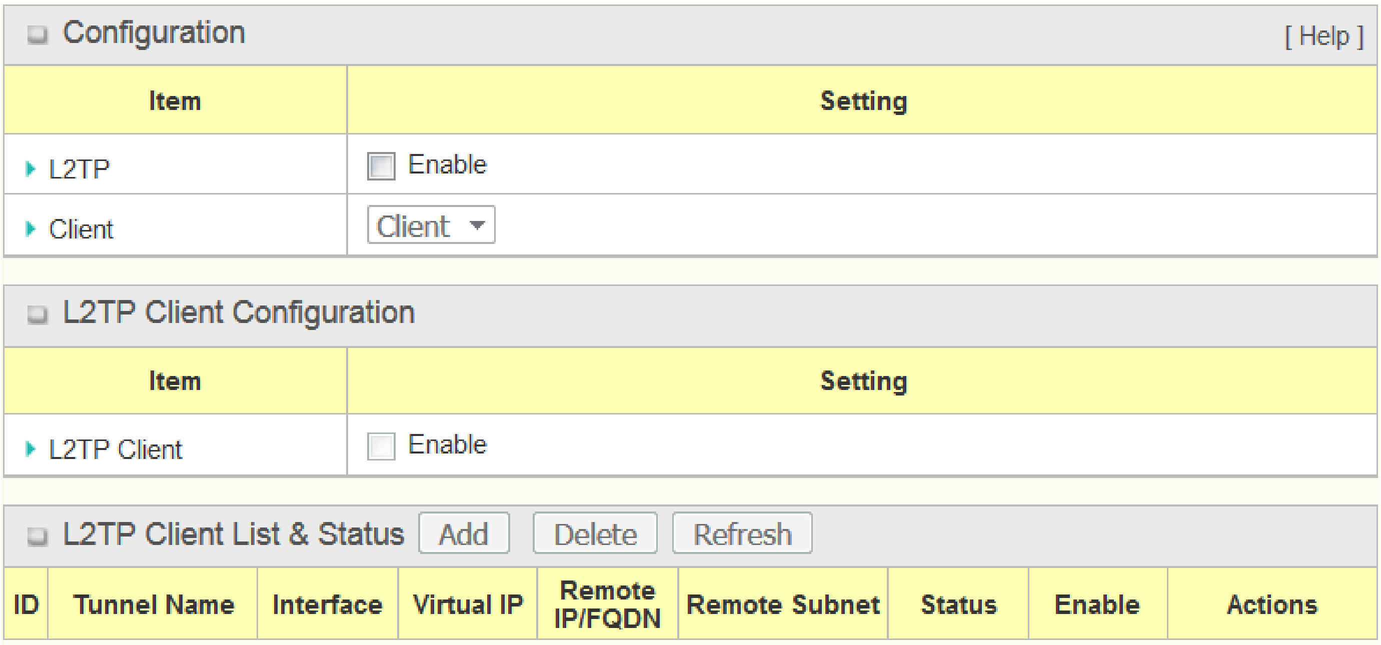
DNS	By default **Automatically** is selected	Specify the setting of **DNS.** It can be **Automatically/Manually.**
Additional Configuration	An Optional setting.	Enter optional configuration string here. Up to 256 characters is allowable. ***Value Range***: 0 ~ 256characters.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **Undo** to cancel the changes.
Back	N/A	Click **Back** to return to last page.



OpenVPN Client Advanced Configuration

Item	Setting
TLS Cipher	None
TLS Auth. Key(Optional)	(Optional)
User Name(Optional)	(Optional)
Password(Optional)	(Optional)
Bridge TAP to	VLAN 1
Firewall Protection	□ Enable
Client IP Address	Dynamic IP
Tunnel MTU	1500
Tunnel UDP Fragment	1500
Tunnel UDP MSS-Fix	□ Enable
nsCertType Verification	□ Enable
TLS Renegotiation Time(seconds)	3600 (seconds)
Connection Retry(seconds)	-1 (seconds)
DNS	Automatically
Additional Configuration	

4.1.3 L2TP



Configuration [Help]

Item	Setting
L2TP	□ Enable
Client	Client ▾

L2TP Client Configuration

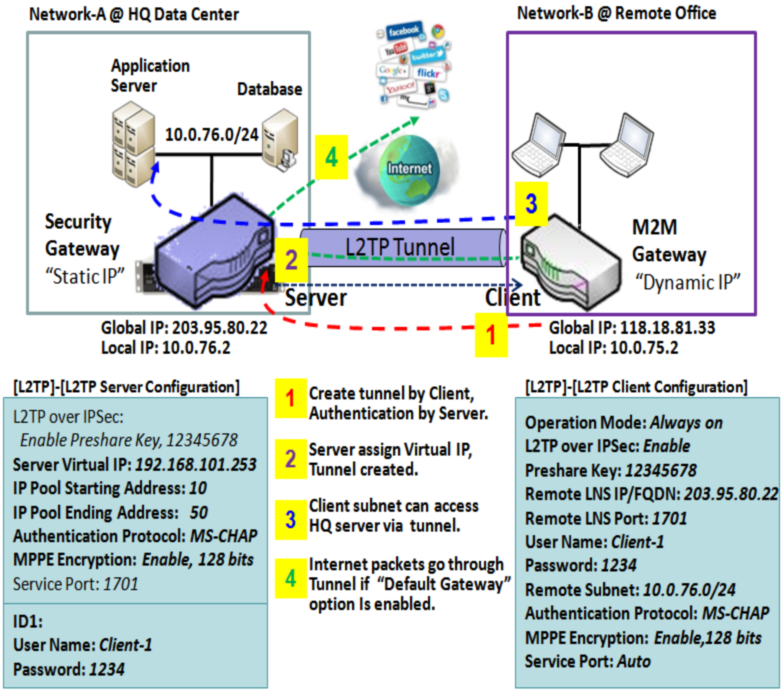
Item	Setting
L2TP Client	□ Enable

L2TP Client List & Status

ID	Tunnel Name	Interface	Virtual IP	Remote IP/FQDN	Remote Subnet	Status	Enable	Actions

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

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



[L2TP]-[L2TP Server Configuration]

L2TP over IPSec:
Enable Preshare Key, 12345678
Server Virtual IP: ***192.168.101.253***
IP Pool Starting Address: ***10***
IP Pool Ending Address: ***50***
Authentication Protocol: ***MS-CHAP***
MPPE Encryption: ***Enable, 128 bits***
Service Port: *1701*

ID1:
User Name: ***Client-1***
Password: ***1234***

1 Create tunnel by Client, Authentication by Server.

2 Server assign Virtual IP, Tunnel created.

3 Client subnet can access HQ server via tunnel.

4 Internet packets go through Tunnel if "Default Gateway" option Is enabled.

[L2TP]-[L2TP Client Configuration]

Operation Mode: ***Always on***
L2TP over IPSec: ***Enable***
Preshare Key: ***12345678***
Remote LNS IP/FQDN: ***203.95.80.22***
Remote LNS Port: ***1701***
User Name: ***Client-1***
Password: ***1234***
Remote Subnet: ***10.0.76.0/24***
Authentication Protocol: ***MS-CHAP***
MPPE Encryption: ***Enable,128 bits***
Service Port: ***Auto***

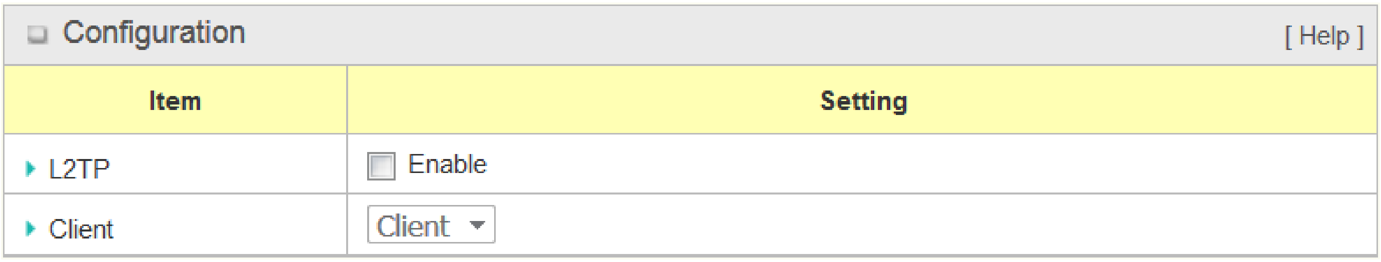
Besides, for the L2TP client peer, a Remote Subnet item is required. It is for the Intranet of L2TP server peer. So, at L2TP client peer, the packets whose destination is in the dedicated subnet will be transferred via the L2TP tunnel. Others will be transferred based on current routing policy of the gateway at L2TP client peer. But, if you entered 0.0.0.0/0 in the Remote Subnet field, it will be treated as a "Default Gateway" setting for the L2TP client peer, all packets, including the Internet accessing of L2TP client peer, will go through the established L2TP tunnel. That means the remote L2TP server peer controls the flow of any packets from the L2TP client peer. Certainly, those packets come through the L2TP tunnel.

L2TP Setting

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

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

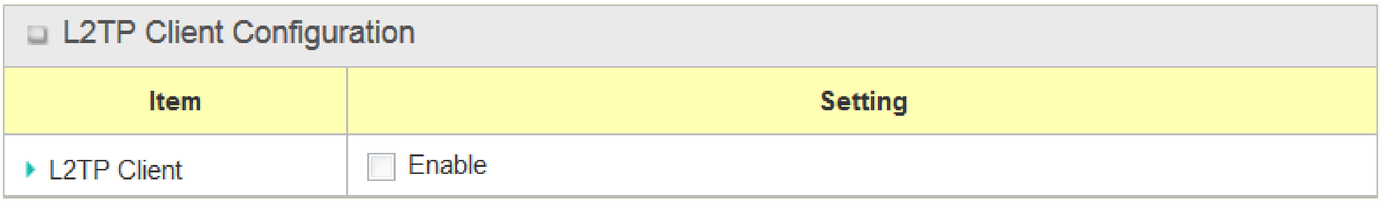
Enable L2TP



Item	Setting
L2TP	□ Enable
Client	Client ▾

Enable L2TP Window		
Item	**Value setting**	**Description**
L2TP	Unchecked by default	Click the **Enable** box to activate L2TP function.
Client	A Must filled setting	Specify the role of L2TP. Only **Client** role is available for this gateway. Below are the configuration windows for L2TP Client.
Save	N/A	Click **Save** button to save the settings

As a L2TP Client

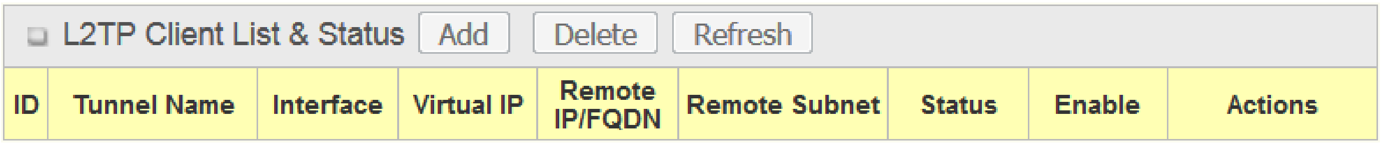


L2TP Client Configuration

Item	Setting
L2TP Client	□ Enable

L2TP Client Configuration		
Item Setting	**Value setting**	**Description**
L2TP Client	The box is unchecked by default	Check the **Enable** box to enable L2TP 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.

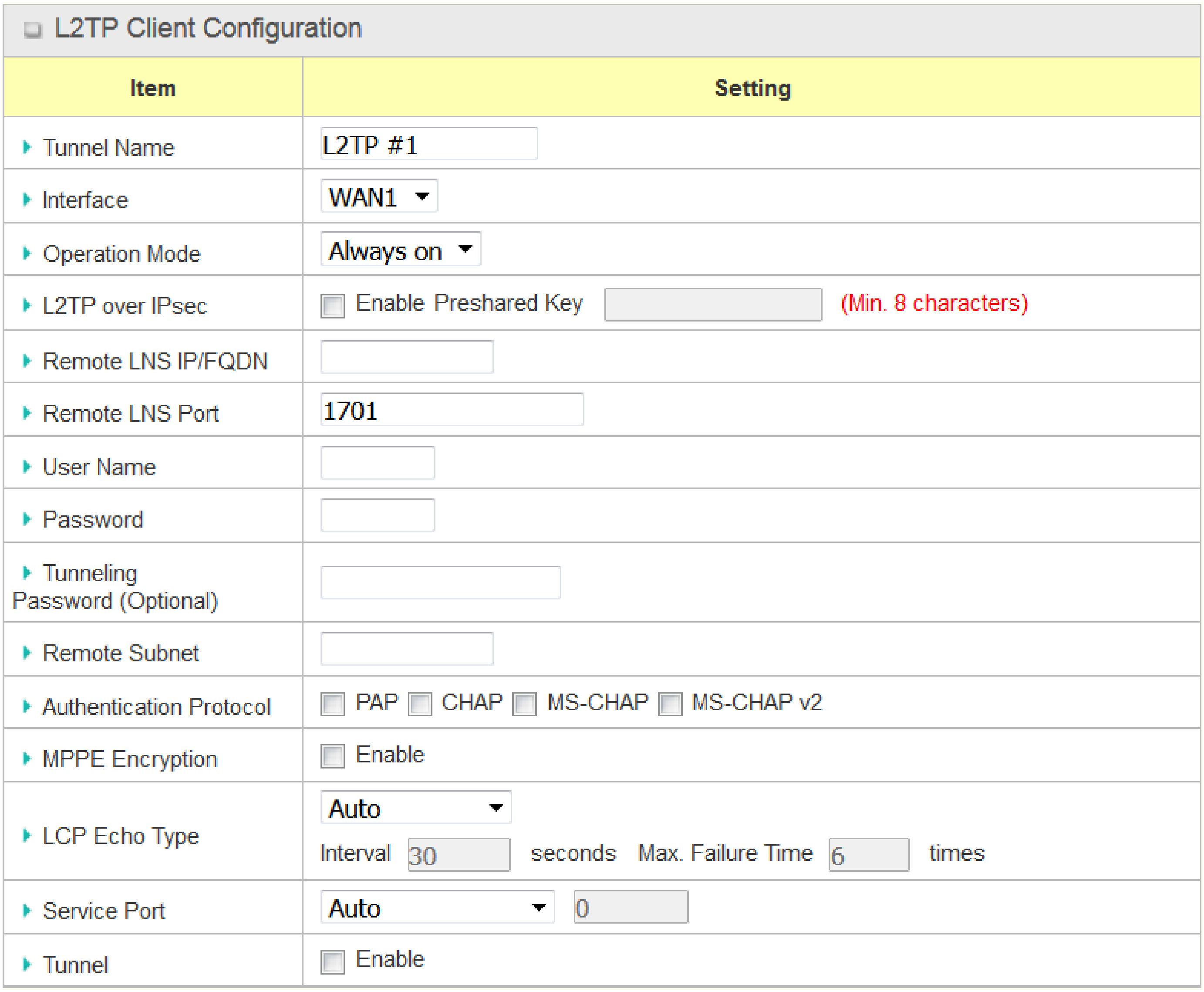
Create/Edit L2TP Client



L2TP Client List & Status

ID	Tunnel Name	Interface	Virtual IP	Remote IP/FQDN	Remote Subnet	Status	Enable	Actions

When **Add/Edit** button is applied, a series of configuration screen will appear. You can add up to 8 L2TP Clients.



L2TP Client Configuration

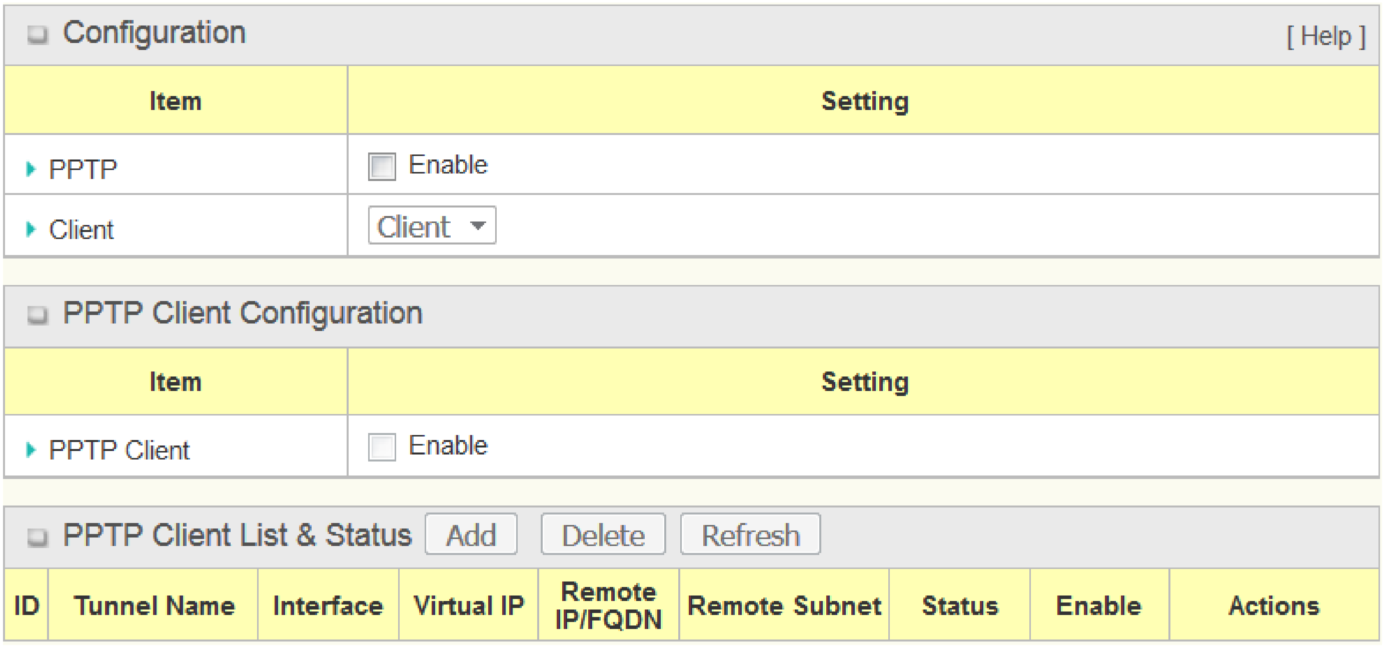
Item	Setting
Tunnel Name	L2TP #1
Interface	WAN1 ▾
Operation Mode	Always on ▾
L2TP over IPsec	□ Enable Preshared Key (Min. 8 characters)
Remote LNS IP/FQDN	
Remote LNS Port	1701
User Name	
Password	
Tunneling Password (Optional)	
Remote Subnet	
Authentication Protocol	□ PAP □ CHAP □ MS-CHAP □ MS-CHAP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

L2TP Client Configuration		
Item Setting	**Value setting**	**Description**
Tunnel Name	A Must filled setting	Enter a tunnel name. Enter a name that is easy for you to identify. ***Value Range***: 1 ~ 32 characters.
Interface	A Must filled setting	Define the selected interface to be the used for this L2TP tunnel (**WAN-1** is available only when WAN-1 interface is enabled) The same applies to other WAN interfaces (e.g. **WAN-2).**
Operation Mode	1. A Must filled setting 2. **Always on** is selected by default	Define operation mode for the L2TP Tunnel. It can be **Always On**, or **Failover**. If this tunnel is set as a failover tunnel, you need to further select a primary tunnel from which to failover to. Note: **Failover** mode is not available for the router with single WAN.
L2TP over IPSec	The box is unchecked by default	Check the **Enable** box to activate L2TP over IPSec, and further specify a Pre-shared Key (8 ~ 32 characters).
Remote LNS IP/FQDN	A Must filled setting	Enter the public IP address or the FQDN of the L2TP server.

Remote LNS Port	1. A Must filled setting 2. **1701** is set by default	Enter the Remote LNS Port for this L2TP tunnel. ***Value Range***: 1 ~ 65535.
User Name	A Must filled setting	Enter the **User Name** for this L2TP tunnel to be authenticated when connect to L2TP server. ***Value Range***: 1 ~ 32 characters.
Password	A Must filled setting	Enter the **Password** for this L2TP tunnel to be authenticated when connect to L2TP server.
Tunneling Password(Optional)	The box is unchecked by default	Enter the **Tunneling Password** for this L2TP tunnel to authenticate.
Remote Subnet	A Must filled setting	Specify the remote subnet for this L2TP tunnel to reach L2TP server. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24). It is for the Intranet of L2TP VPN server. So, at L2TP client peer, the packets whose destination is in the dedicated subnet will be transferred via the L2TP VPN tunnel. Others will be transferred based on current routing policy of the security gateway at L2TP client peer. If you entered 0.0.0.0/0 in the Remote Subnet field, it will be treated as a default gateway setting for the L2TP client peer, all packets, including the Internet accessing of L2TP Client peer, will go through the established L2TP VPN tunnel. That means the remote L2TP VPN server controls the flow of any packets from the L2TP client peer. Certainly, those packets come through the L2TP VPN tunnel.
Authentication Protocol	1. A Must filled setting 2. Unchecked by default	Specify one ore multiple **Authentication Protocol** for this L2TP tunnel. Available authentication methods are **PAP** / **CHAP** / **MS-CHAP** / **MS-CHAP v2**.
MPPE Encryption	1. Unchecked by default 2. an optional setting	Specify whether L2TP 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.
LCP Echo Type	1. Auto is set by default	Specify the LCP Echo Type for this L2TP tunnel. It can be **Auto**, **User-defined**, or **Disable**. **Auto**: the system sets the Interval and Max. Failure Time. **User-defined:** enter the Interval and Max. Failure Time. The default value for Interval is 30 seconds, and Maximum Failure Times is 6 Times. **Disable**: disable the LCP Echo. ***Value Range***: 1 ~ 99999 for Interval Time, 1~999 for Failure Time.
Service Port	A Must filled setting	Specify the **Service Port** for this L2TP tunnel to use. It can be **Auto**, **(1701) for Cisco)**, or **User-defined**. **Auto**: The system determines the service port. **1701 (for Cisco):** The system use port 1701 for connecting with CISCO L2TP Server. **User-defined:** Enter the service port. The default value is 0. ***Value Range***: 0 ~ 65535.

Tunnel	Unchecked by default	Check the **Enable** box to enable this L2TP tunnel.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.

4.1.4 PPTP



Configuration [Help]

Item	Setting
PPTP	□ Enable
Client	Client ▾

PPTP Client Configuration

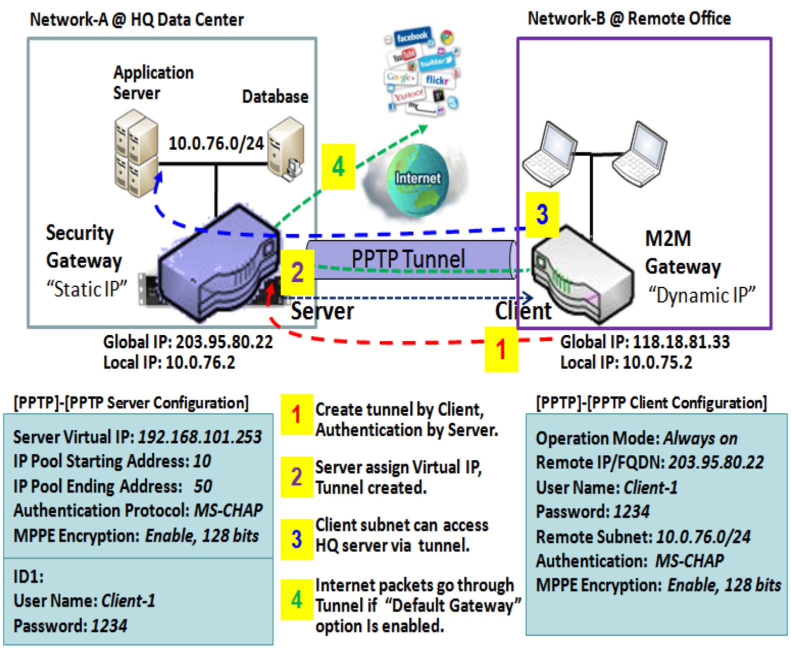
Item	Setting
PPTP Client	□ Enable

ID	Tunnel Name	Interface	Virtual IP	Remote IP/FQDN	Remote Subnet	Status	Enable	Actions

Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. It is a client-server based technology. There are various levels of authentication and encryption for PPTP tunneling, usually natively as standard features of the Windows PPTP stack. The security gateway can only play "PPTP Client" role for a PPTP VPN tunnel. PPTP tunnel process is nearly the same as L2TP.

PPTP Client: It can be mobile users or gateways in remote offices with dynamic IP. To setup tunnel, it should get “user name”, “password” and server’s global IP. In addition, it is required to identify the operation mode for each tunnel as main connection, failover for another tunnel to increase overall bandwidth. It needs to decide “Default Gateway” or “Remote Subnet” for packet flow. Moreover, you can also define what kind of traffics will pass through the PPTP tunnel in the “Default Gateway / Remote Subnet” parameter.

Besides, for the PPTP client peer, a Remote Subnet item is required. It is for the Intranet of PPTP server peer. So, at PPTP client peer, the packets whose destination is in the dedicated subnet will be transferred via the PPTP tunnel. Others will be transferred based on current routing policy of the gateway at PPTP client peer. But, if you entered 0.0.0.0/0 in the Remote Subnet field, it will be treated as a "Default Gateway" setting for the PPTP client peer, all packets, including the Internet accessing of PPTP client peer, will go through the established PPTP tunnel. That means the remote PPTP server peer controls the flow of any packets from the PPTP client peer. Certainly, those packets come through the PPTP tunnel.



[PPTP]-[PPTP Server Configuration]

Server Virtual IP: *192.168.101.253*
IP Pool Starting Address: *10*
IP Pool Ending Address: *50*
Authentication Protocol: *MS-CHAP*
MPPE Encryption: *Enable, 128 bits*

ID1:
User Name: *Client-1*
Password: *1234*

1 Create tunnel by Client, Authentication by Server.

2 Server assign Virtual IP, Tunnel created.

3 Client subnet can access HQ server via tunnel.

4 Internet packets go through Tunnel if "Default Gateway" option Is enabled.

[PPTP]-[PPTP Client Configuration]

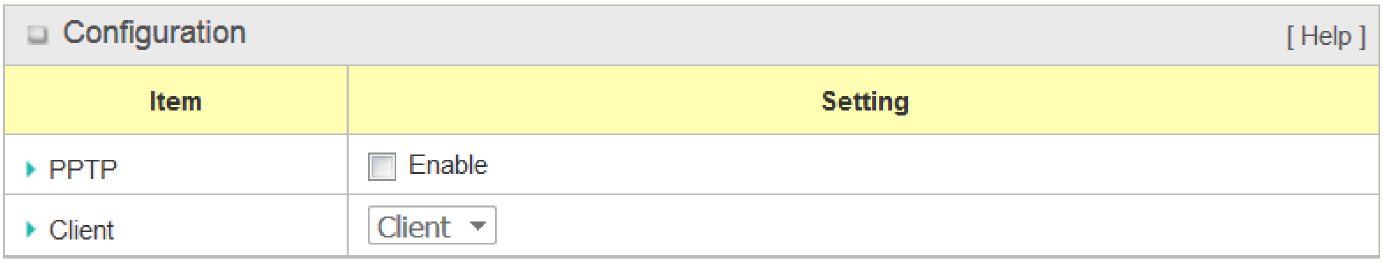
Operation Mode: *Always on*
Remote IP/FQDN: *203.95.80.22*
User Name: *Client-1*
Password: *1234*
Remote Subnet: *10.0.76.0/24*
Authentication: *MS-CHAP*
MPPE Encryption: *Enable, 128 bits*

PPTP Setting

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

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

Enable PPTP

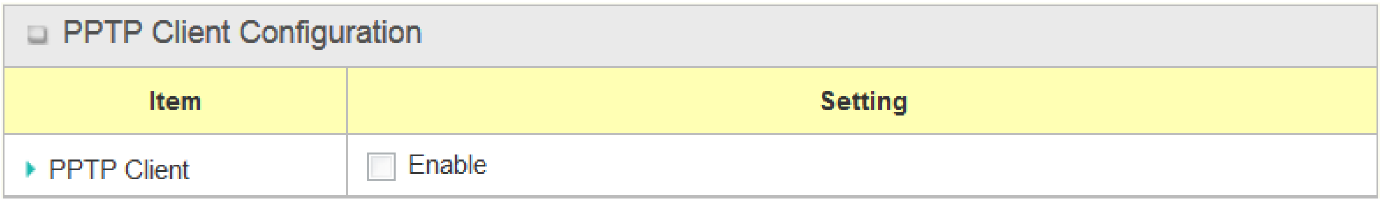


Configuration [Help]

Item	Setting
PPTP	□ Enable
Client	Client ▾

Enable PPTP Window		
Item	**Value setting**	**Description**
PPTP	Unchecked by default	Click the **Enable** box to activate PPTP function.
Client	A Must fill setting	Specify the role of PPTP. Only **Client** role is available for this router. Below are the configuration windows for PPTP Client.
Save	N/A	Click **Save** button to save the settings.

As a PPTP Client

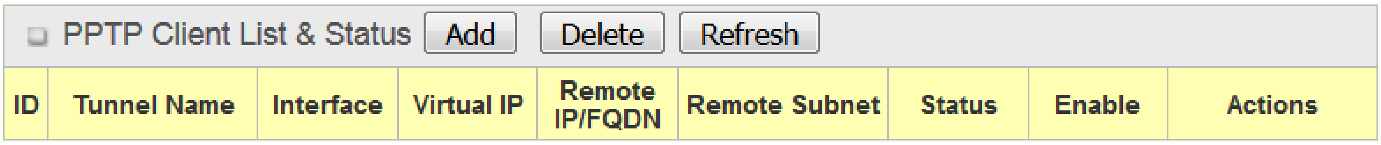


PPTP Client Configuration

Item	Setting
PPTP Client	□ Enable

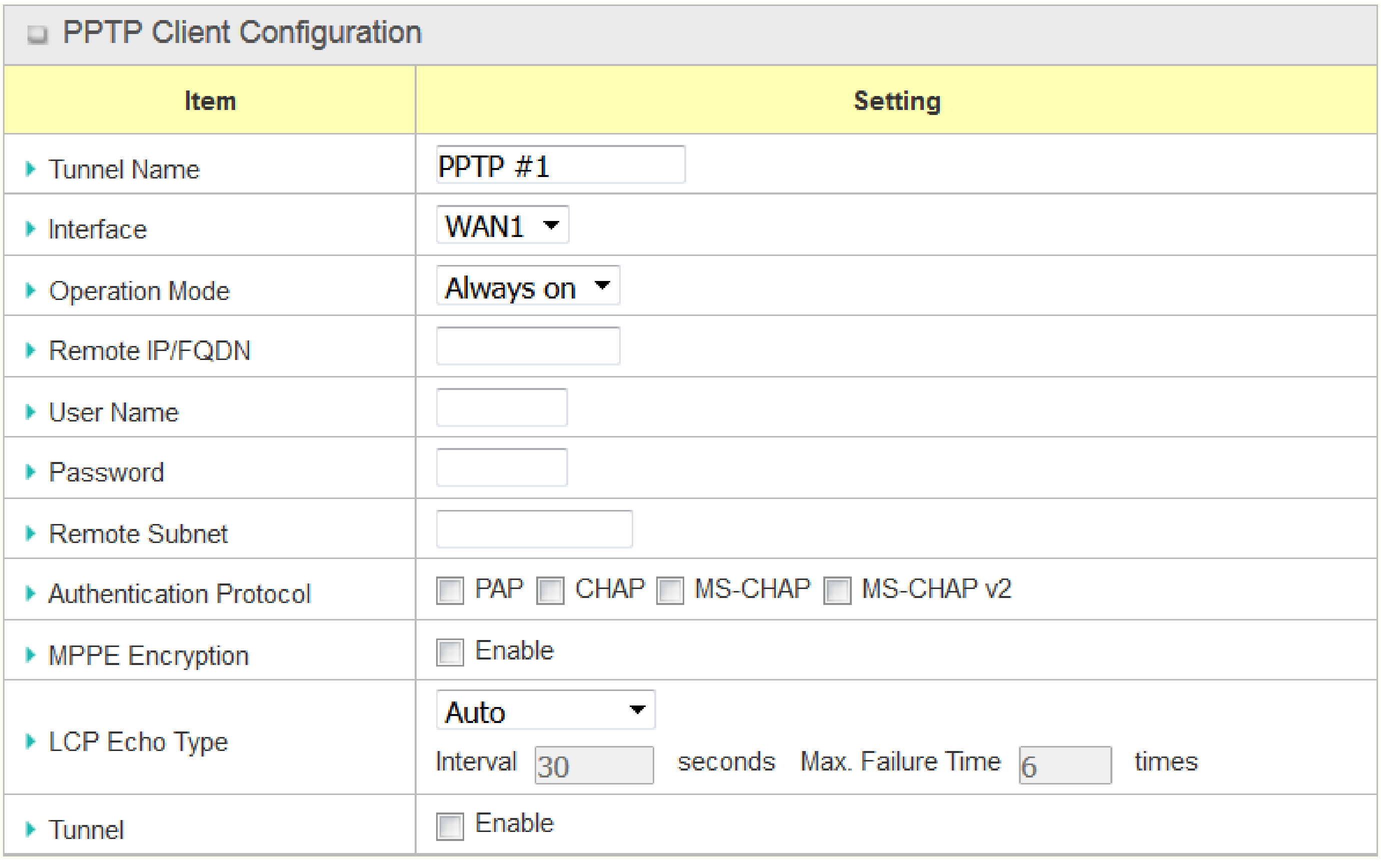
PPTP Client Configuration		
Item	**Value setting**	**Description**
PPTP Client	Unchecked by default	Check the **Enable** box to enable PPTP client role of the router.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.

Create/Edit PPTP Client



ID	Tunnel Name	Interface	Virtual IP	Remote IP/FQDN	Remote Subnet	Status	Enable	Actions

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



PPTP Client Configuration

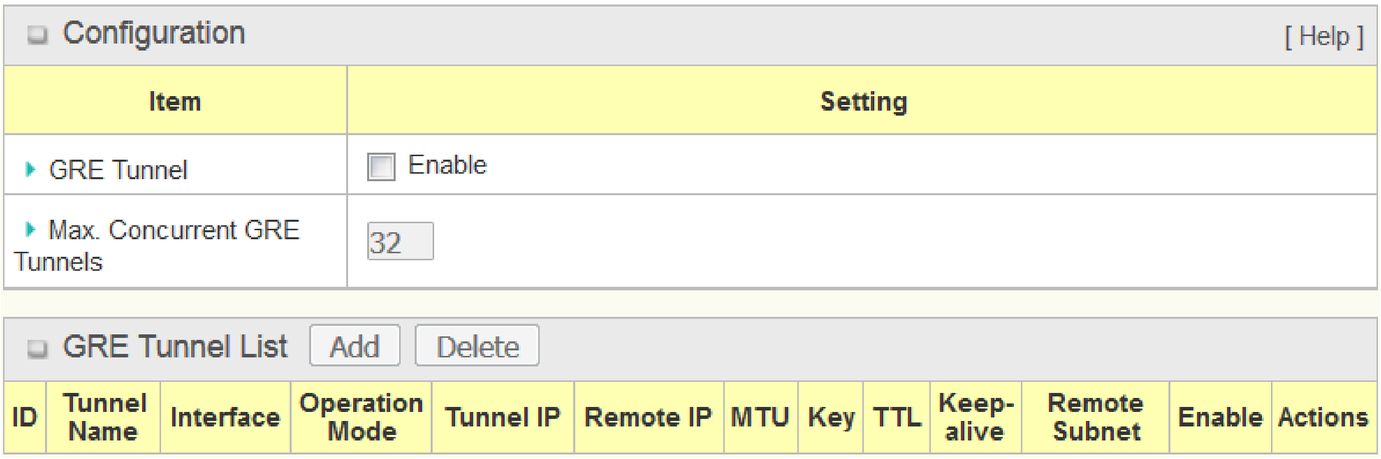
Item	Setting
Tunnel Name	PPTP #1
Interface	WAN1
Operation Mode	Always on
Remote IP/FQDN	
User Name	
Password	
Remote Subnet	
Authentication Protocol	□ PAP □ CHAP □ MS-CHAP □ MS-CHAP v2
MPPE Encryption	□ Enable
LCP Echo Type	Auto Interval 30 seconds Max. Failure Time 6 times
Tunnel	□ Enable

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. ***Value Range***: 1 ~ 32 characters.
Interface	1. A Must fill setting 2. WAN1 is selected by default	Define the selected interface to be the used for this PPTP tunnel (**WAN-1** is available only when WAN-1 interface is enabled) The same applies to other WAN interfaces (e.g. **WAN-2).**
Operation Mode	1. A Must fill setting 2. **Always on** is selected by default	Define operation mode for the PPTP Tunnel. It can be **Always On**, or **Failover**. If this tunnel is set as a failover tunnel, you need to further select a primary tunnel from which to failover to. Note: **Failover** mode is not available for the router with single WAN.
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.
User Name	A Must fill setting	Enter the **User Name** for this PPTP tunnel to be authenticated when connect to PPTP server. ***Value Range***: 1 ~ 32 characters.
Password	A Must fill setting	Enter the **Password** for this PPTP tunnel to be authenticated when connect to PPTP server.
Remote Subnet	A Must fill setting	Specify the remote subnet for this PPTP tunnel to reach PPTP server. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24). It is for the Intranet of PPTP VPN server. So, at PPTP client peer, the packets whose destination is in the dedicated subnet will be transferred via the PPTP VPN tunnel. Others will be transferred based on current routing policy of the security gateway at PPTP client peer. If you entered 0.0.0.0/0 in the Remote Subnet field, it will be treated as a default gateway setting for the PPTP client peer, all packets, including the Internet accessing of PPTP Client peer, will go through the established PPTP VPN tunnel. That means the remote PPTP VPN server controls the flow of any packets from the PPTP client peer. Certainly, those packets come through the PPTP VPN tunnel.
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-CHAP v2**.
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.
LCP Echo Type	Auto is set by default	Specify the LCP Echo Type for this PPTP tunnel. It can be **Auto**, **User-defined**, or **Disable**. **Auto**: the system sets the Interval and Max. Failure Time. **User-defined:** enter the Interval and Max. Failure Time. The default value for Interval is 30 seconds, and Maximum Failure Times is 6 Times. **Disable**: disable the LCP Echo. ***Value Range***: 1 ~ 99999 for Interval Time, 1~999 for Failure Time.

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.

4.1.5 GRE



Configuration [Help]

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

GRE Tunnel List Add Delete

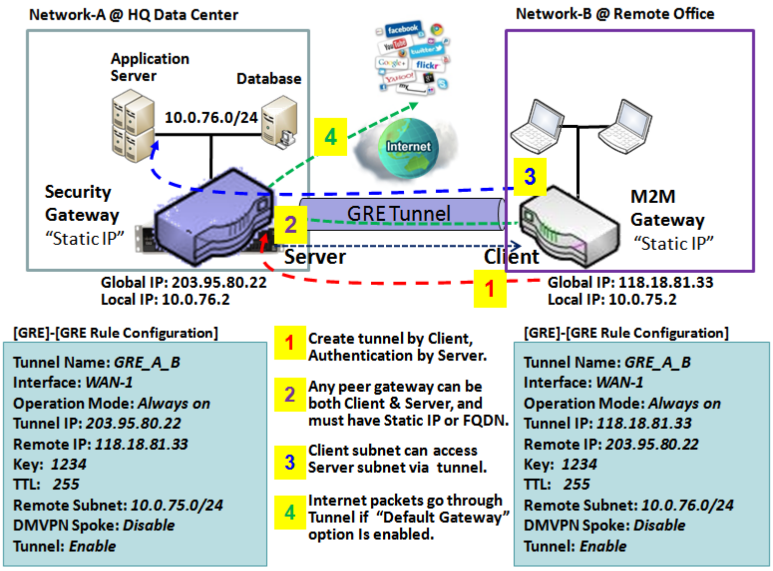
ID	Tunnel Name	Interface	Operation Mode	Tunnel IP	Remote IP	MTU	Key	TTL	Keep-alive	Remote Subnet	Enable	Actions

Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco Systems that encapsulates a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork.

Deploy an ICR-1601 router for remote site and establish a virtual private network with control center by using GRE tunneling. So, all client hosts behind ICR-1601 router can make data communication with server hosts behind control center router.

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 router can be worked as either a client or a server, even using the same set of configuration rule.

GRE Tunnel Scenario



[GRE]-[GRE Rule Configuration]

Tunnel Name: *GRE_A_B*
Interface: *WAN-1*
Operation Mode: *Always on*
Tunnel IP: *203.95.80.22*
Remote IP: *118.18.81.33*
Key: *1234*
TTL: *255*
Remote Subnet: *10.0.75.0/24*
DMVPN Spoke: *Disable*
Tunnel: *Enable*

1 Create tunnel by Client, Authentication by Server.

2 Any peer gateway can be both Client & Server, and must have Static IP or FQDN.

3 Client subnet can access Server subnet via tunnel.

4 Internet packets go through Tunnel if "Default Gateway" option Is enabled.

[GRE]-[GRE Rule Configuration]

Tunnel Name: *GRE_A_B*
Interface: *WAN-1*
Operation Mode: *Always on*
Tunnel IP: *118.18.81.33*
Remote IP: *203.95.80.22*
Key: *1234*
TTL: *255*
Remote Subnet: *10.0.76.0/24*
DMVPN Spoke: *Disable*
Tunnel: *Enable*

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

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

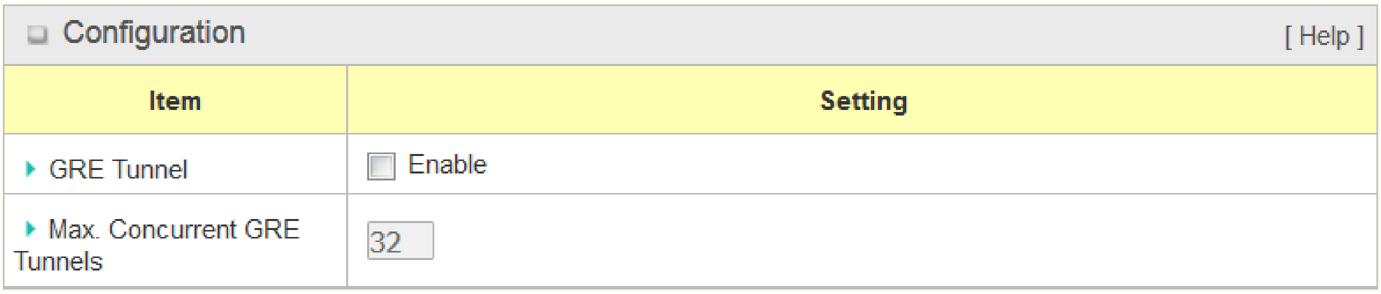
If the GRE server supports DMVPN Hub function, like Cisco router as the VPN concentrator, the GRE client can active the DMVPN spoke function here since it is implemented by GRE over IPSec tunneling.

GRE Setting

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

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

Enable GRE

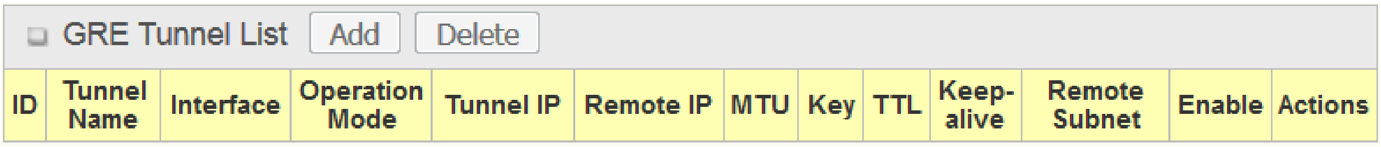


Item	Setting
GRE Tunnel	□ Enable
Max. Concurrent GRE Tunnels	32

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

Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

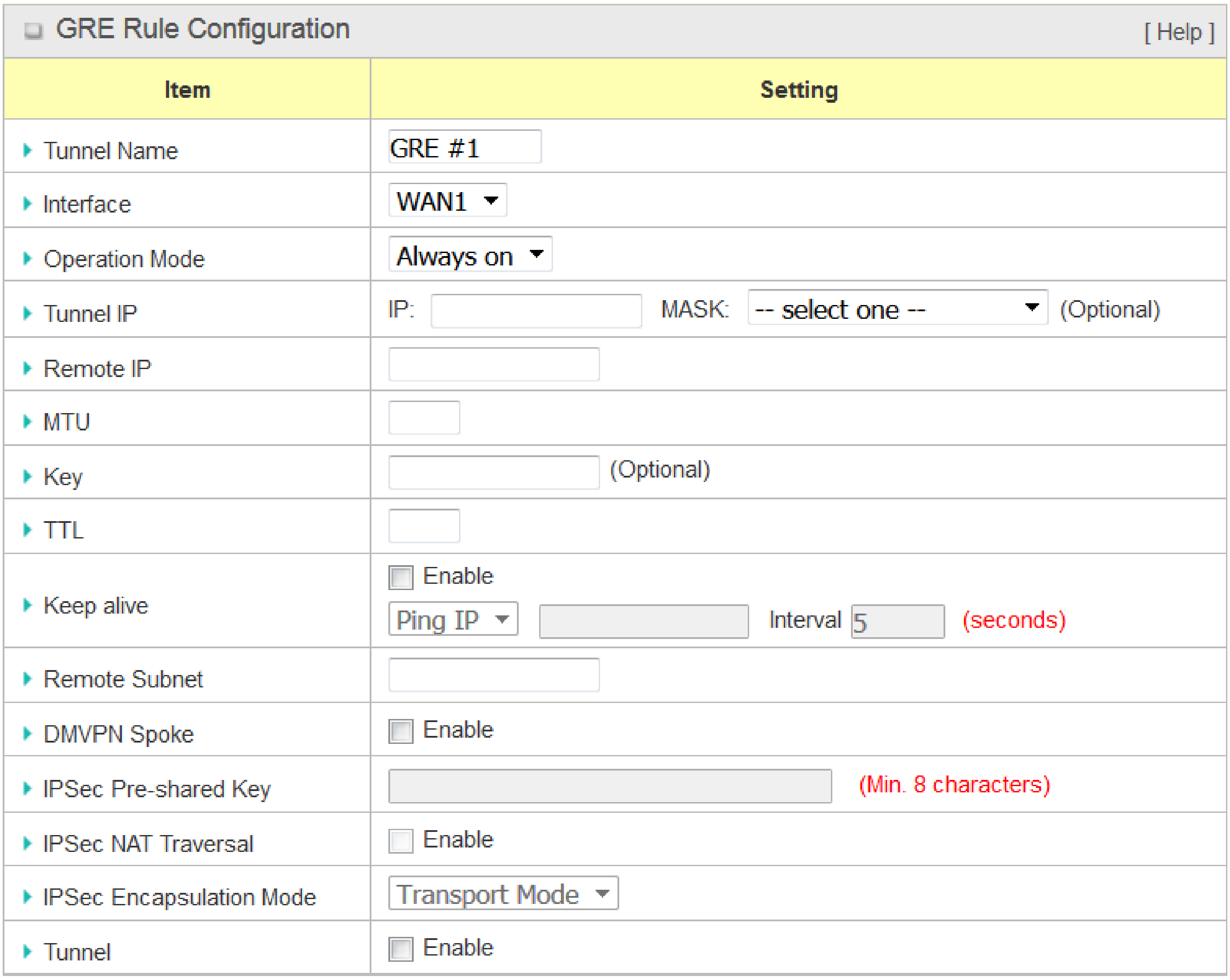
Create/Edit GRE tunnel



GRE Tunnel List [Add] [Delete]

ID	Tunnel Name	Interface	Operation Mode	Tunnel IP	Remote IP	MTU	Key	TTL	Keep-alive	Remote Subnet	Enable	Actions

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



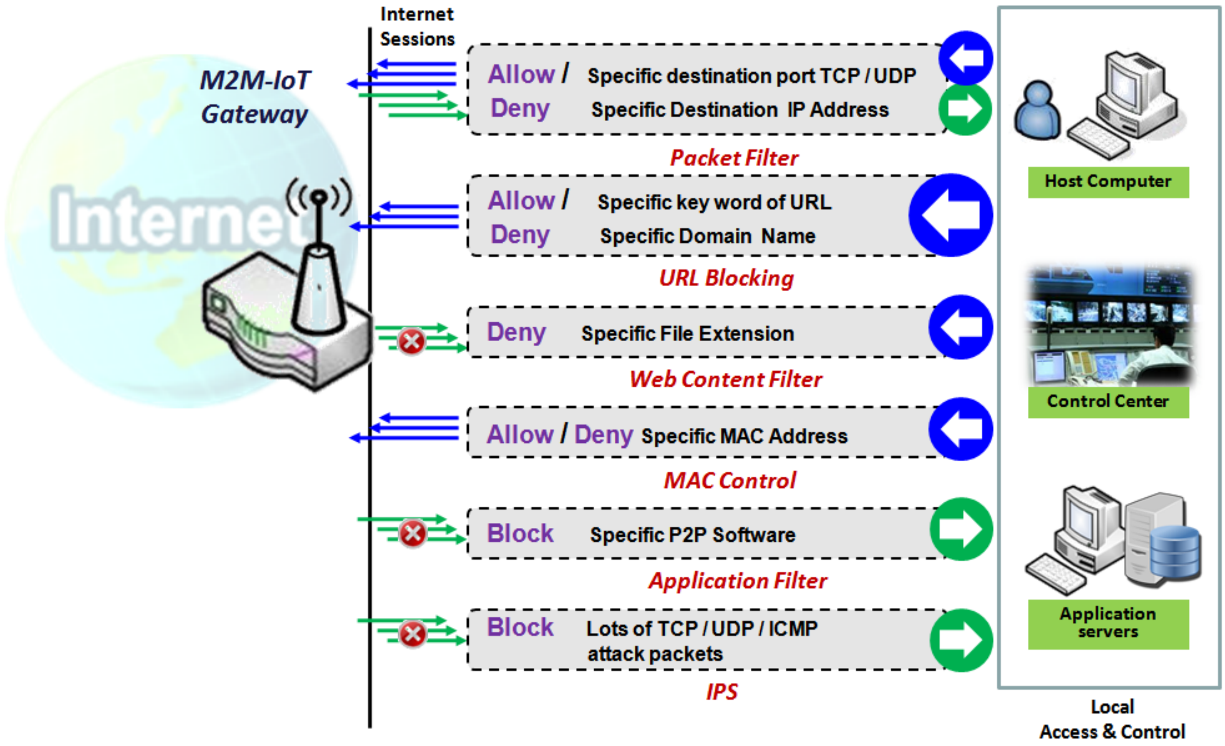
GRE Rule Configuration [Help]

Item	Setting
Tunnel Name	GRE #1
Interface	WAN1 ▾
Operation Mode	Always on ▾
Tunnel IP	IP: ______ MASK: -- select one -- ▾ (Optional)
Remote IP	
MTU	
Key	(Optional)
TTL	
Keep alive	□ Enable Ping IP ▾ ______ Interval 5 (seconds)
Remote Subnet	
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. ***Value Range***: 1 ~ 9 characters.
Interface	1. A Must fill setting 2. **WAN 1** is selected by default	Select the interface on which GRE tunnel is to be established. It can be the available WAN and LAN interfaces.
Operation Mode	1. A Must fill setting 2. **Always on** is selected by default	Define operation mode for the GRE Tunnel. It can be **Always On**, or **Failover**. If this tunnel is set as a failover tunnel, you need to further select a primary tunnel from which to failover to. Note: **Failover** mode is not available for the router with single WAN.
Tunnel IP	An Optional setting	Enter the Tunnel IP address and corresponding subnet mask.
Remote IP	A Must fill setting	Enter the Remote IP address of remote GRE tunnel gateway. Normally this is the public IP address of the remote GRE gateway.
MTU	1. A Must filled setting 2. **Auto** (value zero) is set by default	**MTU** refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. When set to **Auto** (value '0'), the router selects the best MTU for best Internet connection performance. ***Value Range***: 0 ~ 1500.
Key	An Optional setting	Enter the Key for the GRE connection. ***Value Range***: 0 ~ 9999999999.
TTL	1. A Must fill setting 2. 1 to 255 range	Specify **TTL** hop-count value for this GRE tunnel. ***Value Range***: 1 ~ 255.
Keep alive	1. Unchecked by default 2. 5s is set by default	Check the **Enable** box to enable Keep alive function. Select Ping IP to keep live and enter the IP address to ping. Enter the ping time interval in seconds. ***Value Range***: 5 ~ 999 seconds.
Remote Subnet	A Must fill setting	Specify the remote subnet for this GRE tunnel. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24). It is for the Intranet of GRE server peer. So, at GRE client peer, the packets whose destination is in the dedicated subnet will be transferred via the GRE tunnel. Others will be transferred based on current routing policy of the security gateway at GRE client peer. If you entered 0.0.0.0/0 in the Remote Subnet field, it will be treated as a default gateway setting for the GRE client peer, all packets, including the Internet accessing of GRE client peer, will go through the established GRE tunnel. That means the remote GRE server peer controls the flow of any packets from the GRE client peer. Certainly, those packets come through the GRE tunnel.
DMVPN Spoke	Unchecked by default	Specify whether the router will support DMVPN Spoke for this GRE tunnel. Check Enable box to enable DMVPN Spoke.
IPSec Pre-shared Key	A Must fill setting	Enter a DMVPN spoke authentication Pre-shared Key (8 ~ 32 characters). Note: Pre-shared Key is available only when DMVPN Spoke is enabled.
IPSec NAT Traversal	Unchecked by default	Check **Enable** box to enable NAT-Traversal. Note: IPSec NAT Traversal will not be available when DMVPN is not enabled.

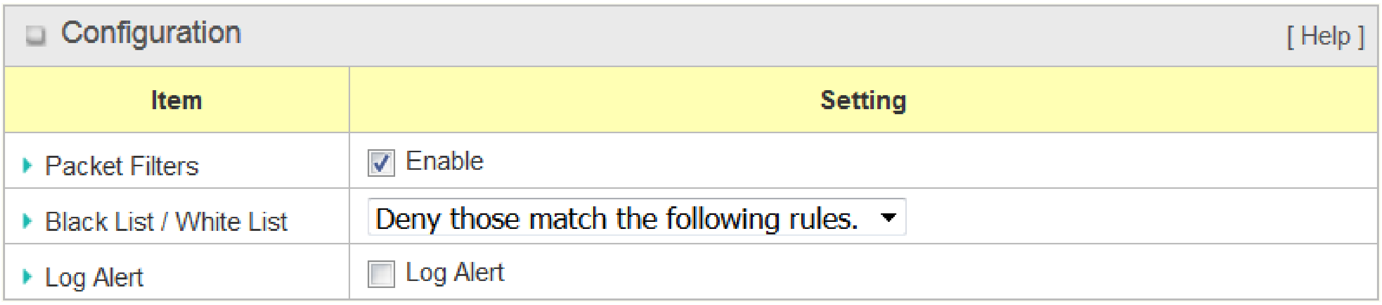
IPSec Encapsulation Mode	Unchecked by default	Specify IPSec Encapsulation Mode from the dropdown box. There are **Transport mode** and **Tunnel mode** supported. Note: IPSec Encapsulation Mode will not be available when DMVPN is not enabled.
Tunnel	Unchecked by default	Check **Enable** box to enable this GRE tunnel.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.
Back	N/A	Click **Back** button to return to the previous page.

4.2 Firewall


Internet Sessions
M2M-IoT Gateway
Internet
Allow / Deny Specific destination port TCP / UDP
Specific Destination IP Address
Packet Filter
Allow / Deny Specific key word of URL
Specific Domain Name
URL Blocking
Deny Specific File Extension
Web Content Filter
Allow / Deny Specific MAC Address
MAC Control
Block Specific P2P Software
Application Filter
Block Lots of TCP / UDP / ICMP attack packets
IPS
Host Computer
Control Center
Application servers
Local Access & Control

The firewall functions include Packet Filter, URL Blocking, Content Filter, MAC Control, Application Filter, IPS and some firewall options. The supported function can be different for the purchased router.

4.2.1 Packet Filter

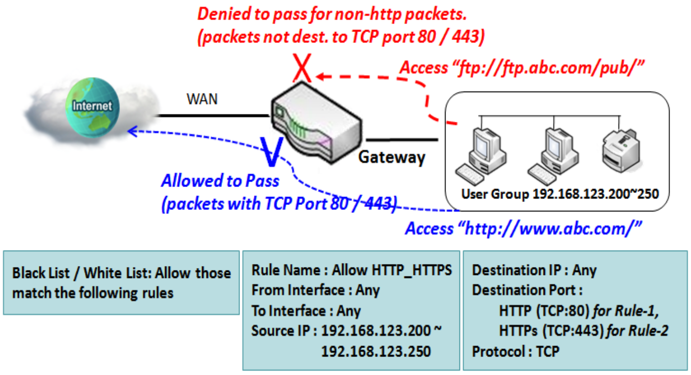


Configuration [Help]

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

"Packet Filter" function can let you define some filtering rules for incoming and outgoing packets. So the router 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 router, the source and destination IP addresses, and destination service port type and port number. In addition, the time schedule to which the rule will be active.

Packet Filter with White List Scenario


Denied to pass for non-http packets.
(packets not dest. to TCP port 80 / 443)
X
Access "ftp://ftp.abc.com/pub/"
Internet
WAN
Gateway
V
Allowed to Pass
(packets with TCP Port 80 / 443)
User Group 192.168.123.200~250
Access "http://www.abc.com/"

Black List / White List: Allow those match the following rules

Rule Name : Allow HTTP_HTTPS
From Interface : Any
To Interface : Any
Source IP : 192.168.123.200 ~ 192.168.123.250

Destination IP : Any
Destination Port :
HTTP (TCP:80) *for Rule-1,*
HTTPs (TCP:443) *for Rule-2*
Protocol : TCP

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

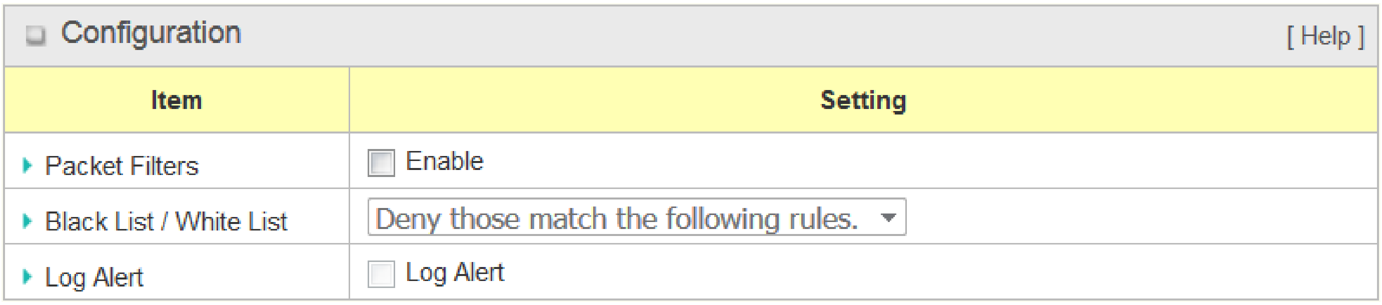
Under such configuration, the gateway will allow only HTTP and HTTPS packets, issued from the IP range 192.168.123.200 to 250, which are targeted to TCP port 80 or 443 to pass the WAN interface.

Packet Filter Setting

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

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

Enable Packet Filter



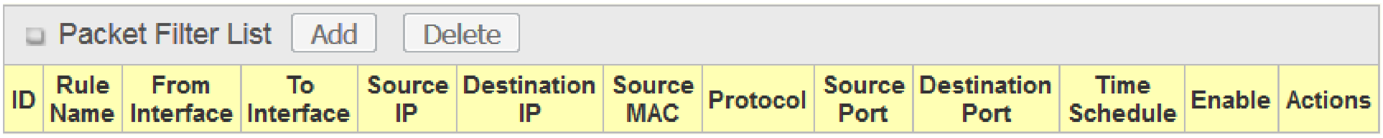
Configuration [Help]

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

Configuration Window		
Item Name	**Value setting**	**Description**
Packet Filter	The box is unchecked by default	Check the **Enable** box to activate Packet Filter function
Black List / White List	Deny those match the following rules is set by default	When ***Deny those match the following rules*** is selected, as the name suggest, packets specified in the rules will be blocked –black listed. In contrast, with ***Allow those match the following rules***, you can specifically white list the packets to pass and the rest will be blocked.
Log Alert	The box is unchecked by default	Check the **Enable** box to activate Event Log.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Create/Edit Packet Filter Rules

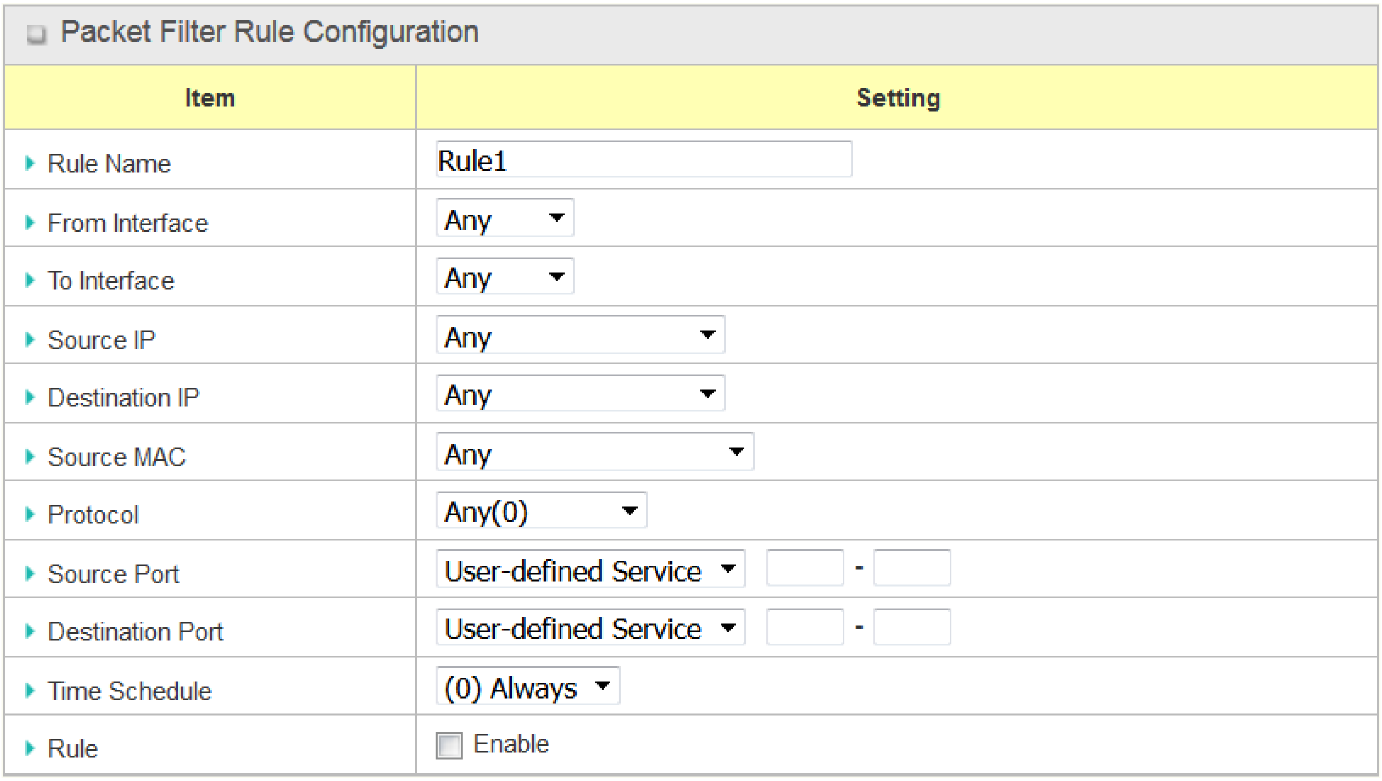
The router allows you to customize your packet filtering rules. It supports up to a maximum of 20 filter rule sets.



Packet Filter List Add Delete

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

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



Packet Filter Rule Configuration

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

Packet Filter Rule Configuration		
Item Name	**Value setting**	**Description**
Rule Name	1. String format can be any text 2. A Must filled setting	Enter a packet filter rule name. Enter a name that is easy for you to remember. ***Value Range***: 1 ~ 30 characters.
From Interface	1. A Must filled setting **2. By default Any is selected**	Define the selected interface to be the packet-entering interface of the router. If the packets to be filtered are coming from **LAN to WAN** then select LAN for this field. Or **VLAN-1 to WAN** then select **VLAN-1** for this field. Other examples are VLAN-1 to VLAN-2. VLAN-1 to WAN. Select **Any** to filter packets coming into the router from any interfaces. Please note that two identical interfaces are not accepted by the router. e.g., VLAN-1 to VLAN-1.

To Interface	1. A Must filled setting 2. By default Any is selected	Define the selected interface to be the packet-leaving interface of the router. If the packets to be filtered are entering from **LAN to WAN then** select **WAN** for this field. Or **VLAN-1 to WAN** then select **WAN** for this field. Other examples are VLAN-1 to VLAN-2. VLAN-1 to WAN. Select **Any** to filter packets leaving the router from any interfaces. Please note that two identical interfaces are not accepted by the router. e.g., VLAN-1 to VLAN-1.
Source IP	1. A Must filled setting 2. By default Any is selected	This field is to specify the **Source IP address**. Select **Any** to filter packets coming from any IP addresses. Select **Specific IP Address** to filter packets coming from an IP address. Select **IP Range** to filter packets coming from a specified range of IP address.
Destination IP	1. A Must filled setting 2. By default Any is selected	This field is to specify the **Destination IP address**. Select **Any** to filter packets that are entering to any IP addresses. Select **Specific IP Address** to filter packets entering to an IP address entered in this field. Select **IP Range** to filter packets entering to a specified range of IP address entered in this field.
Source MAC	1. A Must filled setting 2. By default Any is selected	This field is to specify the **Source MAC address**. Select **Any** to filter packets coming from any MAC addresses. Select **Specific MAC Address** to filter packets coming from a MAC address.
Protocol	1. A Must filled setting 2. By default Any(0) is selected	For **Protocol**, select **Any** to filter any protocol packets Then for **Source Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. Then for **Destination Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. ***Value Range***: 1 ~ 65535 for Source Port, Destination Port.
		For **Protocol**, select **ICMPv4** to filter ICMPv4 packets
		For **Protocol**, select **TCP** to filter **TCP** packets Then for **Source Port**, select a 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. ***Value Range***: 1 ~ 65535 for Source Port, Destination Port.
		For **Protocol**, select **UDP** to filter **UDP** packets Then for **Source Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. Then for **Destination Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. ***Value Range***: 1 ~ 65535 for Source Port, Destination Port.
		For **Protocol**, select **GRE** to filter **GRE** packets
		For **Protocol**, select **ESP** to filter **ESP** packets

		For **Protocol**, select **SCTP** to filter **SCTP** packets
		For **Protocol**, select **User-defined** to filter packets with specified port number. Then enter a pot number in **Protocol Number** box.
Time Schedule	A Must filled setting	Apply **Time Schedule** to this rule, otherwise leave it as Always. If the dropdown list is empty ensure **Time Schedule** is pre-configured. Refer to **Object Definition > Scheduling > Configuration** tab.
Rule	The box is unchecked by default.	Click **Enable** box to activate this rule then save the settings.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings
Back	N/A	When the **Back** button is clicked the screen will return to the Packet Filter Configuration page.

4.2.2 URL Blocking

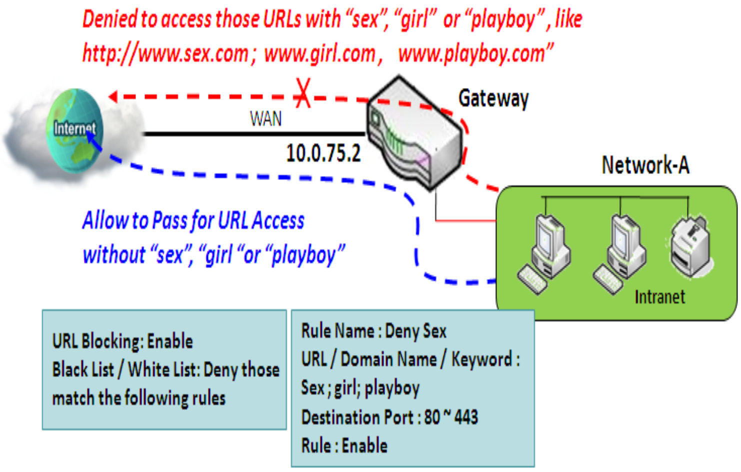
"URL Blocking" function can let you define blocking or allowing rules for incoming and outgoing Web request packets. With defined rules, router can control the Web requests containing the complete URL, partial domain name, or pre-defined keywords. For example, one can filter out or allow only the Web requests based on domain input suffixes like .com or .org or keywords like “bct” or “mpe”.

An URL blocking rule should specify the URL, partial domain name, or included keywords in the Web requests from and to the router and also the destination service port. Besides, a certain time schedule can be applied to activate the URL Blocking rules during pre-defined time interval(s).

The router will logs and displays the disallowed web accessing requests that matched the defined URL blocking rule in the black-list or in the exclusion of the white-list.

When you choose "Allow all to pass except those match the following rules" for the "URL Blocking Rule List", you are setting the defined URL blocking rules to belong to the black list. The packets, listed in the rule list, will be blocked if one pattern in the requests matches to one rule. Other Web requests can pass through the router. In contrast, when you choose "Deny all to pass except those match the following rules" for the "URL Blocking Rule List", you are setting the defined packet filtering rules to belong to the white list. The Web requests, listed in the rule, will be allowed if one pattern in the requests matches to one rule. Other Web requests will be blocked.

URL Blocking Rule with Black List


Denied to access those URLs with "sex", "girl" or "playboy", like
http://www.sex.com; www.girl.com, www.playboy.com"
Internet
WAN
10.0.75.2
Gateway
Network-A
Allow to Pass for URL Access
without "sex", "girl "or "playboy"
Intranet
URL Blocking: Enable
Black List / White List: Deny those match the following rules
Rule Name : Deny Sex
URL / Domain Name / Keyword :
Sex ; girl; playboy
Destination Port : 80 ~ 443
Rule : Enable

When the administrator of the gateway wants to block the Web requests with some dedicated patterns, he can use the "URL Blocking" function to block specific Web requests by defining the black list as shown in above diagram. Certainly, when the administrator wants to allow only the Web requests with some dedicated patterns to go through the gateway, he can also use the "URL Blocking" function by defining the white list to meet the requirement.

As shown in the diagram, enable the URL blocking function and create the first rule to deny the Web requests with "sex" or "sexygirl" patterns and the other to deny the Web requests with "playboy" pattern to go through the gateway. System will block the Web requests with "sex", "sexygirl" or "playboy" patterns to pass through the gateway.

URL Blocking Setting

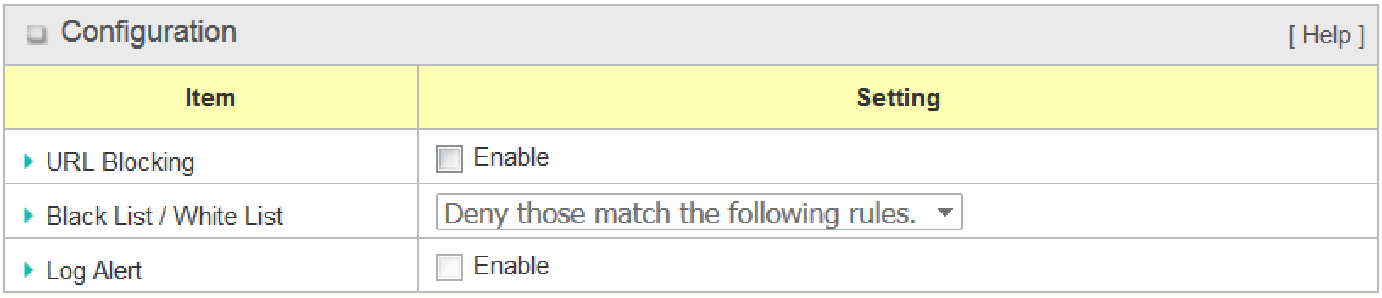
Go to **Security > Firewall > URL Blocking** Tab.

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

The "Configuration" window can let you activate the URL blocking function and specify to black listing or to white listing the packets defined in the "URL Blocking Rule List" entry. In addition, log alerting can be enabled to record on-going events for any disallowed Web request packets. Refer to "System Status" in "6.1.1 System Related" section in this user manual for how to view recorded log.

The "URL Blocking Rule List" window lists all your defined URL blocking rule entry. And finally, the "URL Blocking Rule Configuration" window can let you define URL blocking rules. The parameters in a rule include the rule name, the Source IP or MAC, the URL/Domain Name/Keyword, the destination service ports, the integrated time schedule rule and the rule activation.

Enable URL Blocking



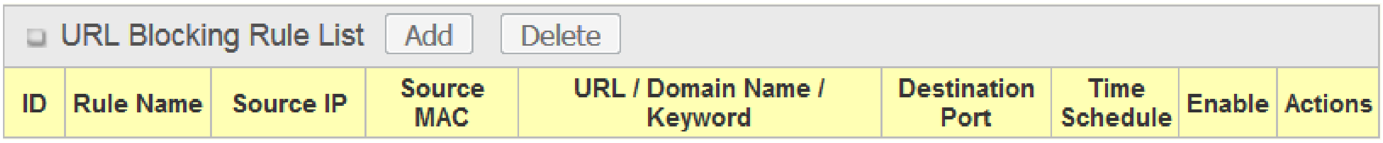
Configuration [Help]

Item	Setting
URL Blocking	□ Enable
Black List / White List	Deny those match the following rules. ▾
Log Alert	□ Enable

Configuration		
Item	**Value setting**	**Description**
URL Blocking	The box is unchecked by default	Check the **Enable** box to activate URL Blocking function.
Black List / White List	**Deny those match the following rules** is set by default	Specify the URL Blocking Policy, either Black List or White List. Black List: When **Deny those match the following rules** is selected, as the name suggest, the matched Web request packets will be blocked. White List: When **Allow those match the following rules** is selected, the matched Web request packets can pass through the Gateway, and the others that don't match the rules will be blocked.
Log Alert	The box is unchecked by default	Check the **Enable** box to activate Event Log.
Save	NA	Click **Save** button to save the settings
Undo	NA	Click **Undo** button to cancel the settings

Create/Edit URL Blocking Rules

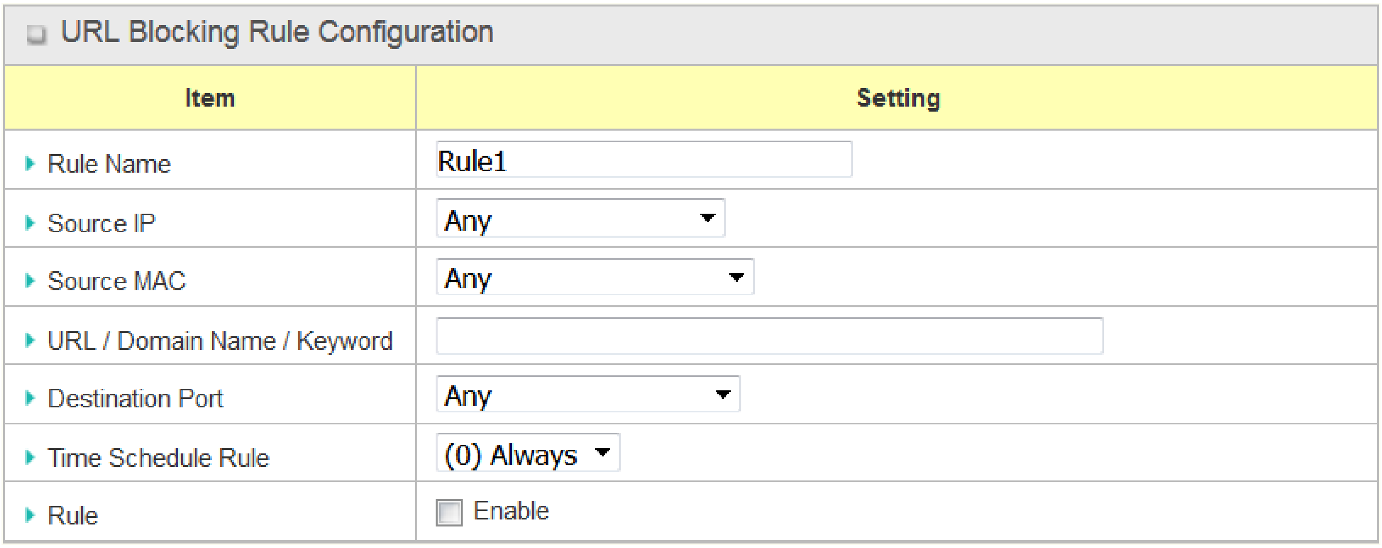
The Gateway supports up to a maximum of 20 URL blocking rule sets. Ensure that the URL Blocking is enabled before we can create blocking rules.



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, the **URL Blocking Rule Configuration** screen will appear.



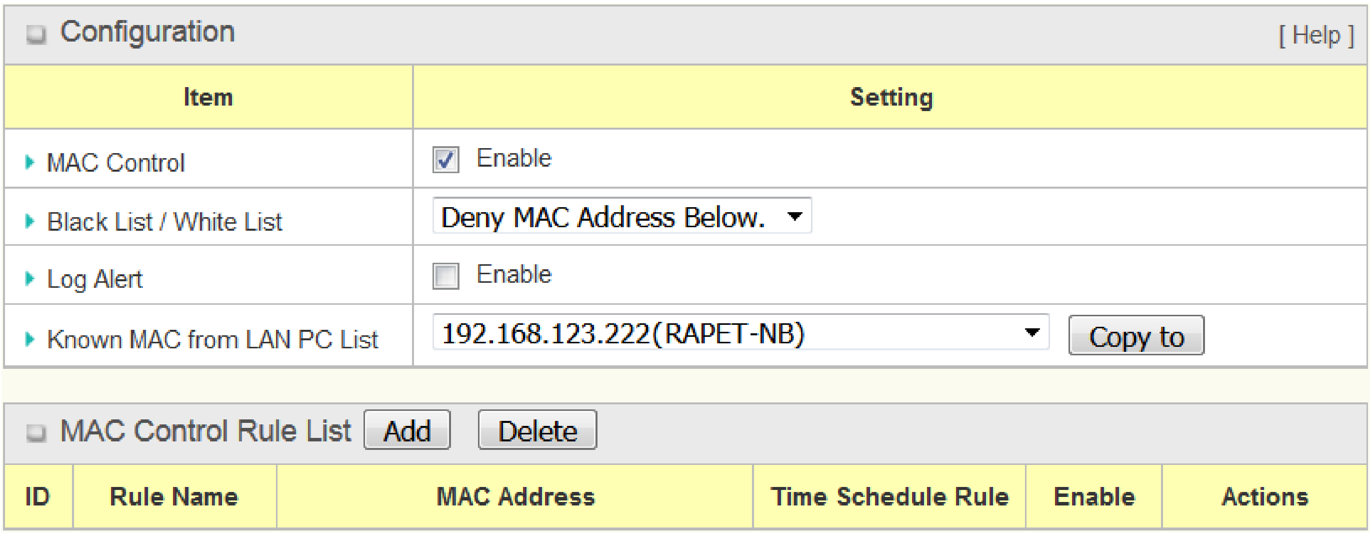
URL Blocking Rule Configuration

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

URL Blocking Rules Configuration		
Item	**Value setting**	**Description**
Rule Name	1. String format can be any text 2. A Must filled setting	Specify an URL Blocking rule name. Enter a name that is easy for you to understand.
Source IP	1. A Must filled setting 2. **Any** is set by default	This field is to specify the **Source IP address**. • Select **Any** to filter packets coming from any IP addresses. • Select **Specific IP Address** to filter packets coming from an IP address entered in this field. • Select **IP Range** to filter packets coming from a specified range of IP address entered in this field.
Source MAC	1. A Must filled setting 2. **Any** is set by default	This field is to specify the **Source MAC address**. • Select **Any** to filter packets coming from any MAC addresses. • Select **Specific MAC Address** to filter packets coming from a MAC address entered in this field.
URL / Domain Name / Keyword	1. A Must filled setting 2. Supports up to a maximum of 10 Keywords in a rule by using the delimiter “;”.	Specify URL, Domain Name, or Keyword list for URL checking. • In the **Black List** mode, if a matched rule is found, the packets will be dropped. • In the **White List** mode, if a matched rule is found, the packets will be accepted and the others which don’t match any rule will be dropped.

Destination Port	1. A Must filled setting 2. **Any** is set by default	This field is to specify the **Destination Port number**. • Select **Any** to filter packets going to any Port. • Select **Specific Service Port** to filter packets going to a specific Port entered in this field. • Select **Port Range** to filter packets going to a specific range of Ports entered in this field.
Time Schedule Rule	A Must filled setting	Apply a specific **Time Schedule** to this rule; otherwise leave it as **(0) Always**. If the dropdown list is empty ensure **Time Schedule** is pre-configured. Refer to **Object Definition** > **Scheduling > Configuration** tab.
Rule	The box is unchecked by default.	Click the **Enable** box to activate this rule.
Save	*NA*	Click the **Save** button to save the settings.
Undo	*NA*	Click the **Undo** button to cancel the changes.
Back	*NA*	Click the **Back** button to return to the URL Blocking Configuration page.

4.2.3 MAC Control



Configuration [Help]

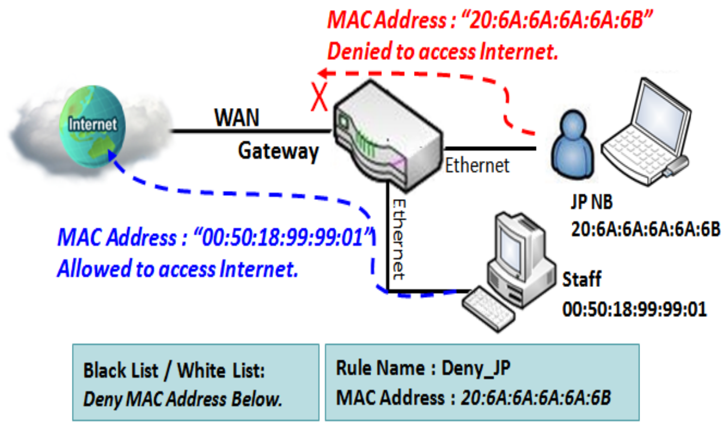
Item	Setting
MAC Control	☑ Enable
Black List / White List	Deny MAC Address Below. ▾
Log Alert	□ Enable
Known MAC from LAN PC List	192.168.123.222(RAPET-NB) ▾ [Copy to]

MAC Control Rule List [Add] [Delete]

ID	Rule Name	MAC Address	Time Schedule Rule	Enable	Actions

"MAC Control" function allows you to assign the accessibility to the gateway for different users based on device’s MAC address. When the administrator wants to reject the traffics from some client hosts with specific MAC addresses, he can use the "MAC Control" function to reject with the black list configuration.

MAC Control with Black List Scenario


MAC Address : "20:6A:6A:6A:6A:6B"
Denied to access Internet.
Internet
WAN
Gateway
Ethernet
JP NB
20:6A:6A:6A:6A:6B
MAC Address : "00:50:18:99:99:01"
Allowed to access Internet.
Ethernet
Staff
00:50:18:99:99:01
Black List / White List:
Deny MAC Address Below.
Rule Name : Deny_JP
MAC Address : 20:6A:6A:6A:6A:6B

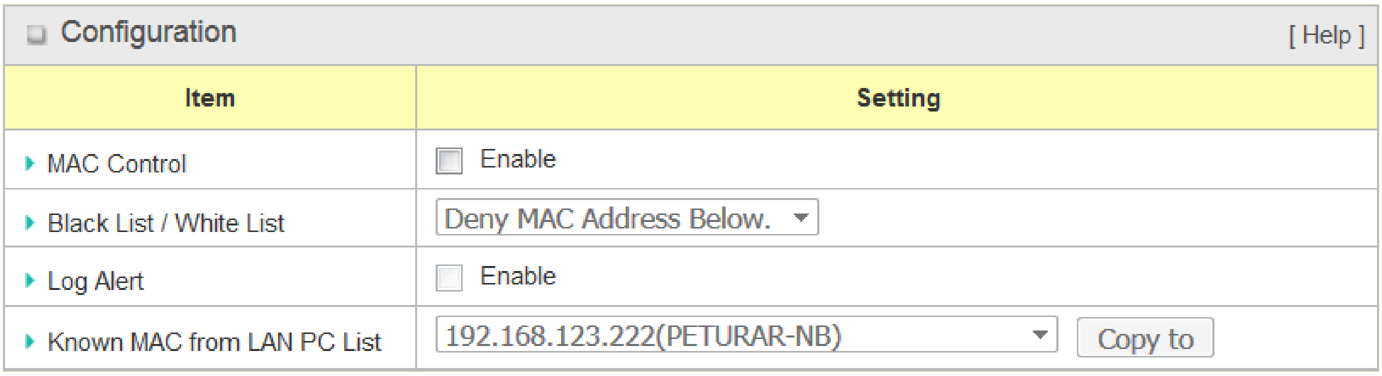
As shown in the diagram, enable the MAC control function and specify the "MAC Control Rule List" is a black list, and configure one MAC control rule for the gateway to deny the connection request from the "JP NB" with its own MAC address 20:6A:6A:6A:6A:6B. System will block the connecting from the "JP NB" to the gateway but allow others.

MAC Control Setting

Go to **Security > Firewall > MAC Control** Tab.

The MAC control setting allows user to create and customize MAC address policies to allow or reject packets with specific source MAC address.

Enable MAC Control



Configuration [Help]

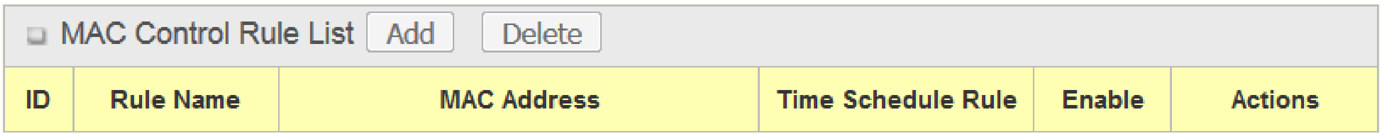
Item	Setting
MAC Control	□ Enable
Black List / White List	Deny MAC Address Below. ▾
Log Alert	□ Enable
Known MAC from LAN PC List	192.168.123.222(PETURAR-NB) ▾ Copy to

Configuration Window		
Item	**Value setting**	**Description**
MAC Control	The box is unchecked by default	Check the **Enable** box to activate the MAC filter function
Black List / White List	Deny MAC Address Below is set by default	When ***Deny MAC Address Below*** is selected, as the name suggest, packets specified in the rules will be blocked –black listed. In contrast, with ***Allow MAC Address Below***, you can specifically white list the packets to pass and the rest will be blocked.
Log Alert	The box is unchecked by default	Check the **Enable** box to activate to activate Event Log.

Known MAC from LAN PC List	N/A	Select a MAC Address from LAN Client List. Click the **Copy to** to copy the selected **MAC Address** to the filter rule.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Create/Edit MAC Control Rules

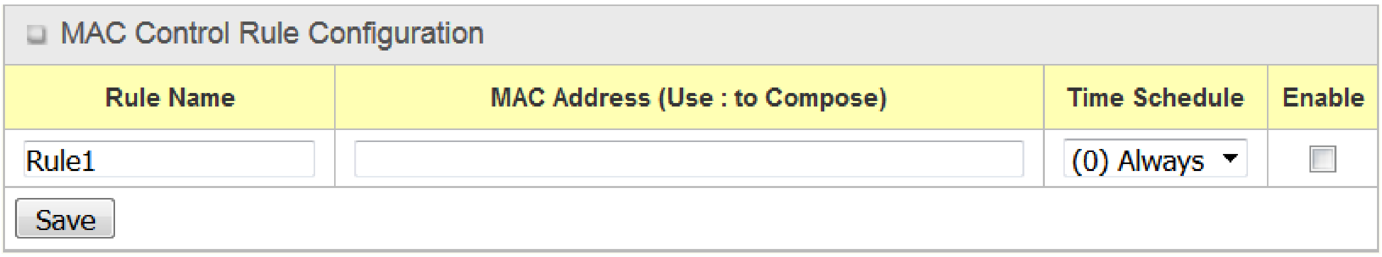
The router supports up to a maximum of 20 filter rule sets. Ensure that the MAC Control is enabled before we can create control rules.



MAC Control Rule List Add Delete

ID	Rule Name	MAC Address	Time Schedule Rule	Enable	Actions

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



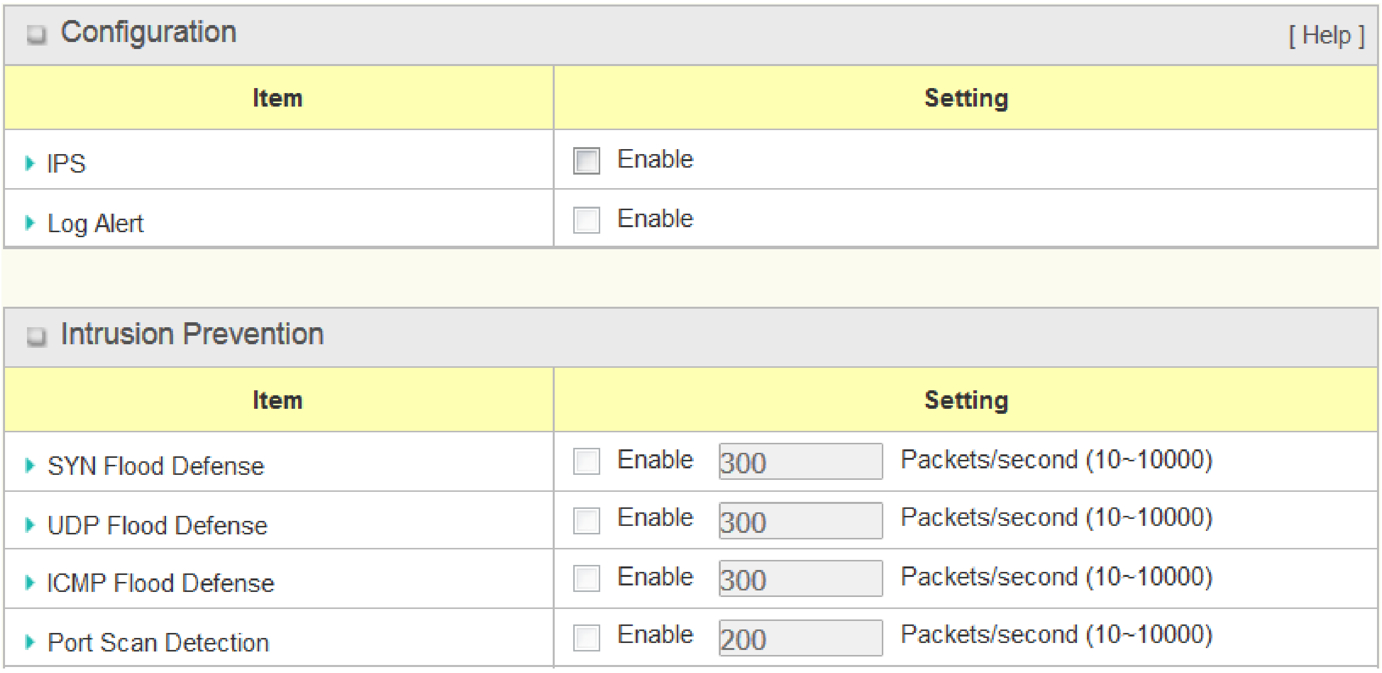
MAC Control Rule Configuration

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

Save

MAC Control Rule Configuration		
Item	**Value setting**	**Description**
Rule Name	1. String format can be any text 2. A Must fill setting	Enter a MAC Control rule name. Enter a name that is easy for you to remember.
MAC Address (Use: to Compose)	1. MAC Address string Format 2. A Must fill setting	Specify the **Source MAC Address** to filter rule.
Time Schedule	A Must fill setting	Apply **Time Schedule** to this rule; otherwise leave it as **(0) Always**. If the dropdown list is empty, ensure **Time Schedule** is pre-configured. Refer to **Object Definition > Scheduling > Configuration tab**
Enable	The box is unchecked by default.	Click **Enable** box to activate this rule, and 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** to return to the MAC Control Configuration page.

4.2.4 IPS



Configuration [Help]

Item	Setting
IPS	□ Enable
Log Alert	□ Enable

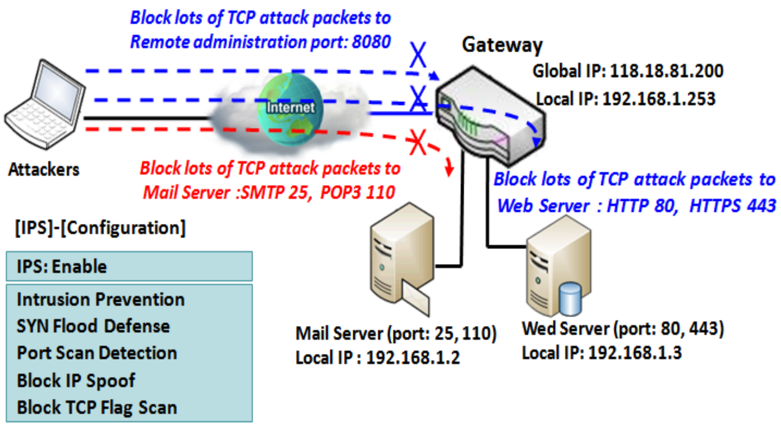
Intrusion Prevention

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)

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

Intrusion Prevention System (IPS) is 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. You can also enable the log alerting so that system will record Intrusion events when corresponding intrusions are detected.

IPS Scenario


Block lots of TCP attack packets to
Remote administration port: 8080
Gateway
Global IP: 118.18.81.200
Local IP: 192.168.1.253
Internet
Attackers
Block lots of TCP attack packets to
Mail Server :SMTP 25, POP3 110
Block lots of TCP attack packets to
Web Server : HTTP 80, HTTPS 443
[IPS]-[Configuration]
IPS: Enable
Intrusion Prevention
SYN Flood Defense
Port Scan Detection
Block IP Spoof
Block TCP Flag Scan
Mail Server (port: 25, 110)
Local IP : 192.168.1.2
Wed Server (port: 80, 443)
Local IP: 192.168.1.3

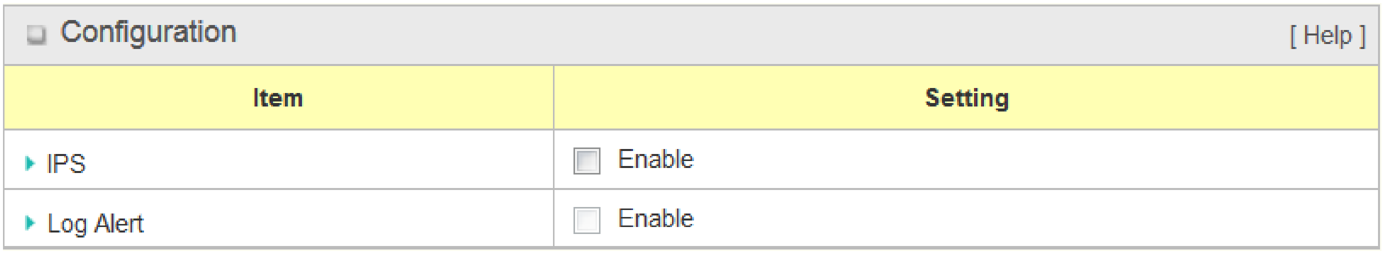
As shown in the diagram, the gateway serves as an E-mail server, Web Server and also provides TCP port 8080 for remote administration. So, remote users or unknown users can request those services from Internet. With IPS enabled, the gateway can detect incoming attack packets, including the TCP ports (25, 80, 110, 443 and 8080) with services. It will block the attack packets and let the normal access to pass through the gateway.

IPS Setting

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

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

Enable IPS Firewall



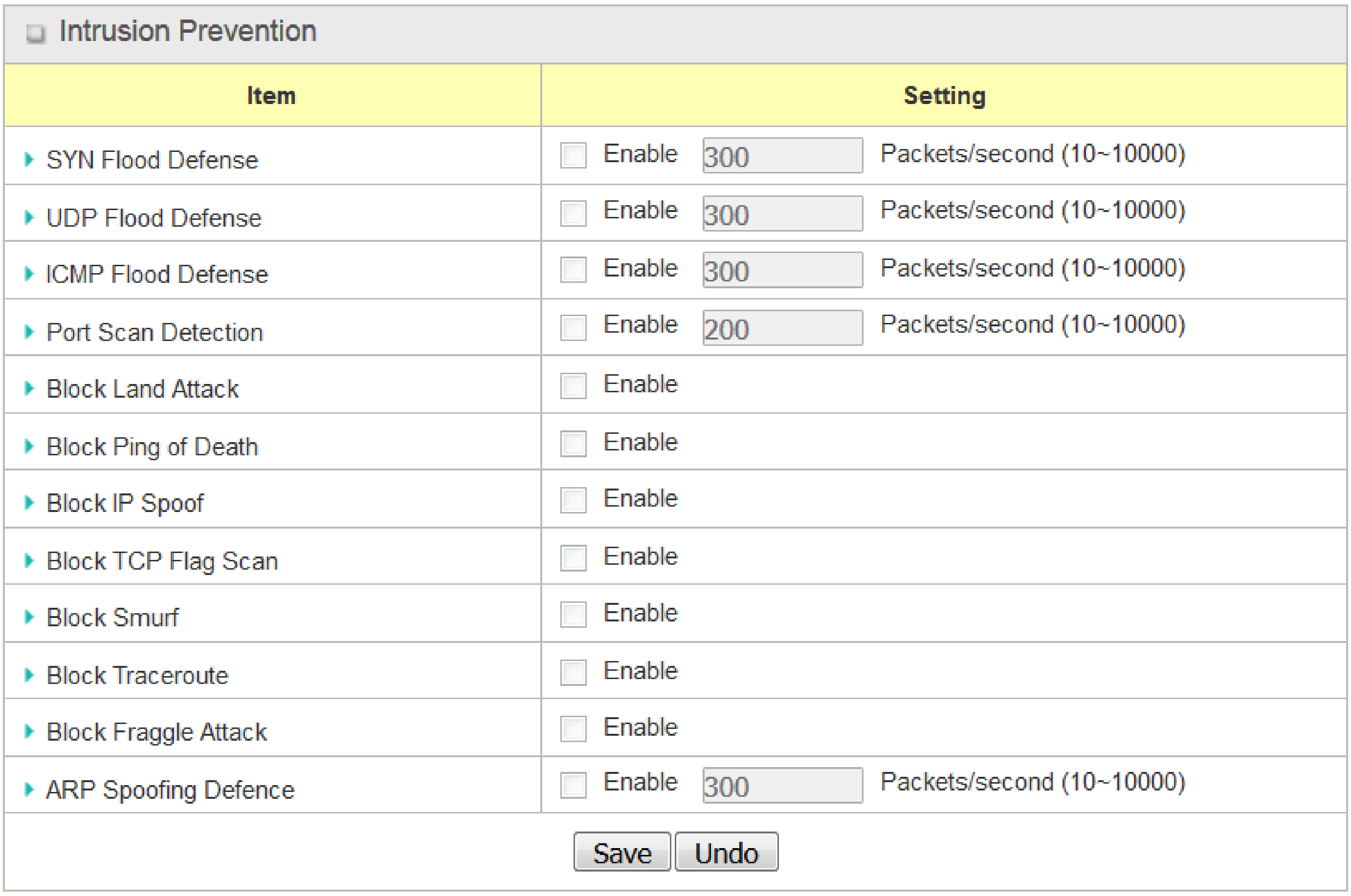
Configuration [Help]

Item	Setting
IPS	□ Enable
Log Alert	□ Enable

Configuration Window		
Item	**Value setting**	**Description**
IPS	The box is unchecked by default	Check the **Enable** box to activate IPS function
Log Alert	The box is unchecked by default	Check the **Enable** box to activate to activate Event Log.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Setup Intrusion Prevention Rules

The router allows you to select intrusion prevention rules you may want to enable. Ensure that the IPS is enabled before we can enable the defense function.



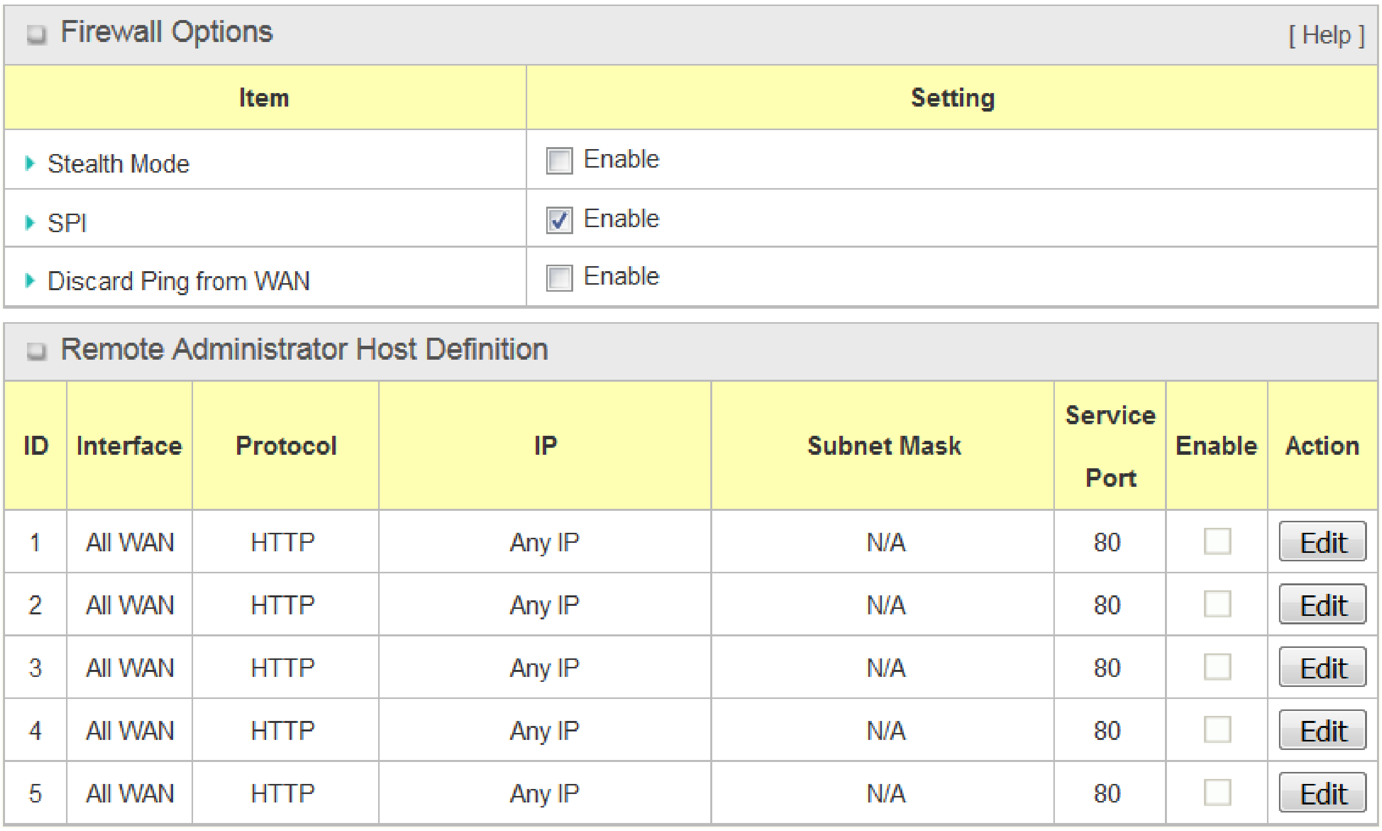
Intrusion Prevention

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

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. ***Value Range***: 10 ~ 10000.
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. *Value Range*: 10 ~ 10000.

Block Land Attack	The box is unchecked by default.	Click **Enable** box to activate this intrusion prevention rule.
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. ***Value Range***: 10 ~ 10000.
Save	NA	Click **Save** to save the settings
Undo	NA	Click **Undo** to cancel the settings

4.2.5 Options



Firewall Options [Help]

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

Remote Administrator Host Definition

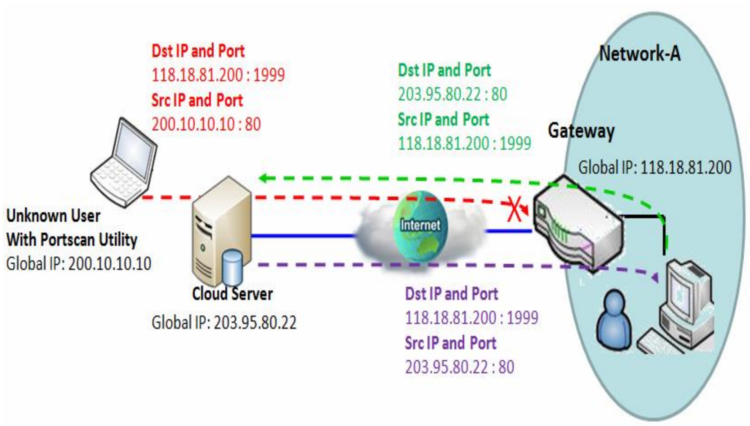
ID	Interface	Protocol	IP	Subnet Mask	Service Port	Enable	Action
1	All WAN	HTTP	Any IP	N/A	80	□	Edit
2	All WAN	HTTP	Any IP	N/A	80	□	Edit
3	All WAN	HTTP	Any IP	N/A	80	□	Edit
4	All WAN	HTTP	Any IP	N/A	80	□	Edit
5	All WAN	HTTP	Any IP	N/A	80	□	Edit

There are some additional useful firewall options in this page:

Stealth Mode lets router not to respond to port scans from the WAN so that makes it less susceptible to discovery and attacks on the Internet. "SPI" enables router to record the packet information like IP address, port address, ACK, SEQ number and so on while they pass through the router, and the router checks every incoming packet to detect if this packet is valid.

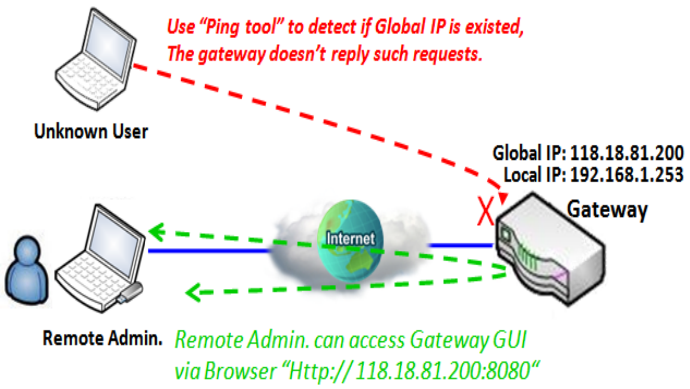
Discard Ping from WAN makes any host on the WAN side can`t ping this router. And finally, "Remote Administrator Hosts" enables you to perform administration task from a remote host. If this feature is enabled, only specified IP address(-es) can perform remote administration.

Enable SPI Scenario



As shown in the diagram, Gateway has the IP address of 118.18.81.200 for WAN interface and 192.168.1.253 for LAN interface. It serves as a NAT gateway. Users in Network-A initiate to access cloud server through the gateway. Sometimes, unknown users will simulate the packets but use different source IP to masquerade. With the SPI feature been enabled at the gateway, it will block such packets from unknown users.

Discard Ping from WAN & Remote Administrator Hosts Scenario


Use "Ping tool" to detect if Global IP is existed,
The gateway doesn't reply such requests.
Unknown User
Global IP: 118.18.81.200
Local IP: 192.168.1.253
Gateway
Internet
Remote Admin.
Remote Admin. can access Gateway GUI
via Browser "Http://118.18.81.200:8080"

"Discard Ping from WAN" makes any host on the WAN side can`t ping this gateway reply any ICMP packets. Enable the Discard Ping from WAN function to prevent security leak when local users surf the internet.

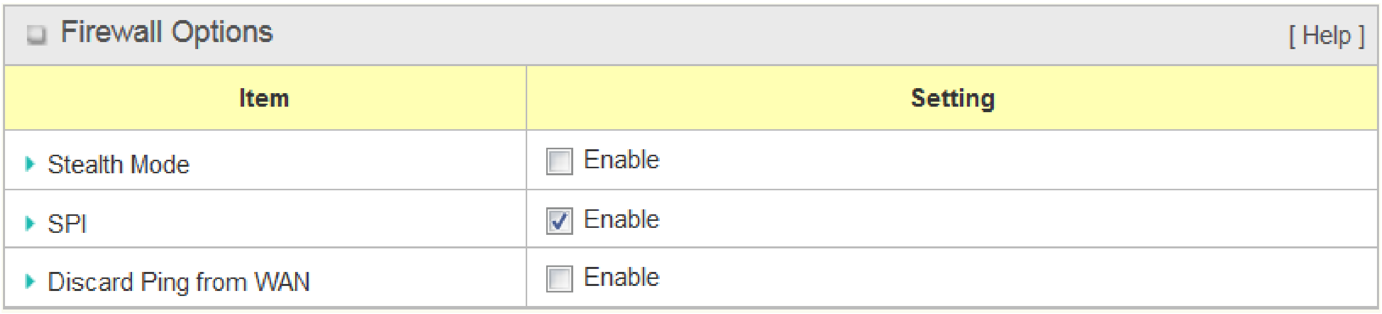
Remote administrator knows the gateway's global IP, and he can access the Gateway GUI via TCP port 8080.

Firewall Options Setting

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

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

Enable Firewall Options



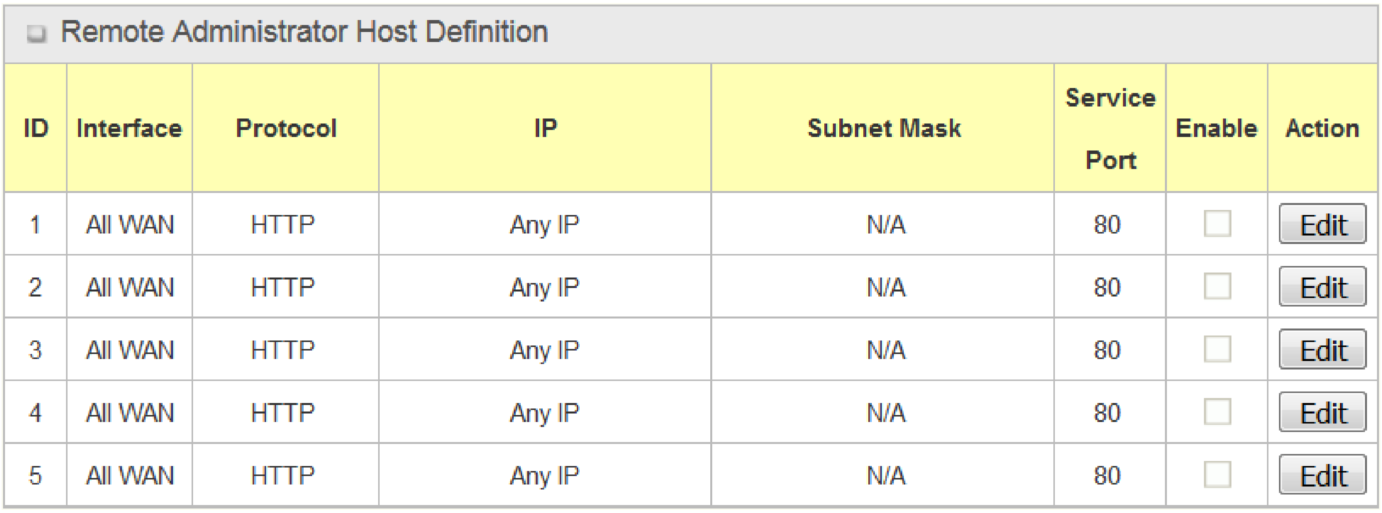
Firewall Options [Help]

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

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

Define Remote Administrator Host

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



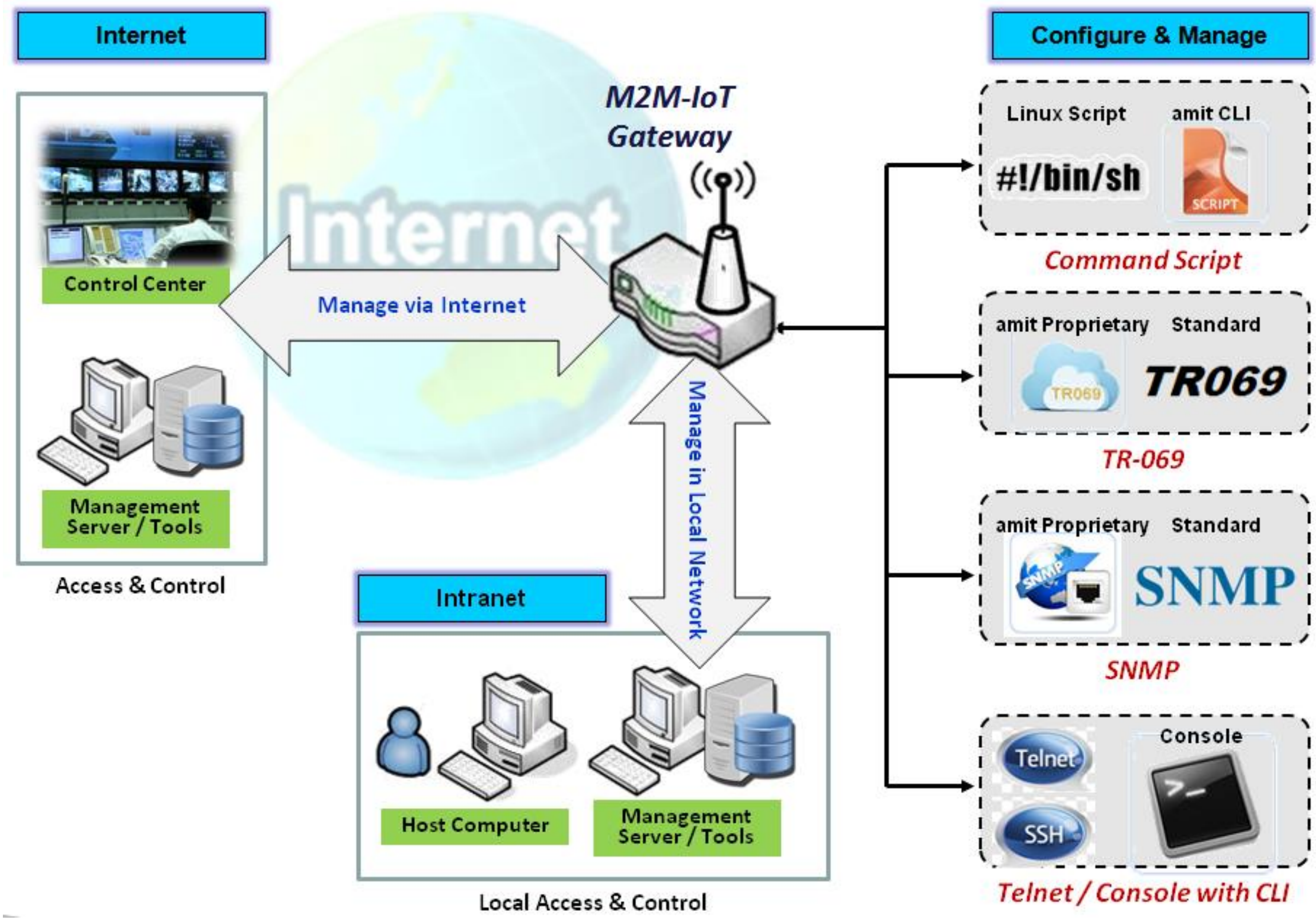
Remote Administrator Host Definition

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

Remote Administrator Host Definition		
Item	**Value setting**	**Description**
Protocol	HTTP is set by default	Select **HTTP** or **HTTPS** method for router access.
IP	A Must filled setting	This field is to specify the remote host to assign access right for remote access. Select **Any IP** to allow any remote hosts Select **Specific IP** to allow the remote host coming from a specific subnet. An IP address entered in this field and a selected **Subnet Mask** to compose the subnet**.**
Service Port	1. 80 for HTTP by default 2. 443 for HTTPS by default	This field is to specify a Service Port to HTTP or HTTPS connection. ***Value Range***: 1 ~ 65535.
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

5. Administration

5.1 Configure & Manage



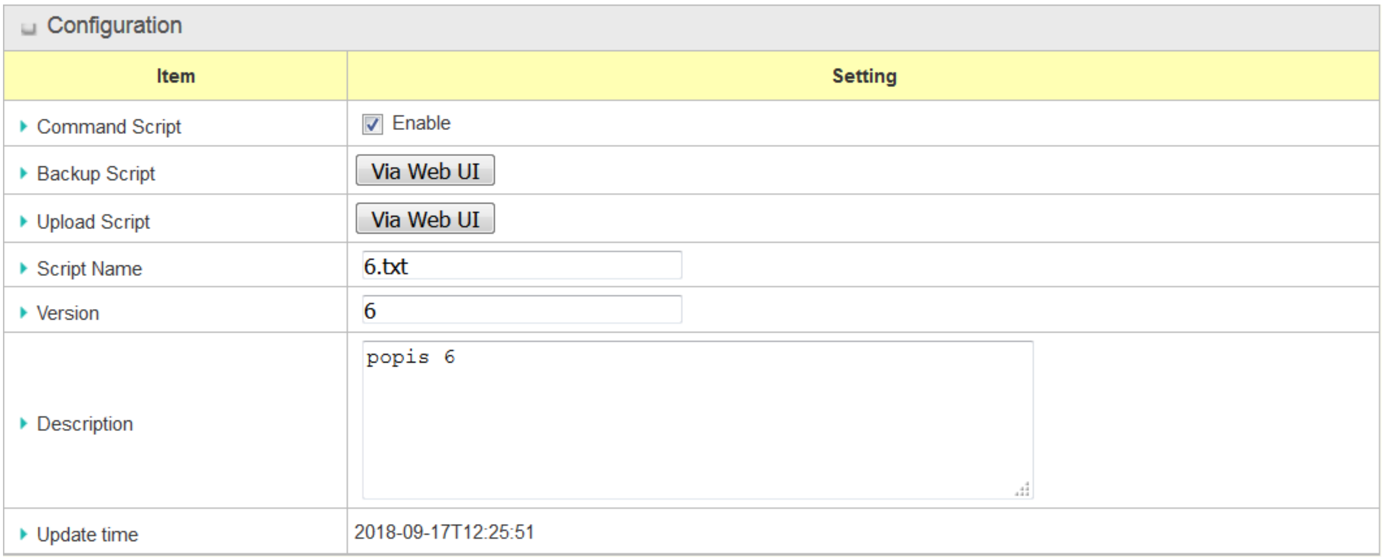
Configure & Manage refers to enterprise-wide administration of distributed systems including (and commonly in practice) computer systems. Centralized management has a time and effort trade-off that is related to the size of the company, the expertise of the IT staff, and the amount of technology being used. This device supports many system management protocols, such as Command Script, TR-069, SNMP, and Telnet with CLI. You can setup those configurations in the "Configure & Manage" section.

5.1.1 Command Script

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

Go to **Administration > Configure & Manage > Command Script** Tab.

Enable Command Script Configuration



Configuration

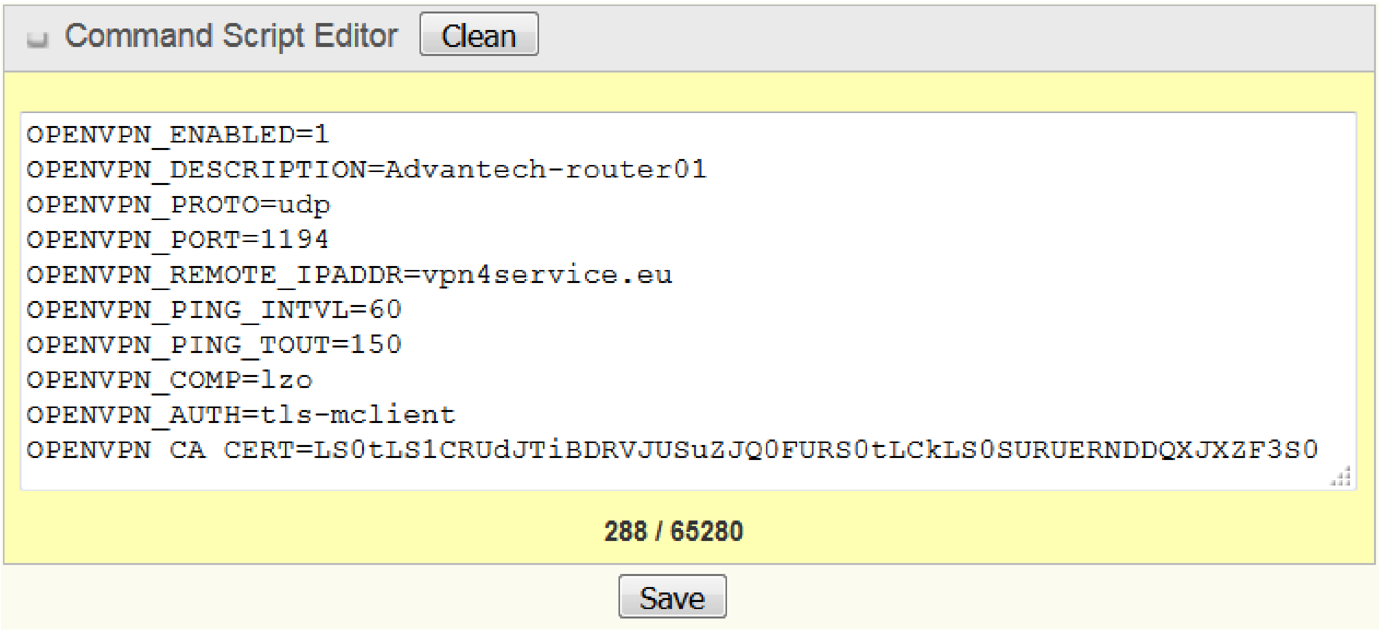
Item	Setting
Command Script	☑ Enable
Backup Script	Via Web UI
Upload Script	Via Web UI
Script Name	6.txt
Version	6
Description	popis 6
Update time	2018-09-17T12:25:51

Configuration

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

Edit Plain Text Command Script Configuration

You can edit the plain text configuration settings in the Command Script Editor window as shown below.



```
OPENVPN_ENABLED=1
OPENVPN_DESCRIPTION=Advantech-router01
OPENVPN_PROTO=udp
OPENVPN_PORT=1194
OPENVPN_REMOTE_IPADDR=vpn4service.eu
OPENVPN_PING_INTVL=60
OPENVPN_PING_TOUT=150
OPENVPN_COMP=lzo
OPENVPN_AUTH=tls-mclient
OPENVPN CA CERT=LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLCkLS0SURUERNDDQXJXZF3S0
```

288 / 65280

Plain Text Configuration		
Item	**Value setting**	**Description**
Clean	*NA*	Clean text area. (You should click **Save** button to further clean the configuration already saved in the system.)
Save	*NA*	Save configuration

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

Configuration Content		
Key	**Value setting**	**Description**
OPENVPN_ENABLED	1 : enable 0 : disable	Enable or disable OpenVPN Client function.
OPENVPN_DESCRIPTION	A Must filled Setting	Specify the tunnel name for the OpenVPN Client connection.
OPENVPN_PROTO	udp tcp	Define the **Protocol** for the OpenVPN Client. • Select **TCP** or **TCP /UDP** ->The OpenVPN will use TCP protocol, and **Port** will be set as 443 automatically. • Select **UDP** -> The OpenVPN will use UDP protocol, and **Port** will be set as 1194 automatically.
OPENVPN_PORT	A Must filled Setting	Specify the **Port** for the OpenVPN Client to use.
OPENVPN_REMOTE_IPADDR	IP or FQDN	Specify the **Remote IP/FQDN** of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the IP address or FQDN.
OPENVPN_PING_INTVL	seconds	Specify the time interval for OpenVPN keep-alive checking.

OPENVPN_PING_TOUT	seconds	Specify the timeout value for OpenVPN Client keep-alive checking.
OPENVPN_COMP	Adaptive	Specify the **LZO Compression** algorithm for OpenVPN client.
OPENVPN_AUTH	Static Key/TLS	Specify the authorization mode for the OpenVPN tunnel. • **TLS** ->The OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Client Cert.** and **Client Key** need to specify as well.
OPENVPN_CA_CERT	A Must filled Setting	Specify the Trusted CA certificate for the OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_CERT	A Must filled Setting	Specify the local certificate for OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_KEY	A Must filled Setting	Specify the local key for the OpenVPN client. It will go through Base64 Conversion.
OPENVPN_EXTRA_OPTS	Options	Specify the extra options setting for the OpenVPN client.
IP_ADDR1	IP	Ethernet LAN IP
IP_NETM1	Net mask	Ethernet LAN MASK
PPP_MONITORING	1 : enable 0 : disable	When the Network Monitoring feature is enabled, the router will use DNS Query or ICMP to periodically check Internet connection – connected or disconnected.
PPP_PING	0 : DNS Query 1 : ICMP Query	With **DNS Query,** the system checks the connection by sending DNS Query packets to the destination specified in PPP_PING_IPADDR. With **ICMP Query,** the system will check connection by sending ICMP request packets to the destination specified in PPP_PING_IPADDR.
PPP_PING_IPADDR	IP	Specify an IP address as the target for sending DNS query/ICMP request.
PPP_PING_INTVL	seconds	Specify the time interval for between two DNS Query or ICMP checking packets.

STARTUP	Script file	For the configurations that can be configured with standard Linux commands, you can put them in a script file, and apply the script file with STARTUP command.
		For example,
		STARTUP=#!/bin/sh
		STARTUP=echo “startup done” > /tmp/demo

Plain Text System Configuration with Telnet

In addition to the web-style plain text configuration as mentioned above, the router system also allow the configuration via Telnet CLI. Administrator can use the proprietary telnet command "***txtConfig***" and related action items to perform the plain system configuration.

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

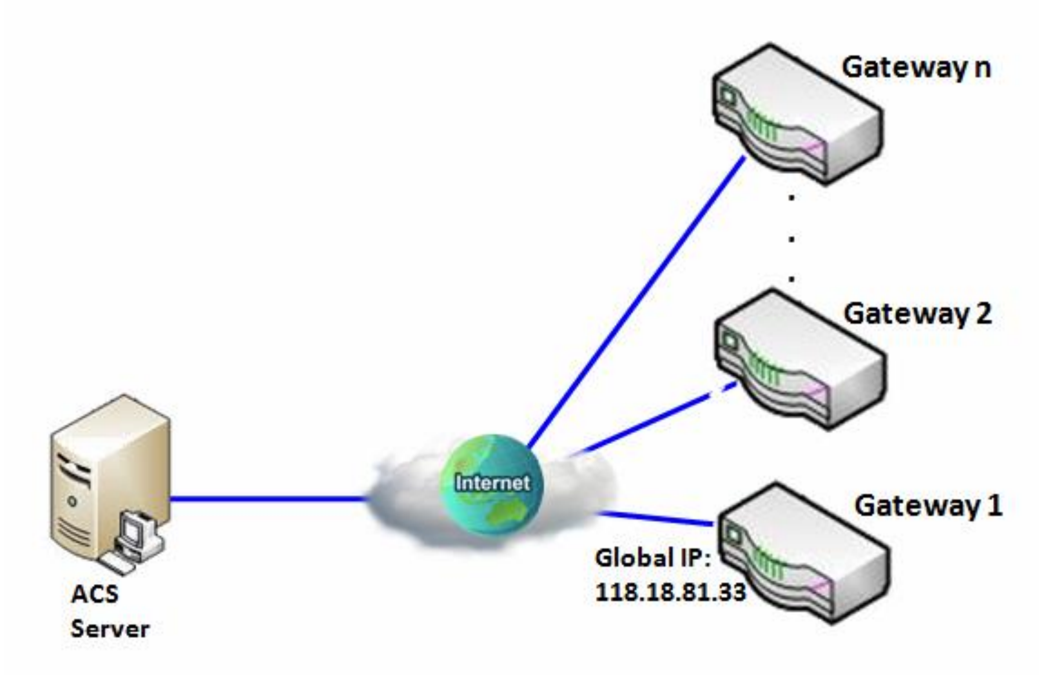
Action	Option	Description
clone	*Output file*	Duplicate the configuration content from database and stored as a configuration file. (ex: *txtConfig clone /tmp/config*) The contents in the configuration file are the same as the plain text commands mentioned above. This action is exactly the same as performing the "Backup" plain text configuration.
commit	an existing file	Commit the configuration content to database. (ex: *txtConfig commit /tmp/config*)
enable	*NA*	Enable plain text system config. (ex: *txtConfig enable*)
disable	*NA*	Disable plain text system config. (ex: *txtConfig disable*)
run_immediately	*NA*	Apply the configuration content that has been committed in database. (ex: *txtConfig run_immediately*)
run_immediately	an existing file	Assign a configuration file to apply. (ex: *txtConfig run_immediately /tmp/config*)

5.1.2 TR-069

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

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

Scenario - Managing deployed gateways through an ACS Server



Scenario Application Timing

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

Scenario Description

- The ACS server can configure, upgrade with latest FW and monitor these gateways.
- Remote gateways inquire the ACS server for jobs to do in each time period.
- The ACS server can ask the gateways to execute some urgent jobs.
- Parameter Setup Example
- Following tables list the parameter configuration as an example for the Gateway 1 in above diagram

with "TR-069" enabling.

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

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

Scenario Operation Procedure

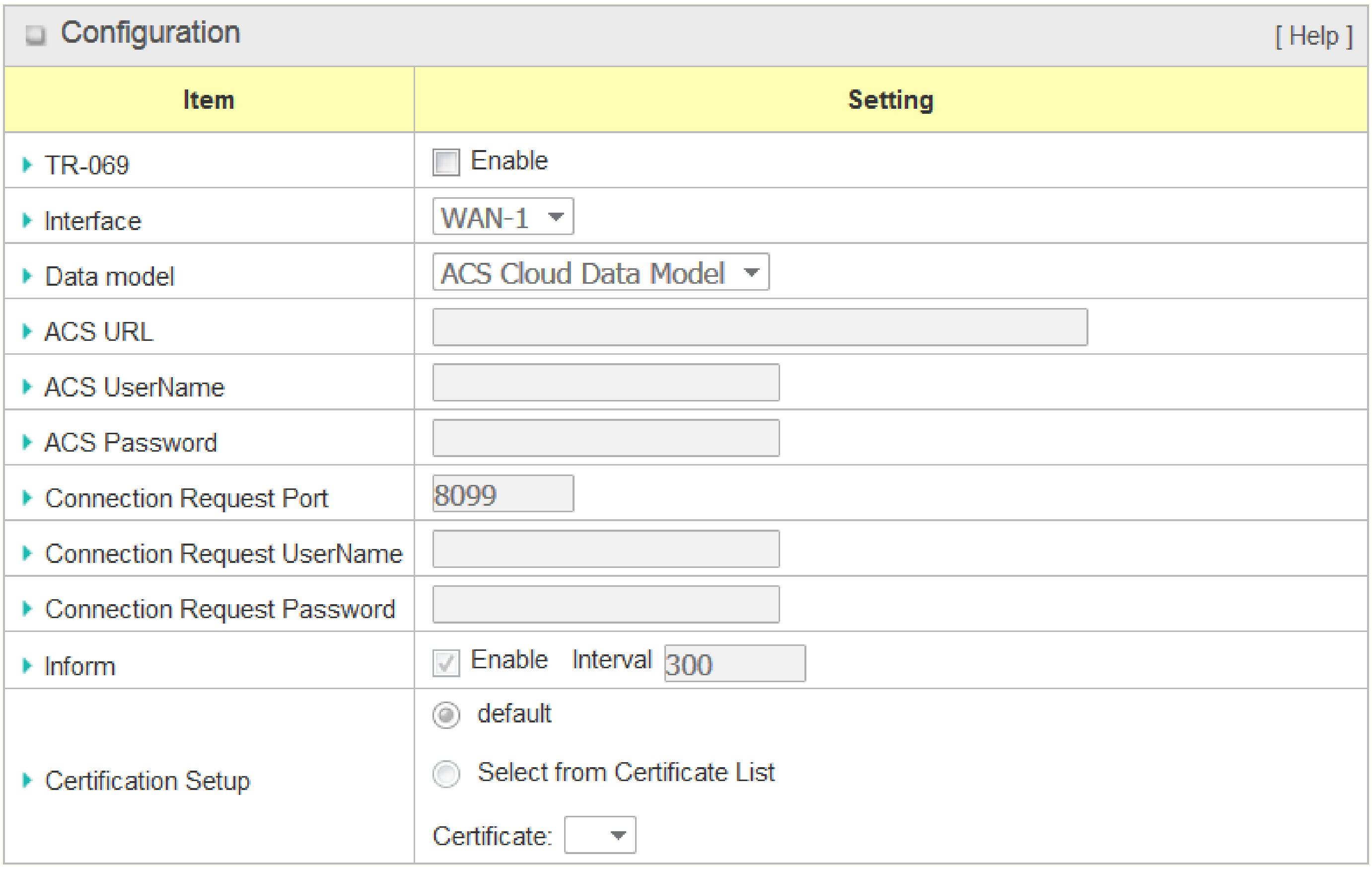
- In above diagram, the ACS server can manage multiple gateways in the Internet. The "Gateway 1" is one of them and has 118.18.81.33 IP address for its WAN-1 interface.
- When all remote gateways have booted up, they will try to connect to the ACS server.
- Once the connections are established successfully, the ACS server can configure, upgrade with latest FW and monitor these gateways.
- Remote gateways inquire the ACS server for jobs to do in each time period.
- If the ACS server needs some urgent jobs to be done by the gateways, it will issue the "Connection Request" command to those gateways. And those gateways make immediate connections in response to the ACS server’s immediate connection request for executing the urgent jobs.

TR-069 Setting

Go to **Administration > Configure & Manage > TR-069** tab.

In "TR-069" page, there is only one configuration window for TR-069 function. In the window, you must specify the related information for your security router to connect to the ACS. Drive the function to work by specifying the URL of the ACS server, the account information to login the ACS server, the service port and the account information for connection requesting from the ACS server, and the time interval for job inquiry. Except the inquiry time, there are no activities between the ACS server and the routers until the next inquiry cycle. But if the ACS server has new jobs that are expected to do by the routers urgently, it will ask these routers by using connection request related information for immediate connection for inquiring jobs and executing.

Enable TR-069



Configuration [Help]

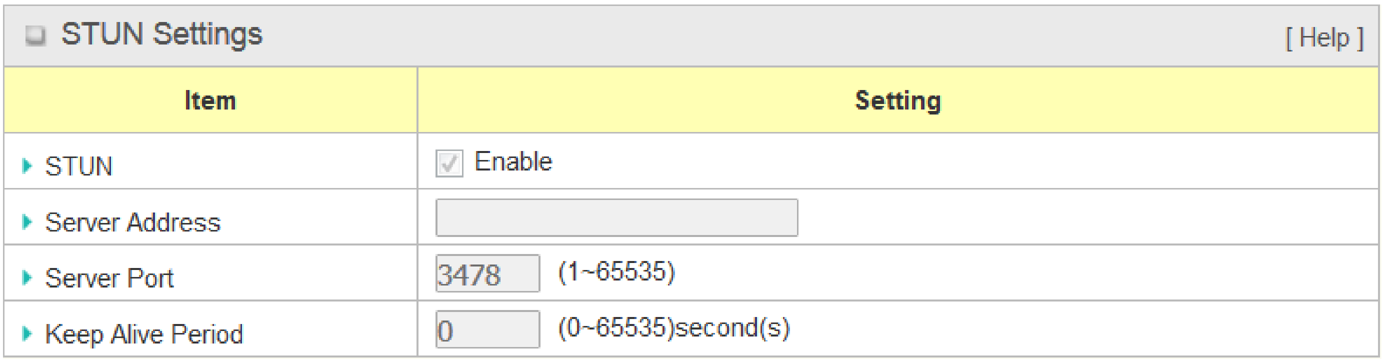
Item	Setting
TR-069	□ Enable
Interface	WAN-1
Data model	ACS Cloud Data Model
ACS URL	
ACS UserName	
ACS Password	
Connection Request Port	8099
Connection Request UserName	
Connection Request Password	
Inform	☑ Enable Interval 300
Certification Setup	● default ○ Select from Certificate List Certificate:

TR-069		
Item	**Value setting**	**Description**
TR-069	The box is unchecked by default	Check the **Enable** box to activate TR-069 function.
Interface	**WAN-1** is selected by default.	When you finish set basic network WAN-1 ~ WAN-n, you can choose WAN-1 ~ WAN-n When you finish set Security > VPN > IPSec/OpenVPN/PPTP/L2TP/GRE, you can choose IPSec/OpenVPN/PPTP/L2TP/GRE tunnel, the interface just like "IPSec #1"
Data Model	**ACS Cloud Data Model** is selected by default.	Select the TR-069 data model for the remote management. **Standard**: the ACS Server is a standard one, which is fully comply with TR-069. **ACS Cloud Data Model**: Select this data model if you intend to use Cloud ACS Server to managing the deployed routers.
ACS URL	A Must filled setting	You can ask ACS manager provide ACS URL and manually set
ACS Username	A Must filled setting	You can ask ACS manager provide ACS username and manually set
ACS Password	A Must filled setting	You can ask ACS manager provide ACS password and manually set
ConnectionRequest Port	1. A Must filled setting. **2. By default 8099 is set.**	You can ask ACS manager provide ACS ConnectionRequest Port and manually set *Value Range*: 0 ~ 65535.
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	1. The box is checked by default. **2. The Interval value is 300 by default.**	When the **Enable** box is checked, the router (CPE) will periodically send inform message to ACS Server according to the **Interval** setting. ***Value Range***: 0 ~ 86400 for Inform Interval.
Certification Setup	The **default** box is selected by default	You can leave it as **default** or select an expected certificate and key from the drop down list. Refer to **Object Definition > Certificate** Section for the Certificate configuration.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **Undo** to cancel the modifications.

When you finish set **ACS URL ACS Username ACS Password,** your router (CPE, Client Premium Equipment) can send inform to ACS Server.

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

Enable STUN Server



STUN Settings [Help]

Item	Setting
STUN	☑ Enable
Server Address	
Server Port	3478 (1~65535)
Keep Alive Period	0 (0~65535)second(s)

STUN Settings Configuration

Item	Value setting	Description
STUN	The box is checked by default	Check the **Enable** box to activate STUN function.
Server Address	1. String format: any IPv4 address 2. It is an optional item.	Specify the IP address for the expected STUN Server.
Server Port	1. An optional setting 2.**3478** is set by default	Specify the port number for the expected STUN Server. *Value Range*: 1 ~ 65535.
Keep Alive Period	1. An optional setting 2.**0** is set by default	Specify the keep alive time period for the connection with STUN Server. *Value Range*: 0 ~ 65535.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **Undo** to cancel the modifications.

5.1.3 SNMP

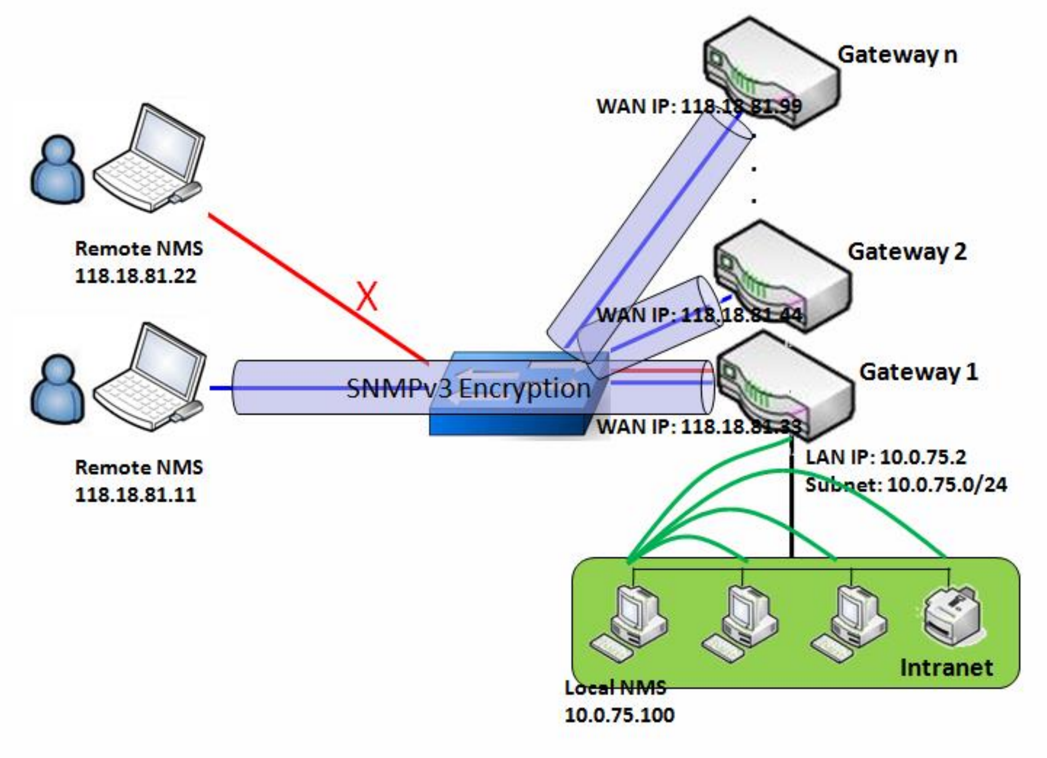
In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

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

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

The device supports several public MIBs and one private MIB for the SNMP agent. The supported MIBs are as follow: MIB-II (RFC 1213, Include IPv6), IF-MIB, IP-MIB, TCP-MIB, UDP-MIB, SMIv1 and SMIv2, SNMPv2-TM and SNMPv2-MIB, and AMIB (a Proprietary MIB)

SNMP Management Scenario



Scenario Application Timing

- There are two application scenarios of SNMP Network Management Systems (NMS).
- Local NMS is in the Intranet and manage all devices that support SNMP protocol in the Intranet. Another one is the Remote NMS to manage some devices whose WAN interfaces are connected together by

using a switch or a router with UDP forwarding.

- If you want to manage some devices and they all have supported SNMP protocol, use either one application scenario, especially the management of devices in the Intranet.
- In managing devices in the Internet, the TR-069 is the better solution. Please refer to last sub-section.

Scenario Description

- The NMS server can monitor and configure the managed devices by using SNMP protocol, and those devices are located at where UDP packets can reach from NMS.
- The managed devices report urgent trap events to the NMS servers.
- Use SNMPv3 version of protocol can protected the transmitting of SNMP commands and responses.
- The remote NMS with privilege IP address can manage the devices, but other remote NMS can't.

Parameter Setup Example

- Following tables list the parameter configuration as an example for the Gateway 1 in above diagram with "SNMP" enabling at LAN and WAN interfaces.
- Use default value for those parameters that are not mentioned in the tables.

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

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

Scenario Operation Procedure

- In above diagram, the NMS server can manage multiple devices in the Intranet or a UDP-reachable network. The "Gateway 1" is one of the managed devices, and it has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. It serves as a NAT router.
- At first stage, the NMS manager prepares related information for all managed devices and records them in the NMS system. Then NMS system gets the status of all managed devices by using SNMP get commands.
- When the manager wants to configure the managed devices, the NMS system allows him to do that by using SNMP set commands. The "UserName1" account is used if the manager uses SNMPv3 protocol

for configuring the "Gateway 1". Only the "UserName1" account can let the "Gateway 1" accept the configuration from the NMS since the authority of the account is "Read/Write".

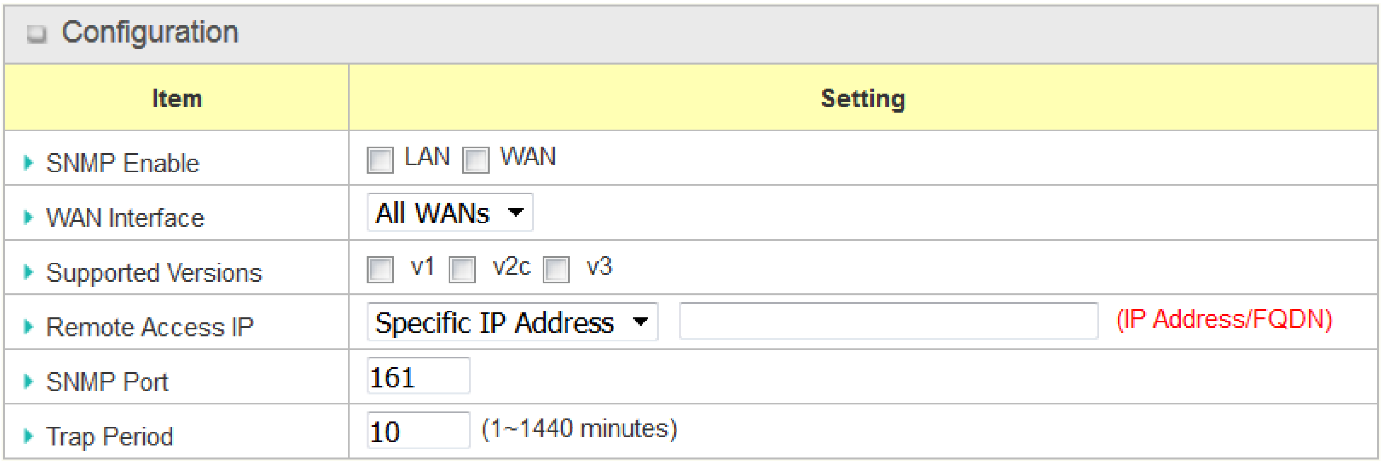
- Once a managed device has an urgent event to send, the device will issue a trap to the Trap Event Receivers. The NMS itself could be one among them.
- If you want to secure the transmitted SNMP commands and responses between the NMS and the managed devices, use SNMPv3 version of protocol.
- The remote NMS without privilege IP address can't manage the "Gateway 1", since "Gateway 1" allows only the NMS with privilege IP address can manage it via its WAN interface.

SNMP Setting

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

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

Enable SNMP



Configuration

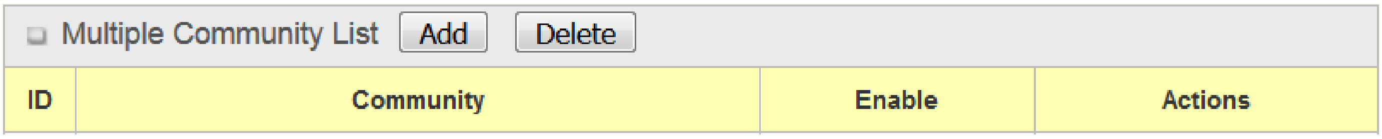
Item	Setting
SNMP Enable	□ LAN □ WAN
WAN Interface	All WANs ▾
Supported Versions	□ v1 □ v2c □ v3
Remote Access IP	Specific IP Address ▾ (IP Address/FQDN)
SNMP Port	161
Trap Period	10 (1~1440 minutes)

SNMP		
Item	**Value setting**	**Description**
SNMP Enable	1.The boxes are unchecked by default	Select the interface for the SNMP and enable SNMP functions. When Check the **LAN** box, it will activate SNMP functions and you can access SNMP from LAN side; When Check the **WAN** box, it will activate SNMP functions and you can access SNMP from WAN side.
WAN Interface	1.A Must filled setting **2. ALL WANs is selected by default**	Specify the WAN interface that a remote SNMP host can access to the device. By default, **All WANs** is selected, and there is no limitation for the WAN interface.

Supported Versions	1.A Must filled setting 2.The boxes are unchecked 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 Access IP	1. String format: any IPv4 address 2. It is an optional item.	Specify the **Remote Access IP** for WAN. Select **Specific IP Address**, and fill in a certain IP address. It means only this IP address can access SNMP from LAN/WAN side. Select **IP Range**, and fill in a range of IP addresses. It means the IP address within specified range can access SNMP from LAN/WAN side. If you left it as blank, it means any IP address can access SNMP from WAN side.
SNMP Port	1. String format: any port number 2. The default SNMP port is **161**. 3. A Must filled setting	Specify the **SNMP Port**. You can fill in any port number. But you must ensure the port number is not to be used. *Value Range*: 1 ~ 65535.
Trap Period	1.A Must filled setting 2. The default Trap Period is 10 minutes	Specify the **Trap Period** in minutes. *Value Range*: 1 ~ 1440.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

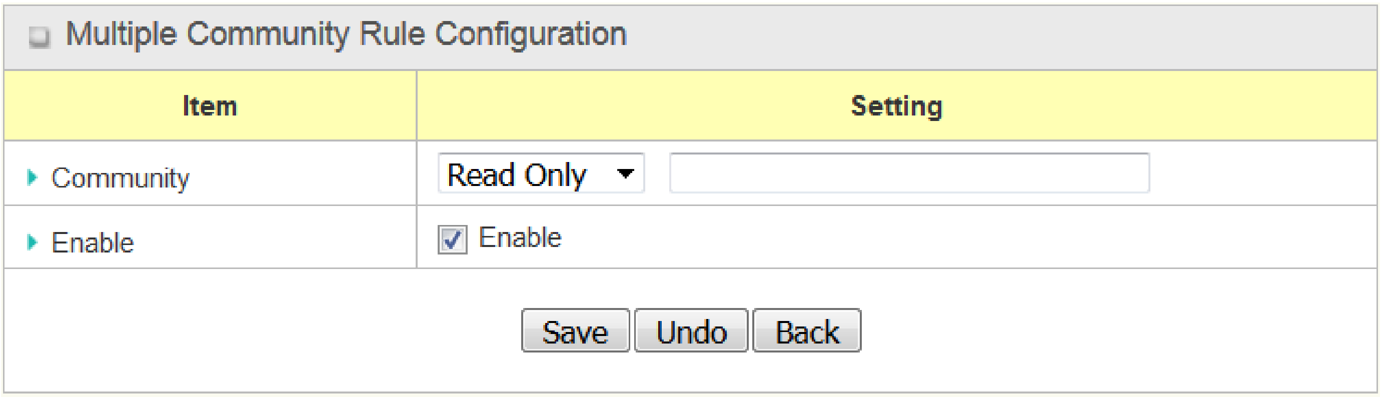
Create/Edit Multiple Community

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.



ID	Community	Enable	Actions

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



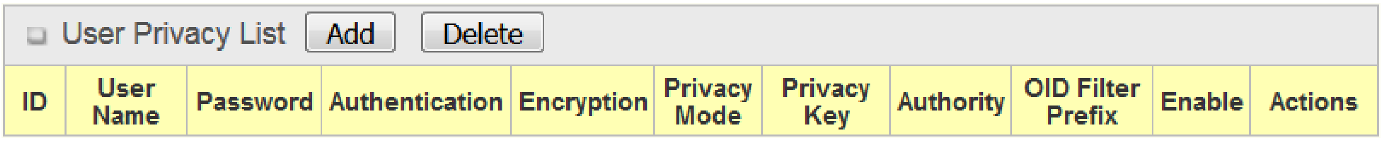
Multiple Community Rule Configuration

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

Create/Edit User Privacy

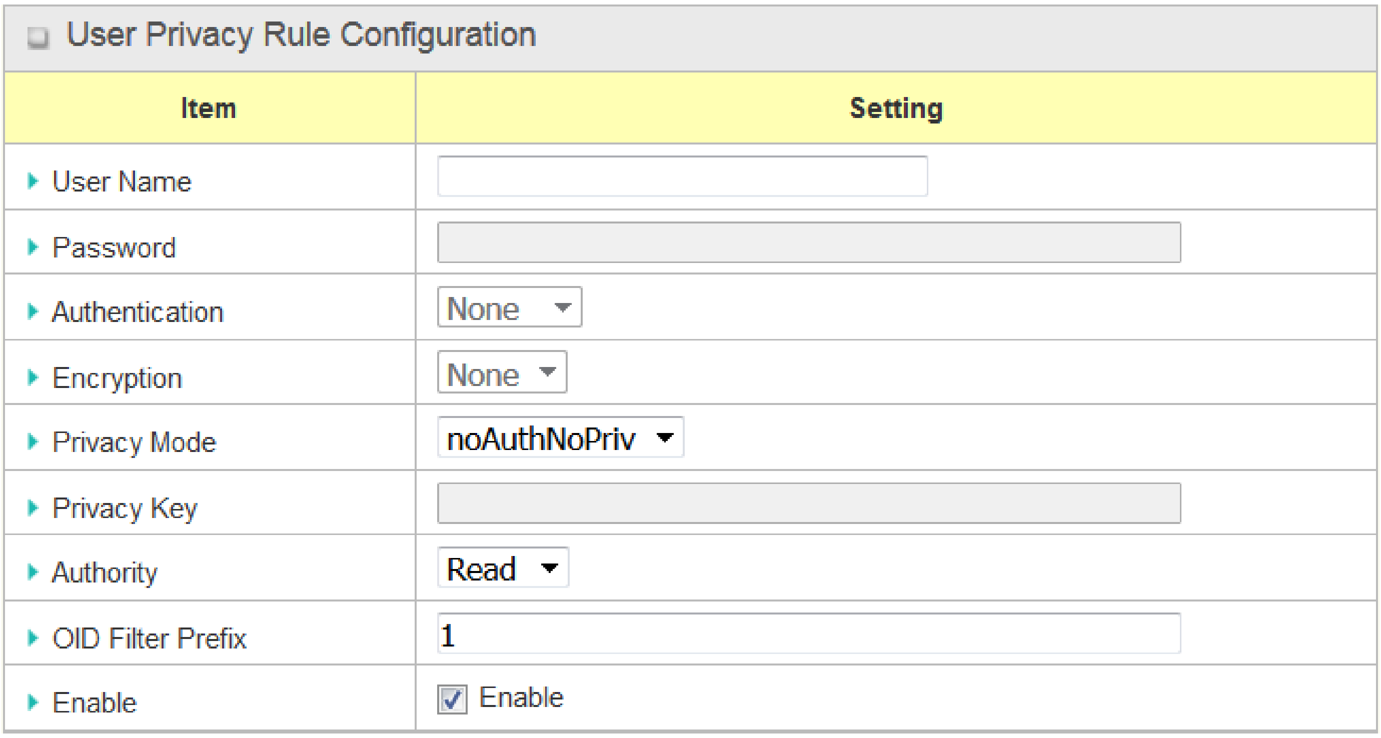
The SNMP allows you to custom your access control for version 3 user. The router supports up to a maximum of 128 User Privacy sets.



User Privacy List

ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	OID Filter Prefix	Enable	Actions

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



User Privacy Rule Configuration

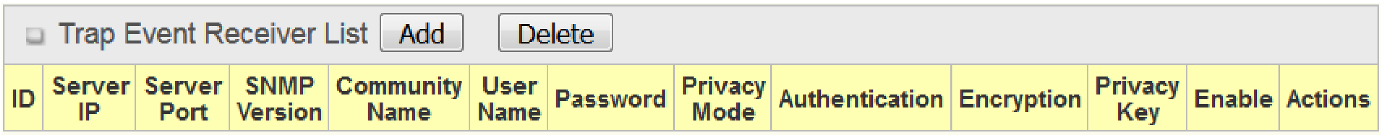
Item	Setting
User Name	
Password	
Authentication	None
Encryption	None
Privacy Mode	noAuthNoPriv
Privacy Key	
Authority	Read
OID Filter Prefix	1
Enable	☑ Enable

User Privacy Rule Configuration		
Item	**Value setting**	**Description**
User Name	1. A Must filled setting 2. String format: any text	Specify the **User Name** for this version 3 user. ***Value Range***: 1 ~ 32 characters.
Password	1. String format: any text	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Password** for this version 3 user. ***Value Range***: 8 ~ 64 characters.
Authentication	1. **None** is selected by default	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Authentication** types for this version 3 user. Selected the authentication types **MD5/ SHA-1** to use.
Encryption	1. **None** is selected by default	When your **Privacy Mode** is **authPriv**, you must specify the **Encryption** protocols for this version 3 user. Selected the encryption protocols **DES / AES** to use.
Privacy Mode	1. **noAuthNoPriv** is selected by default	Specify the **Privacy Mode** for this version 3 user. Selected the **noAuthNoPriv**. You do not use any authentication types and encryption protocols. Selected the **authNoPriv**. You must specify the **Authentication** and **Password**. Selected the **authPriv**. You must specify the Authentication, Password, Encryption and Privacy Key.
Privacy Key	1. String format: any text	When your **Privacy Mode** is **authPriv**, you must specify the **Privacy Key** (8 ~ 64 characters) for this version 3 user.
Authority	1. **Read** is selected by default	Specify this version 3 user's **Authority** that will be allowed **Read Only** (GET and GETNEXT) or **Read-Write** (GET, GETNEXT and SET) access respectively.

OID Filter Prefix	1. The default value is 1 2. A Must filled setting 3. String format: any legal OID	The **OID Filter Prefix** restricts access for this version 3 user to the sub-tree rooted at the given OID. ***Value Range***: 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 the **Undo** button to cancel the settings
Back	N/A	Click the **Back** button to return the last page.

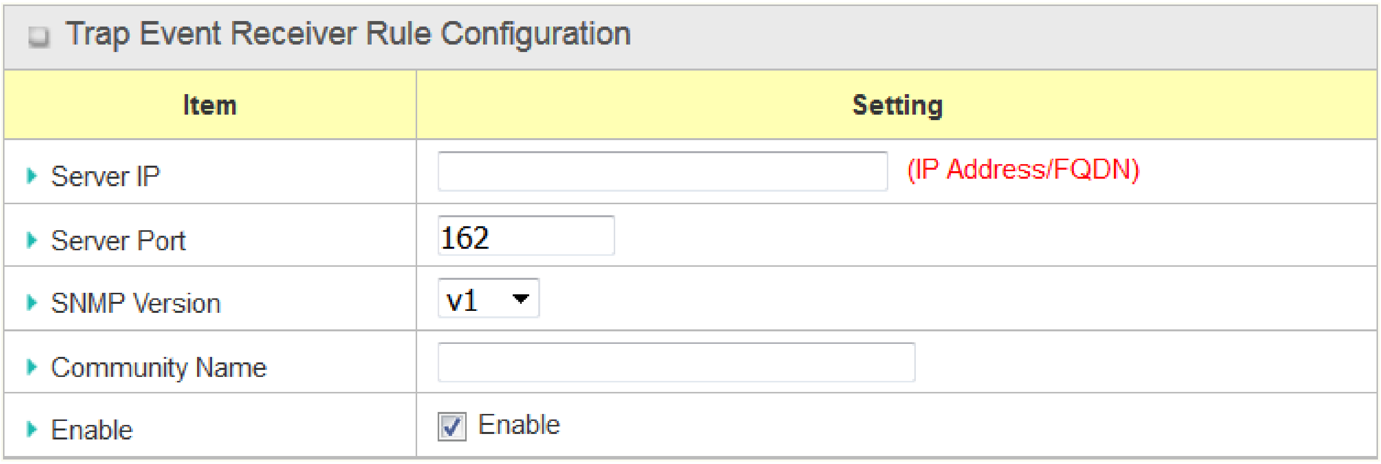
Create/Edit Trap Event Receiver

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



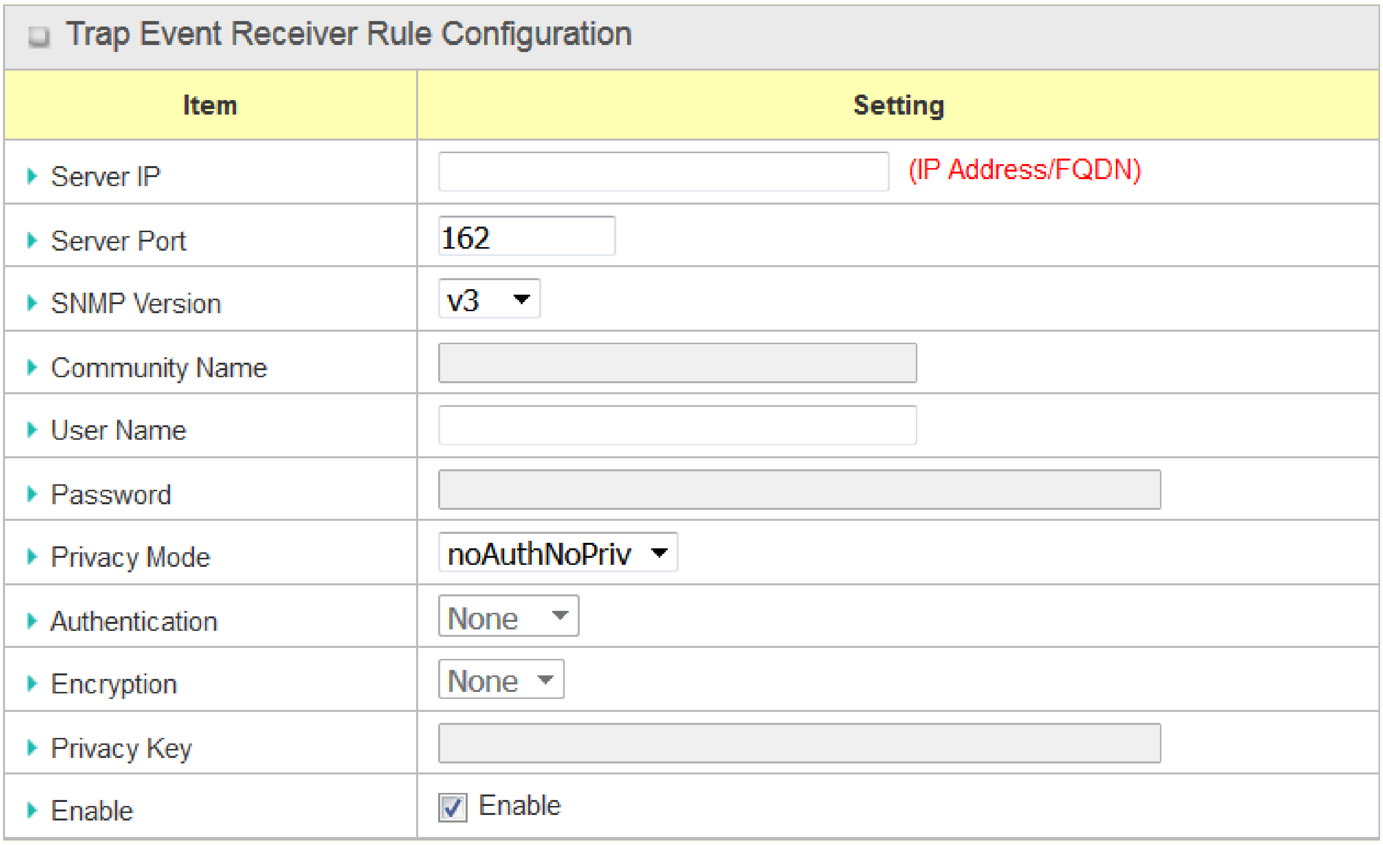
ID	Server IP	Server Port	SNMP Version	Community Name	User Name	Password	Privacy Mode	Authentication	Encryption	Privacy Key	Enable	Actions

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	(IP Address/FQDN)
Server Port	162
SNMP Version	v1
Community Name	
Enable	☑ Enable

When you selected v2c, the configuration screen is exactly the same as that of v1, except the version. When you selected v3, the configuration screen will provide more setting items for the version 3 Trap.



Trap Event Receiver Rule Configuration

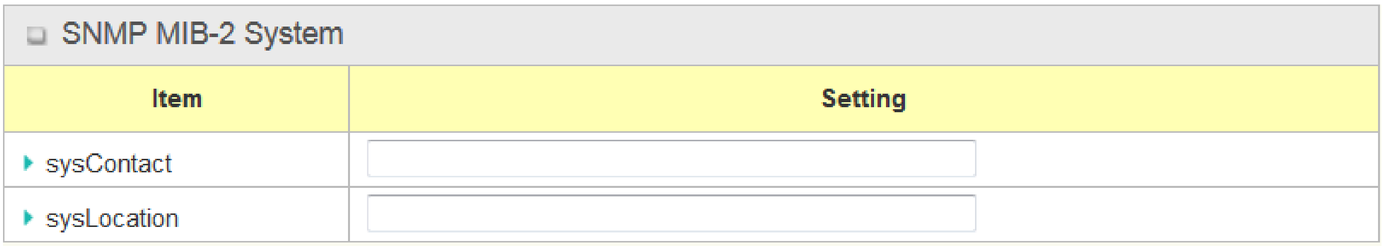
Item	Setting
Server IP	(IP Address/FQDN)
Server Port	162
SNMP Version	v3
Community Name	
User Name	
Password	
Privacy Mode	noAuthNoPriv
Authentication	None
Encryption	None
Privacy Key	
Enable	☑ Enable

Trap Event Receiver Rule Configuration		
Item	**Value setting**	**Description**
Server IP	1. A Must filled setting 2. String format: any IPv4 address or FQDN	Specify the trap **Server IP** or **FQDN**. The DUT will send trap to the server IP/FQDN.
Server Port	1. String format: any port number 2. The default SNMP trap port is 162 3. A Must filled setting	Specify the trap **Server Port**. You can fill in any port number. But you must ensure the port number is not to be used. *Value Range*: 1 ~ 65535.
SNMP Version	1. **v1** is selected by default	Select the version for the trap Selected the **v1**. The configuration screen will provide the version 1 must filled items. Selected the **v2c**. The configuration screen will provide the version 2c must filled items. Selected the **v3**. The configuration screen will provide the version 3 must filled items.
Community Name	1. A **v1** and **v2c** Must filled setting 2. String format: any text	Specify the **Community Name** for this version 1 or version v2c trap. ***Value Range***: 1 ~ 32 characters.

User Name	1. A **v3** Must filled setting 2. String format: any text	Specify the **User Name** for this version 3 trap. ***Value Range***: 1 ~ 32 characters.
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. ***Value Range***: 8 ~ 64 characters.
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** (8 ~ 64 characters) for this version 3 trap.
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 the **Undo** button to cancel the settings.
Back	N/A	Click the **Back** button to return the last page.

Specify SNMP MIB-2 System

If required, you can also specify the required information the MIB-2 System.



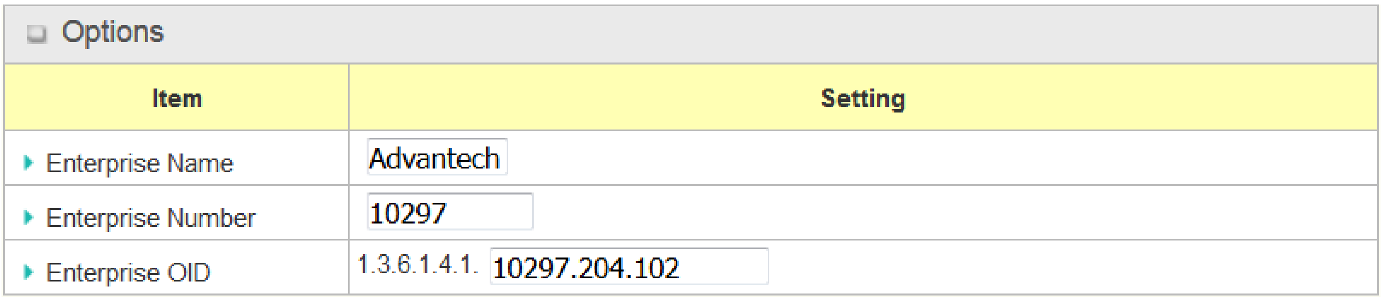
SNMP MIB-2 System

Item	Setting
sysContact	
sysLocation	

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

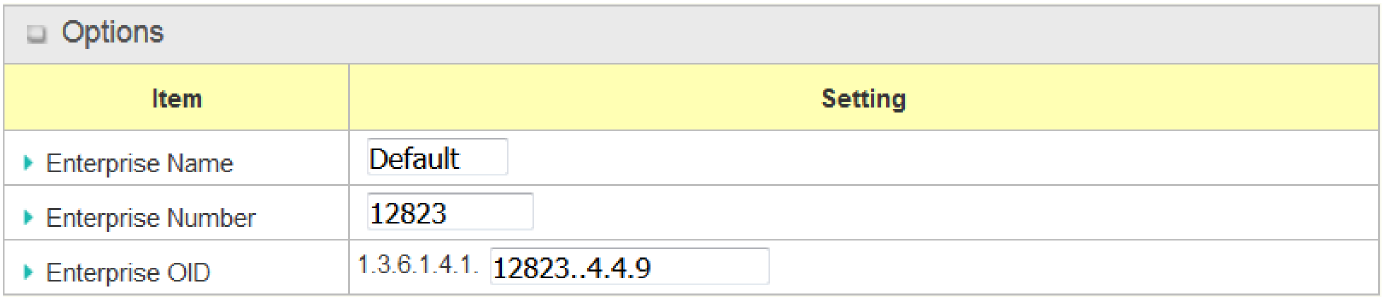
Edit SNMP Options

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



Options

Item	Setting
Enterprise Name	Advantech
Enterprise Number	10297
Enterprise OID	1.3.6.1.4.1. 10297.204.102



Options

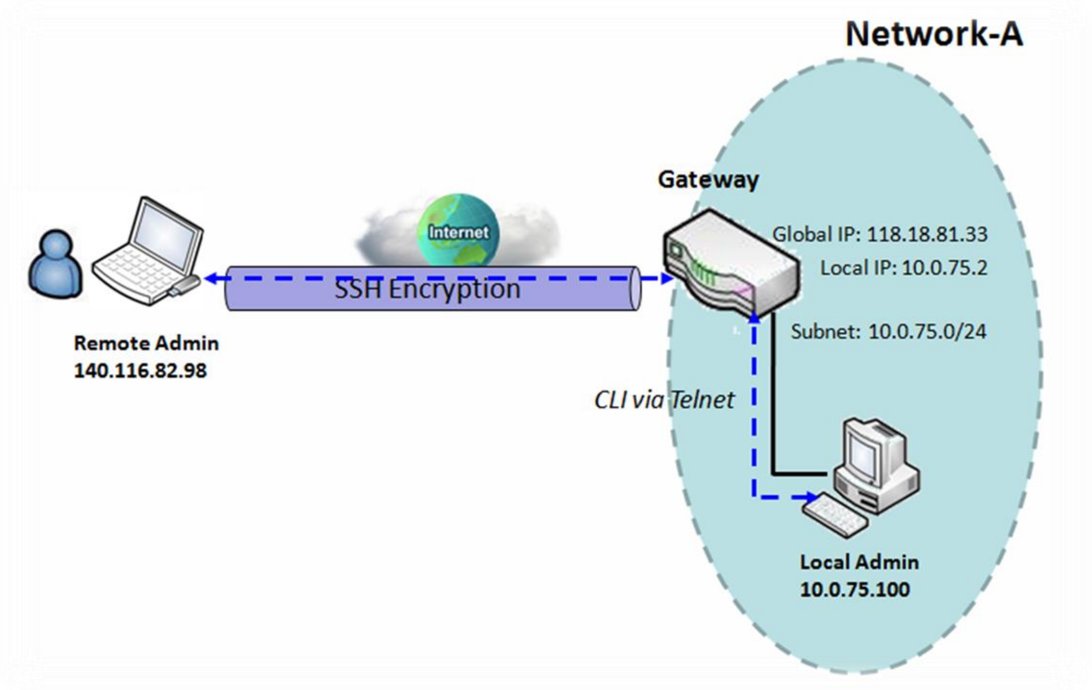
Item	Setting
Enterprise Name	Default
Enterprise Number	12823
Enterprise OID	1.3.6.1.4.1. 12823..4.4.9

Options		
Item	**Value setting**	**Description**
Enterprise Name	1. The default value is **Default** 2. A Must filled setting 3. String format: any text	Specify the **Enterprise Name** for the particular private MIB. ***Value Range*:** 1 ~ 10 characters, and only string with A~Z, a~z, 0~9, ’–‘, ‘_’.
Enterprise Number	The default value is 12823 (Default Enterprise Number) 2. A Must filled setting 3. String format: any number	Specify the **Enterprise Number** for the particular private MIB. ***Value Range*:** 1 ~2080768.
Enterprise OID	1. The default value is 1.3.6.1.4.1.**12823.4.4.9** (Default Enterprise OID) 2. A Must filled setting 3. String format: any legal OID	Specify the **Enterprise OID** for the particular private MIB. 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 the **Undo** button to cancel the settings.

5.1.4 Telnet & SSH

A command-line interface (CLI), also known as command-line user interface, and console user interface are means of interacting with a computer program where the user (or client) issues commands to the program in the form of successive lines of text (command lines). The interface is usually implemented with a command line shell, which is a program that accepts commands as text input and converts commands to appropriate operating system functions. Programs with command-line interfaces are generally easier to automate via scripting. The device supports both Telnet and SSH (Secure Shell) CLI with default service port 23 and 22, respectively.

Telnet & SSH Scenario



Scenario Application Timing

- When the administrator of the gateway wants to manage it from remote site in the Intranet or Internet, he may use "Telnet with CLI" function to do that by using "Telnet" or "SSH" utility.

Scenario Description

- The Local Admin or the Remote Admin can manage the Gateway by using "Telnet" or "SSH" utility with privileged user name and password.
- The data packets between the Local Admin and the Gateway or between the Remote Admin and the Gateway can be plain texts or encrypted texts. Suggest they are plain texts in the Intranet for Local Admin to use "Telnet" utility, and encrypted texts in the Internet for Remote Admin to use "SSH" utility.

Parameter Setup Example

- Following table lists the parameter configuration as an example for the Gateway in above diagram with "Telnet with CLI" enabling at LAN and WAN interfaces.
- Use default value for those parameters that are not mentioned in the table.

Configuration Path	[Telnet & SSH]-[Configuration]
Telnet	LAN: ■ ***Enable*** WAN: □ ***Enable*** Service Port: ***23***
SSH	LAN: ■ ***Enable*** WAN: ■ ***Enable*** Service Port: ***22***

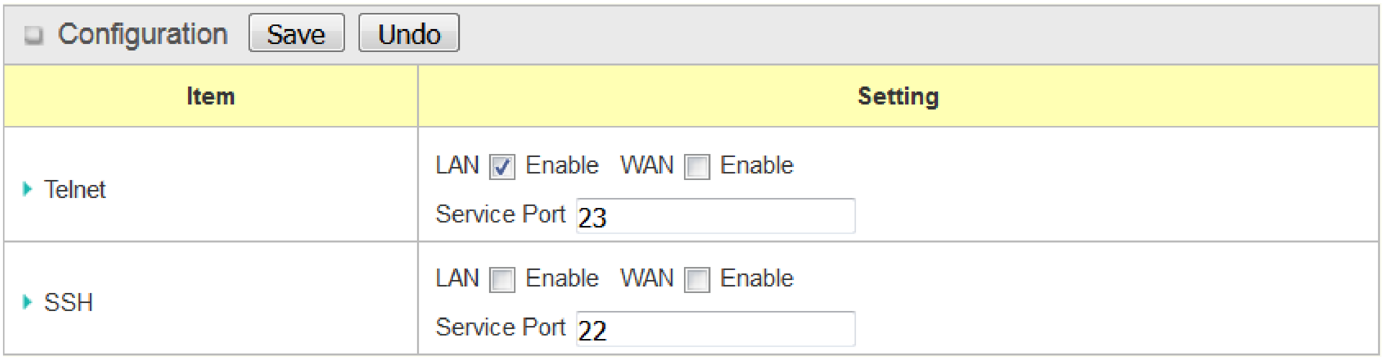
Scenario Operation Procedure

- In above diagram, "Local Admin" or "Remote Admin" can manage the "Gateway" in the Intranet or Internet. The "Gateway" is the gateway of Network-A, and the subnet of its Intranet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for LAN interface and 118.18.81.33 for WAN-1 interface. It serves as a NAT gateway.
- The "Local Admin" in the Intranet uses "Telnet" utility with privileged account to login the Gateway.
- Or the "Remote Admin" in the Internet uses "SSH" utility with privileged account to login the Gateway.
- The administrator of the gateway can control the device as like he is in front of the gateway.

Telnet & SSH Setting

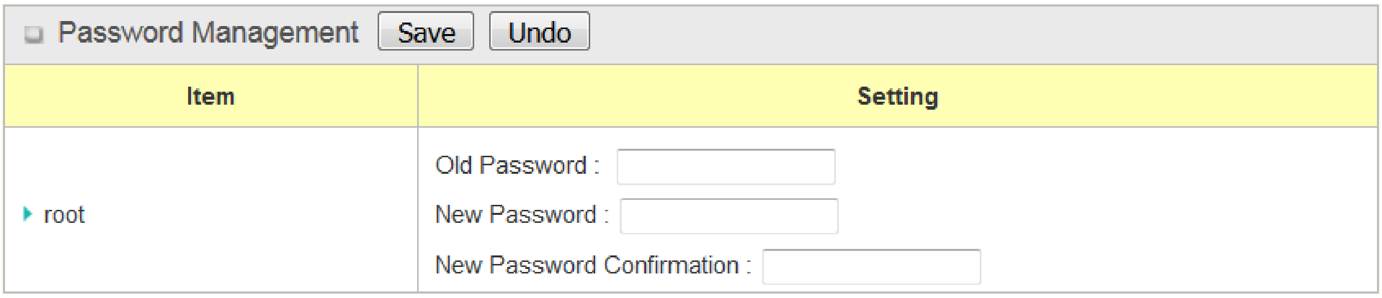
Go to **Administration > Configure & Manage > Telnet & SSH** tab.

The Telnet & SSH setting allows administrator to access this device through the traditional Telnet or SSH Telnet program. Before you can telnet (login) to the device, please configure the related settings and password with care. The password management part allows you to set root password for logging telnet and SSH.



Item	Setting
Telnet	LAN ☑ Enable WAN □ Enable Service Port 23
SSH	LAN □ Enable WAN □ Enable Service Port 22

Configuration		
Item	**Value setting**	**Description**
Telnet	1. The LAN Enable box is checked by default. 2. By default **Service Port** is 23.	Check the **Enable** box to activate the Telnet function for connecting from LAN or WAN interfaces. You can set which number of **Service Port** you want to provide for the corresponding service. ***Value Range***: 1 ~65535.
SSH	3. The LAN Enable box is checked by default. 4. By default **Service Port** is 22.	Check the **Enable** box to activate the SSH Telnet function for connecting from LAN or WAN interfaces. You can set which number of **Service Port** you want to provide for the corresponding service. ***Value Range***: 1 ~65535.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings



Password Management [Save] [Undo]

Item	Setting
root	Old Password : New Password : New Password Confirmation :

Configuration		
Item	**Value setting**	**Description**
root	1. String: any text but no blank character 2. The default password for telnet is '**wirelessm2m**'.	Type old password and specify new password to change root password. ***Note_1: You are highly recommended to change the default telnet password with yours before the device is deployed.*** ***Note_2: If you have trouble for the default password for previous FW version, please check the corresponding User Manual to get the correct one.***
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

5.2 System Operation

System Operation allows the network administrator to manage system, settings such as web-based utility access password change, system information, system time, system log, firmware/configuration backup & restore, and reset & reboot.

5.2.1 Password & MMI

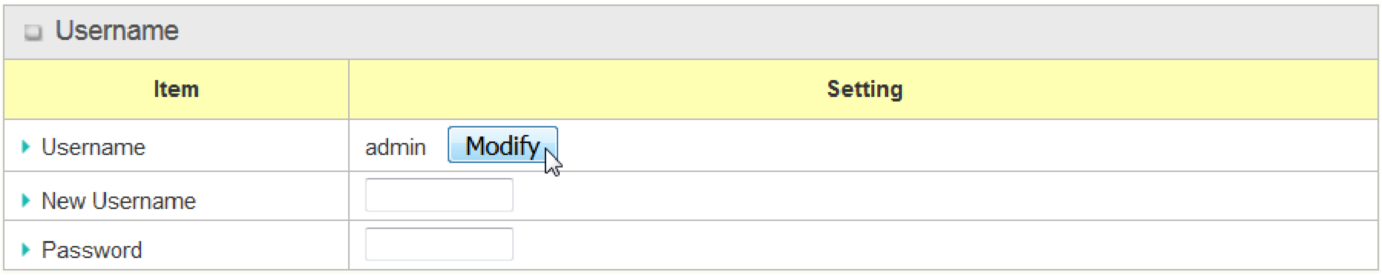
Go to **Administration > System Operation > Password & MMI** tab.

Change Host Name

Change Host Name screen allows network administrator to change the web-based MMI login account to access router.

Change UserName

Change Username screen allows network administrator to change the web-based MMI login account to access router. Click the **Modify** button and provide the new username setting.



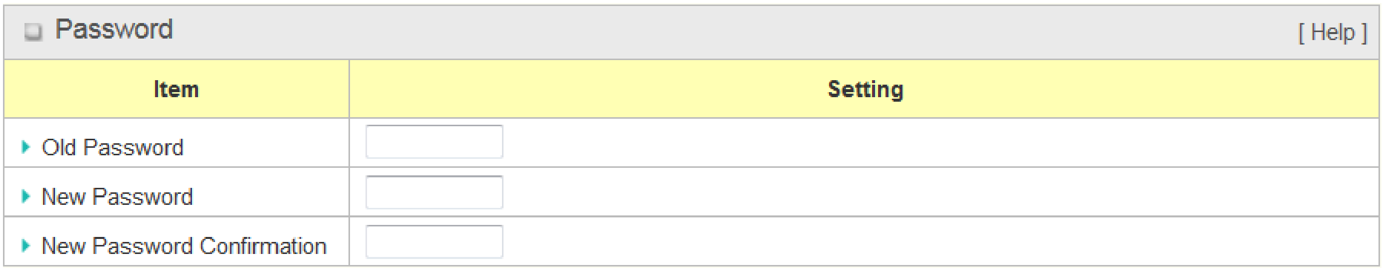
Username

Item	Setting
Username	admin Modify
New Username	
Password	

Username Configuration		
Item	**Value setting**	**Description**
Username	1. The default Username for web-based MMI is '**admin**'.	Display the current MMI login account (Username).
New Username	String: any text	Enter new Username to replace the current setting.
Password	String: any text	Enter current password to verify if you have the permission to change the username setting.
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

Change Password

Change password screen allows network administrator to change the web-based MMI login password to access router.



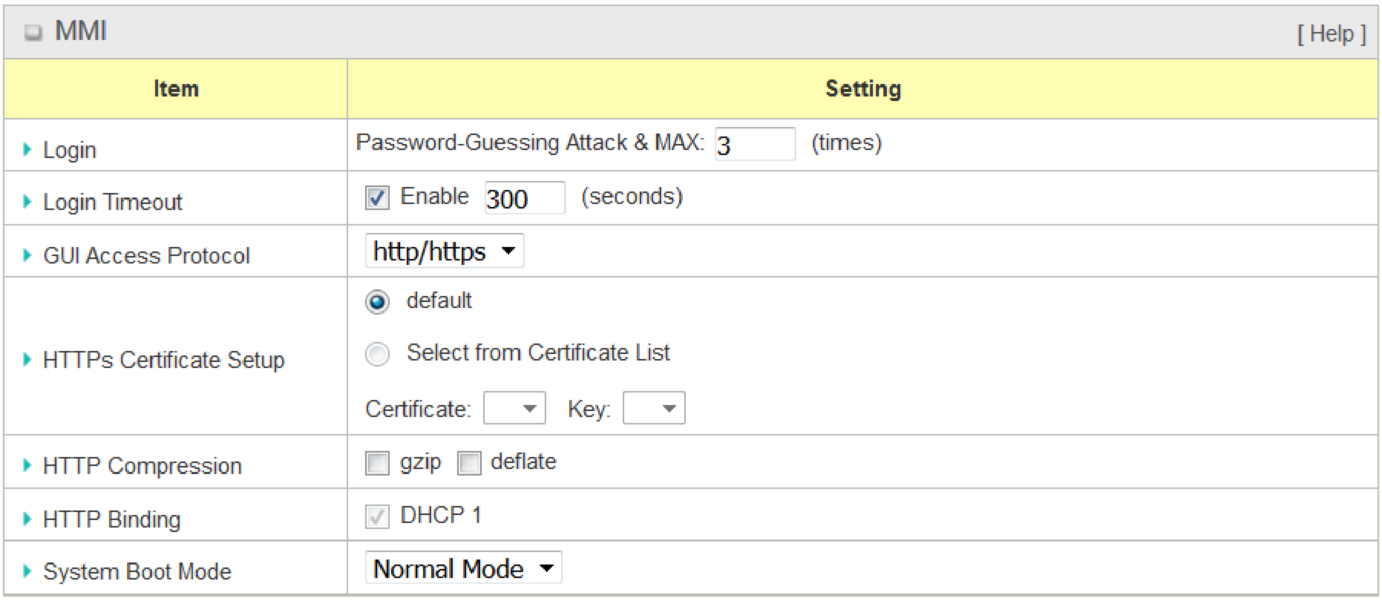
Password [Help]

Item	Setting
Old Password	
New Password	
New Password Confirmation	

Password Configuration		
Item	**Value setting**	**Description**
Old Password	1. String: any text **2. The default password for web-based MMI is 'admin'.**	Enter the current password to enable you unlock to change password.
New Password	String: any text	Enter new password
New Password Confirmation	String: any text	Enter new password again to confirm
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

Change MMI Setting for Accessing

This is the router’s web-based MMI access which allows administrator to access the router for management. The router’s web-based MMI will automatically logout when the idle time has elapsed. The setting allows administrator to enable automatic logout and set the logout idle time. When the login timeout is disabled, the system won’t logout the administrator automatically.



MMI [Help]

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

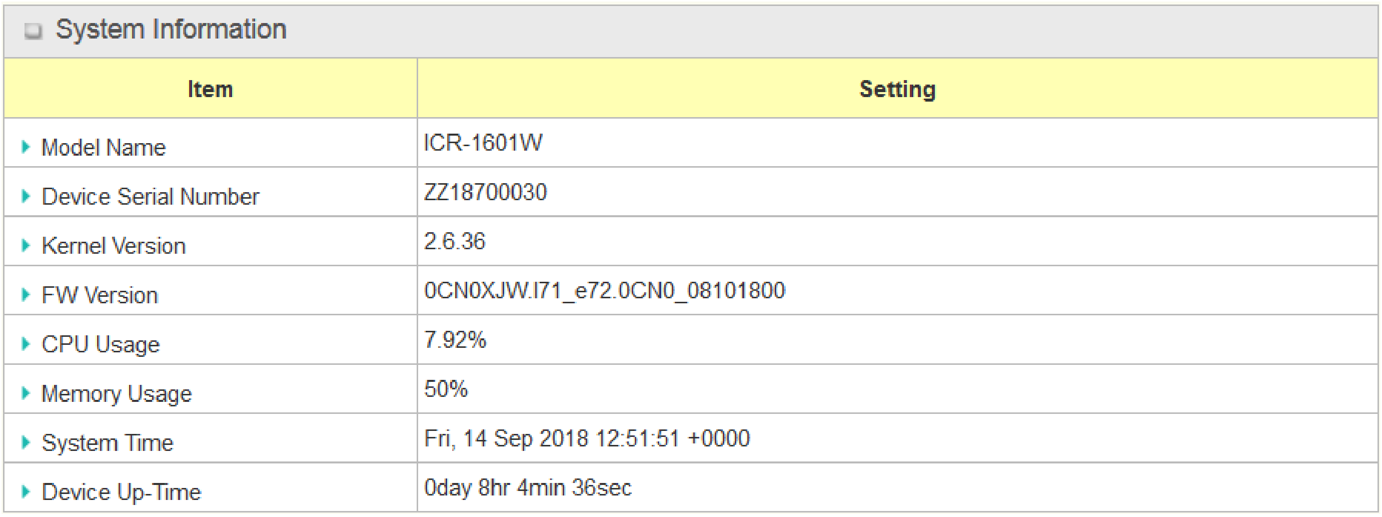
MMI Configuration		
Item	**Value setting**	**Description**
Login	3 times is set by default	Enter the login trial counting value. ***Value Range***: 3 ~ 10. If someone tried to login the web GUI with incorrect password for more than the counting value, an warning message “***Already reaching maximum Password-Guessing times, please wait a few seconds!***” will be displayed and ignore the following login trials.
Login Timeout	The Enable box is checked, and 300 is set by default.	Check the Enable box to activate the auto logout function, and specify the maximum idle time as well. ***Value Range***: 30 ~ 65535.
GUI Access Protocol	**http/https** is selected by default.	Select the protocol that will be used for GUI access. It can be **http/https**, **http only**, or **https only**.
HTTPs Certificate Setup	The **default** box is selected by default	If the https Access Protocol is selected, the HTTPs Certificate Setup option will be available for further configuration. You can leave it as default or select an expected certificate and key from the drop down list. Refer to **Object Definition > Certificate** Section for the Certificate configuration.
HTTP Compression	The box is unchecked by default.	Check the box (**gzip**, or **deflate**) if any compression method is preferred.

HTTP Binding	A Must filled setting	Select **HTTP Binding**.
System Boot Mode	**Normal Mode** is selected by default.	Select the system boot mode that will be adopted to boot up the device. **Normal Mode**: It takes longer boot up time, about 200 seconds, with complete firmware image check during the device booting. **Fast Mode**: It takes shorter boot up time, about 120 seconds, without checking the firmware image during the device booting. **Quick Mode**: It takes shorter boot up time, about 90 seconds, without checking the firmware image and create the internal database for User/Group/Captive Portal functions. **Note**: Use **Quick Mode** with care, once selected, the User/Group/Captive Portal function will become non-functional.
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

5.2.2 System Information

System Information screen gives network administrator a quick look up on the device information for the purchased router.

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



System Information

Item	Setting
Model Name	ICR-1601W
Device Serial Number	ZZ18700030
Kernel Version	2.6.36
FW Version	0CN0XJW.I71_e72.0CN0_08101800
CPU Usage	7.92%
Memory Usage	50%
System Time	Fri, 14 Sep 2018 12:51:51 +0000
Device Up-Time	0day 8hr 4min 36sec

System Information

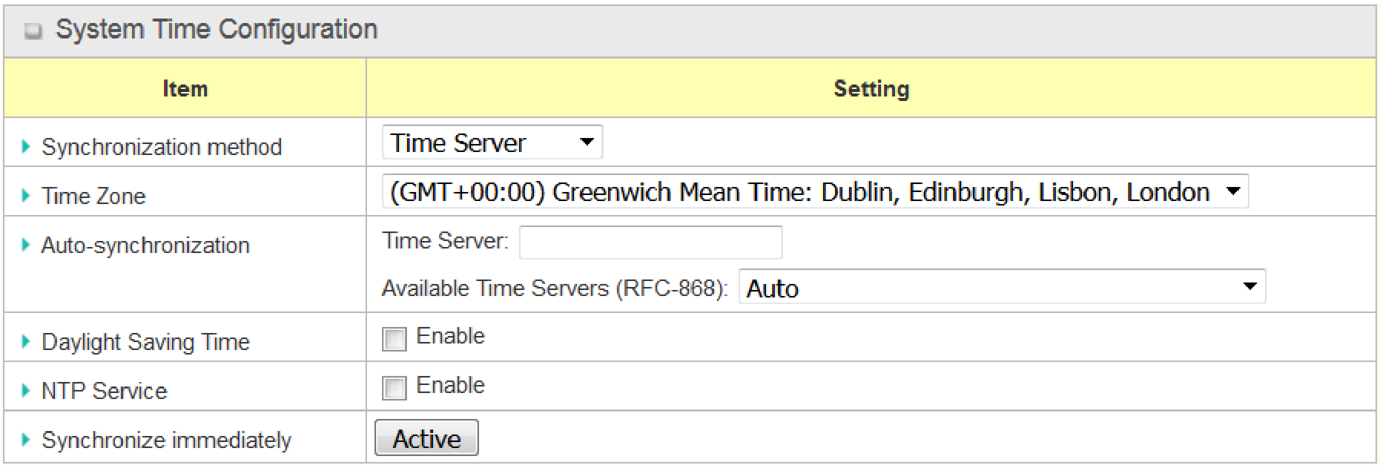
Item	Value Setting	Description
Model Name	N/A	It displays the model name of this product.
Device Serial Number	N/A	It displays the serial number of this product.
Kernel Version	N/A	It displays the Linux kernel version of the product
FW Version	N/A	It displays the firmware version of the product
CPU Usage	N/A	It displays the percentage of CPU utilization.

Memory Usage	N/A	It displays the percentage of device memory utilization.
System Time	N/A	It displays the current system time that you browsed this web page.
Device Up-Time	N/A	It displays the statistics for the device up-time since last boot up.
Refresh	N/A	Click the **Refresh** button to update the system Information immediately.

5.2.3 System Time

The router provides manually setup and auto-synchronized approaches for the administrator to setup the system time for the router.

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



System Time Configuration

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

System Time Information		
Item	**Value Setting**	**Description**
Synchronization method	1. A must fill setting. 2. **Time Server** is selected by default.	Select the synchronization method from **Time Server**, **Manual**, **PC** or **Cellular Module**.
Time Zone	1. It is an optional item. 2. **GMT+00 :00** is selected by default.	Select a time zone where this device locates.
Auto-synchronization	1. Checked by default. 2. Auto is selected by default.	Check the **Enable** button to activate the time auto-synchronization function with a certain NTP server. You can enter the IP or FQDN for the NTP server you expected, or leave it as auto mode so that the available server will be used for time synchronization one by one.
Daylight Saving Time	1. It is an optional item. 2. Un-checked by default	Check the **Enable** button to activate the daylight saving function. When you enabled this function, you have to specify the start date and end date for the daylight saving time duration.
Set Date & Time	1. It is an optional item.	If you do not enable the time auto-synchronization function, you can also manually set the date (Year/Month/Day) and time (Hour:Minute:Second).
NTP Service	1. Unchecked by default. 2. NTP Service is	Check the **Enable** button to activate the NTP service.

	disabled by default.	
Synchronize immediately	N/A	Click the **Active** button to synchronize time immediately.
Save	N/A	Click the **Save** button to save the settings.
Refresh	N/A	Click the **Refresh** button to update the system time immediately.

Instead of manually configuring the system time for the router, there are two simple and quick solutions for you to set the correct time information and set it as the system time for the router.

The first one is “Sync with Timer Server”. Based on your selection of time zone and time server in above time information configuration window, system will communicate with time server by NTP Protocol to get system date and time after you click on the **Sync with Timer Server** button.

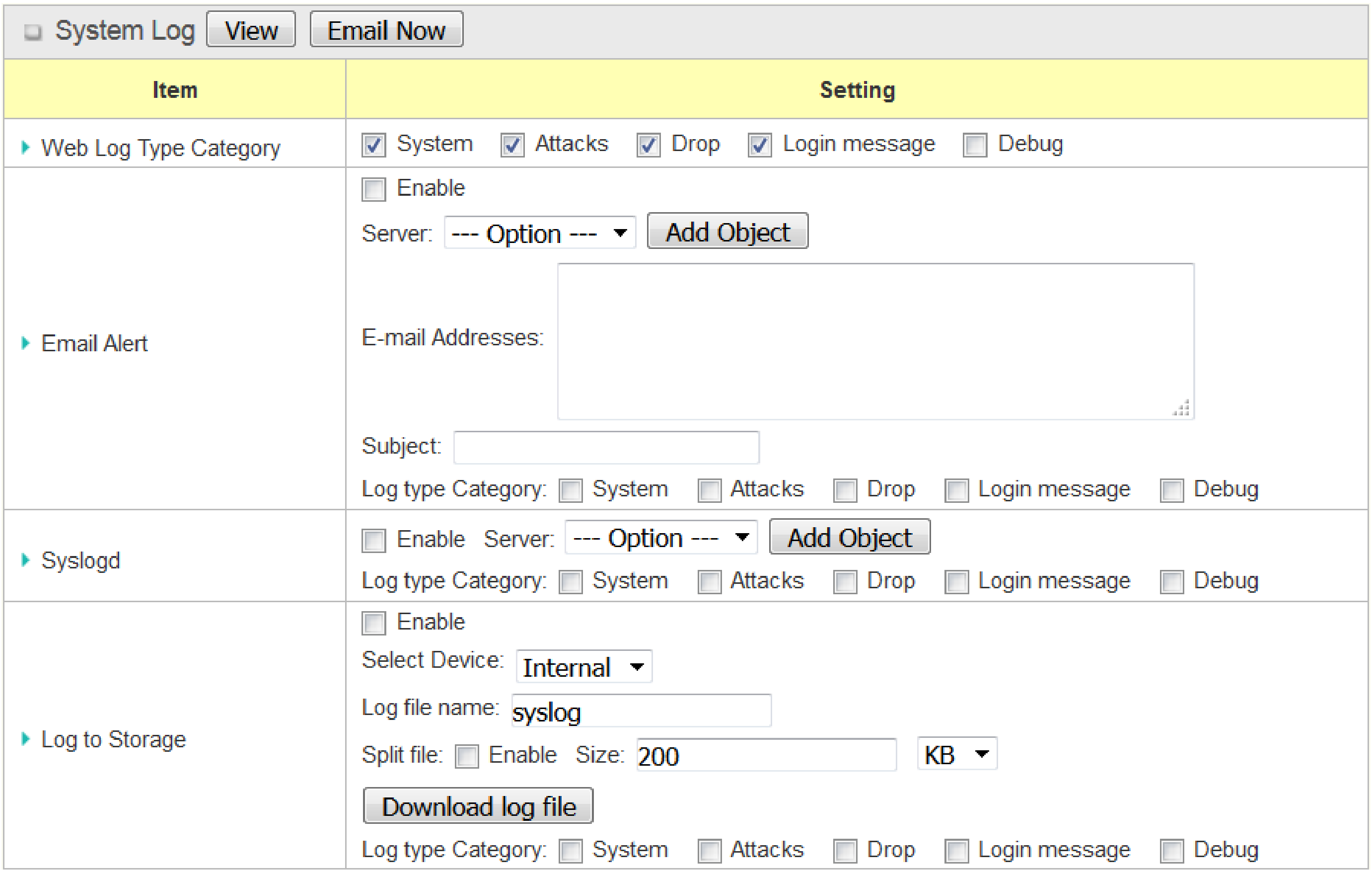
Note: Remember to select a correct time zone for the device, otherwise, you will just get the UTC (Coordinated Universal Time) time, not the local time for the device.

The second one is “Sync with my PC”. Click on the **Sync with my PC** button to let system synchronize its date and time to the time of the administration PC.

5.2.4 System Log

System Log screen contains various event log tools facilitating network administrator to perform local event logging and remote reporting.

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



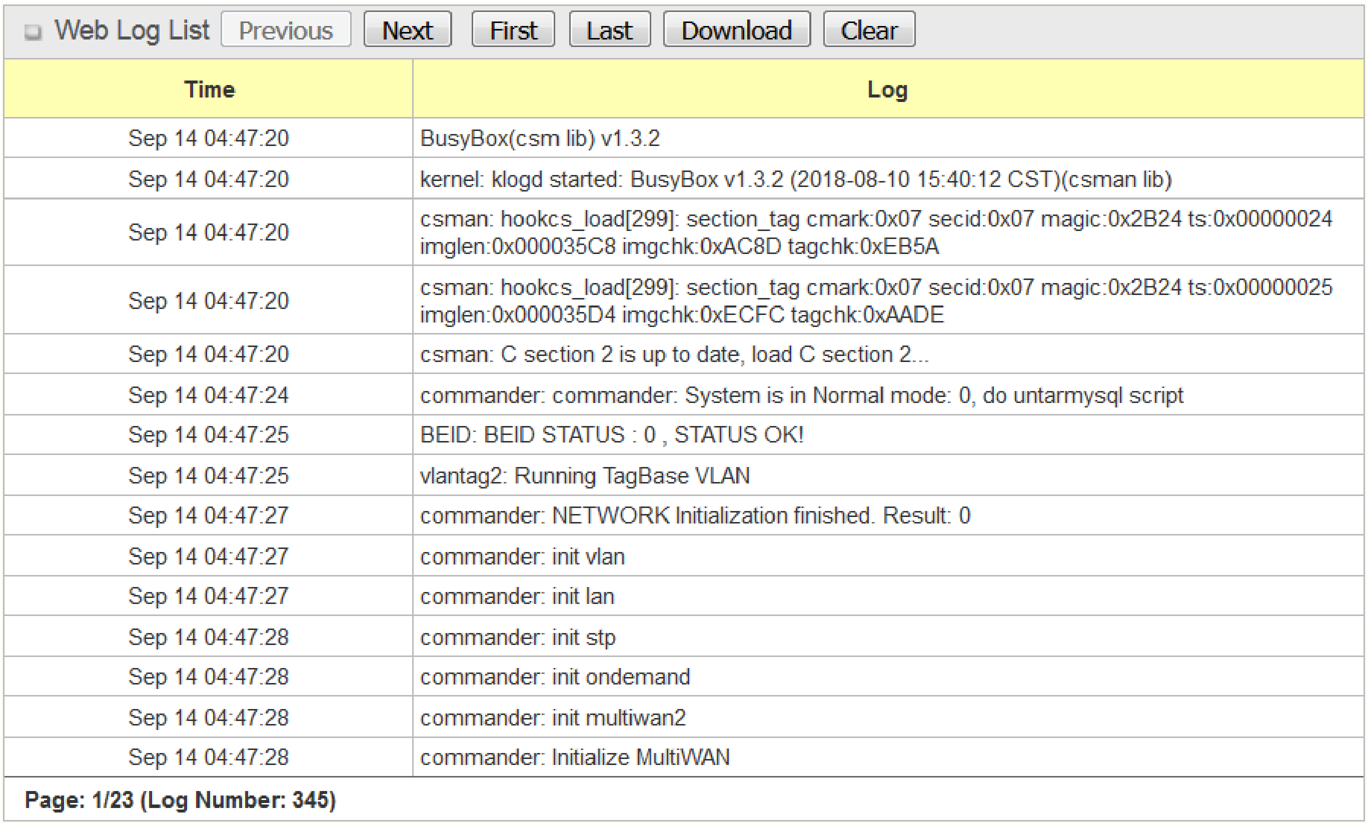
System Log [View] [Email Now]

Item	Setting
Web Log Type Category	☑ System ☑ Attacks ☑ Drop ☑ Login message □ Debug
Email Alert	□ Enable Server: --- Option --- [Add Object] E-mail Addresses: Subject: Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug
Syslogd	□ Enable Server: --- Option --- [Add Object] Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug
Log to Storage	□ Enable Select Device: Internal Log file name: syslog Split file: □ Enable Size: 200 KB [Download log file] Log type Category: □ System □ Attacks □ Drop □ Login message □ Debug

View & Email Log History

View button is provided for network administrator to view log history on the router. **Email Now** button enables administrator to send instant Email for analysis.

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



Time	Log
Sep 14 04:47:20	BusyBox(csm lib) v1.3.2
Sep 14 04:47:20	kernel: klogd started: BusyBox v1.3.2 (2018-08-10 15:40:12 CST)(csman lib)
Sep 14 04:47:20	csman: hookcs_load[299]: section_tag cmark:0x07 secid:0x07 magic:0x2B24 ts:0x00000024 imglen:0x000035C8 imgchk:0xAC8D tagchk:0xEB5A
Sep 14 04:47:20	csman: hookcs_load[299]: section_tag cmark:0x07 secid:0x07 magic:0x2B24 ts:0x00000025 imglen:0x000035D4 imgchk:0xECFC tagchk:0xAADE
Sep 14 04:47:20	csman: C section 2 is up to date, load C section 2...
Sep 14 04:47:24	commander: commander: System is in Normal mode: 0, do untarmysql script
Sep 14 04:47:25	BEID: BEID STATUS : 0 , STATUS OK!
Sep 14 04:47:25	vlantag2: Running TagBase VLAN
Sep 14 04:47:27	commander: NETWORK Initialization finished. Result: 0
Sep 14 04:47:27	commander: init vlan
Sep 14 04:47:27	commander: init lan
Sep 14 04:47:28	commander: init stp
Sep 14 04:47:28	commander: init ondemand
Sep 14 04:47:28	commander: init multiwan2
Sep 14 04:47:28	commander: Initialize MultiWAN

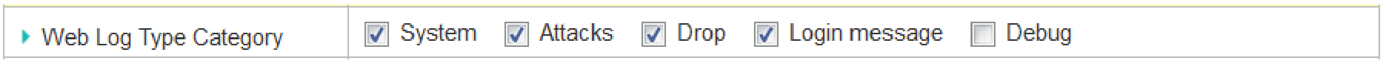
Page: 1/23 (Log Number: 345)

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 the **Back** button to return to the previous page.

Web Log Type Category

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

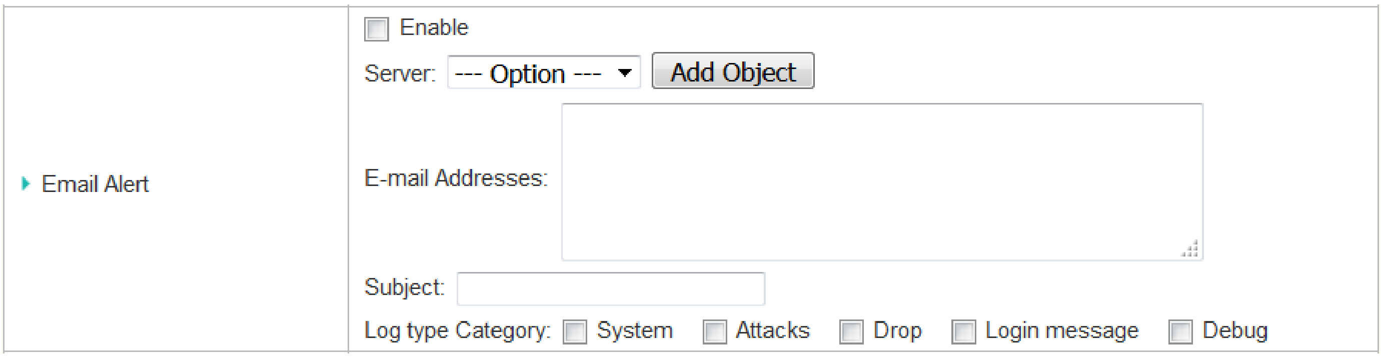


Web Log Type Category ☑ System ☑ Attacks ☑ Drop ☑ Login message □ Debug

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

Email Alert

Email Alert screen allows network administrator to select the type of event to log and be sent to the destined Email account.



Email Alert

□ Enable

Server: --- Option --- Add Object

E-mail Addresses:

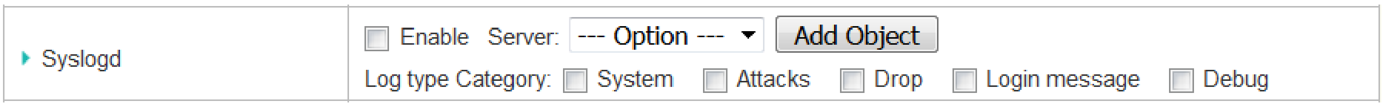
Subject:

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

Email Alert Setting Window		
Item	**Value Setting**	**Description**
Enable	Un-checked by default	Check **Enable** box to enable sending event log messages to destined Email account defined in the E-mail Addresses blank space.
Server	N/A	Select one email server from the Server dropdown box to send Email. If none has been available, click the **Add Object** button to create an outgoing Email server. You may also add an outgoing Email server from Object Definition > External Server > External Server tab.
E-mail address	String : email format	Enter the recipient's Email address. Separate Email addresses with comma ',' or semicolon ' ;' Enter the Email address in the format of '*myemail@domain.com*'
Subject	String : any text	Enter an Email subject that is easy for you to identify on the Email client.
Log type category	Default unchecked	Select the type of events to log and be sent to the designated Email account. Available events are System, Attacks, Drop, Login message, and Debug.

Syslogd

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



▸ Syslogd

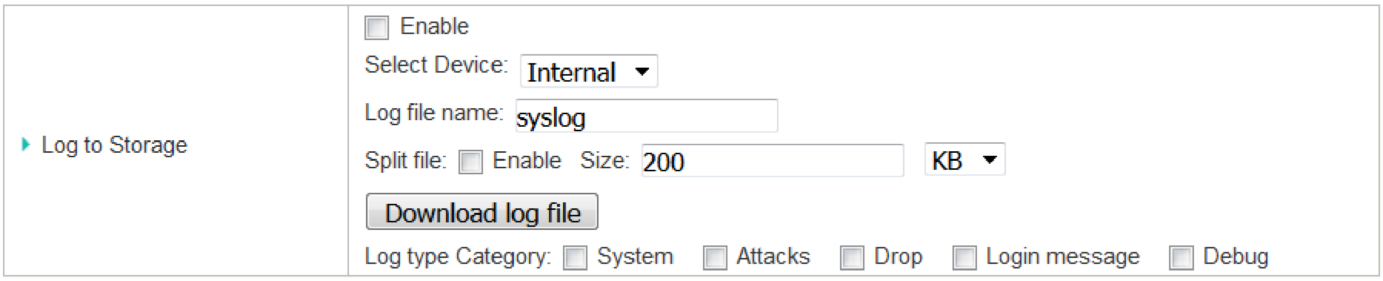
□ Enable Server: --- Option --- ▾ Add Object

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

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

Log to Storage

Log to Storage screen allows network administrator to select the type of events to log and be stored at an internal or an external storage.



▸ Log to Storage

□ Enable

Select Device: Internal ▾

Log file name: syslog

Split file: □ Enable Size: 200 KB ▾

Download log file

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

Log to Storage Setting Window		
Item	**Value Setting**	**Description**
Enable	Un-checked by default	Check to enable sending log to storage.
Select Device	Internal is selected by default	Select internal or external storage.
Log file name	Un-checked by default	Enter log file name to save logs in designated storage.
Split file Enable	Un-checked by default	Check **enable** box to split file whenever log file reaching the specified limit.
Split file Size	**200 KB** is set by default	Enter the file size limit for each split log file. ***Value Range***: 10 ~1000.
Log type category	Un-checked by default	Check which type of logs to send: System, Attacks, Drop, Login message, Debug

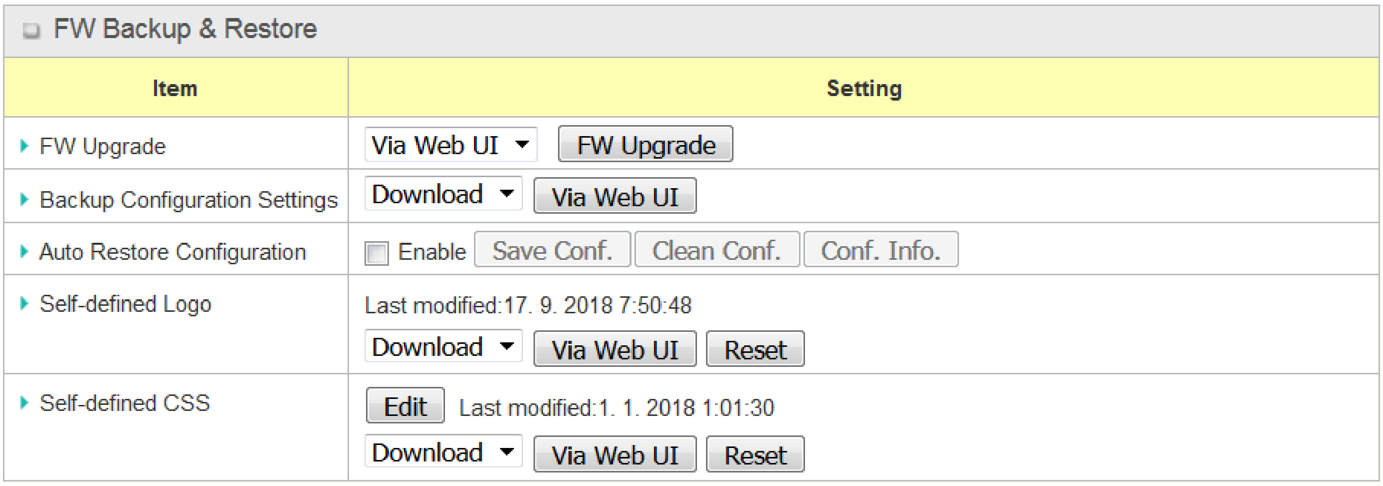
Log to Storage Button Description		
Item	**Value setting**	**Description**
Download log file	N/A	Click the **Download log file** button to download log files to a log.tar file.

5.2.5 Backup & Restore

In the Backup & Restore window, you can upgrade the device firmware when new firmware is available and also backup / restore the device configuration.

In addition to the factory default settings, you can also customize a special configuration setting as a customized default value. With this customized default value, you can reset the device to the expected default setting if needed. Also, the regular Auto Upgrade via HTTP(S)/FTP(S) source is feasible.

Go to **Administration > System Operation > Backup & Restore** tab.



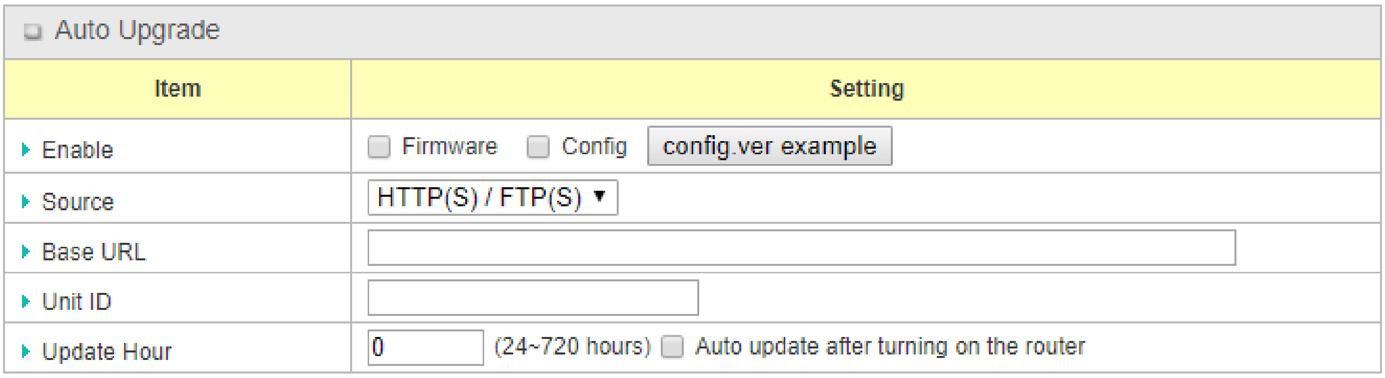
FW Backup & Restore

Item	Setting
FW Upgrade	Via Web UI ▾ [FW Upgrade]
Backup Configuration Settings	Download ▾ [Via Web UI]
Auto Restore Configuration	□ Enable [Save Conf.] [Clean Conf.] [Conf. Info.]
Self-defined Logo	Last modified:17. 9. 2018 7:50:48 Download ▾ [Via Web UI] [Reset]
Self-defined CSS	[Edit] Last modified:1. 1. 2018 1:01:30 Download ▾ [Via Web UI] [Reset]

FW Backup & Restore

Item	Value Setting	Description
FW Upgrade	Via Web UI is selected by default	If new firmware is available, click the **FW Upgrade** button to upgrade the device firmware **via Web UI**, or **Via Storage**. After clicking on the “FW Upgrade” command button, you need to specify the file name of new firmware by using “Browse” button, and then click “Upgrade” button to start the FW upgrading process on this device. If you want to upgrade a firmware which is from GPL policy, please check “Accept unofficial firmware”
Backup Configuration Settings	Download is selected by default	You can backup or restore the device configuration settings by clicking the ***Via Web UI*** button. **Download**: for backup the device configuration to a config.bin file. **Upload**: for restore a designated configuration file to the device. **Via Web UI**: to retrieve the configuration file via Web GUI.
Auto Restore Configuration	The Enable box is unchecked by default	Chick the **Enable** button to activate the customized default setting function. Once the function is activated, you can save the expected setting as a customized default setting by clicking the **Save Conf.** button, or clicking the **Clean Conf.** button to erase the stored customized configuration.
Self-defined Logo	Download is selected by default.	The logo for the web UI can be downloaded or uploaded from or to the router. Note: The file name must be “logo.gif”.
Self-defined CSS	Download is selected by default.	The style of web UI can be downloaded or uploaded from or to the router through the CSS file. The CCS style can also be edited directly by Edit button. Note: The file name must be “wmqa01.css”.

Auto Upgrade via HTTP(S)/FTP(S) source can be configured in the bottom part. If the Firmware or Configuration found on the server is newer than the current one, it will be updated.



Auto Upgrade

Item	Setting
Enable	□ Firmware □ Config config.ver example
Source	HTTP(S) / FTP(S) ▼
Base URL	
Unit ID	
Update Hour	0 (24~720 hours) □ Auto update after turning on the router

Auto Upgrade		
Item	**Value Setting**	**Description**
Enable	The boxes are unchecked by default.	Enable Firmware or Configuration upgrade or both: **Firmware:** the router will look for a newer firmware file and update when found. **Config**: the router will check if there is a configuration file on the remote server with newer date than the current configuration, it will update its configuration to the new settings and reboot. **config .ver example** button will prompt the download of .ver file example needed on server for Config update. See the explanation in **HTTP(S) / FTP(S) Server configuration** part below the table.
Source	HTTP(S) / FTP(S) is selected by default	Select the location of the upgrade files: **HTTP(S) / FTP(S):** Updates are downloaded from the Base URL address below. Used protocol is specified by the address: HTTP, HTTPS, FTP or FTPS.
Base URL	Blank is set by default	IP address from which the configuration file will be downloaded. This option also specifies the communication protocol. Example: **http://**example.com
Unit ID	1. An optional setting 2. Blank is set by default	Name of configuration file (name of the file without extension). If not filled, the MAC address of the router is used as the filename (the dots are used as delimiter instead of colons.)
Update Hour	0 is set by default. The box is unchecked by default.	Set the time (range 24 to 720 hours) to regularly check for updates. If the **Auto update after turning on the router** box is enabled, the check is performed five minutes after every turning on the router (reboot). If the detected firmware or configuration file is newer than the running one, it is downloaded and the router is rebooted automatically.

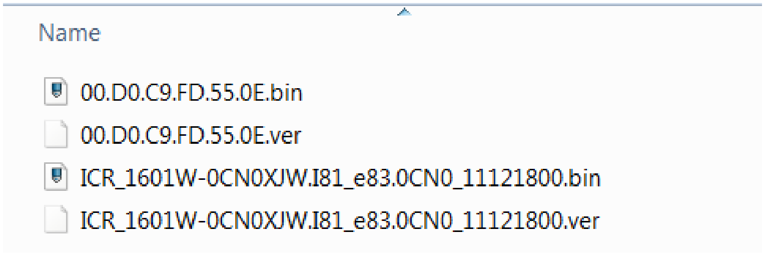
HTTP(S) / FTP(S) Server configuration:

To make Auto Upgrade working, both the Firmware and Config file need to have a .ver file stored in the same folder on HTTP(S) / FTP(S) server. The updates are triggered by the content of the .ver files (newer date).

- For the firmware, the .ver file will comes with the general release. Upload both Firmware files **.bin** and **.ver** in the same folder.

- For the configuration file, .ver file example can be generated by the **config .ver example** button in the Enable row in the router Auto Upgrade configuration. Both **config.bin** and **.ver** files has to be uploaded in the same folder. The name of .ver file and config.bin has to be the same. It can be the chosen Unit ID or MAC (note that when the parameter Unit ID is filled, the configuration filename is defined, and the hardware MAC address name will not be used). Edit the time on .ver file for configuration to make sure the configuration will be updated.

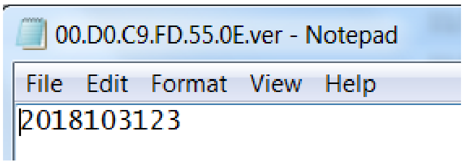
Example of the Firmware and Configuration files on the HTTP(S) / FTP(S) server:



Name

00.D0.C9.FD.55.0E.bin
00.D0.C9.FD.55.0E.ver
ICR_1601W-0CN0XJW.I81_e83.0CN0_11121800.bin
ICR_1601W-0CN0XJW.I81_e83.0CN0_11121800.ver

Example of the configuration .ver file content (date including hours in format YYYYMMDDHH):



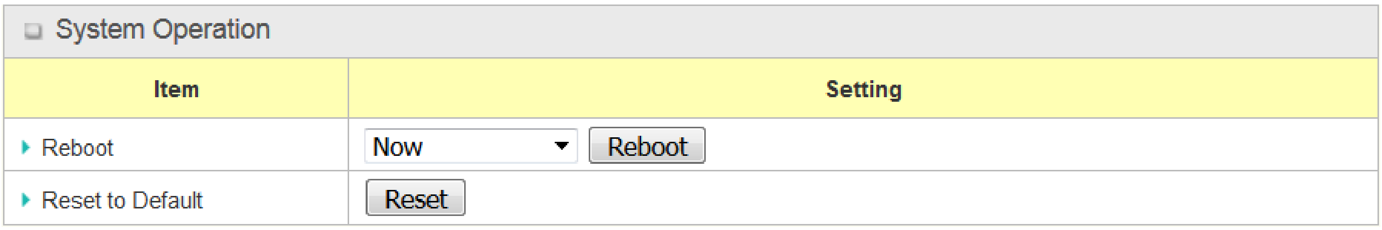
```
2018103123
```

5.2.6 Reboot & Reset

For some special reason or situation, you may need to reboot the router or reset the device configuration to its default value. In addition to perform these operations through the Power ON/OFF, or pressing the reset button on the device panel, you can do it through the web GUI too.

Go to **Administration > System Operation > Reboot & Reset** tab.

In the Reboot & Reset window, you can reboot this device by clicking the “Reboot” button, and reset this device to default settings by clicking the “Reset” button.



System Operation

Item	Setting
Reboot	Now ▾ Reboot
Reset to Default	Reset

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

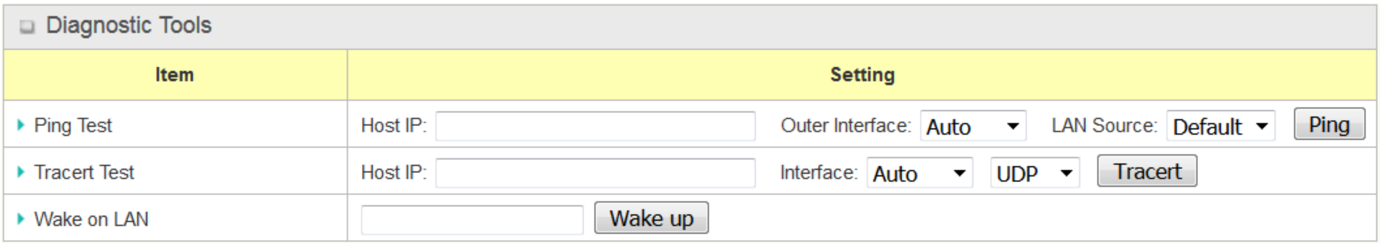
5.3 Diagnostic

This router supports simple network diagnosis tools for the administrator to troubleshoot and find the root cause of the abnormal behavior or traffics passing through the router. There can be a Packet Analyzer to help record the packets for a designated interface or specific source/destination host, and another Ping and **Tracert** tools for testing the network connectivity issues.

5.3.1 Diagnostic Tools

The Diagnostic Tools provide some frequently used network connectivity diagnostic tools (approaches) for the network administrator to check the device connectivity.

Go to **Administration > Diagnostic > Diagnostic Tools** tab.



Diagnostic Tools

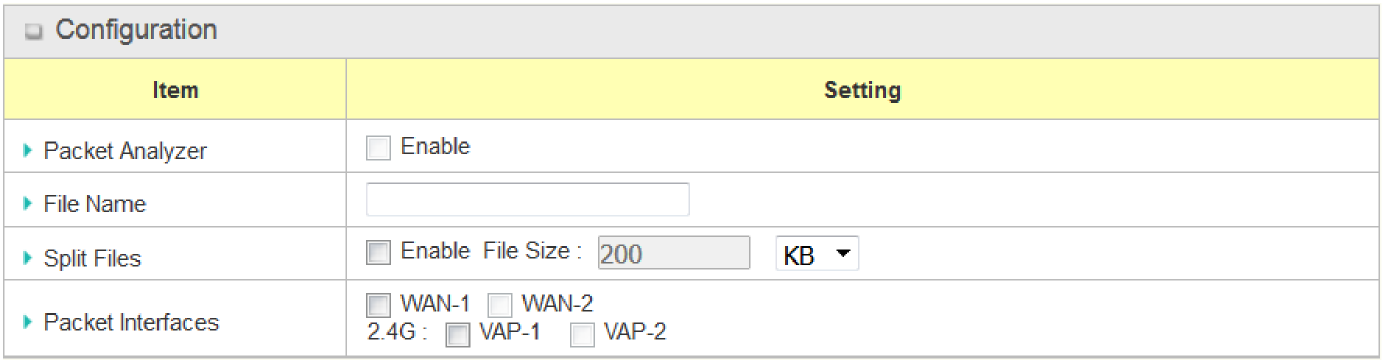
Item	Setting
▸ Ping Test	Host IP: Outer Interface: Auto ▾ LAN Source: Default ▾ Ping
▸ Tracert Test	Host IP: Interface: Auto ▾ UDP ▾ Tracert
▸ Wake on LAN	Wake up

Diagnostic Tools		
Item	**Value setting**	**Description**
Ping Test	Optional Setting	This allows you to specify an IP / FQDN and the test interface (LAN, WAN, or Auto), so system will try to ping the specified device to test whether it is alive after clicking on the **Ping** button. A test result window will appear beneath it.
Tracert Test	Optional setting	Trace route (tracert) command is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Trace route proceeds until all (three) sent packets are lost for more than twice, then the connection is lost and the route cannot be evaluated. First, you need to specify an IP / FQDN, the test interface (LAN, WAN, or Auto) and the protocol (UDP or ICMP), and by default, it is **UDP**. Then, system will try to trace the specified host to test whether it is alive after clicking on **Tracert** button. A test result window will appear beneath it.
Wake on LAN	Optional setting	Wake on LAN (WOL) is an Ethernet networking standard that allows a computer to be turned on or awakened by a network message. You can specify the MAC address of the computer, in your LAN network, to be remotely turned on by clicking on the **Wake up** command button.
Save	N/A	Click the **Save** button to save the configuration.

5.3.2 Packet Analyzer

The Packet Analyzer can capture packets depend on user settings. User can specify interfaces to capture packets and filter by setting rule. Ensure the log storage is available (either embedded SD-Card or external USB Storage), otherwise **Packet Analyzer** cannot be enabled.

Go to **Administration > Diagnostic > Packet Analyzer** tab.

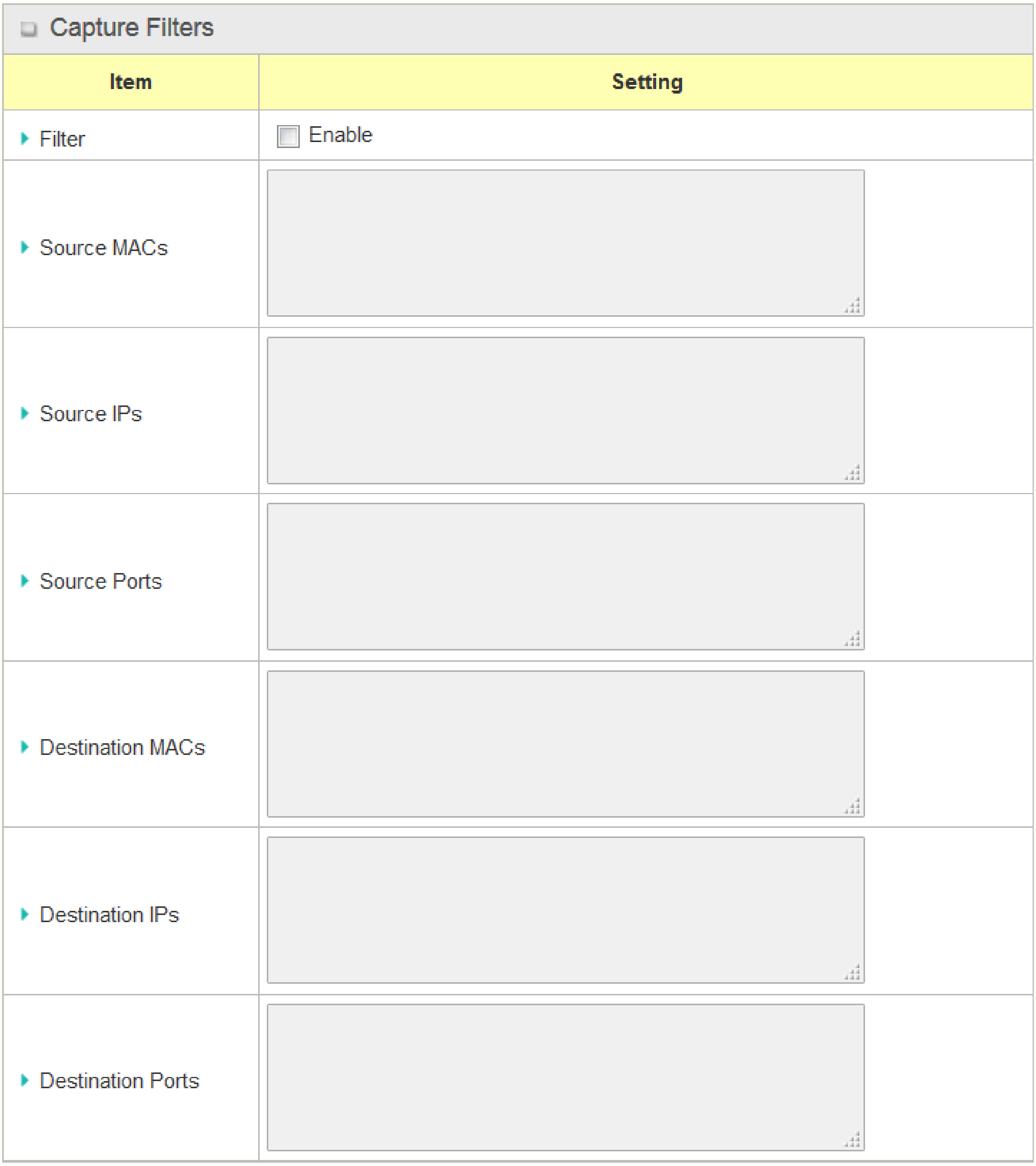


Configuration

Item	Setting
Packet Analyzer	□ Enable
File Name	
Split Files	□ Enable File Size : 200 KB
Packet Interfaces	□ WAN-1 □ WAN-2 2.4G : □ VAP-1 □ VAP-2

Configuration		
Item	**Value setting**	**Description**
Packet Analyzer	The box is unchecked by default.	Check **Enable** box to activate the Packet Analyzer function. If you cannot enable the checkbox, please check if the storage is available or not. Plug in the USB storage and then enable the Package Analyzer function.
File Name	1. An optional setting 2. Blank is set by default, and the default file name is **<Interface>_<Date>_<index>.**	Enter the file name to save the captured packets in log storage. If **Split Files** option is also enabled, the file name will be appended with an index code "**_<index>**"**.** The extension file name is **.pcap**.
Split Files	1. An optional setting 2. The default value of **File Size** is 200 KB.	Check **enable** box to split file whenever log file reaching the specified limit. If the **Split Files** option is enabled, you can further specify the **File Size** and **Unit** for the split files. ***Value Range***: 10 ~ 99999. NOTE: **File Size** cannot be less than 10 KB
Packet Interfaces	An optional setting	Define the interface(s) that **Packet Analyzer** should work on. At least, one interface is required, but multiple selections are also accepted. The supported interfaces can be: ● **WAN**: When the WAN is enabled at **Physical Interface**, it can be selected here. ● **VAP**: This means the virtual AP. When WiFi and VAP are enabled, it can be selected here.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.

Once you enabled the Packet Analyzer function on specific Interface(s), you can further specify some filter rules to capture the packets which matched the rules.



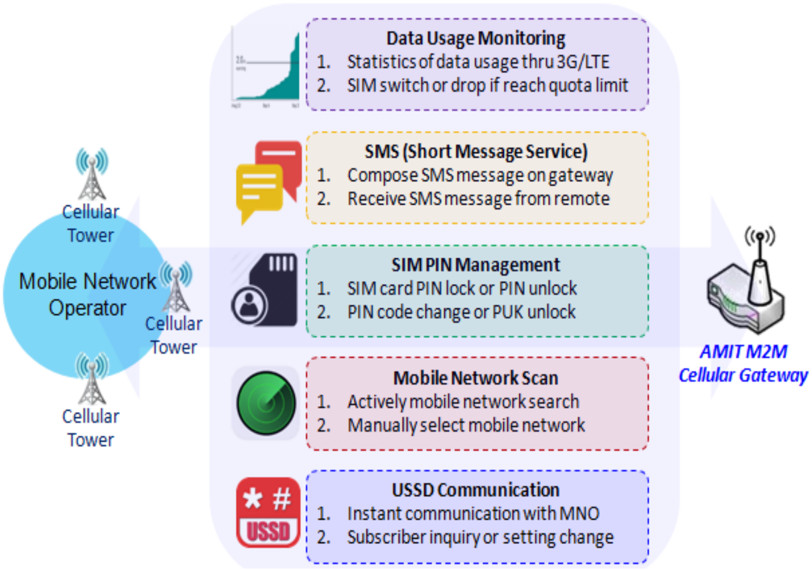
Capture Filters

Item	Setting
Filter	□ Enable
Source MACs	
Source IPs	
Source Ports	
Destination MACs	
Destination IPs	
Destination Ports	

Capture Fitters		
Item	**Value setting**	**Description**
Filter	Optional setting	Check **Enable** box to activate the Capture Filter function.
Source MACs	Optional setting	Define the filter rule with **Source MACs**, which means the source MAC address of packets. Packets which match the rule will be captured. Up to 10 MACs are supported, but they must be separated with "**;**", e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when match any one MAC in the rule.
Source IPs	Optional setting	Define the filter rule with **Source IPs**, which means the source IP address of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with "**;**", e.g. 192.168.1.1; 192.168.1.2 The packets will be captured when match any one IP in the rule.
Source Ports	Optional setting	Define the filter rule with **Source Ports**, which means the source port of packets. The packets will be captured when match any port in the rule. Up to 10 ports are supported, but they must be separated with "**;**", e.g. 80; 53 ***Value Range*:** 1 ~ 65535.
Destination MACs	Optional setting	Define the filter rule with **Destination MACs**, which means the destination MAC address of packets. Packets which match the rule will be captured. Up to 10 MACs are supported, but they must be separated with "**;**", e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when match any one MAC in the rule.
Destination IPs	Optional setting	Define the filter rule with **Destination IPs**, which means the destination IP address of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with "**;**", e.g. 192.168.1.1; 192.168.1.2 The packets will be captured when match any one IP in the rule.
Destination Ports	Optional setting	Define the filter rule with **Destination Ports**, which means the destination port of packets. The packets will be captured when match any port in the rule. Up to 10 ports are supported, but they must be separated with "**;**", e.g. 80; 53 ***Value Range*:** 1 ~ 65535.

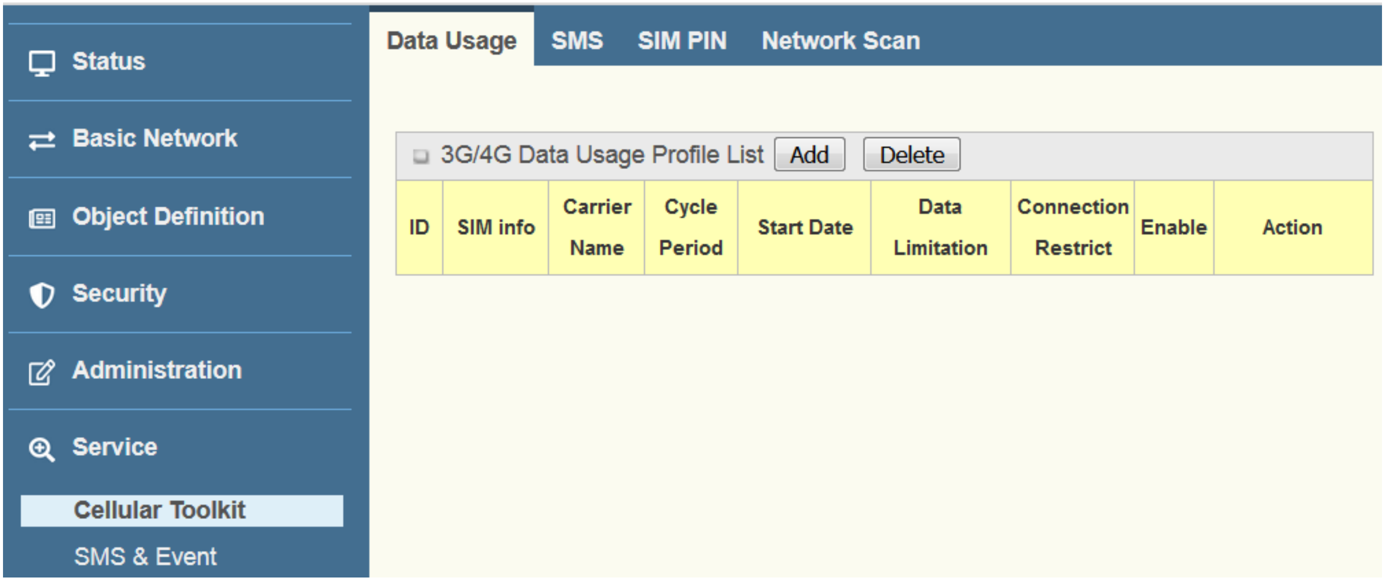
6. Service

6.1 Cellular Toolkit


Data Usage Monitoring
1. Statistics of data usage thru 3G/LTE
2. SIM switch or drop if reach quota limit
SMS (Short Message Service)
1. Compose SMS message on gateway
2. Receive SMS message from remote
SIM PIN Management
1. SIM card PIN lock or PIN unlock
2. PIN code change or PUK unlock
Mobile Network Scan
1. Actively mobile network search
2. Manually select mobile network
USSD Communication
1. Instant communication with MNO
2. Subscriber inquiry or setting change
Cellular Tower
Mobile Network Operator
Cellular Tower
Cellular Tower
AMIT M2M Cellular Gateway
USSD

Besides cellular data connection, you may also like to monitor data usage of cellular WAN, sending text message through SMS, changing PIN code of SIM card or doing a cellular network scan for diagnostic purpose.

In Cellular Toolkit section, it includes several useful features that are related to cellular configuration or application. You can configure settings of Data Usage, SMS, SIM PIN, and Network Scan here. Please note at least a valid SIM card is required to be inserted to device before you continue settings in this section.



□ 3G/4G Data Usage Profile List

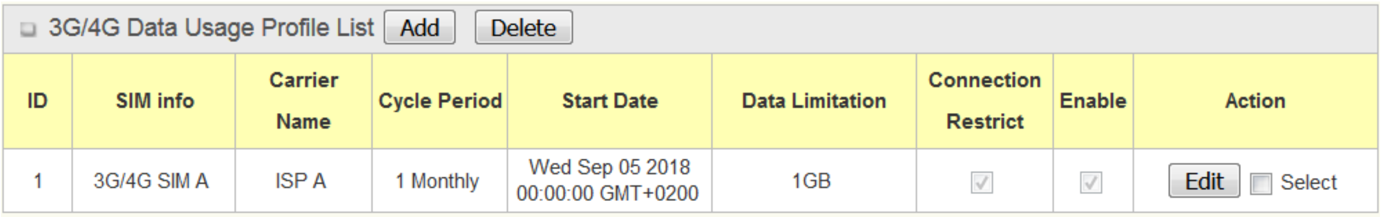
ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable	Action

6.1.1 Data Usage

Most of data plan for cellular connection is with a limited amount of data usage. If data usage has been over limited quota, either you will get much lower data throughput that may affect your daily operation, or you will get a 'bill shock' in the next month because carrier/ISP charges a lot for the over-quota data usage.

With help from Data Usage feature, device will monitor cellular data usage continuously and take actions. If data usage reaches limited quota, device can be set to drop the cellular data connection right away. Otherwise, if secondary SIM card is inserted, device will switch to secondary SIM and establish another cellular data connection with secondary SIM automatically.

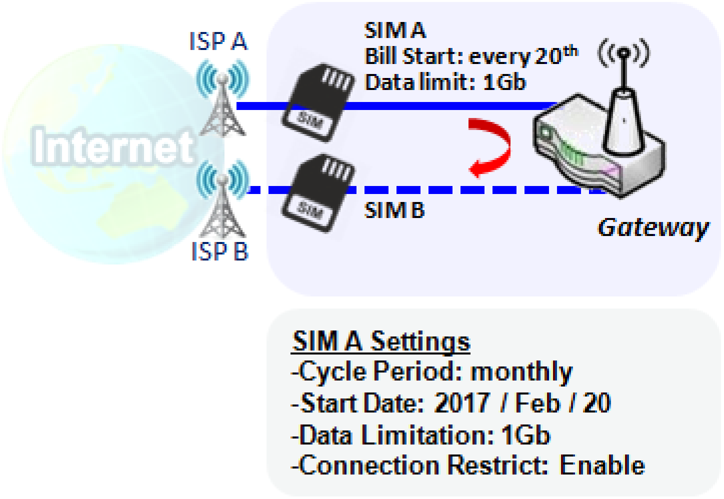
If Data Usage feature is enabled, all history of cellular data usage can be viewed at **Status** > **Statistics & Reports** > **Cellular Usage** tab.



3G/4G Data Usage Profile List Add Delete

ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable	Action
1	3G/4G SIM A	ISP A	1 Monthly	Wed Sep 05 2018 00:00:00 GMT+0200	1GB	☑	☑	Edit □ Select

3G/4G Data Usage



SIM A Settings
-Cycle Period: monthly
-Start Date: 2017 / Feb / 20
-Data Limitation: 1Gb
-Connection Restrict: Enable

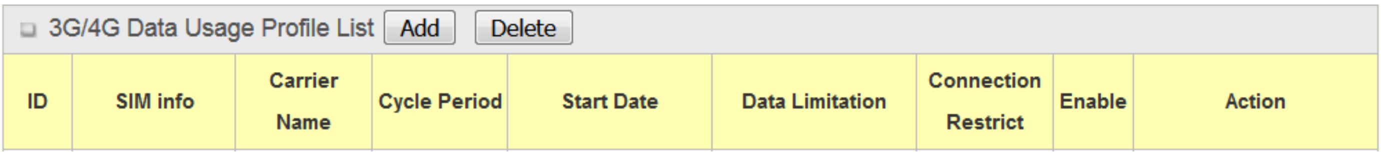
Data Usage feature enabling router device to continuously monitor cellular data usage and take actions. In the diagram, quota limit of SIM A is **1Gb** per month and bill start date is **20th** of every month. The device is smart to start a new calculation of data usage on every 20th of month. Enable Connection Restrict will force router device to drop cellular connection of SIM A when data usage reaches quota limit (1Gb in this case). If SIM failover feature is configured in **Internet Setup**, then router will switch to SIM B and establish a new cellular data connection automatically.

Data Usage Setting

Go to **Service** > **Cellular Toolkit** > **Data Usage** tab.

Before finished settings for Data Usage, you need to know bill start date, bill period, and quota limit of data usage according to your data plan. You can ask this information from your carrier or ISP.

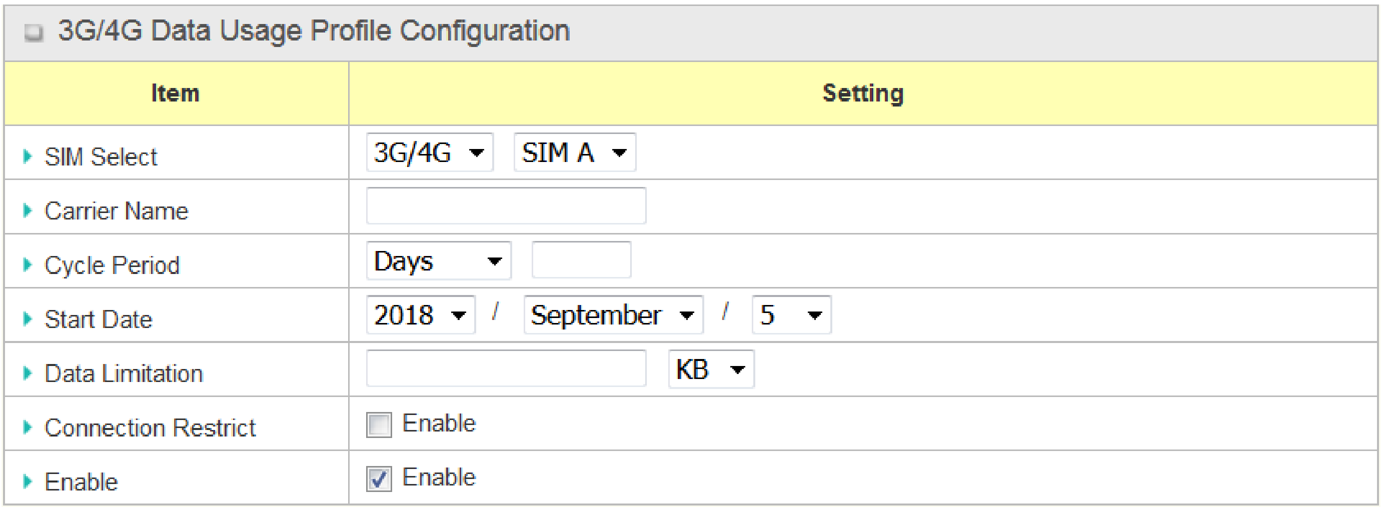
Create / Edit 3G/4G Data Usage Profile



3G/4G Data Usage Profile List [Add] [Delete]

ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable	Action

When **Add** button is applied, 3G/4G Data Usage Profile Configuration screen will appear. You can create up to four data usage profiles, one profile for each SIM card used in the Router.



3G/4G Data Usage Profile Configuration

Item	Setting
SIM Select	3G/4G ▾ SIM A ▾
Carrier Name	
Cycle Period	Days ▾
Start Date	2018 ▾ / September ▾ / 5 ▾
Data Limitation	KB ▾
Connection Restrict	□ Enable
Enable	☑ Enable

3G/4G Data Usage Profile Configuration		
Item Setting	**Value setting**	**Description**
SIM Select	3G/4G-1 and SIM A by default.	Choose a cellular interface (**3G/4G-1** or **3G/4G-2**), and a SIM card bound to the selected cellular interface to configure its data usage profile.
Carrier Name	It is an optional item.	Fill in the Carrier Name for the selected SIM card for identification.
Cycle Period	Days by default	The first box has three types for cycle period. They are **Days**, **Weekly** and **Monthly**. **Days**: For per Days cycle periods, you have to further specify the number of days in the second box. ***Value Range***: 1 ~ 90 days. **Weekly**, **Monthly**: The cycle period is one week or one month.
Start Date	N/A	Specify the date to start measure network traffic. Please don't select the day before now, otherwise, the traffic statistics will be incorrect.
Data Limitation	N/A	Specify the allowable data limitation for the defined cycle period.

Connection Restrict	Un-Checked by default.	Check the **Enable** box to activate the connection restriction function. During the specified cycle period, if the actual data usage exceeds the allowable data limitation, the cellular connection will be forced to disconnect.
Enable	Un-Checked by default.	Check the **Enable** box to activate the data usage profile.

6.1.2 SMS

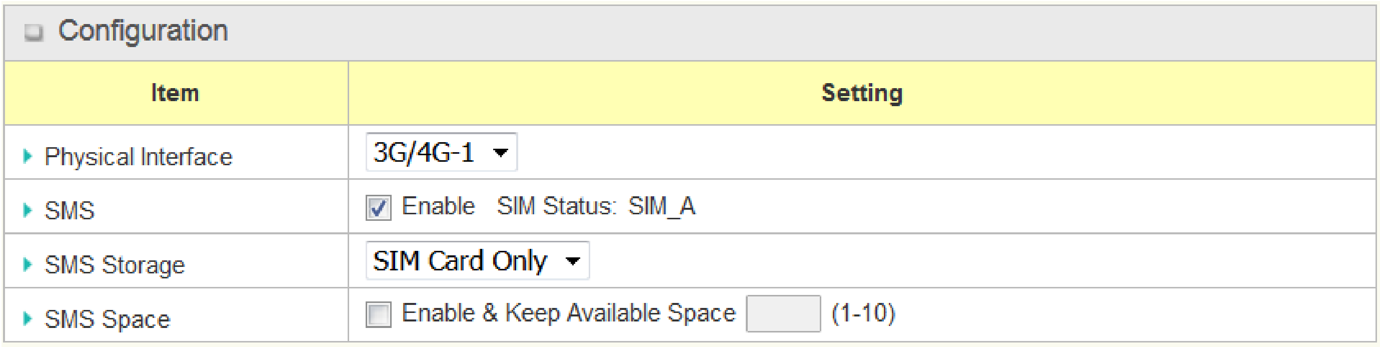
Short Message Service (SMS) is a text messaging service, which is used to be widely-used on mobile phones. It uses standardized communications protocols to allow mobile phones or cellular devices to exchange short text messages in an instant and convenient way.

SMS Setting

Go to **Service** > **Cellular Toolkit** > **SMS** tab

With this router device, you can send SMS text messages or browse received SMS messages as you usually do on a cellular phone.

Setup SMS Configuration



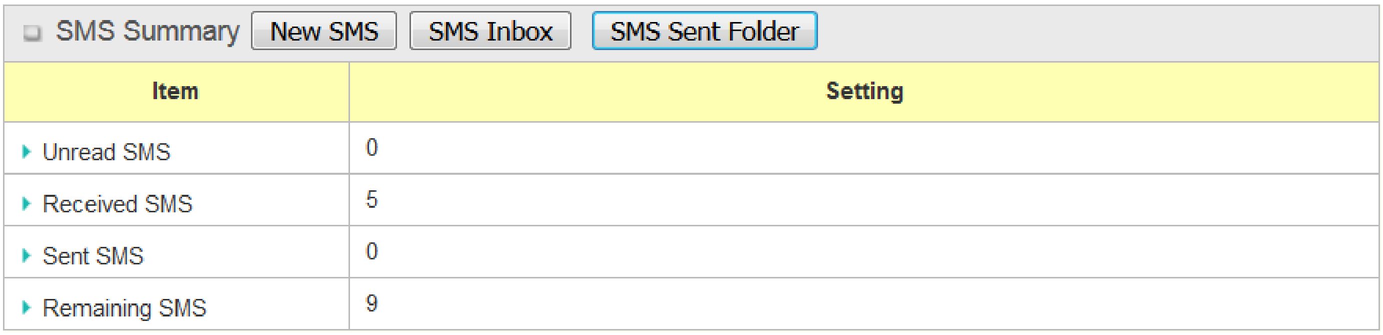
Configuration

Item	Setting
Physical Interface	3G/4G-1 ▾
SMS	☑ Enable SIM Status: SIM_A
SMS Storage	SIM Card Only ▾
SMS Space	□ Enable & Keep Available Space [ ] (1-10)

Configuration		
Item	**Value setting**	**Description**
Physical Interface	The box is 3G/4G-1 by default	Choose a cellular interface (**3G/4G-**1 or **3G/4G-2**) for the following SMS function configuration.
SMS	The box is checked by default	This is the SMS switch. If the box checked that the SMS function enable, if the box unchecked that the SMS function disable.
SIM Status	N/A	Depend on currently SIM status. The possible value will be **SIM_A** or **SIM_B**.
SMS Storage	The box is SIM Card Only by default	This is the SMS storage location. Currently the option only **SIM Card Only.**
SMS Space	The box is unchecked by default	Settings to keep SMS available space. Value Range: 1 ~ 10
Save	N/A	Click the **Save** button to save the settings

SMS Summary

Show **Unread SMS**, **Received SMS**, **Remaining SMS**, and edit SMS context to send, read SMS from SIM card.

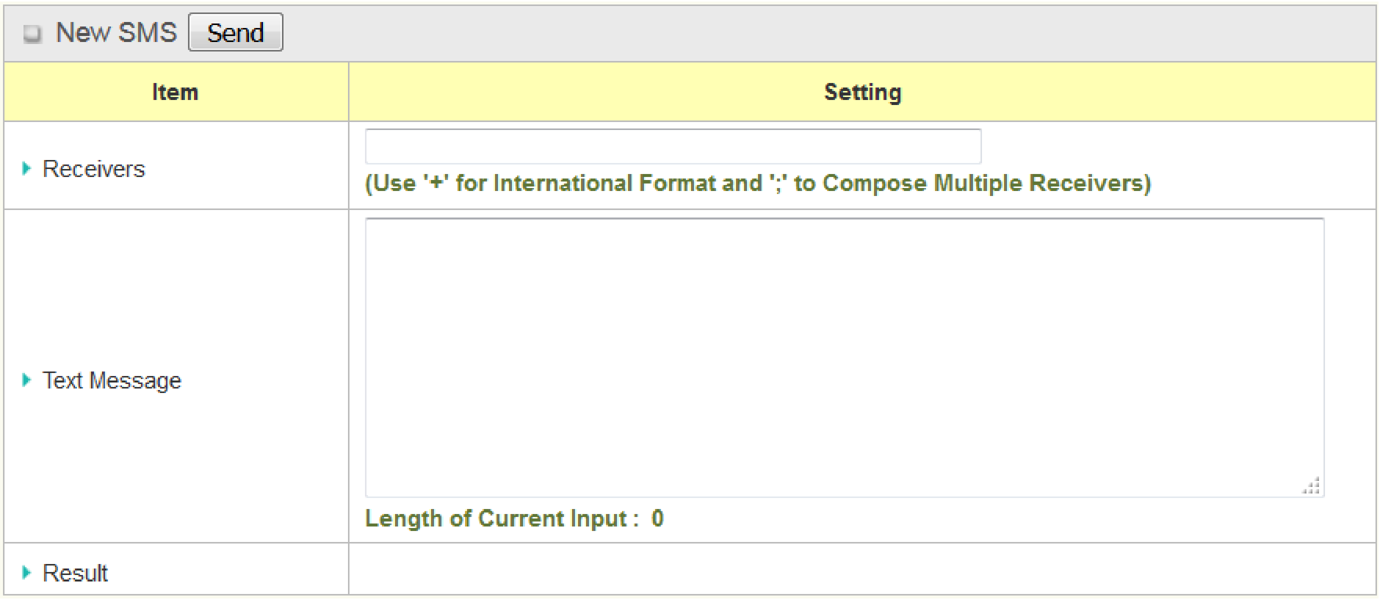


Item	Setting
Unread SMS	0
Received SMS	5
Sent SMS	0
Remaining SMS	9

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.
Sent SMS	N/A	This value record the sent SMS numbers from SIM card. When sent 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.
SMS Sent Folder	N/A	Folder with list of sent SMS.
Refresh	N/A	Click the **Refresh** button to update the SMS summary immediately.

New SMS

You can set the SMS setting from this screen.



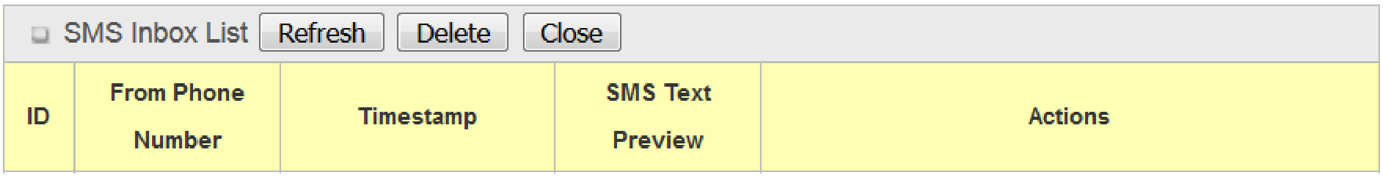
□ New SMS Send

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

New SMS		
Item	**Value setting**	**Description**
Receivers	N/A	Write the receivers to send SMS. User need to add the semicolon and compose multiple receivers that can group send SMS.
Text Message	N/A	Write the SMS context to send SMS. The router supports up to a maximum of 1023 character for SMS context length.
Send	N/A	Click the **Send** button, above text message will be sent as a SMS.
Result	N/A	If SMS has been sent successfully, it will show **Send OK**, otherwise **Send Failed** will be displayed.

SMS Inbox List

You can read or delete SMS, reply SMS or forward SMS from this screen.



□ SMS Inbox List Refresh Delete Close

ID	From Phone Number	Timestamp	SMS Text Preview	Actions

SMS Inbox List		
Item	**Value setting**	**Description**
ID	N/A	The number or SMS.
From Phone Number	N/A	What the phone number from SMS

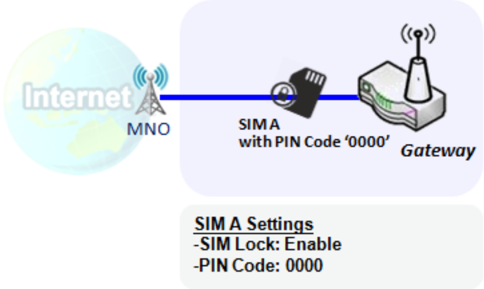
Timestamp	N/A	What time receive SMS
SMS Text Preview	N/A	Preview the SMS text. Click the **Detail** button to read a certain message.
Action	The box is unchecked by default	Click the **Detail** button to read the SMS detail; Click the **Reply** / **Forward** button to reply/forward SMS. Besides, you can check the box(-es), and then click the **Delete** button to delete the checked SMS(s).
Refresh	N/A	Refresh the SMS Inbox List.
Delete	N/A	Delete the SMS for all checked box from Action.
Close	N/A	Close the Detail SMS Message screen.

6.1.3 SIM PIN

With most cases in the world, users need to insert a SIM card (a.k.a. UICC) into end devices to get on cellular network for voice service or data surfing. The SIM card is usually released by mobile operators or service providers. Each SIM card has a unique number (so-called ICCID) for network owners or service providers to identify each subscriber. As SIM card plays an important role between service providers and subscribers, some security mechanisms are required on SIM card to prevent any unauthorized access.

Enabling a PIN code in SIM card is an easy and effective way of protecting cellular devices from unauthorized access. This router device allows you to activate and manage PIN code on a SIM card through its web GUI.

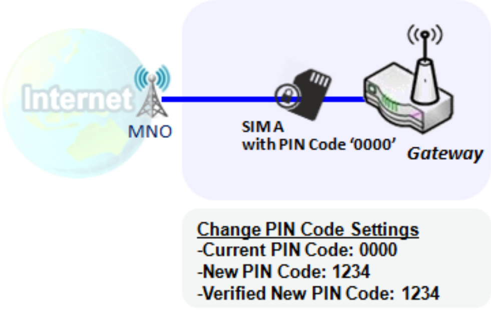
Activate PIN code on SIM Card



SIM A Settings
-SIM Lock: Enable
-PIN Code: 0000

This gateway device allows you to activate PIN code on SIM card. This example shows how to activate PIN code on SIM-A for 3G/4G-1 with default PIN code "**0000**".

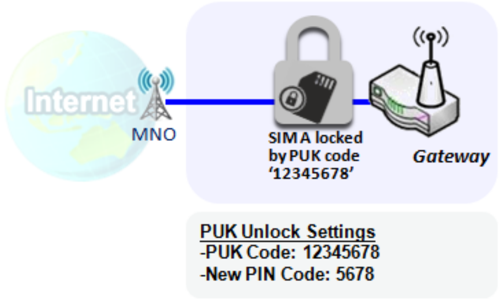
Change PIN code on SIM Card



Change PIN Code Settings
-Current PIN Code: 0000
-New PIN Code: 1234
-Verified New PIN Code: 1234

This gateway device allows you to change PIN code on SIM card. Following the example above, you need to type original PIN code "**0000**", and then type new PIN code with '**1234**' if you like to set new PIN code as '**1234**'. To confirm the new PIN code you type is what you want, you need to type new PIN code '**1234**' in Verified New PIN Code again.

Unlock SIM card by PUK Code



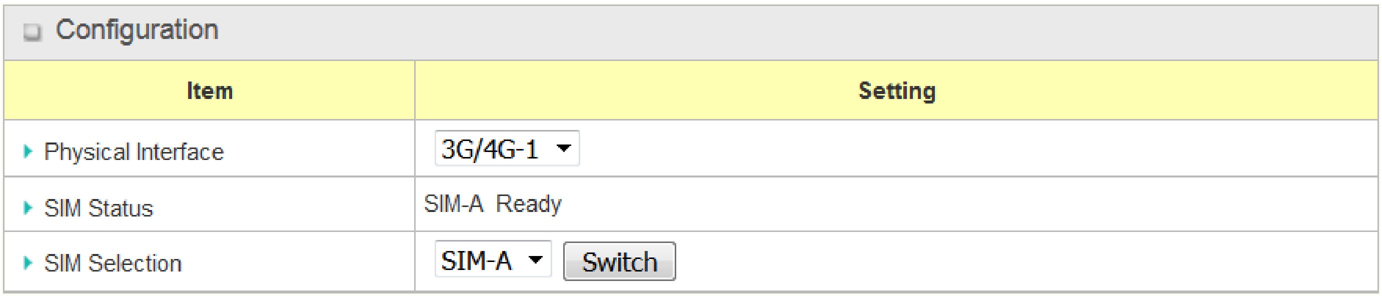
If you entered incorrect PIN code at configuration page for 3G/4G-1 WAN over three times, and then it will cause SIM card to be locked by PUK code. Then you have to call service number to get a PUK code to unlock SIM card. In the diagram, the PUK code is "**12345678**" and new PIN code is "**5678**".

SIM PIN Setting

Go to **Service** > **Cellular Toolkit** > **SIM PIN** Tab

With the SIM PIN Function window, it allows you to enable or disable SIM lock (which means protected by PIN code), or change PIN code. You can also see the information of remaining times of failure trials as we mentioned earlier. If you run out of these failure trials, you need to get a PUK code to unlock SIM card.

Select a SIM Card



Configuration

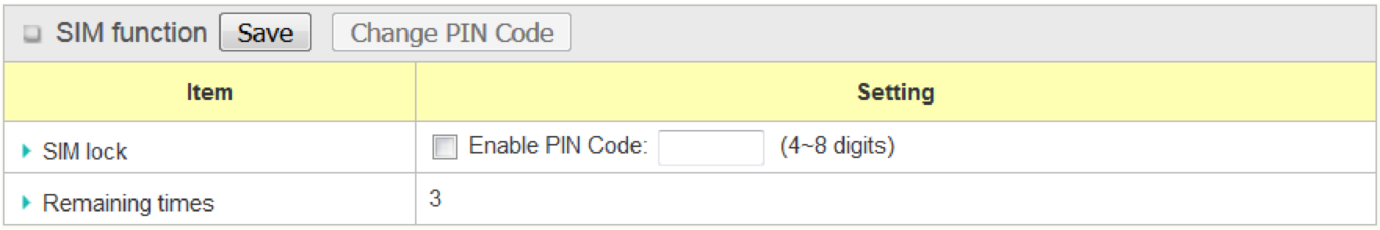
Item	Setting
Physical Interface	3G/4G-1 ▾
SIM Status	SIM-A Ready
SIM Selection	SIM-A ▾ Switch

Configuration Window

Item	Value setting	Description
Physical Interface	The box is 3G/4G-1 by default	Choose a cellular interface (**3G/4G-**1 or **3G/4G-2**) to change the SIM PIN setting for the selected SIM Card. The number of physical modems depends on the gateway model you purchased.
SIM Status	N/A	Indication for the selected SIM card and the SIM card status. The status could be **Ready**, **Not Insert**, or **SIM PIN**. **Ready** -- SIM card is inserted and ready to use. It can be a SIM card without PIN protection or that SIM card is already unlocked by correct PIN code. **Not Insert** -- No SIM card is inserted in that SIM slot. **SIM PIN** -- SIM card is protected by PIN code, and it's not unlocked by a correct PIN code yet. That SIM card is still at locked status.
SIM Selection	N/A	Select the SIM card for further SIM PIN configuration. Press the **Switch** button, then the Router will switch SIM card to another one. After that, you can configure the SIM card.

Enable / Change PIN Code

Enable or Disable PIN code (password) function, and even change PIN code function.

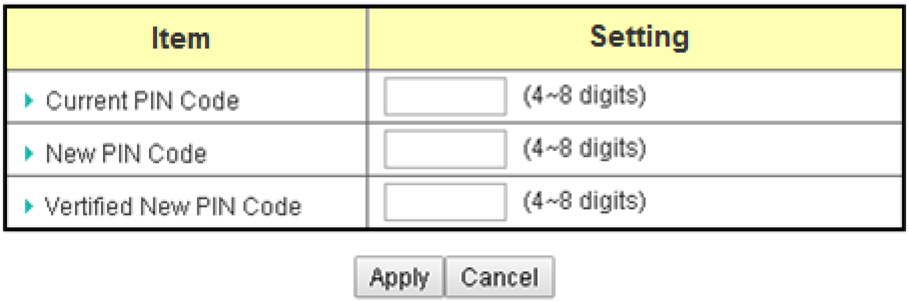


☐ SIM function [Save] [Change PIN Code]

Item	Setting
SIM lock	☐ Enable PIN Code: (4~8 digits)
Remaining times	3

SIM function Window		
Item Setting	**Value setting**	**Description**
SIM lock	Depend on SIM card	Click the **Enable** button to activate the SIM lock function. For the first time you want to enable the SIM lock function, you have to fill in the PIN code as well, and then click **Save** button to apply the setting.
Remaining times	Depend on SIM card	Represent the remaining trial times for the SIM PIN unlocking.
Save	N/A	Click the **Save** button to apply the setting.
Change PIN Code	N/A	Click the **Change PIN code** button to change the PIN code (password). If the **SIM Lock** function is not enabled, the **Change PIN code** button is disabled. In the case, if you still want to change the PIN code, you have to enable the SIM Lock function first, fill in the PIN code, and then click the **Save** button to enable. After that, You can click the **Change PIN code** button to change the PIN code.

When **Change PIN Code** button is clicked, the following screen will appear.



Item	Setting
Current PIN Code	(4~8 digits)
New PIN Code	(4~8 digits)
Vertified New PIN Code	(4~8 digits)

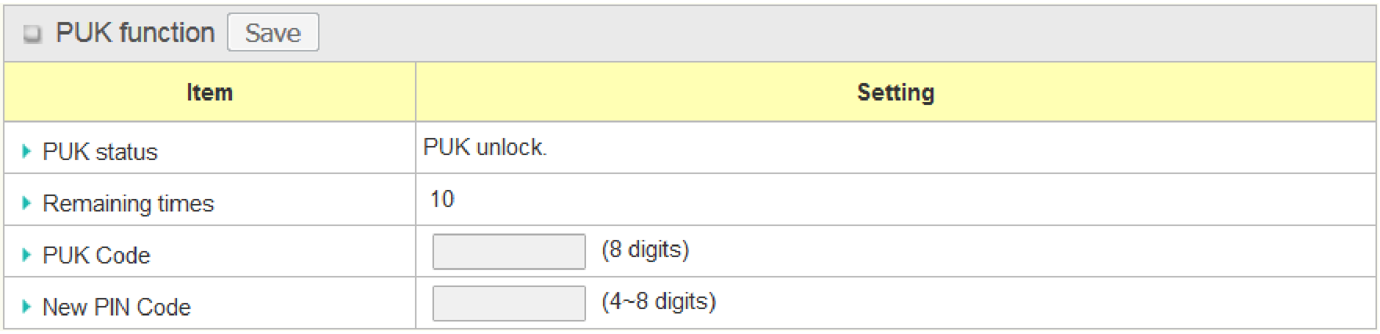
[Apply] [Cancel]

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

Note: If you changed the PIN code for a certain SIM card, you must also change the corresponding PIN code specified in the **Basic Network** > **WAN & Uplink** > **Internet Setup** > **Connection with SIM Card** page. Otherwise, it may result in wrong SIM PIN trials with invalid (old) PIN code.

Unlock with a PUK Code

The PUK Function window is only available for configuration if that SIM card is locked by PUK code. It means that SIM card is locked and needs additional PUK code to unlock. Usually it happens after too many trials of incorrect PIN code, and the remaining times in SIM Function table turns to 0. In this situation, you need to contact your service provider and request a PUK code for your SIM card, and try to unlock the locked SIM card with the provided PUK code. After unlocking a SIM card by PUK code successfully, the SIM lock function will be activated automatically.



PUK function Save

Item	Setting
PUK status	PUK unlock.
Remaining times	10
PUK Code	(8 digits)
New PIN Code	(4~8 digits)

PUK Function Window		
Item	**Value setting**	**Description**
PUK status	**PUK Unlock** / **PUK Lock**	Indication for the PUK status. The status could be **PUK Lock** or **PUK Unlock**. As mentioned earlier, the SIM card will be locked by PUK code after too many trials of failure PIN code. In this case, the PUK Status will turns to **PUK Lock**. In a normal situation, it will display **PUK Unlock**.
Remaining times	Depend on SIM card	Represent the remaining trial times for the PUK unlocking. Note : **DO NOT make the remaining times down to zero, it will damage the SIM card FOREVER !** Call for your ISP's help to get a correct PUK and unlock the SIM if you don't have the PUK code.
PUK Code	A Must filled setting	Fill in the PUK code (8 digits) that can unlock the SIM card in PUK unlock status.
New PIN Code	A Must filled setting	Fill in the New PIN Code (4~8 digits) for the SIM card. You have to determine your new PIN code to replace the old, forgotten one. Keep the PIN code (password) in mind with care.
Save	N/A	Click the **Save** button to apply the setting.

Note: If you changed the PUK code and PIN code for a certain SIM card, you must also change the corresponding PIN code specified in the **Basic Network** > **WAN & Uplink** > **Internet Setup** > **Connection with SIM Card** page. Otherwise, it may result in wrong SIM PIN trials with invalid (old) PIN code.

6.1.4 Network Scan

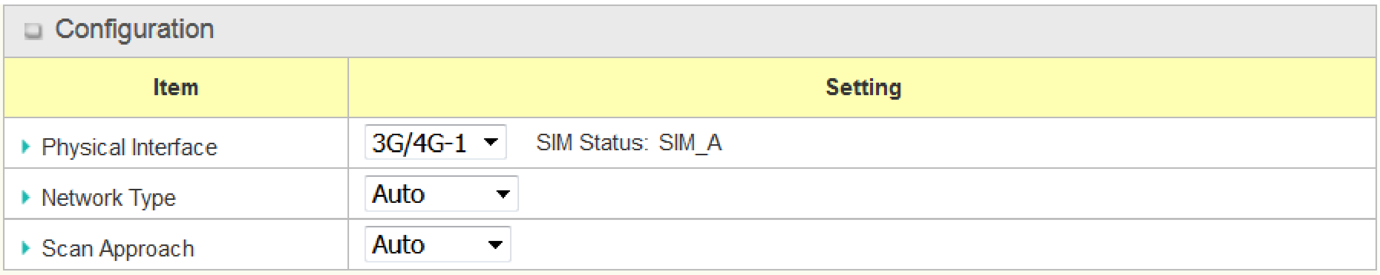
"Network Scan" function can let administrator specify the device how to connect to the mobile system for data communication in each 3G/4G interface. For example, administrator can specify which generation of mobile system is used for connection, 2G, 3G or LTE. Moreover, he can define their connection sequence for the router device to connect to the mobile system automatically. Administrator also can scan the mobile systems in the air manually, select the target operator system and apply it. The manual scanning approach is used for problem diagnosis.

Network Scan Setting

Go to **Service** > **Cellular Toolkit** > **Network Scan** tab.

In "Network Scan" page, there are two windows for the Network Scan function. The "Configuration" window 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.

Network Scan Configuration

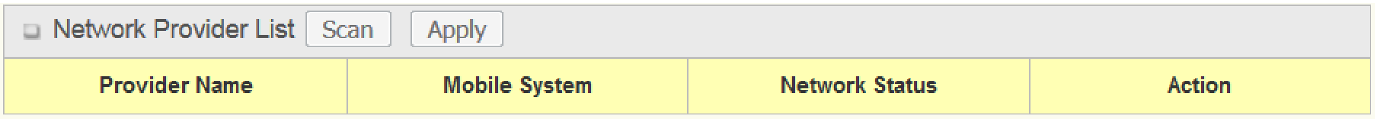


Configuration

Item	Setting
Physical Interface	3G/4G-1 ▾ SIM Status: SIM_A
Network Type	Auto ▾
Scan Approach	Auto ▾

Configuration		
Item	**Value setting**	**Description**
Physical Interface	The box is **3G/4G-1** by default	Choose a cellular interface (**3G/4G-**1 or **3G/4G-2**) for the network scan function. **Note: 3G/4G-2** is only available for the product with dual cellular module.
SIM Status	N/A	Show the connected cellular service (identified with **SIM_A** or **SIM_B**).
Network Type	**Auto** is selected by default.	Specify the network type for the network scan function. It can be Auto, 2G Only, 2G prefer, 3G Only, 3G prefer, or LTE Only. When **Auto** is selected, the network will be register automatically; If the **prefer** option is selected, network will be register for your option first; If the **only** option is selected, network will be register for your option only.
Scan Approach	**Auto** is selected by default.	When **Auto** selected, cellular module register automatically. If the **Manually** option is selected, a **Network Provider List** screen appears. Press **Scan** button to scan for the nearest base stations. Select (check the box) the preferred base stations then click **Apply** button to apply settings.
Save	N/A	Click **Save** to save the settings

The second window is the "Network Provider List" window and it appears when the **Manually** Scan Approach is selected in the Configuration window. By clicking on the "Scan" button and wait for 1 to 3 minutes, the found mobile operator system will be displayed for you to choose. Click again on the "Apply" button to drive system to connect to that mobile operator system for the dedicated 3G/4G interface.



Provider Name	Mobile System	Network Status	Action

6.2 Event Handling

Event handling is the application that allows administrator to setup the pre-defined events, handlers, or response behavior with individual profiles. With properly configuring the event handling function, administrator can easily and remotely obtain the status and information via the purchased router.

The supported events are categorized into two groups: the **managing events** and **notifying events**.

The **managing events** are the events that are used to manage the router or change the setting / status of the specific functionality of the router. On receiving the managing event, the router will take action to change the functionality, and collect the required status for administration simultaneously.

The **notifying events** are the events that some related objects have been triggered and take corresponding actions on the occurrence of the events. It could be an event for alerting the administrator something happened with SMS message, Email, and SNMP Trap, etc...

For ease of configuration, administrator can create and edit the common pre-defined managing / notifying event profiles for taking instant reaction on a certain event or managing the devices for some advanced useful purposes. For example, sending/receiving remote managing SMS for the router's routine maintaining, and so on. All of such management and notification function can be realized effectively via the Event Handling feature.

The following is the summary lists for the provided profiles, and events:

- Profiles (Rules):
  - SMS Configuration and Accounts
  - Email Accounts

- Managing Events:
  - Trigger Type: SMS, SNMP Trap
  - Actions: Get the Network Status; or Configure the LAN/VLAN behavior, WIFI behavior, NAT behavior, Firewall behavior, VPN behavior, System Management, Administration.

- Notifying Events:
  - Trigger Type: Connection Change (WAN, LAN & VLAN, WiFi, DDNS), Administration, and Data Usage.
  - Actions: Notify the administrator with SMS, Syslog, SNMP Trap or Email Alert.

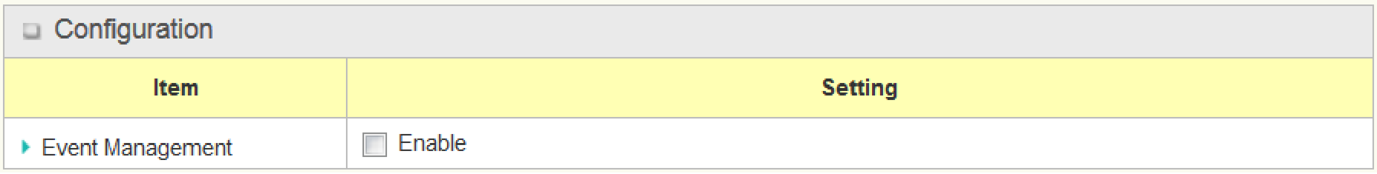
To use the event handling function, First of all, you have to enable the event management setting and configure the event details with the provided profile settings. You can create or edit pre-defined profiles for individual managing / notifying events. The profile settings are separated into several items; they are the SMS Account Definition, and Email Service Definition. Then, you have to configure each managing / notifying event with identifying the event's trigger condition, and the corresponding actions (reaction for the event) for the event. For each event, more than one action can be activated simultaneously.

6.2.1 Configuration

Go to **Service** > **Event Handling** > **Configuration** Tab.

Event handling is the service that allows administrator to setup the pre-defined events, handlers, or response behavior with individual profiles.

Enable Event Management



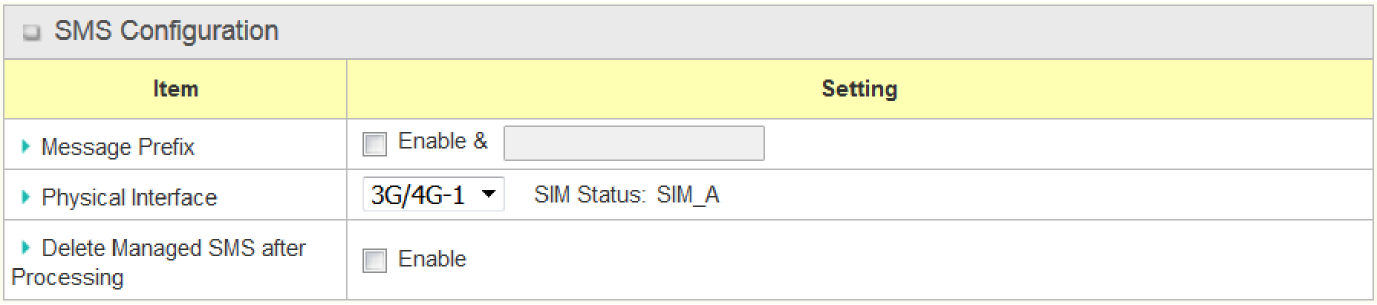
Configuration

Item	Setting
Event Management	□ Enable

Configuration		
Item	**Value setting**	**Description**
Event Management	The box is unchecked by default	Check the **Enable** box to activate the Event Management function.

Enable SMS Management

To use the SMS management function, you have to configure some important settings first.



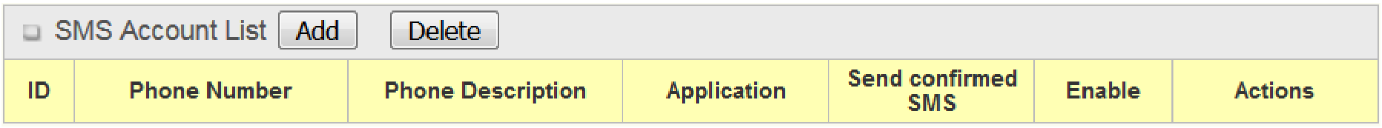
SMS Configuration

Item	Setting
Message Prefix	□ Enable &
Physical Interface	3G/4G-1 ▾ SIM Status: SIM_A
Delete Managed SMS after Processing	□ Enable

SMS Configuration		
Item	**Value setting**	**Description**
Message Prefix	The box is unchecked by default	Click the **Enable** box to enable the SMS prefix for validating the received SMS. Once the function is enabled, you have to enter the prefix behind the checkbox. The received managing events SMS must have the designated prefix as an initial identifier, then corresponding handlers will become effective for further processing.
Physical Interface	The box is 3G/4G-1 by default.	Choose a cellular interface (**3G/4G-**1 or **3G/4G-2**) to configure the SMS management setting. **Note: 3G/4G-2** is only available for the product with dual cellular module.
SIM Status	N/A	Show the connected cellular service (identified with **SIM_A** or **SIM_B**).
Delete Managed SMS after Processing	The box is unchecked by default	Check the **Enable** box to delete the received managing event SMS after it has been processed.

Create / Edit SMS Account

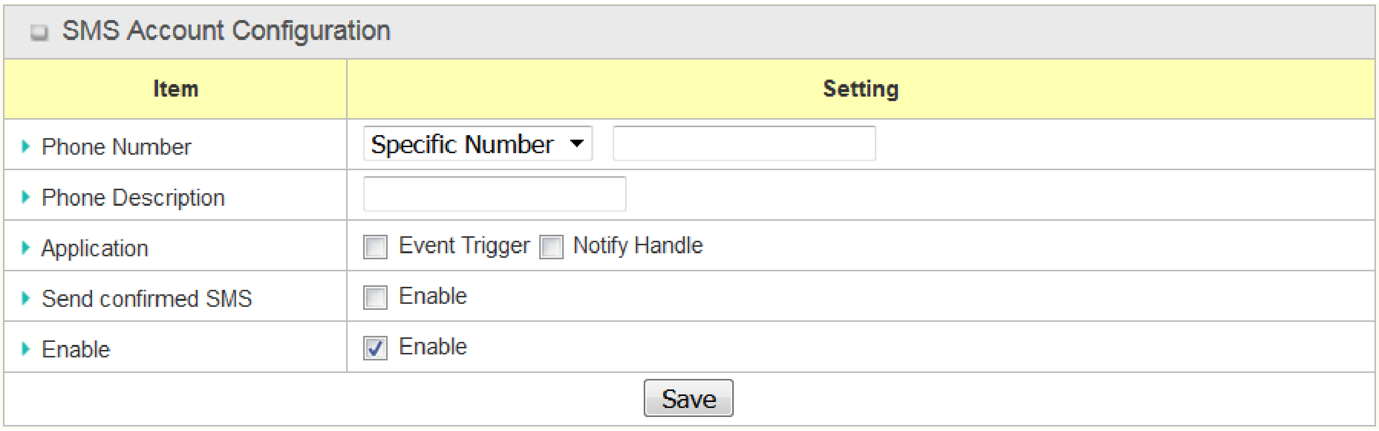
Setup the SMS Account for managing the router through the SMS. It supports up to a maximum of 5 accounts.



SMS Account List

ID	Phone Number	Phone Description	Application	Send confirmed SMS	Enable	Actions

You can click the **Add / Edit** button to configure the SMS account.



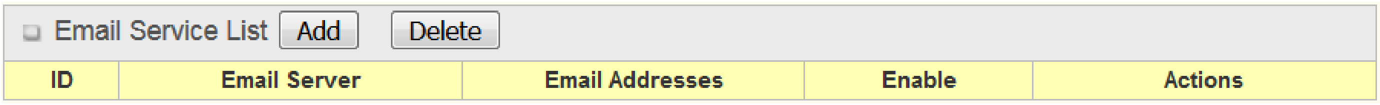
SMS Account Configuration

Item	Setting
Phone Number	Specific Number ▾
Phone Description	
Application	□ Event Trigger □ Notify Handle
Send confirmed SMS	□ Enable
Enable	☑ Enable

SMS Account Configuration		
Item	**Value setting**	**Description**
Phone Number	1. Mobile phone number format 2. A Must filled setting	Select the Phone number policy from the drop list, and specify a mobile phone number as the SMS account identifier if required. It can be **Specific Number**, or **Allow Any**. If **Specific Number** is selected, you have to specify the phone number as the SMS account identifier. ***Value Range***: -1 ~ 32 digits.
Phone Description	1. Any text 2. An Optional setting	Specify a brief description for the SMS account.
Application	A Must filled setting	Specify the application type. It could be **Event Trigger, Notify Handle,** or **both**. If the Phone Number policy is **Allow Any**, the Notify Handle will be unavailable.
Send confirmed SMS	1. An Optional setting 2. The box is unchecked by default.	Click **Enable** box to active the SMS response function. The router will send a confirmed message back to the sender whenever it received a SMS managing event. The confirmed message is similar to following format: *"Device received a SMS with command xxxxx."*
Enable	The box is unchecked by default.	Click **Enable** box to activate this account.
Save	*NA*	Click the **Save** button to save the configuration.

Create / Edit Email Service Account

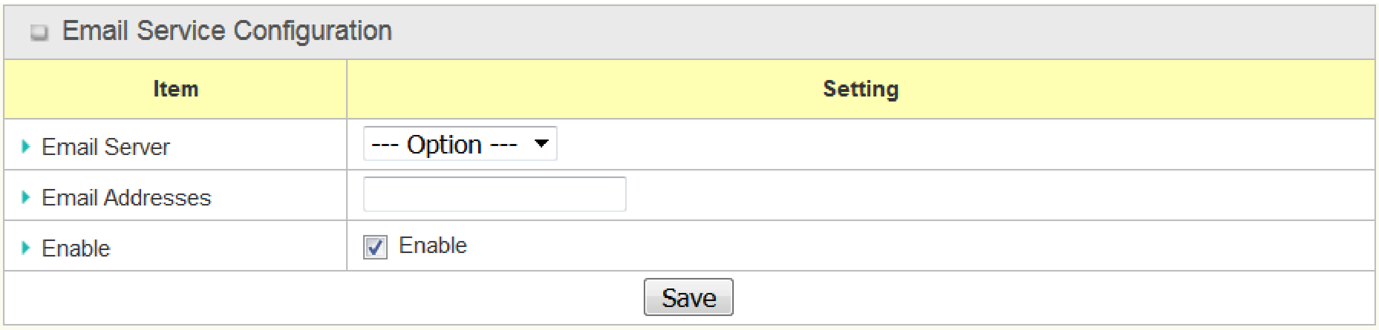
Setup the Email Service Account for event notification. It supports up to a maximum of 5 accounts.



Email Service List

ID	Email Server	Email Addresses	Enable	Actions

You can click the **Add / Edit** button to configure the Email account.



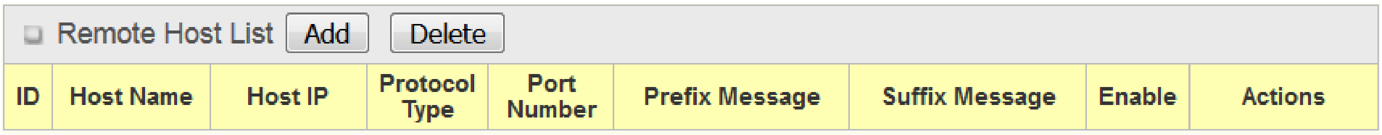
Email Service Configuration

Item	Setting
Email Server	--- Option ---
Email Addresses	
Enable	☑ Enable

Email Service Configuration		
Item	**Value setting**	**Description**
Email Server	--- Option ---	Select an Email Server profile from **External Server** setting for the email account setting.
Email Addresses	1. Internet E-mail address format 2. A Must filled setting	Specify the Destination Email Addresses.
Enable	The box is unchecked by default.	Click **Enable** box to activate this account.
Save	*NA*	Click the **Save** button to save the configuration

Create / Edit Remote Host

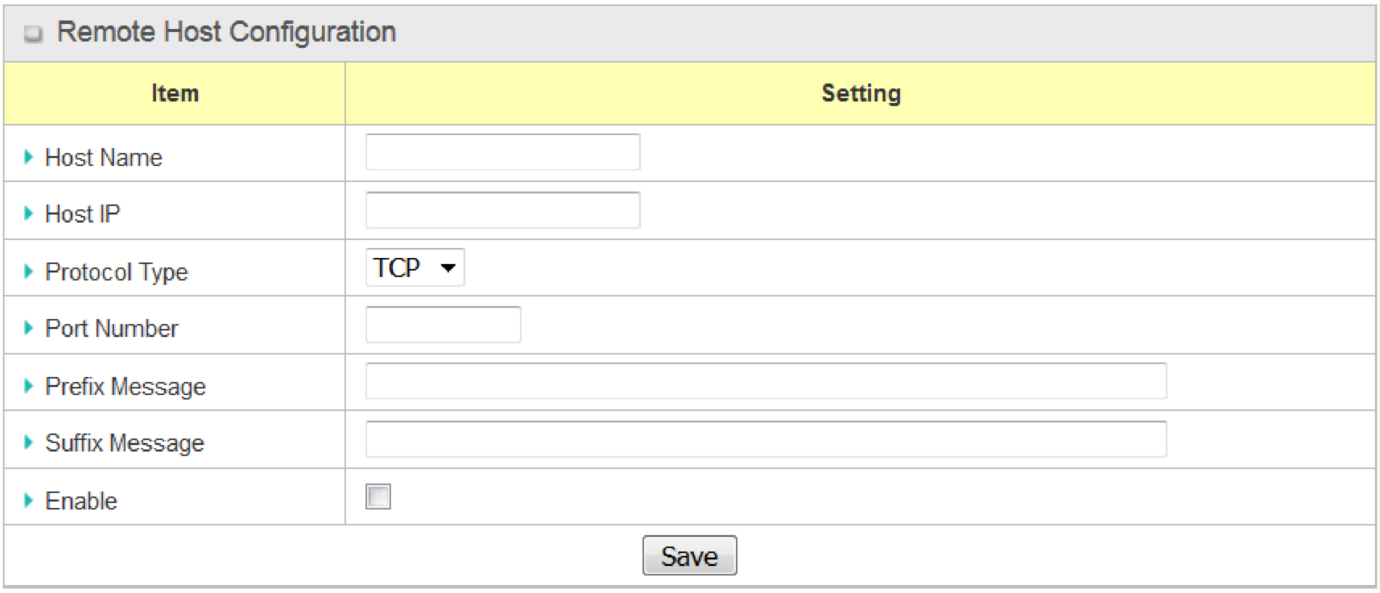
Setup the Remote Host for managing the router through the remote host. It supports up to a maximum of 5 accounts.



Remote Host List

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

You can click the **Add / Edit** button to configure the host account.



Remote Host Configuration

Item	Setting
Host Name	
Host IP	
Protocol Type	TCP
Port Number	
Prefix Message	
Suffix Message	
Enable	□

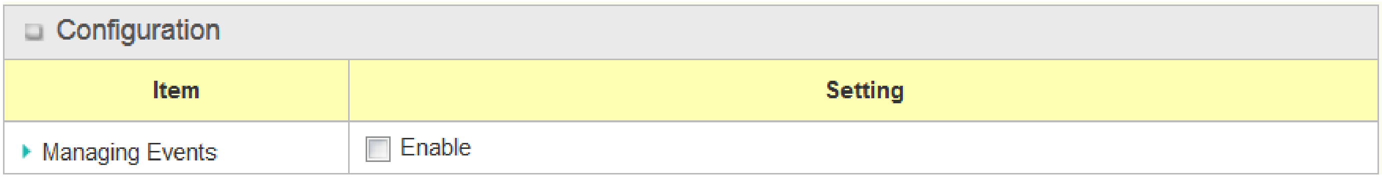
Remote Host Configuration		
Item	**Value setting**	**Description**
Host Name	String format: any text. 2. A Must filled setting	Specify the name of the host.
Host IP	1. IP address 2. A Must filled setting	Specify the host IP address.
Protocol Type	1. TCP/UDP 2. A Must filled setting	Select type of protocol, TCP or UDP.
Port Number	1. Port number 2. A Must filled setting	Specify TCP/UDP port number.
Prefix Message	String format: any text.	Enter message prefix.
Suffix Message	String format: any text.	Enter message suffix.
Enable	The box is unchecked by default.	Click **Enable** box to activate this account.
Save	*NA*	Click the **Save** button to save the configuration

6.2.2 Managing Events

Managing Events allow administrator to define the relationship (rule) among event trigger, handlers and response.

Go to **Service** > **Event Handling** > **Managing Events** Tab.

Enable Managing Events



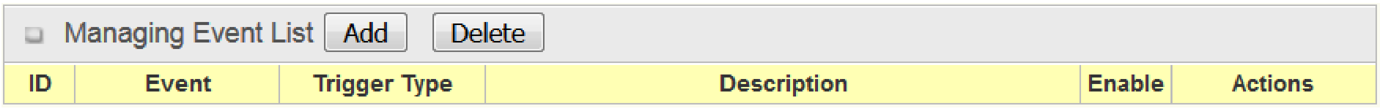
Configuration

Item	Setting
Managing Events	□ Enable

Configuration		
Item	**Value setting**	**Description**
Managing Events	The box is unchecked by default	Check the **Enable** box to activate the Managing Events function.

Create / Edit Managing Event Rules

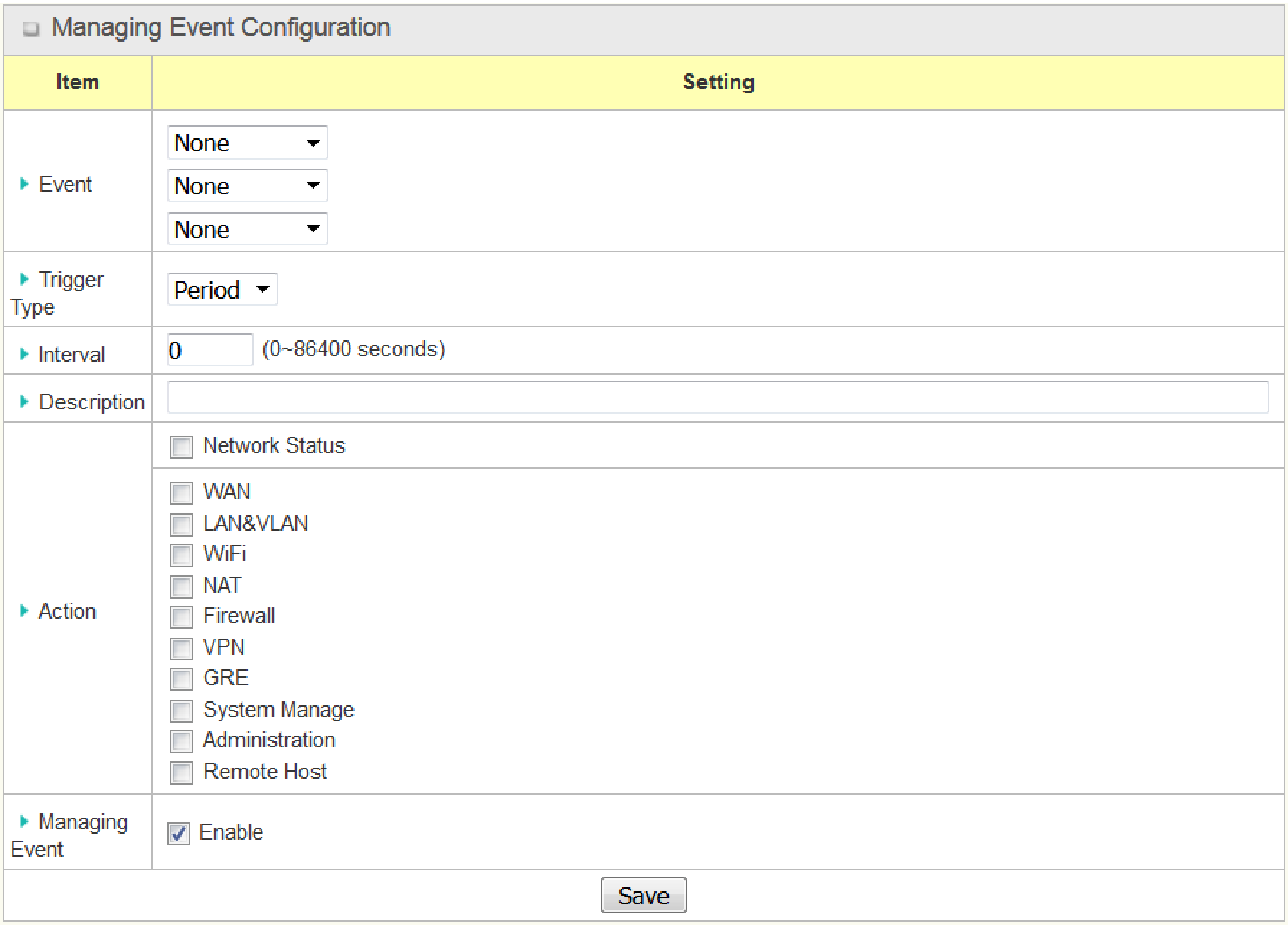
Setup the Managing Event rules. It supports up to a maximum of 128 rules.



Managing Event List

ID	Event	Trigger Type	Description	Enable	Actions

When **Add** or **Edit** button is applied, the **Managing Event Configuration** screen will appear.



Managing Event Configuration

Item	Setting
Event	None None None
Trigger Type	Period
Interval	0 (0~86400 seconds)
Description	
Action	□ Network Status □ WAN □ LAN&VLAN □ WiFi □ NAT □ Firewall □ VPN □ GRE □ System Manage □ Administration □ Remote Host
Managing Event	☑ Enable

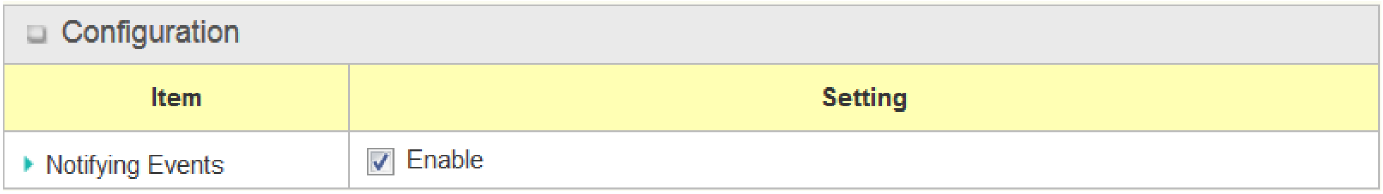
Managing Event Configuration		
Item	**Value setting**	**Description**
Event	**SMS** (or **SNMP Trap**) by default	Specify the Event type (**SMS**, **SNMP Trap**) and an event identifier / profile. **SMS**: Select **SMS** and fill the message in the textbox to as the trigger condition for the event; **SNMP**: Select **SNMP Trap** and fill the message in the textbox to specify SNMP Trap Event; *Note: The available Event Type could be different for the purchased product.*
Trigger Type	**Period** (or **Once**) by default	Specify the Trigger Type (**Period**, **Once**). **Period:** Event will be executed in a period set by Interval below. **Once:** Event will be executed just once.
Interval	Number in seconds	Time interval for event execution in period. Interval: 0 ~ 86400 *Note: Available for Trigger Type set to Period only.*
Description	String format: any text.	Enter a brief description for the Managing Event.
Action	All box is unchecked by default.	Specify **Network Status**, or at least one rest action to take when the expected event is triggered. **Network Status**: Select Network Status Checkbox to get the network status as the action for the event; **WAN:** Select **WAN** checkbox and the interested sub-items (Connect/Disconnect, Auto/LTE/3G/2G), the router will change the settings as the action for the event; **LAN&VLAN**: Select **LAN&VLAN** Checkbox and the interested sub-items (Port link On/Off), the router will change the settings as the action for the event; **WiFi**: Select **WiFi** Checkbox and the interested sub-items (WiFi radio On/Off), the router will change the settings as the action for the event; **NAT**: Select **NAT** Checkbox and the interested sub-items (Virtual Server Rule On/Off, DMZ On/Off), the router will change the settings as the action for the event; **Firewall**: Select **Firewall** Checkbox and the interested sub-items (Remote Administrator Host ID On/Off), the router will change the settings as the action for the event; **VPN**: Select **VPN** Checkbox and the interested sub-items (IPSec Tunnel ON/Off, PPTP Client On/Off, L2TP Client On/Off, OpenVPN Client On/Off), the router will change the settings as the action for the event; **GRE**: Select **GRE** Checkbox and the interested sub-items (GRE Tunnel On/Off), the router will change the settings as the action for the event; **System Manage**: Select **System Manage** Checkbox and the interested sub-items (WAN SSH Service On/Off, TR-069 On/Off), the router will change the settings as the action for the event; **Administration**: Select **Administration** Checkbox and the interested sub-items (Backup Config, Restore Config, Reboot, Save Current Setting as Default), the router will change the settings as the action for the event; **Remote Host:** Select **Remote Host** checkbox and one of defined remote hosts. *Note: The available Event Type could be different for the purchased product.*
Managing Event	The box is unchecked by default.	Click **Enable** box to activate this Managing Event setting.
Save	*NA*	Click the **Save** button to save the configuration
Undo	*NA*	Click the **Undo** button to restore what you just configured back to the previous setting.

6.2.3 Notifying Events

Go to **Service** > **Event Handling** > **Notifying Events** Tab.

Notifying Events Setting allows administrator to define the relationship (rule) between event trigger and handlers.

Enable Notifying Events



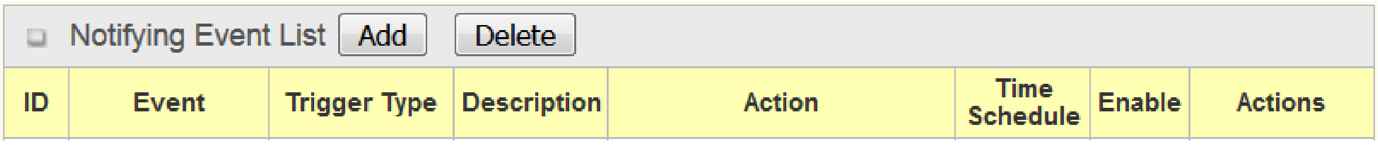
Configuration

Item	Setting
Notifying Events	☑ Enable

Configuration		
Item	**Value setting**	**Description**
Notifying Events	The box is unchecked by default	Check the **Enable** box to activate the Notifying Events function.

Create / Edit Notifying Event Rules

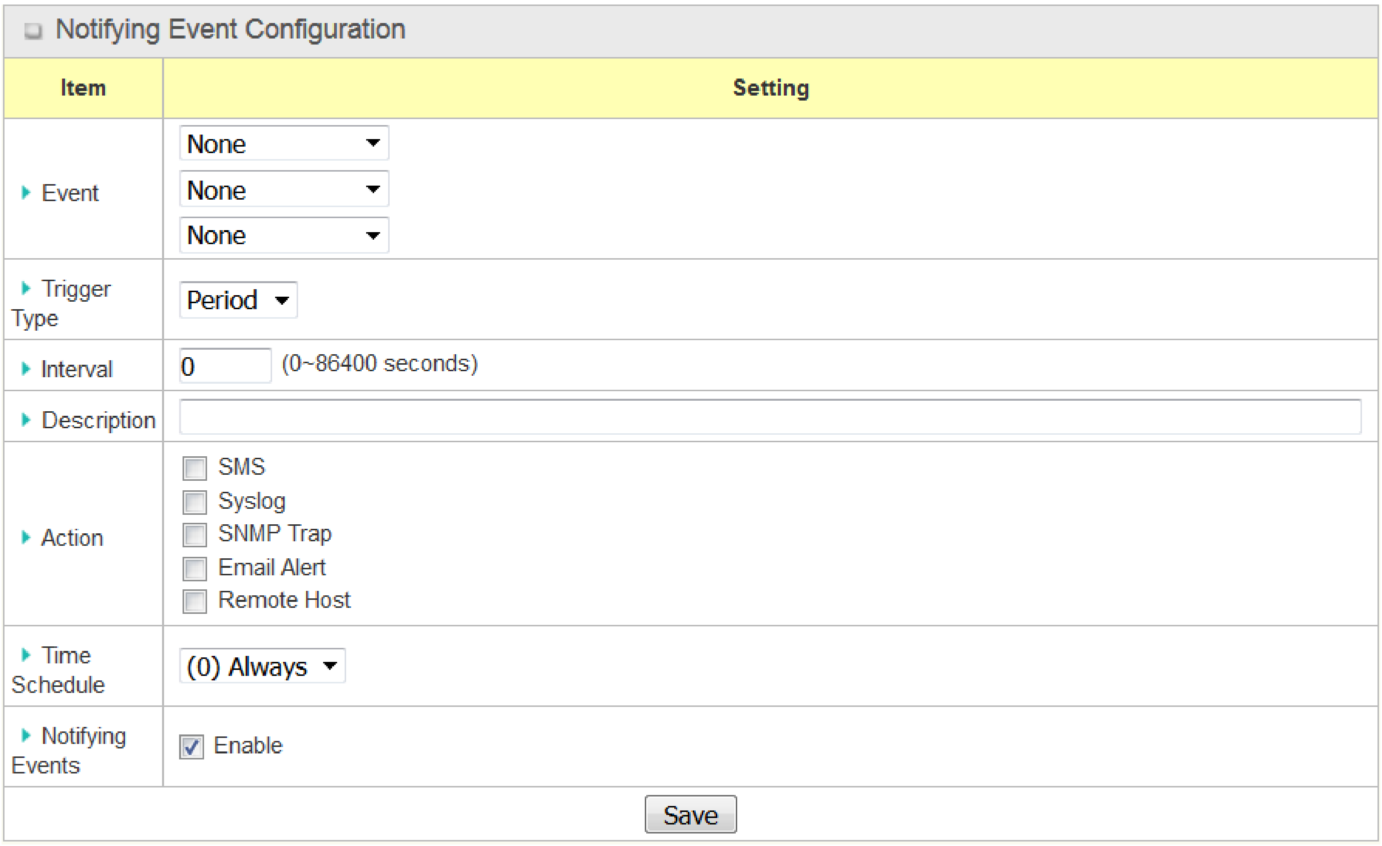
Setup your Notifying Event rules. It supports up to a maximum of 128 rules.



Notifying Event List

ID	Event	Trigger Type	Description	Action	Time Schedule	Enable	Actions

When **Add** or **Edit** button is applied, the **Notifying Event Configuration** screen will appear.



Notifying Event Configuration

Item	Setting
Event	None None None
Trigger Type	Period
Interval	0 (0~86400 seconds)
Description	
Action	□ SMS □ Syslog □ SNMP Trap □ Email Alert □ Remote Host
Time Schedule	(0) Always
Notifying Events	☑ Enable

Notifying Event Configuration

Item	Value setting	Description
Event	**WAN** is selected by default	Specify the Event type and corresponding event configuration. The supported Event Type could be: **WAN**: Select **WAN** and a trigger condition to specify a certain WAN Event; **LAN&VLAN**: Select **LAN&VLAN** and a trigger condition to specify a certain LAN&VLAN Event; **WiFi**: Select **WiFi** and a trigger condition to specify a certain WiFi Event; **DDNS**: Select **DDNS** and a trigger condition to specify a certain DDNS Event; **Administration**: Select **Administration** and a trigger condition to specify a certain Administration Event; **Data Usage**: Select **Data Usage**, the SIM Card (Cellular Service) and a trigger condition to specify a certain Data Usage Event; *Note: The available Event Type could be different for the purchased product.*
Trigger Type	**Period** (or **Once**) by default	Specify the Trigger Type (**Period**, **Once**). **Period:** Event will be executed in a period set by Interval below. **Once:** Event will be executed just once.
Interval	Number in seconds	Time interval for event execution in period. Interval: 0 ~ 86400 *Note: Available for Trigger Type set to Period only.*
Description	String format : any text.	Enter a brief description for the Notifying Event.
Action	All box is unchecked by default.	Specify at least one action to take when the expected event is triggered. **SMS**: Select **SMS**, and the router will send out a SMS to all the defined SMS accounts as the action for the event;

		Syslog: Select **Syslog** and select/unselect the Enable Checkbox to as the action for the event; **SNMP Trap**: Select **SNMP Trap**, and the router will send out SNMP Trap to the defined SNMP Event Receivers as the action for the event; **Email Alert**: Select **Email Alert**, and the router will send out an Email to the defined Email accounts as the action for the event; **Remote Host:** Select **Remote Host** checkbox and one of defined remote hosts. *Note: The available Event Type could be different for the purchased product.*
Time Schedule	**(0) Always** is selected by default	Select a time scheduling rule for the Notifying Event.
Notifying Events	The box is unchecked by default.	Click **Enable** box to activate this Notifying Event setting.
Save	*NA*	Click the **Save** button to save the configuration
Undo	*NA*	Click the **Undo** button to restore what you just configured back to the previous setting.

7. Status

7.1 Basic Network

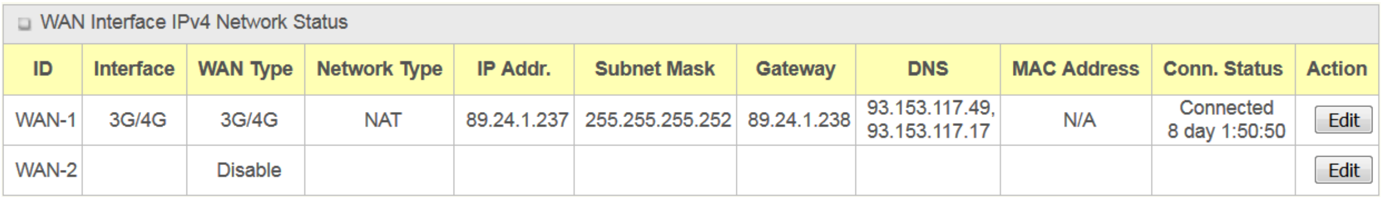
7.1.1 WAN & Uplink Status

Go to **Status > Basic Network > WAN & Uplink** tab.

The **WAN & Uplink Status** window shows the current status for different network type, including network configuration, connecting information, modem status and traffic statistics. The display will be refreshed on every five seconds.

WAN interface IPv4 Network Status

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



WAN Interface IPv4 Network Status

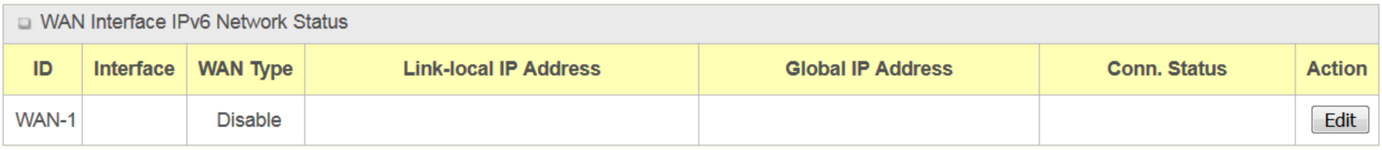
ID	Interface	WAN Type	Network Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Action
WAN-1	3G/4G	3G/4G	NAT	89.24.1.237	255.255.255.252	89.24.1.238	93.153.117.49, 93.153.117.17	N/A	Connected 8 day 1:50:50	Edit
WAN-2		Disable								Edit

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, etc...
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.
Network Type	N/A	It displays the network type for the WAN interface(s). Depending on the model purchased, it can be NAT, Routing, Bridge, or IP Pass-through.
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 & Uplink > Internet Setup**) and WAN connection status is disconnected. **Disconnect** button allows user to manually disconnect the device from the Internet. Note: **Connect** button is available when Connection Control in WAN Type setting is set to Connect Manually (Refer to **Edit** button in **Basic Network > WAN & Uplink > Internet Setup**) and WAN connection status is connected.

WAN interface IPv6 Network Status

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



❑ WAN Interface IPv6 Network Status

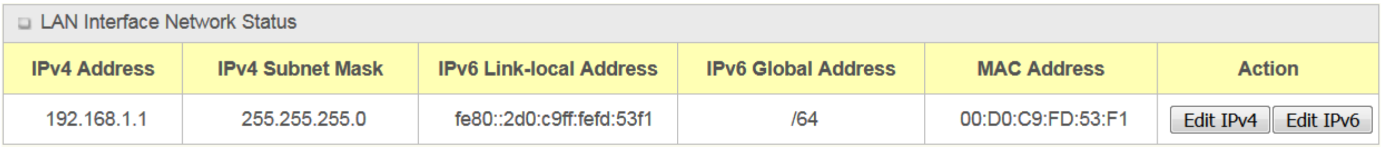
ID	Interface	WAN Type	Link-local IP Address	Global IP Address	Conn. Status	Action
WAN-1		Disable				Edit

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, etc...
WAN Type	N/A	It displays the method which public IP address is obtained from your ISP. WAN type setting can be changed from **Basic Network > IPv6 > Configuration**.
Link-local IP Address	N/A	It displays the LAN IPv6 Link-Local address.
Global IP Address	N/A	It displays the IPv6 global IP address assigned by your ISP for your Internet connection.

Conn. Status	N/A	It displays the connection status. The status can be connected, disconnected and connecting.
Action	N/A	This area provides functional buttons. **Edit Button** when pressed, web-based utility will take you to the IPv6 configuration page. (**Basic Network > IPv6 > Configuration**.)

LAN Interface Network Status

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



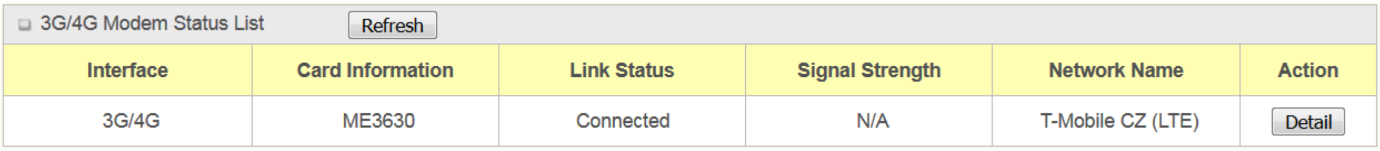
LAN Interface Network Status

IPv4 Address	IPv4 Subnet Mask	IPv6 Link-local Address	IPv6 Global Address	MAC Address	Action
192.168.1.1	255.255.255.0	fe80::2d0:c9ff:fefd:53f1	/64	00:D0:C9:FD:53:F1	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.
MAC Address	N/A	It displays the LAN MAC Address of the router
Action	N/A	This area provides functional buttons. **Edit IPv4 Button** when press, web-based utility will take you to the Ethernet LAN configuration page. (**Basic Network > LAN & VLAN > Ethernet LAN** tab). **Edit IPv6 Button** when press, web-based utility will take you to the IPv6 configuration page. (**Basic Network > IPv6 > Configuration**.)

3G/4G Modem Status

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



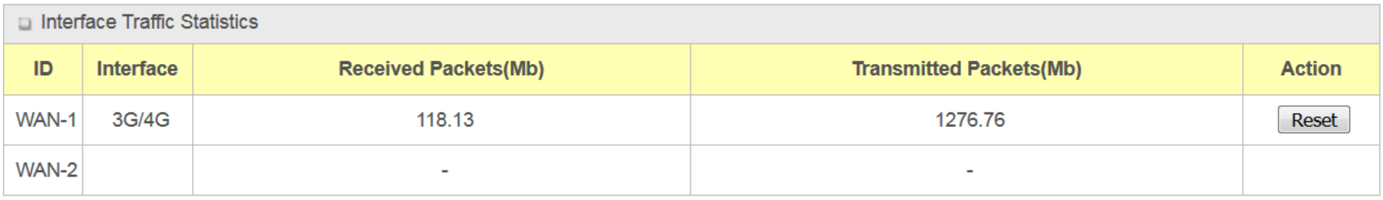
Interface	Card Information	Link Status	Signal Strength	Network Name	Action
3G/4G	ME3630	Connected	N/A	T-Mobile CZ (LTE)	Detail

3G/4G Modem Status List		
Item	**Value setting**	**Description**
Physical Interface	N/A	It displays the type of WAN physical interface. 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.

When the **Detail** button is pressed, 3G/4G modem information windows such as Modem Information, SIM Status, Service Information, Signal Strength / Quality, and Error Message will appear.

Interface Traffic Statistics

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



ID	Interface	Received Packets(Mb)	Transmitted Packets(Mb)	Action
WAN-1	3G/4G	118.13	1276.76	Reset
WAN-2		-	-	

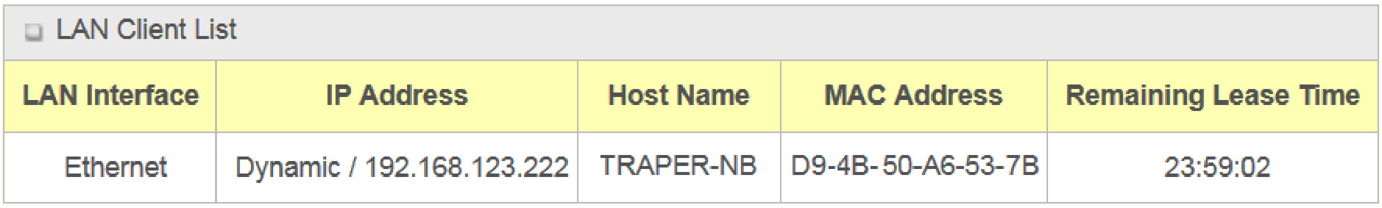
Interface Traffic Statistics		
Item	**Value setting**	**Description**
ID	N/A	It displays corresponding WAN interface WAN IDs.
Interface	N/A	It displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, 3G/4G, etc…
Received Packets (Mb)	N/A	It displays the downstream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

7.1.2 LAN & VLAN Status

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

Client List

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



LAN Client List

LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time
Ethernet	Dynamic / 192.168.123.222	TRAPER-NB	D9-4B-50-A6-53-7B	23:59:02

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.

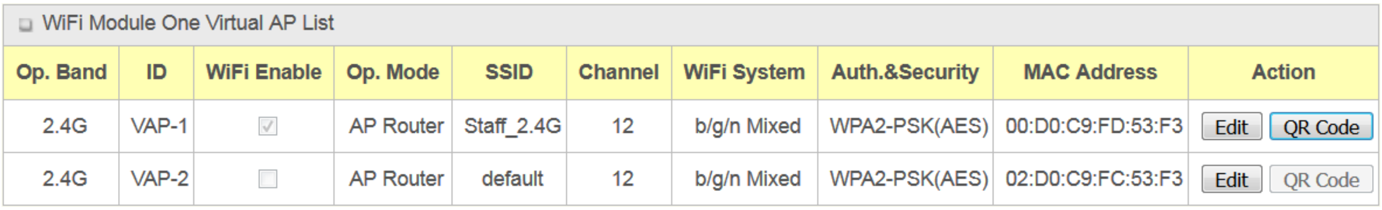
7.1.3 WiFi Status

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

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

WiFi Virtual AP List

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



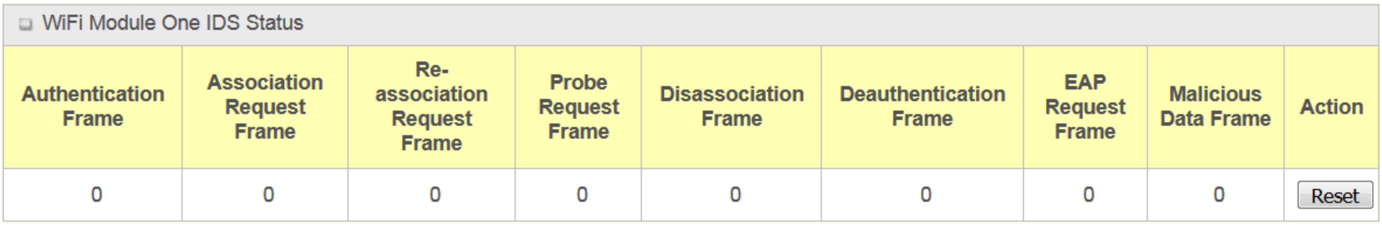
WiFi Module One Virtual AP List

Op. Band	ID	WiFi Enable	Op. Mode	SSID	Channel	WiFi System	Auth.&Security	MAC Address	Action
2.4G	VAP-1	☑	AP Router	Staff_2.4G	12	b/g/n Mixed	WPA2-PSK(AES)	00:D0:C9:FD:53:F3	Edit QR Code
2.4G	VAP-2	☐	AP Router	default	12	b/g/n Mixed	WPA2-PSK(AES)	02:D0:C9:FC:53:F3	Edit QR Code

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

WiFi IDS Status

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



WiFi Module One IDS Status

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

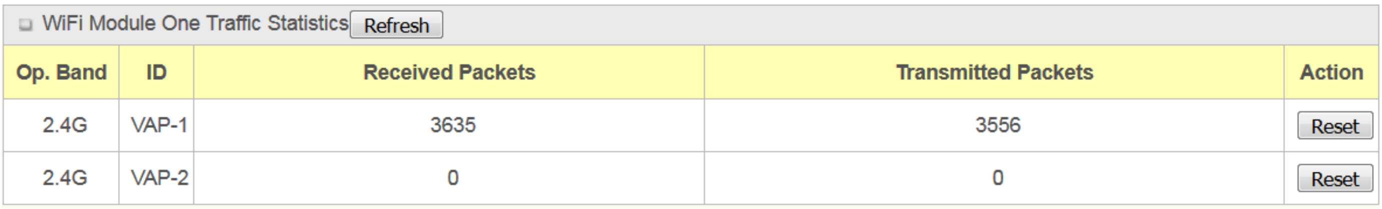
WiFi IDS Status

Item	Value setting	Description
Authentication Frame	N/A	It displays the receiving Authentication Frame count.
Association Request Frame	N/A	It displays the receiving Association Request Frame count.
Re-association Request Frame	N/A	It displays the receiving Re-association Request Frame count.
Probe Request Frame	N/A	It displays the receiving Probe Request Frame count.
Disassociation Frame	N/A	It displays the receiving Disassociation Frame count.
Deauthentication Frame	N/A	It displays the receiving Deauthentication Frame count.
EAP Request Frame	N/A	It displays the receiving EAP Request Frame count.
Malicious Data Frame	N/A	It displays the number of receiving unauthorized wireless packets.
Action	N/A	Click the **Reset** button to clear the entire statistic and reset counter to 0.

- Ensure WIDS function is enabled
- Go to Basic Network > WiFi > Advanced Configuration tab

WiFi Traffic Statistic

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



WiFi Module One Traffic Statistics Refresh

Op. Band	ID	Received Packets	Transmitted Packets	Action
2.4G	VAP-1	3635	3556	Reset
2.4G	VAP-2	0	0	Reset

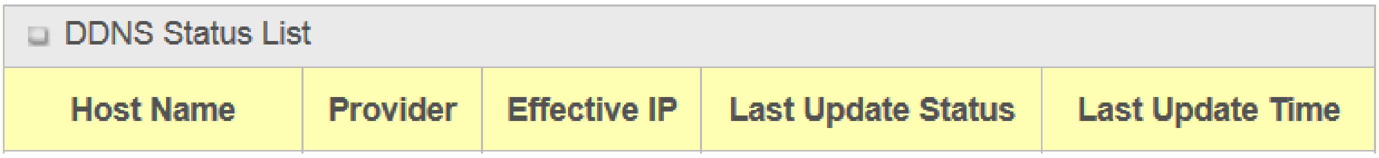
WiFi Traffic Statistic		
Item	**Value setting**	**Description**
Op. Band	N/A	It displays the Wi-Fi Operation Band 2.4G of VAP.
ID	N/A	It displays the VAP ID.
Received Packets	N/A	It displays the number of received packets.
Transmitted Packet	N/A	It displays the number of transmitted packets.
Action	N/A	Click the **Reset** button to clear individual VAP statistics.
Refresh Button	N/A	Click the **Refresh** button to update the entire VAP Traffic Statistic instantly.

7.1.4 DDNS Status

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

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

DDNS Status

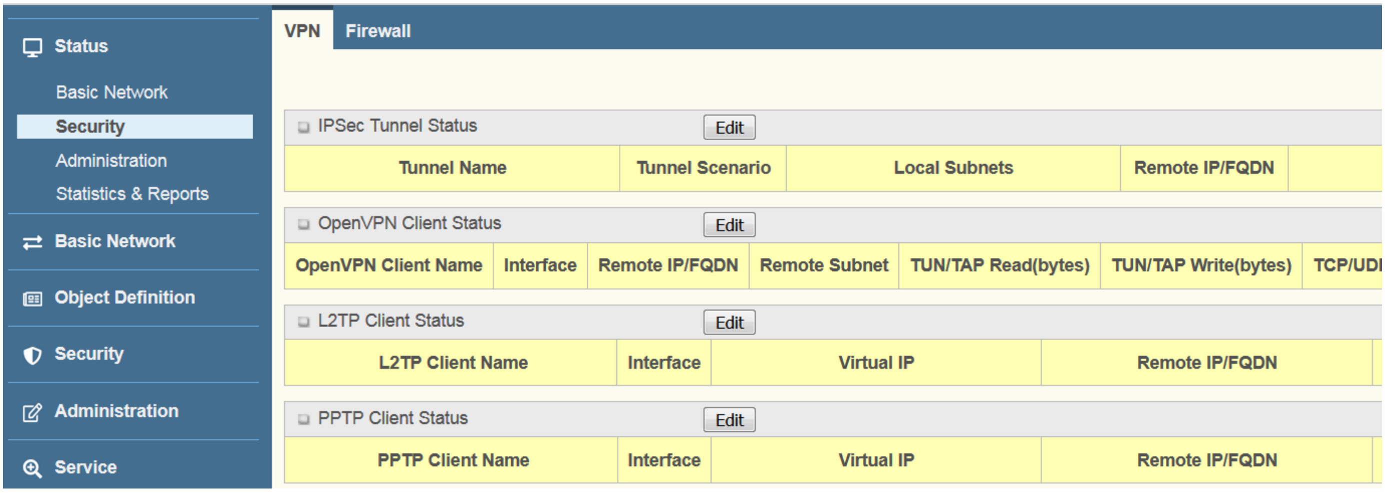


DDNS Status List

Host Name	Provider	Effective IP	Last Update Status	Last Update Time

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

7.2 Security



IPSec Tunnel Status

Tunnel Name	Tunnel Scenario	Local Subnets	Remote IP/FQDN

OpenVPN Client Status

OpenVPN Client Name	Interface	Remote IP/FQDN	Remote Subnet	TUN/TAP Read(bytes)	TUN/TAP Write(bytes)	TCP/UDI

L2TP Client Status

L2TP Client Name	Interface	Virtual IP	Remote IP/FQDN

PPTP Client Status

PPTP Client Name	Interface	Virtual IP	Remote IP/FQDN

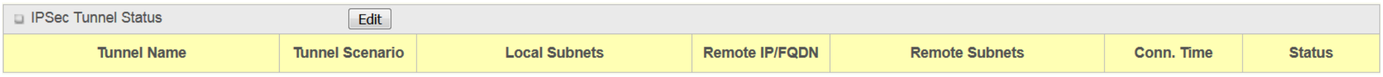
7.2.1 VPN Status

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

The **VPN Status** widow shows the overall VPN tunnel status. The display will be refreshed on every five seconds.

IPSec Tunnel Status

IPSec Tunnel Status windows show the configuration for establishing IPSec VPN connection and current connection status.

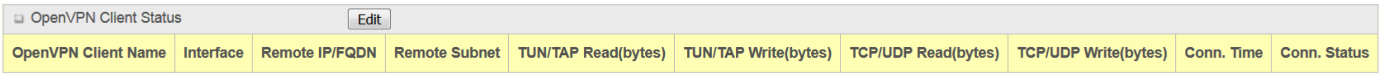


IPSec Tunnel Status

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

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

OpenVPN Client Status



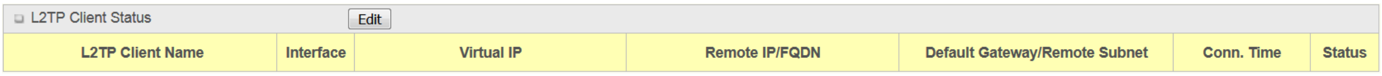
OpenVPN Client Status Edit

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

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

L2TP Client Status

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



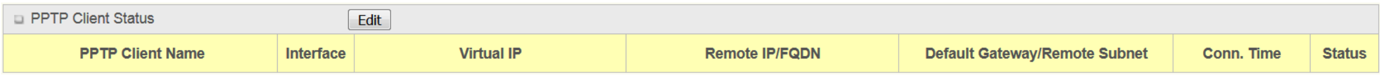
L2TP Client Status Edit

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

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

PPTP Client Status

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



PPTP Client Status Edit

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

PPTP Client Status

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

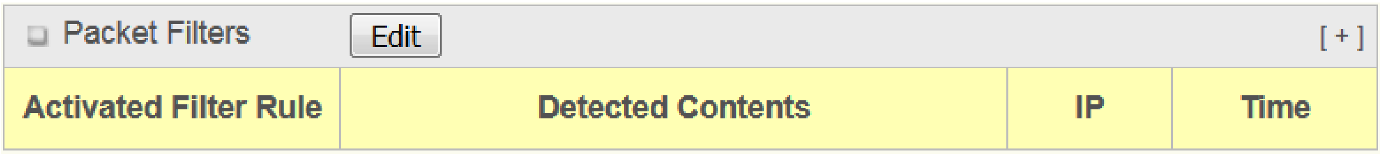
7.2.2 Firewall Status

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

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

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

Packet Filter Status



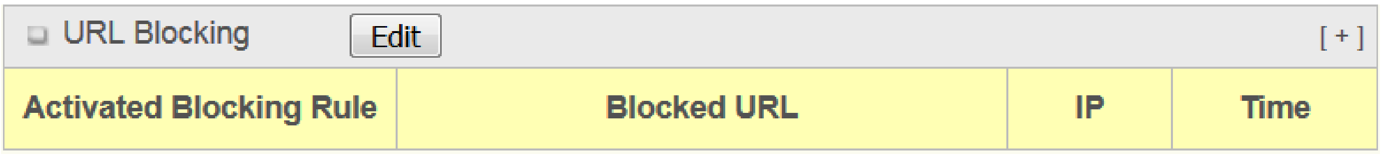
□ Packet Filters Edit [+]

Activated Filter Rule	Detected Contents	IP	Time

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

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

URL Blocking Status



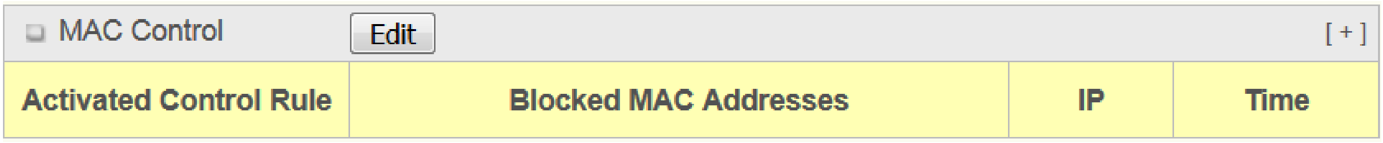
□ URL Blocking Edit [+]

Activated Blocking Rule	Blocked URL	IP	Time

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

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

MAC Control Status



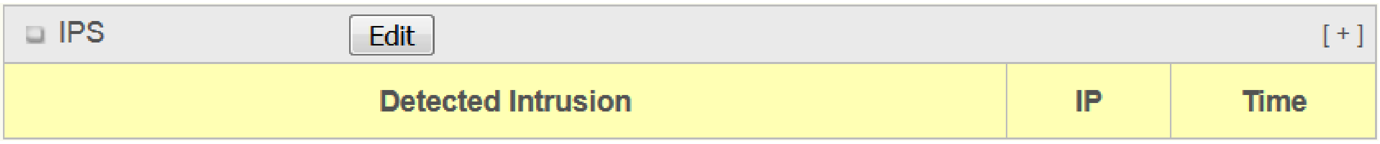
MAC Control	Edit		[+]
Activated Control Rule	Blocked MAC Addresses	IP	Time

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

Note: Ensure MAC Control Log Alert is enabled.

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

IPS Status



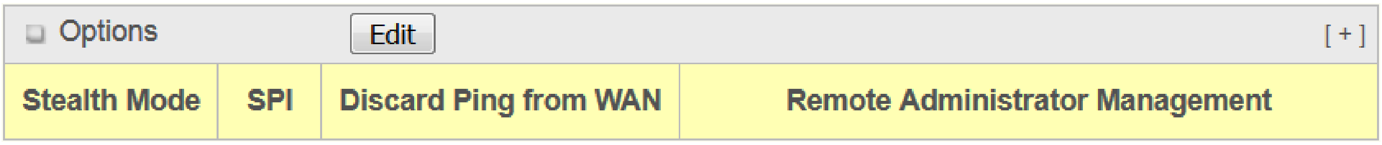
IPS	Edit		[+]
Detected Intrusion		IP	Time

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

Note: Ensure IPS Log Alert is enabled.

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

Firewall Options Status



□ Options Edit [+]

Stealth Mode	SPI	Discard Ping from WAN	Remote Administrator Management

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

Note: Ensure Firewall Options Log Alert is enabled.

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

7.3 Administration

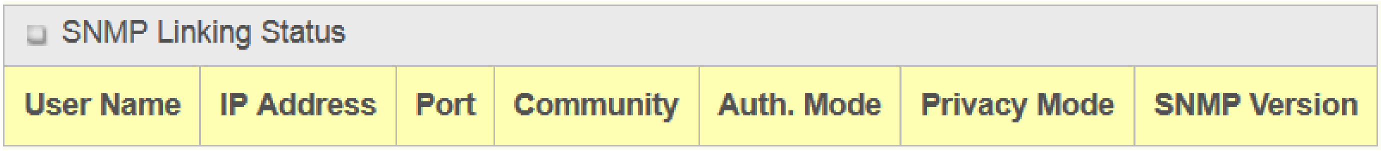
7.3.1 Configure & Manage Status

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

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

SNMP Linking Status

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



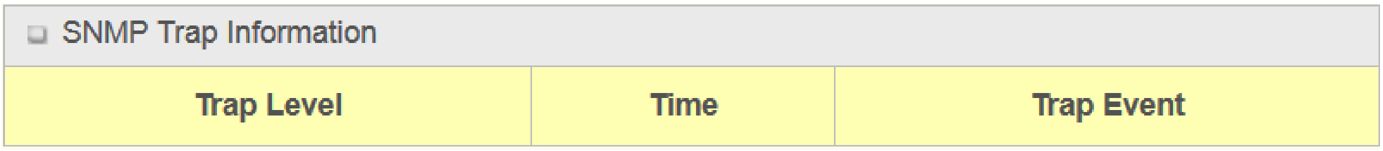
SNMP Linking Status

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

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

SNMP Trap Information

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



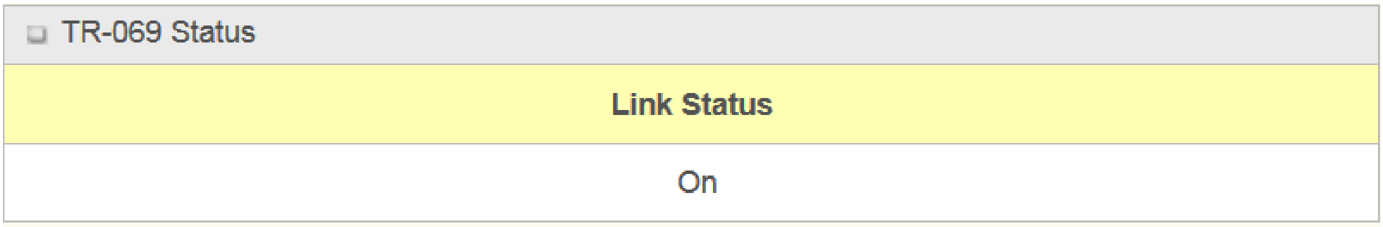
SNMP Trap Information

Trap Level	Time	Trap Event

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

TR-069 Status

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

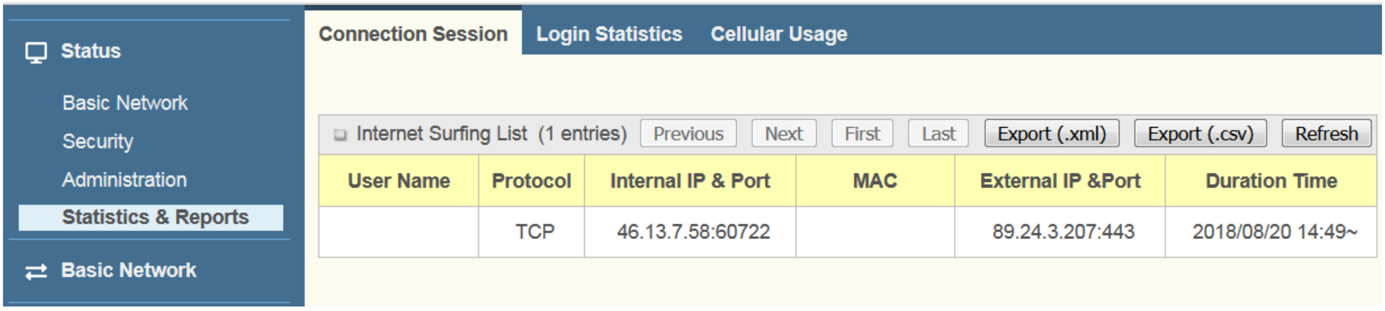


TR-069 Status

Link Status
On

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.

7.4 Statistics & Report



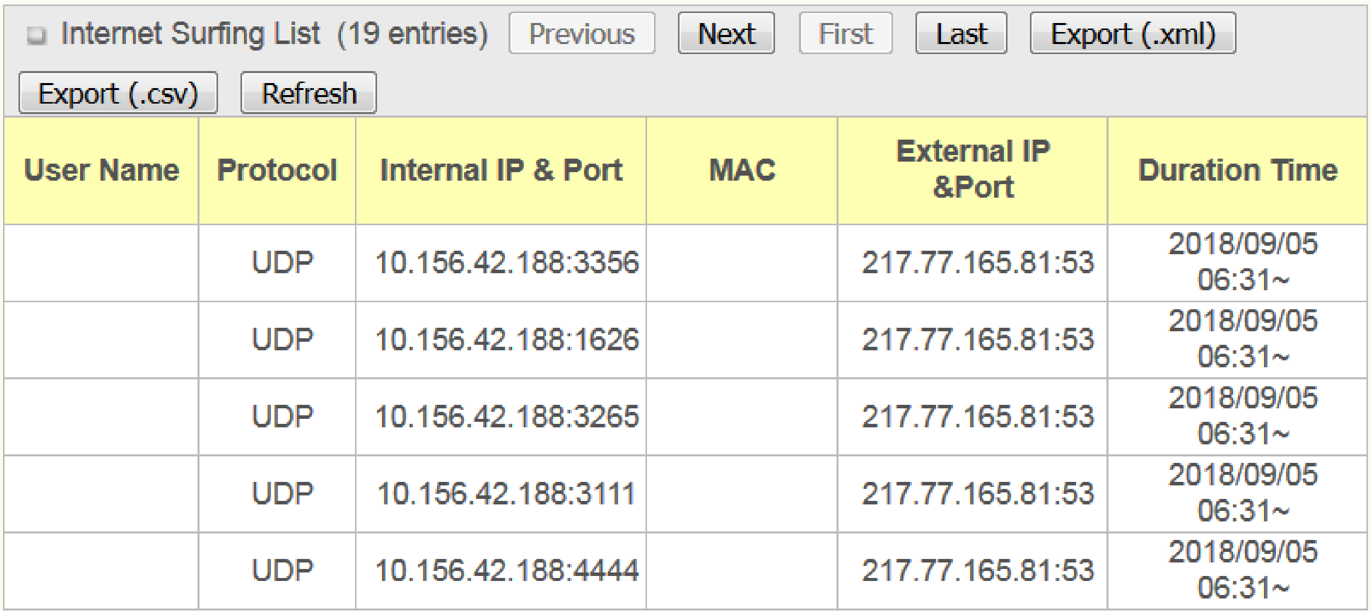
Internet Surfing List (1 entries) Previous Next First Last Export (.xml) Export (.csv) Refresh

User Name	Protocol	Internal IP & Port	MAC	External IP &Port	Duration Time
	TCP	46.13.7.58:60722		89.24.3.207:443	2018/08/20 14:49~

7.4.1 Connection Session

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

Internet Surfing Statistic shows the connection tracks on this router.



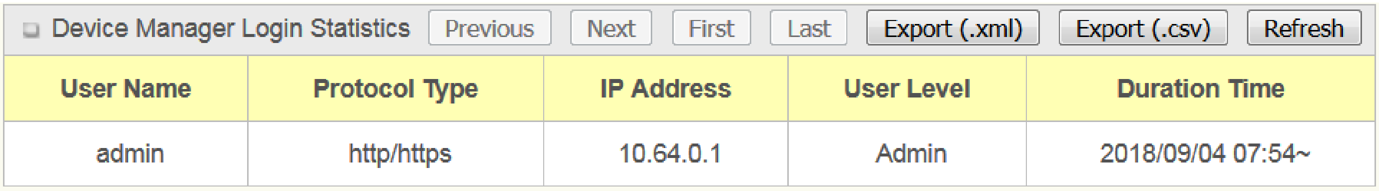
User Name	Protocol	Internal IP & Port	MAC	External IP &Port	Duration Time
	UDP	10.156.42.188:3356		217.77.165.81:53	2018/09/05 06:31~
	UDP	10.156.42.188:1626		217.77.165.81:53	2018/09/05 06:31~
	UDP	10.156.42.188:3265		217.77.165.81:53	2018/09/05 06:31~
	UDP	10.156.42.188:3111		217.77.165.81:53	2018/09/05 06:31~
	UDP	10.156.42.188:4444		217.77.165.81:53	2018/09/05 06:31~

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

7.4.2 Device Administration

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

Login Statistics shows the login information.



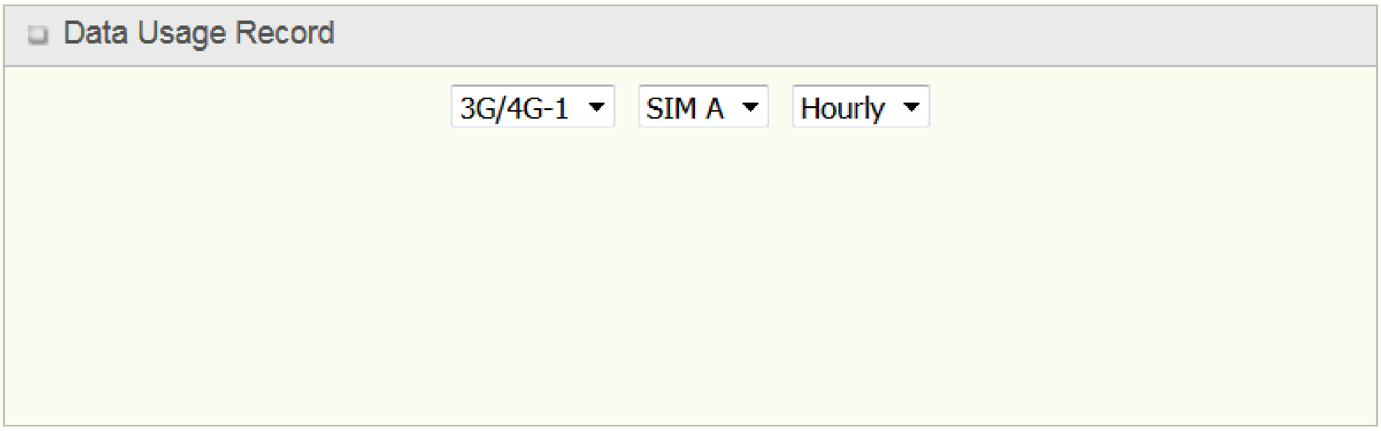
User Name	Protocol Type	IP Address	User Level	Duration Time
admin	http/https	10.64.0.1	Admin	2018/09/04 07:54~

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

7.4.3 Cellular Usage

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

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



Data Usage Record

3G/4G-1 ▾ SIM A ▾ Hourly ▾

8. GPL Written Offer

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

GPSBabel
Version 1.4.4
Copyright (C) 2002-2005 Robert Lipe<robertlipe@usa.net>
GPL License: https://www.gpsbabel.org/

Curl
Version 7.19.6
Copyright (c) 1996-2009, Daniel Stenberg, <daniel@haxx.se>.
MIT/X derivate License: https://curl.haxx.se/

OpenSSL
Version 1.0.2c
Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
GPL License: https://www.openssl.org/

brctl - ethernet bridge administration
Stephen Hemminger <shemminger@osdl.org>
Lennert Buytenhek <buytenh@gnu.org>
version 1.1
GNU GENERAL PUBLIC LICENSE Version 2, June 1991

tc - show / manipulate traffic control settings
Stephen Hemminger<shemminger@osdl.org>
Alexey Kuznetsov<kuznet@ms2.inr.ac.ru>
version iproute2-ss050330
GNU GENERAL PUBLIC LICENSE Version 2, June 1991

dhcp-fwd — starts the DHCP forwarding agent
Enrico Scholz <enrico.scholz@informatik.tu-chemnitz.de>
version 0.7
GNU GENERAL PUBLIC LICENSE Version 2, June 1991

lftp - Sophisticated file transfer program
Alexander V. Lukyanov <lav@yars.free.net>
version:4.5.x
Copyright (c) 1996-2014 by Alexander V. Lukyanov (lav@yars.free.net)

dnsmasq - A lightweight DHCP and caching DNS server.
Simon Kelley <simon@thekelleys.org.uk>
version:2.72
dnsmasq is Copyright (c) 2000-2014 Simon Kelley

socat - Multipurpose relay
Version: 2.0.0-b8
GPLv2
http://www.dest-unreach.org/socat/

LibModbus
Version: 3.0.3
LGPL v2
http://libmodbus.org/news/

LibIEC60870
GPLv2
Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
https://sourceforge.net/projects/mrts/

Openswan
Version: v2.6.38 GNU GENERAL PUBLIC LICENSE Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
https://www.openswan.org/

Opennhrp
Version: v0.14.1
OpenNHRP is an NHRP implementation for Linux. It has most of the RFC2332
and Cisco IOS extensions.
Project homepage: http://sourceforge.net/projects/opennhrp
Git repository: git://opennhrp.git.sourceforge.net/gitroot/opennhrp
LICENSE
OpenNHRP is licensed under the MIT License. See MIT-LICENSE.txt for
additional details.
OpenNHRP embeds libev. libev is dual licensed with 2-clause BSD and
GPLv2+ licenses. See libev/LICENSE for additional details.
OpenNHRP links to c-ares. c-ares is licensed under the MIT License.
https://sourceforge.net/projects/opennhrp/

IPSec-tools
Version: v0.8
No GPL be written
http://ipsec-tools.sourceforge.net/

PPTP
Version: pptp-1.7.1
GNU GENERAL PUBLIC LICENSE Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.
http://pptpclient.sourceforge.net/

PPTPServ
Version: 1.3.4
GNU GENERAL PUBLIC LICENSE Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. http://poptop.sourceforge.net/

L2TP
Version: 0.4
Copying All software included in this package is Copyright 2002 Roaring
Penguin Software Inc. You may distribute it under the terms of the GNU General Public License (the "GPL"), Version 2, or (at your option) any later version.
http://www.roaringpenguin.com/

L2TPServ
Version: v 1.3.1 GNU GENERAL PUBLIC LICENSEVersion 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.
http://www.xelerance.com/software/xl2tpd/

Mpstat: from sysstat, system performance tools for Linux
Version: 10.1.6
Copyright: (C) 1999-2013 by Sebastien Godard (sysstat <at> orange.fr)

SSHD: dropbear, a SSH2 server
Version: 0.53.1
Copyright: (c) 2002-2008 Matt Johnston

Libncurses: The ncurses (new curses) library is a free software emulation of curses in System V Release 4.0 (SVr4), and more.
Version: 5.9
Copyright: (c) 1998, 2000, 2004, 2005, 2006, 2008, 2011, 2015 Free Software Foundation, Inc., 51 Franklin Street, Boston, MA 02110-1301, USA

MiniUPnP: The miniUPnP daemon is an UPnP IGD (internet gateway device) which provide NAT traversal services to any UPnP enabled client on the network.
Version: 1.7
Copyright: (c) 2006-2011, Thomas BERNARD

CoovaChilli is an open-source software access controller for captive portal (UAM) and 802.1X access provisioning.
Version: 1.3.0
Copyright: (C) 2007-2012 David Bird (Coova Technologies) <support@coova.com>

Krb5: Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.
Version: 1.11.3
Copyright: (C) 1985-2013 by the Massachusetts Institute of Technology and its contributors

OpenLDAP: a suite of the Lightweight Directory Access Protocol (v3) servers, clients, utilities, and development tools.
Version: 2.4
Copyright: 1998-2014 The OpenLDAP Foundation

Samba3311: the free SMB and CIFS client and server for UNIX and other operating systems
Version: 3.3.11
Copyright: (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>

NTPClient: an NTP (RFC-1305, RFC-4330) client for unix-alike computers
Version: 2007_365
Copyright: 1997, 1999, 2000, 2003, 2006, 2007 Larry Doolittle

exFAT: FUSE-based exFAT implementation
Version: 0.9.8
Copyright: (C) 2010-2012 Andrew Nayenko

ONTFS_3G: The NTFS-3G driver is an open source, freely available read/write NTFS driver for Linux, FreeBSD, Mac OS X, NetBSD, Solaris and Haiku.
Version: 2009.4.4
Copyright: (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

mysql-5_1_72: a release of MySQL, a dual-license SQL database server
Version: 5.1.72
Copyright: (c) 2000, 2013, Oracle and/or its affiliates
FreeRadius: a high performance and highly configurable RADIUS server
Version: 2.1.12
Copyright: (C) 1999-2011 The FreeRADIUS server project and contributors

Linux IPv6 Router Advertisement Daemon – **radvd**
Version: V 1.15
Copyright (c) 1996,1997 by Lars Fenneberg<lf@elemental.net>
BSD License: http://www.litech.org/radvd/

WIDE-DHCPv6
Dynamic Host Configuration Protocol for IPv6 (DHCPv6) clients, servers, and relay agents.
Version: 20080615
Copyright (C) 1998-2004 WIDE Project.
BSD License: https://sourceforge.net/projects/wide-dhcpv6/

9. Recommended literature

[1] Advantech B+B SmartWorx: **Start Guide for ICR-1601**,

[2] Advantech B+B SmartWorx: **ICR-1601 User Manual**.

Product related documents and applications can be obtained on Engineering Portal at https://ep.advantech-bb.cz/ address.

10. Customers Support

10.1 Customer Support for NAM

E-mail: support@advantech-bb.com
Web: www.advantech-bb.com

10.2 Customer Support for Europe

E-mail: iiotcustomerservice@advantech.eu
Web: www.advantech-bb.com

10.3 Customer Support for Asia

E-mail: icg.support@advantech.com.tw
Web: www.advantech.com

Upkeep – Advices:

- The SIM-card must be handled carefully as with a credit card. Don't bend, don't scratch on this and do not expose to static electricity.
- During cleaning of the router do not use aggressive chemicals, solvents and abrasive cleaners!

CE Hereby, Advantech Co., Ltd. company declares that the radio equipment type ICR-1601 is in compliance with EU Directive **2014/53/EU**.

The full text of the EU Declaration of Conformity is available at the following internet address: www.advantech-bb.cz/eudoc.