M2M Cellular Gateway

IDG500 / IOG500 (LTE cat. 4)

User Manual

M2M Cellular Gateway

Chapter 1 Introduction

1.1 Introduction

Congratulations on your purchase of this outstanding product: M2M Cellular Gateway. For M2M (Machine-to-Machine) applications, AMIT M2M Cellular Gateway is absolutely the right choice. With built-in world-class 3G/4G module, you just need to insert SIM card from local mobile carrier to get to Internet. By VPN tunneling technology, remote sites easily become a part of Intranet, and all data are transmitted in a secure (256-bit AES encryption) link.

Main 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.

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

1.2 Contents List

1.2.1 Package Contents

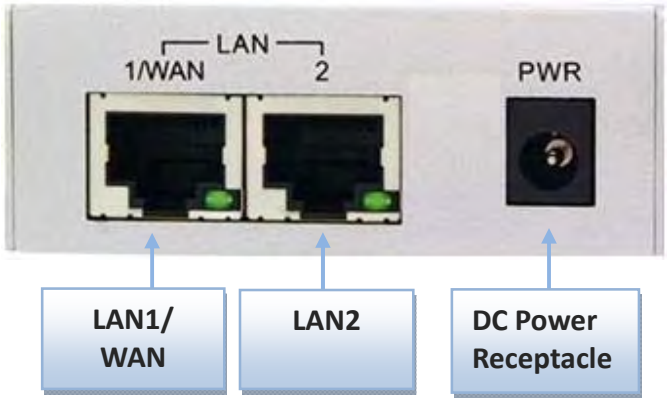
#Standard Package

Items	Description	Contents	Quantity
1	**IDG500** **M2M Cellular Gateway**		1pcs
2	**Power Adapter** **(DC 5V/2A)** (*[1])		1pcs
3	**DIN-Rail Bracket**		1 set (2pcs)
4	**Male DC Jack to Screw Terminal Block Adaptor**		1pcs
5	**Rubber Feet**		4pcs
6	**CD** **(Manual)**		1pcs

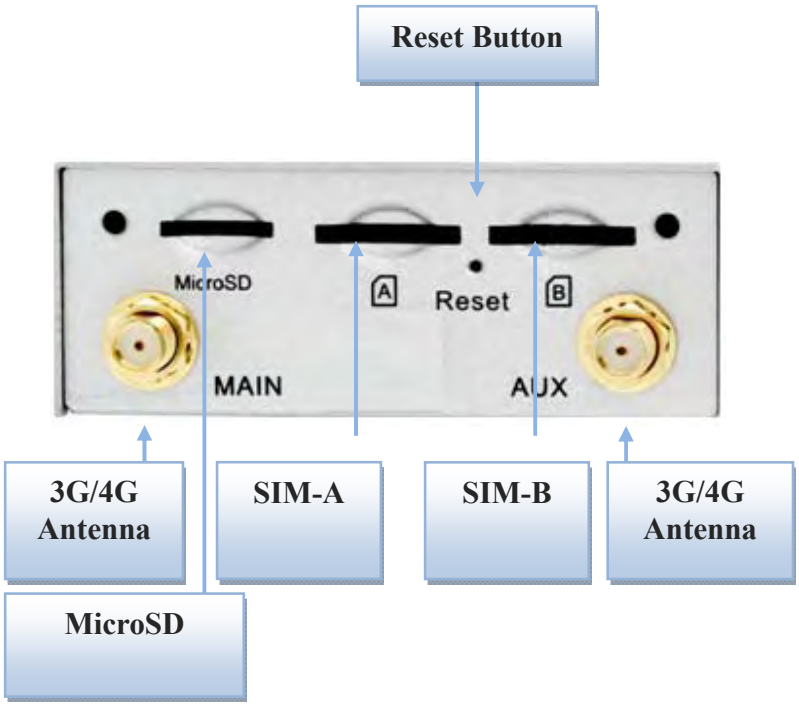
1 The maximum power consumption of IDG500 series product is 7.0W.

1.3 Hardware Configuration

➢ Left View



➢ Right View



※Reset Button

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

1.4 LED Indication

Indication	LED Color	Description
Signal LTE/3G	Blue Purple Red	When the LED color is shown in: • **Blue:** Cellular module is in LTE Mode. • **Purple:** Cellular module is in HSPA/3G Mode. • **Red:** Cellular module is in GSM/2G Mode. When the behavior of LED is: • **Fast Flash (per 0.5 second):** Signal Strength is 0~30% • **Flash (Slow, per second):** Signal Strength is 31~60% • **Steady On:** Signal Strength is 61~100%
Status	Blue	**Flash (per second):** The gateway works normally. **Flash (Fast):** The gateway is in Recovery Mode or abnormal situation. **Note:** If you encountered the abnormal situation, even power OFF / ON the device, there might be something wrong during the device boot up session and it was damaged. You need to call for RMA service to recover it.
LAN/WAN	Green	**Off:** Host disconnected. **On:** Ethernet connection established. **Flash:** Data packet transferred via Ethernet.

1.5 Installation & Maintenance Notice

1.5.1 SYSTEM REQUIREMENTS

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

1.5.2 WARNING

Attention

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

1.5.3 HOT SURFACE CAUTION

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

1.5.4 Product Information for CE RED Requirements

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

(1) Frequency Band & Maximum Power

1.a Frequency Band for Cellular Connection (for ME3630 E1C version) [3]

Band number	Operating Frequency	Max output power
LTE FDD BAND 1	Uplink: 1920-1980 MHz Downlink: 2110-2170 MHz	23 ±2.7 dBm
LTE FDD BAND 3	Uplink: 1710-1785 MHz Downlink: 1805-1880 MHz	
LTE FDD BAND 7	Uplink: 2500-2570 MHz Downlink: 2620-2690 MHz	
LTE FDD BAND 8	Uplink: 880-915 MHz Downlink: 925-960 MHz	
LTE FDD BAND 20	Uplink: 832-862 MHz Downlink: 791-821 MHz	
WCDMA BAND 1	Uplink: 1920-1980 MHz Downlink: 2110-2170 MHz	24 +1/-3 dBm
WCDMA BAND 8	Uplink: 880-915 MHz Downlink: 925-960 MHz	
E-GSM	Uplink: 880-915 MHz Downlink: 925-960 MHz	33 ±2 dBm
DCS	Uplink: 1710-1785 MHz Downlink: 1805-1880 MHz	30 ±2 dBm

1.b Frequency Band for Cellular Connection (for EC25-E version)

Band number	Operating Frequency	Max output power
LTE FDD BAND 1	Uplink: 1920-1980 MHz Downlink: 2110-2170 MHz	23.1 dBm
LTE FDD BAND 3	Uplink: 1710-1785 MHz Downlink: 1805-1880 MHz	23.0 dBm
LTE FDD BAND 7	Uplink: 2500-2570 MHz Downlink: 2620-2690 MHz	22.8 dBm
LTE FDD BAND 8	Uplink: 880-915 MHz Downlink: 925-960 MHz	23.2 dBm
LTE FDD BAND 20	Uplink: 832-862 MHz	23.5 dBm

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

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

	Downlink: 791-821 MHz	
LTE FDD BAND 38	Uplink: 2570-2620 MHz Downlink: 2570-2620 MHz	21.7 dBm
LTE FDD BAND 40	Uplink: 2300-2400 MHz Downlink: 2300-2400 MHz	21.5 dBm
WCDMA BAND 1	Uplink: 1920-1980 MHz Downlink: 2110-2170 MHz	23.3 dBm
WCDMA BAND 8	Uplink: 880-915 MHz Downlink: 925-960 MHz	
E-GSM	Uplink: 880-915 MHz Downlink: 925-960 MHz	32.9 dBm
DCS	Uplink: 1710-1785 MHz Downlink: 1805-1880 MHz	29.9 dBm

1.c Frequency Band for Cellular Connection (for UC20-G version)

Band number	Operating Frequency	Max output power
WCDMA BAND 1	Uplink: 1922.4-1977.6 MHz Downlink: 2112.4-2167.6 MHz	22.47 dBm
WCDMA BAND 8	Uplink: 882.4-912.6 MHz Downlink: 927.4-957.6 MHz	22.48 dBm
E-GSM	Uplink: 880.2-914.8 MHz Downlink: 925.2-959.8 MHz	32.1 dBm
DCS	Uplink: 1710.2-1784.8 MHz Downlink: 1805.2-1879.8 MHz	28.9 dBm

(2) DoC Information

You can get the DoC information of this product from the following URL:
http://www.amit.com.tw/products-doc/

(3) RF Exposure Statements

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

1.6 Hardware Installation

This chapter describes how to install and configure the hardware

1.6.1 Mount the Unit

The IDG500 series can be placed on a desktop, or mounted on the wall.

1.6.2 Insert the SIM Card

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

The SIM card slots are located at the right side of IDG500 series housing in order to protect the SIM card. You need to unscrew and remove the outer SIM card cover before installing or removing the SIM card. Please follow the instructions to insert or eject a SIM card. After SIM card is well placed, screw back the outer SIM card cover.

Step 1:
Loosen the screws and remove the SIM cover.

Step 2:
Push the SIM card into the slot A (SIM-A) or slot B (SIM-B).

Step 3:
Push the inserted SIM card again to eject it from the SIM slot.

1.6.3 Install the External Antenna

As illustrated in Section 1.3, there are several SMA antenna Jacks for you to install the required antennas for the RF signal transmission and receiving. You have to purchase required RF cables and antennas separately for a specific project or installation site to get excellent RF performance.

Since there is limited spacing for allocating all SMA antenna Jacks around the enclosure, the separation among SMA Jacks (or direct-attached antennas) could be not the optimized arrangement. It is very likely to get degraded RF performance at specific circumstances. It depends heavily on the environment.

However, there are well-known rules of thumb for solving the antenna separation issue.

1. ***The horizontal distance between antennas should be greater than 1/4 of its wavelength, and there will be best separation at 1/2 of its wavelength.***

2. ***If multiple frequency antennas are near each other, then use spacing distance of the lower frequency antenna, or even better try to satisfy the rule for both frequencies.***

Wavelength Table for Major RF Category

RF Category	Frequency	Wavelength	1/2 Wave Length (Best Separation)	1/4 Wave Length (Good Separation)
Celllular LTE	2600MHz	11.5cm	5.8cm	2.9cm
Cellular LTE	2100MHz	14.3cm	7.1cm	3.7cm
Cellular LTE	900MHz	33.3cm	16.6cm	8.3cm
Cellular LTE	700MHz	42.8cm	21.4cm	10.7cm

So, it is recommended to use some external RF cables to extend and separate the adjacent antennas and get better antenna separation and RF performance.

1.6.4 Connecting Power

There are a DC5V/2A power adapter[4] and a 2-pin Terminal Block adapter in the package for you to easily connect DC power to this gateway.

If you powered the gateway with other DC Power Source, Please make sure the DC Power voltage is comply to 5V ~ 18V, and the electrodes have been plugged into the right pins according to their assignments ('+' for the DC Power and '-' for the GND wire).

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

1.6.5 Connecting to the Network or a Host

The IDG500 series product provides one RJ45 port to connect 10/100Mbps Ethernet. It can auto detect the transmission speed on the network and configure itself automatically. Connect one Ethernet cable to the RJ45 port (LAN) of the device and plug another end of the Ethernet cable into your computer's network port. In this way, you can use the RJ45 Ethernet cable to connect the device to the host PC's Ethernet port for configuring the device.

4 The maximum power consumption of IDG500 series product is 7.0W.

1.6.6 Setup by Configuring WEB UI

You can browse web UI to configure the device.

Type in the IP Address (**http://192.168.123.254**)[5]

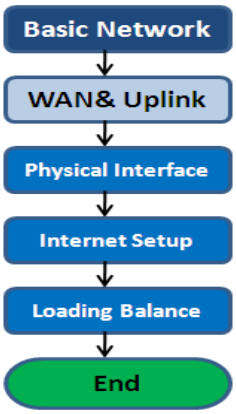
When you see the login page, enter the user name and password and then click **'Login'** button.
The default setting for both username and password is **'admin'** [6].

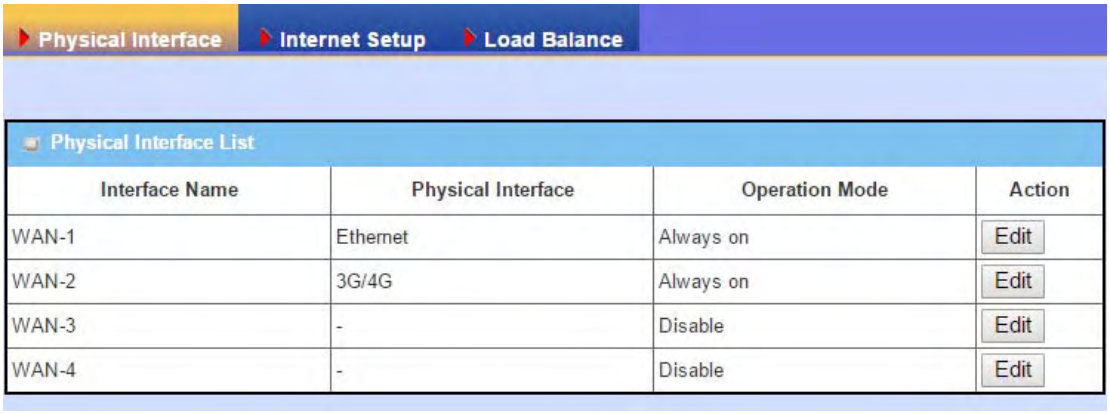
5 The default LAN IP address of this gateway is 192.168.123.254. If you change it, you need to login by using the new IP address.

6 For security consideration, you are strongly recommended to change the login username and password from default values. Refer to Section 6.1.2 for how to change the setting.

Chapter 2 Basic Network

2.1 WAN & Uplink

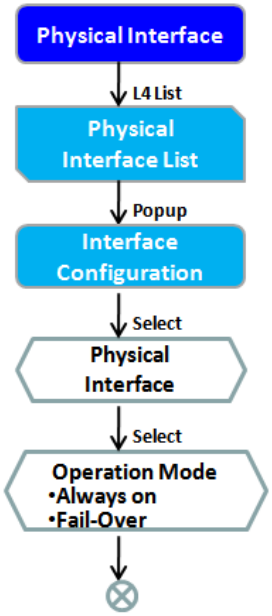




The gateway provides multiple WAN interfaces to let all client hosts in Intranet of the gateway access the Internet via ISP. But ISPs in the world apply various connection protocols to let gateways or user's devices dial in ISPs and then link to the Internet via different kinds of transmit media.

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

2.1.1 Physical Interface



Physical Interface List

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

Interface Configuration (WAN - 1)

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

M2M gateways 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 gateway has one or more RJ45 WAN ports 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 gateway 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.

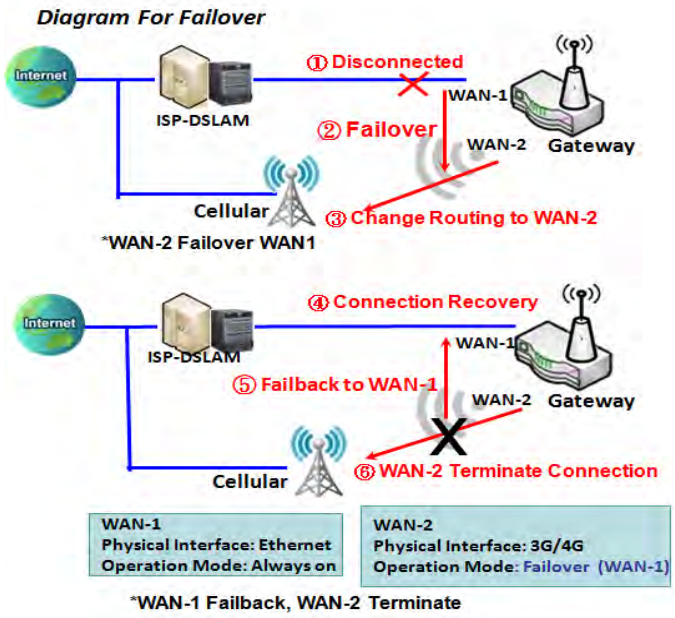
- Please **MUST POWER OFF** the gateway before you insert or remove SIM card.
- The SIM card can be damaged if you insert or remove SIM card while the gateway is in operation.

Operation Mode:

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

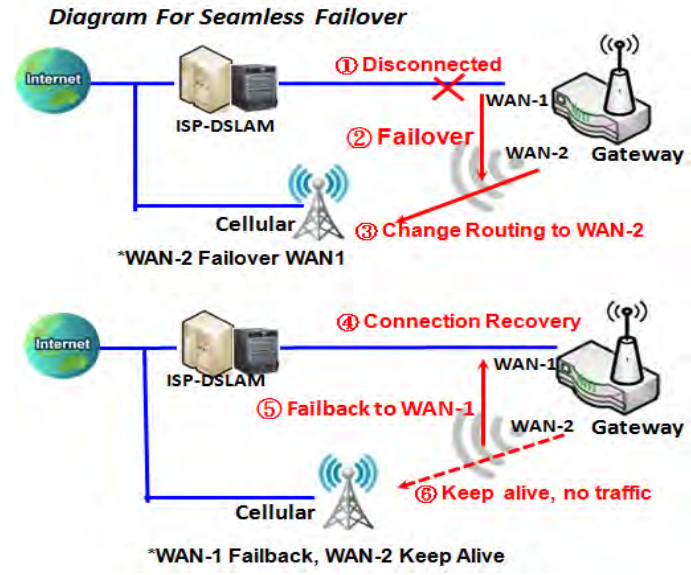
Always on: Set this WAN interface to be active all the time. When two or more WAN are established at "Always on" mode, outgoing data will through these WAN connections base on load balance policies.

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 Gateway 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 > Physical Interface** tab.

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

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

Physical Interface List

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

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

Interface Configuration:

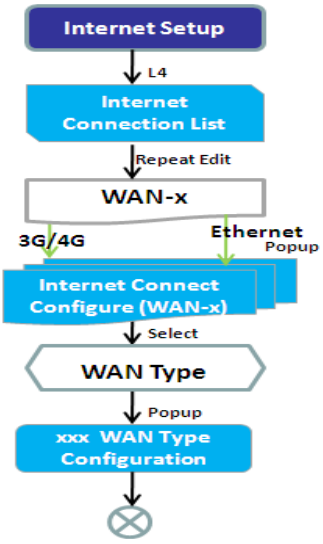
Interface Configuration (WAN - 1)

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

Interface Configuration		
Item	**Value setting**	**Description**
Physical Interface	1. A Must fill setting 2. WAN-1 is the primary interface and is factory set to Always on.	Select one expected interface from the available interface dropdown list. It can be **3G/4G** or **Etherent**. Depending on the gateway model, **Disable** and **Failover** options will be available only to multiple WAN gateways. WAN-2 ~ WAN-4 interfaces are only available to multiple WAN gateway.

Operation Mode	A Must fill setting	Define the operation mode of the interface. Select **Always on** to make this WAN always active. Select **Disable** to disable this WAN interface. Select **Failover** to make this WAN a Failover WAN when the primary or the secondary WAN link failed. Then select the primary or the existed secondary WAN interface to switch Failover from. (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 Internet Setup



Internet Connection List

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

Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	Dynamic IP

Dynamic IP WAN Type Configuration

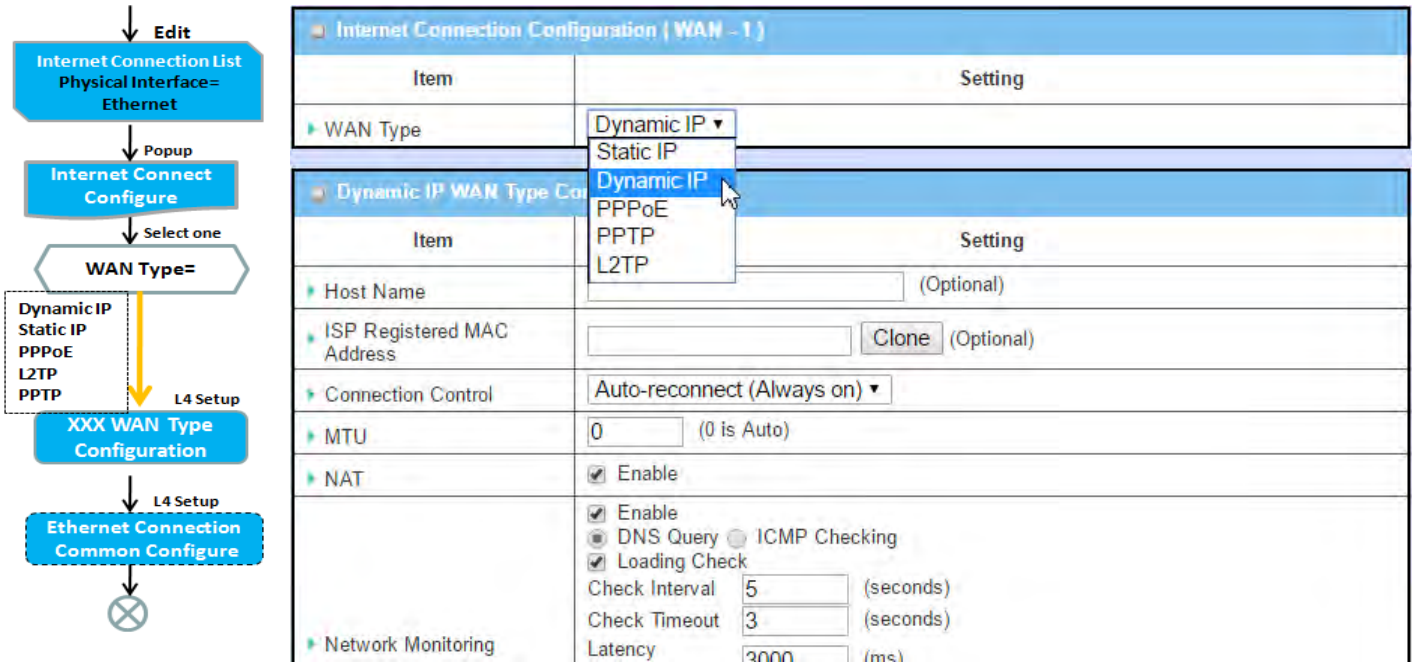
Item	Setting
Host Name	(Optional)
ISP Registered MAC Address	Clone (Optional)
Connection Control	Auto-reconnect
MTU	0 (0 is Auto)
NAT	Enable

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 gateway can access the Internet.

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

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

Internet Connection List - Ethernet WAN



WAN Type for Ethernet Interface:

Ethernet is the most common WAN and uplink interface for M2M gateways. 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 subsribe the service. Usually is more expensive but very importat 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

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

WAN Type = Dynamic IP

Internet Connection Configuration (WAN - 1)	
Item	Setting
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

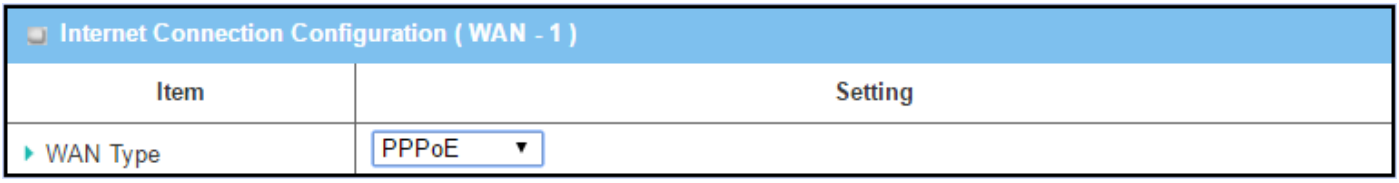
Internet Connection Configuration (WAN - 1)	
Item	Setting
WAN Type	Static IP ▾

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

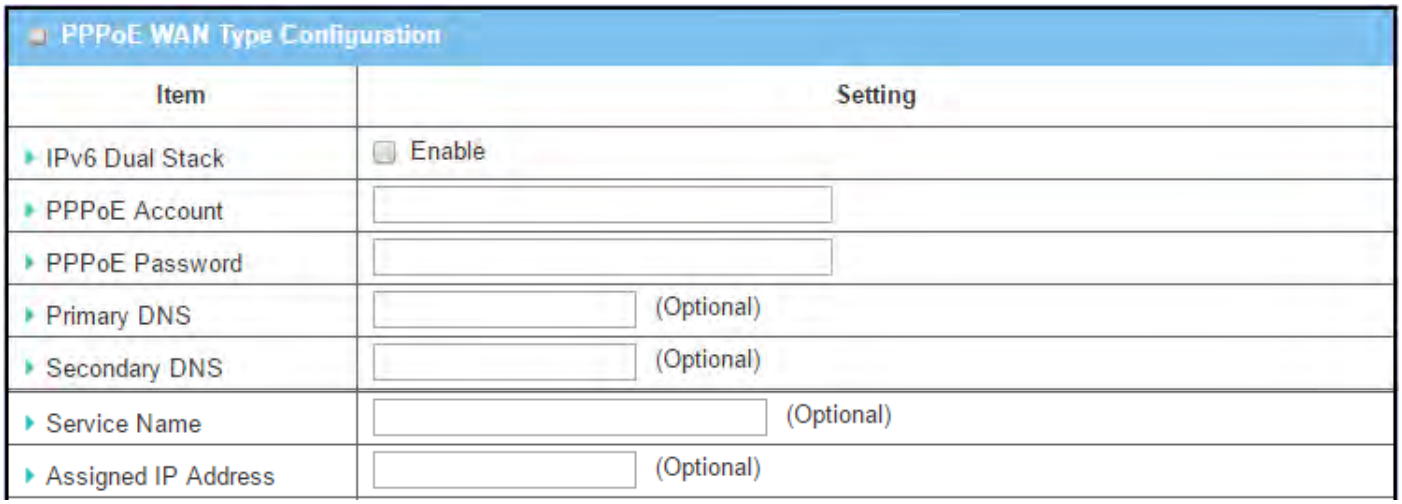
Static IP WAN Type Configuration	
Item	Setting
WAN IP Address	
WAN Subnet Mask	255.255.255.0 (/24) ▾
WAN Gateway	
Primary DNS	
Secondary DNS	(Optional)

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

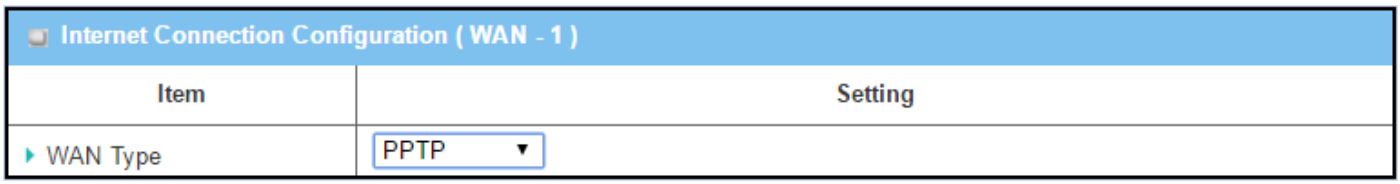


When you select it, "PPPoE WAN Type Configuration" will appear. Items and setting is explained below

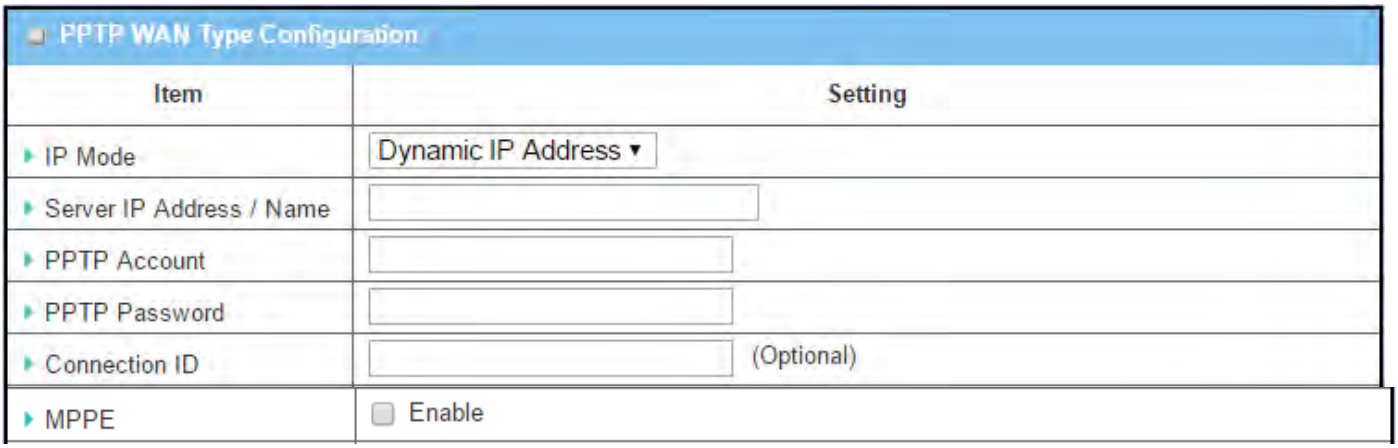


PPPoE WAN Type Configuration		
Item	**Value setting**	**Description**
PPPoE Account	A Must filled setting	Enter the PPPoE User Name provided by your Service Provider.
PPPoE Password	A Must filled setting	Enter the PPPoE password provided by your Service Provider.
Primary DNS	An optional setting	Enter 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.

WAN Type= PPTP

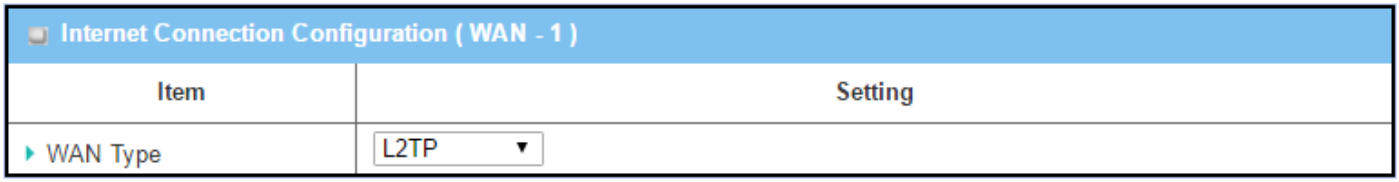


When you select it, "PPTP WAN Type Configuration" will appear. Items and setting is explained below

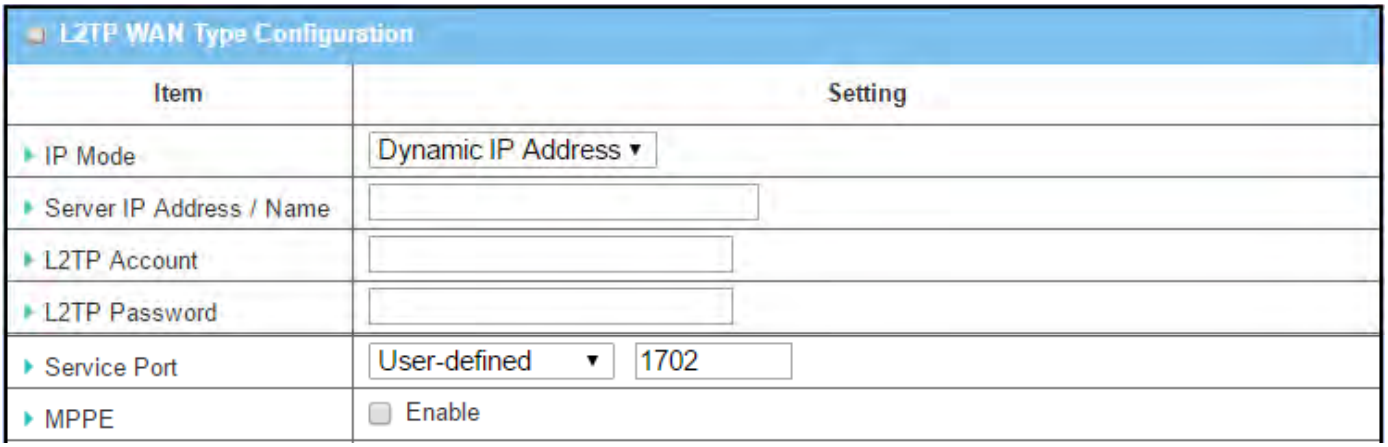


PPTP WAN Type Configuration		
Item	**Value setting**	**Description**
IP Mode	A Must filled setting	Select either Static or Dynamic IP address for PPTP Internet connection. ● When **Static IP Address** is selected, you will need to enter the **WAN IP Address**, **WAN Subnet Mask,** and **WAN Gateway**. ■ **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

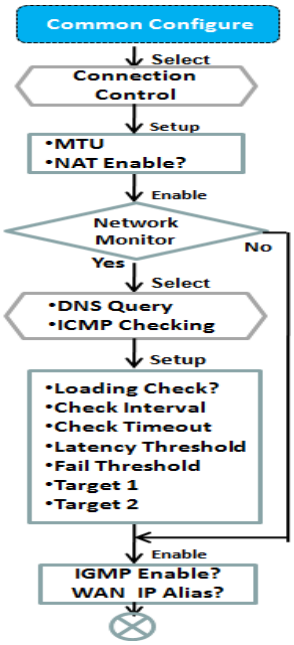


When you select it, "L2TP WAN Type Configuration" will appear. Items and setting is explained below



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



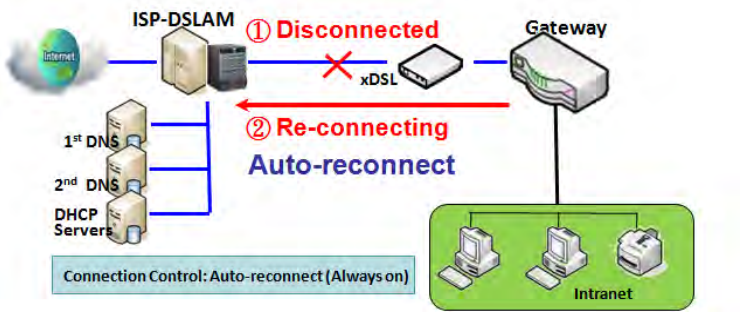
Connection Control	Auto-reconnect
MTU Setup	Enable
NAT	Enable
IGMP	Disable
WAN IP Alias	Enable 10.0.0.1

Network Monitoring Configuration

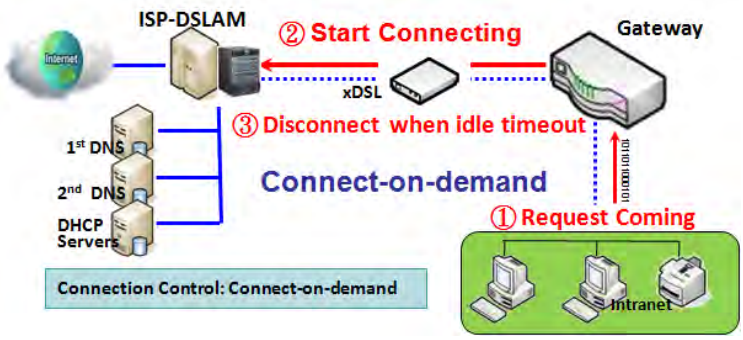
Item	Setting
Network Monitoring Configuration	Enable
Checking Method	DNS Query
Loading Check	Enable
Query Interval	5 (seconds)
Latency Threshold	3000 (ms)
Fail Threshold	5 (Times)
Target1	DNS1
Target2	None

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

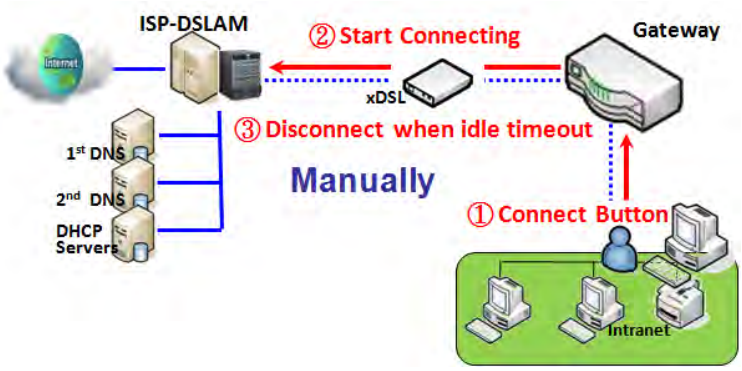
Connection Control.



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.



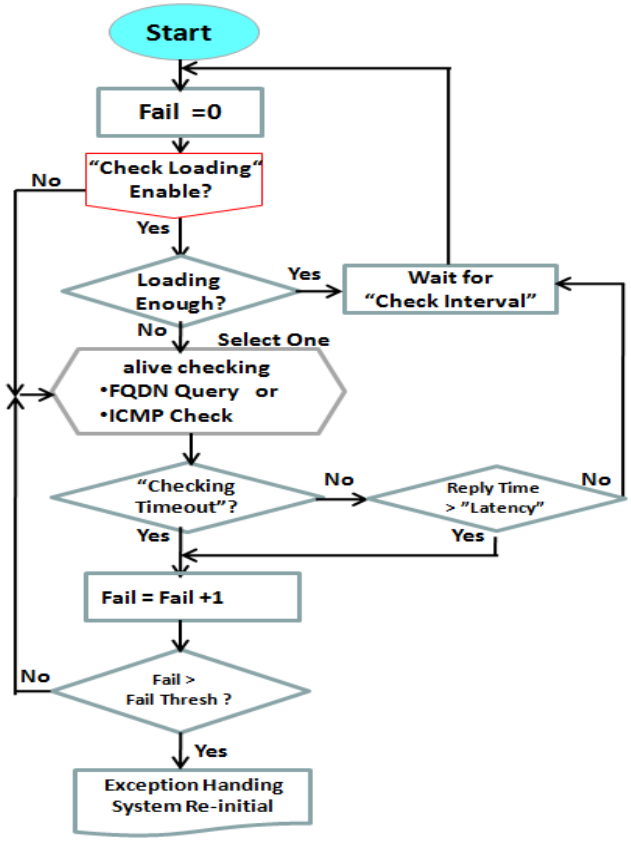
Connect-on-demand: This gateway won't start to establish Internet connection until local data is going to be sent to WAN side. After normal data transferring between LAN and WAN sides, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time.



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 trafiic 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.

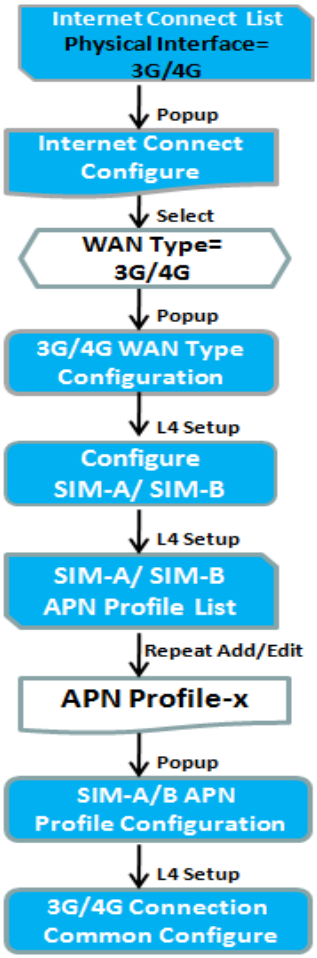
When you do "Network Monitoring", if reply time longer than "Latency" or even no response longer than "Checking Timeout", "Fail" count will be increased. If it is continuous and "Fail" count is more than "Fail Threshold", gateway will do exception handing process and re-initial this connection again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

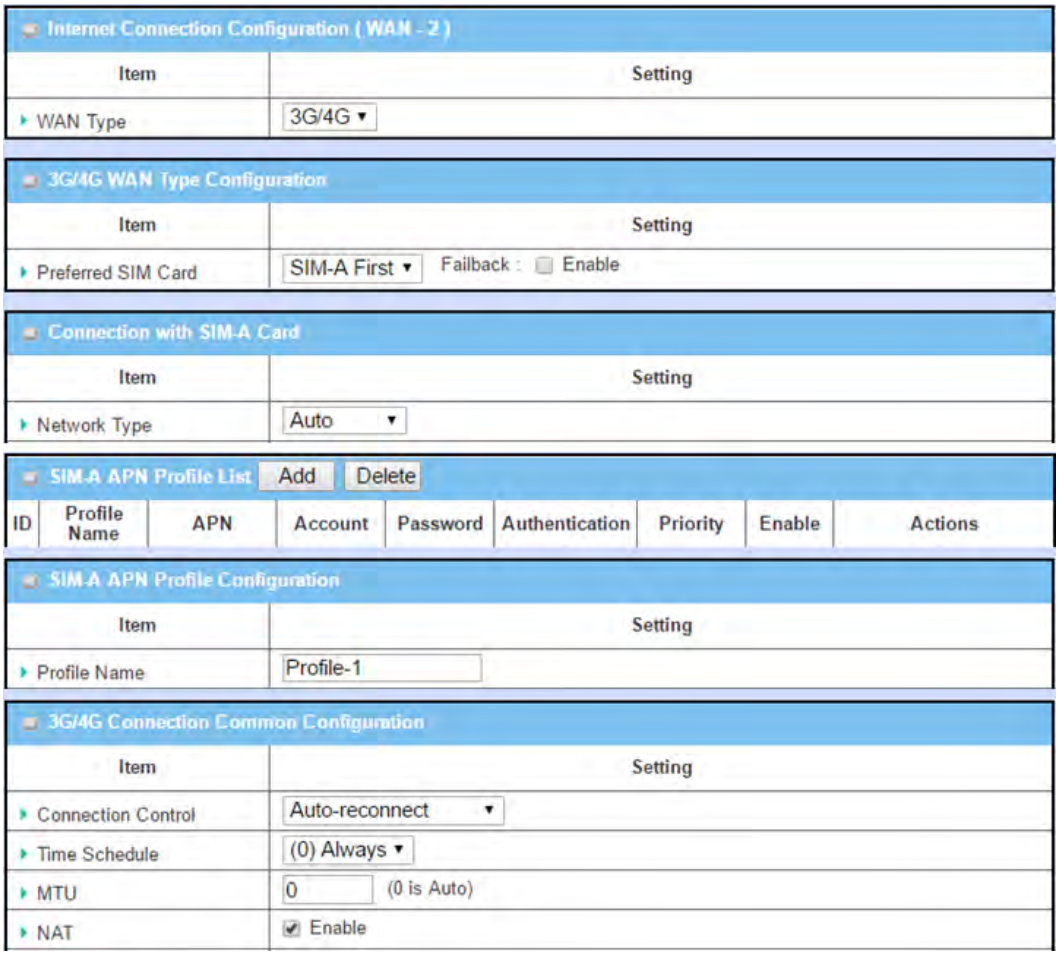
Set up "Ethernet Common Configuration"

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



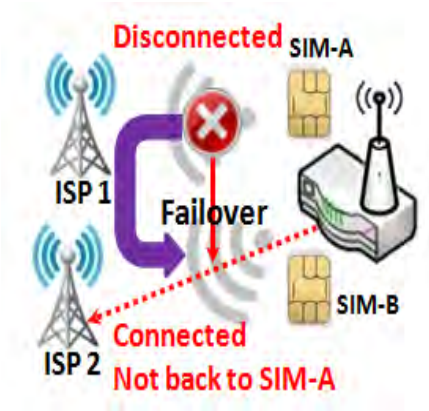


Preferred SIM Card – Dual SIM Fail Over

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”.

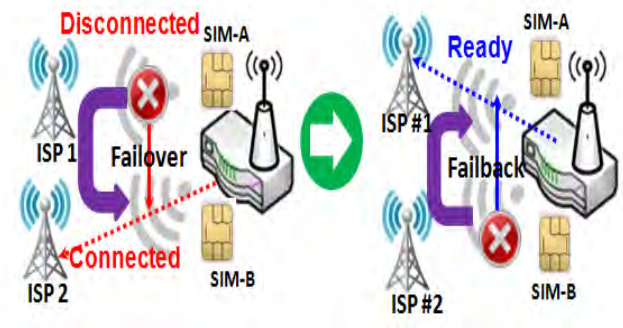
SIM-A/SIM-B only: When “SIM-A Only” or “SIM-B Only” is used, the specified SIM slot card is the only one to be used for negotiation parameters between gateway device and cellular ISP.

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 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 phycially. 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	
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.

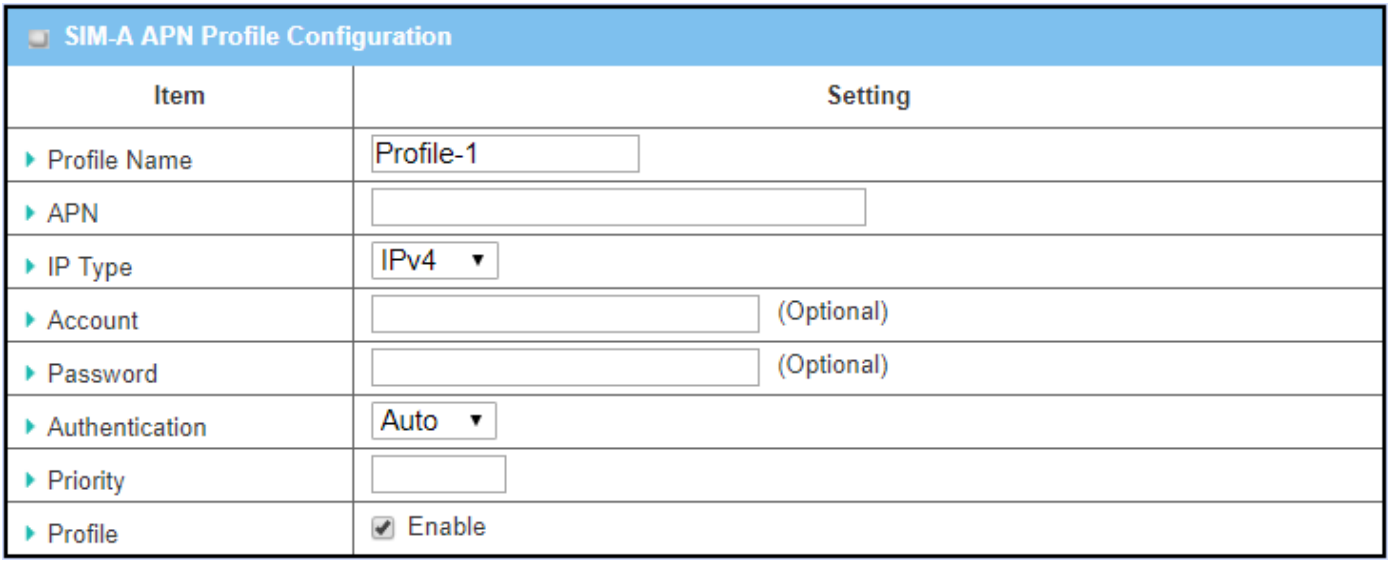
		Select **Auto-detection** to automatically bring out all configurations needed while dialing-up, by comparing the IMSI of the SIM card to the record listed in the manufacturer's database. **Note_1:** You are highly recommended to select the **Manual** or **APN Profile List** to specify the network for 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 serveice provided by your 3G/4G network. It can be **IPv4**, **IPv6**, or **IPv4/6**.
PIN code	1. An Optional setting 2. String format : interger	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**.

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.

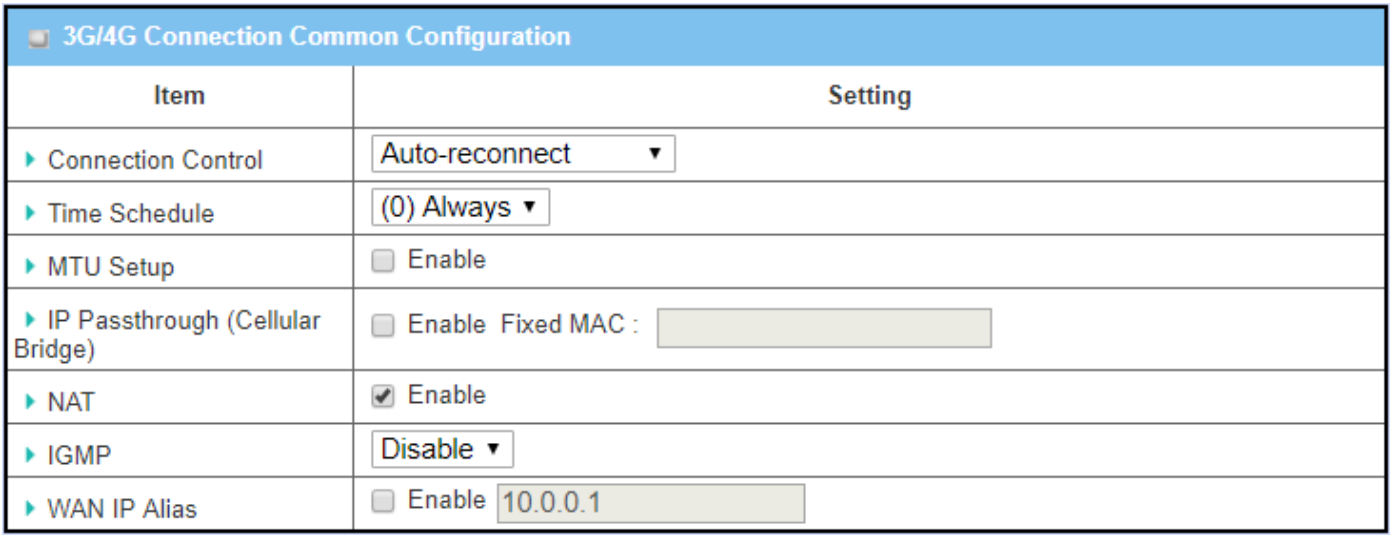


SIM-A/-B APN Profile Configuration		
Item	**Value setting**	**Description**
Profile Name	1. By default **Profile-x** is listed 2. String format : any text	Enter the profile name you want to describe for this profile.
APN	String format : any text	Enter the **APN** you want to use to establish the connection.
IP Type	1. A Must filled setting 2. By default **IPv4** is selected	Specify the IP type of the network serveice 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.

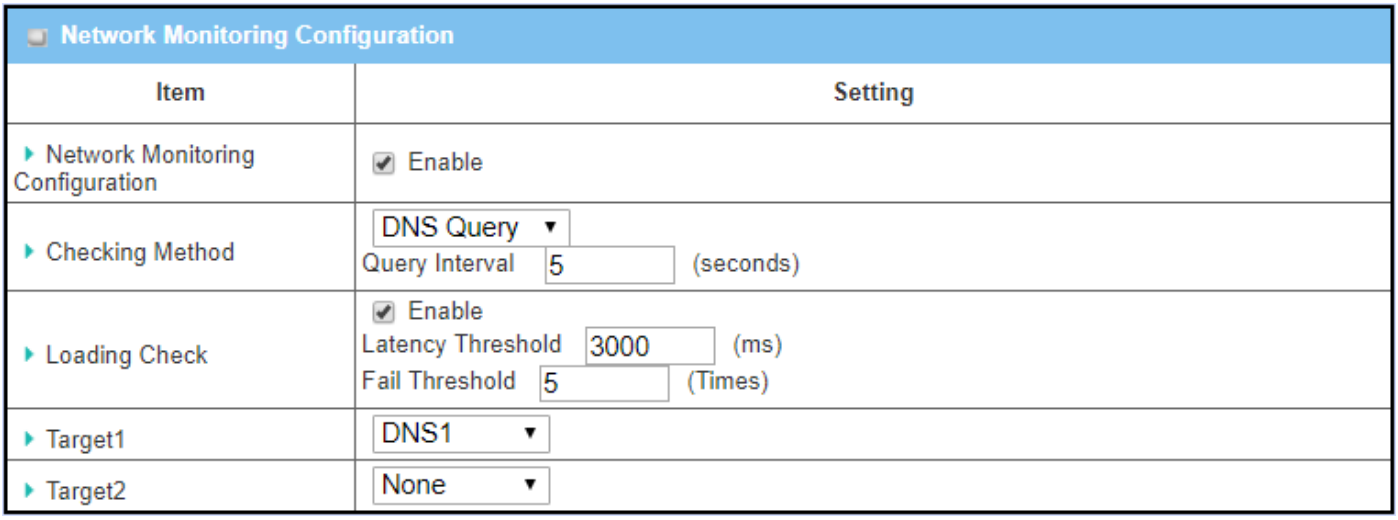
Setup 3G/4G Connection Common Configuration

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



3G/4G Connection Common Configuration		
Item	**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.



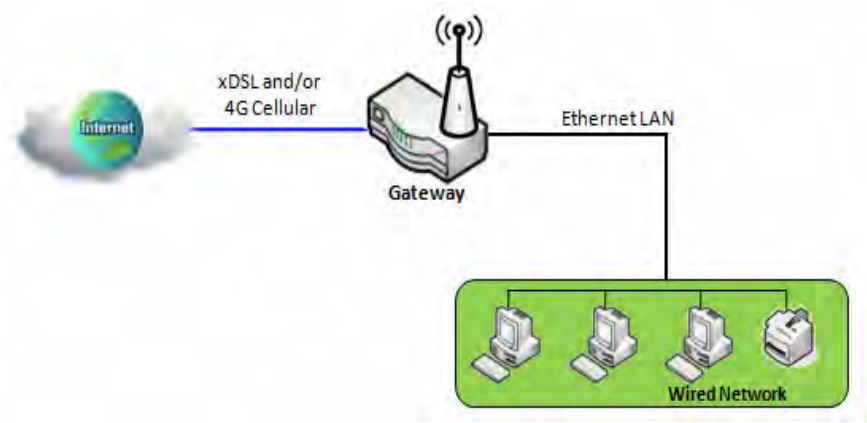
Network Monitoring Configuration Item	Value setting	Description
Network Monitoring Configuration	1. An optional setting 2. Box is checked by default	Check the **Enable** box to activate the network monitoring function.
Checking Method	1. An Optional setting 2. **DNS Query** is set by default	Choose either **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. **Query Interval** defines the transmitting interval between two DNS Query or ICMP checking packets.
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. **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.
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.

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 interconnects 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)

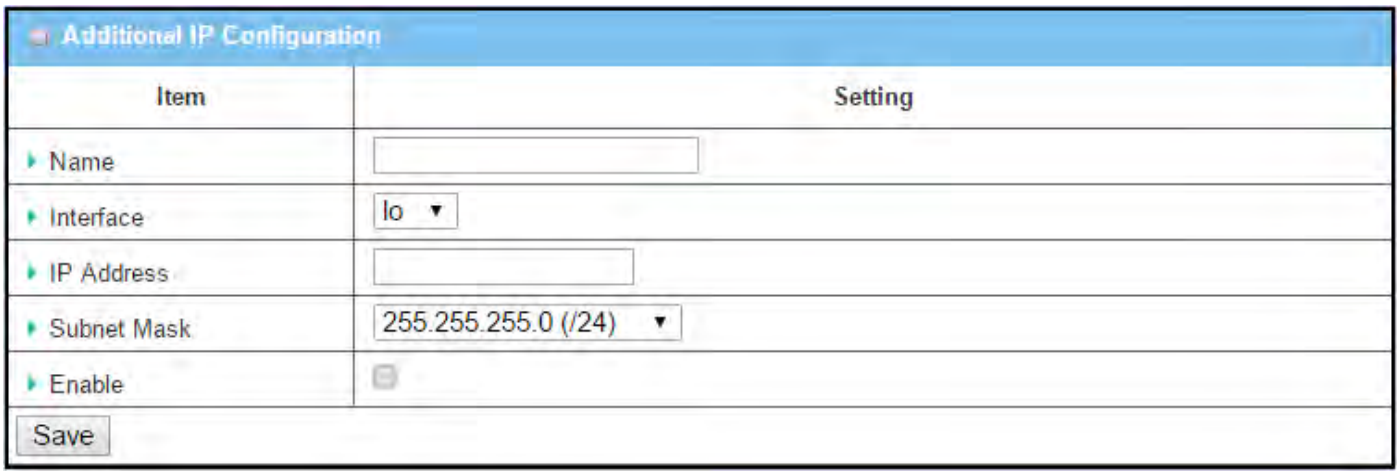
Configuration Item	Value setting	Description
IP Mode	N/A	It shows the LAN IP mode for the gateway according the related configuration. **Static IP**: If there is at least one WAN interface activated, the LAN IP mode is fixed in Static IP mode. **Dynamic IP**: If all the available WAN inferfaces are disabled, the LAN IP mode can be Dynamic IP mode.
LAN IP Address	1. A Must filled setting **2.** 192.168.123.254 **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	Select the subnet mask for this gateway from the dropdown list. Subnet mask defines how many clients are allowed in one network or subnet.

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

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



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.** 192.168.123.254 **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

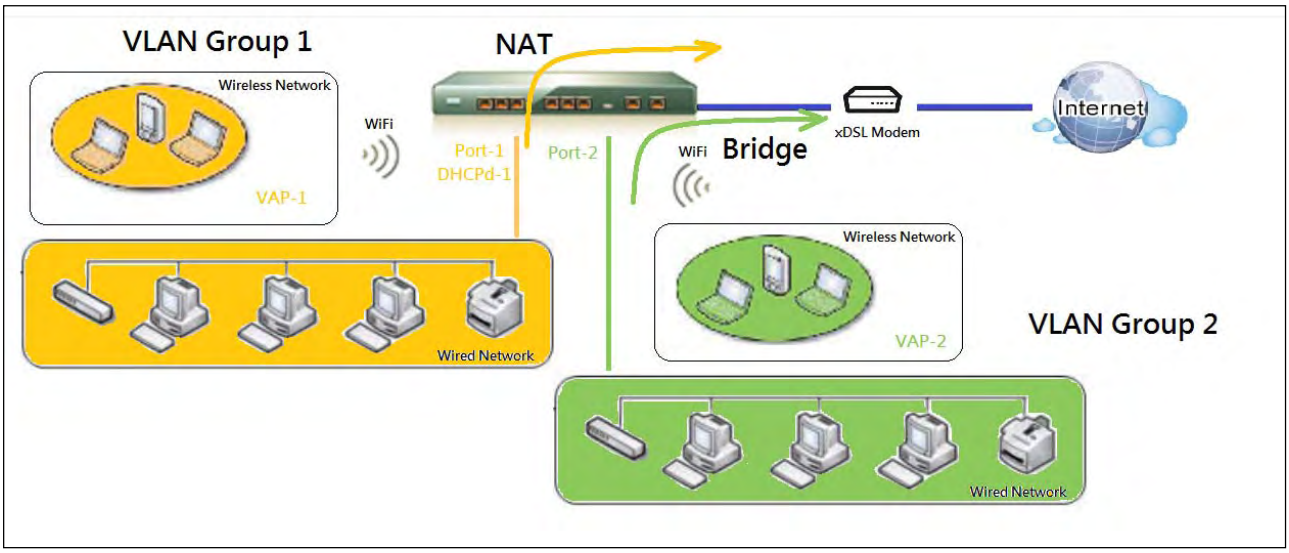
2.2.2 VLAN

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.

If the gateway has only one physical Ethernet LAN port, only very limited configuration is available if you enable the Port-based VLAN.

➢ Port-based VLAN

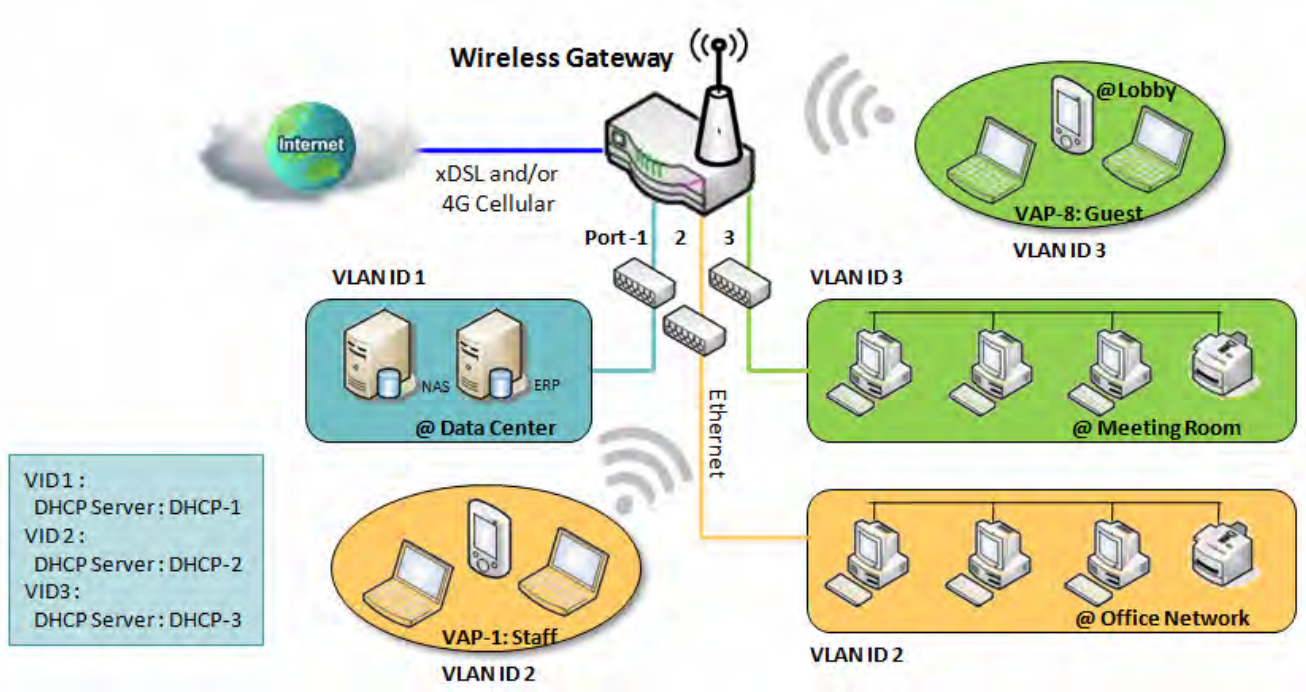
Port-based VLAN function can group Ethernet ports, Port-1 ~ Port-4, and WiFi Virtual Access Points, VAP-1 ~ VAP-8, together for differentiated services like Internet surfing, multimedia enjoyment, VoIP talking, and so on. Two operation modes, NAT and Bridge, can be applied to each VLAN group. One DHCP 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.



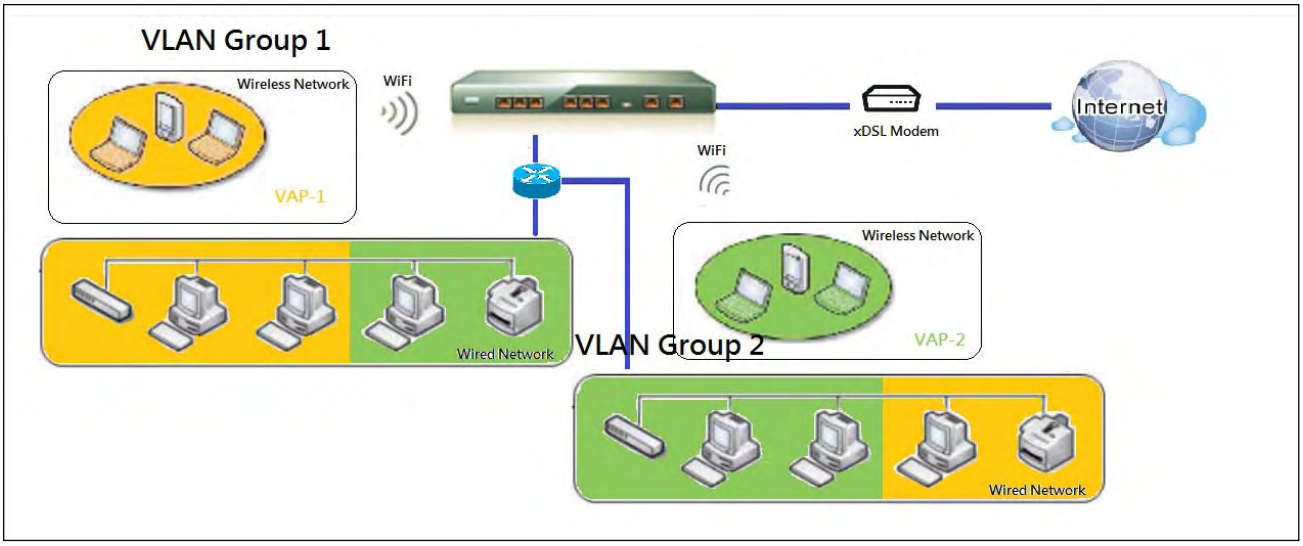
Above is the general case for 3 Ethernet LAN ports in the gateway. But if the device just has one Ethernet LAN port, there will be only one VLAN group for the device. Under such situation, it still supports both the NAT and Bridge mode for the Port-based VLAN configuration.

➢ Tag-based VLAN

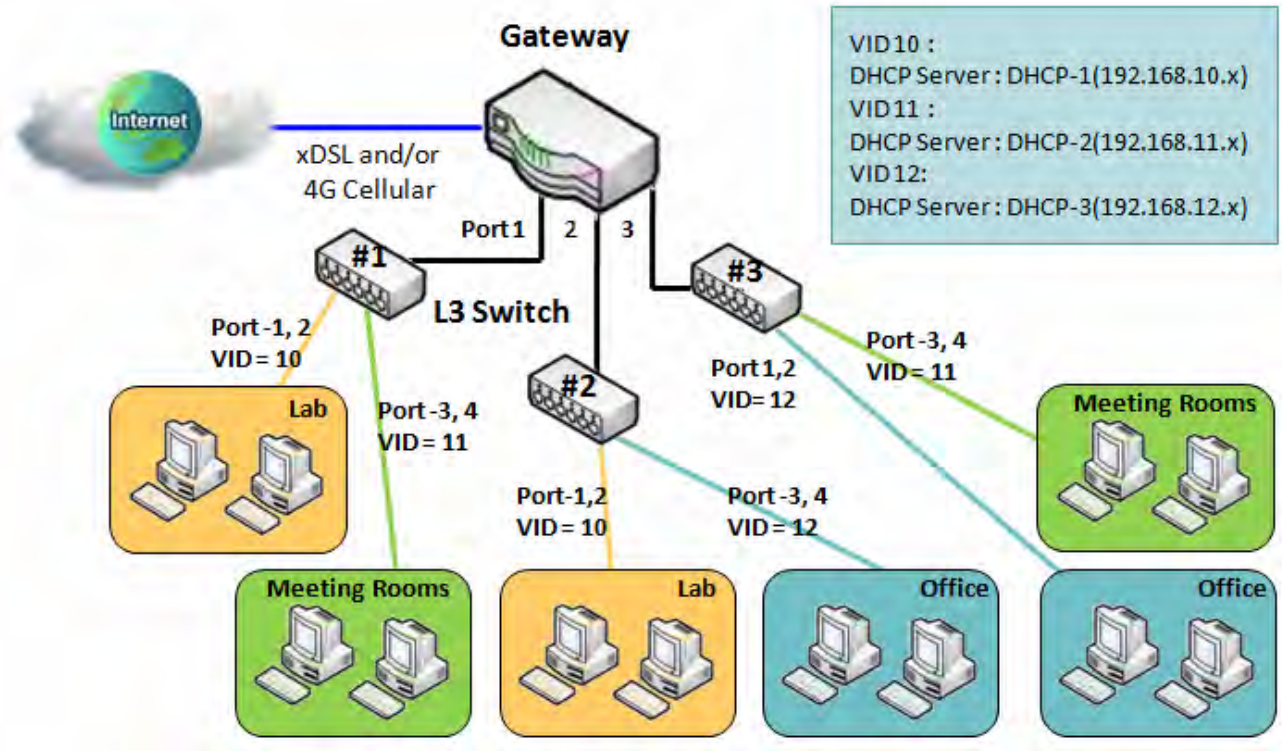
Tag-based VLAN function can group Ethernet ports, Port-1 ~ Port-4, and WiFi Virtual Access Points, VAP-1 ~ VAP-8, together with different VLAN tags for deploying subnets in Intranet. All packet flows can carry with different VLAN tags even at the same physical Ethernet port for Intranet. These flows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

M2M Cellular Gateway



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.

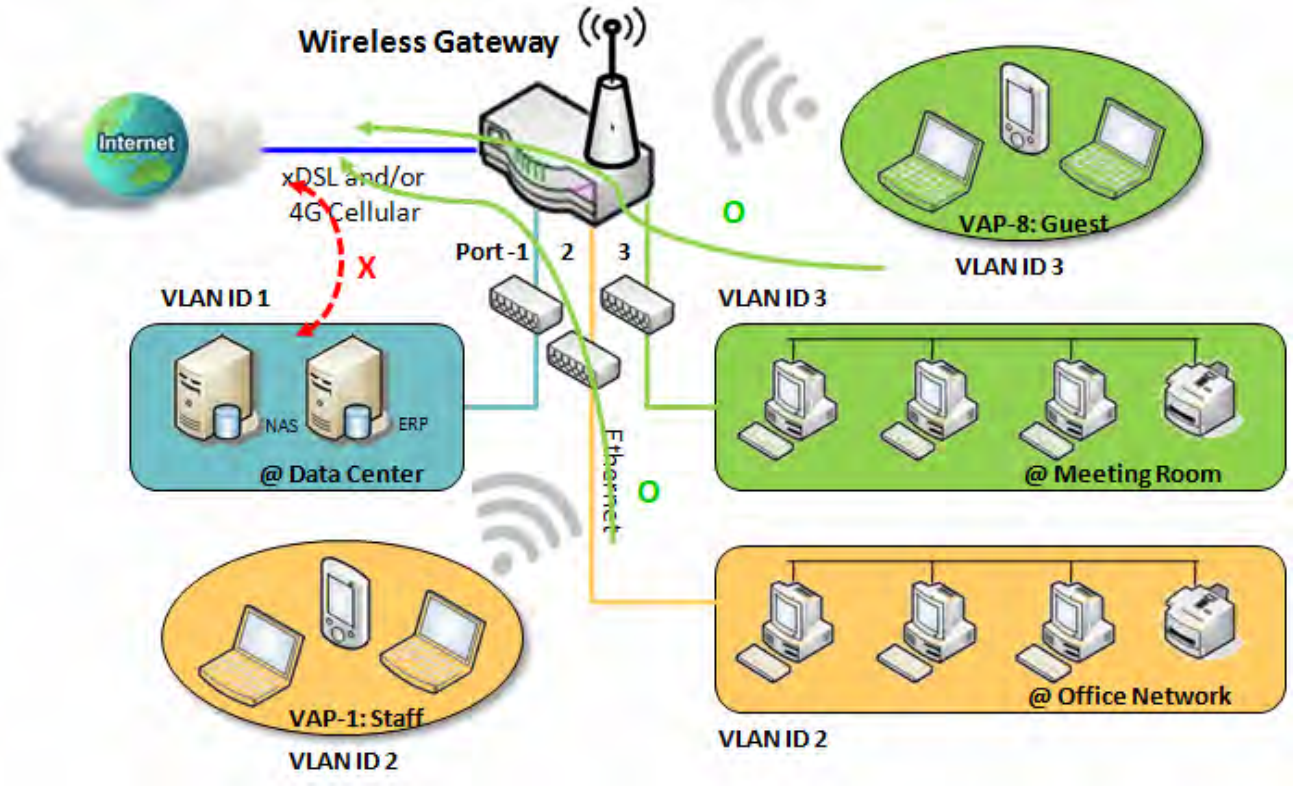


➢ VLAN Groups Access Control

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

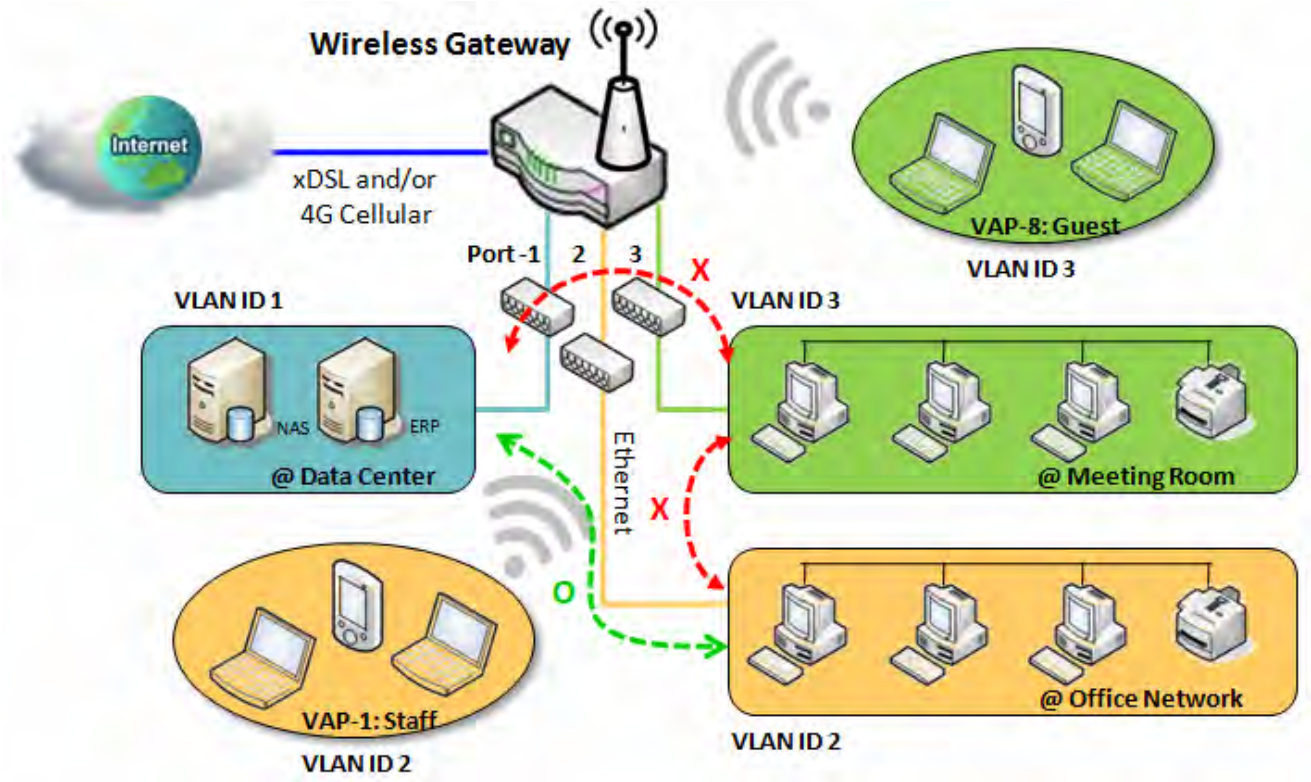
Administrator can specify members of one VLAN group to be able to access Internet or not. Following is an example that VLAN groups of VID is 2 and 3 can access Internet but the one with VID is 1 cannot access Internet. That is, visitors in meeting room and staffs in office network can access Internet. 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.



M2M Cellular Gateway

Inter VLAN Group Routing:

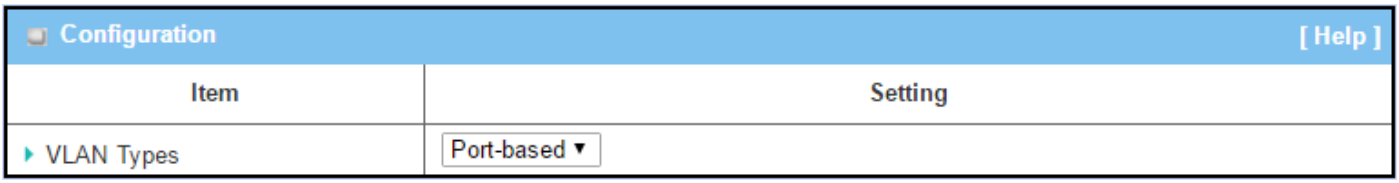
In Port-based tagging, administrator can specify member hosts of one VLAN group to be able to communicate with the ones of another VLAN group or not. This is a communication pair, and one VLAN group can join many communication pairs. But communication pair doesn't have the transitive property. That is,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

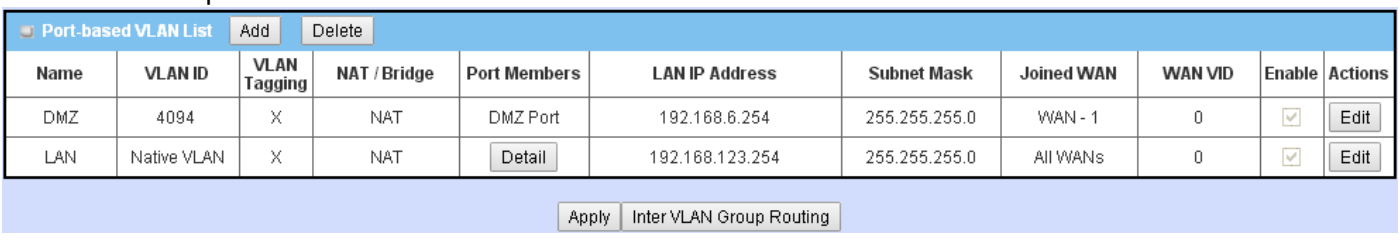
The VLAN function allows you to divide local network into different virtual LANs. There are Port-based and Tag-based VLAN types. Select one that applies.



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

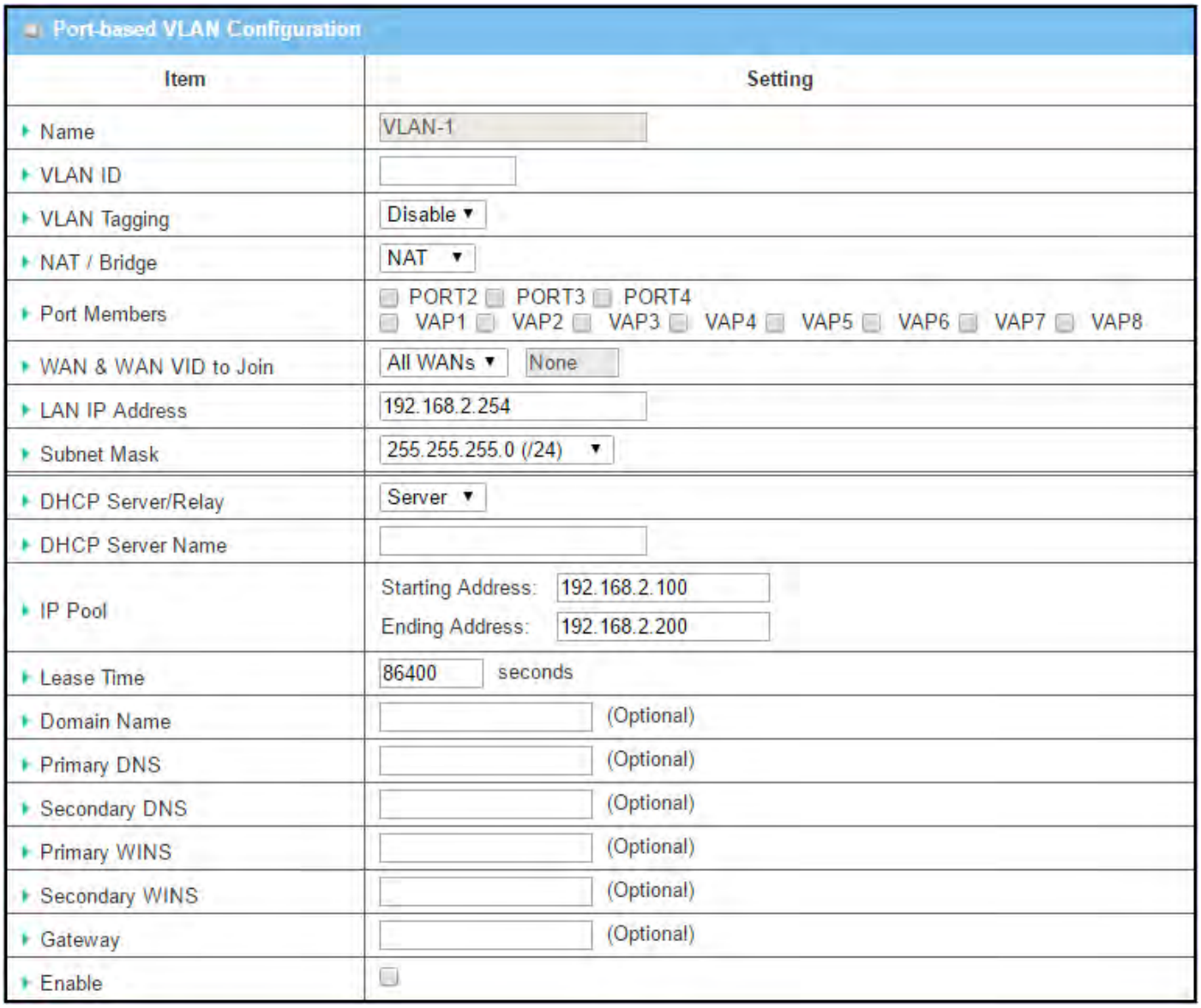
Port-based VLAN – Create/Edit VLAN Rules

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



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)

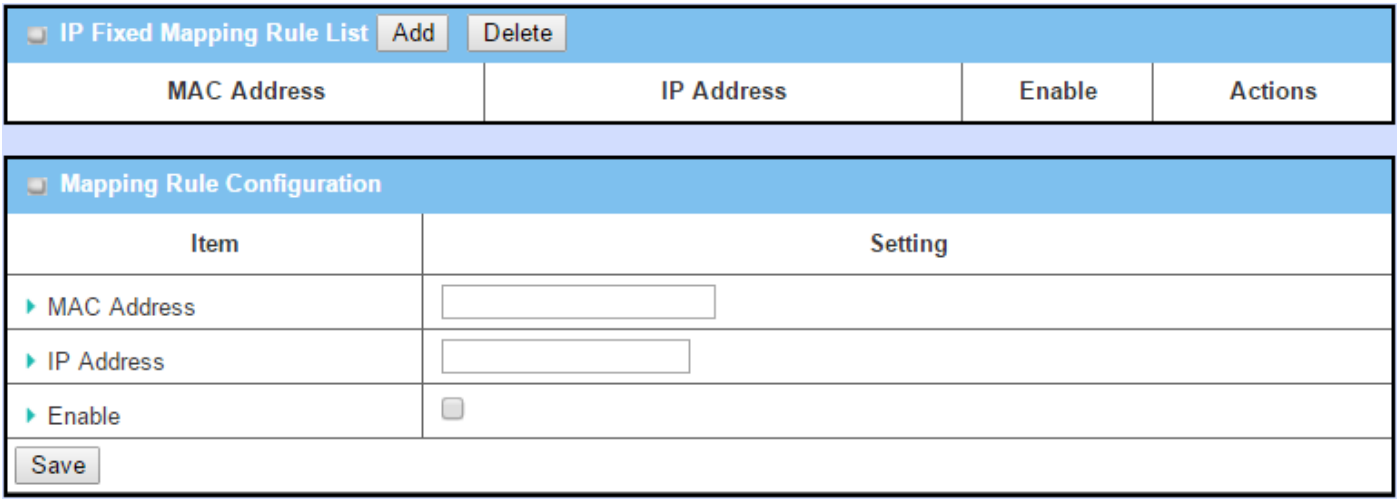
Port-based VLAN - Configuration



Port-based VLAN Configuration		
Item	**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.

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.

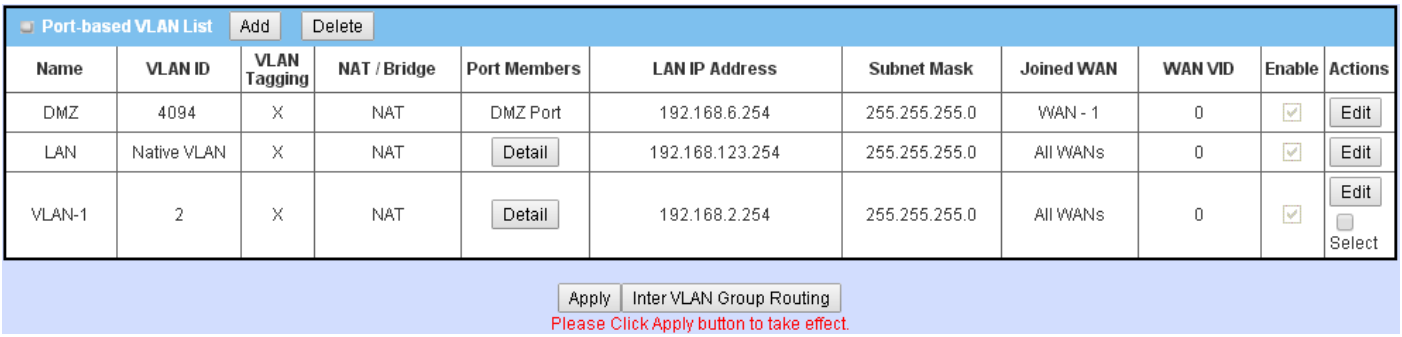
Besides, you can add some IP rules in the **IP Fixed Mapping Rule List** if DHCP Server for the VLAN groups is required.



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

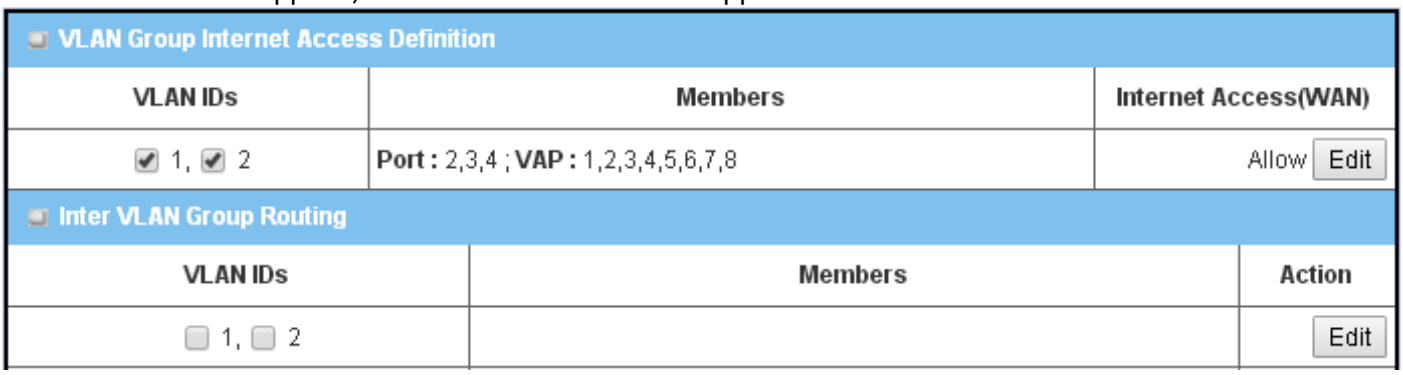
Note: ensure to always click on **Apply** button to apply the changes after the web browser refreshed taken you back to the VLAN page.



Port-based VLAN – Inter VLAN Group Routing

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

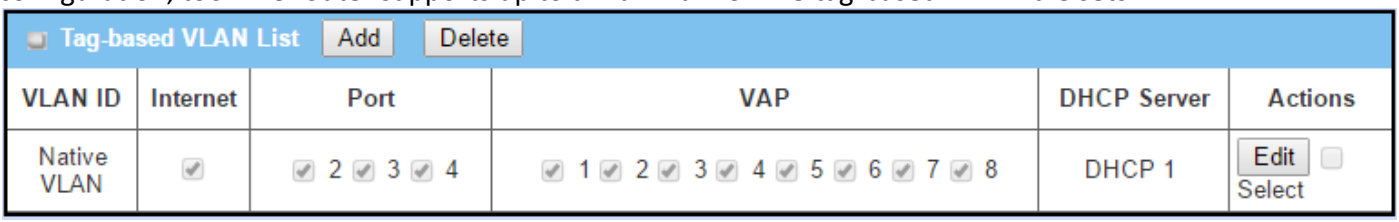
When **Edit** button is applied, a screen similar to this will appear.



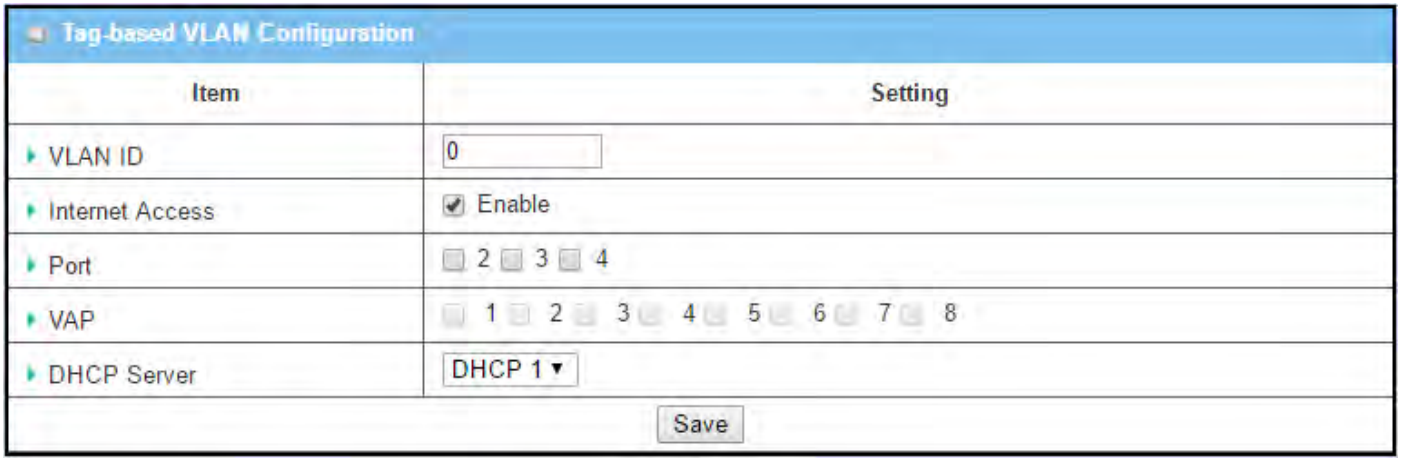
Inter VLAN Group Routing		
Item	**Value setting**	**Description**
VALN Group Internet Access Definition	All boxes are checked by default.	By default, all boxes are checked means all **VLAN ID** members are allow to access WAN interface. If uncheck a certain **VLAN ID** box, it means the VLAN ID member 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.



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

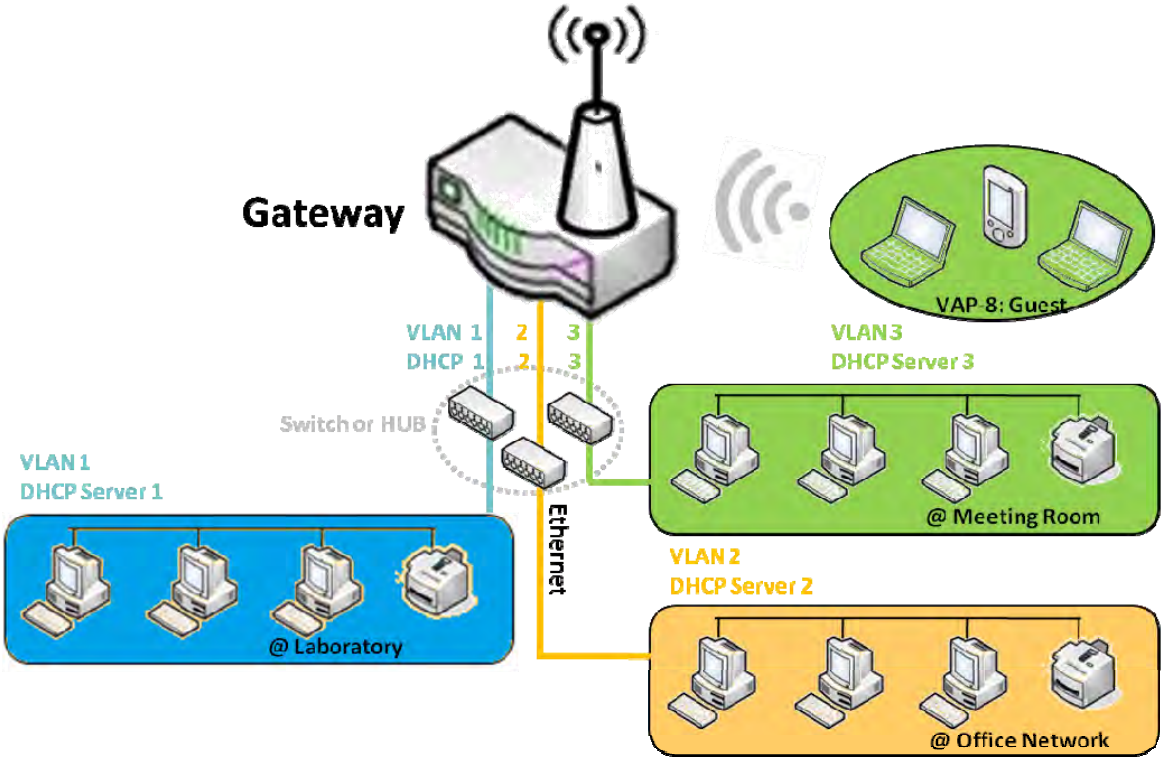


Tag-based VLAN Configuration		
Item	**Value setting**	**Description**
VALN ID	A Must filled setting	Define the **VLAN ID** number, range is 6~4094.
Internet Access	The box is checked by default.	Click **Enable** box to allow the members in the VLAN group access to internet.
Port	The box is unchecked 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

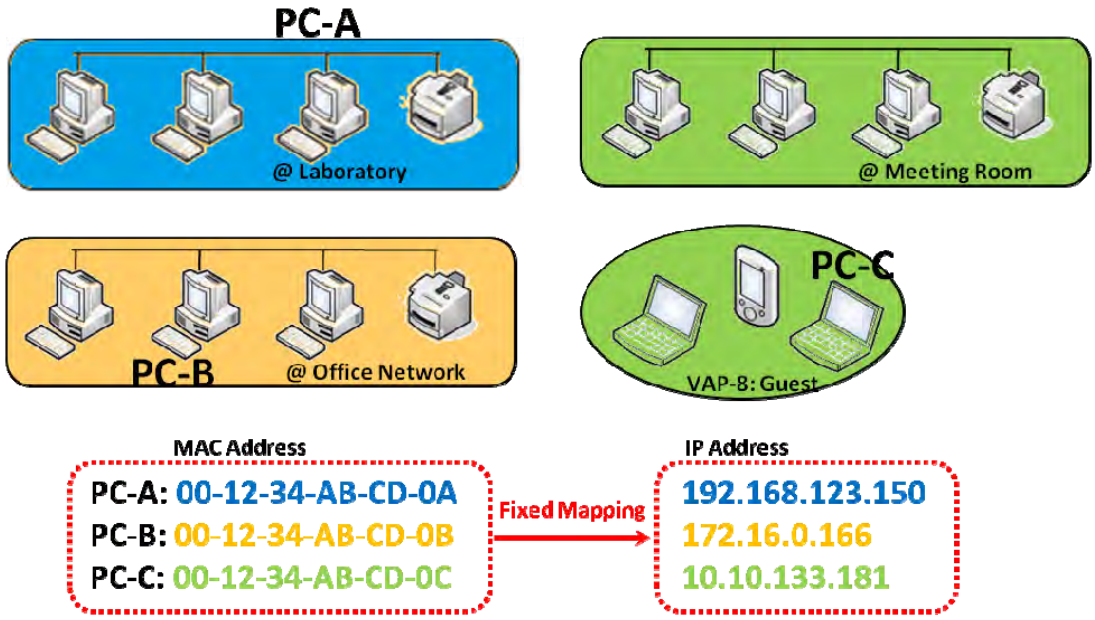
The gateway supports up to 4 DHCP servers to fulfill the DHCP requests from different VLAN groups (please refer to VLAN section for getting more usage details). And there is one default setting for whose LAN IP Address is the same one of gateway LAN interface, with its default Subnet Mask setting as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



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

➢ Fixed Mapping

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



DHCP Server Setting

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 gateway 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 List | Add | Delete | DHCP Client List | [Help]

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	192.168.123.100-192.168.123.200	3600		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.

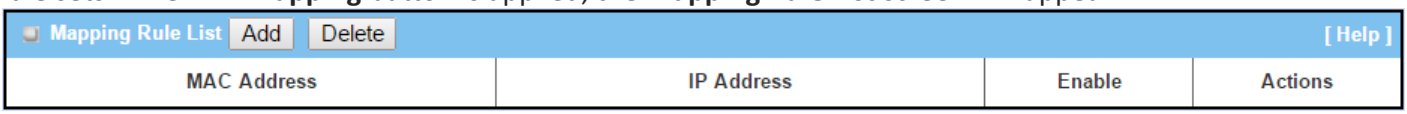
DHCP Server Configuration

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

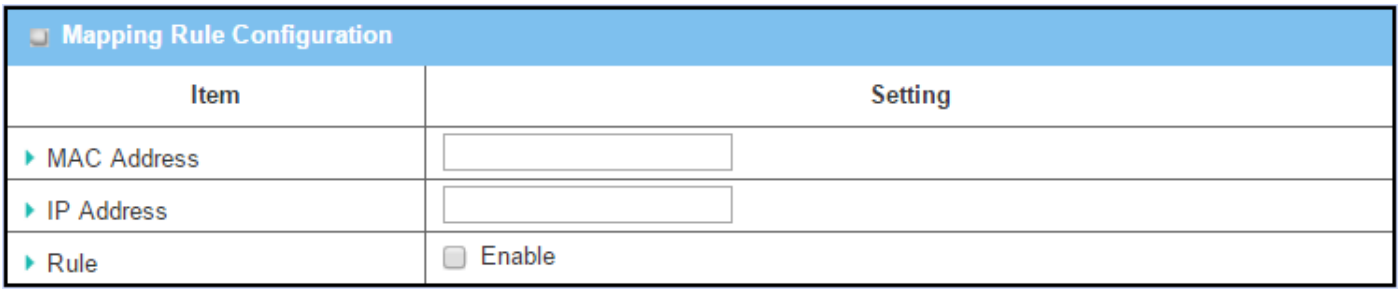
DHCP Server Configuration		
Item	**Value setting**	**Description**
DHCP Server Name	1. String format can be any text 2. A Must filled setting	Enter a DHCP Server name. Enter a name that is easy for you to understand.
LAN IP Address	1. IPv4 format. 2. A Must filled setting	The LAN IP Address of this DHCP 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. Numberic 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 gateway 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.



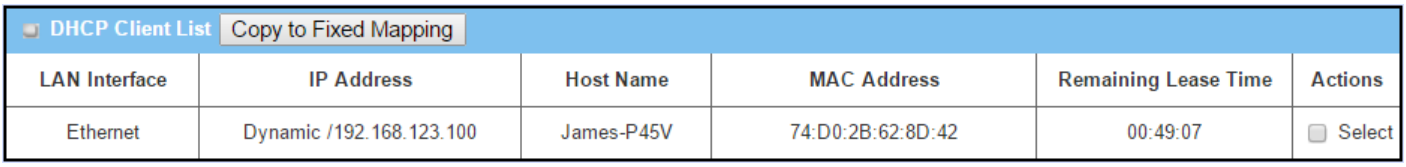
When **Add** button is applied, **Mapping Rule Configuration** screen will appear.



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.

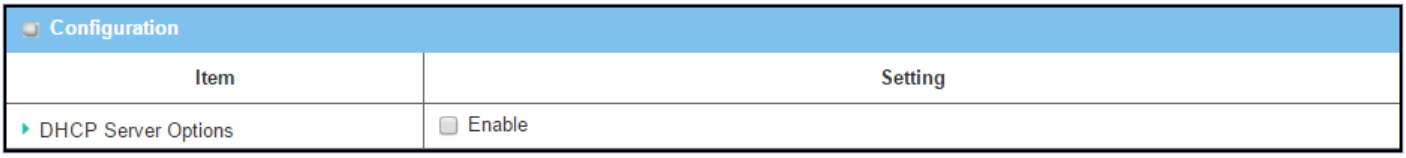


When the DHCP Client is selected and **Copy to Fixed Mapping** button is applied. The IP and MAC address of DHCP Client will apply to the Mapping Rule List on specific DHCP Server automatically.

Enable / Disable DHCP Server Options

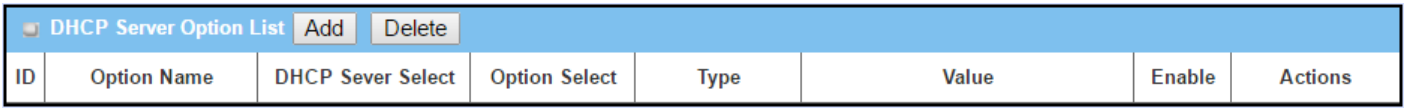
The **DHCP Server Options** setting allows user to set **DHCP OPTIONS 66**, **72**, or **114**. Click the **Enable** button to activate the DHCP option function, and the DHCP Server will add the expected options in its sending out DHCPOFFER DHCPACK packages.

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

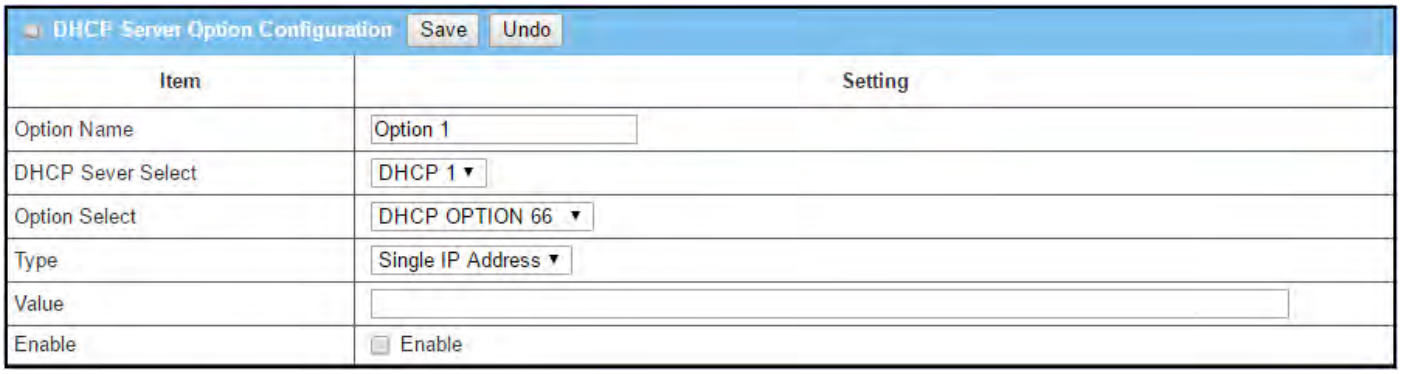


Create / Edit DHCP Server Options

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



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



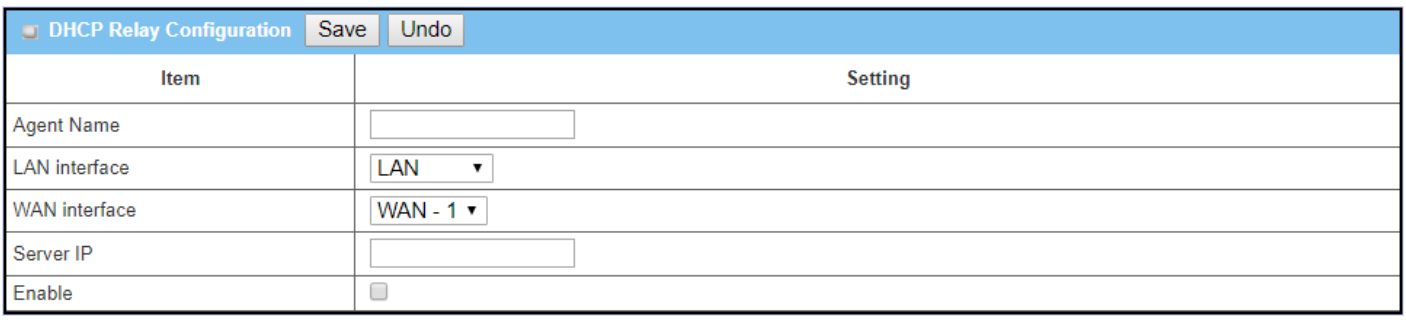
DHCP Server Option Configuration		
Item	**Value setting**	**Description**
Option Name	1. String format can be any text 2. A Must filled setting.	Enter a DHCP Server Option name. Enter a name that is easy for you to understand.
DHCP Server Select	Dropdown list of all available DHCP servers.	Choose the DHCP server this option should apply to.
Option Select	1. A Must filled setting. 2. **Option 66** is selected by default.	Choose the specific option from the dropdown list. It can be **Option 66**, **Option 72**, **Option 144**, **Option 42**, **Option 150**, **or Option 160**. **Option 42** for ntp server; **Option 66** for tftp; **Option 72** for www;

		Option 144 for url;		
Type	Dropdown list of DHCP server option value's type	Each different options has different value types.		
		66	Single IP Address	
			Single FQDN	
		72	IP Addresses List, separated by ","	
		114	Single URL	
		42	IP Addresses List, separated by ","	
		150	IP Addresses List, separated by ","	
		160	Single IP Address	
			Single FQDN	
Value	1. IPv4 format 2. FQDN format 3. IP list 4. URL format 5. A Must filled setting	Should conform to Type :		
			Type	Value
		66	Single IP Address	IPv4 format
			Single FQDN	FQDN format
		72	IP Addresses List, separated by ","	IPv4 format, separated by ","
		114	Single URL	URL format
Enable	The box is unchecked by default.	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.		

Create / Edit DHCP Relay

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

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



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.

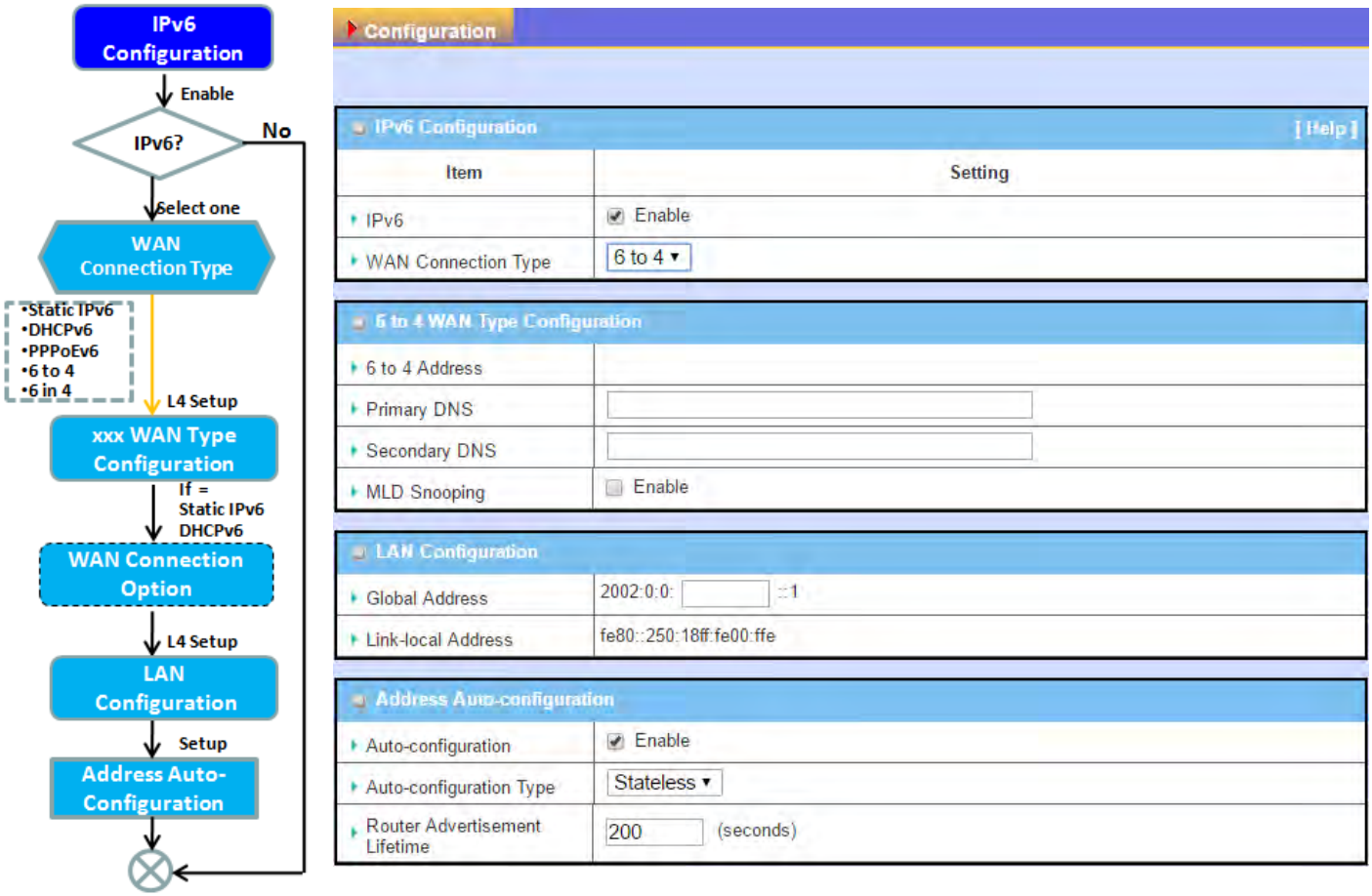
2.3 WiFi (not supported)

Not supported feature for the purchased product, leave it as blank.

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



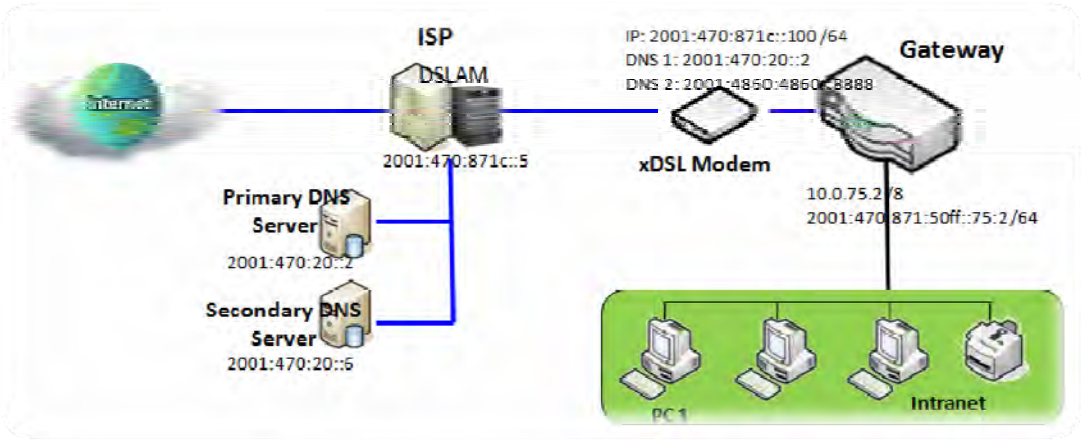
The **IPv6 Configuration** setting allows user to set the IPv6 connection type to access the IPv6 network. This gateway supports various types of IPv6 connection, including **Static IPv6**, **DHCPv6**, and **PPPoEv6**

Note: 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

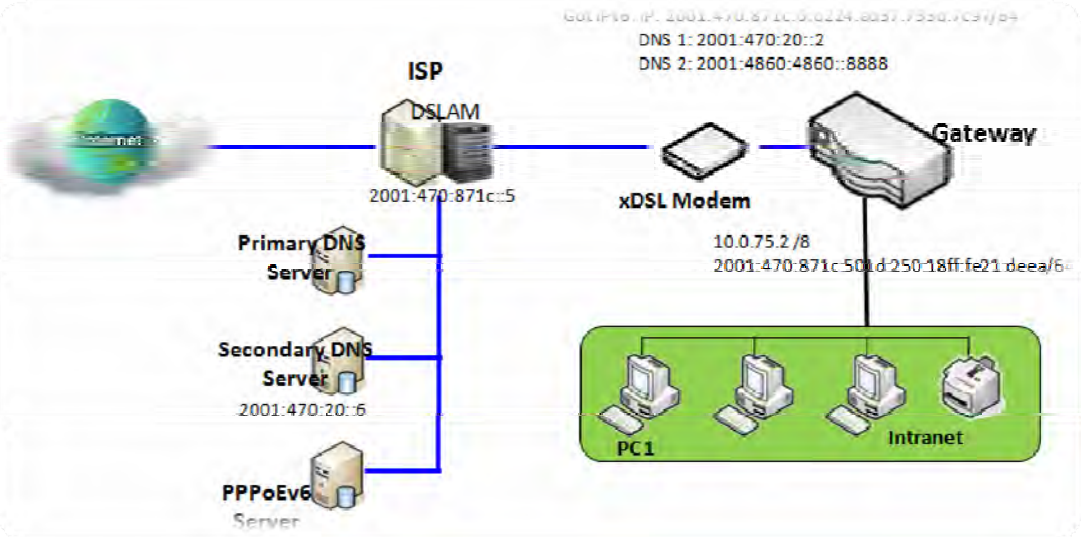
Static IPv6 does the same function as static IPv4. The static IPv6 provides manual setting of IPv6 address, IPv6 default gateway address, and IPv6 DNS.



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

DHCPv6

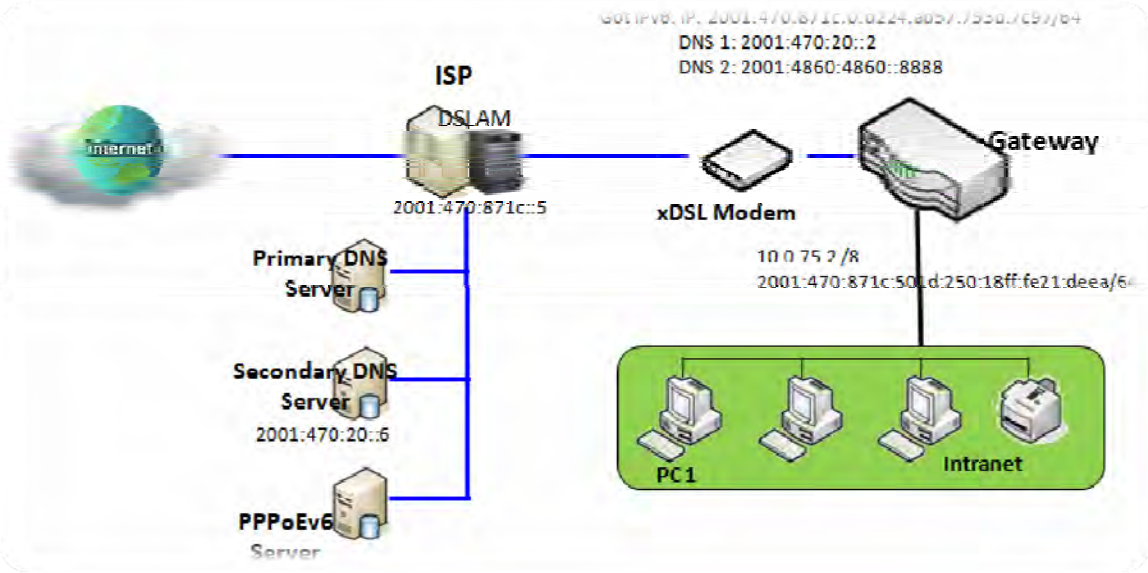
DHCP in IPv6 does the same function as DHCP in IPv4. The DHCP server sends IP address, DNS server addresses and other possible data to the DHCP client to configure automatically. The server also sends a lease time of the address and time to re-contact the server for IPv6 address renewal. The client has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



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

PPPoEv6

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

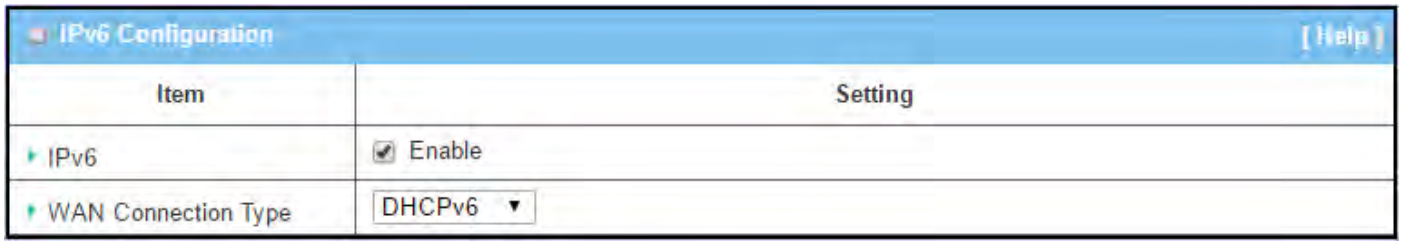


The diagram above depicts the IPv6 addressing through PPPoE, PPPoEv6 server (DSLAM) on the ISP side provides IPv6 configuration upon receiving PPPoEv6 client request. When PPPoEv6 server gets client request and successfully authenticates it, the server sends IP address, DNS server addresses and other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

IPv6 Configuration Setting

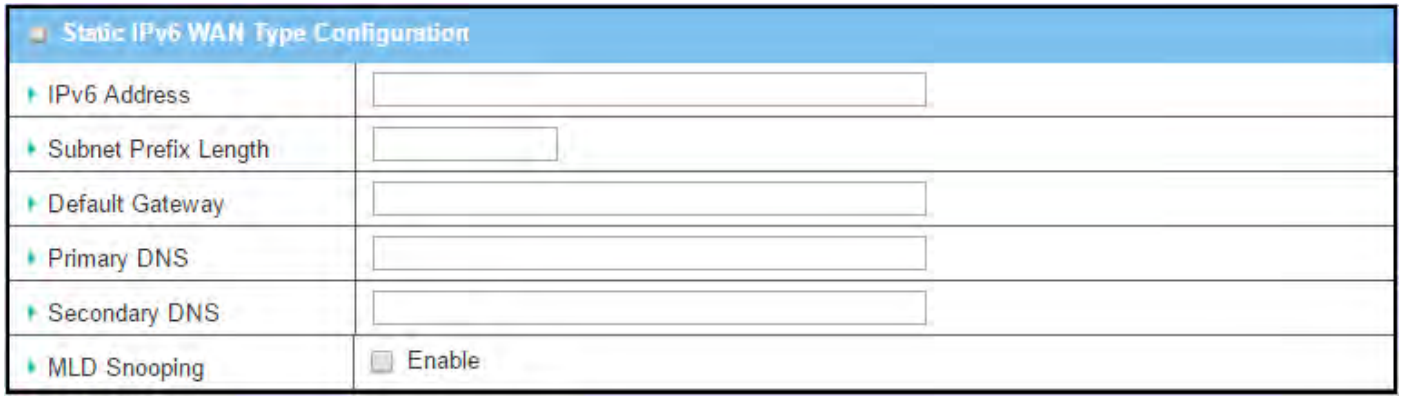
Go to **Basic Network > IPv6 > Configuration** Tab.

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



IPv6 Configuration		
Item	**Value setting**	**Description**
IPv6	The box is unchecked by default,	Check the **Enable** box to activate the IPv6 function.
WAN Connection Type	1. Only can be selected when IPv6 Enable 2. A Must filled setting	Define the selected IPv6 WAN Connection Type to establish the IPv6 connectivity. Select **Static IPv6** when your ISP provides you with a set IPv6 addresses. Then go to **Static IPv6 WAN Type Configuration**. Select **DHCPv6** when your ISP provides you with DHCPv6 services. Select **PPPoEv6** when your ISP provides you with PPPoEv6 account settings. Select **IPv6** when you want to use IPv6 connection. **Note**: For the products just having 3G/4G WAN interface, only **IPv6** is supported.

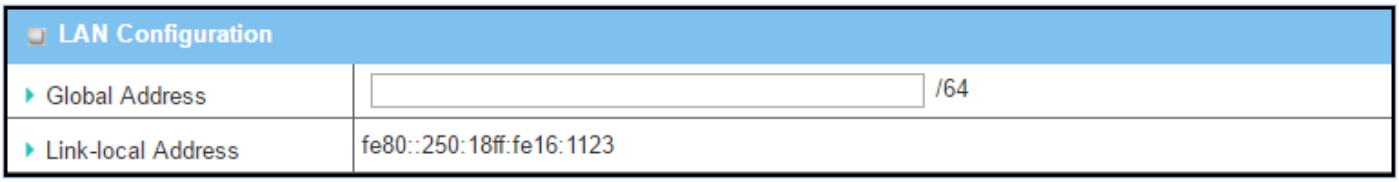
Static IPv6 WAN Type Configuration



Static IPv6 WAN Type Configuration

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

LAN Configuration

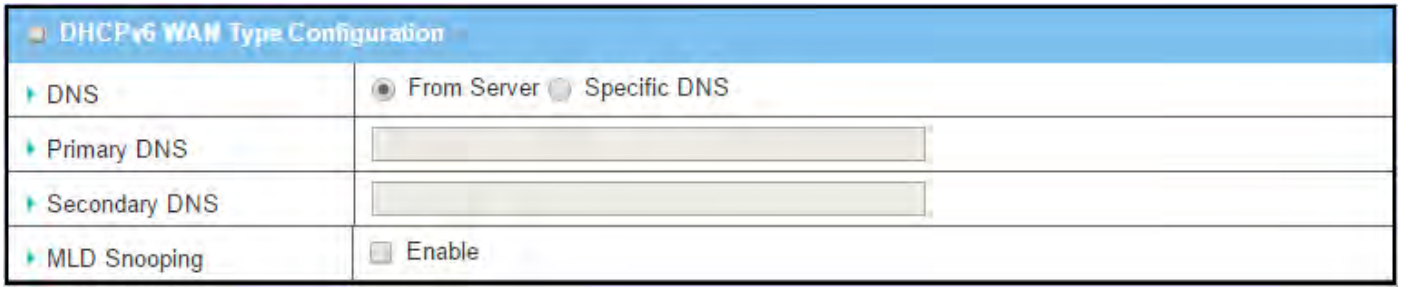


LAN Configuration		
Item	**Value setting**	**Description**
Global Address	A Must filled setting	Enter the LAN **IPv6 Address** for the router.
Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

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

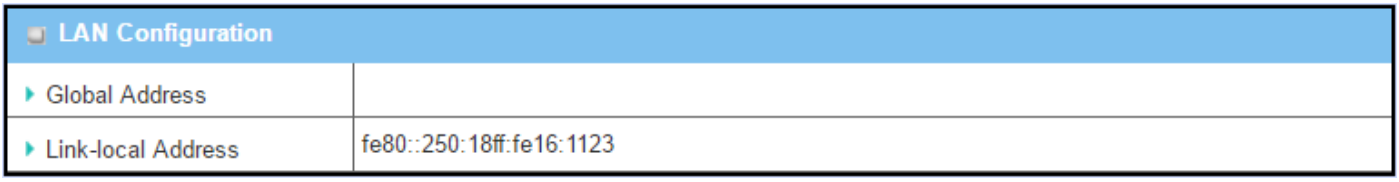
If above setting is configured, click the **Save** button to save the configuration, and click the **Reboot** button to reboot the router.

DHCPv6 WAN Type Configuration



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

LAN Configuration

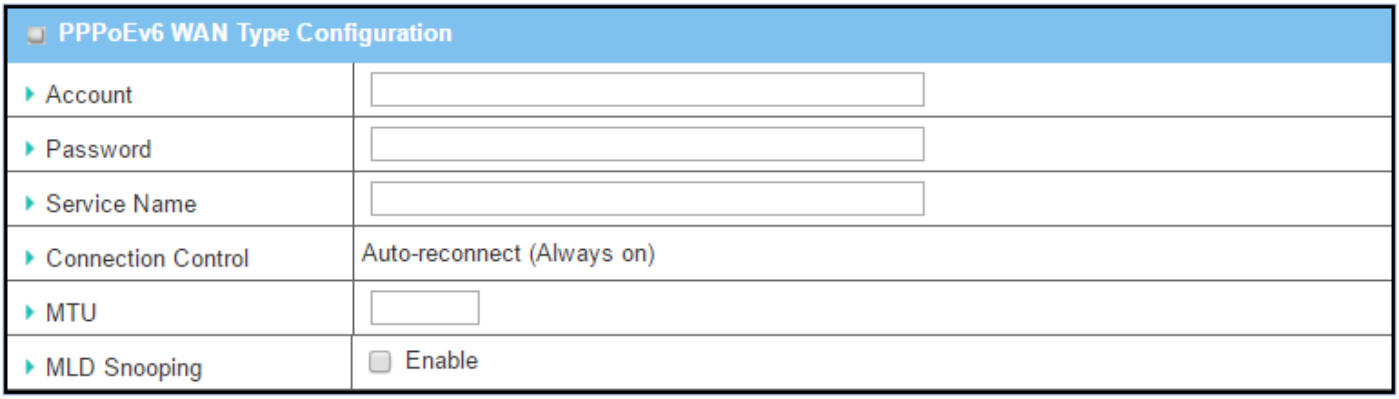


LAN Configuration		
Item	**Value setting**	**Description**
Global Address	Value auto-created	Enter the LAN **IPv6 Address** for the router.
Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

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

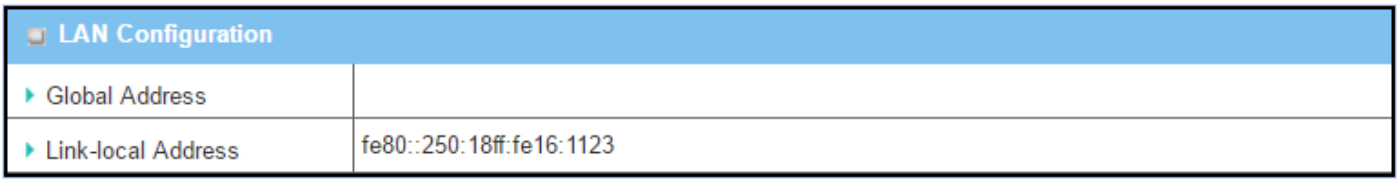
If above setting is configured, click the **Save** button to save the configuration, and click **Reboot** button to reboot the router.

PPPoEv6 WAN Type Configuration



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

LAN Configuration



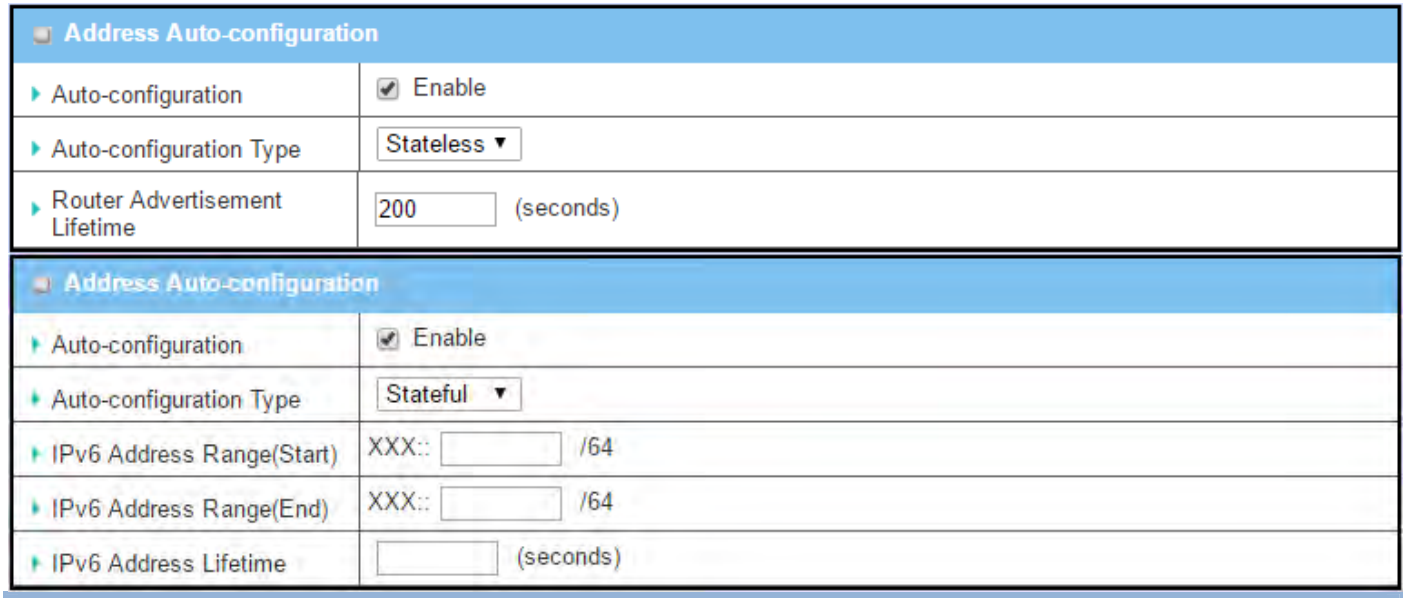
LAN Configuration		
Item	**Value setting**	**Description**
Global Address	Value auto-created	The LAN **IPv6 Address** for the router.
Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

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

the router.

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

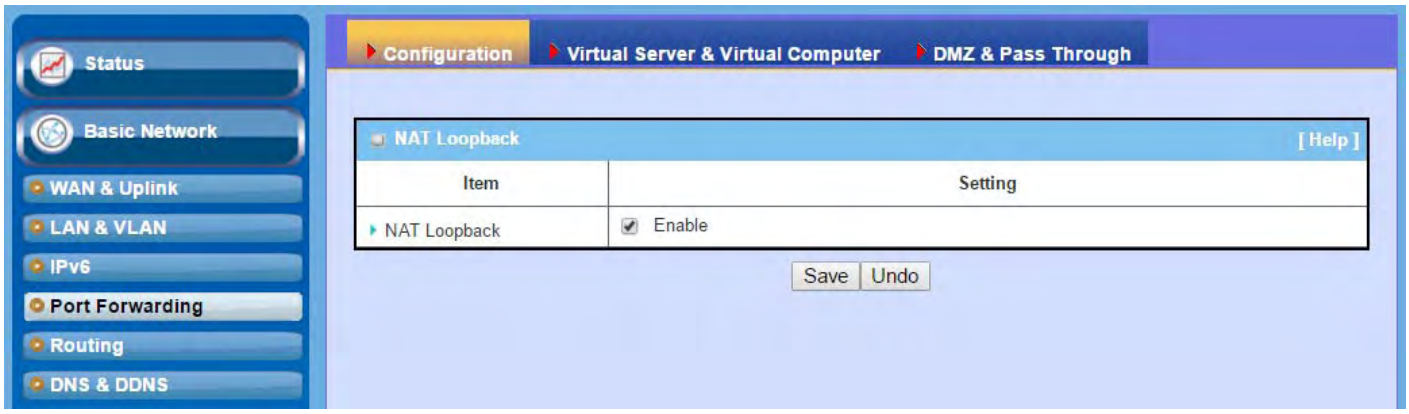


Address Auto-configuration		
Item	**Value setting**	**Description**
Auto-configuration	The box is unchecked by default	Check to enable the Auto configuration feature.
Auto-configuration Type	1. Only can be selected when **Auto-configuration** enabled 2. Stateless is selected by default	Define the selected 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. Select **Stateful** to manage the Local Area Network to be **Stateful (DHCPv6)**. **IPv6 Address Range (Start)** (A Must filled setting): Enter the start IPv6 Address for the DHCPv6 range for your local computers. 0100 is set by default. ***Value Range*:** 0001 ~ FFFF. **IPv6 Address Range (End)** (A Must filled setting): Enter the end IPv6 Address for the DHCPv6 range for your local computers. 0200 is set by default. ***Value Range*:** 0001 ~ FFFF.

	IPv6 Address Lifetime (A Must filled setting): Enter the DHCPv6 lifetime for your local computers. 36000 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.



Usually all local hosts or servers behind corporate gateway 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 gateway (external network), by remapping the destination IP address and port number

There are several optional Port Forwarding related functions in this gateway. 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

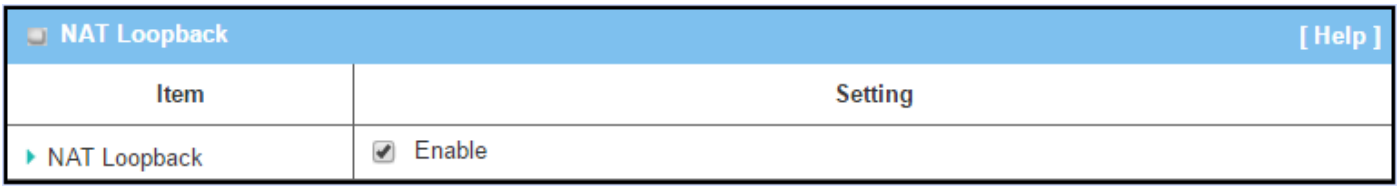
This feature allows you to access the WAN global IP address from your inside NAT local network. It is useful when you run a server inside your network. For example, if you set a mail server at LAN side, your local devices can access this mail server through gateway's global IP address when enable NAT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

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



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 Add Delete

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 Add Delete

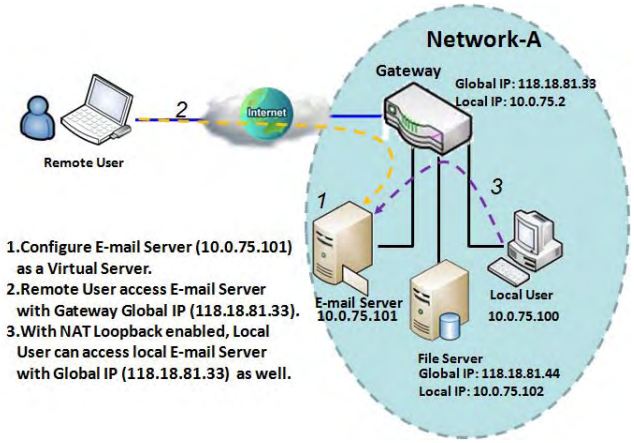
ID	Global IP	Local IP	Enable	Actions
1	118.18.81.44	10.0.75.102		Edit Select

There are some important Pot Forwarding functions implemented within the gateway, 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 gateway. 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 gateway whose IP address is a global one and is visible to the outside world. Since it is behind NAT, it is protected by gateway firewall. To configure Virtual Computer, you just have to map the local IP of the virtual computer to a global IP.

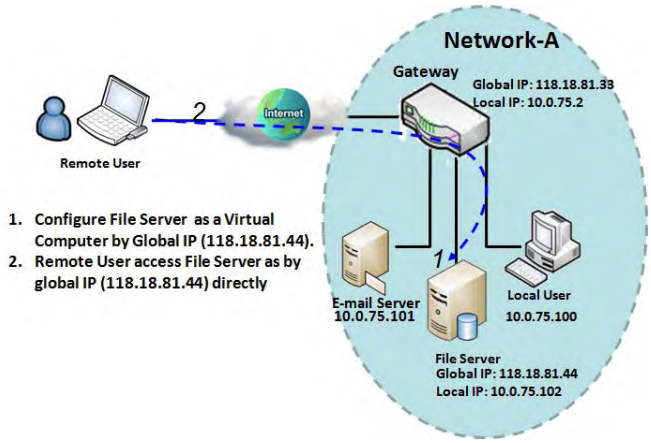
Virtual Server & NAT Loopback



"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

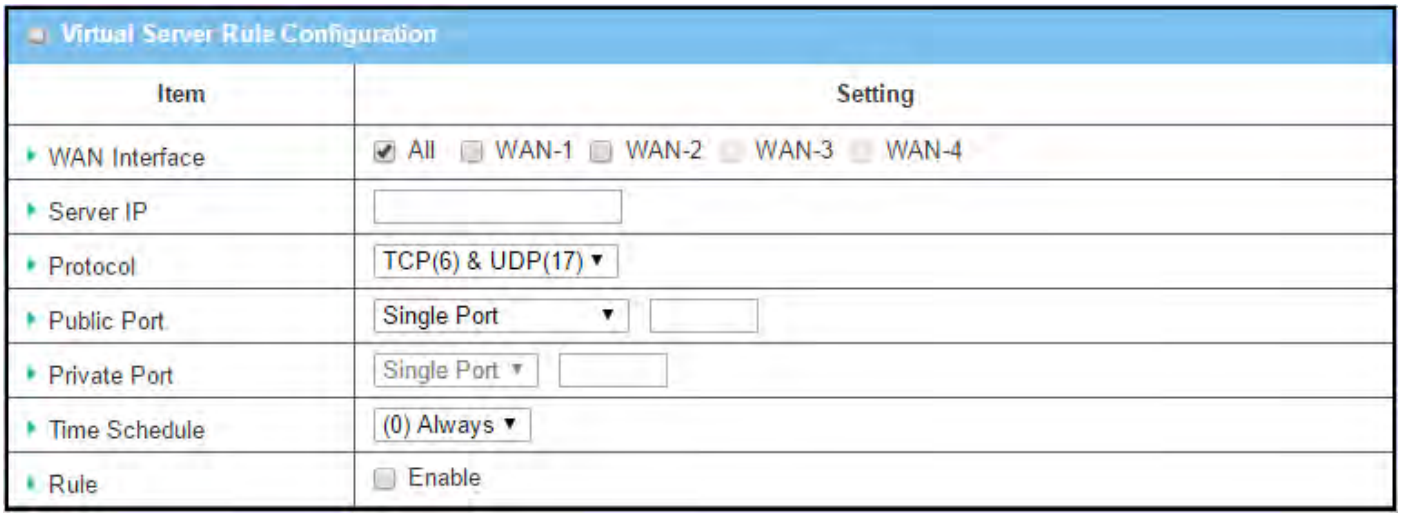
Configuration		
Item	**Value setting**	**Description**
Virtual Server	The box is unchecked by default	Check the **Enable** box to activate this port forwarding function
Virtual Computer	The box is checked by default	Check the **Enable** box to activate this port forwarding function
Save	N/A	Click the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

Create / Edit Virtual Server

The gateway 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.



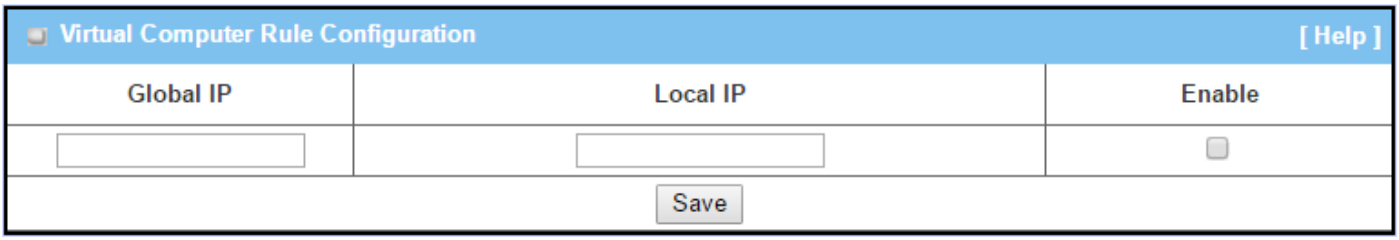
Virtual Server Rule Configuration		
Item	**Value setting**	**Description**
WAN Interface	1. A Must filled setting 2. Default is **ALL**.	Define the selected interface to be the packet-entering interface of the gateway. If the packets to be filtered are coming from **WAN-x** then select **WAN-x** for this field. Select **ALL** for packets coming into the gateway 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	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 gateway allows you to custom your Virtual Computer rules. It supports up to a maximum of 20 rule-based Virtual Computer sets.

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

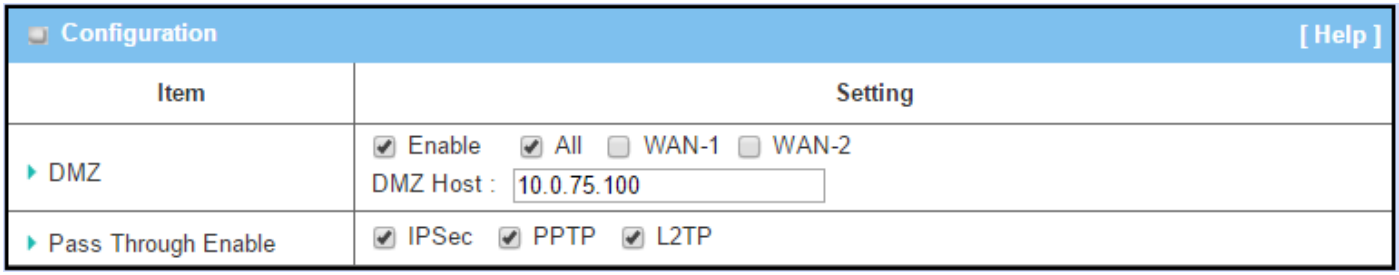


Virtual Computer Rule Configuration		
Item	**Value setting**	**Description**
Global IP	A Must filled setting	This field is to specify the IP address of the WAN IP.
Local IP	A Must filled setting	This field is to specify the IP address of the LAN IP.
Enable	N/A	Then check **Enable** box to enable this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

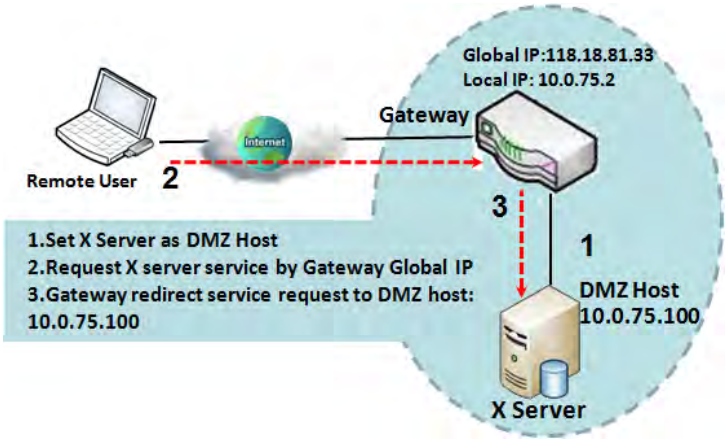
2.5.3 DMZ & Pass Through

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

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

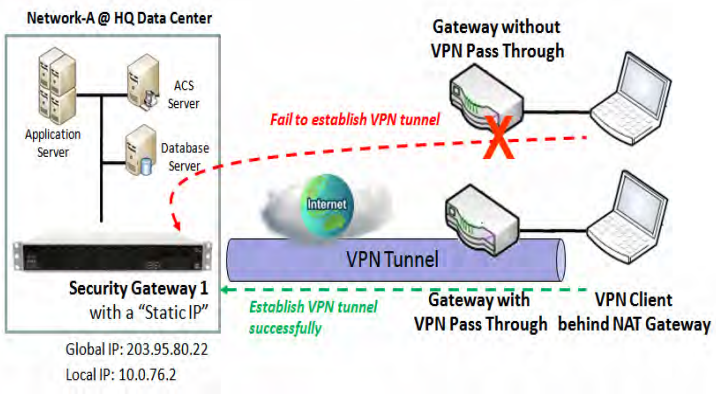


DMZ Scenario



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



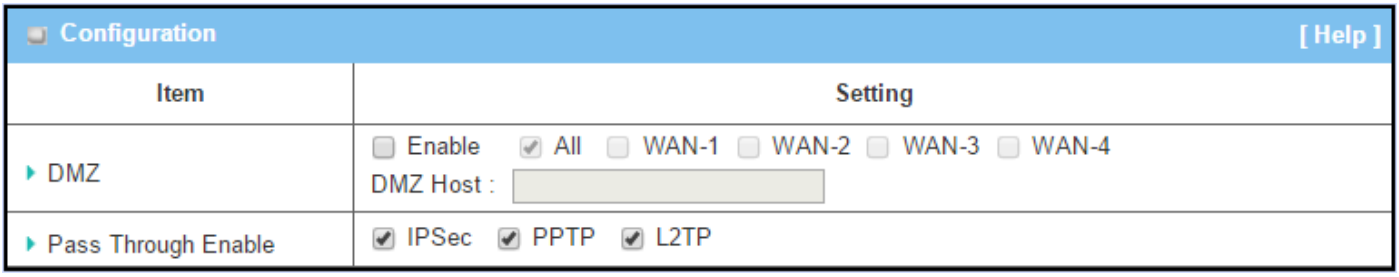
Since VPN traffic is different from that of TCP or UDP connection, it will be blocked by NAT gateway. To support the pass through function for the VPN connections initiating from VPN clients behind NAT gateway, the gateway must implement some kind of VPN pass through function for such application. The 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 gateway device.

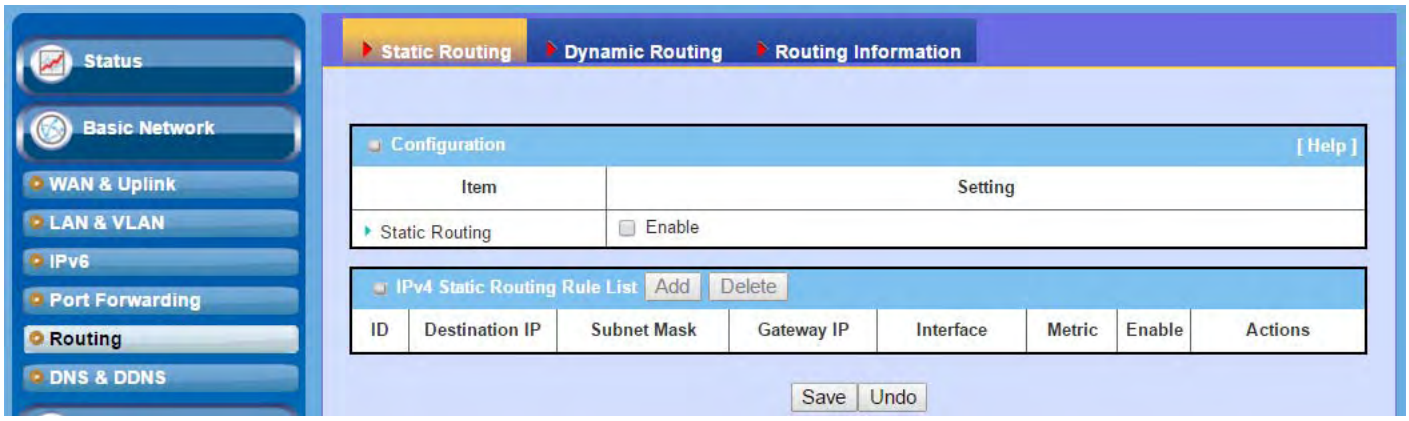
Enable DMZ and Pass Through



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 gateway, 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 gateway 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

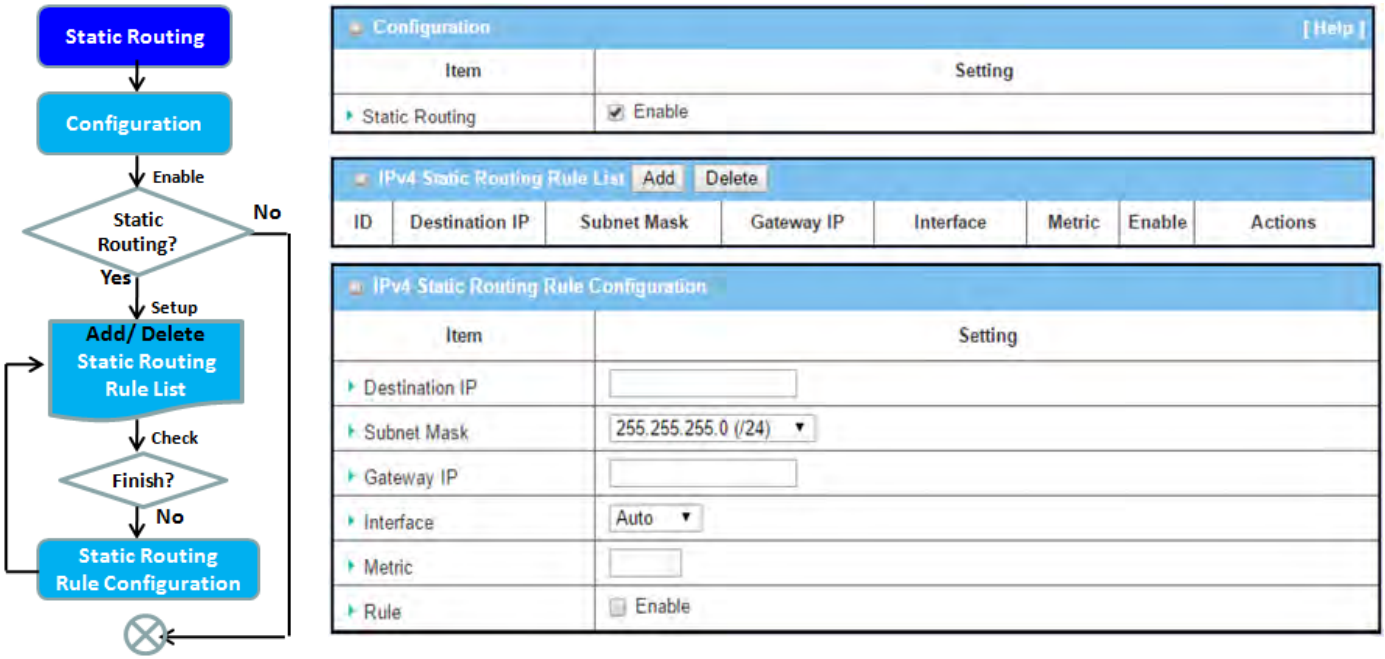
2.6 Routing



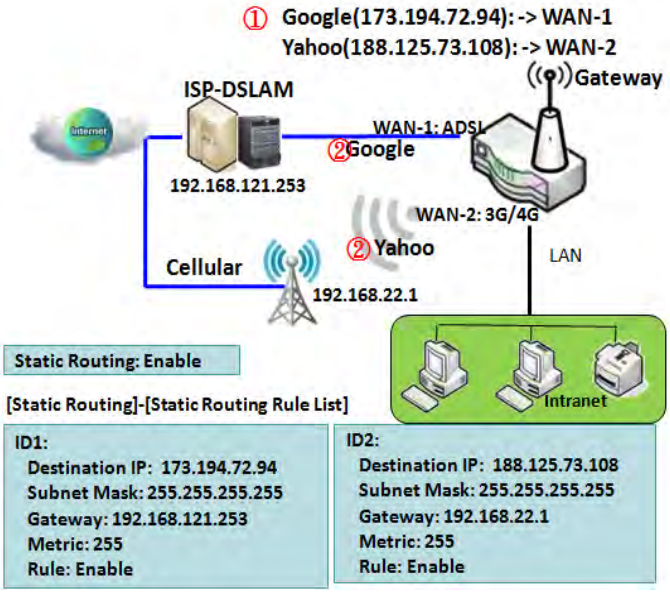
If you have more than one router and subnet, you will need to enable routing function to allow packets to find proper routing path and allow different subnets to communicate with each other. Routing is the process of selecting best paths in a network. It is performed for many kinds of networks, like 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 gateway 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



"Static Routing" function lets you define the routing paths for some dedicated hosts/servers or subnets to store in the routing table of the gateway. The gateway 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

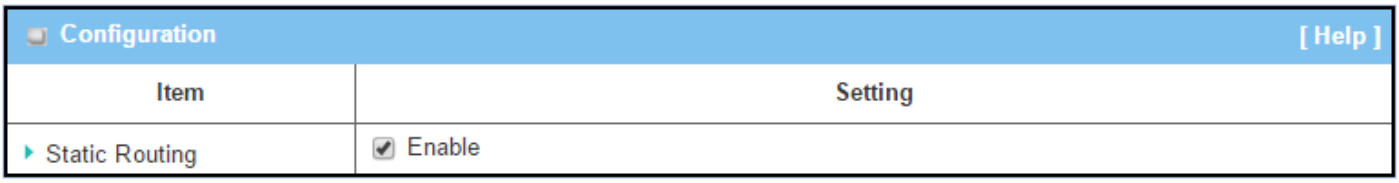
Go to **Basic Network** > **Routing** > **Static Routing** Tab.

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

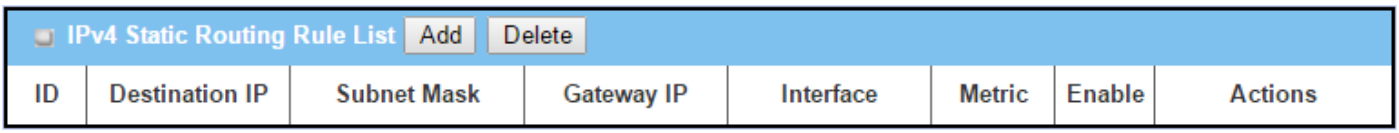
Just check the **Enable** box to activate the "Static Routing" feature.



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

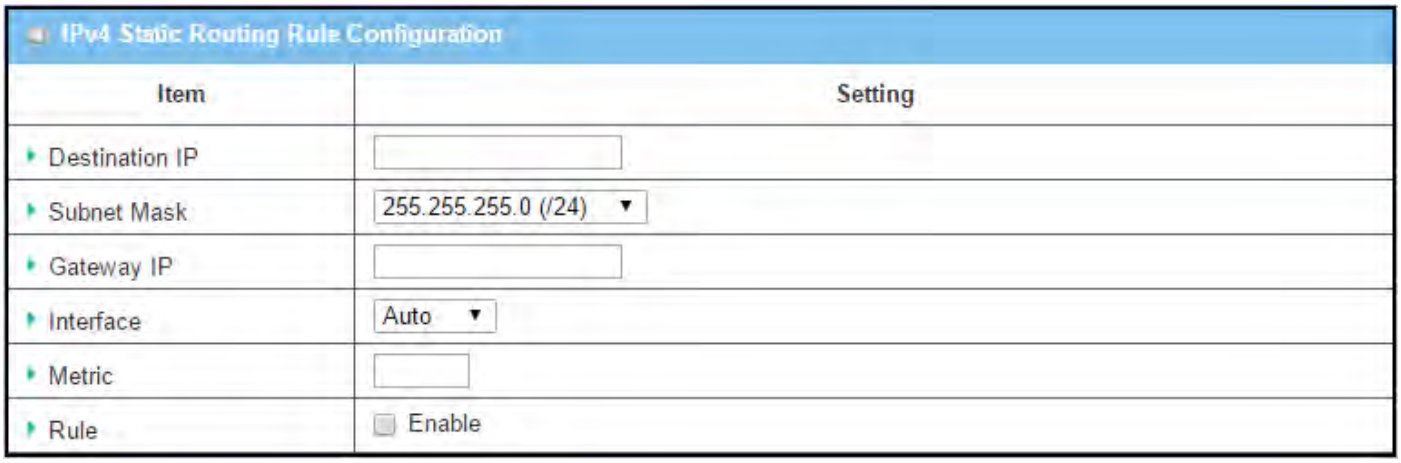
Create / Edit Static Routing Rules

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.



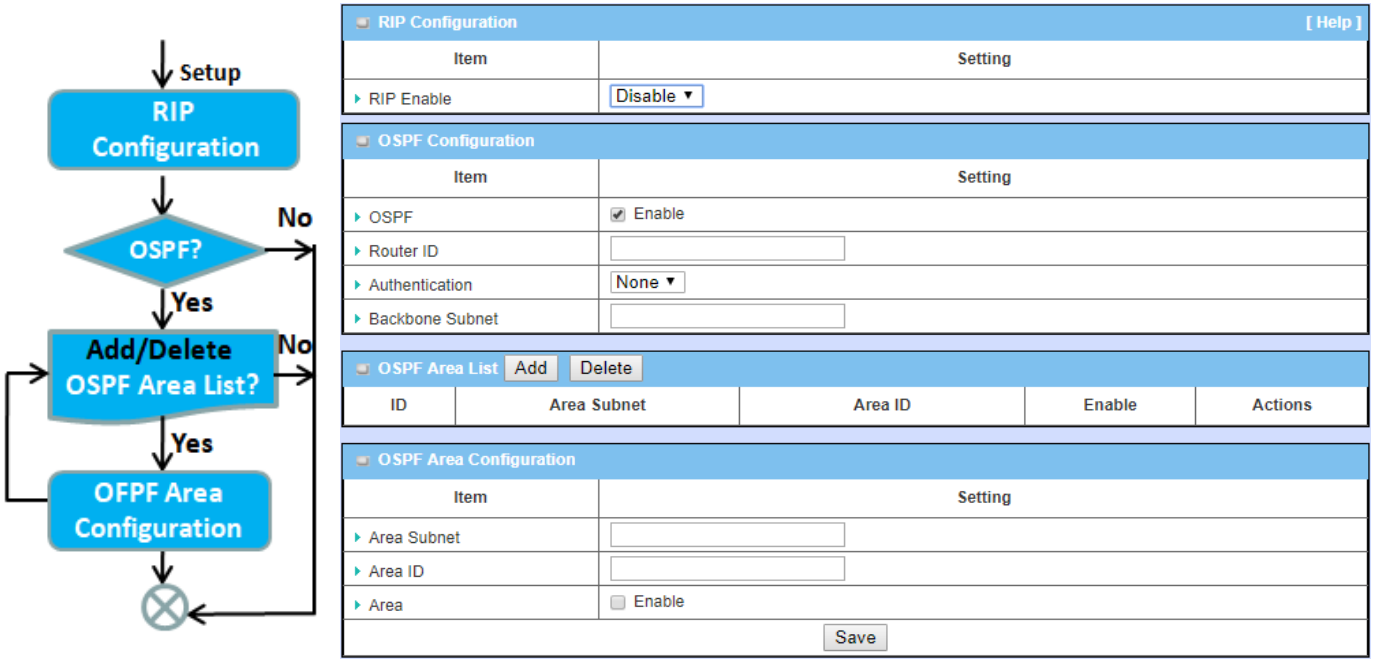
The gateway allows you to custom your static routing rules. It supports up to a maximum of 64 rule sets. When **Add** button is applied, **Static Routing Rule Configuration** screen will appear, while the **Edit** button at the end

of each static routing rule can let you modify the rule.



IPv4 Static Routing 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. Numberic 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



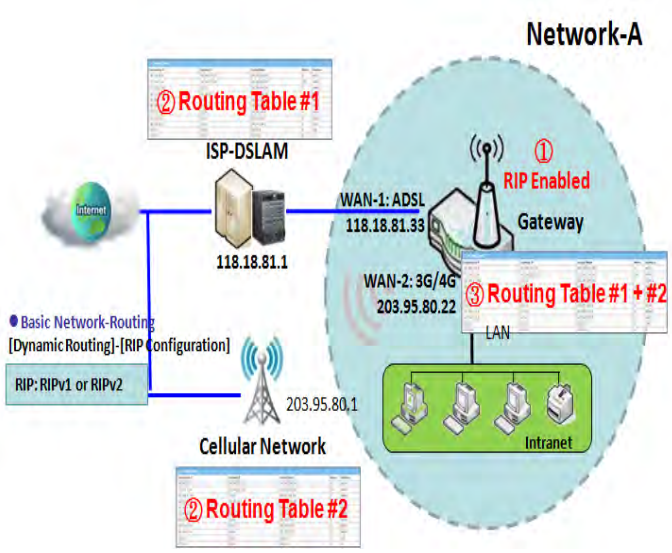
Dynamic Routing, also called adaptive routing, describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in network conditions.

This gateway 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.

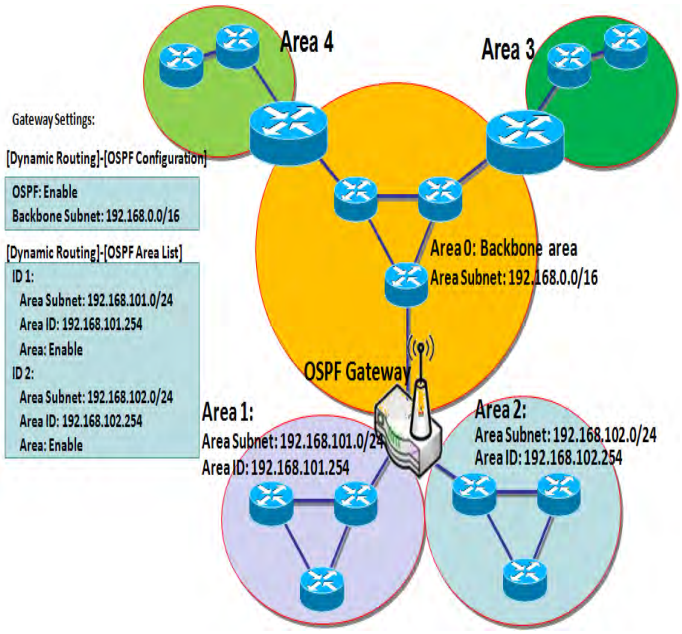
M2M Cellular Gateway

RIP Scenario



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

OSPF Scenario



Open Shortest Path First (OSPF) is a routing protocol 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.

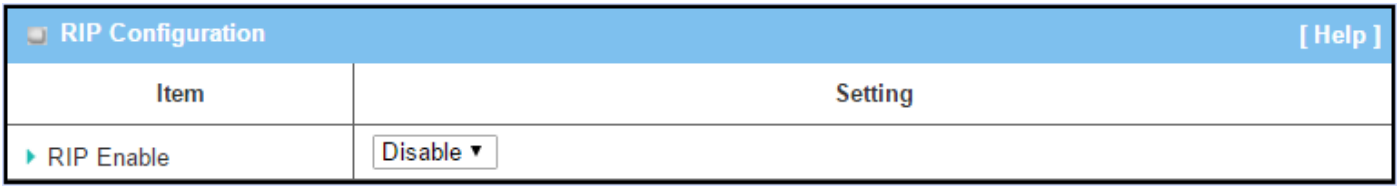
The dynamic routing setting allows user to customize RIP, and OSPF protocols through the router based on their office setting.

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

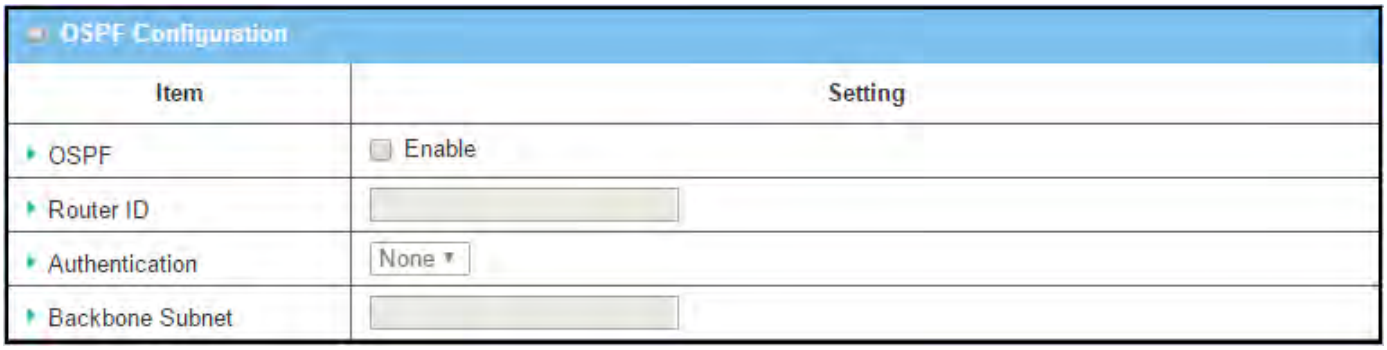
The RIP configuration setting allows user to customize RIP protocol through the router based on their office setting.



RIP Configuration		
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.

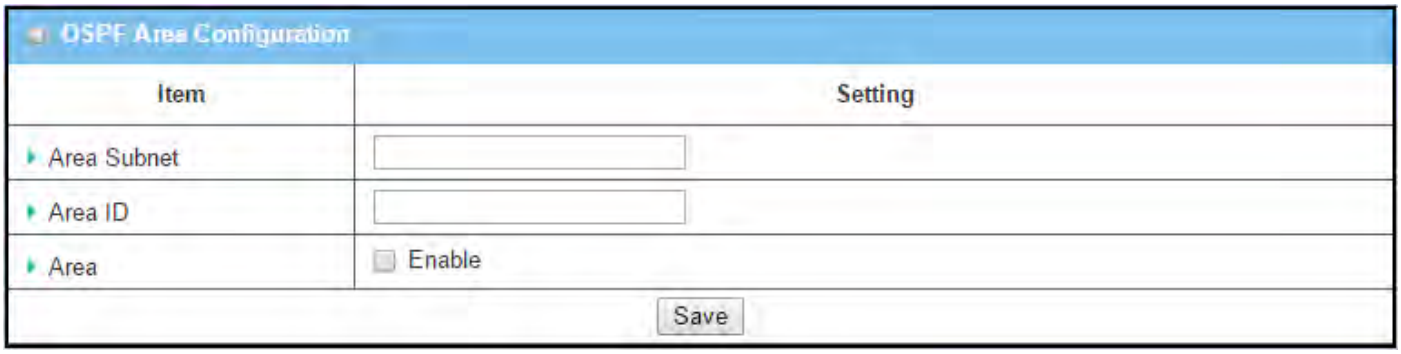


OSPF Configuration		
Item	**Value setting**	**Description**
OSPF	Disable is set by default	Click **Enable** box to activate the OSPF protocol.
Router ID	1. IPv4 Format 2. A Must filled setting	The Router ID of this router on OSPF protocol
Authentication	None is set by default	The Authentication method 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 gateway allows you to custom your OSPF Area List rules. It supports up to a maximum of 32 rule sets.

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



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. Policy Routing Information is only available when the Load Balance function is enabled and the Load Balance Strategy is By User Policy.

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

Routing Table

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

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

Policy Routing Information

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

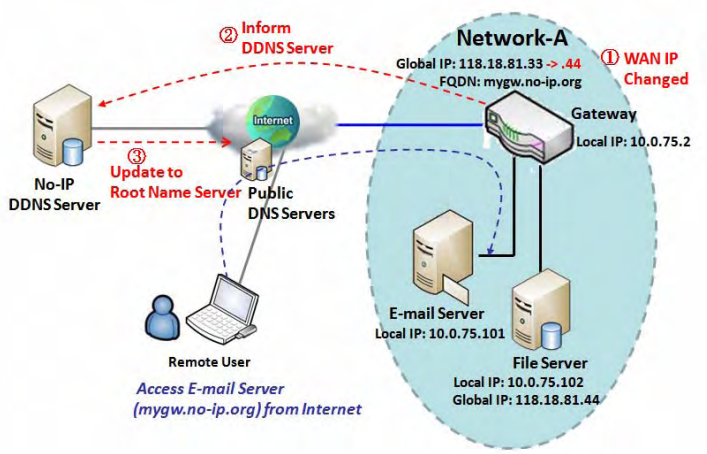
Policy Routing Information		
Item	**Value setting**	**Description**
Policy Routing Source	N/A	Policy Routing of Source. String Format.
Source IP	N/A	Policy Routing of Source IP. IPv4 Format.
Destination IP	N/A	Policy Routing of Destination IP. IPv4 Format.
Destination Port	N/A	Policy Routing of Destination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

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[7,8].

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.

7 http://en.wikipedia.org/wiki/Domain_Name_System
8 http://en.wikipedia.org/wiki/Dynamic_DNS

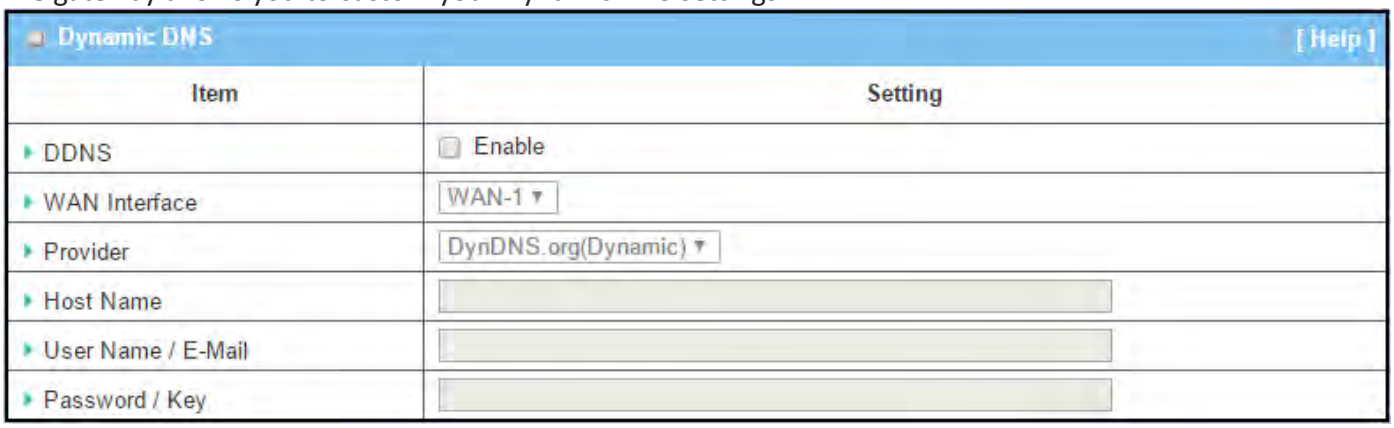
DNS & DDNS Setting

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

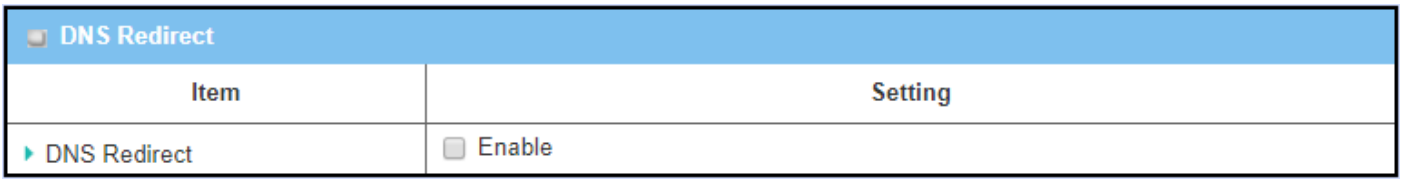
The gateway allows you to custom your Dynamic DNS settings.



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 gateway.
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 addresss of Dynamic DNS.
Password / Key	1. String format can be any text 2. A Must filled setting	Enter your Password or Key of Dynamic DNS.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Setup DNS Redirect

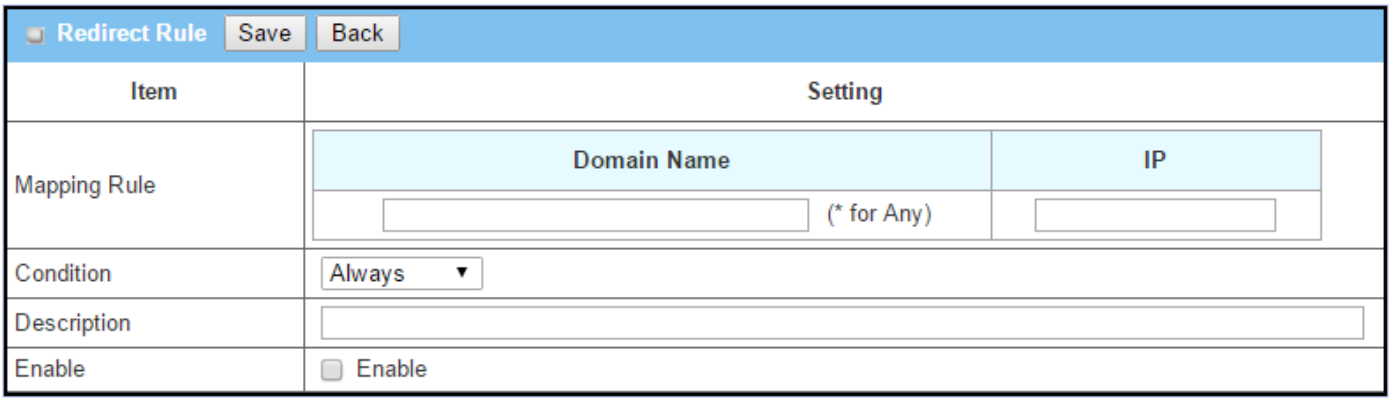
DNS redirect is a special function to redirect certain traffics to a specified host. Administator can manage the internet / intranet traffics that are going to access some restricted DNS and force those traffics to be redirected to a specified host.



DNS Redirect 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 gateway can redirect the traffic that matched the DNS to corresponding pre-defined IP address.

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



Redirect Rule Configuration		
Item	**Value setting**	**Description**
Domain Name	1. String format can be any text	Enter a domain name to be redirect. The traffic to specified domain name will be redirect to the following IP address.

	2. A Must filled setting	***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 will the DNS redirect action can be applied. It can be **Always**, or **WAN Block**. **Always:** The DNS redirect function can be applied to matched DNS all the time. **WAN Block:** The DNS redirect function can be applied to matched DNS only when the WAN connection is disconneced, 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