TW-LTE/4G/3G

WLAN 802.11ac

router

User Manual

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B.

TABLE OF CONTENTS

Introduction

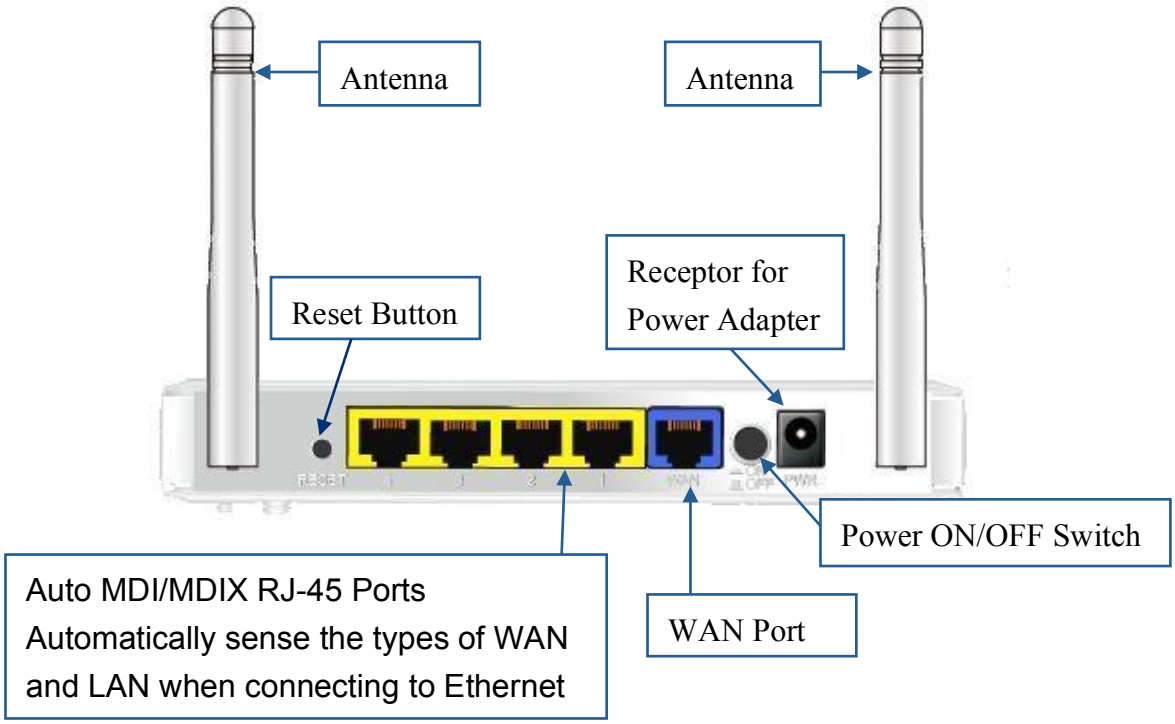
Congratulations on your purchase of this outstanding product: TW-LTE/4G Wlan Router. This residential gateway is specifically designed for those who need to have the data, voice, video and file sharing services beyond his home and office. It provides a complete solution for Internet surfing and broadband sharing. Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read this manual carefully for fully exploiting the functions of this product.

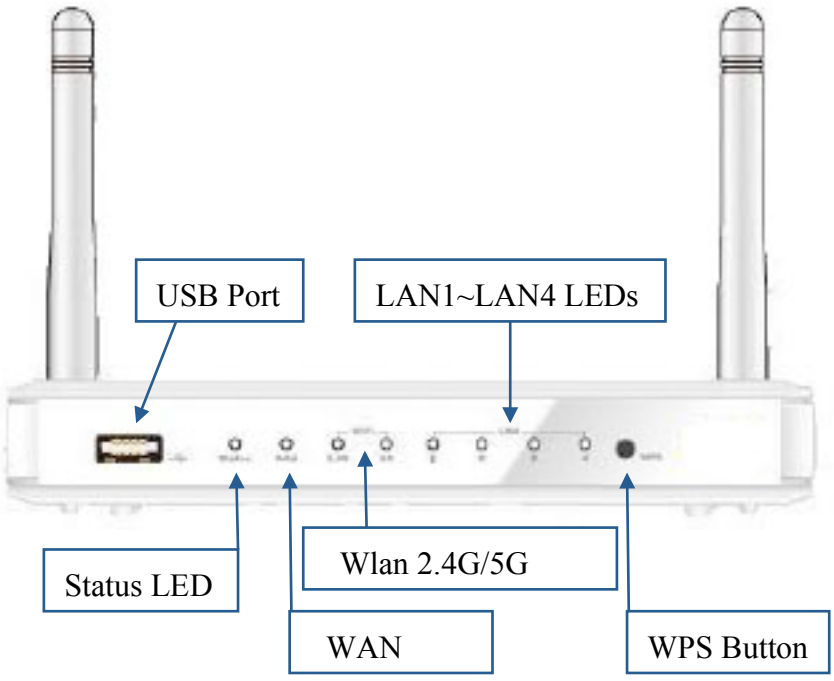
Package List

Items	Description	Contents	Quantity
1	TW-LTE/4G/3G router		1
2	CD		1
3	Power Adapter		1
4	Manual		1
5	Ethernet cable		1

Hardware Installation

Hardware configuration





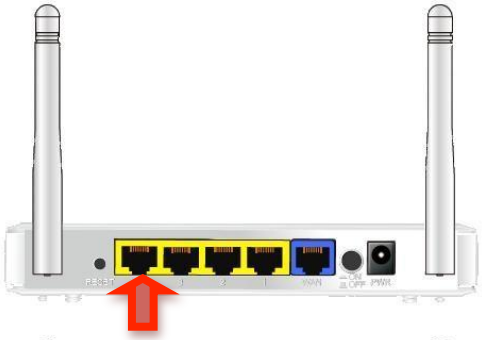
LED indicators

	LED Status	Description
Status (USB)	Green in flash	power is on
	Green in fast flash	Reset mode
	Green	USB storage attached
	Green in flash	Data access
WAN WAN	Green	WAN is on.
	Green in flash	Data access
WLAN 2.4G	Green	Wlan is on.
	Green in flash	Data access
WLAN 5G	Green	Wlan is on.
	Green in flash	Data access
LAN1~4	Green	LAN is on.
	Green in flash	Data access

How to Operate_

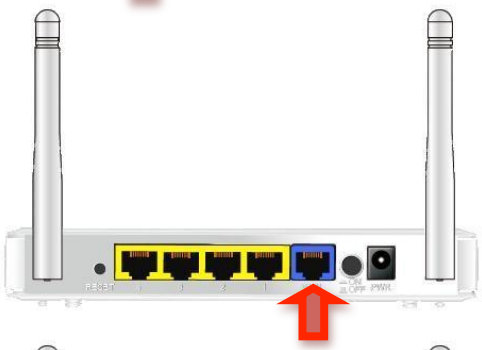
Step 1.

Plug the RJ45 cable into LAN port 1~4 and connect with your PC or NB.



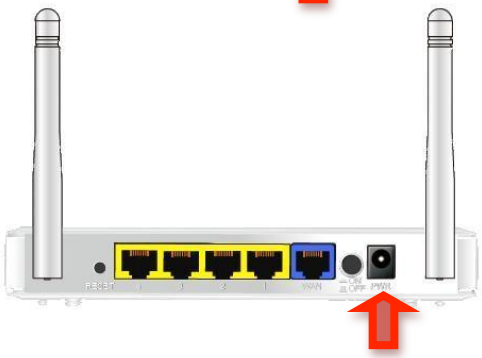
Step 2.

Plug your RJ-45 into the WAN port and connect with your xDSL modem.



Step 3.

Plug the power jack into it.



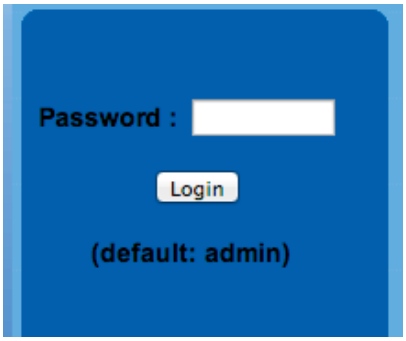
Step 4

Prepare a USB Storage or 3G/4G/LTE dongle, and then plug into the USB port if need to enable wireless WAN.

Making Configuration

Whenever you want to configure your network or this device, you can access the Configuration Menu by opening the web-browser and typing in the IP Address of the device. The default IP Address is: 192.168.0.254.

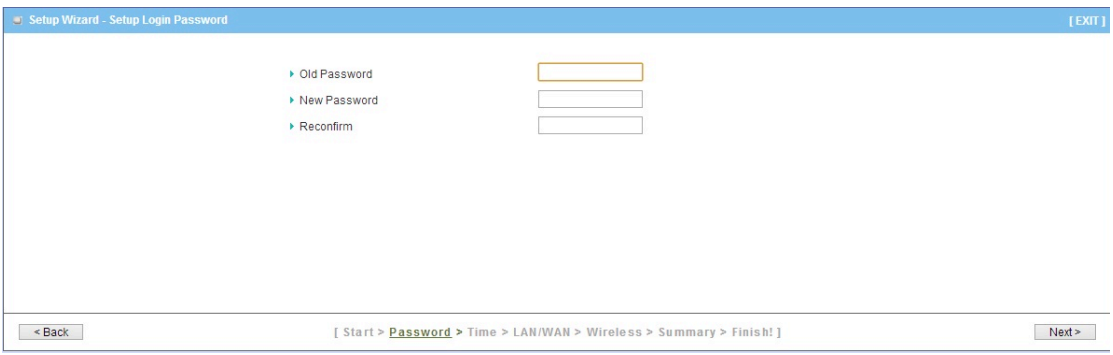
Enter the default username “admin” in the System Password and then click ‘login’ button.



Configure with the setup wizard

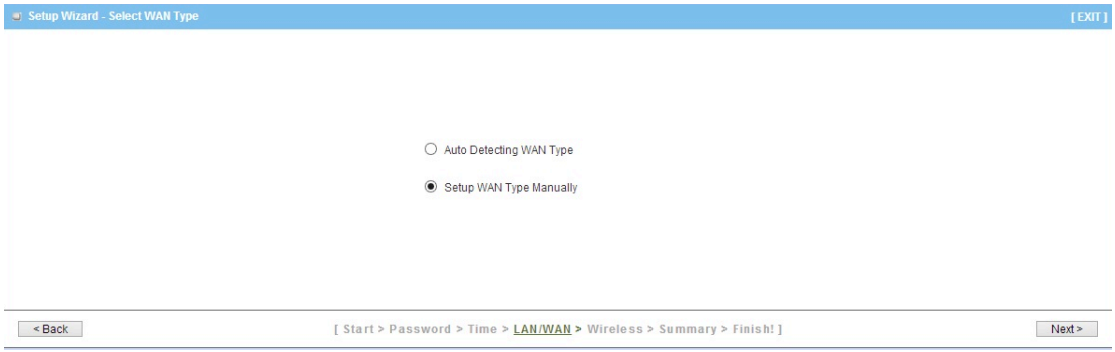
Select “Wizard” for basic settings in a simple way

Press “Next” to start the Setup Wizard



You can change the password of administrator here

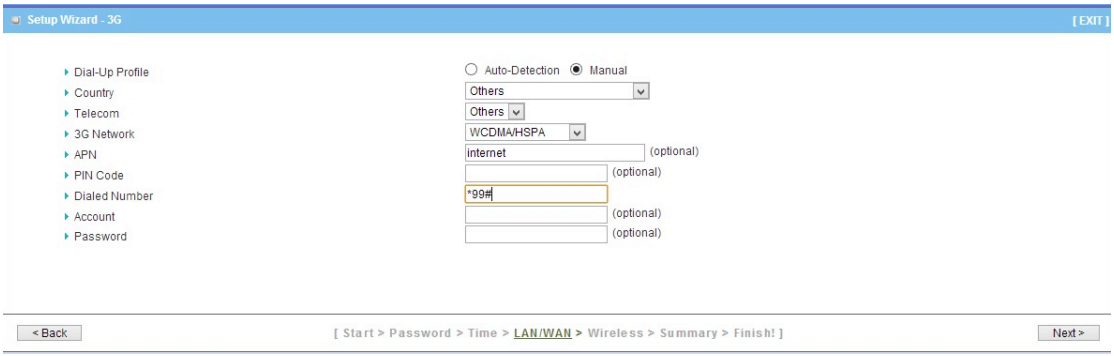
Select Time Zone



Select “auto detecting WAN type” or “setup wan type manually”

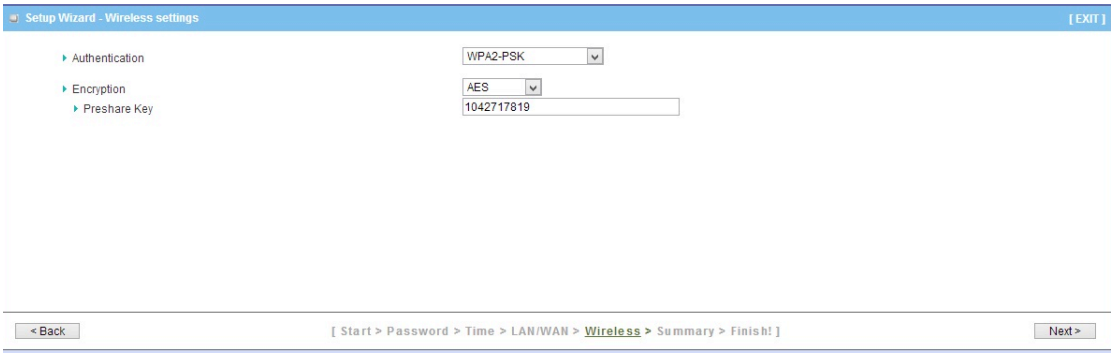
If selected manually, next select Wireless WAN or Ethernet WAN and setup WAN type followingly

If selected Ethernet, also select WAN type

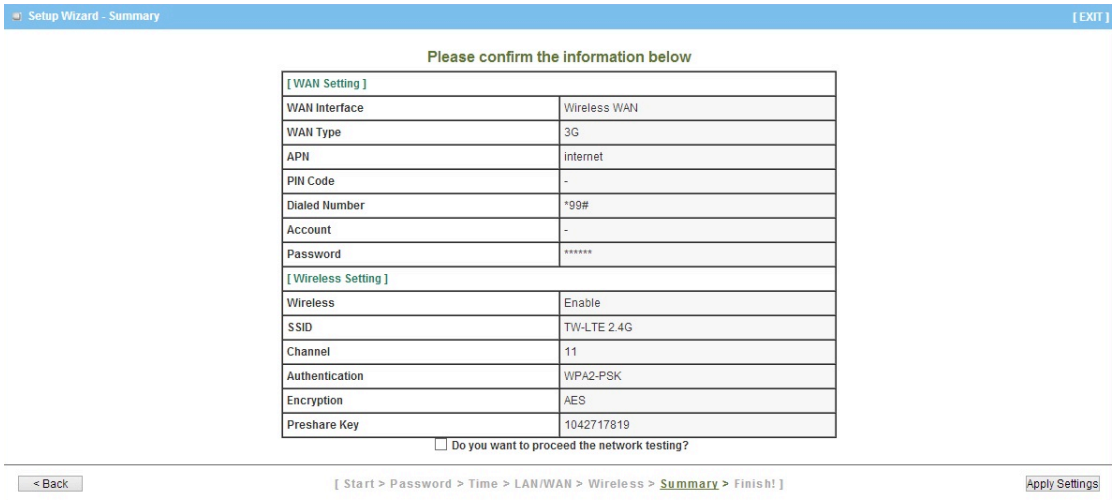


If selected Wireless LAN, please put settings as in picture (usually in Finland)

Wireless settings (first 2,4G and after that 5G)



Wireless authentication and encryption



Check the information again

Click next and System is applying the setting. Click finish to complete it

Afterwards, you can go Basic Network, Advanced Network, Application or System respectively on left hand side of web page.

1. Basic Network

Status page

IPv4 System Status [HELP]

Item	Status	Sidenote
IP Address	10.184.153.204	
Subnet Mask	255.255.255.248	
Gateway	10.184.153.201	
Domain Name Server	195.197.54.100 , 195.74.0.47	
Connection Time	00:40:44	

Wireless Modem Information

Item	Status	Sidenote
Card Info	E3276	
Link Status	Connected.	
Signal Strength	N/A	
Network Name	Elisa	

Statistics Information

	Receive	Transmit
WAN	0 Packets	6 Packets
LAN	43617 Packets	82889 Packets
WLAN	0 Packets	0 Packets

Select Wireless Status - 2.4G

Wireless Status 2.4G AP 1

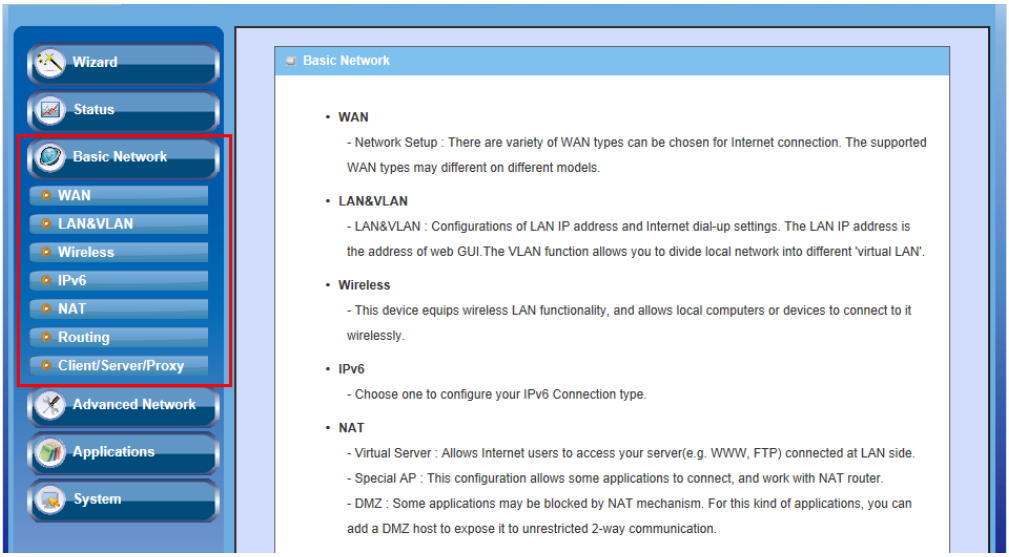
Item	WLAN Status	Sidenote
Wireless mode	Enable	(B/G/N Mixed)
SSID	TW-LTE 2.4G	Edit
Channel	11	
Security	WPA2-PSK	(AES)
MAC address	00:50:18:67:3F:92	

Wireless Status 2.4G AP 2

Item	WLAN Status	Sidenote
Wireless mode	Disable	(B/G/N Mixed)
SSID	TW-LTE 2.4G_2	Edit
Channel	11	
Security	Auto	(None)
MAC address	02:50:18:64:3F:92	

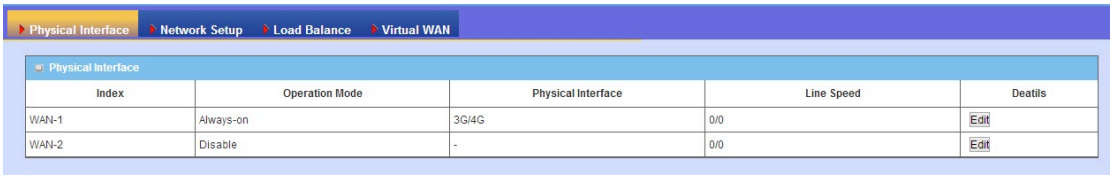
Note : You can see all the status of this RG on ‘Status’ page.

You can enter Basic Network for **WAN, LAN&VLAN, Wireless, IPv6, NAT, Routing,** and **Client/Server/Proxy** settings as the icon here shown



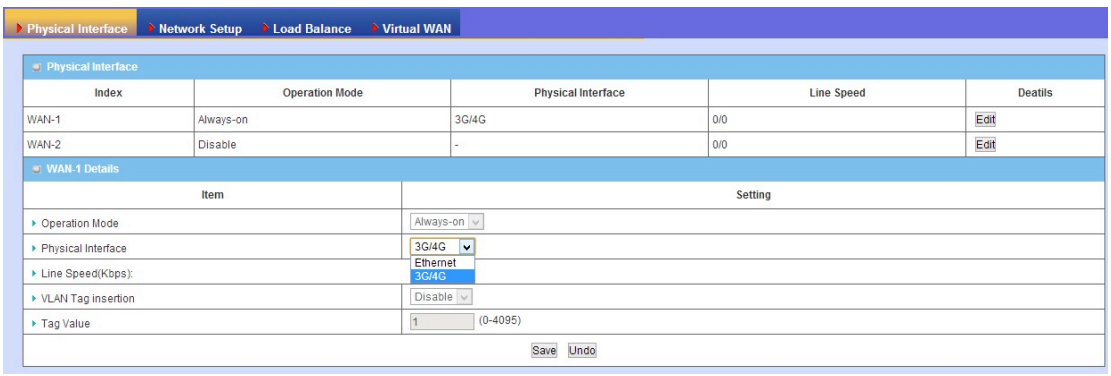
1.1 WAN Setup

You can enter Basic Network, WAN for Ethernet and 3G/4G/LTE setting as below.



1.1.1 Physical Interface

Click on the "**Edit**" button for each WAN interface and you can get the detail physical interface settings and then configure the settings as well.



1. **WAN-1**: The operation mode of this interface is forced to "**Always-on**" mode, and operates as the primary internet connection. You can click on the respective "**Edit**" button and configure the rest items for this interface.
2. **WAN-2**: The operation mode of this interface is disabled by default, you can click on the respective "**Edit**" button and configure the second WAN interface to operate as "**fail over**" mode, so that when the WAN-1 connection broken, the device will try to failover the internet connection to WAN-2.
3. **Physical Interface**: Select the WAN interface from the available list. For this device, there are "Ethernet" and "3G/4G/LTE" items. If you would like the RJ45 WAN port to operate as the primary internet connection, Please choose "Ethernet"; Otherwise, choose "3G/4G" for configuring the embedded 3G/4G/LTE modem as primary WAN connection.
4. **Line Speed (Kbps)**: You can specify the downstream / upstream speed for the corresponding WAN connection. Such information will be referred in QoS and load balance function to manage the traffic load for each WAN connection.
5. **VLAN Tag Insertion, Tag Value**: If your ISP required a VLAN tag been inserted into the WAN packets, you can enable this setting, and enter the specified tag value.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

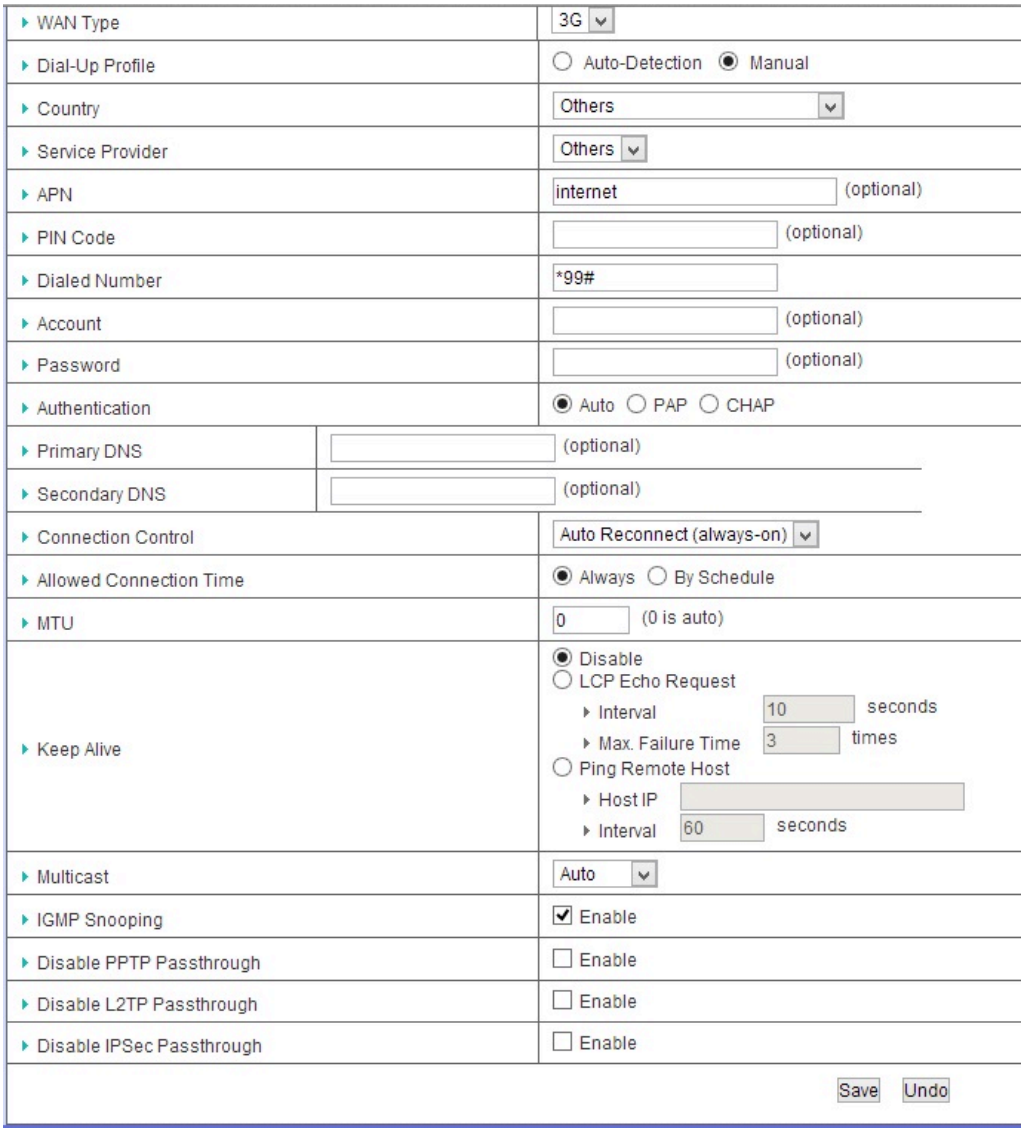
1.1.2 Network Setup

There are two physical WAN interfaces that you can configure one by one to get proper internet connection setup. They include the Wireless WAN - the remote wireless ISP such as 3G/4G/LTE and the Ethernet WAN - the DSL ISP such as Dynamic IP, Static IP, PPPoE, PPTP and L2TP

1.1.2.1 Wireless WAN – 3G/4G/LTE

Click on the "**Edit**" button for the 3G/4G/LTE WAN interface and you can get the detail WAN settings and then configure the settings as well.

1. **WAN Type**: Choose “3G” from the drop list
2. **Dial-up Profile:** Choose “Auto-Detection” or “Manual”. If you select “Auto-Detection”, then system will check the information automatically. If you select “Manual”, then you have to specify more ISP-related settings, such as Country, Service Provider, and APN, to get the 3G/4G/LTE service. The “Auto-Detection” option is suggested.



3. **PIN Code**: Enter the PIN Code for your SIM card(Optional)
4. **Dialed Number**: Enter the dialed number that is provided by your ISP.
5. **Account, Password**: Enter the account / Password that is provided by your ISP(Optional).
6. **Authentication**: Choose “auto”, “PAP”, or “CHAP” according your ISP’s authentication approach.
7. **Primary / Secondary DNS**: Enter the Domain Name Server settings

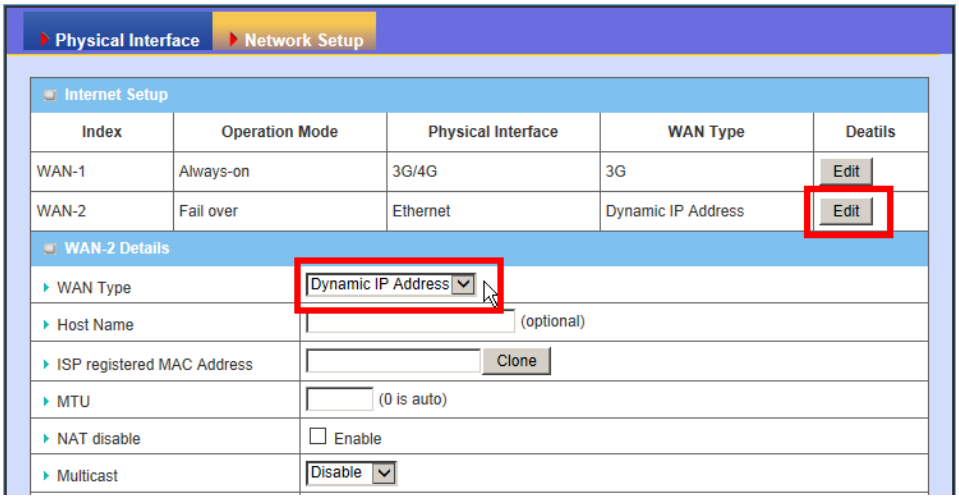
(Optional)

8. **Connection Control**: Select your connection control scheme from the drop list; “auto-reconnect (always-on)” option is recommended.
9. **Allowed Connection Time**: You can select **“Always”** or **“By Schedule”** for connection method. If you choose “**By Schedule**” rule, you have to add a new schedule for this connection.
10. **MTU**: Most ISP offers MTU value to users. The default value is o (auto).
11. **Keep Alive:** You can do preferred settings by using this feature to prevent the built-in 3G/4G/LTE modem from some sort of auto-timeout and disconnects from the internet after a period of inactivity.
12. **Multicast:** Enable or disable multicast traffics from the internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
13. **IGMP Snooping:** Enable or disable IGMP snooping function. If you enable the IGMP snooping function, this device will detect all IGMP messages exchanged on the link and will maintain a table indicating for each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.
14. **Disable PPTP / L2TP / IPSec Passthrough:** By default, the device allows the PPTP / L2TP / IPSec VPN traffic that initiated from local VPN client to pass through to Internet. If you want to disable such function, just change the setting to disable it.

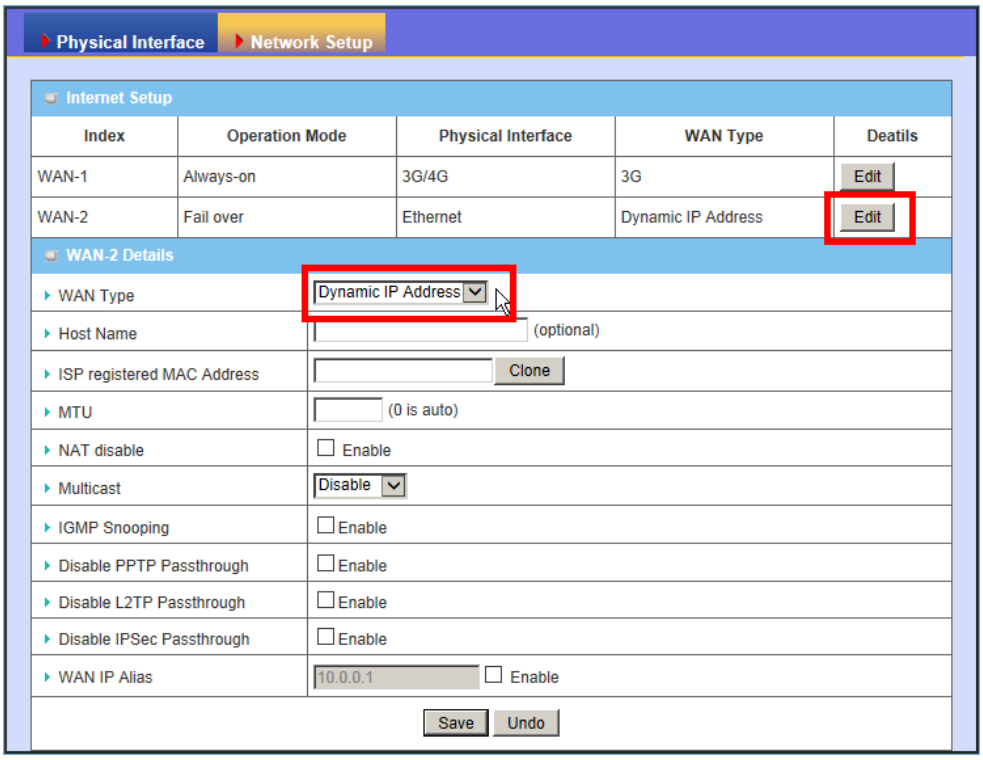
Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

1.1.2.2 Ethernet WAN

Click on the “Edit” button for the Ethernet WAN interface and you can get the detail WAN settings and then configure the settings as well.



1.1.2.2.1 Dynamic IP address



1. **WAN Type**: choose “Dynamic IP Address” from the drop list
2. **Host Name**: Optional, required by some ISPs, for example, @Home.
3. **ISP registered MAC Address**: Enter the WAN MAC address of this device. (Optional)
4. **MTU**: Most ISP offers MTU value to users. The default value is o (auto)
5. **NAT disable:** If you enable this option, it will act with a non-NAT function.
6. **Multicast:** Enable or disable multicast traffics from the internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
7. **IGMP Snooping:** Enable or disable IGMP snooping function. If you enable

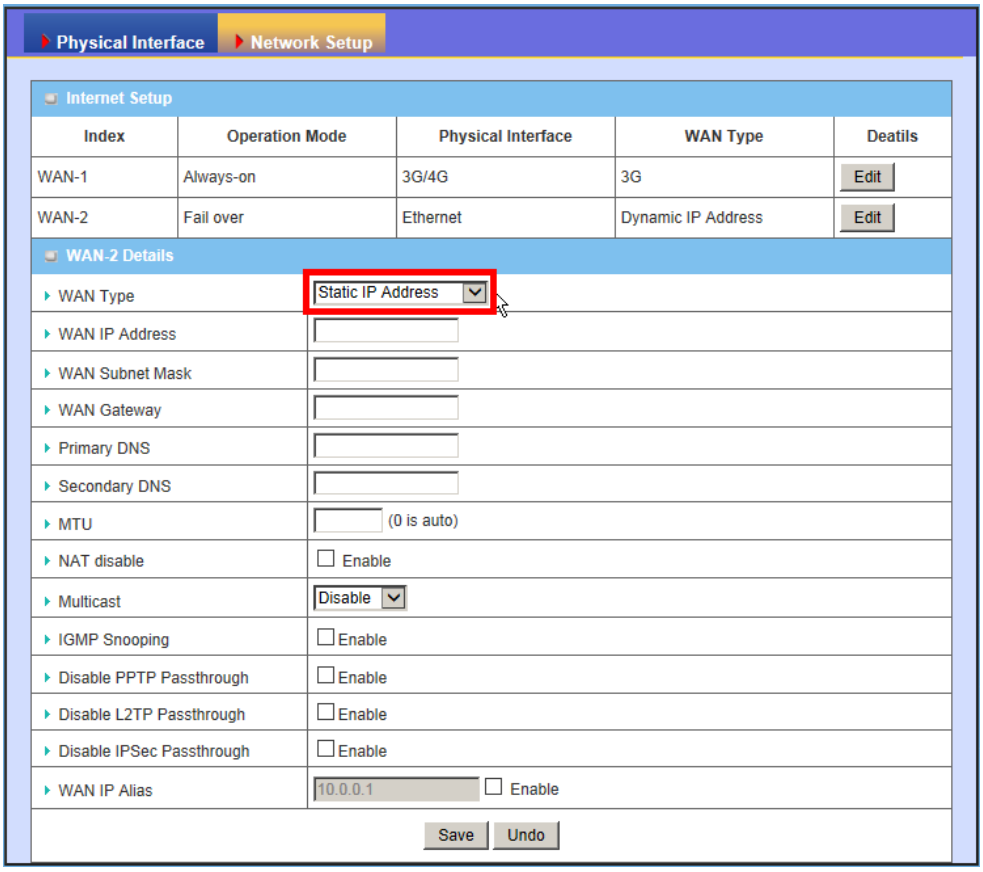
the IGMP snooping function, this device will detect all IGMP messages exchanged on the link and will maintain a table indicating for each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.

8. **Disable PPTP / L2TP / IPSec Passthrough:** By default, the device allows the PPTP / L2TP / IPSec VPN traffic that initiated from local VPN client to pass through to Internet. If you want to disable such function, just change the setting to disable it.

   Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

1.1.2.2.2 Static IP Address

Select this option to give your static IP information. You will need to enter in the IP address, subnet mask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.



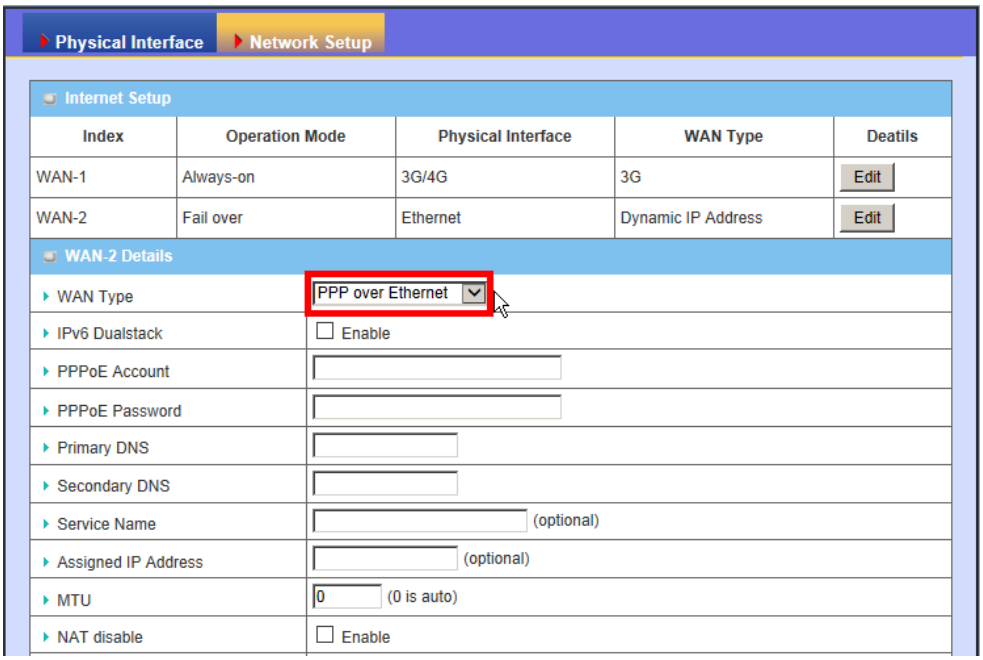
1. **WAN Type:** Choose “Static IP Address” from the drop list
2. **WAN IP address/ Subnet Mask/ Gateway:** Enter the IP address, subnet mask, and gateway address, provided to you by your ISP.

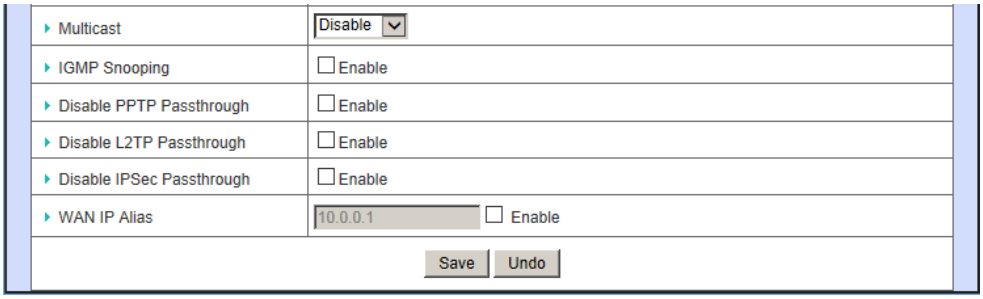
3. **Primary DNS/ Secondary DNS:** input the Primary/Secondary DNS if necessary.
4. **MTU**: Most ISP offers MTU value to users. The default value is o (auto)
5. **NAT disable:** If you enable this option, it will act with a non-NAT function.
6. **Multicast:** Enable or disable multicast traffics from the internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
7. **IGMP Snooping:** Enable or disable IGMP snooping function. If you enable the IGMP snooping function, this device will detect all IGMP messages exchanged on the link and will maintain a table indicating for each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.
8. **Disable PPTP / L2TP / IPSec Passthrough:** By default, the device allows the PPTP / L2TP / IPSec VPN traffic that initiated from local VPN client to pass through to Internet. If you want to disable such function, just change the setting to disable it.
9. **WAN IP alias**: The device supports 2 WAN IP address, one is for primary connection that provides users/devices in the LAN to access Internet; the other is a virtual connection that let remote user to manage this device.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

1.1.2.2.3 PPP over Ethernet

Select this option if your ISP requires you to use a PPPoE connection. This option is typically used for DSL services.





1. **WAN Type:** Choose “PPP Over Ethernet” from the drop list
2. **IPv6 Dualstack**: You can enable / disable the function of IPv4/IPv6 dual stack.
3. **PPPoE Account** and **Password:** The account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it blank.
4. **Primary DNS / Secondary DNS:** Input the Primary/Secondary DNS if necessary.
5. **Service Name / Assigned IP Address**: Input the Service Name and Assigned IP address if necessary.
6. **MTU:** Most ISP offers MTU value to users. The default MTU value is 0 (auto)
7. **NAT disable :** If you enable this option, it will act with a non-NAT function.
8. **Multicast:** Enable or disable multicast traffics from the internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
9. **IGMP Snooping:** Enable or disable IGMP snooping function. If you enable the IGMP snooping function, this device will detect all IGMP messages

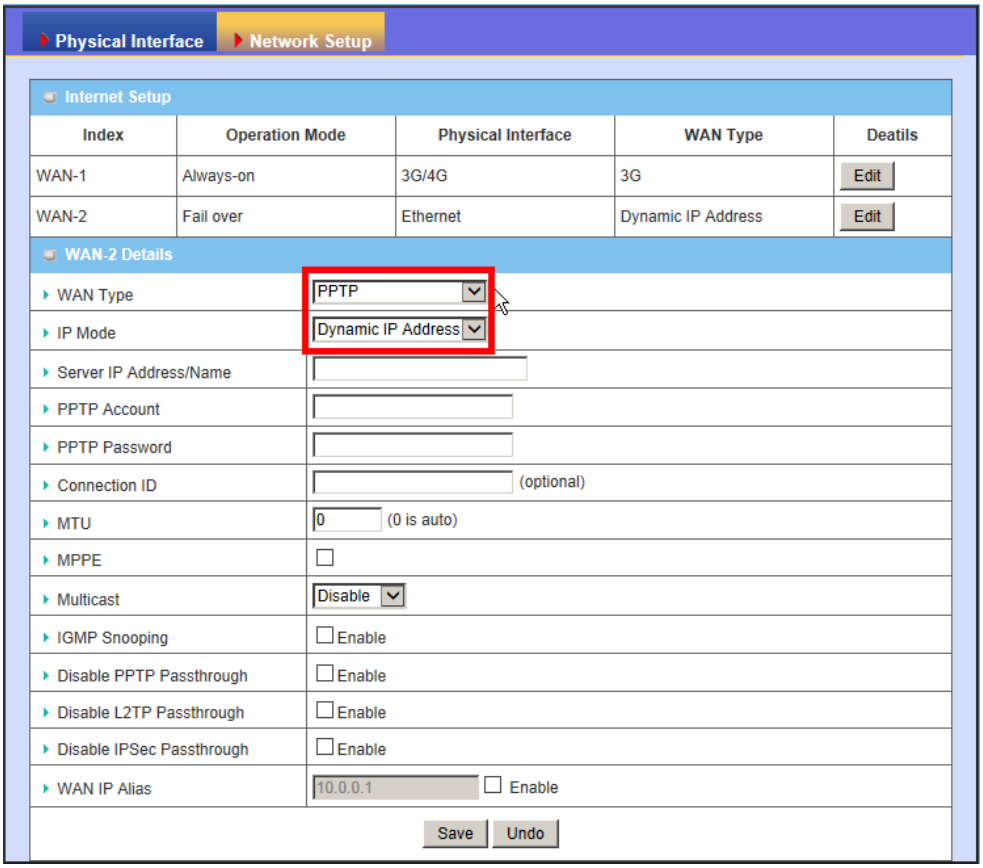
exchanged on the link and will maintain a table indicating for each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.

10. **Disable PPTP / L2TP / IPSec Passthrough:** By default, the device allows the PPTP / L2TP / IPSec VPN traffic that initiated from local VPN client to pass through to Internet. If you want to disable such function, just change the setting to disable it.
11. **WAN IP alias**: The device supports 2 WAN IP address, one is for primary connection that provides users/devices in the LAN to access Internet; the other is a virtual connection that let remote user to manage this device.

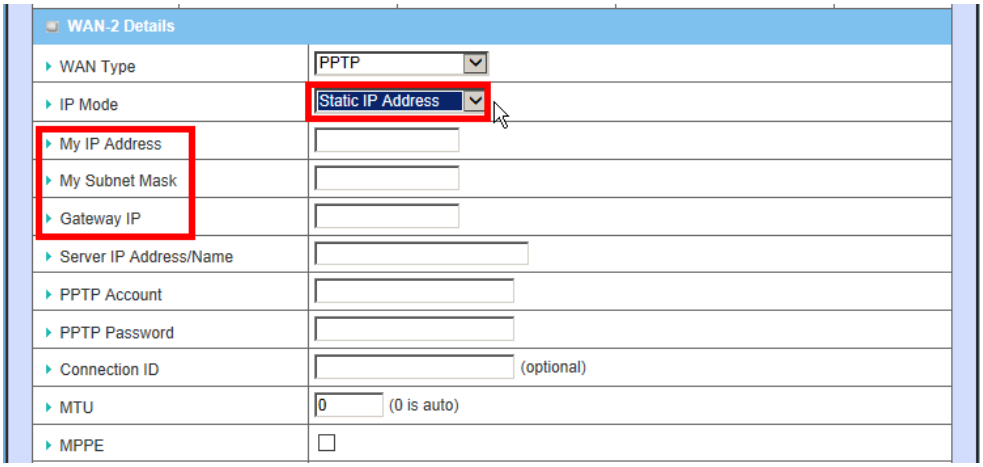
Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

1.1.2.2.4 PPTP

Choose PPTP (Point-to-Point Tunneling Protocol) if your ISP used a PPTP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.



1. **WAN Type:** Choose “PPTP” from the drop list
2. **IP Mode**: Please check the IP mode your ISP assigned, and select “Static IP Address” or “Dynamic IP Address” accordingly. If you select “Static IP Address” option, you have to specify additional “My IP Address”, “My Subnet Mask”, and “Gateway IP” settings provided by your ISP.



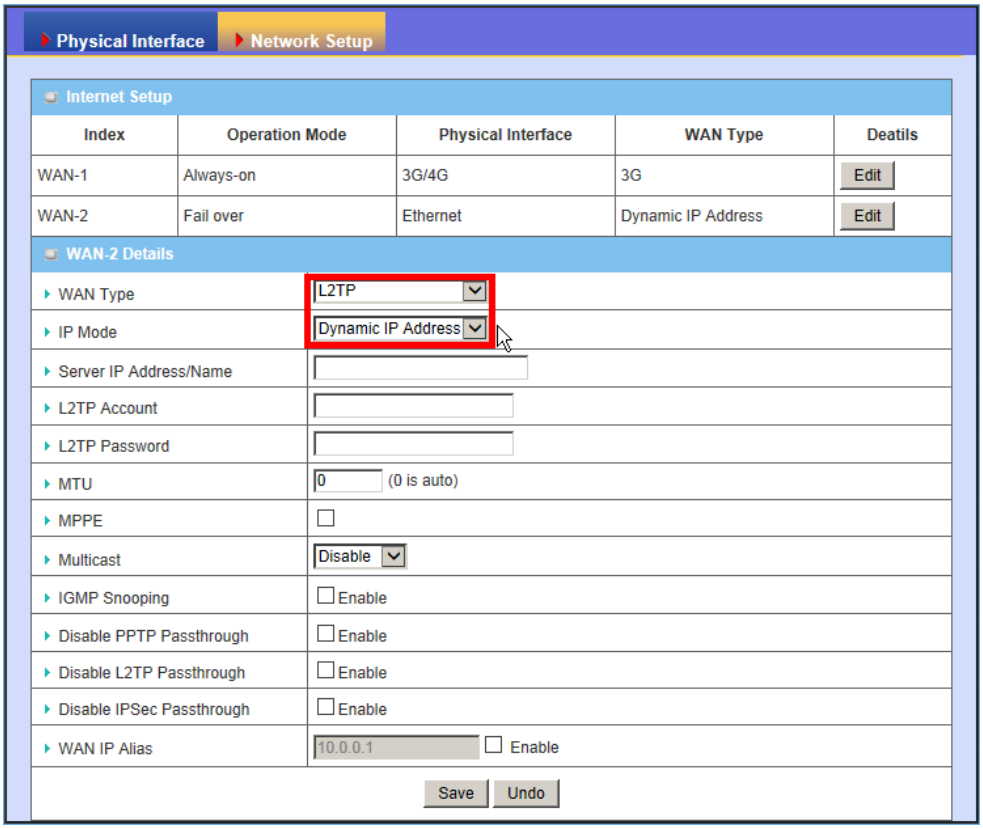
3. **Server IP Address / Name**: The IP address of the PPTP server and designated Gateway provided by your ISP.
4. **PPTP Account** and **Password:** The account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it blank.
5. **Connection ID:** Optional, input the connection ID if your ISP requires it.
6. **MTU :** Most ISP offers MTU value to users. The default MTU value is 0 (auto)
7. **MPPE (Microsoft Point-to-Point Encryption):** Enable or disable this function.
8. **Multicast:** Enable or disable multicast traffics from the internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
9. **IGMP Snooping:** Enable or disable IGMP snooping function. If you enable the IGMP snooping function, this device will detect all IGMP messages exchanged on the link and will maintain a table indicating for each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.
10. **Disable PPTP / L2TP / IPSec Passthrough:** By default, the device allows the PPTP / L2TP / IPSec VPN traffic that initiated from local VPN client to pass through to Internet. If you want to disable such function, just change the setting to disable it.

11. **WAN IP alias**: The device supports 2 WAN IP address, one is for primary connection that provides users/devices in the LAN to access Internet; the other is a virtual connection that let remote user to manage this device.

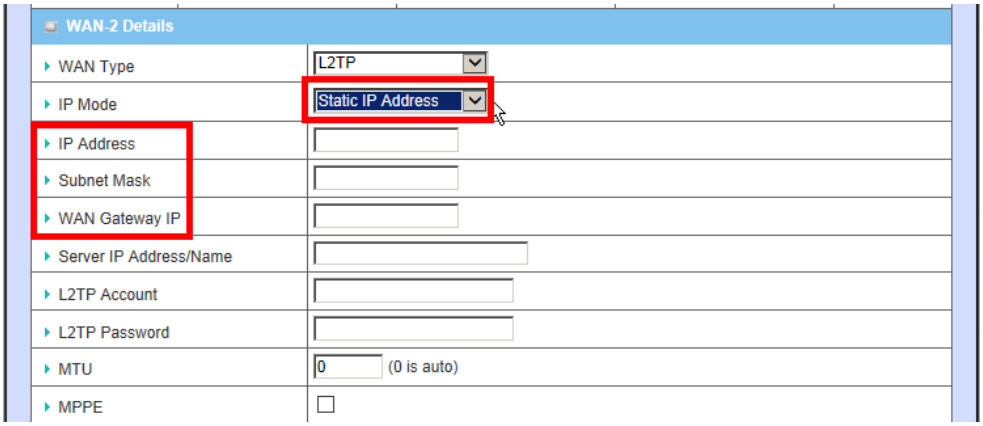
    Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

1.1.2.2.5 L2TP

Choose L2TP (Layer 2 Tunneling Protocol) if your ISP used a L2TP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.



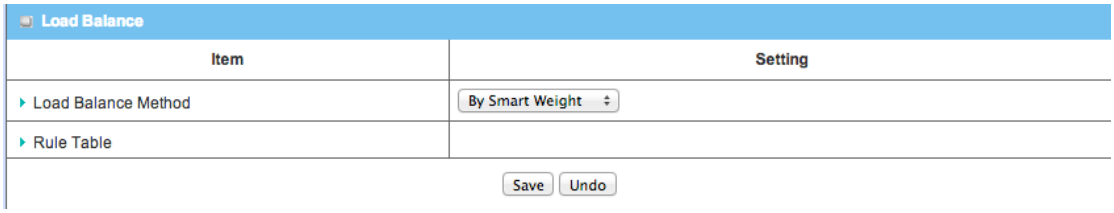
1. **WAN Type:** Choose “L2TP” from the drop list
2. **IP Mode**: Please check the IP mode your ISP assigned, and select “Static IP Address” or “Dynamic IP Address” accordingly. If you select “Static IP Address” option, you have to specify additional “IP Address”, “Subnet Mask”, and “WAN Gateway IP” settings provided by your ISP.



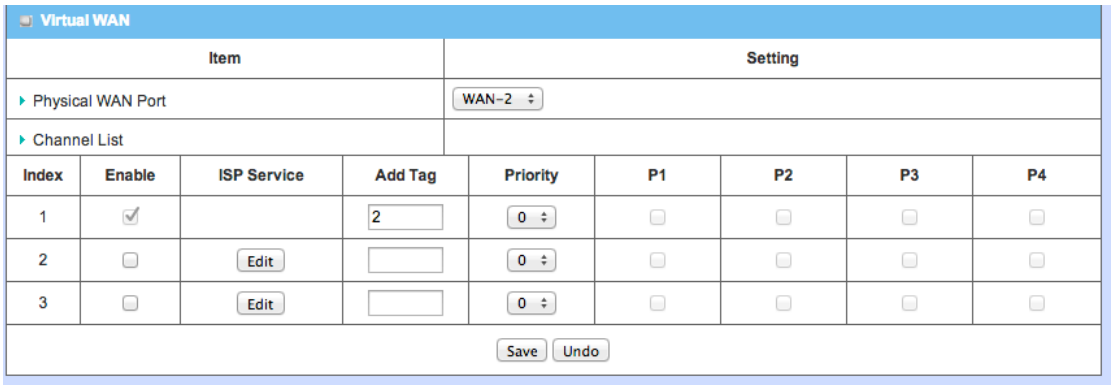
3. **Server IP Address / Name**: The IP address of the PPTP server and designated Gateway provided by your ISP.
4. **L2TP Account** and **Password:** The account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it blank.
5. **MTU :** Most ISP offers MTU value to users. The default MTU value is 0 (auto)
6. **MPPE (Microsoft Point-to-Point Encryption):** Enable or disable this function.
7. **Multicast:** Enable or disable multicast traffics from the internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
8. **IGMP Snooping:** Enable or disable IGMP snooping function. If you enable the IGMP snooping function, this device will detect all IGMP messages exchanged on the link and will maintain a table indicating for each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.
9. **Disable PPTP / L2TP / IPSec Passthrough:** By default, the device allows the PPTP / L2TP / IPSec VPN traffic that initiated from local VPN client to pass through to Internet. If you want to disable such function, just change the setting to disable it.
10. **WAN IP alias**: The device supports 2 WAN IP address, one is for primary connection that provides users/devices in the LAN to access Internet; the other is a virtual connection that let remote user to manage this device.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

1.1.3 Load Balance

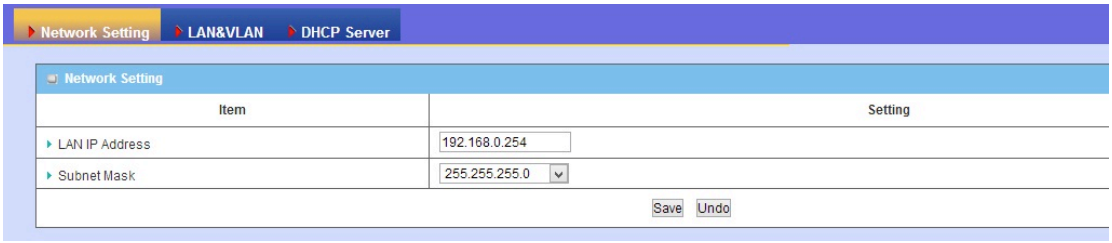


1.1.4 Virtual WAN



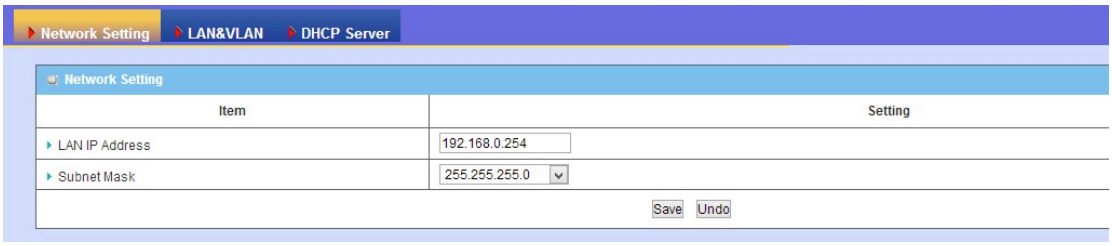
1.2 LAN & VLAN Setup

This device is equipped with four fast Ethernet LAN ports as to connect your local devices via Ethernet cables. Besides, VLAN function is provided to organize your local networks.



1.2.1 Network Setting

Please follow the following instructions to do IPv4 Network Setup.



1. **LAN IP Address:** The local IP address of this device. The computer on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary.
2. **Subnet Mask:** Input your Subnet mask. (All devices in the network must have the same subnet mask.) The default subnet mask is 255.255.255.0

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

1.2.2 LAN & VLAN

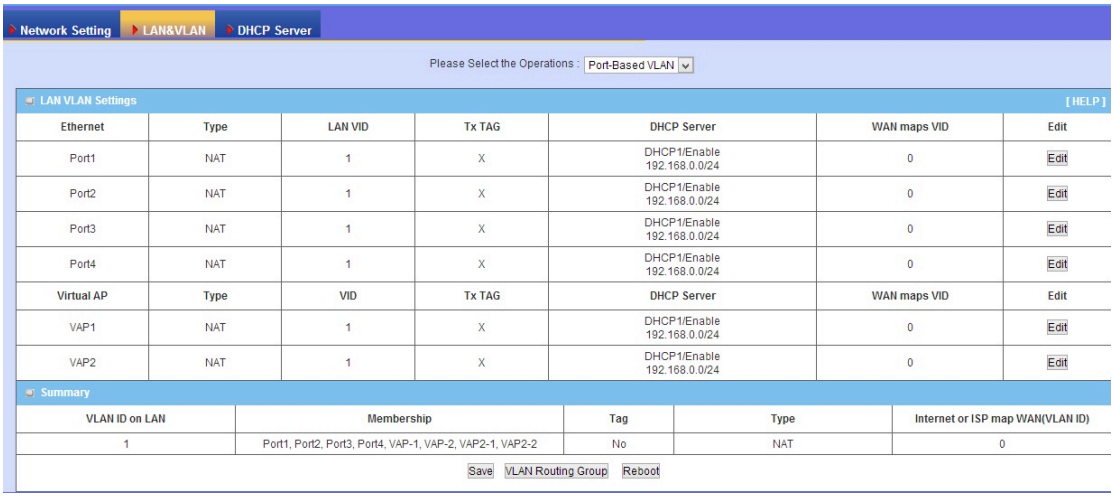
This section provides a brief description of VLANs and explains how to create, and modify virtual LANs which are more commonly known as VLANs. A VLAN is a group of ports that form a logical network under a certain switch or router device. The ports of a VLAN form an independent traffic domain in which the traffic generated by the nodes remains within the VLAN.

The VLAN function allows you to divide local network into different **“**virtual LANs”. In some cases, ISP may need router to support “VLAN tag” for certain kinds of services (e.g. IPTV) to work properly.

This Device supports port-based VLAN and tag-based VLAN. You can select either one operation mode and then configure according to your network configuration.

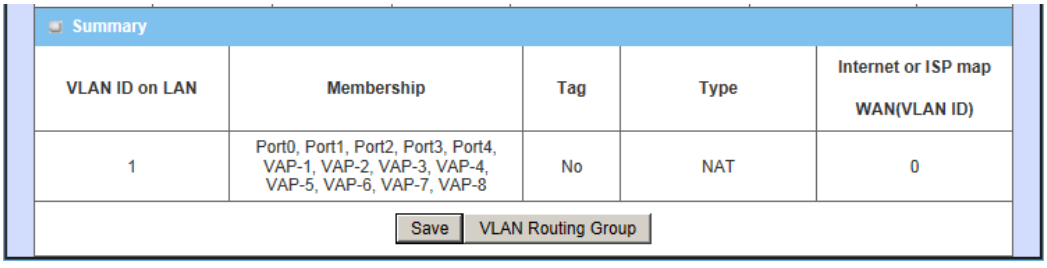
1.2.2.1 Port-Based VLAN

A port-based VLAN is a group of ports on a Ethernet switch or router that form a logical Ethernet segment. There are four LAN ports and up to eight virtual APs in this device, so you can have various VLAN configurations to organization the available LAN ports and virtual APs if required.



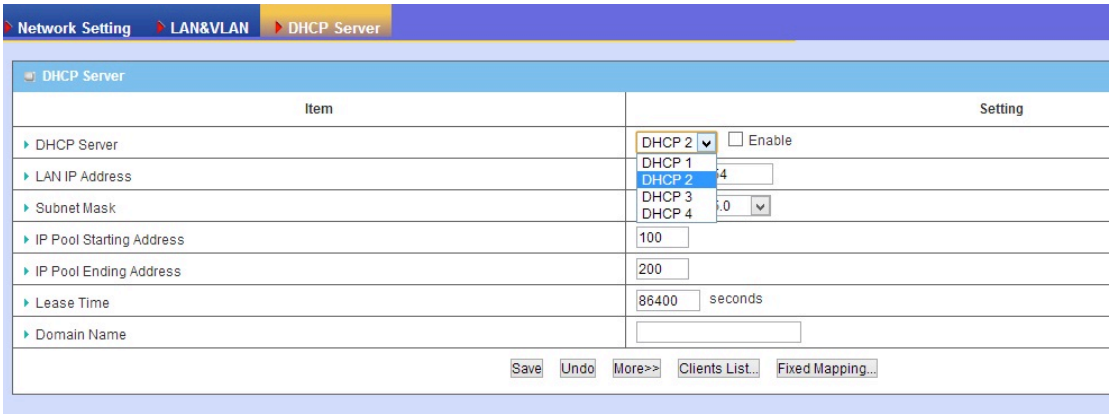
By default, all the 4 LAN ports and 8 virtual APs belong to one VLAN, and this VLAN is a NAT type network, all the local device IP addresses are allocated by DHCP server 1. If you want to divide them into different VLANs, click on the “Edit” button related to each port.

1. **Type**: Select “NAT” or “Bridge” to identify if the packets are directly bridged to the WAN port or processed by NAT mechanism.
2. **LAN VID**: Specify a VLAN identifier for this port. The ports with the same VID are in the same VLAN.
3. **Tx TAG**: If ISP requests a **“VLAN Tag”** with your outgoing data, please check the checkbox of “Tx TAG”.
4. **DHCP Server**: Specify a DHCP server for the configuring VLAN. This device provides up to 4 DHCP servers to serve the DHCP requests from different VLANs.
5. **WAN Maps VID**: The VLAN Tag ID that come from the ISP service. For NAT type VLAN, no WAN VLAN tag is allowed, and the value is forced to “0”; For Bridge type VLAN, You have to specify the VLAN Tag value that is provided by your ISP.



Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

1.2.3 DHCP server



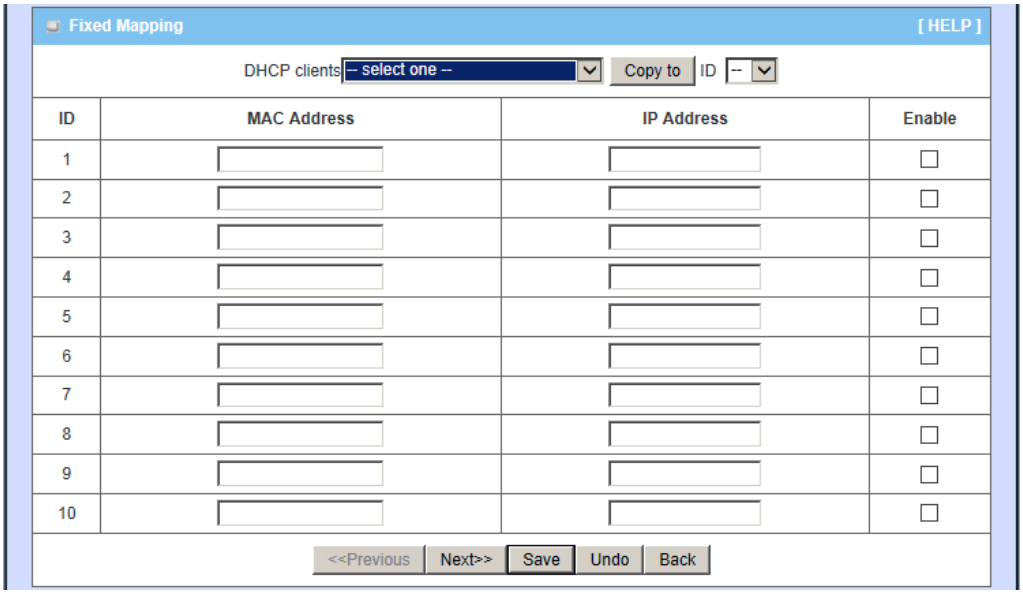
1. **DHCP Server:** Choose DHCP Server to **Enable**. If you enable the DHCP Server function, the following settings will be effective. This device provides up to 4 DHCP servers to serve the DHCP requests from different VLANs.
2. **IP Pool Starting/Ending Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool.
3. **Lease Time:** DHCP lease time to the DHCP client.
4. **Domain Name:** Optional, this information will be passed to the clients.

Press **"More>>"** and you can find more settings.

5. **Primary DNS/Secondary DNS:** Optional. This feature allows you to assign a DNS Servers
6. **Primary WINS/Secondary WINS:** Optional. This feature allows you to assign a WINS Servers
7. **Gateway:** Optional. Gateway Address would be the IP address of an alternate Gateway. This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.

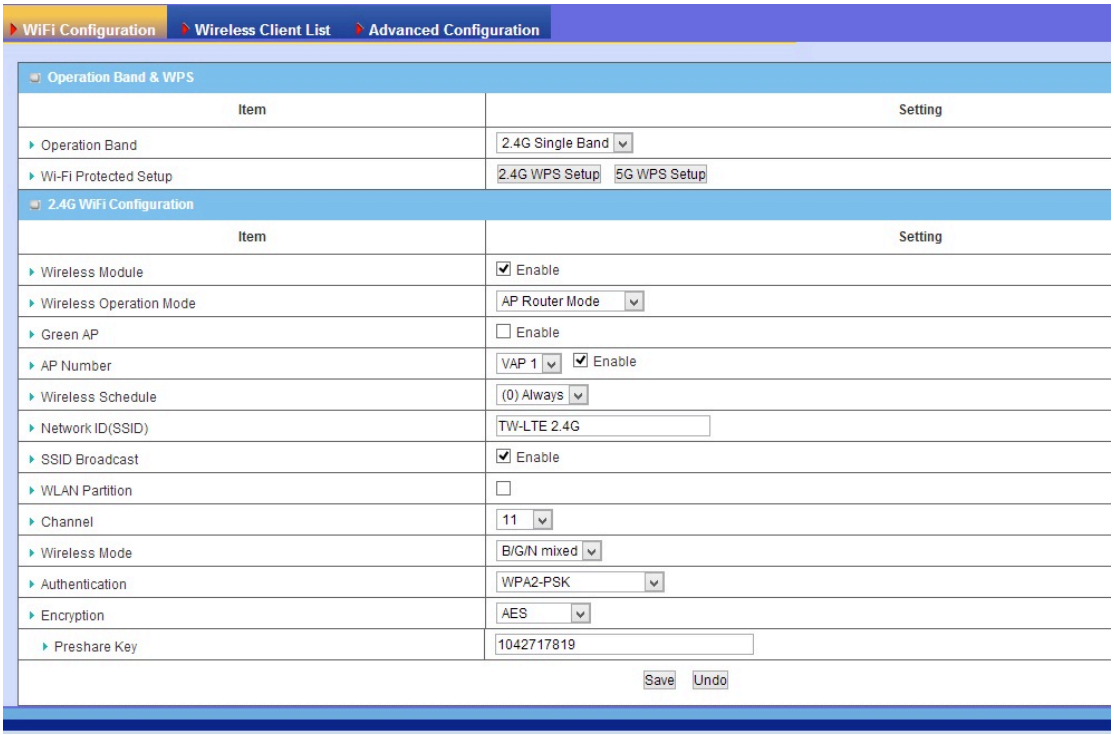
Press **"Clients List"** and the list of DHCP clients will be shown consequently.

Press **"Fixed Mapping"** and you can specify a certain IP address for designated local device (MAC address), so that the DHCP Server will reserve the special IP for designated devices.



1.3 Wireless Setup

Wireless settings allow you to set the WLAN configuration items. When the wireless configuration is done your wireles LAN is ready to support your local wireless devices such as your laptop PC, wireless printer and some portable wireless devices.

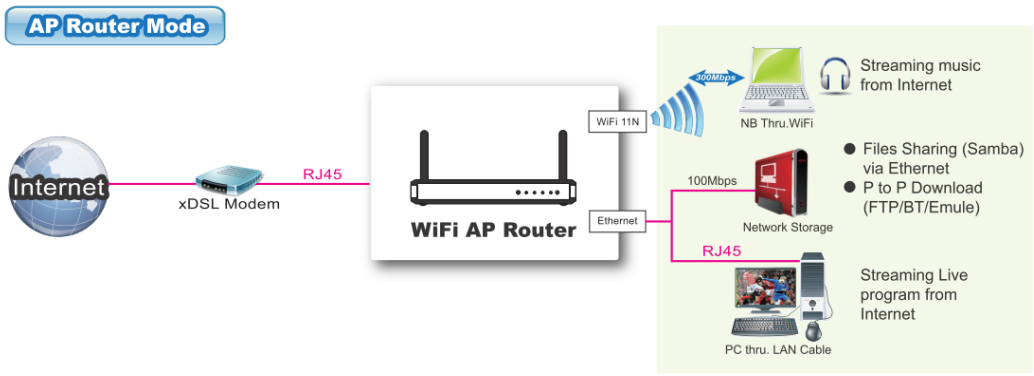


1.3.1 Wifi Configuration

There are several wireless operation modes provided by this device. They are: "**AP Router Mode**", "**AP Only Mode**", "**WDS Hybrid Mode**", "**WDS Only Mode**", and "**Universal Repeater Mode**". You can choose the expected mode from the list on 2.4GHz /5GHz separately.

1.3.1.1 AP Router mode

This mode allows you to get your wired and wireless devices connected with NAT.



Operation Band & WPS	
Item	Setting
Operation Band	2.4G Single Band
Wi-Fi Protected Setup	2.4G WPS Setup 5G WPS Setup
2.4G WiFi Configuration	
Item	Setting
Wireless Module	☑ Enable
Wireless Operation Mode	AP Router Mode
Green AP	☐ Enable
AP Number	VAP 1 ☑ Enable
Wireless Schedule	(0) Always
Network ID(SSID)	TW-LTE 2.4G
SSID Broadcast	☑ Enable
WLAN Partition	☐
Channel	11
Wireless Mode	B/G/N mixed
Authentication	WPA2-PSK
Encryption	AES
Preshare Key	1042717819
	Save Undo

1. **Wireless Module:** Enable the wireless function.
2. **Wireless Operation Mode:** Choose "**AP Router Mode**" from the list.

3. **Green AP:** Enable the Green AP function to reduce the power consumption when there is no wireless traffics.
4. **AP Number:** This device supports up to 8 SSIDs for you to manage your wireless network. You can select AP1 ~ AP8 and configure each wireless network if it is required.
5. **Wireless Schedule:** The wireless radio can be turn off according to the schedule rule you specified. By default, the wireless radio is always turned on when the wireless module is enabled.
6. **Network ID (SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is “default”)
7. **SSID Broadcast:** The router will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, the wireless clients can not find the device from beacons.
8. **WLAN Partition:** You can check the WLAN Partition function to separate the wireless clients. The wireless clients can’t communicate each other, but they can access the internet and other Ethernet LAN devices.
9. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.
10. **Wireless Mode:** Choose “B/G mixed”, “B only”, “G only”, “N only”, “G/N mixed” or “B/G/N mixed”. The factory default setting is “B/G/N mixed”.
11. **Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.
    - **Open**

      Open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration.
    - **Shared**

      Shared key authentication relies on the fact that both stations taking part in the authentication process have the same "shared" key or passphrase. The shared key is manually set on both the client station and the AP/router. Three types of shared key authentication are available today for home or small office WLAN

environments.

- **Auto**

  The AP will Select the Open or Shared by the client's request automatically.

- **WPA-PSK**

  Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits, or 8 to 63 ASCII characters as the pre-share key.

- **WPA**

  Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address, and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server.

- **WPA2-PSK**

  Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits, or 8 to 63 ASCII characters as the pre-share key.

- **WPA2**

  Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address, and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server.

- **WPA-PSK/WPA2-PSK**

  Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits, or 8 to 63 ASCII characters as the pre-share key.

- **WPA/WPA2**

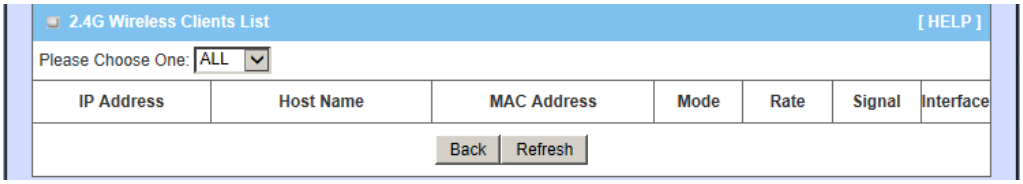
  Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address, and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

Press **"WPS Setup"**, you can configure and enable the easy setup feature WPS (Wi-Fi Protection Setup) for your wireless network.

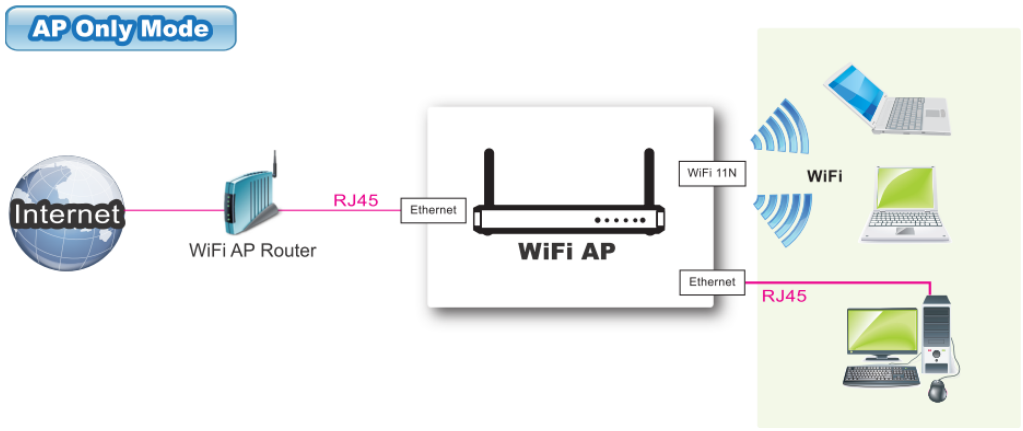
1. **WPS:** You can enable this function by selecting “Enable”. WPS offers a safe and easy way to allow the wireless clients connected to your wireless network.
2. **AP PIN**: You can press Generate New Pin to get an AP PIN.
3. **Config Mode**: Select your configuration Mode from “Registrar” or “Enrollee”. For a AP router or AP, it should be in “Registrar” mode, so that other wireless clients in “Enrollee” mode can connect to the discovered “Registrar”.
4. **Config Status**: It shows the status of your configuration.
5. **Config Method**: You can select the Configuration Method here from “Pin Code” or “Push Button”.
6. **WPS status**: According to your setting, the status will show “Start Process” or “No used”.

Press **“Wireless Clients List”**, and the list of connected wireless clients will be shown consequently.



1.3.1.2 AP Only mode

When acting as an access point, this device connects all the wireless stations to a wired network and the WAN Port is disabled consequently.



WiFi Configuration | Wireless Client List | Advanced Configuration

Operation Band & WPS

Item	
Operation Band	2.4G Single Band
Wi-Fi Protected Setup	2.4G WPS Setup 5G WPS Setup

2.4G WiFi Configuration

Item	
Wireless Module	☑ Enable
Wireless Operation Mode	AP Only Mode
Green AP	☐ Enable
AP Number	VAP 1 ☑ Enable
Wireless Schedule	(0) Always
Network ID(SSID)	TW-LTE 2.4G
SSID Broadcast	☑ Enable
Channel	11
Wireless Mode	B/G/N mixed
Authentication	WPA2-PSK
Encryption	AES
Preshare Key	1042717819

Save Undo

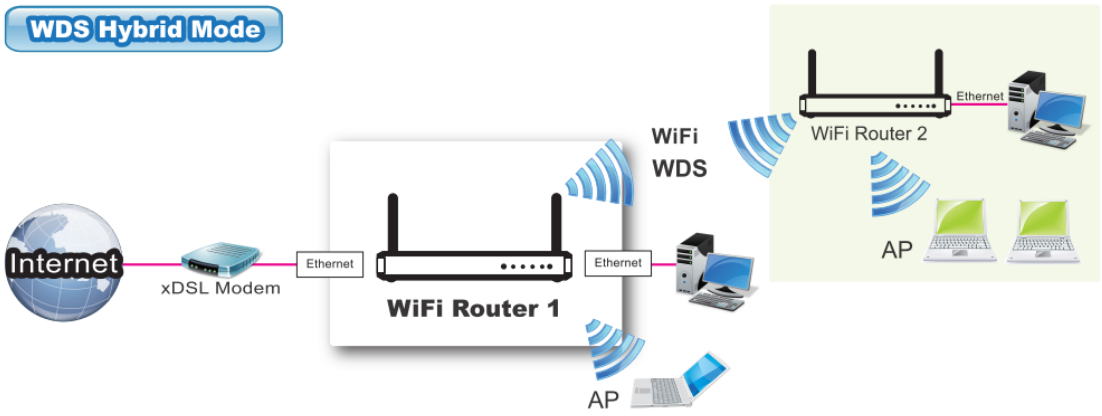
1. **Wireless Module:** Enable the wireless function.
2. **Wireless Operation Mode:** Choose "**AP Only Mode**" from the list.
3. **Green AP:** Enable the Green AP function to reduce the power consumption when there is no wireless traffics.
4. **AP Number:** This device supports up to 8 SSIDs for you to manage your wireless network. You can select AP1 ~ AP8 and configure each wireless network if it is required.
5. **Wireless Schedule:** The wireless radio can be turn off according to the schedule rule you specified. By default, the wireless radio is always turned on when the wireless module is enabled.

6. **Network ID (SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is “default”)
7. **SSID Broadcast:** The device will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, the wireless clients can not find the device from beacons.
8. **WLAN Partition:** You can check the WLAN Partition function to separate the wireless clients. The wireless clients can’t communicate each other, but they can access the internet and other Ethernet LAN devices.
9. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.
10. **Wireless Mode:** Choose “B/G mixed”, “B only”, “G only”, “N only”, “G/N mixed” or “B/G/N mixed”. The factory default setting is “B/G/N mixed”.
11. **Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.

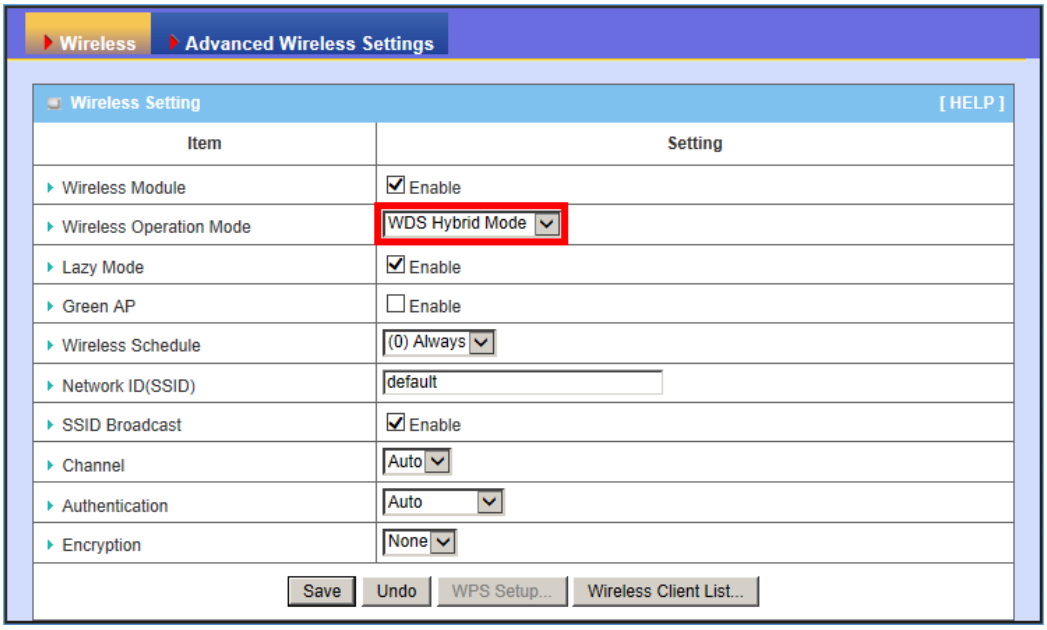
Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

1.3.1.3 WDS Hybrid mode

While acting as a wireless Bridge, Wireless Router 1 and Wireless Router 2 can communicate with each other through wireless interface (with WDS). Thus All Stations can communicate each other and are able to access Internet if Wireless Router 1 has the Internet connection



.



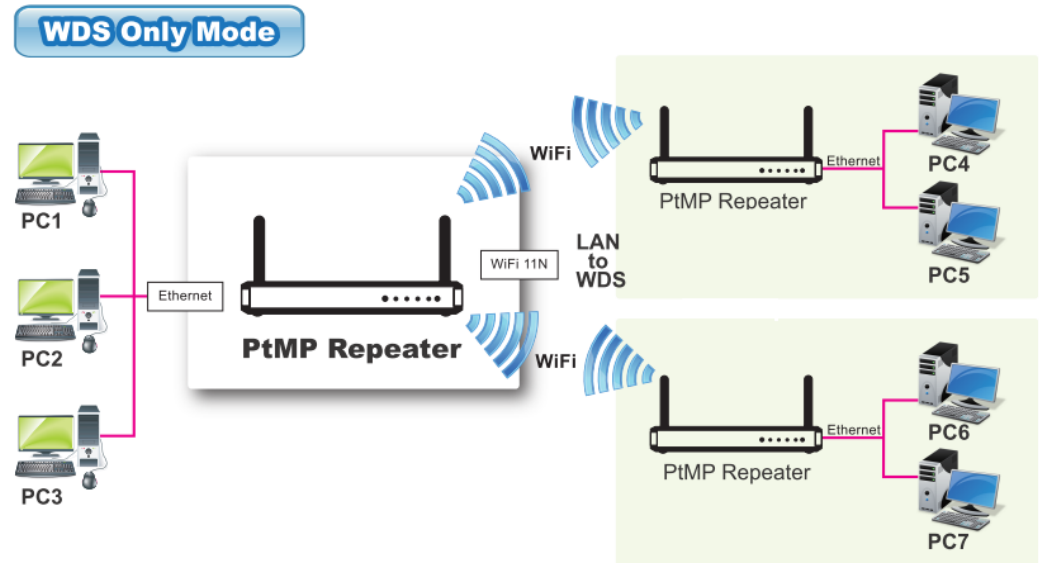
1. **Lazy Mode:** This device support the Lazy Mode to automatically learn the MAC address of WDS peers, you don't have to input other peer AP's MAC address. However, not all the APs can be set to enable the Lazy mode simultaneously; at least there must be one AP with all the WDS peers' MAC address filled.
2. **Green AP:** Enable the Green AP function to reduce the power consumption when there is no wireless traffics.
3. **Wireless Schedule:** The wireless radio can be turn off according to the schedule rule you specified. By default, the wireless radio is always turned on when the wireless module is enabled.
4. **Network ID (SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is "default")
5. **SSID Broadcast:** The device will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as "Disable", the wireless clients can not find the device from beacons.
6. **WLAN Partition:** You can check the WLAN Partition function to separate the wireless clients. The wireless clients can't communicate each other, but they can access the internet and other Ethernet LAN devices.
7. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.
8. **Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.

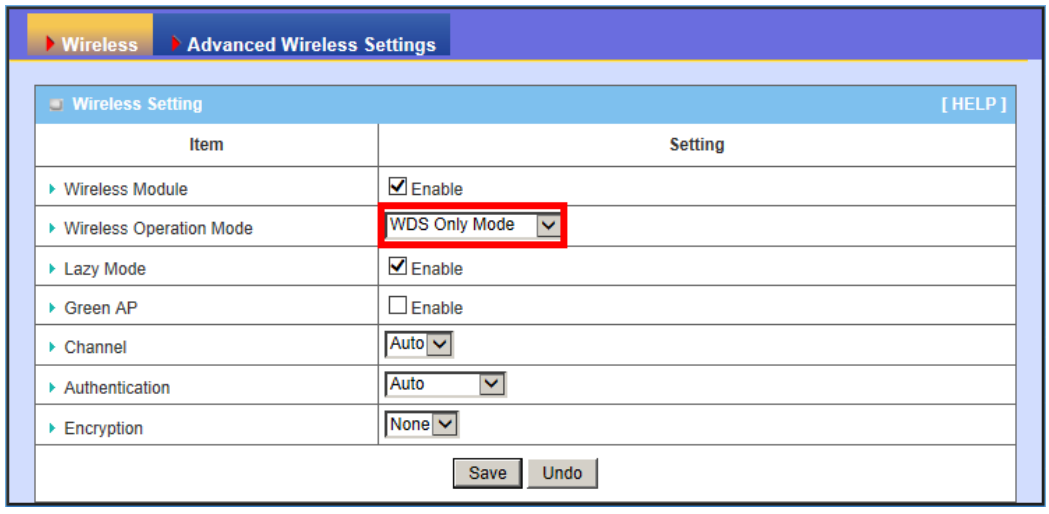
9. **Remote AP MAC 1 ~ Remote AP MAC 4:** If you do not enable the Lazy mode, you have to enter the wireless MAC address for each WDS peer one by one.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

1.3.1.4 WDS Only mode

WDS (Wireless Distributed System) function let this access point acts as a wireless LAN access point and repeater at the same time. Users can use this feature to build up a large wireless network in a large space like airports, hotels and schools …etc.





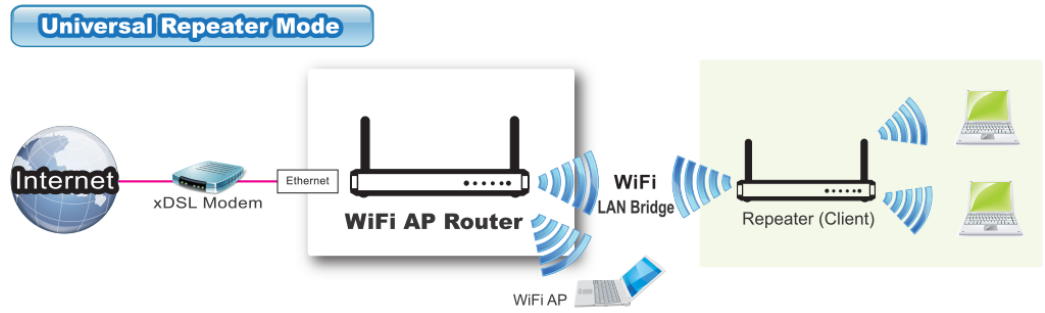
1. **Lazy Mode:** This device support the Lazy Mode to automatically learn the MAC address of WDS peers, you don’t have to input other peer AP's MAC address. However, not all the APs can be set to enable the Lazy mode simultaneously; at least there must be one AP with all the WDS peers’ MAC address filled.
2. **Green AP:** Enable the Green AP function to reduce the power consumption when there is no wireless traffics.

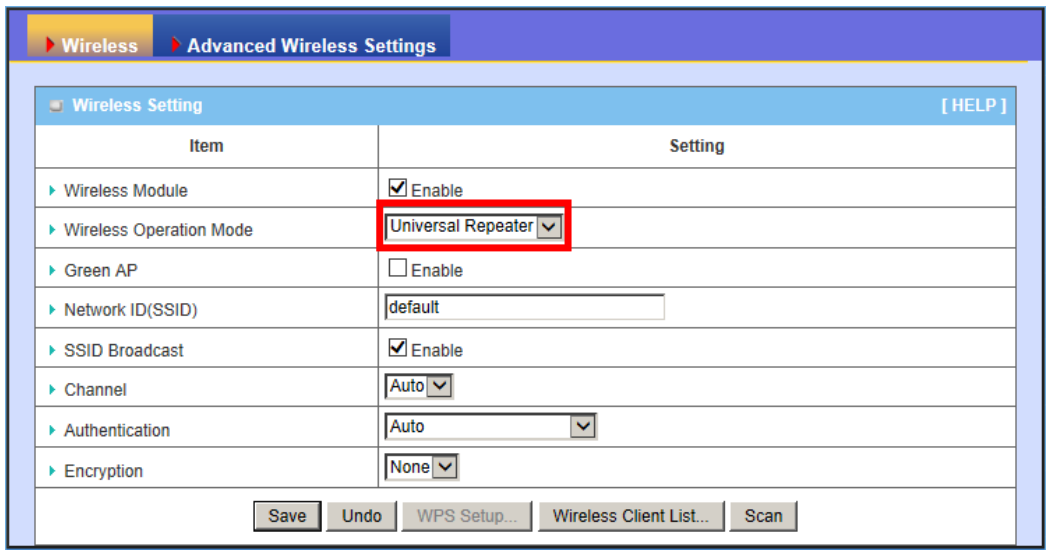
3. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.
4. **Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.
5. **Remote AP MAC 1 ~ Remote AP MAC 4:** If you do not enable the Lazy mode, you have to enter the wireless MAC address for each WDS peer one by one.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

1.3.1.5 Universal repeater mode

Universal Repeater is a technology used to extend wireless coverage. It provides the function to act as Adapter (Client) and AP at the same time and can use this function to connect to a Root AP and use AP (SSID name must be the same as that of Root AP) function to service all wireless stations within its coverage. All the stations within the coverage of this access point can be bridged to the Root AP.





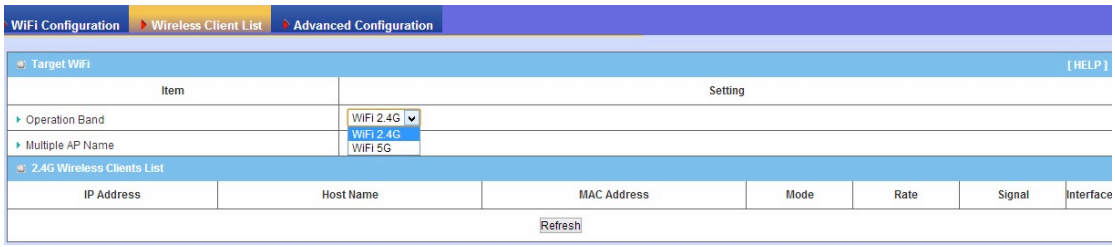
1. **Green AP:** Enable the Green AP function to reduce the power consumption when there is no wireless traffics.
2. **Network ID (SSID):** Network ID is used for identifying the Wireless LAN (WLAN).

Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is “default”)

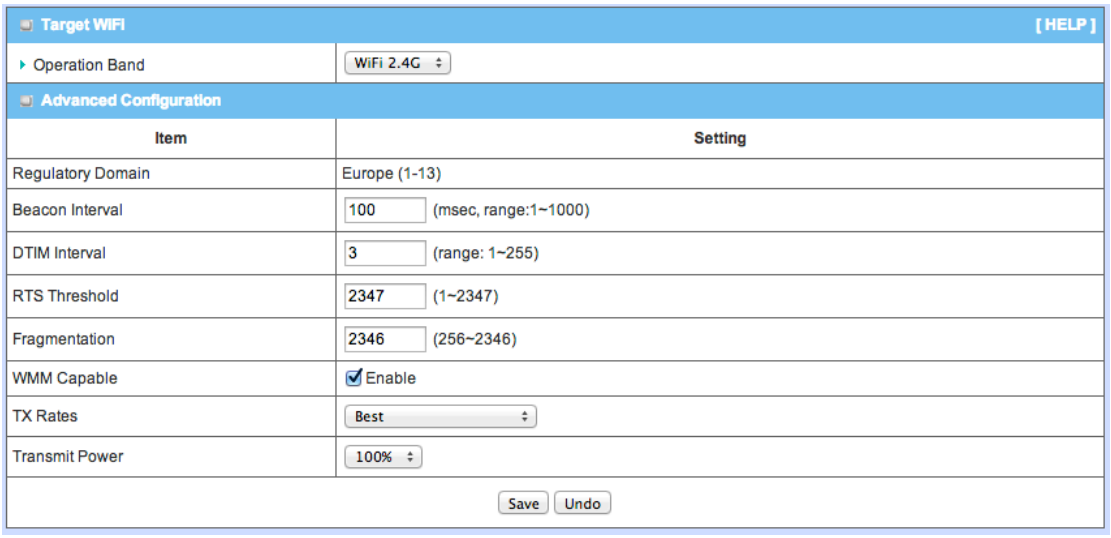
3. **SSID Broadcast:** The device will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, the wireless clients can not find the device from beacons.
4. **WLAN Partition:** You can check the WLAN Partition function to separate the wireless clients. The wireless clients can’t communicate each other, but they can access the internet and other Ethernet LAN devices.
5. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.
6. **Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

1.3.2 Wireless Client List



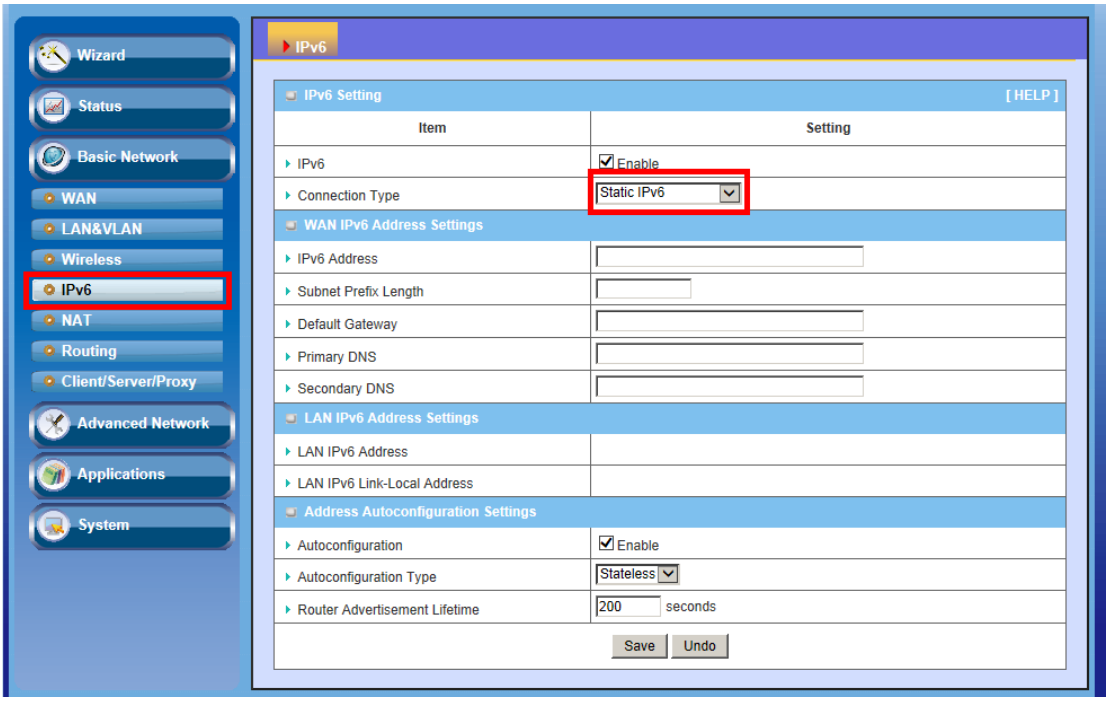
1.3.3 Advanced Configuration



1.4 IPv6 Setup

The growth of the Internet has created a need for more addresses than are possible with IPv4. **IPv6** (**Internet Protocol version 6**) is a version of the Internet Protocol (IP) intended to succeed IPv4, which is the protocol currently used to direct almost all Internet traffic. IPv6 also implements additional features not present in IPv4. It simplifies aspects of address assignment (stateless address auto-configuration), network renumbering and router announcements when changing Internet connectivity providers. This router supports various types of IPv6 connection (Static IPv6 / DHCPv6 / PPPoE / 6 to 4 / IPv6 in IPv4 tunnel). **Please ask your ISP of what type of IPv6 is supported before you proceed with IPv6 setup.**

1.4.1 Static IPv6



When “Static IPv6” is selected you need to do the following settings:

1. WAN IPv6 address settings:

A. **IPv6 address:** Enter the IPv6 address here; IPv6 addresses have a size of 128 bits. Therefore, IPv6 has a vastly enlarged address space compared to IPv4.

B. **Subnet Prefix Length:** Enter the Prefix length of the Subnet Mask here; The subnet mask was the forerunner of the modern IP address prefix length. For example a subnet mask of 255.255.255.0 conveys exactly the same information as a prefix length of /24, a subnet mask of 255.255.255.240 is equivalent to a prefix length of /28.

C. **Default Gateway:** Enter the Default Gateway address here; A default gateway is the node on the computer network that the network software uses when an IP address does not match any other routes in the routing table.

D. **Primary / Secondary DNS:** You may select to obtain DNS server address automatically or use following DNS address. You may add IPv6 address Primary DNS address and secondary DNS address.

2. LAN IPv6 address settings: Please enter “LAN IPv6 address” and ignore the “LAN IPv6 Link-Local address”.

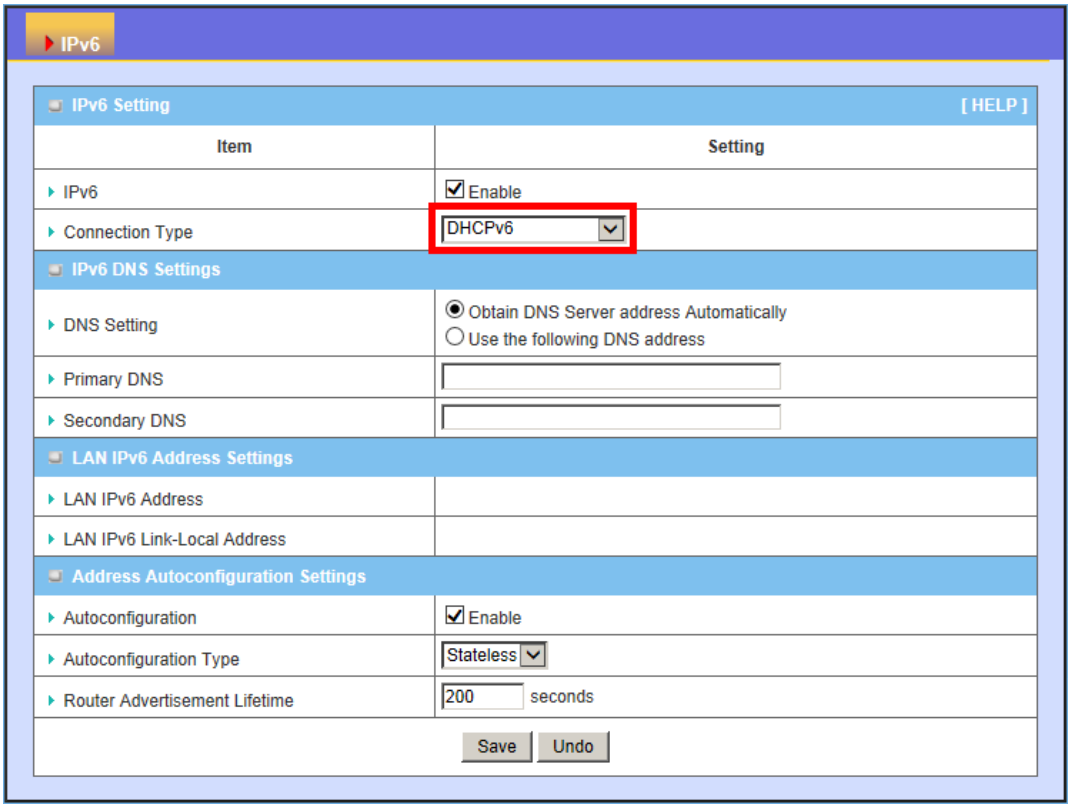
3. Address auto configuration settings:

A. **Auto-configuration:** Disable or enable this auto configuration setting.

B. **Auto-configuration type:** You may set stateless or stateful (Dynamic IPv6).

C. **Router advertisement Lifetime:** You can set the time for the period that the router send (broadcast) its router advertisement. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address(es) of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if and only if no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

1.4.2 DHCP v6



When “DHCP v6” is selected you need to do the following settings:

1. **IPv6 DNS (WAN IPv6 address) settings:** You may select to obtain DNS server address automatically or use following DNS address. You may add IPv6 address

Primary DNS address and secondary DNS address.

2. **LAN IPv6 address settings**: Please enter “LAN IPv6 address” and ignore the “LAN IPv6 Link-Local address”.

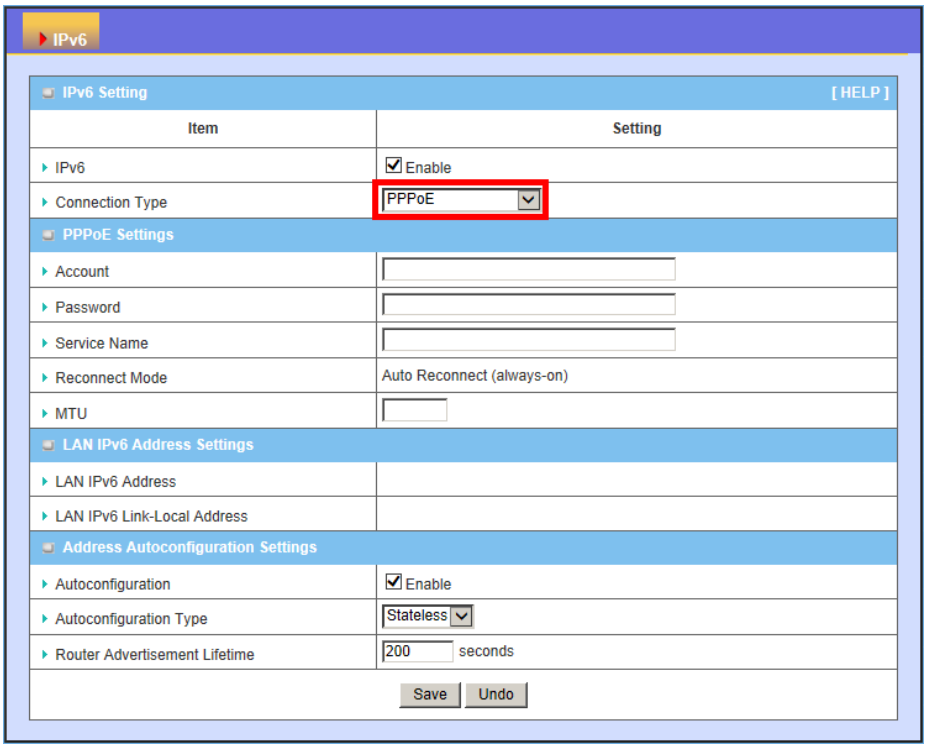
3. **Address auto configuration settings:**

   A. **Auto-configuration:** Disable or enable this auto configuration setting.

   B. **Auto-configuration type:** You may set stateless or stateful (Dynamic IPv6).

   C. **Router advertisement Lifetime:** You can set the time for the period that the router send (broadcast) its router advertisement. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address(es) of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if and only if no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

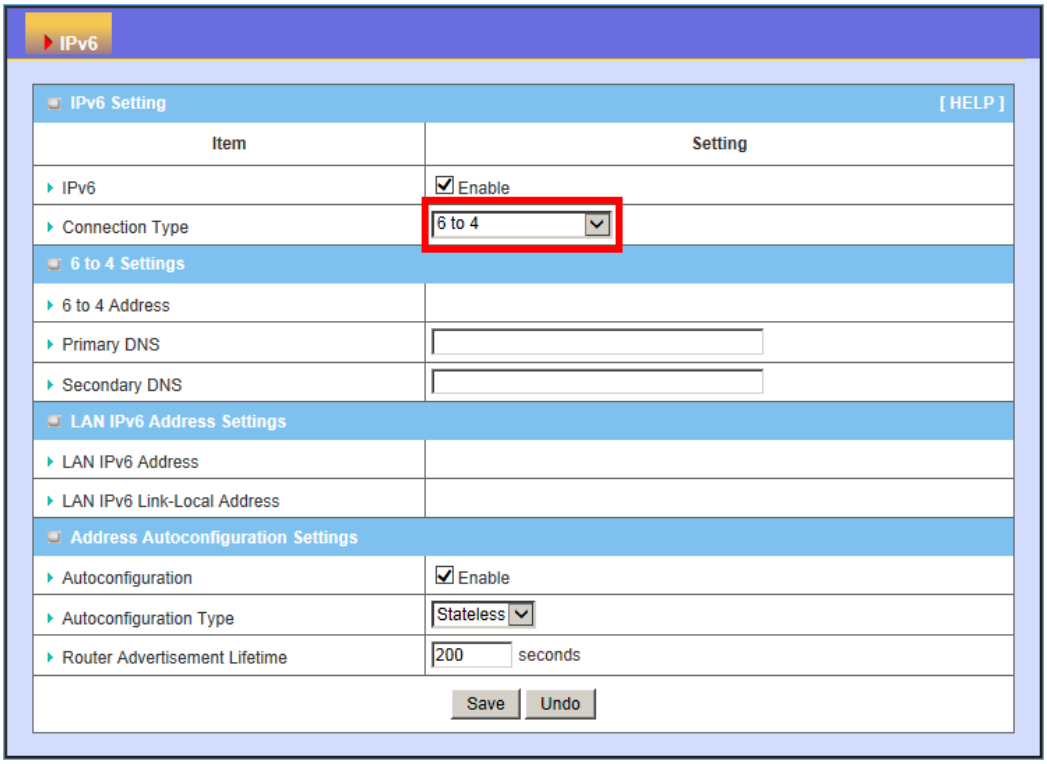
1.4.3 PPPoE



When “PPPoE” is selected you need to do the following settings:

1. **WAN IPv6 address settings:**
   A. **Username:** enter the Username that you got from your ISP
   B. **Password:** enter the Password that you got from your ISP
   C. **Service Name:** enter the Service Name that you got from your ISP
   D. **Reconnection Mode:** leave the setting as “AutoReconnect (always-on)”
   E. **Max.** Idle Time: give max. idle time that you want here
   F. **MTU (Maximum Transmission Unit):** Most ISP offers MTU value to users. The default MTU value is 0 (auto).
2. **LAN IPv6 address settings**: Please enter “LAN IPv6 address” and ignore the “LAN IPv6 Link-Local address”.
3. **Address auto configuration settings:**
   A. **Auto-configuration:** Disable or enable this auto configuration setting.
   B. **Auto-configuration type:** You may set stateless or stateful (Dynamic IPv6).
   C. **Router advertisement Lifetime:** You can set the time for the period that the router send (broadcast) its router advertisement. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address(es) of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if and only if no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

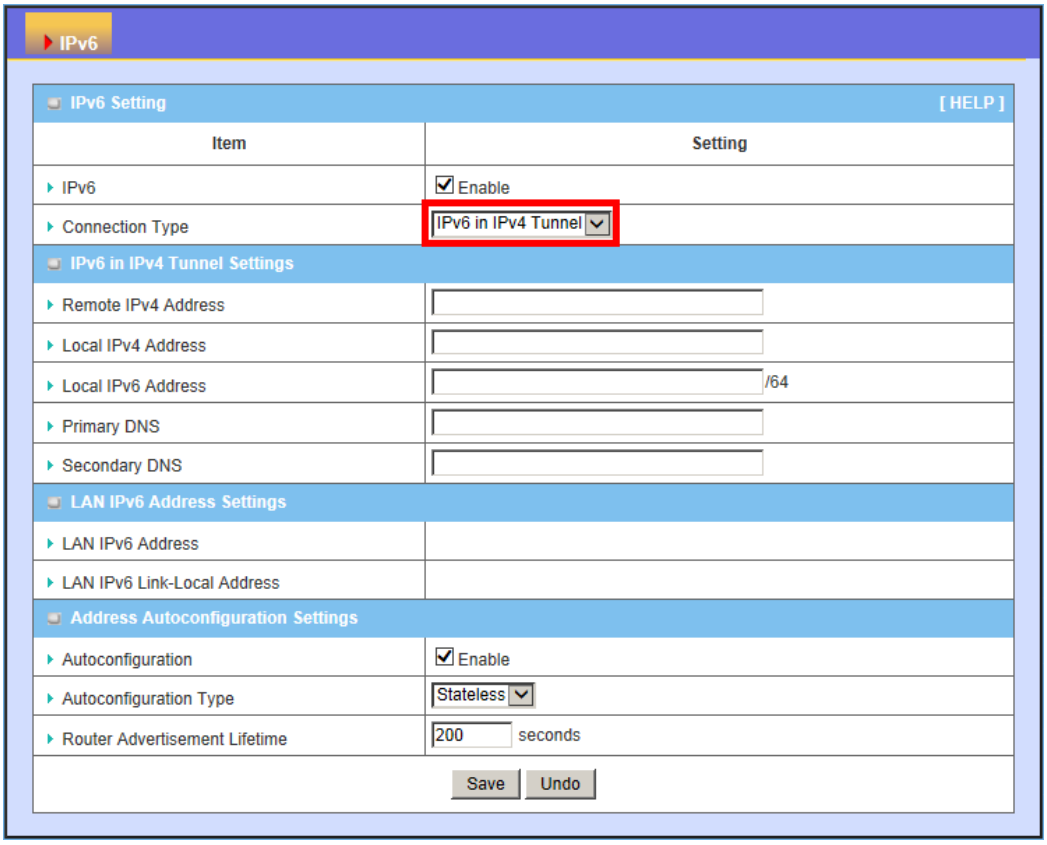
1.4.4 6 to 4



When “6 to 4 IPv6” is selected you need to do the following settings:

1. **6 to 4 Settings**: You may obtain IPv6 DNS automatically or set DNS address manually for Primary DNS address and secondary DNS address.
2. **LAN IPv6 address settings**: Enter “LAN IPv6 address” and “LAN IPv6 Link-Local address”.
3. **Address auto configuration settings:** Disable or enable this auto configuration setting. You may set stateless or stateful (Dynamic IPv6), and also check if need to send Router advertisement messages periodically.

1.4.5 IPv6 in IPv4 tunnel



When “IPv6 in IPv4 Tunnel” is selected you need to do the following settings:

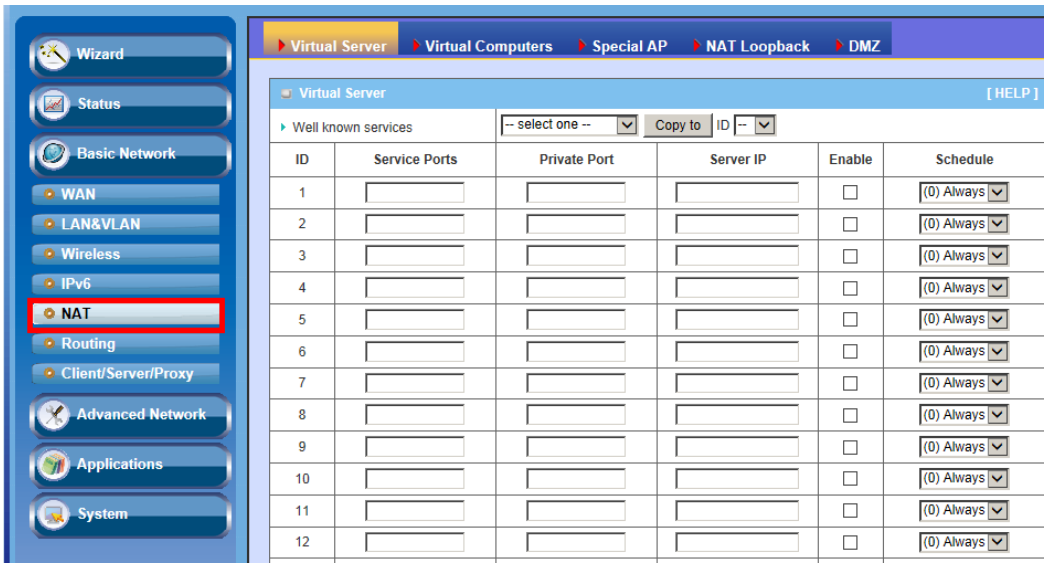
1. **IPv6 in IPv4 Tunnel Settings**: you may add remote / local IPv4 address and local IPv6 address, then set DNS address manually for Primary DNS address and secondary DNS address.
2. **LAN IPv6 address setting**: LAN IPv6 address and LAN IPv6 Link-Local address.
3. **Address auto configuration setting:** Disable or enable this auto configuration setting. You may set stateless or stateful (Dynamic IPv6), and also check if need to send Router advertisement messages periodically.

1.5 NAT

1.5.1 Virtual Server

This device's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this device are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

A virtual server is defined as a **Service Port**, and all requests to this port will be redirected to the computer specified by the **Server IP. Virtual Server** can work with **Scheduling Rules**, and give user more flexibility on Access control. For the details, please refer to **Scheduling Rule**.

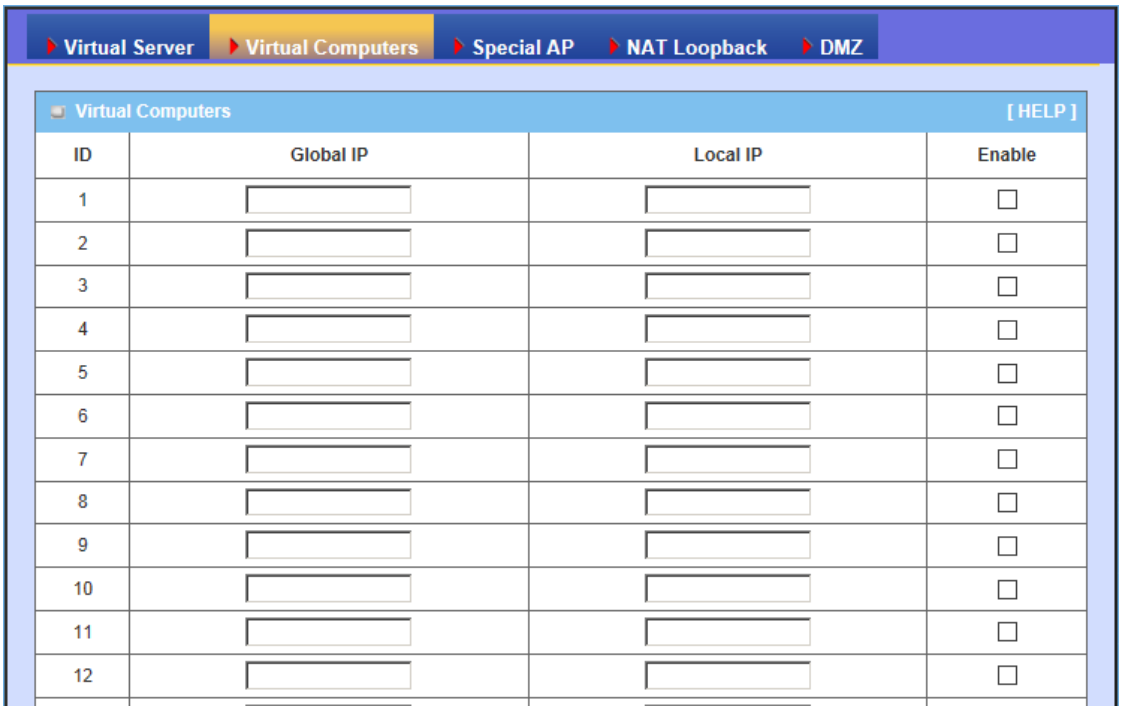


For example, if you have an **FTP server (Service port 21) at 192.168.0.1**, a **Web server1 (Service port 80) at 192.168.0.2,** a **Web server2 (Service Port 8080 and Private port 80) at 192.168.0.3,** and a **VPN server at 192.168.0.6,** then you need to specify the following virtual server mapping table

Service Port	Private Port	Server IP	Enable
21		192.168.0.1	V
80		192.168.0.2	V
8080	80	192.168.0.3	v
1723		192.168.0.6	V

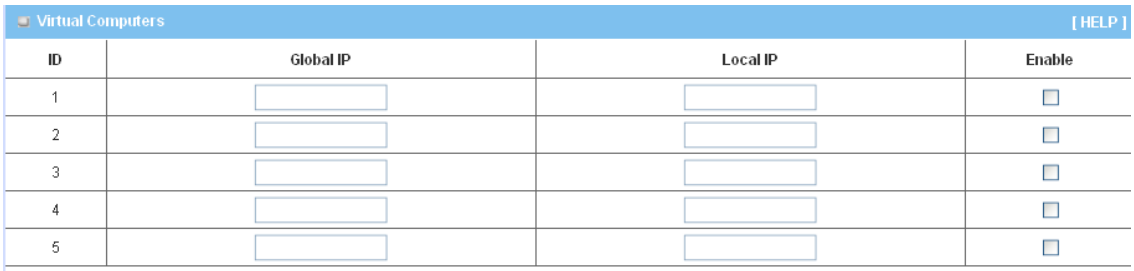
Afterwards, click on **"Save"** to store your settings or click **"Undo"** to give up the changes.

1.5.2 Virtual Computers



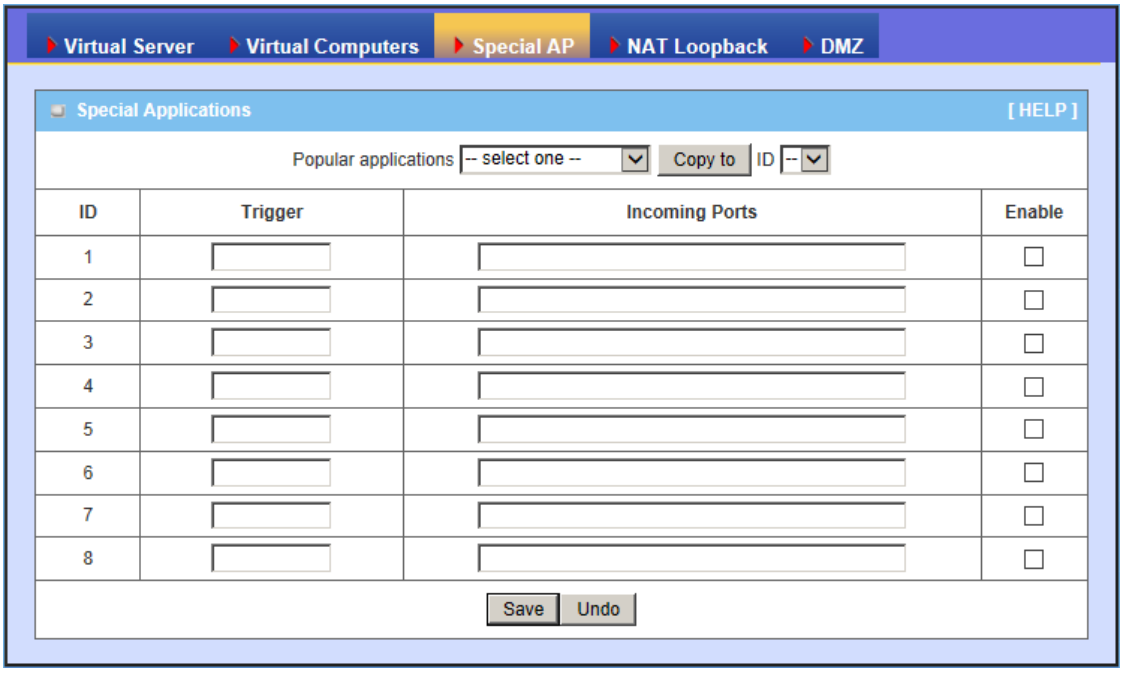
Virtual Computer enables you to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple global IP address and local IP address.

1. **Global IP**: Enter the global IP address assigned by your ISP.
2. **Local IP**: Enter the local IP address of your LAN PC corresponding to the global IP address.
3. **Enable**: Check this item to enable the Virtual Computer feature.



1.5.3 Special AP

Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. **The Special Applications** feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the DMZ host instead.

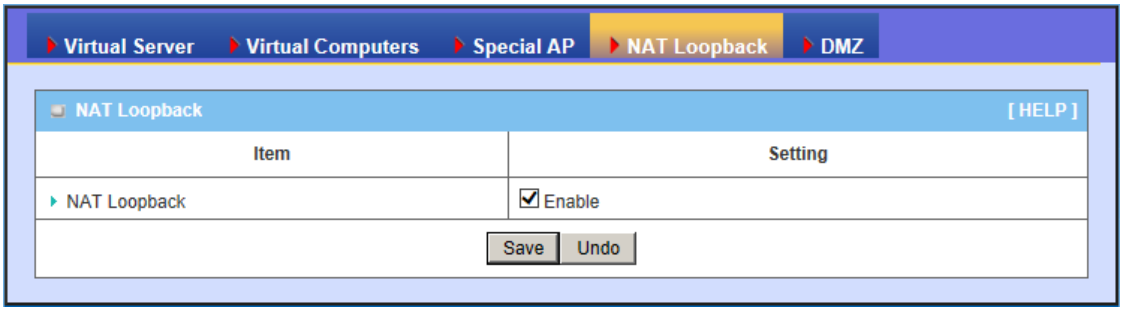


This device provides some predefined settings. Select your application and click "**Copy to"** to add the predefined setting to your list.

1. **Trigger:** The outbound port number issued by the application.
2. **Incoming Ports**: When the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.
3. **Enable**: Check this item to enable the Special AP feature.

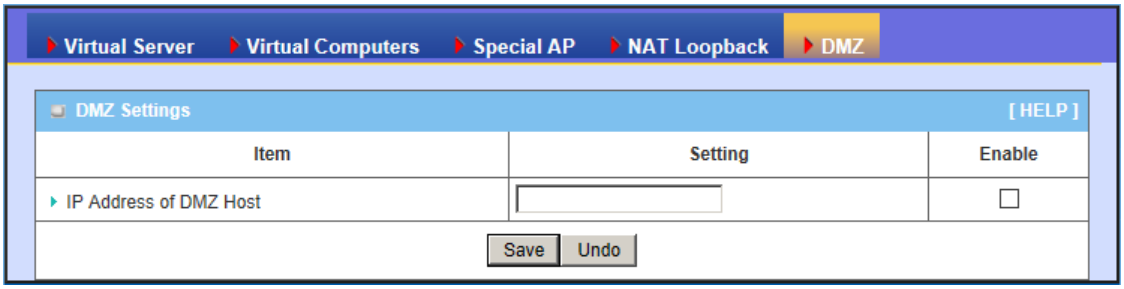
Afterwards, Click on "Save" to store your settings or click "Undo" to give up the changes.

1.5.4 NAT Loopback



Allow you to access the external IP address from inside your home or office network. This is useful when you run a server inside your network.

1.5.5 DMZ



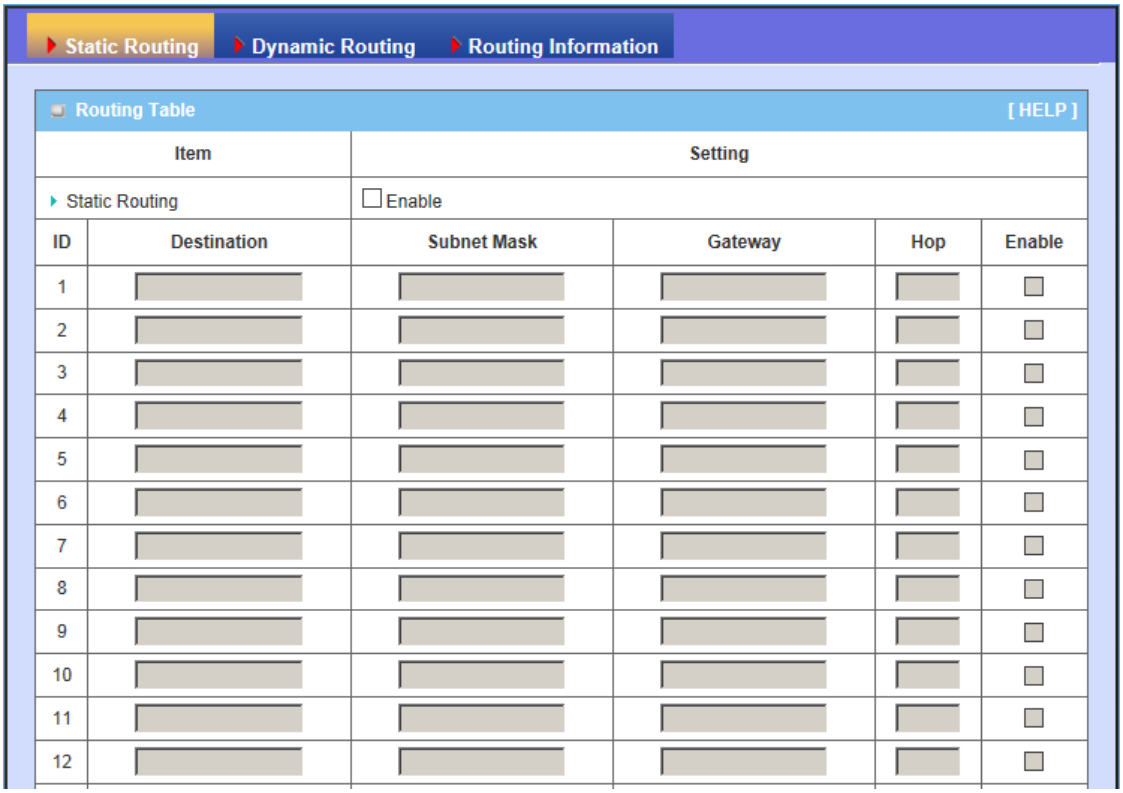
DMZ (DeMilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

NOTE: This feature should be used only when needed.

1.6 Routing Setup

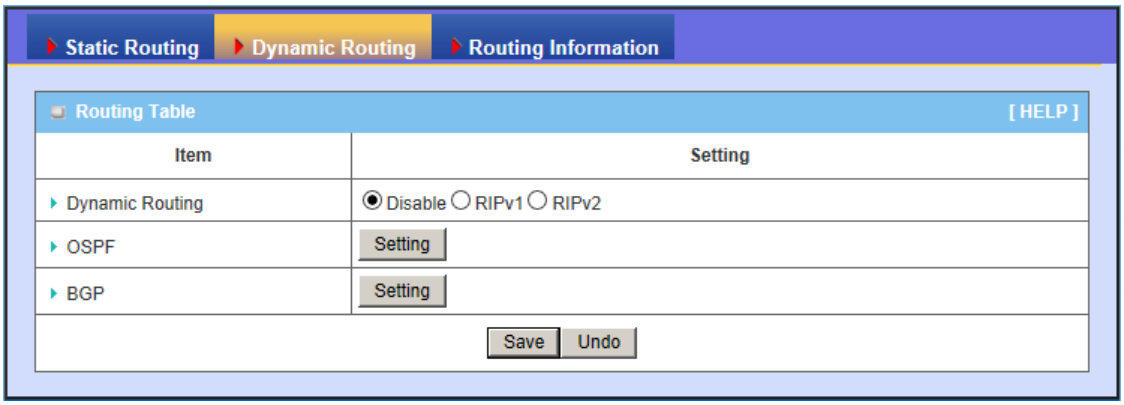
If you have more than one routers and subnets, you will need to enable routing function to allow packets to find proper routing path and allow different subnets to communicate with each other.

1.6.1 Static Routing



For static routing, you can specify up to 32 routing rules. The routing rules allow you to determine which physical interface addresses are utilized for outgoing IP data grams. You can enter the **destination IP address**, **subnet mask**, **gateway**, and **hop** for each routing rule, and then enable or disable the rule by checking or un-checking the Enable checkbox.

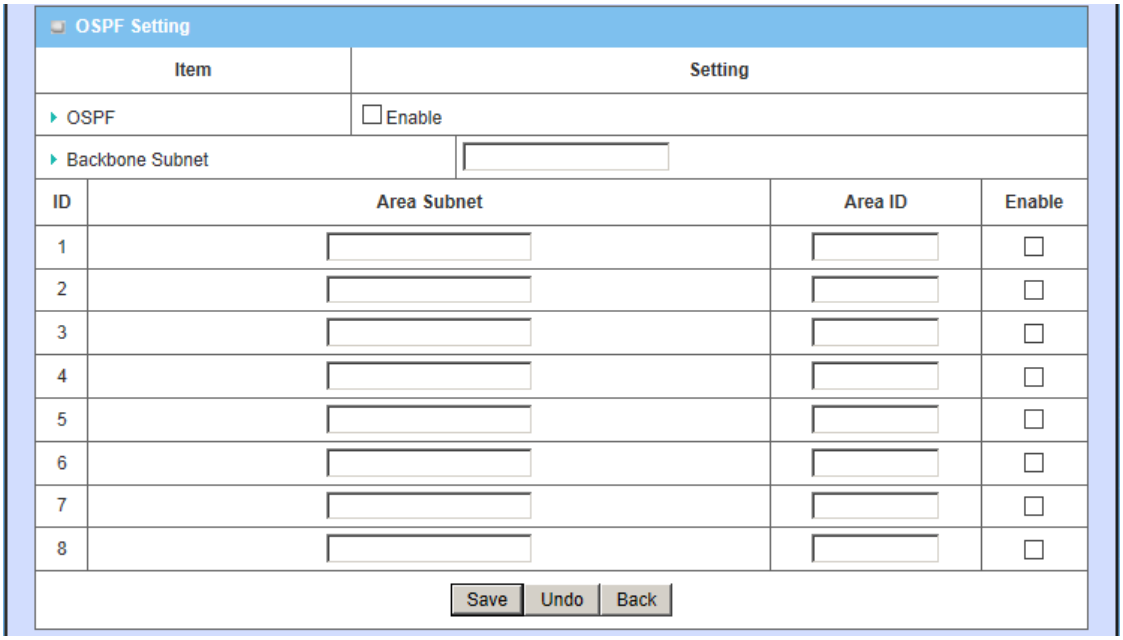
1.6.2 Dynamic Routing



1. **Dynamic Routing**: Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnets in your network. Otherwise, please select RIPv1 if you need this protocol.

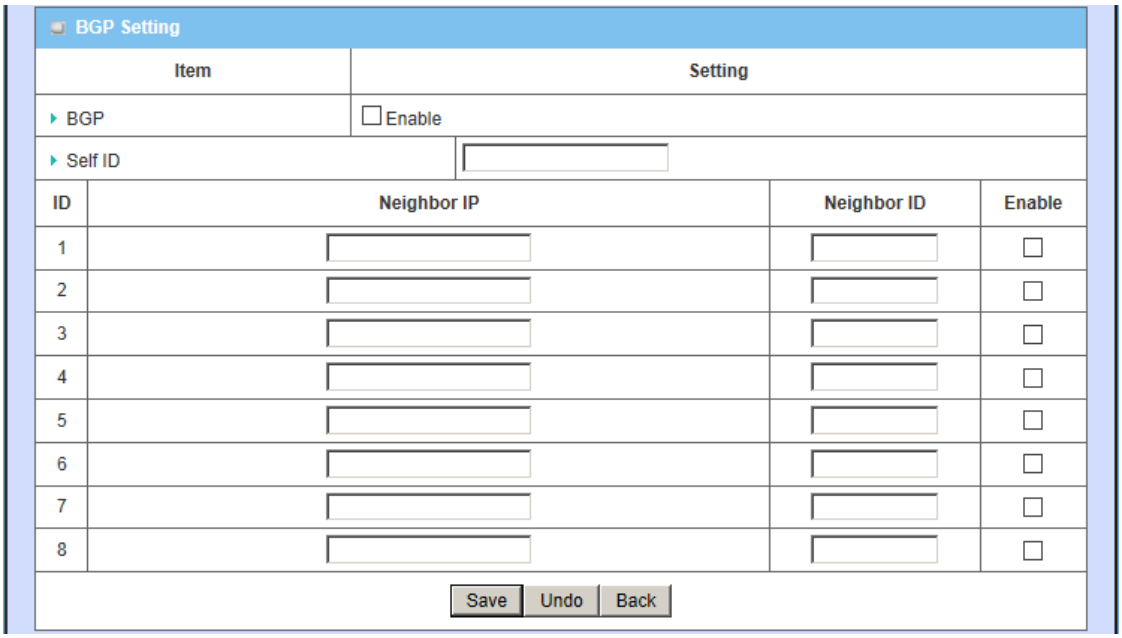
   When you finished setting, click on **"Save"** to store your settings or click **"Undo"** to give up the changes.

2. **OSPF**: OSPF is an interior gateway protocol that routes Internet Protocol (IP) packets solely within a single routing domain (autonomous system). It gathers link state information from available routers and constructs a topology map of the network. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.



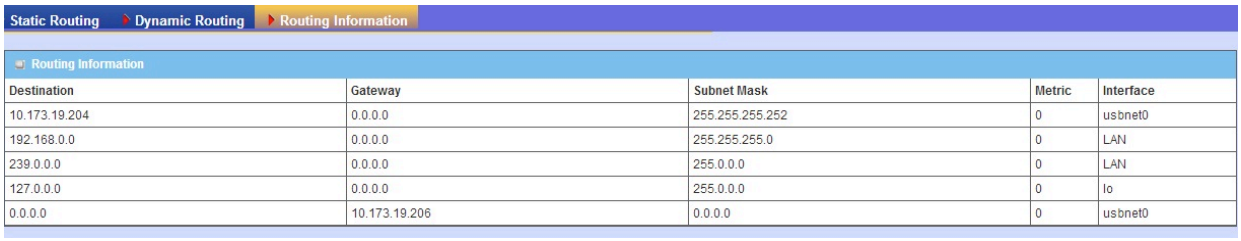
You can enable the OSPF routing function by click on the “Setting” button and fill in the corresponding setting for your OSPF routing configuration. When you finished setting, click on **“Save”** to store your settings or click **“Undo”** to give up the changes.

3. **BGP**: Border Gateway Protocol (BGP) is the protocol backing the core routing decisions on the Internet. It maintains a table of IP networks or 'prefixes' which designate network reach-ability among autonomous systems (AS). It is described as a path vector protocol. BGP does not use traditional Interior Gateway Protocol (IGP) metrics, but makes routing decisions based on path, network policies and/or rule-sets. For this reason, it is more appropriately termed a reach-ability protocol rather than routing protocol.



You can enable the BGP routing function by click on the “Setting” button and fill in the corresponding setting for your BGP routing configuration. When you finished setting, click on **“Save”** to store your settings or click **“Undo”** to give up the changes.

1.6.3 Routing information



Destination	Gateway	Subnet Mask	Metric	Interface
10.173.19.204	0.0.0.0	255.255.255.252	0	usbnet0
192.168.0.0	0.0.0.0	255.255.255.0	0	LAN
239.0.0.0	0.0.0.0	255.0.0.0	0	LAN
127.0.0.0	0.0.0.0	255.0.0.0	0	lo
0.0.0.0	10.173.19.206	0.0.0.0	0	usbnet0

A routing table, or routing information base (RIB), is a data table stored in a router or a networked computer that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes. The routing table contains information about the topology of the network immediately around it.

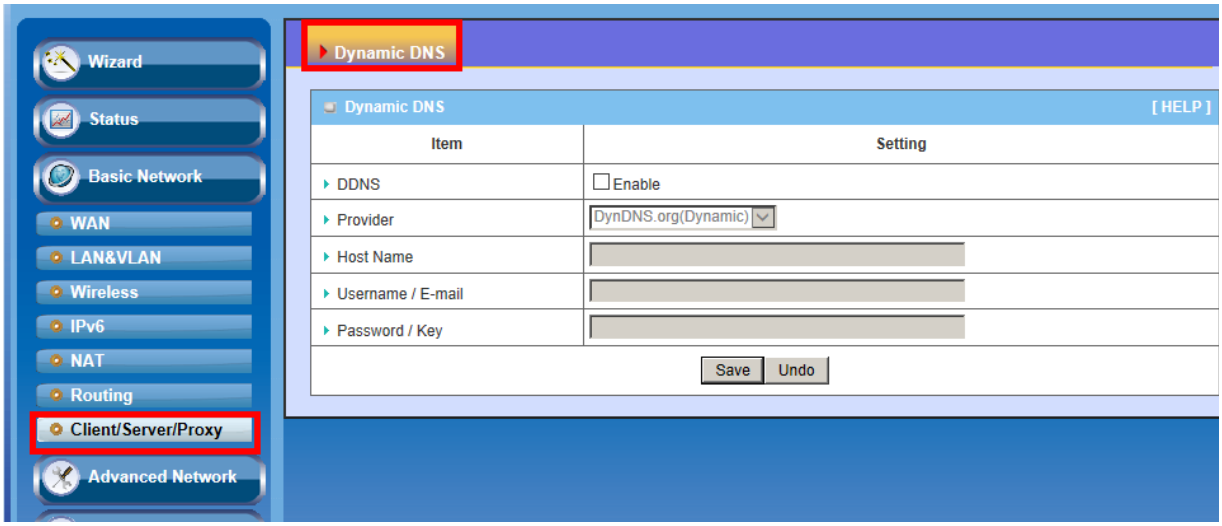
This page displays the routing table maintained by this device. It is generated according to your network configuration.

1.7 Client / Server / Proxy

1.7.1 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 name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

Before you enable **Dynamic DNS**, you need to register an account on one of these Dynamic DNS servers that we list in **Provider** field.



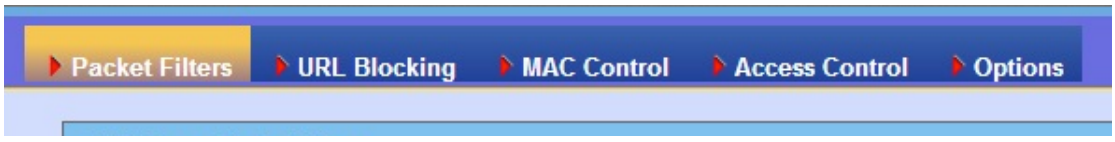
1. **DDNS:** Select enable if you would like to trigger this function.
2. **Provider:** The DDNS provider supports service for you to bind your IP(even private IP) with a certain Domain name. You could choose your favorite provider.
3. **Host Name:** Register a domain name to the DDNS provider. The fully domain name is concatenated with hostname(you specify) and a suffix(DDNS provider specifies).
4. **Username/E-mail:** Input username or E-mail based on the DDNS provider you select.
5. **Password/Key:** Input password or key based on the DDNS provider you select.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

2. Advanced Network

2.1 Firewall

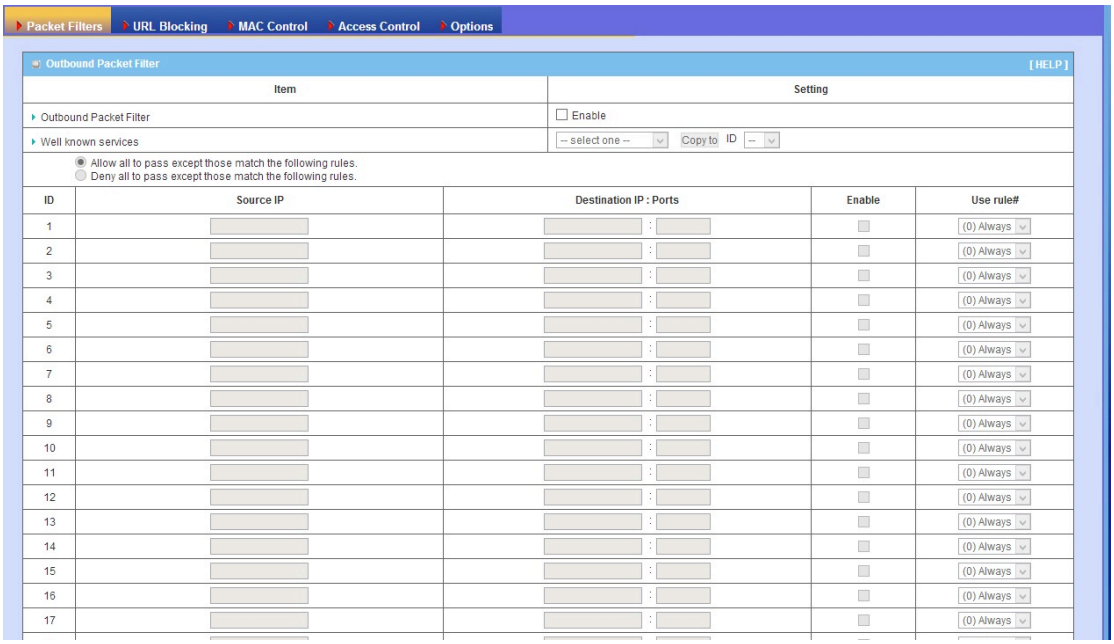
The Firewall include Packet Filters, URL Blocking, MAC Control, Access Control and Options



2.1.1 Packet Filters

Packet Filters include both outbound filter and inbound filter. And they have the same way to setting. It enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, inbound filter applies on packets that destined to virtual servers or DMZ host only. You can select one of the two filtering policies:

1. Allow all to pass except those match the following rules.
2. Deny all to pass except those match the specified rules.



You can specify rules for each direction: inbound or outbound. For each rule, you can define the following:

- Source IP address or range
- Destination IP address or range
- Destination port
- Protocol: TCP or UDP or both.
- Use Rule Schedule#

For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.20~30). An empty implies all IP addresses.

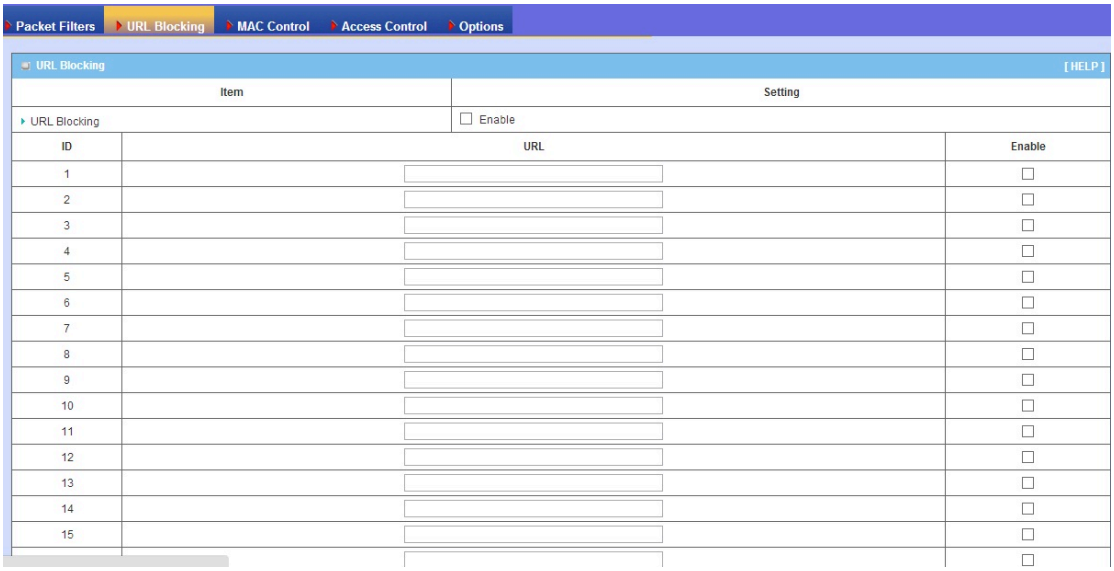
For destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999, No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. Packet Filter can work with **Scheduling Rules,** and give user more flexibility on Access control. For more details, please refer to the **Scheduling Rule** section.

Each rule can be enabled or disabled individually.

Afterwards, click on **"Save"** to store your settings or click **"Undo"** to give up the changes.

2.1.2 URL Blocking

URL Blocking will block the webs containing pre-defined key words. This feature can both filter domain input suffix (like .com or .org, etc) and a keyword "bct" or "mpe".

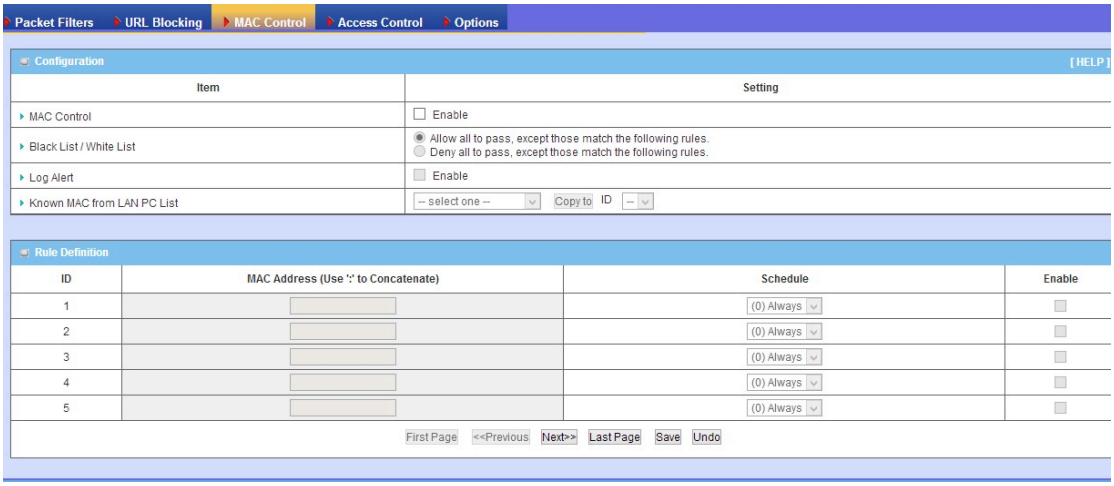


1. **URL Blocking**: Check if you want to enable URL Blocking.
2. **URL:** If any part of the Website's URL matches the pre-defined word, the connection will be blocked. You can enter up to 10 pre-defined words in a rule and each URL keyword is separated by ",", e.g., "abc, bt, org"; In addition to URL keywords, it can also block the designated domain name, like "www.xxx.com", "www.123aaa.org, mma.com".
3. **Enable**: Check to enable each rule.
4. **Schedule:** The rule can be turn off according to the schedule rule you specified. By default, it is always turned on when the rule is enabled.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

2.1.3 MAC Control

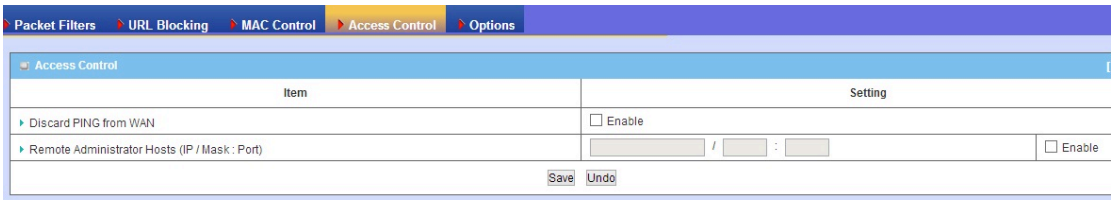
MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.



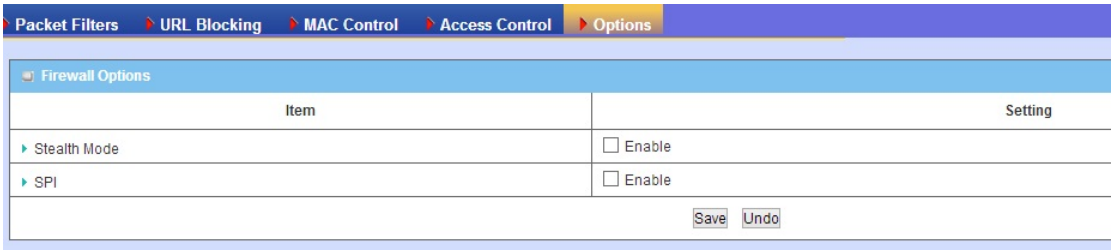
1. **MAC Address Control**: Check “Enable” to enable the “MAC Address Control”. All of the settings in this page will take effect only when “Enable” is checked.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

2.1.4 Access Control



2.1.5 Options



1. **Keep WAN in stealth mode:** If enabled, the router will not respond to port scans from the WAN, thus making it less susceptible to discovery and attacks.

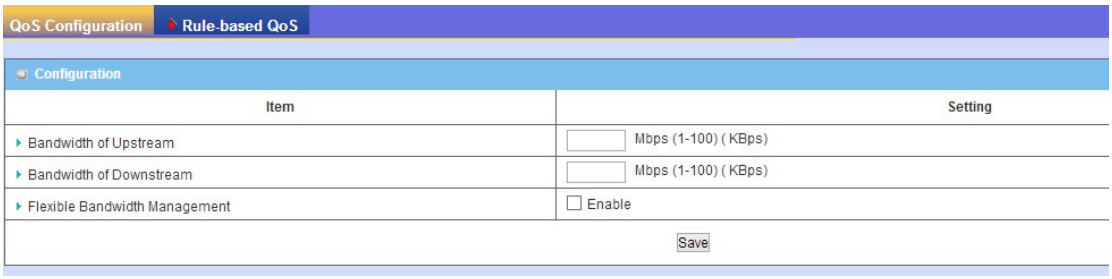
2. **SPI Mode:** SPI ("stateful packet inspection" also known as "dynamic packet filtering") helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through that session conforms to the protocol

   Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

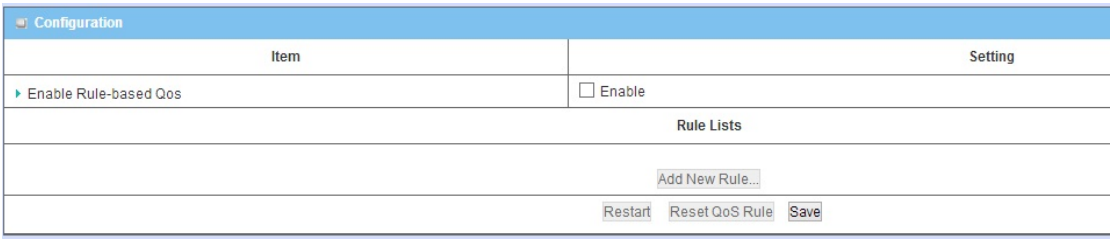
2.2 QoS (Quality of Service)

The main goal of QoS (Quality of Service) is prioritizing incoming data, and preventing data loss due to factors such as jitter, delay and dropping. Another important aspect of QoS is ensuring that prioritizing one data flow doesn’t interfere with other data flows.

QoS helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based on priority. This is useful when there are certain types of data you want to give higher priority to, such as voice packets given higher priority than Web data packets.



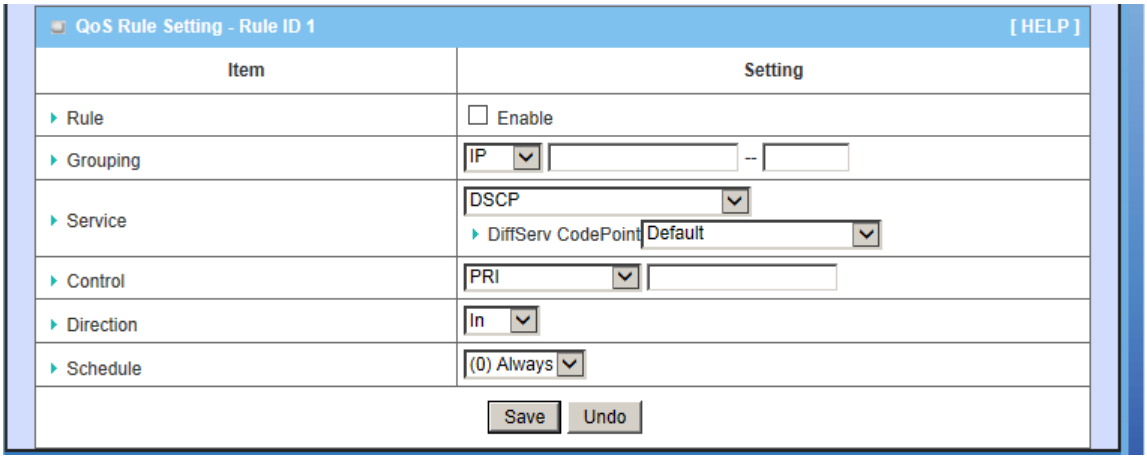
2.2.1 Rule-based QoS



1. **QoS:** You can enable/disable this QoS function.

Create a QoS Rule:

You can click on the button “Add New Rule” shown in the icon above to create a new QoS rule.



1. **Rule**: Enable the rule setting first.
2. **Grouping**: Select the QoS grouping class from the drop list, and specify the grouping information accordingly.

Grouping	Description
IP	IP address based
MAC	MAC based

3. **Service**: Set your own “Service” type to enable the QoS rule as below.

Service	Description
DSCP	DiffServ Code Point
Service Port	Mean TCP or UDP Port
Pre-defined Application profiles	Normal service Application
Connection Sessions	NAT Session

4. **Control**: Set the corresponding control type for the selected service type.

Control	Description	Data
DSCP Marking	Priority as you select DiffServ CodePoint	CS1 ~ AF
PRI	Priority	1~6(1 is highest Priority)
MAXR	Maximum bandwidth Rate	KBps/MBps
MINR	Minimum bandwidth Rate	KBps/MBps
SESSION	Connection session	Number (1~20000)

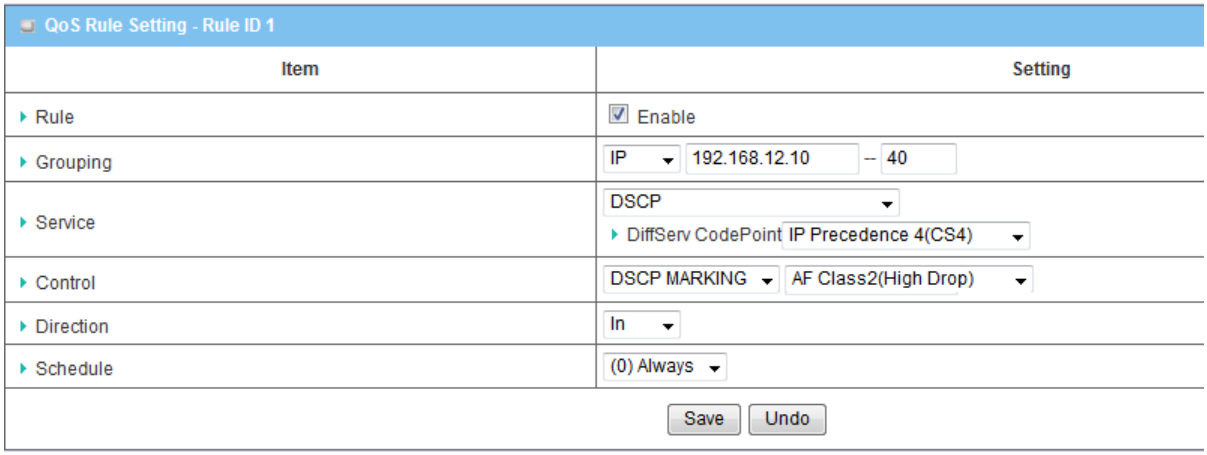
5. **Direction**: Select the traffic direction to be applied for this QoS rule.

Direction	
IN	In-bond
OUT	Out-bond
BOTH	In-bond & Out-bond

6. **Schedule**: The QoS rule can be turn off according to the schedule you specified. By default, it is always turned on when the rule is enabled.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

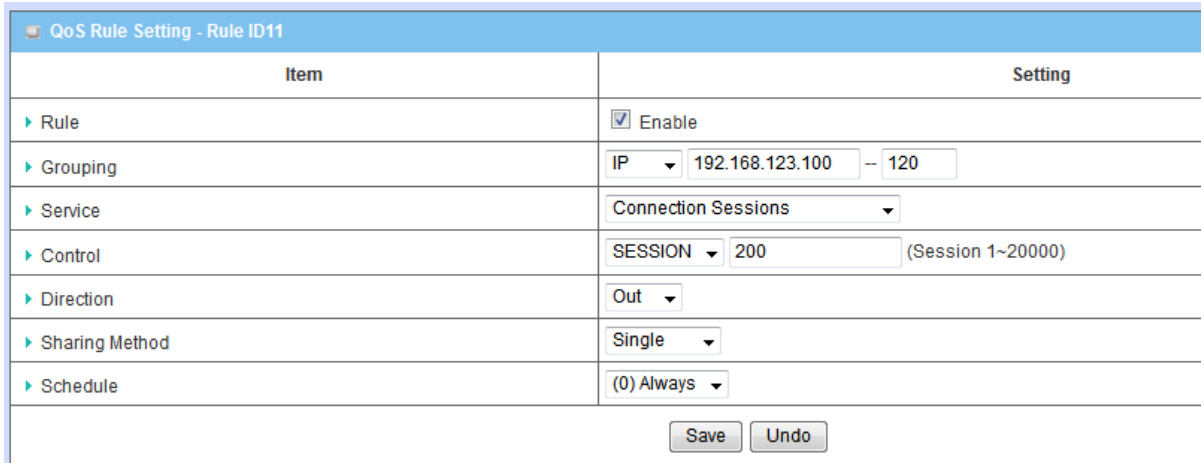
Example for adding a “DSCP” type QoS rule:



Grouping: Select “IP” and entry IP Range.
Service: Select “DSCP” and “Source Network Packets” which DiffServ are set as CS4.
Control: Select “DSCP Marking” and mark these Packets as “AF Class 2”.
Direction: Select “IN” for In-bound traffic only.
Schedule: Leave the default value of “(0)Always” as it is.

This Rule means IP Packets from WAN or other interfaces with DiffServ value of CS4 will be modified with DSCP Marking of “AF Class 2”, then forward corresponding packets to the Clients whose IP address is in the range of 192.168.12.10~40.

Example for adding a “Connection Sessions” type QoS rule:



Control: Set NAT session number as 200.
Direction: Select “Out” for Out-bound traffic only. It is for the client devices under the Gateway to establish session with servers on the Internet.
Sharing Method: Select “Single” or “Grouping” from the drop list. In this

case, “Single” is selected.
Schedule: leave the default value of “(0)Always” as it is.
This Rule defines that each single user, whose IP address is in the range of 192.168.123.100~120, can access to a remote server on the Internet, and keep a maximum 200 sessions at the same time.

Finishing QoS settings:
Once you saved the QoS rule, it will be displayed in the Rule List area as below.

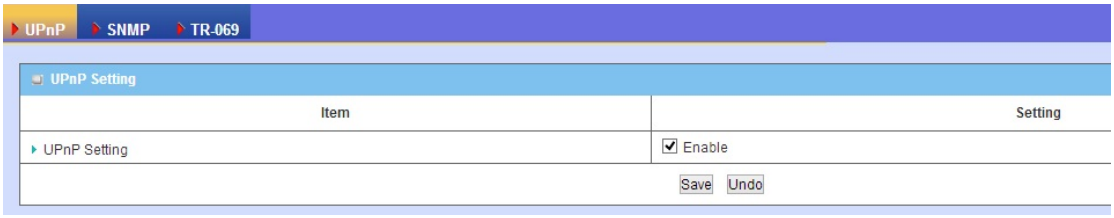
Besides, you can move up or down the priority of all rules by clicking on the ‘↑’or ’↓’ icon if you want to change the priority of rules. You can also unmark any rule in the list if you don’t want to enable it.

2.3 Management

2.3.1 UPnP

UPnP Internet Gateway Device (IGD) Standardized Device Control Protocol is a NAT port mapping protocol and is supported by some NAT routers. It is a common communication protocol of automatically configuring port forwarding. Applications using peer-to-peer networks, multiplayer gaming, and remote assistance programs need a way to

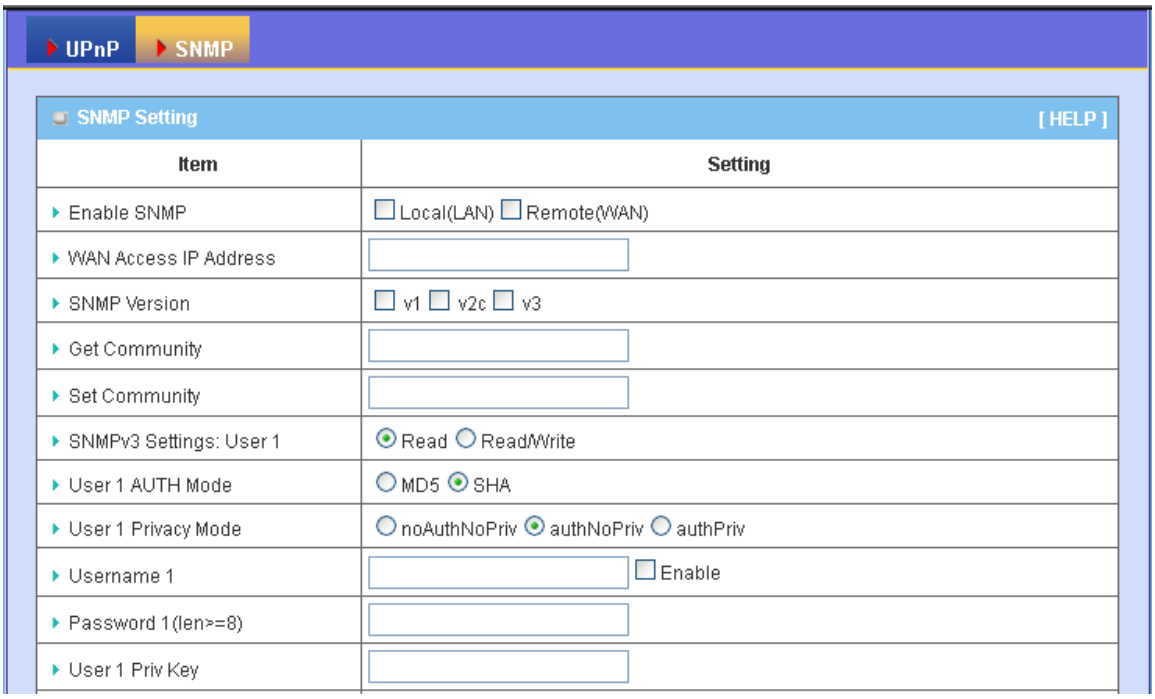
communicate through home and business gateways. Without IGD one has to manually configure the gateway to allow traffic through, a process which is error prone and time consuming

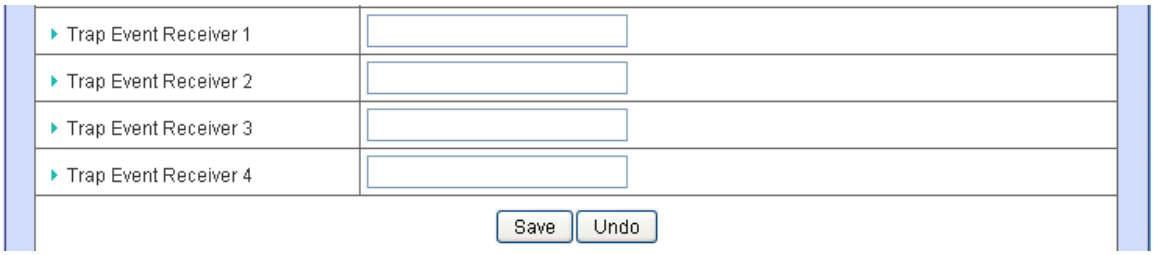


This device supports the UPnP Internet Gateway Device (IGD) feature. By default, it is enabled.

2.3.2 SNMP

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





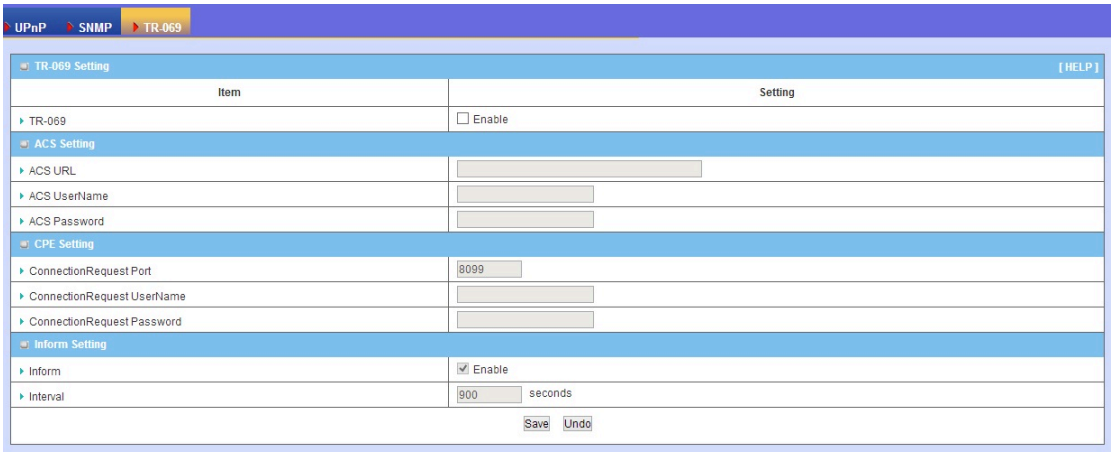
1. **Enable SNMP**: You can check “Local”, “Remote” or both to enable SNMP function. If “Local” is checked, this device will respond to the request from LAN. If “Remote” is checked, this device will respond to be request from WAN.
2. **WAN Access IP Address:** If you want to limit the remote SNMP access to specific computer, please enter the PC`s IP address. The default value is 0.0.0.0, and it means that any internet connected computer can get some information of the device with SNMP protocol.
3. **SNMP Version:** Supports SNMP V1, V2c, and V3.
4. **Get Community:** The community of GetRequest that this device will respond. This is a text password mechanism that is used to weakly authenticate queries to agents of managed network devices.
5. **Set Community:** The community of SetRequest that this device will accept.
6. **SNMPv3 Settings: User 1/2**: This device supports up to two SNMP management accounts. You can specify the account permission as “Read” or “Read/Write” respectively.
7. **User 1/2 AUTH Mode**: Select MD5 or SHA as the method of password encryption for the specified level of access, or to disable authentication.
8. **User 1/2 Privacy Mode:** You can configure the SNMP privacy mode. There are three modes for you to choose: “noAuthNoPriv” for both authentication and private key are not required, “authNoPriv” for no private key required, and “authPriv” for both authentication and private key required.
9. **Username 1/2:** Use this field to identify the user name for the specified level of access.
10. **Password 1/2:** Use this field to set the password for the specified level of access.
11. **User 1/2 Priv Key:** Use this field to define the encryption key for the

specified level of access.

12. **Trap Event Receiver 1 ~ 4:** Enter the IP addresses or Domain Name of your SNMP Management PCs. You have to specify the IP address, so that the device can send SNMP Trap message to the management PCs consequently.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

2.3.3 TR069



1. **TR-069**: Disable or enable the TR-069 settings.

2. **ACS setting**: you may add ACS URL/ Username/ Password.

3. **CPE setting**: you may add CPE connection request port/ username /password.

4. **Inform setting**: you may enable/disable the interval of informing CPE.

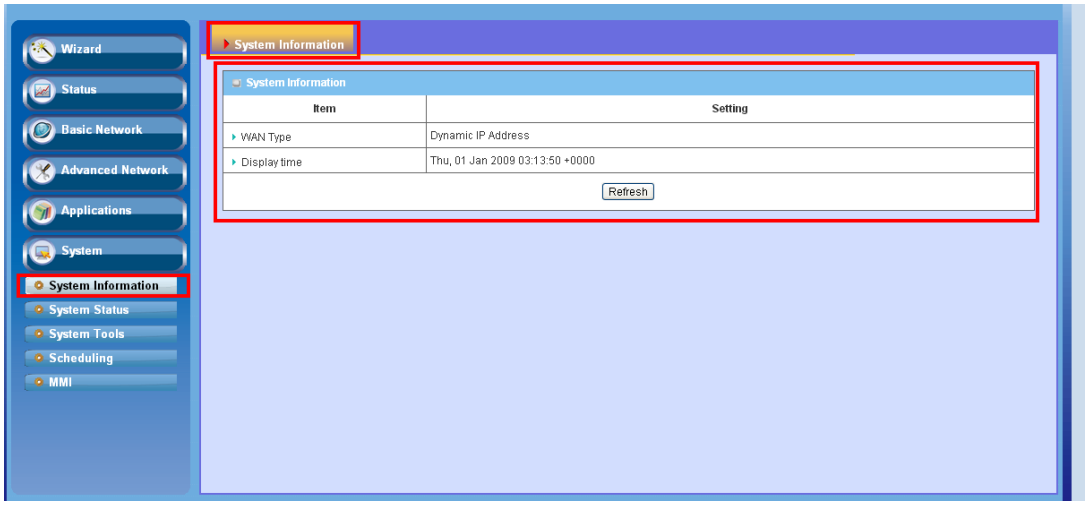
5. **Interval** : you may input seconds for every interval.

3. System

In this section you can see system information, system logs, use system tools for system update and do service scheduling and system administration setting.

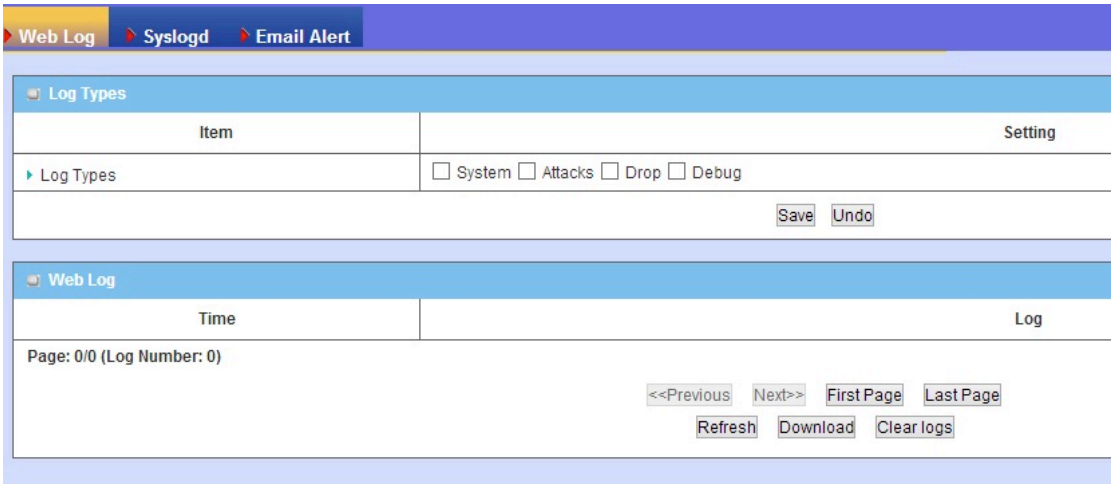
3.1 System Information

You can view the System Information in this page.



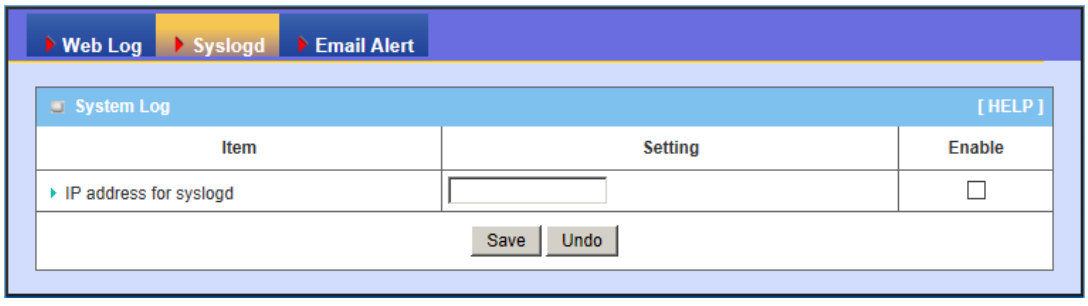
3.2 System status

3.2.1 Web Log



1. **Log Types**: You can select the log types to be collected in the web log area. There are “System”, “Attacks”, “Drop”, and “Debug” types for you to select.
2. **Web Log**: You can browse, refresh, download, and clear the log messages.

3.2.2 Syslog

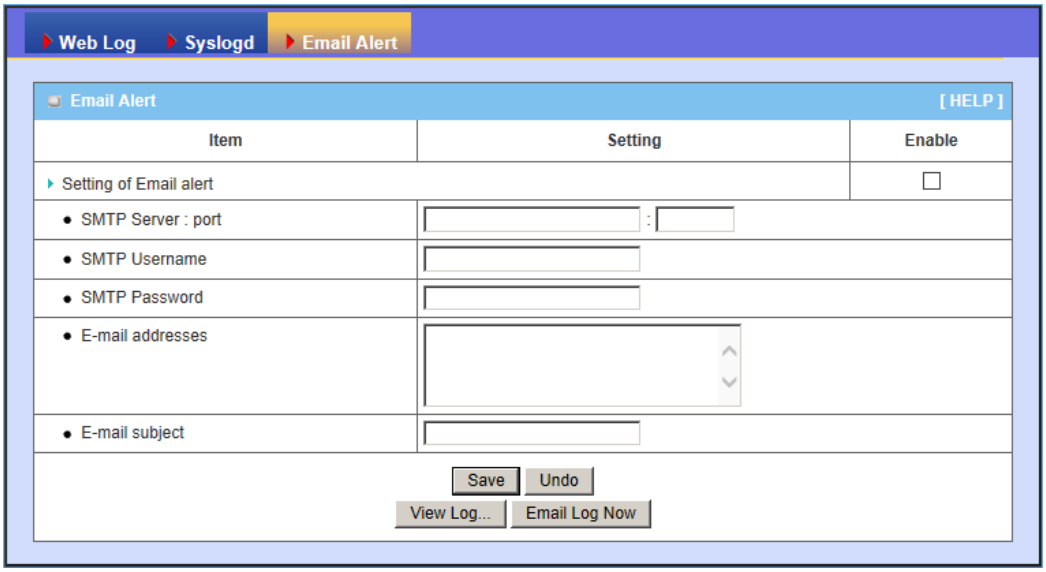


This device can also export system logs to specific destination by means of syslog (UDP) and SMTP(TCP). With enabled Syslog function, this device will send log to a certain host periodically. You need to install a syslog utility on a host to receive syslogs

The items you have to setup include:

1. **IP Address for syslogd**: Host IP of destination where syslog will be sent to. Check **Enable** to enable this function.

3.2.3 Email Alert



This device can also export system logs via sending emails to specific recipients. The items you have to setup include:

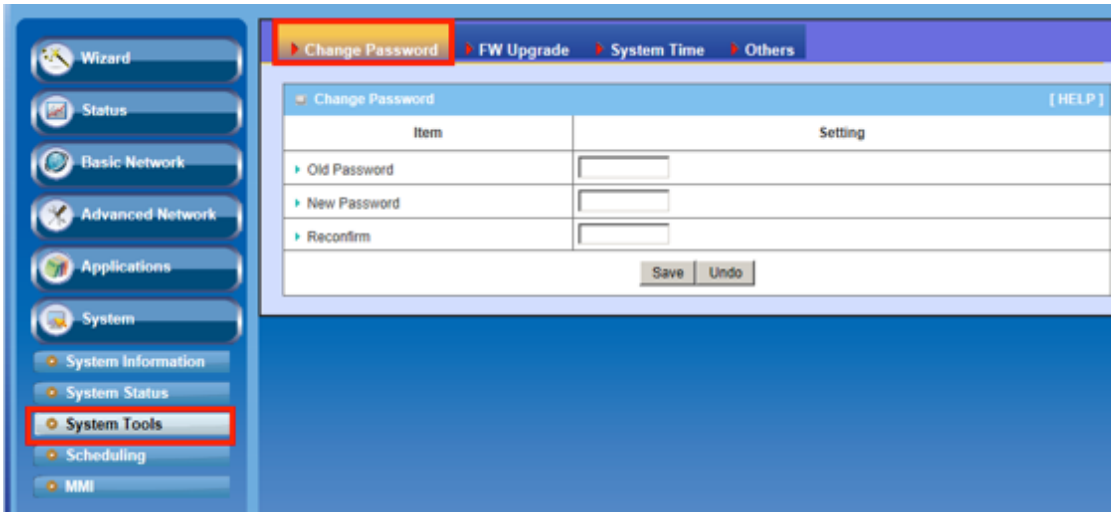
1. **Setting of Email alert**: Check if you want to enable Email alert (send syslog via email).
2. **SMTP Server: Port**: Input the SMTP server IP and port, which are connected with ':'. If you do not specify port number, the default value is 25.
   For example, "mail.your_url.com" or "192.168.1.100:26".
3. **SMTP Username:** Enter the Username offered by your ISP.
4. **SMTP Password:** Enter the password offered by your ISP.
5. **E-mail Addresses:** The recipients are the ones who will receive these logs. You can assign more than 1 recipient, using ';' or ',' to separate these email addresses.
6. **E-mail Subject**: The subject of email alert is optional.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.3 System Tools

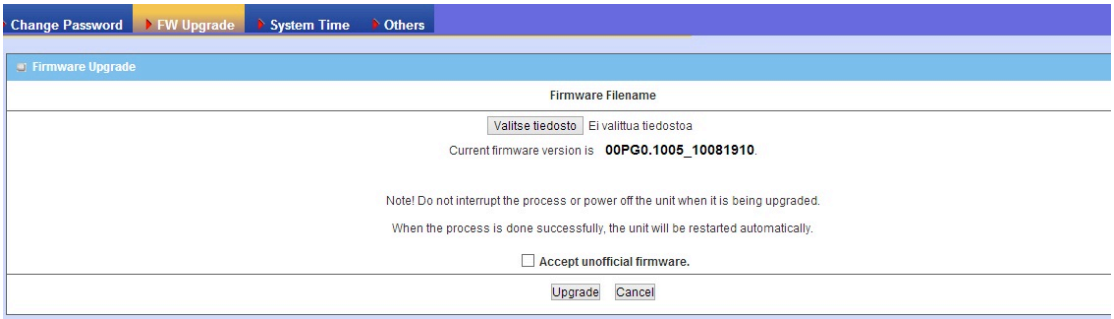
3.3.1 Change Password

You can change the System Password here. We **strongly** recommend you to change the system password for security reason. Click on “Save” to store your settings or click “Undo” to give up the changes.



3.3.2 Firmware Upgrade

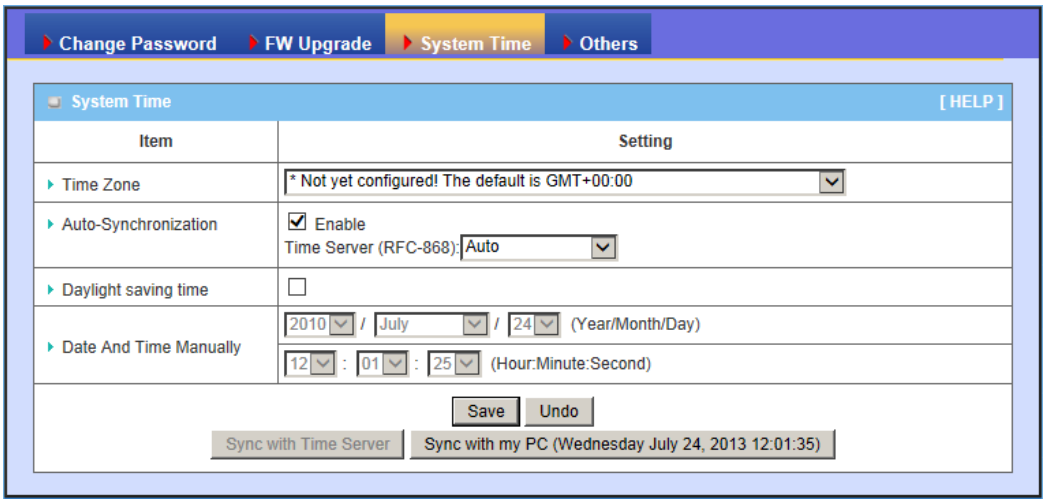
If new firmware is available, you can upgrade router firmware through the WEB GUI here.



Press “browse” button to indicate the file name of new firmware, and then press Upgrade button to start to upgrade new firmware on this device. If you want to upgrade a firmware which is from GPL policy, please check “Accept unofficial firmware”.

NOTE. PLEASE DO NOT TURN THE DEVICE OFF WHEN UPGRADE IS PROCEEDING.

3.3.3 System Time

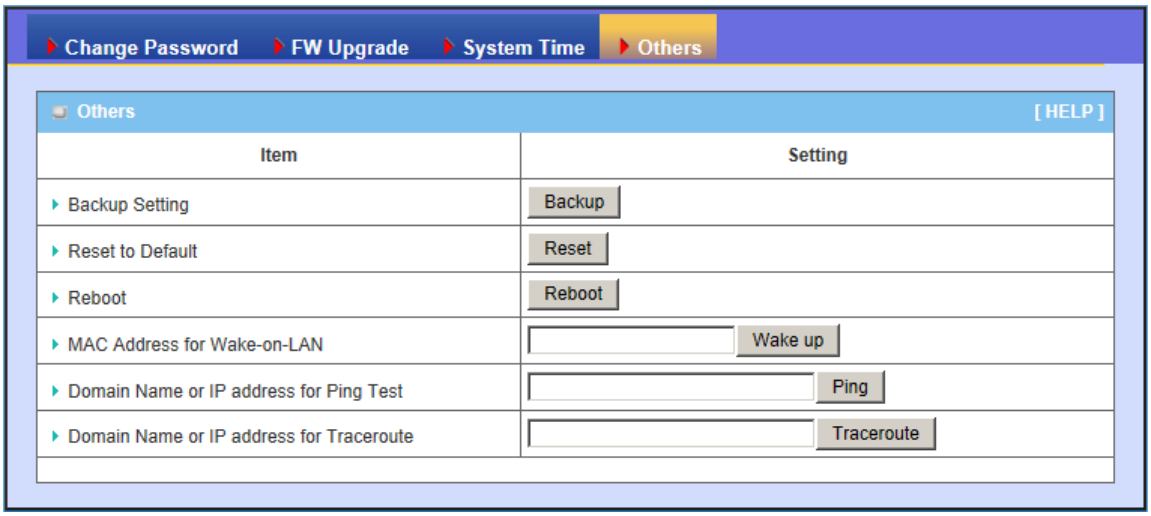


1. **Time Zone**: Select a time zone where this device locates.
2. **Auto-Synchronization**: Check the "Enable" checkbox to enable this function. Besides, you can select a NTP time server to consult UTC time.
3. **Sync with Time Server**: Click on the button if you want to set Date and Time by NTP Protocol.
4. **Sync with my PC**: Click on the button if you want to set Date and Time using the PC's Date and Time.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

3.3.4 Others

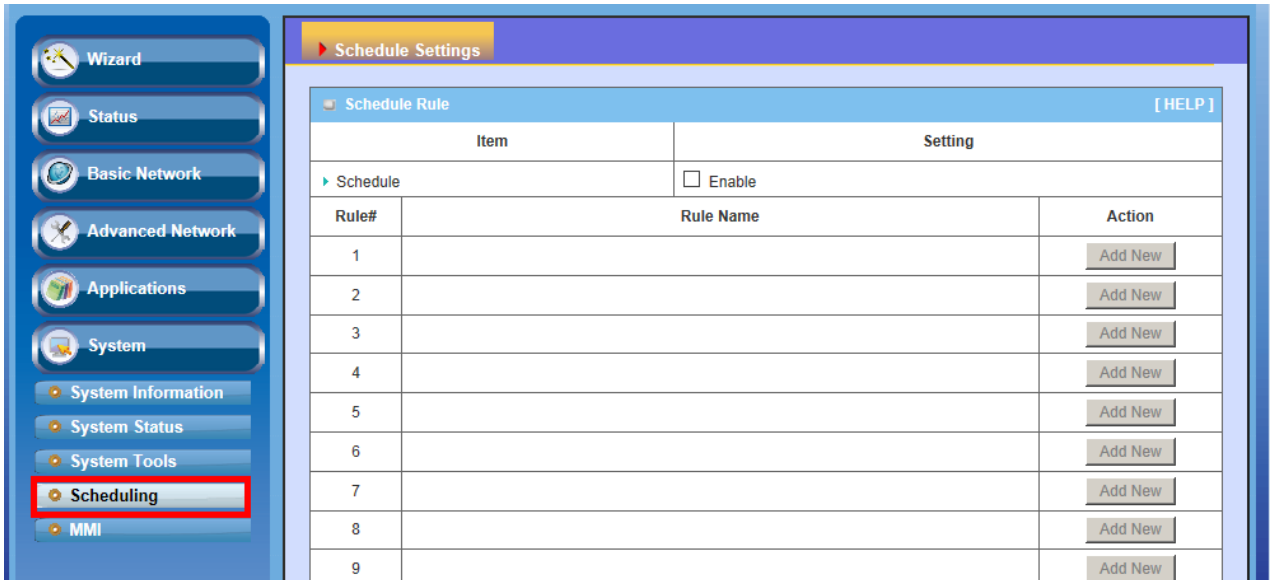
In this section you can do system backup, reset to default, system reboot settings and ping test.



1. **Backup Setting**: You can backup your settings by clicking the "**Backup"** button and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you saved.
2. **Reset to Default**: You can also reset this device to factory default settings by clicking the "**Reset**" button.
3. **Reboot**: You can also reboot this device by clicking the "**Reboot**" button.
4. **MAC Address for Wake-on-LAN**: Wake-on-LAN (WOL) is an Ethernet networking standard that allows a computer to be turned on or awakened by a network message. You can enter the MAC address of the computer, in your LAN network, to be remotely turned on.
5. **Domain Name or IP address for Ping Test**: This allows you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.
6. **Domain Name or IP address for Traceroute**: Traceroute is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Traceroute proceeds unless all (three) sent packets are lost more than twice, then the connection is lost and the route cannot be evaluated. Ping, on the other hand, only computes the final round-trip times from the destination point

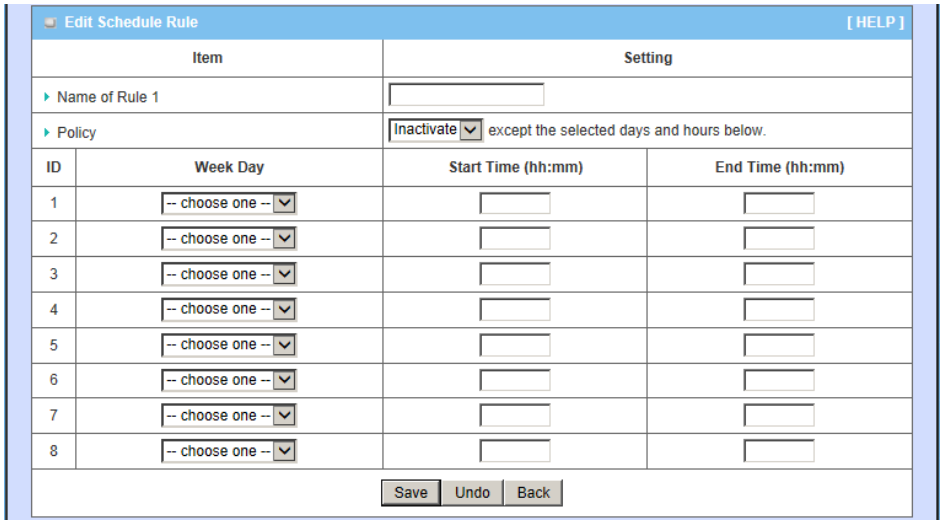
3.4 Scheduling

You can set the schedule time to decide which service will be turned on or off. The added rules will be listed.



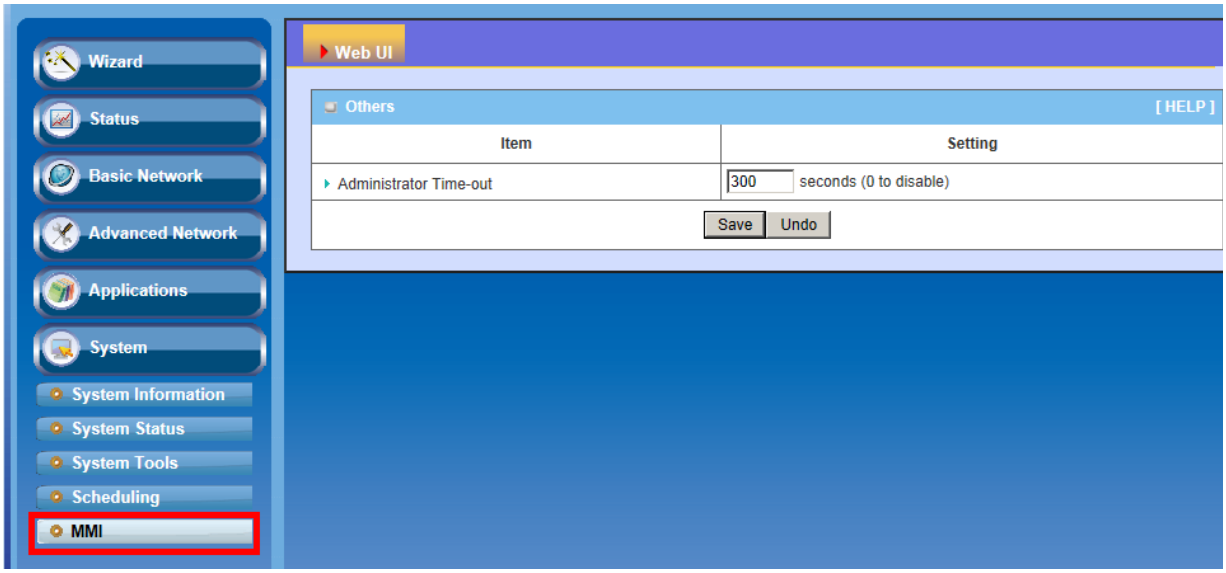
Add New Rule: To create a schedule rule, click the “Add New” button or the “Add New Rule…” button at the bottom. When the next dialog popped out you can edit the **Name of Rule**, **Policy**, and set the schedule time (**Week day**, **Start Time**, and **End Time**).

Afterwards, click **“save”** to store your settings or click **“Undo”** to give up the changes.



3.5 MMI

Web UI



You can set UI administration time-out duration give remote administration host port in this page. When the host port is given please remember to check the enable box and save your settings.

CE

EC-Declaration of Conformity

For the following equipment:

TW-LTE/4G/3G router

(Product Name)

TW-LTE/4G/3G router

(Model Designation / Brand Name)

TeleWell Oy

(Company Name)

Kinnarinkatu 1, 04430 Järvenpää, Finland

(Company Address)

The below mentioned product has been tested in typical configuration by Compliance Certification Services, Inc. and was found to comply with the essential requirement of " DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of conformity" . The following standards are applied:

[V] **EMC**
EN 301 489-01 V1.6.1 (2005)
EN 301 489-17 V1.2.1 (2002)

[V] **Radio Spectrum**
EN 300 328 V1.7.1 (2006)

[V] **Safety**
EN 60950-1: 2001+A11

This product follows the provisions of R&TTE Directive 1999/5/EC.

The following manufacturer / importer or authorized representative established within the EUT is responsible for this declaration:

TeleWell Oy

(Company Name)

Kinnarinkatu 1, 04430 Järvenpää, Finland

(Company Address)

Person responsible for making this declaration:

Markku Åberg

(Name, Surname)

Managing Director

(Position / Title)

Järvenpää 2013-10-15

(Place) (Date) (Legal Signature)

TeleWell

04430 Järvenpää

LEO Mr. Markku Åberg