User Manual

CDW68AAM-U01
WiFi Broadband Router

Copyright

Trademarks

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

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

802.11a (UNII) RF exposure statement

According to FCC 15.407(e), the device is intended to operate in the frequency band of 5.15GHz to 5.25GHz under all conditions of normal operation. Normal operation of this device is restricted to indoor used only to reduce any potential for harmful interference to co-channel MSS operations.

FCC Part 15.19 Caution:

1. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
   (1) this device may not cause harmful interference and
   (2) this device must accept any interference received, including interference that may cause undesired operation
2. This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.
3. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

Table of contents

Chapter 1 Introduction

CDW68AAM-U01 is a 802.11n concurrent dual band mobile broadband router with USB slots for 3G modem card and USB storage. It can support 3G/4G mobile broadband. It also provides a physical WAN port for fixed-line broadband and supporting varieties of WAN connection types, such as PPPoE, static IP, dynamic IP (DHCP client), PPTP, and L2TP. There's also a built-in 4-port full-duplex 10/100/1000 gigabit switch to connect your wired Ethernet devices together.

This concurrent dual band router is the high performance gateway of your home or office network, and it is particularly designed for video streaming applications, user can extend the wireless by 802.11n compliant 5GHz/2.4GHz 450Mbps+300Mbps RF.

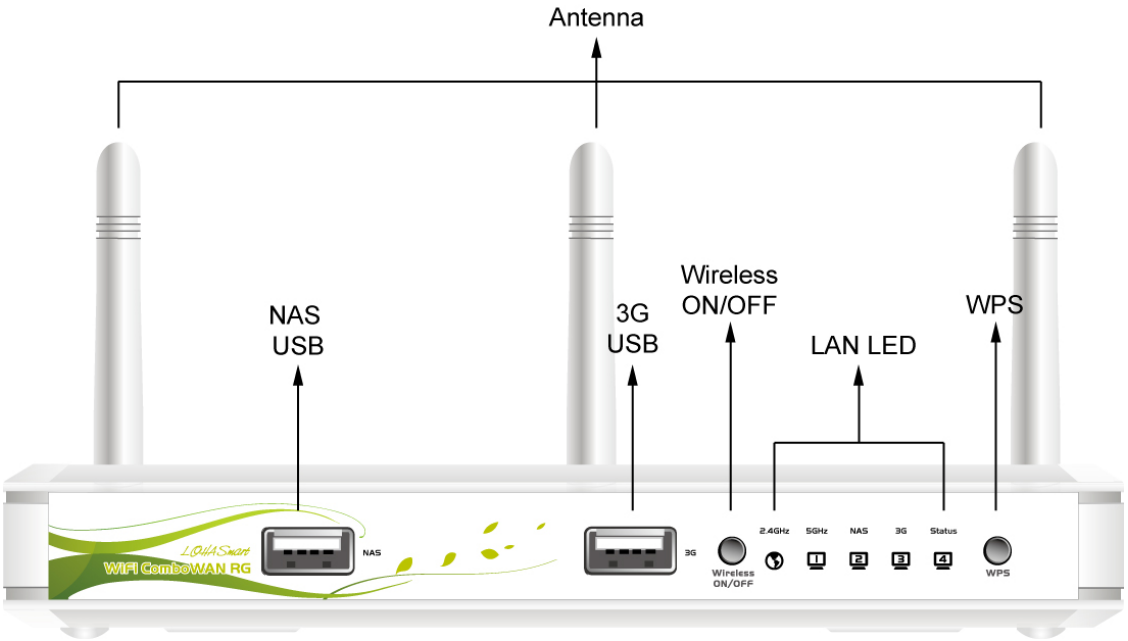
Moreover, the USB port is designed to share files under the same network. For NAS function, it can support FAT16/FAT32, EXT2, NTFS file system, user can plug the USB Hard drive or pen drive, and share files instantly. Once you want to enable FTP/HTTP/BT download service, you can follow easy steps to let it download files without turning on a PC. With this powerful residential/SOHO gateway, you can connect everyone in your home or small office to the network sharing function for music, gaming, video, and achieving higher speed as WiFi 11n, which is faster and much better coverage than 11b/g.

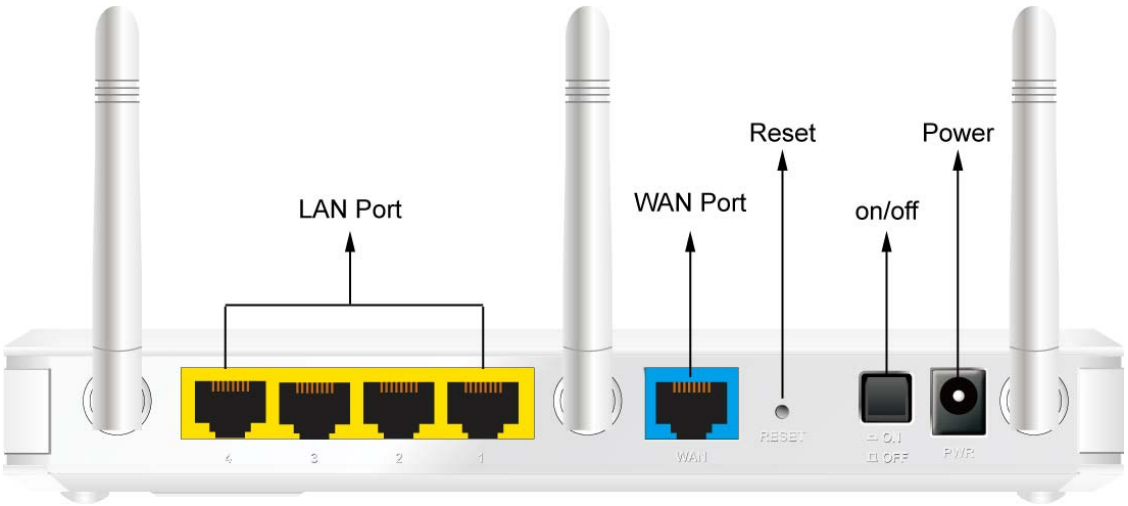
1.1 Package List

Items	Description	Contents	Quantity
1	WiFi Broadband Router		1
2	Power adapter		1
3	CD		1

1.2 Hardware Installation

A. Hardware configuration





B. Buttons

Button	Behavior
WPS Button	Continually press 3 seconds to enter WPS PBC mode for 2.4G wireless
	Continually press 8 seconds to enter WPS PBC mode for 5G wireless
Wireless On/Off Button	Continually press 3 seconds to switch on/off for 2.4G wireless radio
	Continually press 8 seconds to switch on/off for 5G wireless radio
Reset Button	Continually press 6 seconds to reset device settings to factory default

C. LED indicators

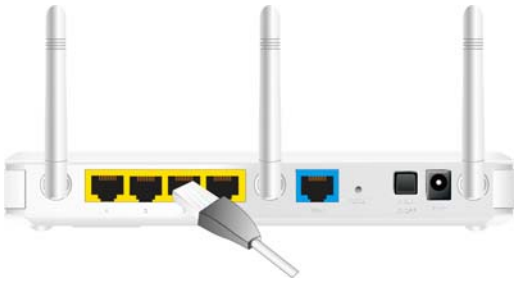
LED	Indicator	Description
Status	Green and flash once per second	This device is working
	Green and Steady On	An error occurred
	OFF	Device is powered off or an error occurred
Ethernet WAN	Green and Steady On	Ethernet WAN connection is established
	Green and Blinking	Data packet transferred via Ethernet WAN
Ethernet LAN 1~4	Green and Steady On	Ethernet LAN connection is established
	Green and Blinking	Data packet transferred via Ethernet LAN
2.4GHz	Green and Blinking	Data packet transferred via 2.4G WiFi
	Green and Fast Blinking	In WPS PBC mode
	OFF	2.4GHz wireless radio is disabled
5GHz	Green and Blinking	Data packet transferred via 5G WiFi
	Green and Fast Blinking	In WPS PBC mode
	OFF	5GHz wireless radio is disabled
NAS	Green and Steady On	An external USB storage is attached
	Green and Blinking	Data packet transferred via attached USB storage device (e.g. USB drive)
	OFF	No USB storage is attached
3G	Green and Steady On	3G connection is established
	Green and Blinking	Data packet transferred via 3G WAN
	OFF	3G connection is not established

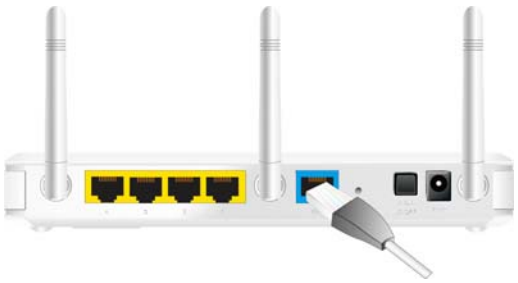
D. Installation Steps

Note: ***DO NOT*** connect the router to power before performing the installation steps below.

Step 1.
Plug a USB modem into USB port.

Step 2.
Insert RJ45 cable into LAN Port on the back panel of the router. Then plug the other end of into computer.





Step 3.
Plug the power jack into the receptor on the back panel of the router. Then plug the other end into a wall outlet or power strip.

Chapter 2 Getting Started with Easy Setup Utility

There are two approaches for you to set up the WiFi Broadband Router quickly and easily. One is through executing the provided Windows Easy Setup Utility on your PC, and the other is through browsing the device web pages and configuration.

2.1 Easy Setup by Windows Utility

Step 1 :

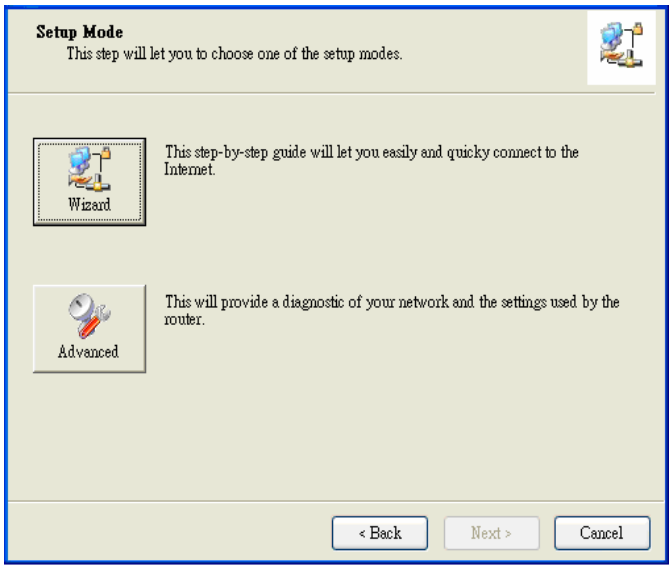
Install the Easy Setup Utility from the provided CD then follow the steps to configure the device.

Step 2 :

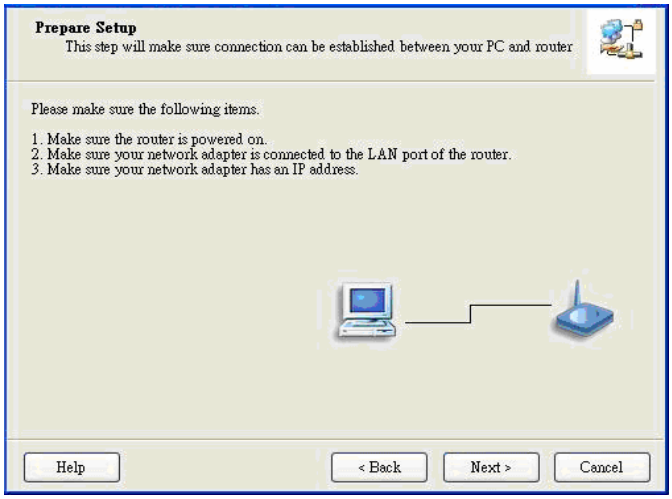
Select Language then click “Next” to continue.

Step 3 :

Then click the “Wizard” to continue.

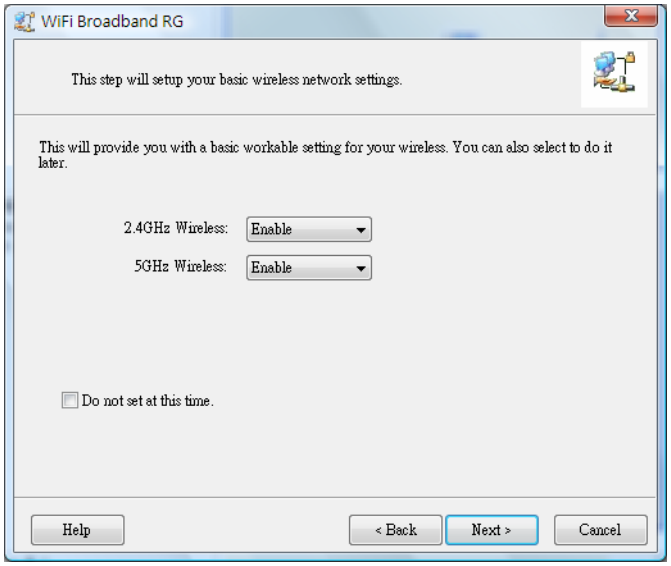


Step 4 :
Click “Next” to continue.

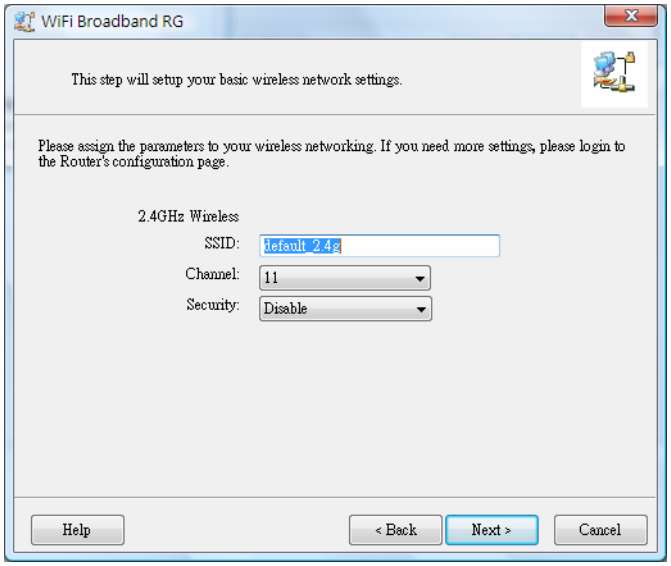


Step 5 :
Select Wireless Enable, and then click “Next” to continue.

Note. You can configure 2.4GHz wireless and 5GHz wireless separately.

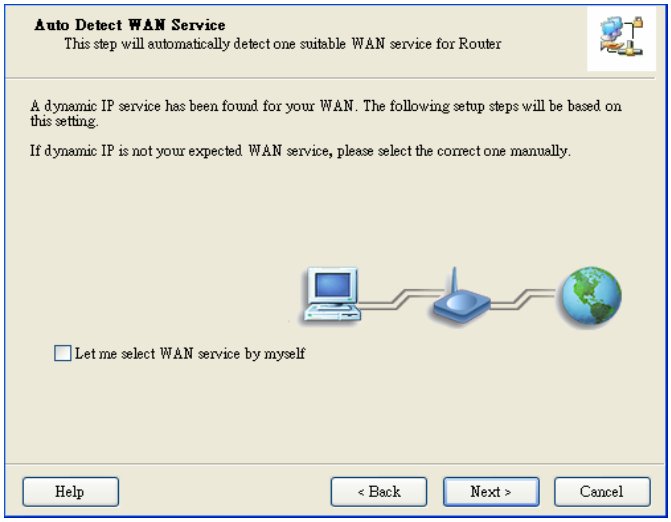


Step 6 :
Enter SSID, Channel and Security options, and then click “Next” to continue.



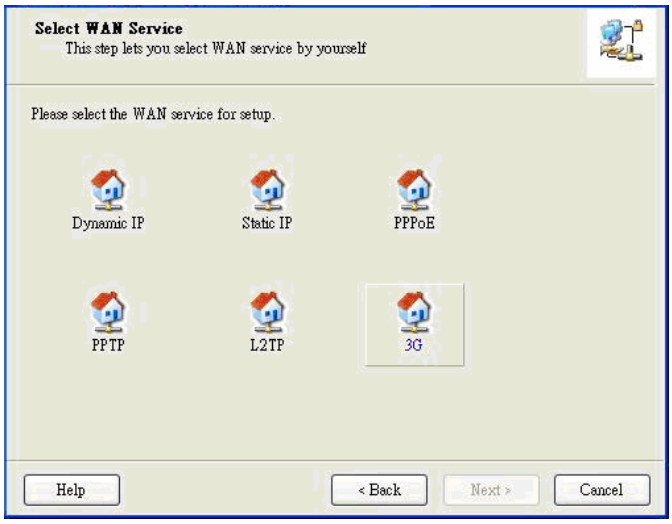
Step 7：

Click” Let me select WAN service by myself” to select WAN service manually.



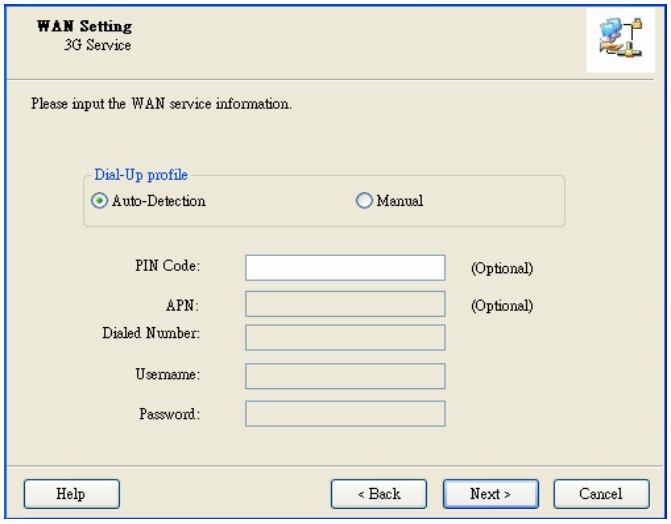
Step 8：

Select 3G Service by clicking 3G icon to continue.

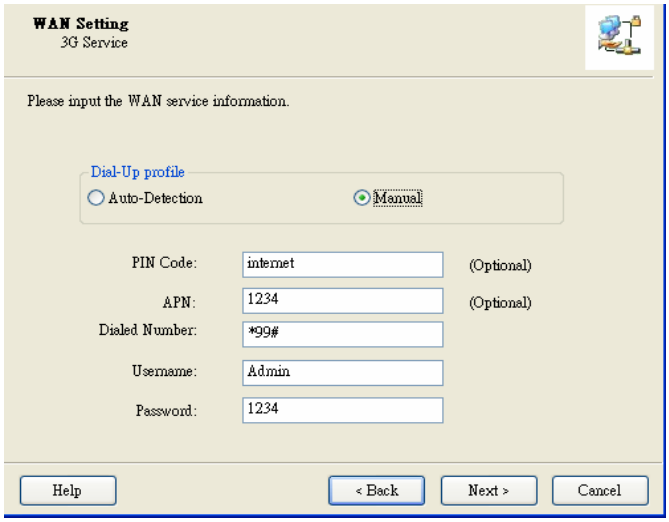


Step 9-1：

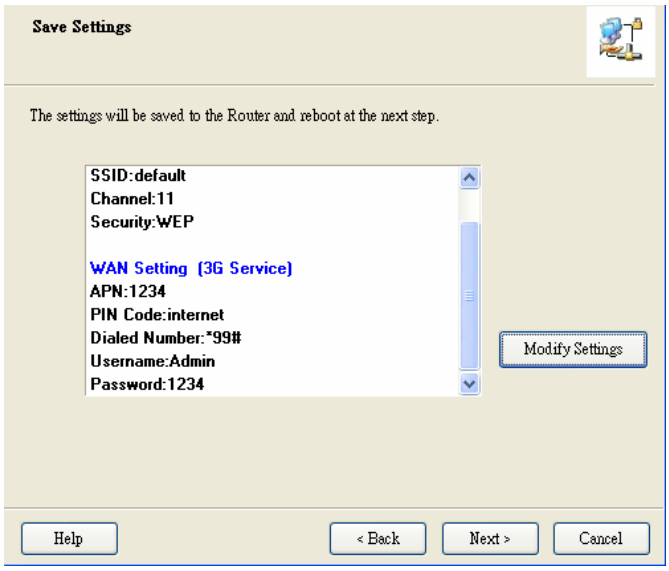
Select “Auto-Detection” and the Utility will try to detect and configure the required 3G service settings automatically. Click “Next” to continue.



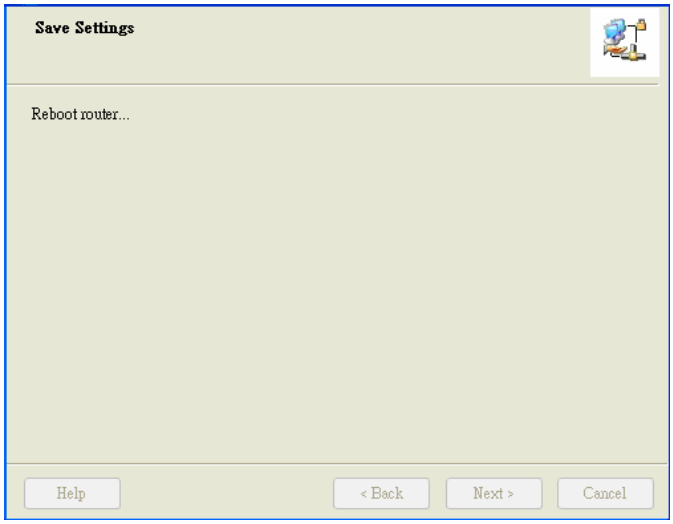
Step 9-2 :
Or you can select “Manual” and manually fill in the required 3G service settings provided by your ISP.
Click “Next” to continue.



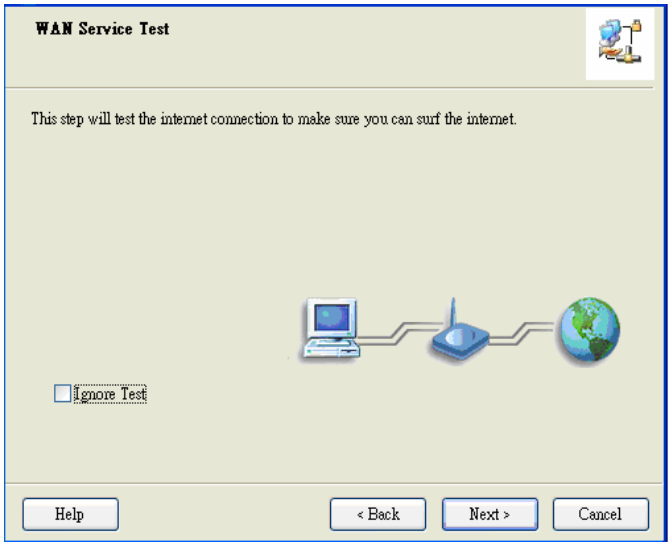
Step 10:
Click “Next” to save your setting.



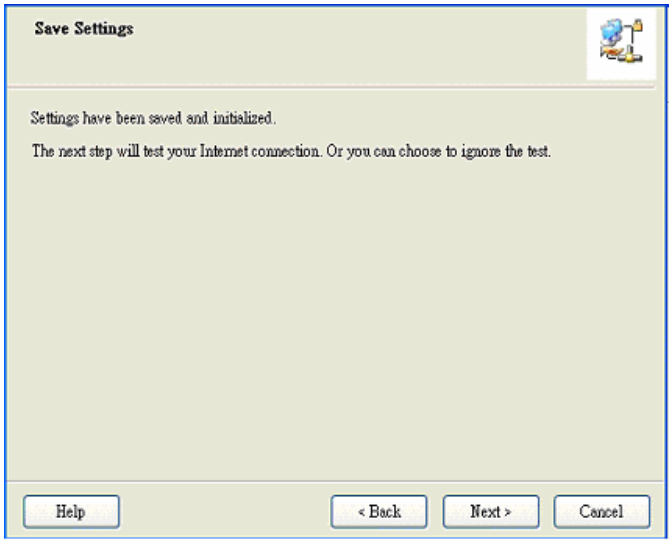
Step 11 :
The WiFi Broadband Router is rebooted to make your entire configuration take effect.



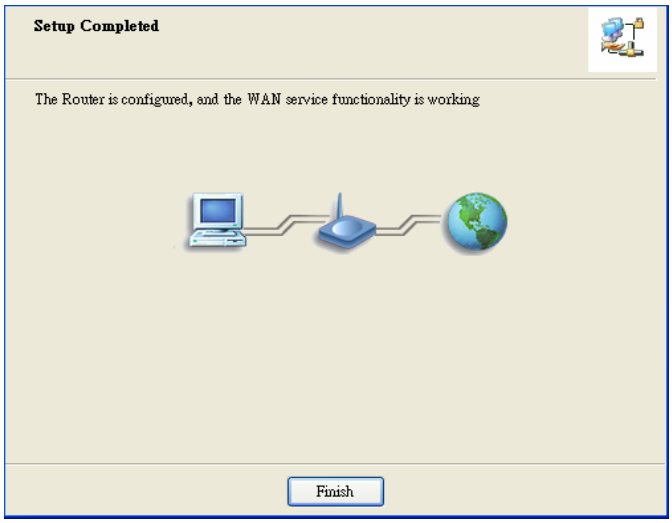
Step 12 :
Click “Next” to test the Internet connection or you can ignore test.



Step 13 :
Click “Next” to test WAN Networking service.



Step 14 :
Setup is completed.

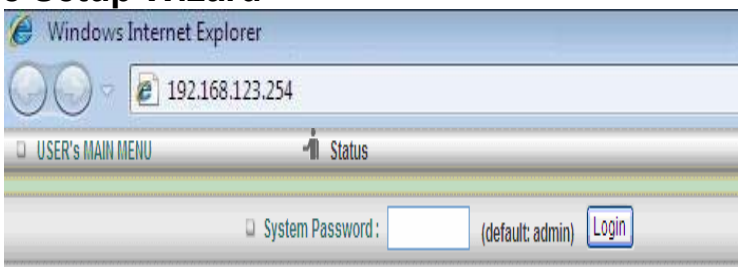


2.2 Easy Setup by Configuring Web Pages

You can also browse web UI to configure the device.

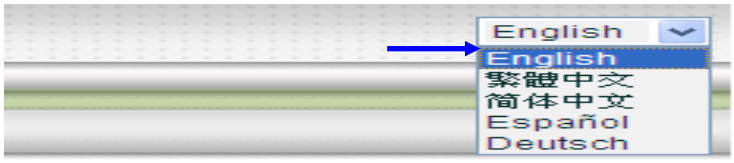
Browse to Activate the Setup Wizard

Type in the IP Address (http://192.168.123.254)

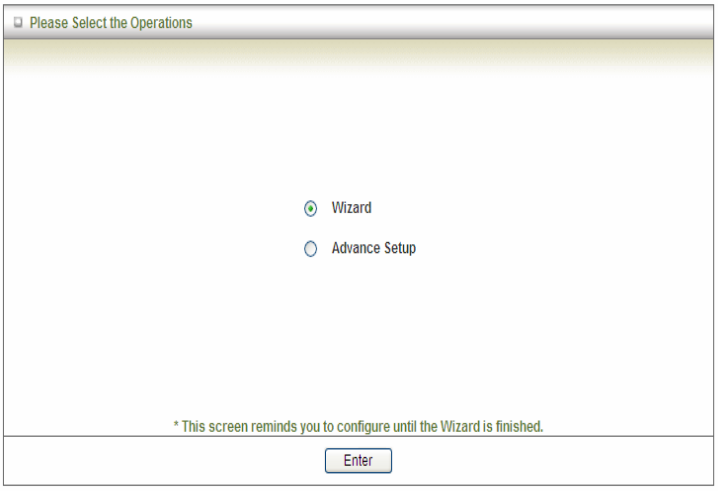


Type in the default password “admin” in the System Password and then click ‘login’ button.

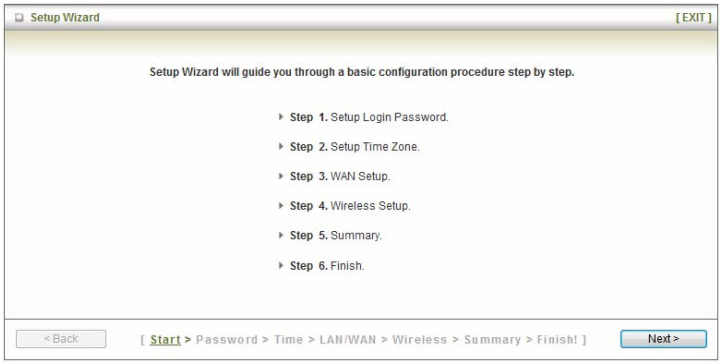
Select your language.



Select “Wizard” for basic settings with simple way.

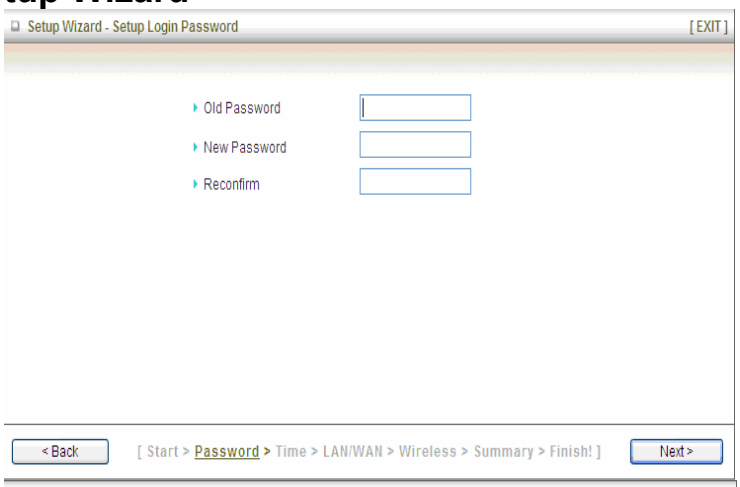


Press “Next” to start the Setup Wizard.

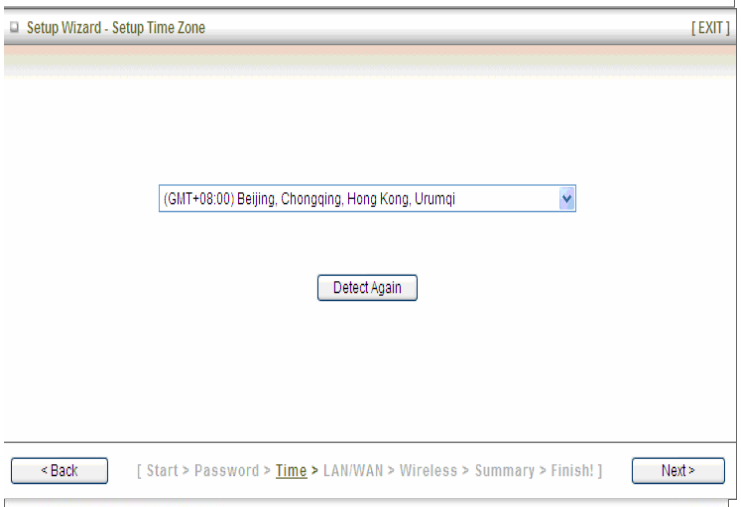


Configure with the Setup Wizard

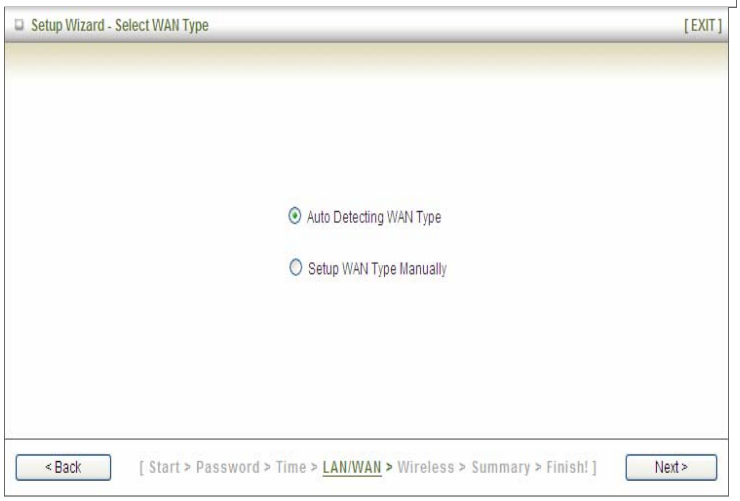
Step 1: Change System Password.
Set up your system password. (Default：admin)



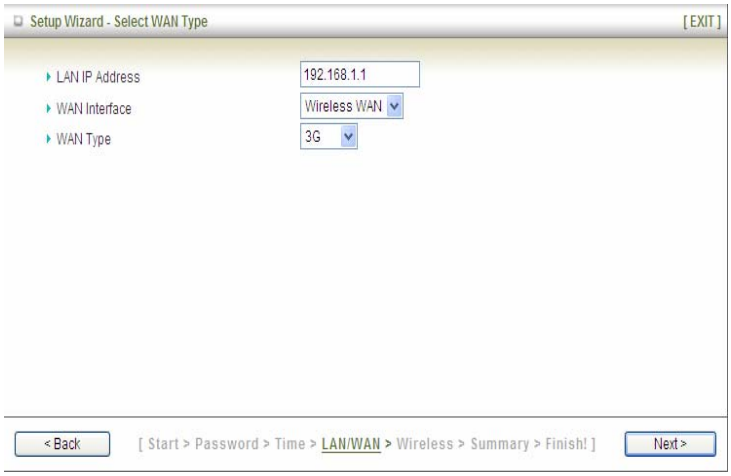
Step 2: Select Time Zone.



Step 3: Select WAN Type.
Choose Auto-Detecting or Manually to set WAN Type.



Step 4: Select Wan Type.
If you want to use 3G service as the main Internet access, please set the WAN interface as “Wireless WAN” and the WAN type as “3G”.



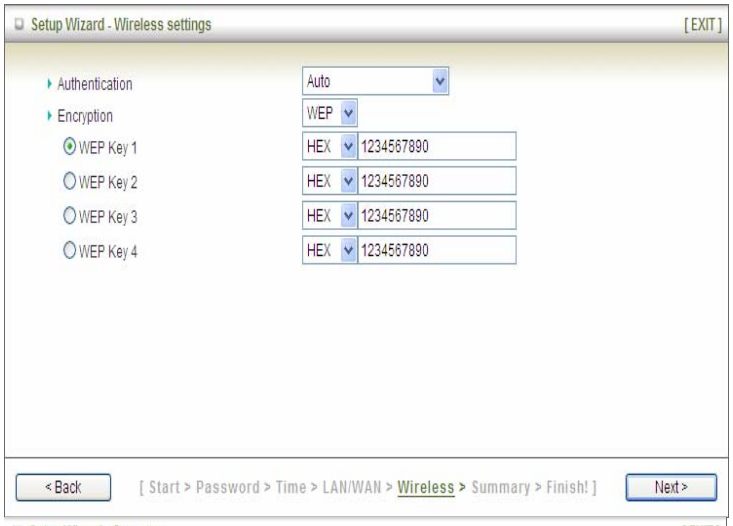
Step 5: 3G Mode.
Select Auto-Detection then click “Next” to continue.

Step 6: Set up your Wireless Network.

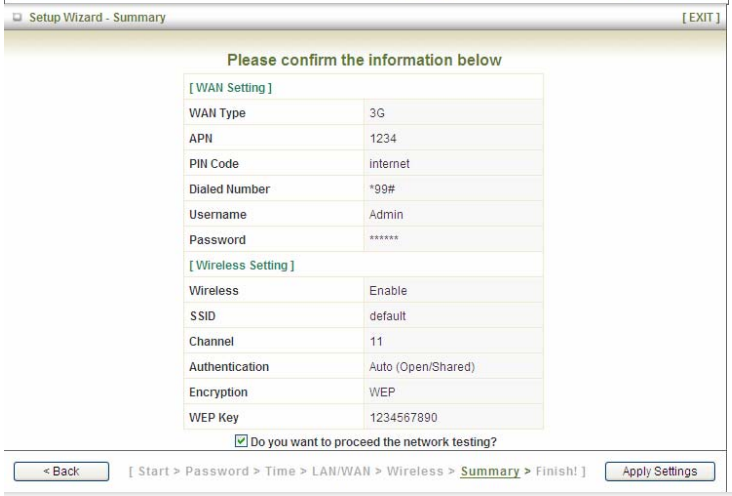
Select which wireless band you want to configure.
(e.g. Wireless 2.4G)

Setup your SSID and wireless channel.

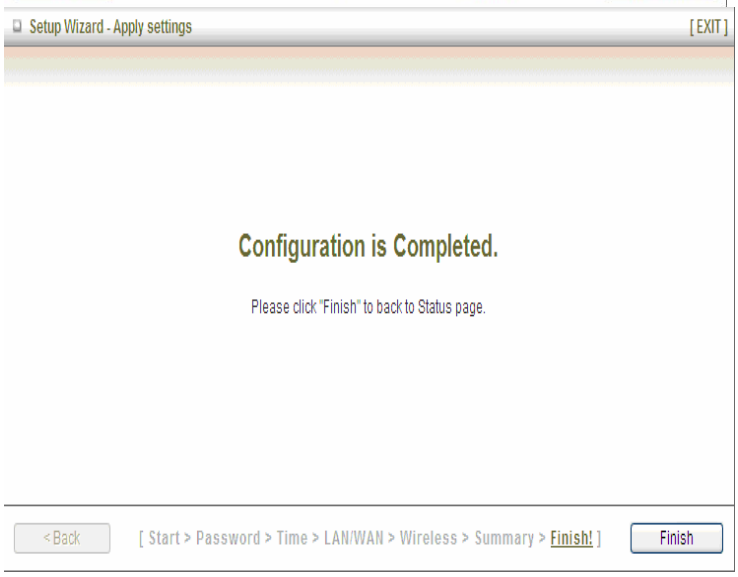
Step 7: Setup your Encryption Key here, then click"Next" to continue.



Step 8: Apply your Setting. Then click Apply Setting.



Step 9:
Click Finish to complete it.



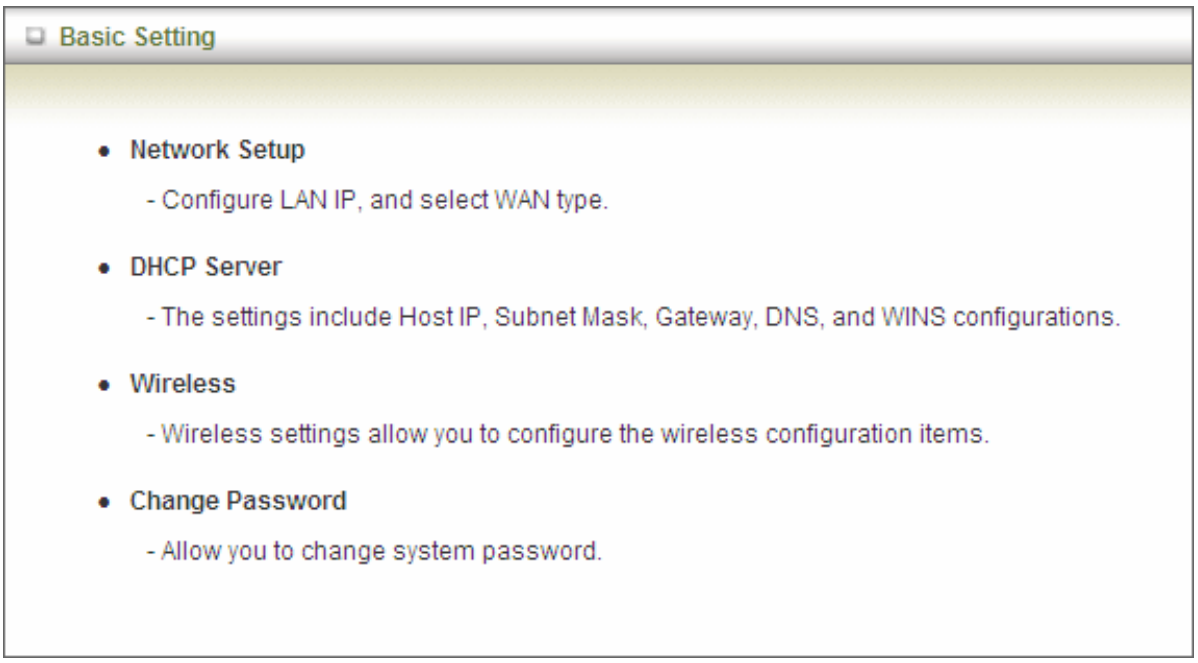
Chapter 3 Making Configuration

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: 192.168.123.254

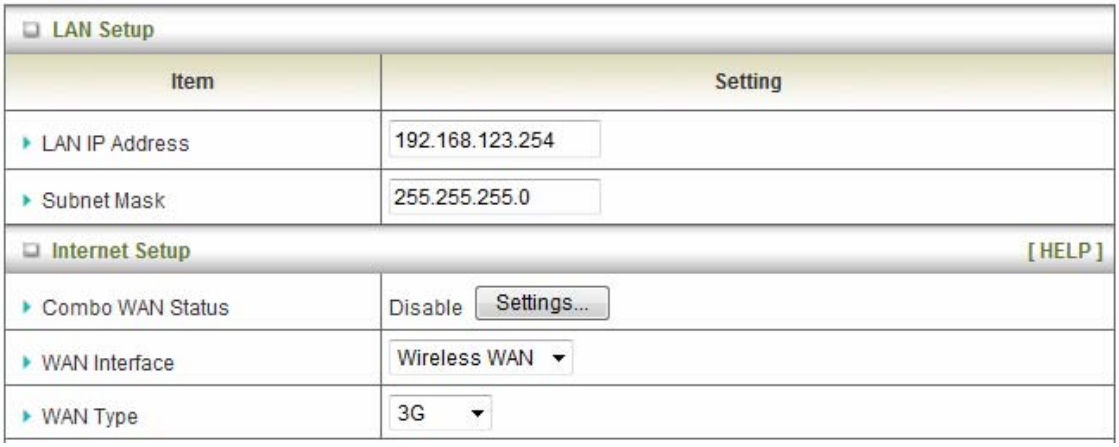
Enter the default password “admin” in the System Password and then click ‘login’ button.

Then, you can browse the “Advanced” configuration pages for configuring this device.

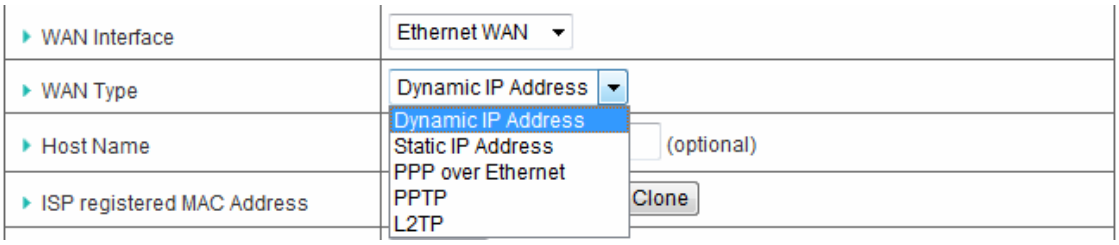
3.1 Basic Setting

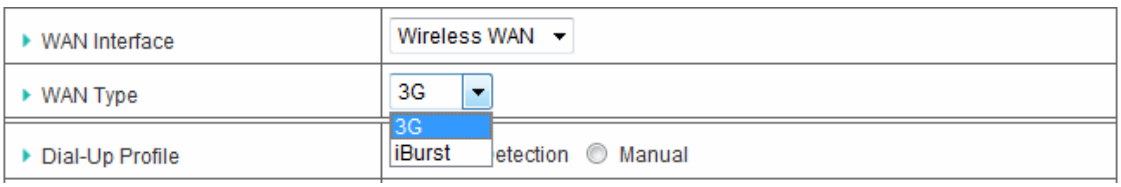


3.1.1. Network Setup



1. **LAN IP Address:** The local IP address of this device. The computers 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.
3. **Combo WAN Status:** Display status of combo WAN. With Combo WAN feature, you can choose one primary WAN connection, and set another WAN connection for backup. Otherwise, you can also choose “Load Sharing” to use Ethernet WAN and 3G WAN simultaneously. The combo WAN status will be showed here. Press “Settings” button to configure this feature.
4. **WAN Interface:** Select Ethernet WAN or Wireless WAN to continue.
5. **WAN Type**: WAN type of your Internet connection. You can choose a correct one from the following options.

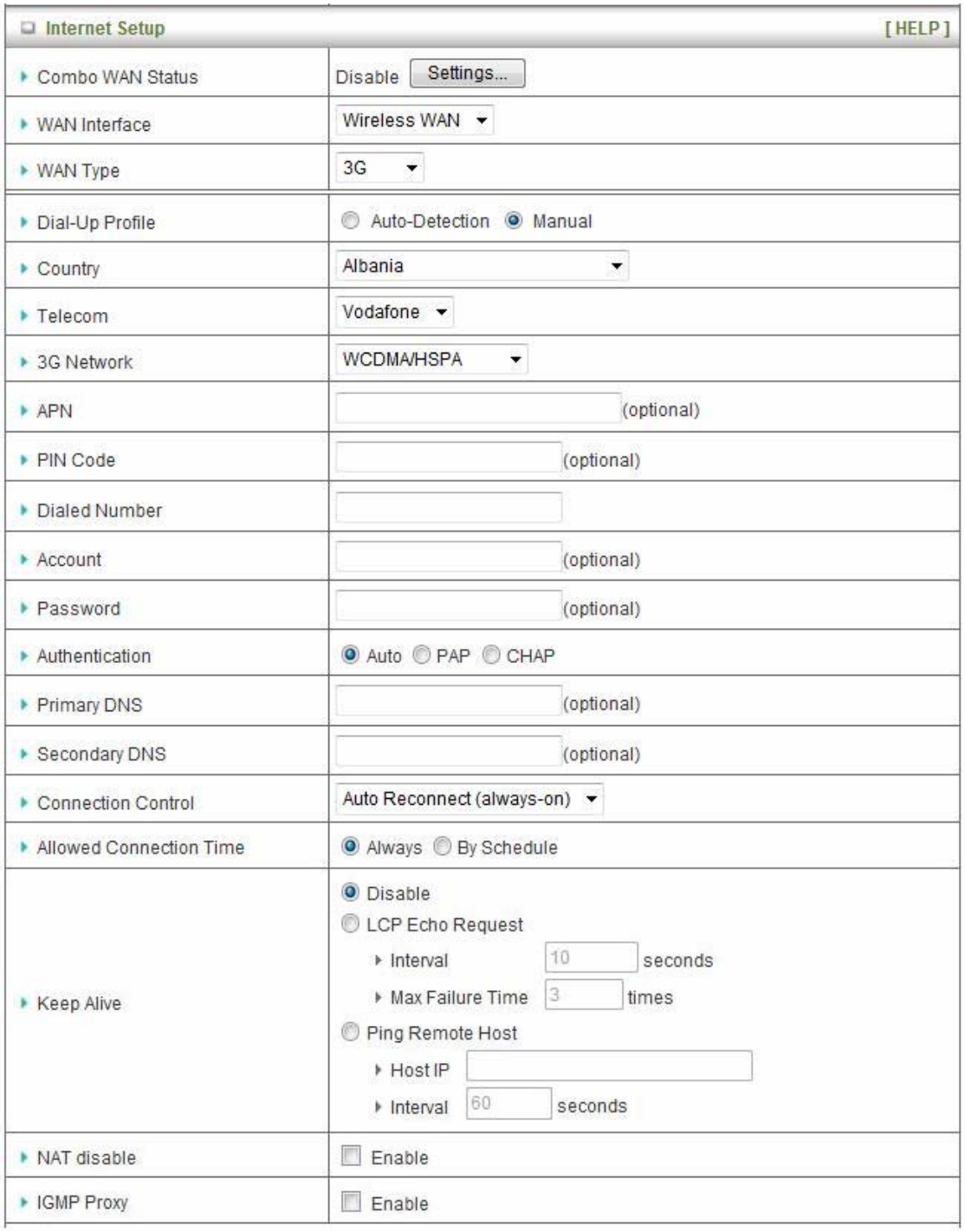




A. 3G

This device supports different WAN types of connection for users to connect to remote wireless ISP, such as 3G (WCDMA, HSxPA, HSPA+, CDMA2000, EV-DO, TD-SCDMA), iBurst, or Wi-Fi Hotspot.

Note. Users need to insert USB modem card for 3G WAN connections.



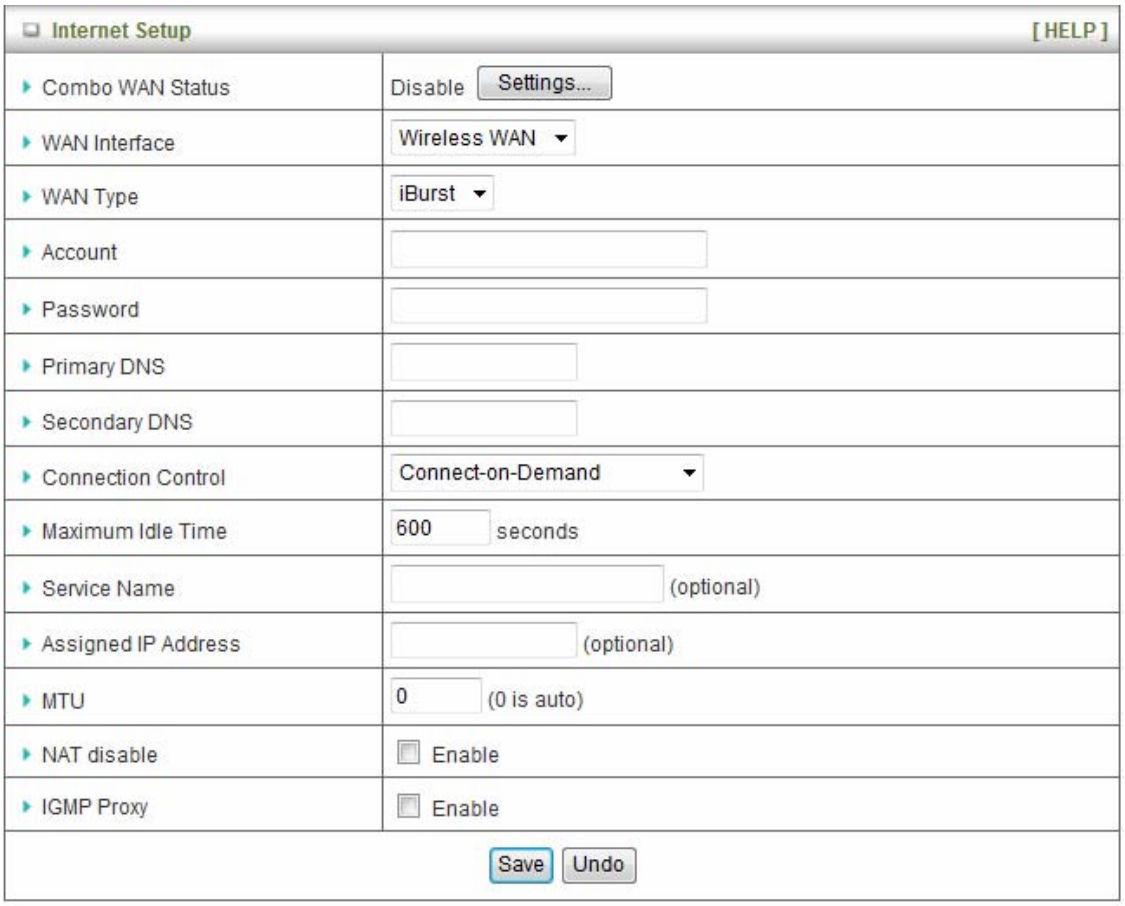
1. **WAN Type:** Choose 3G for WAN connection.
2. **Dial-Up Profile:** Please select Auto-Detection or Manual. You can choose “Auto-Detection”, and the router will try to detect and configure the required 3G service settings automatically. Otherwise, you can select “Manual”, and manually fill in the required 3G service settings provided by your carrier or ISP.
3. **Country*:** select your country.
4. **Telecom*:** select your telecom.
5. **3G Network*:** select the 3G network
6. **APN*:** APN information for your 3G data card. It will show a value after you choose country and telecom. You can also change it manually.
7. **PIN Code:** Enter the PIN Code for your SIM card if required. (Optional)
8. **Dialed Number*:** It will show a value after you choose country and telecom. You can also change it manually.
9. **Account*:** The user name for 3G connection. It will show a value after you choose country and telecom. You can also change it manually.
10. **Password*:** The password for 3G connection. It will show a value after you choose country and telecom. You can also change it manually.
11. **Authentication*:** Choose authentication of 3G connection. You can leave it as “Auto” if you are not sure.
12. **Primary DNS*:** You can assign a Primary DNS server if required. (Optional)
13. **Secondary DNS*:** You can assign a Secondary DNS server if required. (Optional)
14. **Connection Control:** There are 3 options to start connection:
    - Auto Reconnect (Always-on): The device will always try to link to Internet.
    - Connect-on-demand: The device won’t try to connect to Internet until LAN PCs or devices try to go to Internet. Once Internet connection is established, this device will drop the connection if maximum idle time is reached.
    - Manually: The device won’t try to connect to Internet until users press “connect” button at Status page. Once Internet connection is established, this device will drop the connection if maximum idle time is reached.
15. **Allowed Connection Time:** You can limit WAN connection in a period of time if required.
16. **Keep Alive:** There are three options for keep alive feature as below.
    - Disable: Disable keep alive feature.
    - LCP Echo Request: The device will constantly send LCP packets for keeping alive. Enter the time interval and the maximum failure count.
    - Ping Remote Host: Enter the Remote host IP address and the time interval to send the ping packets for keeping alive.
17. **NAT Disable:** You can disable NAT feature if required.
18. **IGMP Proxy:** Enable this feature allows multicast stream (e.g. IPTV stream) to pass-through

this device.

Note. The items with * above are only available when choosing Manual for Dial-up Profile.

B. iBurst

Note. Users need to insert USB modem card for iBurst WAN connections.

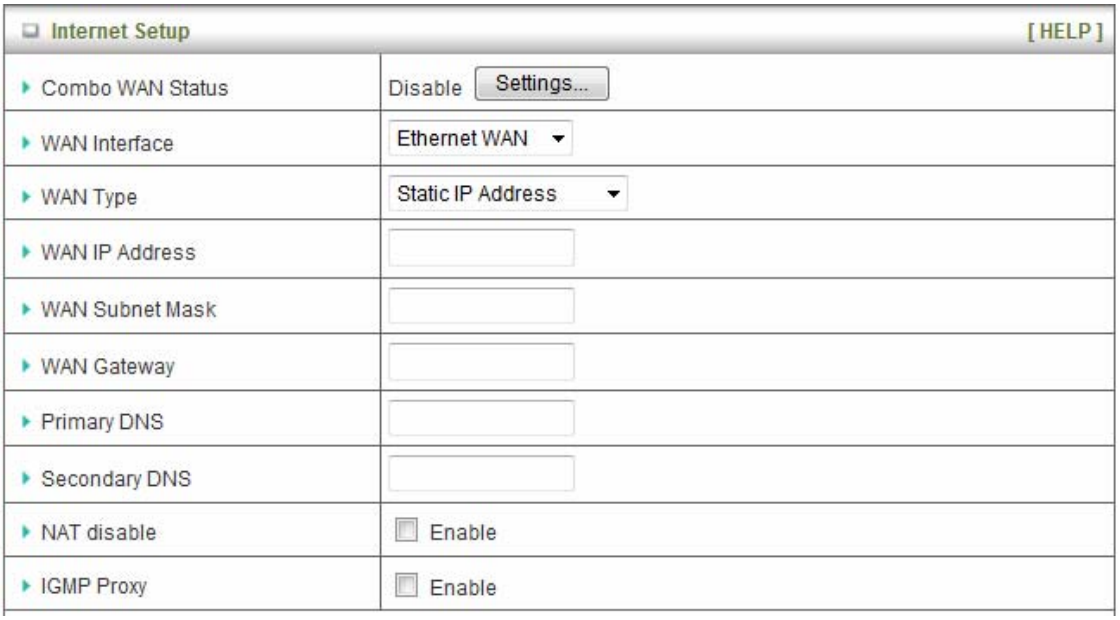


1. **WAN Type:** Choose iBurst for WAN connection.
2. **Account:** Enter the User Name for iBurst connection.
3. **Password:** Enter new Password for iBurst connection.
4. **Primary DNS:** You can assign a Primary DNS server if required. (Optional)
5. **Secondary DNS:** You can assign a Secondary DNS server if required. (Optional)
6. **Connection Control:** There are 3 options to start connection:
   - Auto Reconnect (Always-on): The device will always try to link to Internet.
   - Connect-on-demand: The device won't try to connect to Internet until LAN PCs or devices try to go to Internet. Once Internet connection is established, this device will drop the connection if maximum idle time is reached.

- Manually: The device won't try to connect to Internet until users press "connect" button at Status page. Once Internet connection is established, this device will drop the connection if maximum idle time is reached.

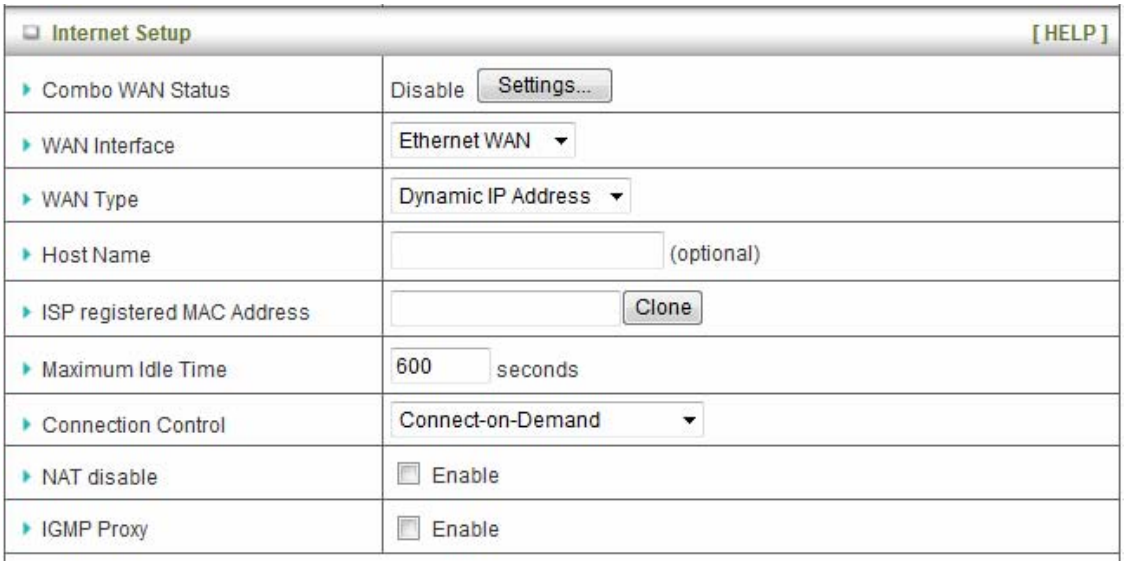
7. **Maximum Idle Time:** The amount of time of inactivity before disconnecting Internet connection. Set it to zero, or choosing "Auto-reconnect" mode to disable this feature.
8. **Service Name:** Input the service name if your ISP requires it. (Optional)
9. **Assigned IP Address:** Input a IP address if your ISP requires it. (Optional)
10. **Maximum Transmission Unit (MTU):** You can change MTU value if required. The default MTU value is set to 0 (auto).
11. **NAT disable:** You can disable NAT feature if required.
12. **IGMP Proxy:** Enable this feature allows multicast stream (e.g. IPTV stream) to pass-through this device.

C. Static IP Address



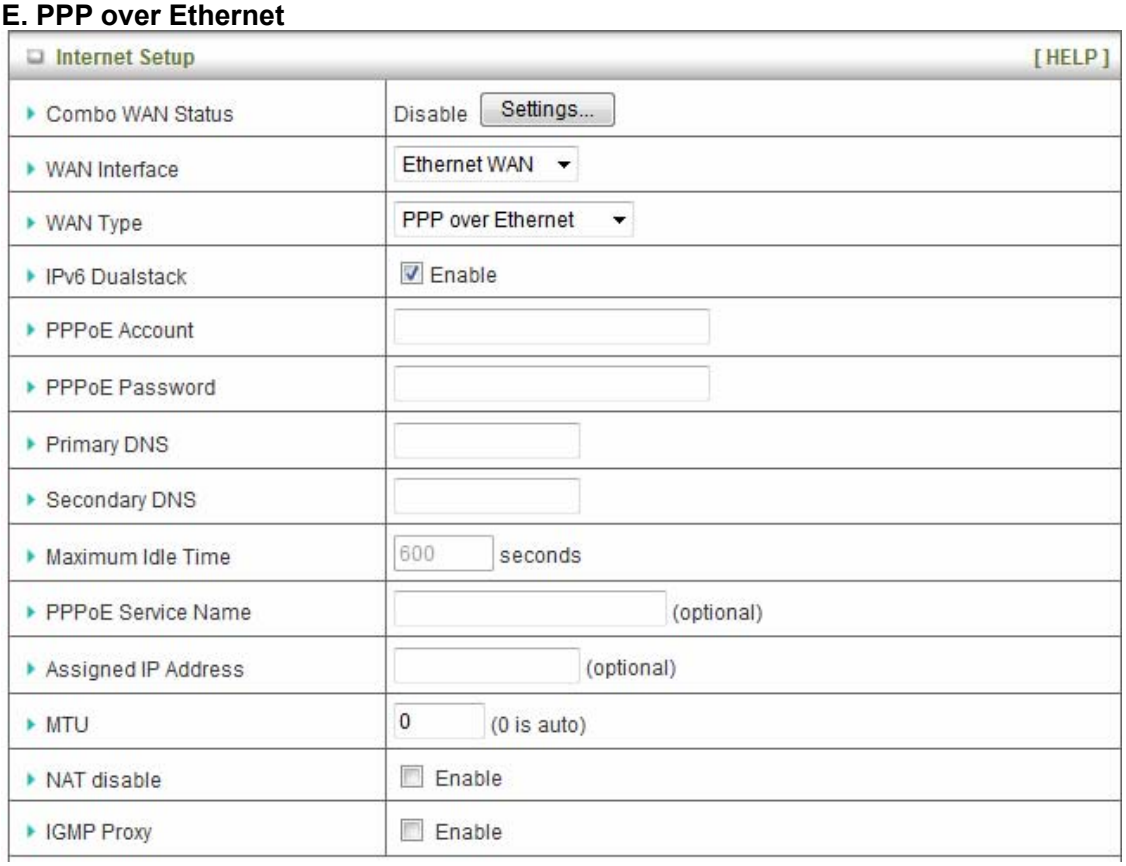
1. **WAN Type:** Choose Static IP Address.
2. **WAN IP Address:** Input the IP address you got from ISP.
3. **Subnet Mask:** Input the subnet mask of IP address you got from ISP.
4. **WAN Gateway:** Input the IP address of WAN gateway you got from ISP.
5. **Primary DNS:** Input the IP address of primary DNS you got from ISP.
6. **Secondary DNS:** Input the IP address of secondary DNS you got from ISP.
7. **NAT disable:** You can disable NAT feature if required.
8. **IGMP Proxy:** Enable this feature allows multicast stream (e.g. IPTV stream) to pass-through this device.

D. Dynamic IP Address



1. **WAN Type:** Choose Dynamic IP Address.
2. **Host Name**: Optional, required by some ISPs, for example, @Home.
3. **ISP registered MAC Address**: Some ISP (Cable company) will record your MAC address on PC. You can press “Clone” button to copy the MAC address on your PC here, or you can input it manually.
4. **Maximum Idle Time:** The amount of time of inactivity before disconnecting Internet connection. Set it to zero, or choosing “Auto-reconnect” mode to disable this feature.
5. **Connection Control:** There are 3 options to start connection:
   - Auto Reconnect (Always-on): The device will always try to link to Internet.
   - Connect-on-demand: The device won’t try to connect to Internet until LAN PCs or devices try to go to Internet. Once Internet connection is established, this device will drop the connection if maximum idle time is reached.
   - Manually: The device won’t try to connect to Internet until users press “connect” button at Status page. Once Internet connection is established, this device will drop the connection if maximum idle time is reached.
6. **NAT disable:** You can disable NAT feature if required.
7. **IGMP Proxy:** Enable this feature allows multicast stream (e.g. IPTV stream) to pass-through this device.

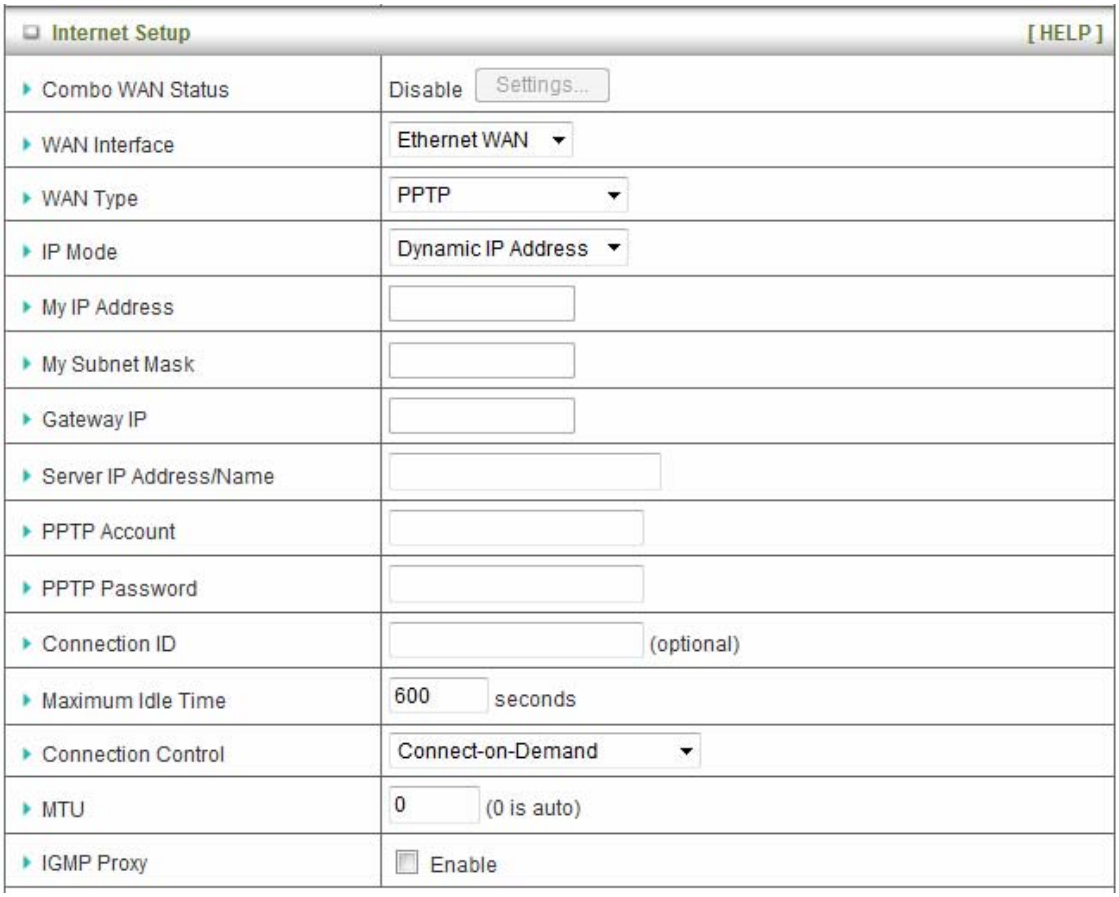
E. PPP over Ethernet



1. **WAN Type:** Choose PPP over Ethernet.
2. **IPv6 Dual Stack:** If your ISP supports IPv6 dual stack, you can check this check box to get an IPv4 address and an IPv6 address via one PPPoE connection. After you check this check box, you also need to enable IPv6 function at **Advanced Setting->IPv6** setting page.
3. **PPPoE Account** and **Password**: The account and password your ISP assigned to you.
4. **Primary DNS:** You can indicate IP address of primary DNS if required.
5. **Secondary DNS:** You can indicate IP address of secondary DNS if required.
6. **Connection Control:** There are 3 options to start connection:
   - Auto Reconnect (Always-on): The device will always try to link to Internet.
   - Connect-on-demand: The device won't try to connect to Internet until LAN PCs or devices try to go to Internet. Once Internet connection is established, this device will drop the connection if maximum idle time is reached.
   - Manually: The device won't try to connect to Internet until users press "connect" button at Status page. Once Internet connection is established, this device will drop the connection if maximum idle time is reached.
7. **Maximum Idle Time**: the amount of time of inactivity before disconnecting your PPPoE session. Set it to zero or enable "Auto-reconnect" to disable this feature.

8. **PPPoE Service Name**: Optional. Input the service name if your ISP requires it.
9. **Assigned IP Address:** You can input a IP address if you got a fix IP address from ISP.
10. **Maximum Transmission Unit (MTU):** Most ISP offers MTU value to users. The default MTU value is 0 (auto).
11. **NAT disable:** You can disable NAT feature if required.
12. **IGMP Proxy:** Enable this feature allows multicast stream (e.g. IPTV stream) to pass-through this device.

F. PPTP

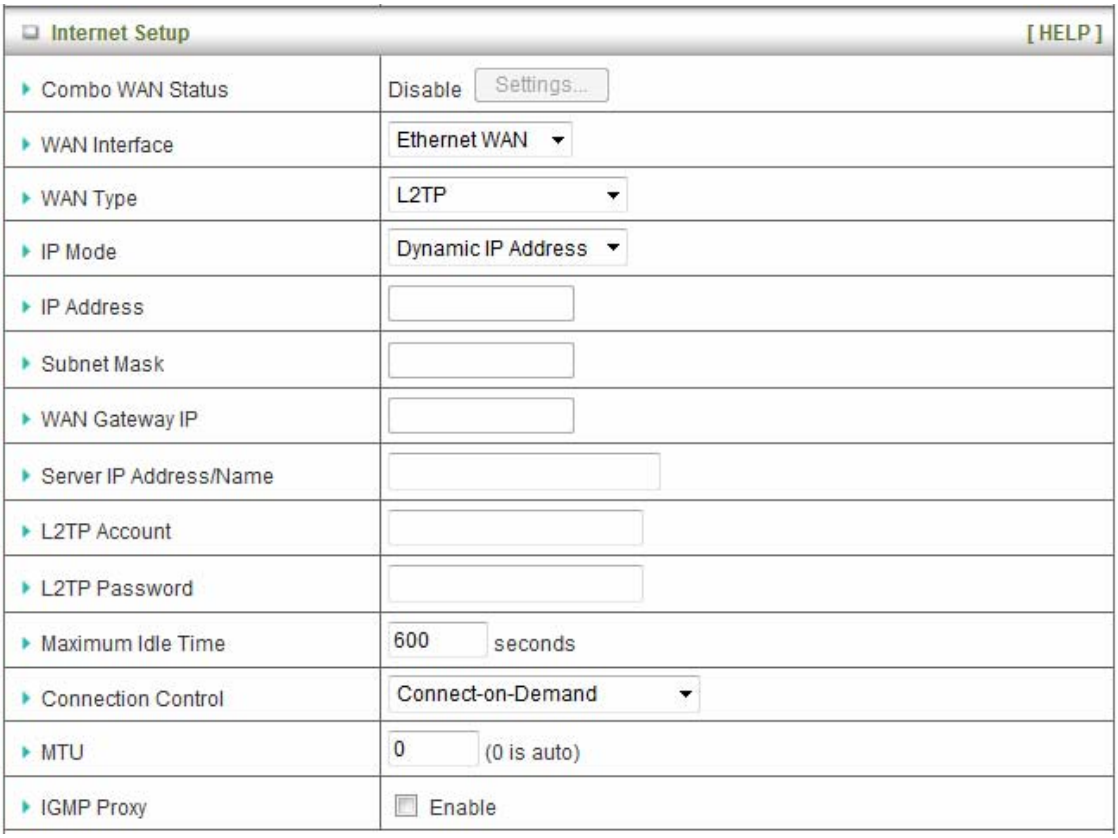


1. **WAN Type:** Choose PPTP.
2. **IP Mode**: You can select “Static IP Address” or “Dynamic IP Address”.
3. **My IP Address***, **My Subnet Mask*, and Gateway IP***: The IP address, subnet mask, and IP address of gateway your ISP assigned to you.
4. **Server IP Address/Name**: The IP address of the PPTP server.
5. **PPTP Account** and **Password**: The account and password your ISP assigned to you.
6. **Connection ID**: Optional. Input the connection ID if your ISP requires it.
7. **Connection Control:** There are 3 options to start connection:
   - Auto Reconnect (Always-on): The device will always try to link to Internet.
   - Connect-on-demand: The device won’t try to connect to Internet until LAN PCs or devices try to go to Internet. Once Internet connection is established, this device will drop the connection if maximum idle time is reached.
   - Manually: The device won’t try to connect to Internet until users press “connect” button at Status page. Once Internet connection is established, this device will drop the connection if maximum idle time is reached.
8. **Maximum Idle Time**: the time of no activity to disconnect your PPTP session. Set it to zero or enable “Auto-reconnect” to disable this feature.

9. **Maximum Transmission Unit (MTU)**: Most ISP offers MTU value to users. The default MTU value is 0 (auto).
10. **IGMP Proxy:** Enable this feature allows multicast stream (e.g. IPTV stream) to pass-through this device.

Note. The items with * above are only available when choosing Static IP Address in IP mode.

G. L2TP



1. **WAN Type:** Choose L2TP.
2. **IP Mode**: You can select “Static IP Address” or “Dynamic IP Address”.
3. **My IP Address***, **My Subnet Mask*, and Gateway IP***: The IP address, subnet mask, and IP address of gateway your ISP assigned to you.
4. **Server IP Address/Name**: The IP address of the L2TP server.
5. **L2TP Account** and **Password**: The account and password your ISP assigned to you.
6. **Connection ID**: Optional. Input the connection ID if your ISP requires it.
7. **Connection Control:** There are 3 options to start connection:
   - Auto Reconnect (Always-on): The device will always try to link to Internet.
   - Connect-on-demand: The device won’t try to connect to Internet until LAN PCs or devices try to go to Internet. Once Internet connection is established, this device will drop the connection if maximum idle time is reached.
   - Manually: The device won’t try to connect to Internet until users press “connect” button at Status page. Once Internet connection is established, this device will drop the connection if maximum idle time is reached.
8. **Maximum Idle Time**: the time of no activity to disconnect your L2TP session. Set it to zero or enable “Auto-reconnect” to disable this feature.
9. **Maximum Transmission Unit (MTU)**: Most ISP offers MTU value to users. The default

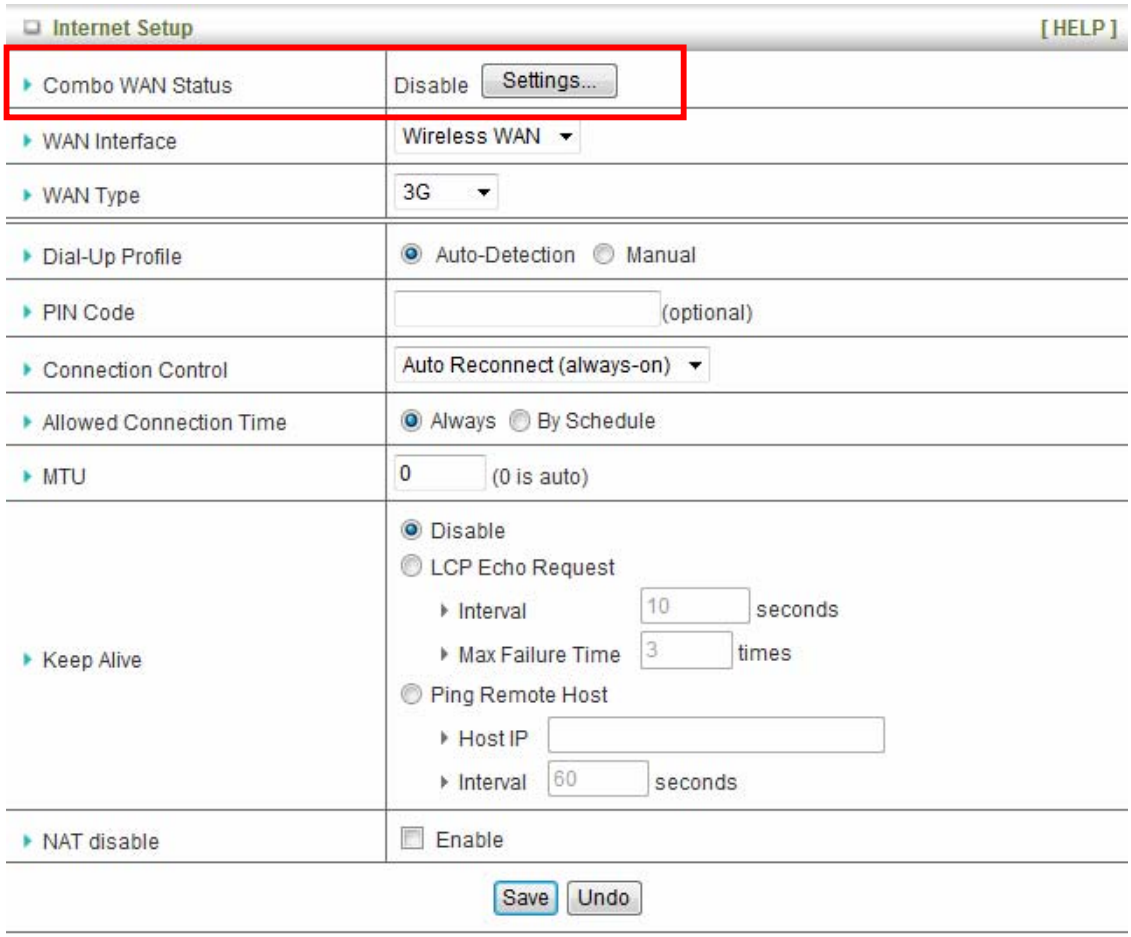
MTU value is 0 (auto).

10. **IGMP Proxy:** Enable this feature allows multicast stream (e.g. IPTV stream) to pass-through this device.

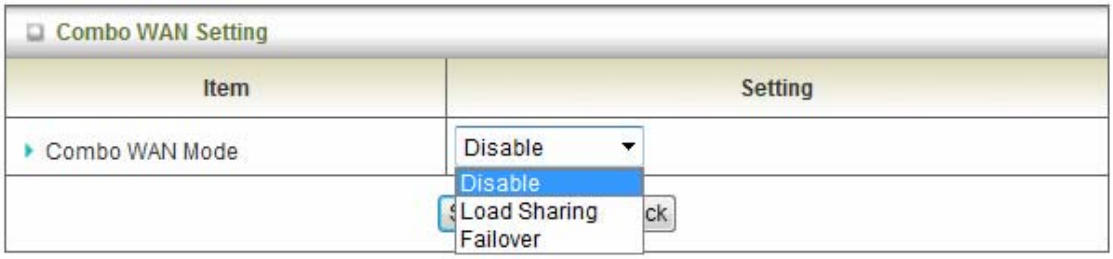
Note. The items with * above are only available when choosing Static IP Address in IP mode.

H. Combo WAN Setting

With Combo WAN feature, you can choose one primary WAN connection, and set another WAN connection for backup. Otherwise, you can also choose “Load Sharing” to use Ethernet WAN and 3G WAN simultaneously. The combo WAN status will be showed at Internet Setup page. Press “Settings” button to configure this feature.

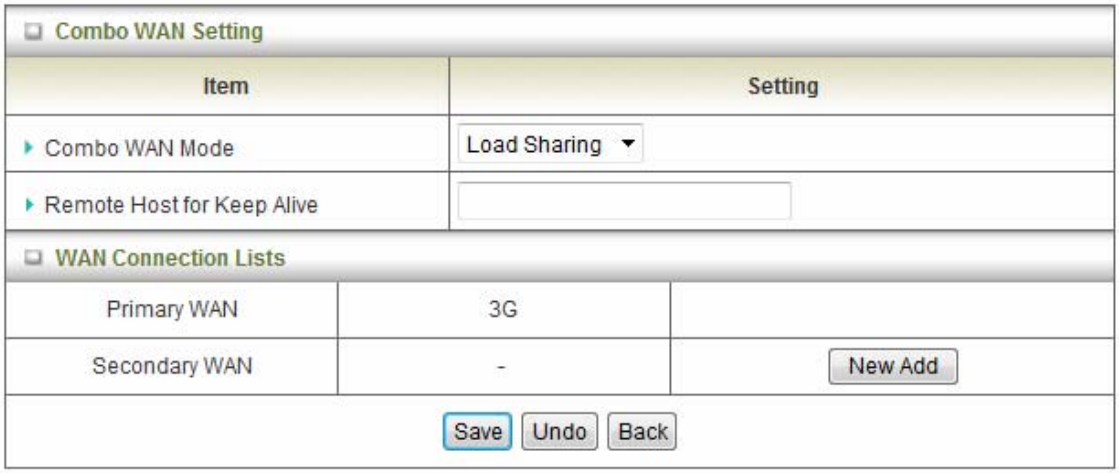


At Combo WAN setting page, you can choose Disable, Load Sharing, or Failover options.
This Combo WAN feature will be deactivated if you select “Disable” from the list.

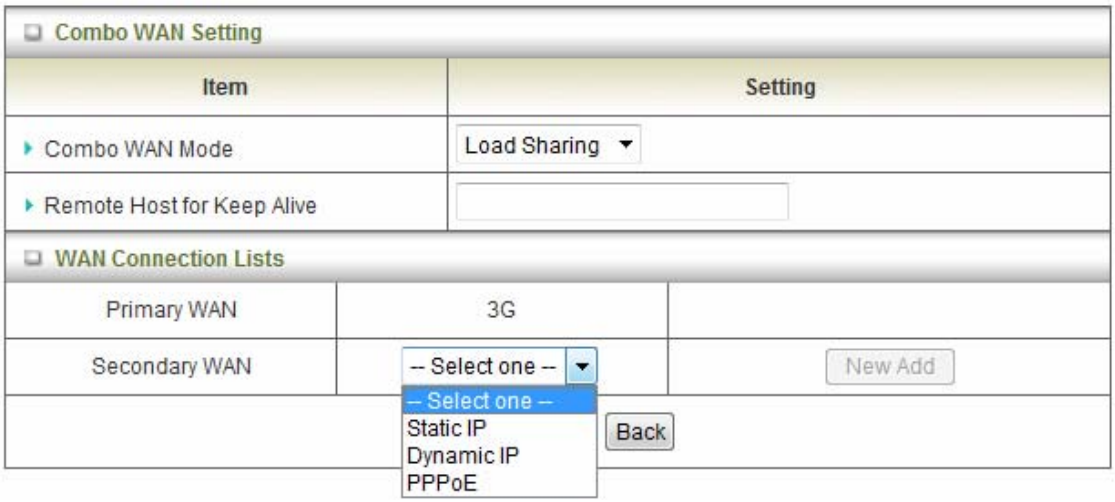


Load Sharing

The feature of Load Sharing will activate 3G WAN and Ethernet WAN simultaneously.

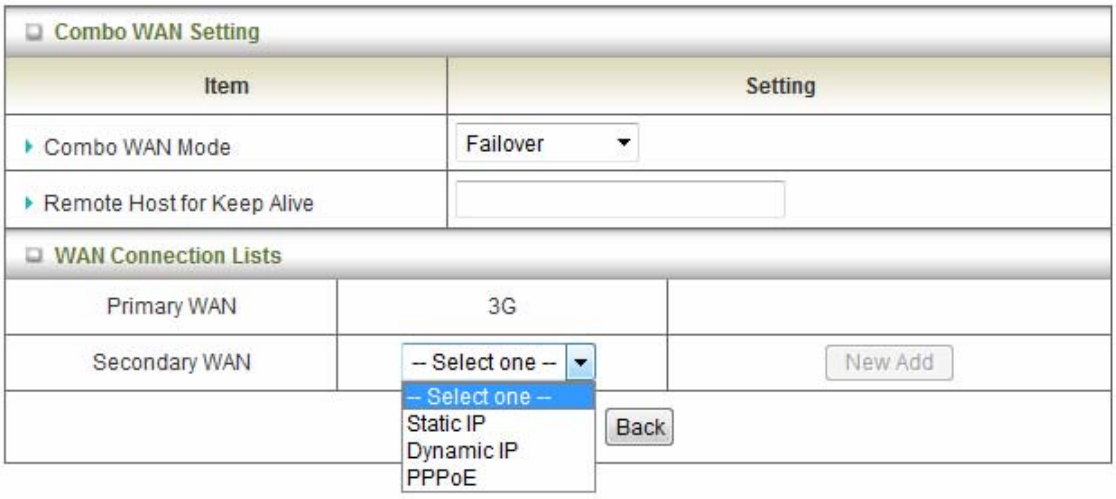


1. **Combo WAN Mode**: Choose Load Sharing mode.
2. **Remote Host for Keep Alive**: Type an IP address or domain name of remote host to detect if Internet connection is alive.
3. **Primary WAN**: The primary WAN is the WAN type you set at Internet Setup page.
4. **Secondary WAN**: Press “New Add” button to add the secondary WAN. If the primary WAN is 3G or iBurst, then you can choose one of Static IP, Dynamic IP, and PPPoE as the secondary WAN. However, 3G can be the secondary WAN if primary WAN is Static IP, Dynamic IP, or PPPoE.



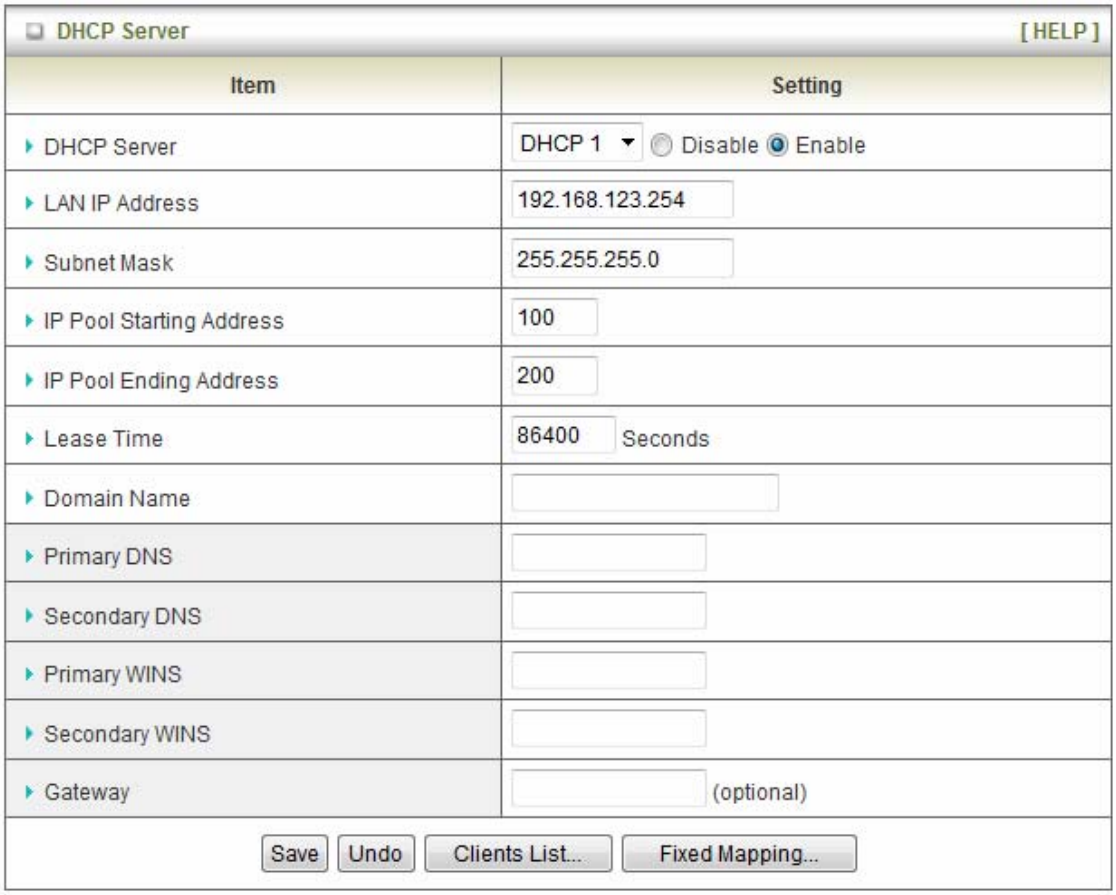
Failover

With this function enabled, when the primary WAN connection is broken, the device will automatically switch to secondary WAN connection and keep you connected to Internet. Meanwhile, if the device detects that the primary WAN connection is recovered, your Internet connection will be switched from secondary WAN back to primary WAN.



1. **Combo WAN Mode**: Choose Failover mode.
2. **Remote Host for Keep Alive**: Type an IP address or domain name of remote host to detect if Internet connection is alive.
3. **Primary WAN**: The primary WAN is the WAN type you set at Internet Setup page.
4. **Secondary WAN**: Press “New Add” button to add the secondary WAN. If the primary WAN is 3G or iBurst, then you can choose one of Static IP, Dynamic IP, and PPPoE as the secondary WAN. However, 3G can be the secondary WAN if primary WAN is Static IP, Dynamic IP, or PPPoE.

3.1.2. DHCP Server

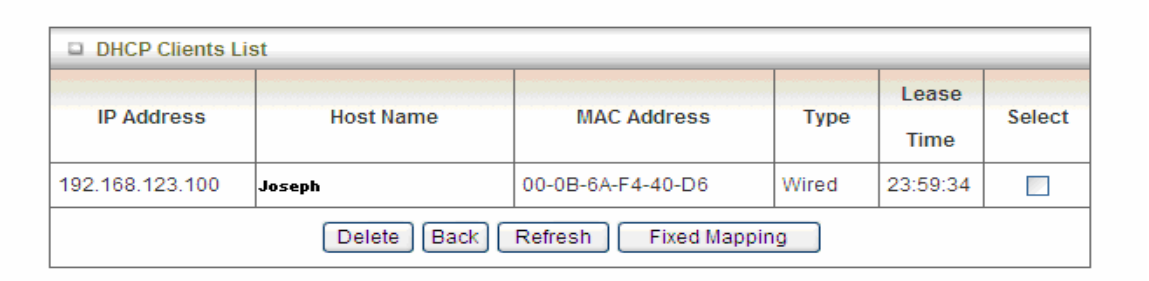


1. **DHCP Server:** You can have total four (DHCP1~DHCP4) different settings of DHCP server configurations on this device. If you divide LAN network into different groups via VLAN ID (Please refer to **Advanced Setting->VLAN** for detail), you can have different DHCP server settings for each of them.
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.
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

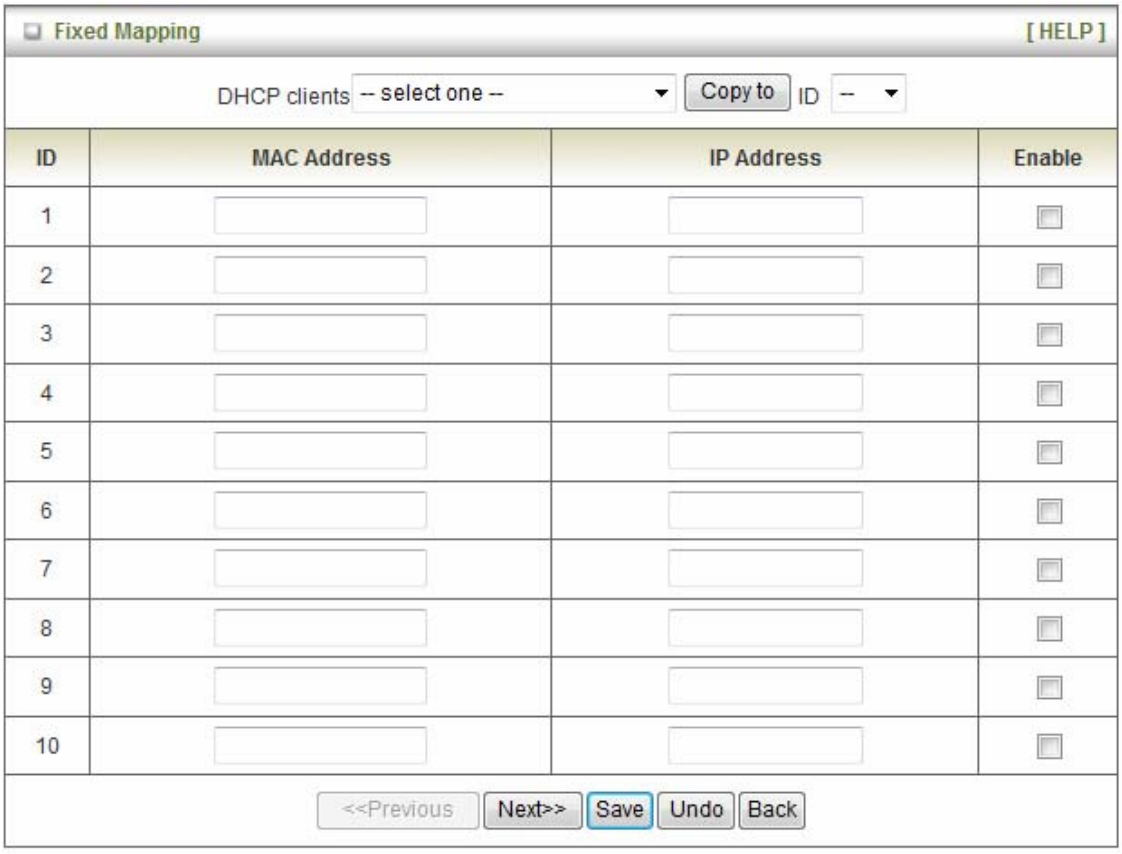
offers an IP to your PC.

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

Press “Clients List” and the list of DHCP clients will be shown consequently.

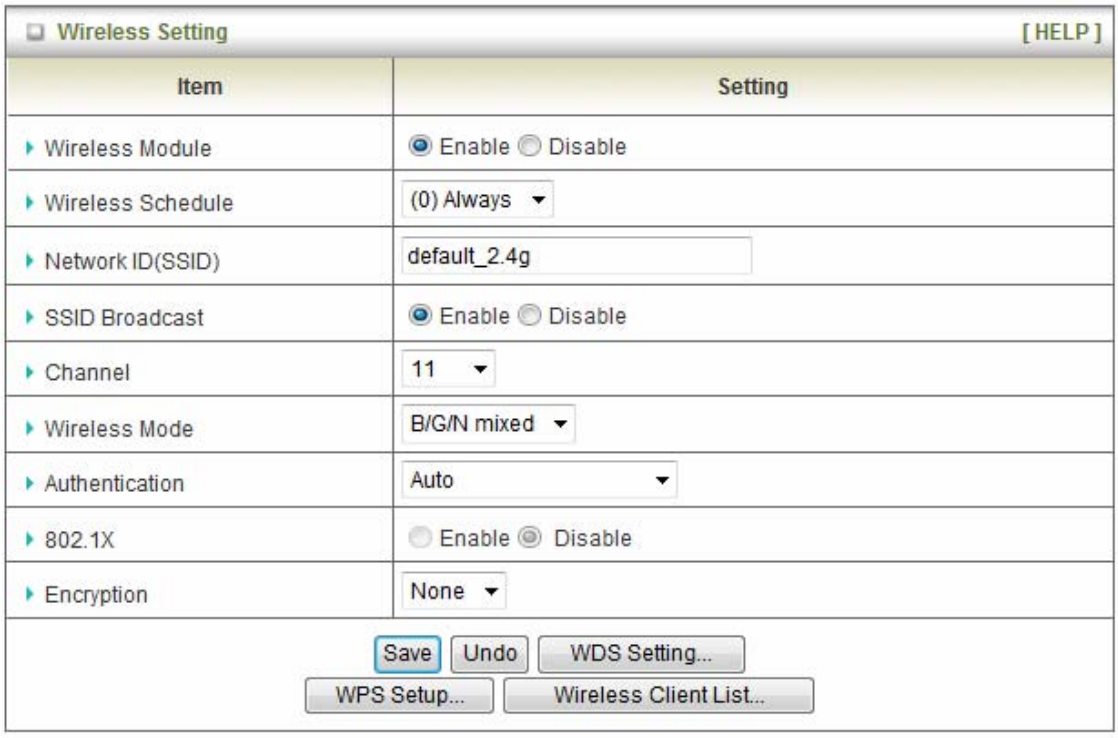


Press “Fixed Mapping” and the DHCP Server will reserve the special IP for designated MAC address.



3.1.3. Wireless 2.4G Settings

Here you can configure settings for 2.4GHz wireless functions.



Wireless settings allow you to set the wireless configuration items.

1. **Wireless Module:** You can enable or disable wireless function.
2. **Wireless Schedule:** You can limit Wi-Fi functions in a period of time if required.
3. **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_2.4g”)
4. **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.
5. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is as follow: channel 1~11 for North America. (Channel 1~13 for European (ETSI); channel1~ 14 for Japan).
6. **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”.
7. **Authentication mode:** You may select one of authentication 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 and Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits.

If you select ASCII, the length of pre-share key is from 8 to 63.

Fill in the key, Ex 12345678

WPA

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server IP address or the 802.1X server’s domain-name.

Select Encryption and RADIUS Shared Key

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If you select ASCII, the length of pre-share key is from 8 to 63.

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

WPA-PSK2

WPA-PSK2 user AES and TKIP for Same the encryption, the others are same the WPA-PSK.

WPA2

WPA2 add uses AES and TKIP for encryption, the others are same the WPA.

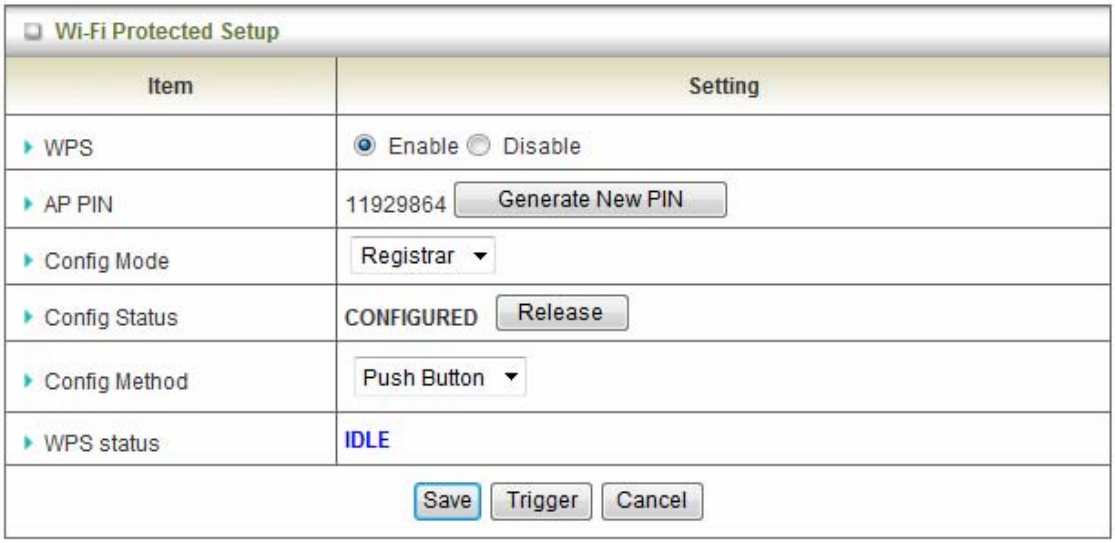
WPA-PSK/WPA-PSK2

Another encryption options for WPA-PSK-TKIP and WPA-PSK2-AES, the others are same the WPA-PSK.

WPA/WPA2

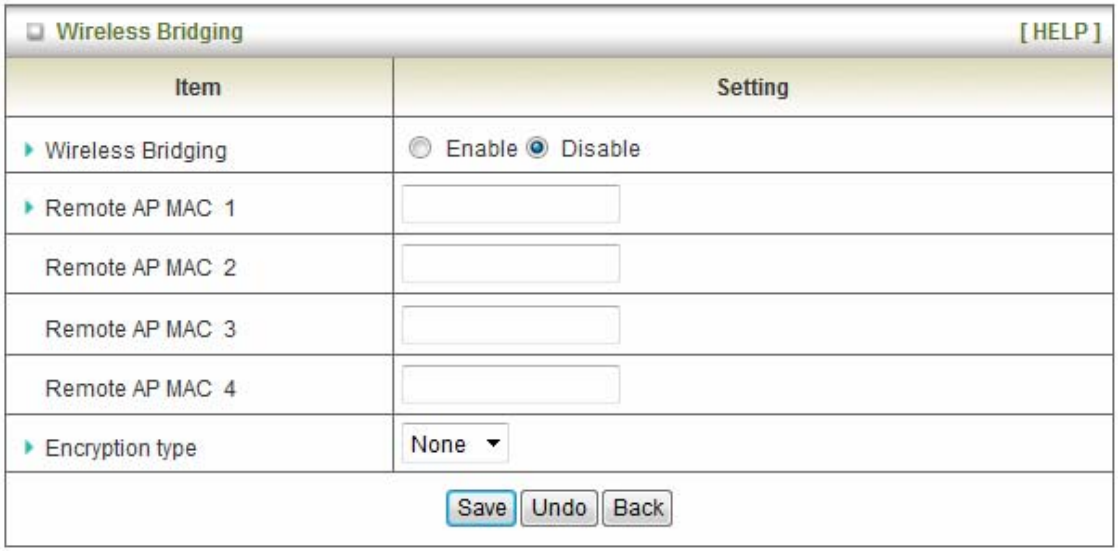
Another encryption options for WPA-TKIP and WPA2-AES, the others are same the WPA.

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



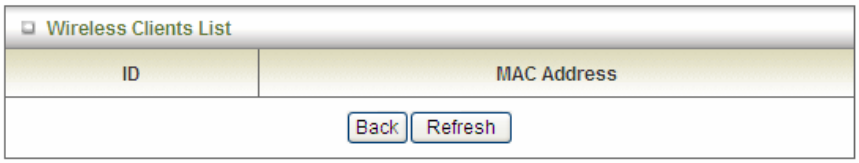
1. **WPS:** You can enable this function by selecting "Enable". WPS offers a safe and easy way to allow the wireless clients connected to your wireless network.
2. **AP PIN**: You can press Generate New Pin to get an AP PIN.
3. **Config Mode**: Select your config Mode from "Registrar" or "Enrollee".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

By pressing **"WDS Setup"**, you can connect this device to another AP via WDS connection.



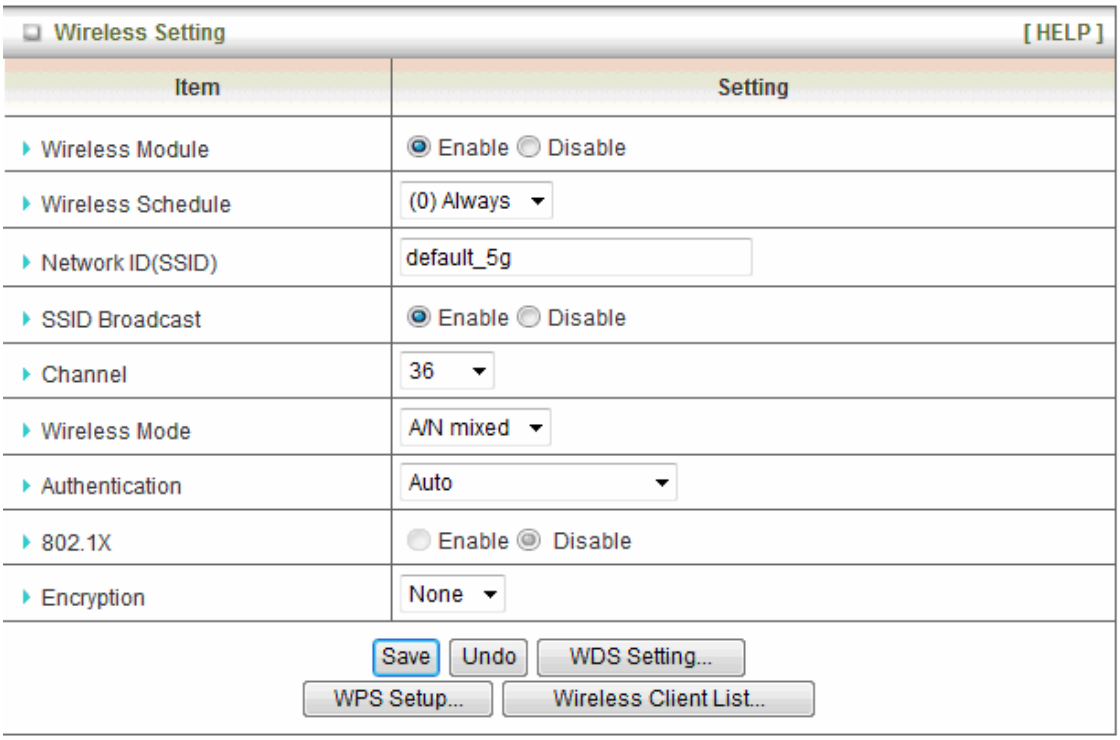
1. **Wireless Bridging:** You can enable this function by selecting "Enable".
2. **Remote AP MAC 1~4:** Enter the MAC address for remote AP that you want to connect via WDS.
3. **Encryption type:** Select the appropriate category. Once you set up that type of encryption, second LAN PC must enter the same encryption type as the first one.

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



3.1.4. Wireless 5G Settings

Here you can configure settings for 5GHz wireless functions.



Wireless settings allow you to set the wireless configuration items.

1. **Wireless Module:** You can enable or disable wireless function.
2. **Wireless Schedule:** You can limit Wi-Fi functions in a period of time if required.
3. **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_5g”)
4. **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.
5. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain.
6. **Wireless Mode:** Choose “A/N mixed”, “A only”, “N only”. The factory default setting is “A/N mixed”.
7. **Authentication mode:** You may select one of authentication 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 and Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits.

If you select ASCII, the length of pre-share key is from 8 to 63.

Fill in the key, Ex 12345678

WPA

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server IP address or the 802.1X server's domain-name.

Select Encryption and RADIUS Shared Key

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits

If you select ASCII, the length of pre-share key is from 8 to 63.

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

WPA-PSK2

WPA-PSK2 user AES and TKIP for Same the encryption, the others are same the WPA-PSK.

WPA2

WPA2 add uses AES and TKIP for encryption, the others are same the WPA.

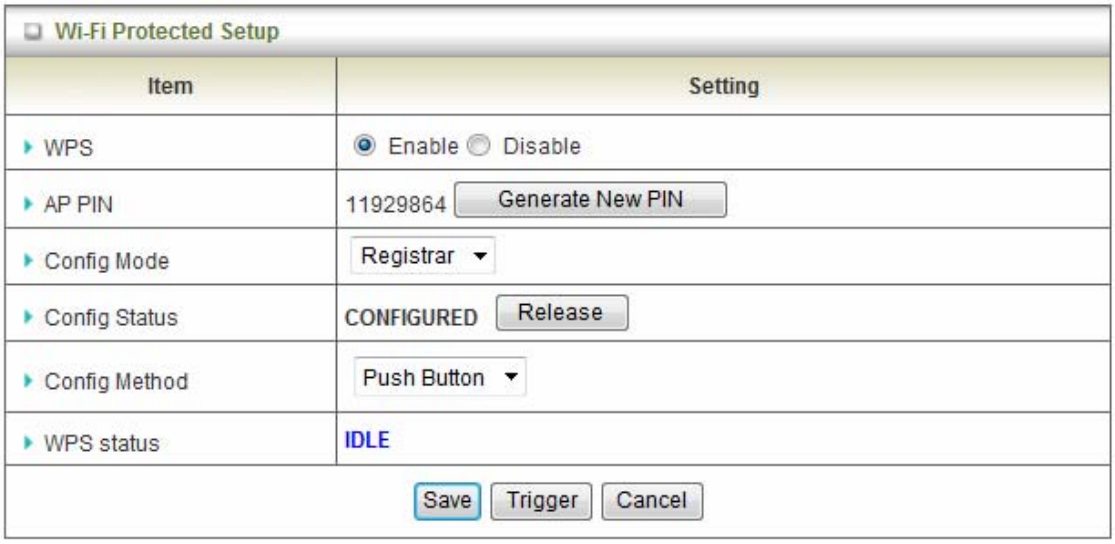
WPA-PSK/WPA-PSK2

Another encryption options for WPA-PSK-TKIP and WPA-PSK2-AES, the others are same the WPA-PSK.

WPA/WPA2

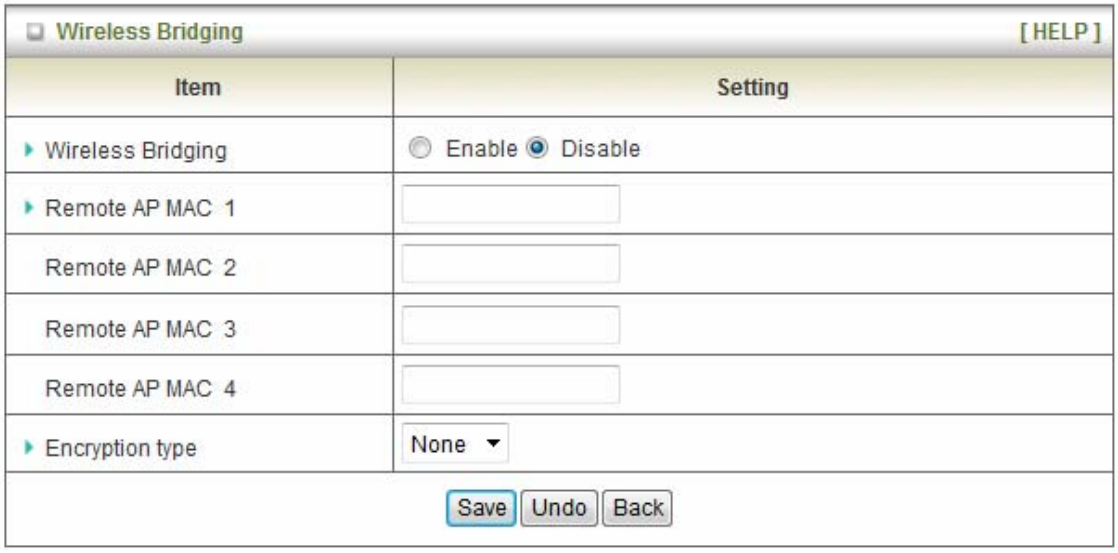
Another encryption options for WPA-TKIP and WPA2-AES, the others are same the WPA.

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



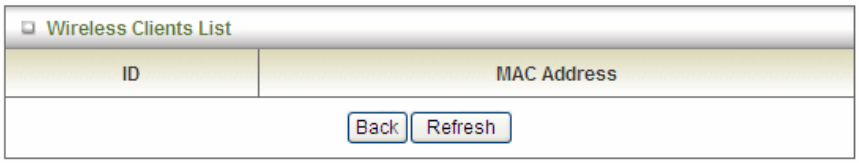
7. **WPS:** You can enable this function by selecting "Enable". WPS offers a safe and easy way to allow the wireless clients connected to your wireless network.
8. **AP PIN**: You can press Generate New Pin to get an AP PIN.
9. **Config Mode**: Select your config Mode from "Registrar" or "Enrollee".
10. **Config Status**: It shows the status of your configuration.
11. **Config Method**: You can select the Config Method here from "Pin Code" or "Push Button".
12. **WPS status**: According to your setting, the status will show "Start Process" or "No used"

By pressing **"WDS Setup"**, you can connect this device to another AP via WDS connection.

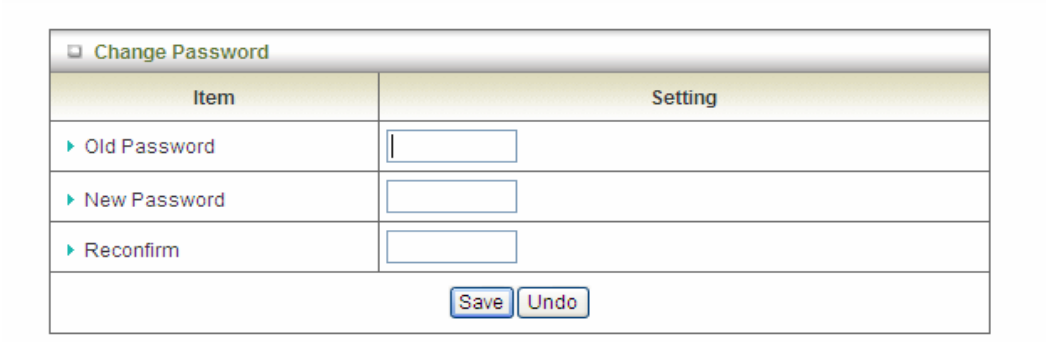


4. **Wireless Bridging:** You can enable this function by selecting "Enable".
5. **Remote AP MAC 1~4:** Enter the MAC address for remote AP that you want to connect via WDS.
6. **Encryption type:** Select the appropriate category. Once you set up that type of encryption, second LAN PC must enter the same encryption type as the first one.

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



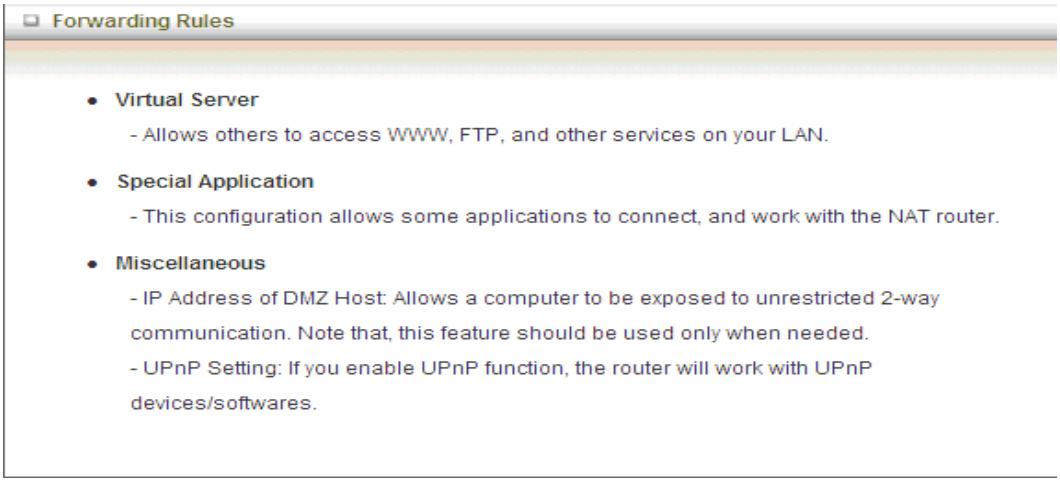
3.1.5. Change Password



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.

3.2 Forwarding Rules



3.2.1 Virtual Server

This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product 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**.

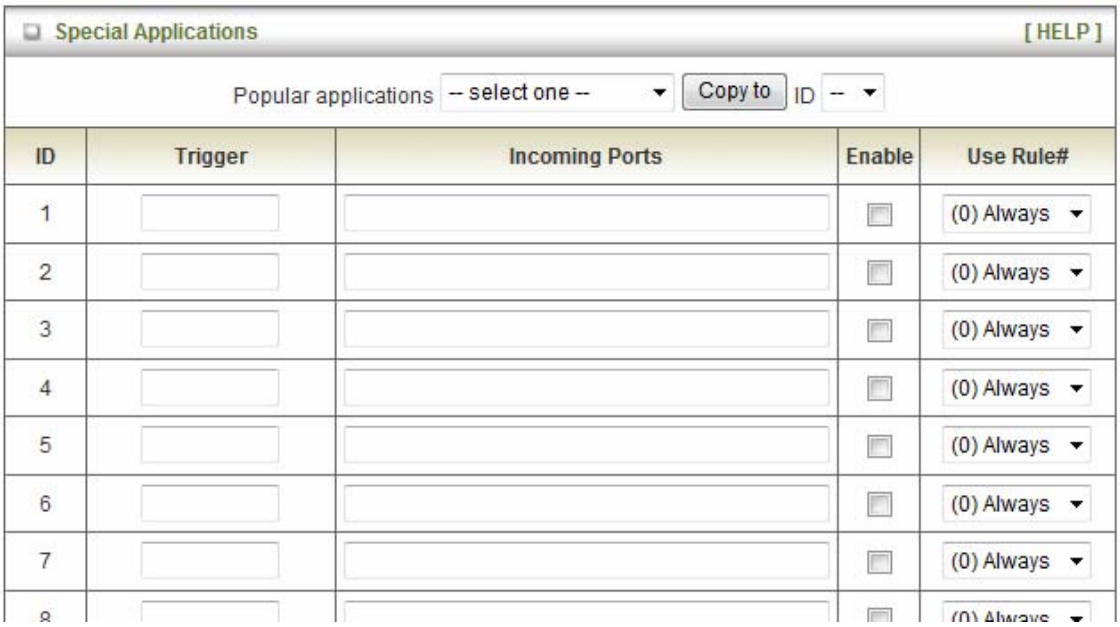
For example, if you have an FTP server (port 21) at 192.168.123.1, a Web server (port 80) at 192.168.123.2, and a VPN server at 192.168.123.6, then you need to specify the following virtual server mapping table:

Service Port	Server IP	Enable
21	192.168.123.1	V
80	192.168.123.2	V
1723	192.168.123.6	V

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

3.2.2 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.

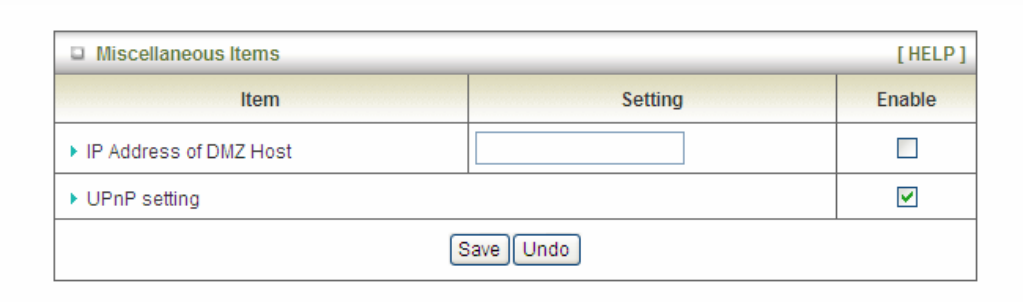


1. **Trigger:** The outbound port number issued by the application.
2. **Incoming Ports**: When the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.
3. **Enable:** Check the checkbox to activate each of rule.
4. **Use Rule#:** you can set a schedule rule for each of rule.

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

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

3.2.3 Miscellaneous



1. **IP Address of DMZ Host**

   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.

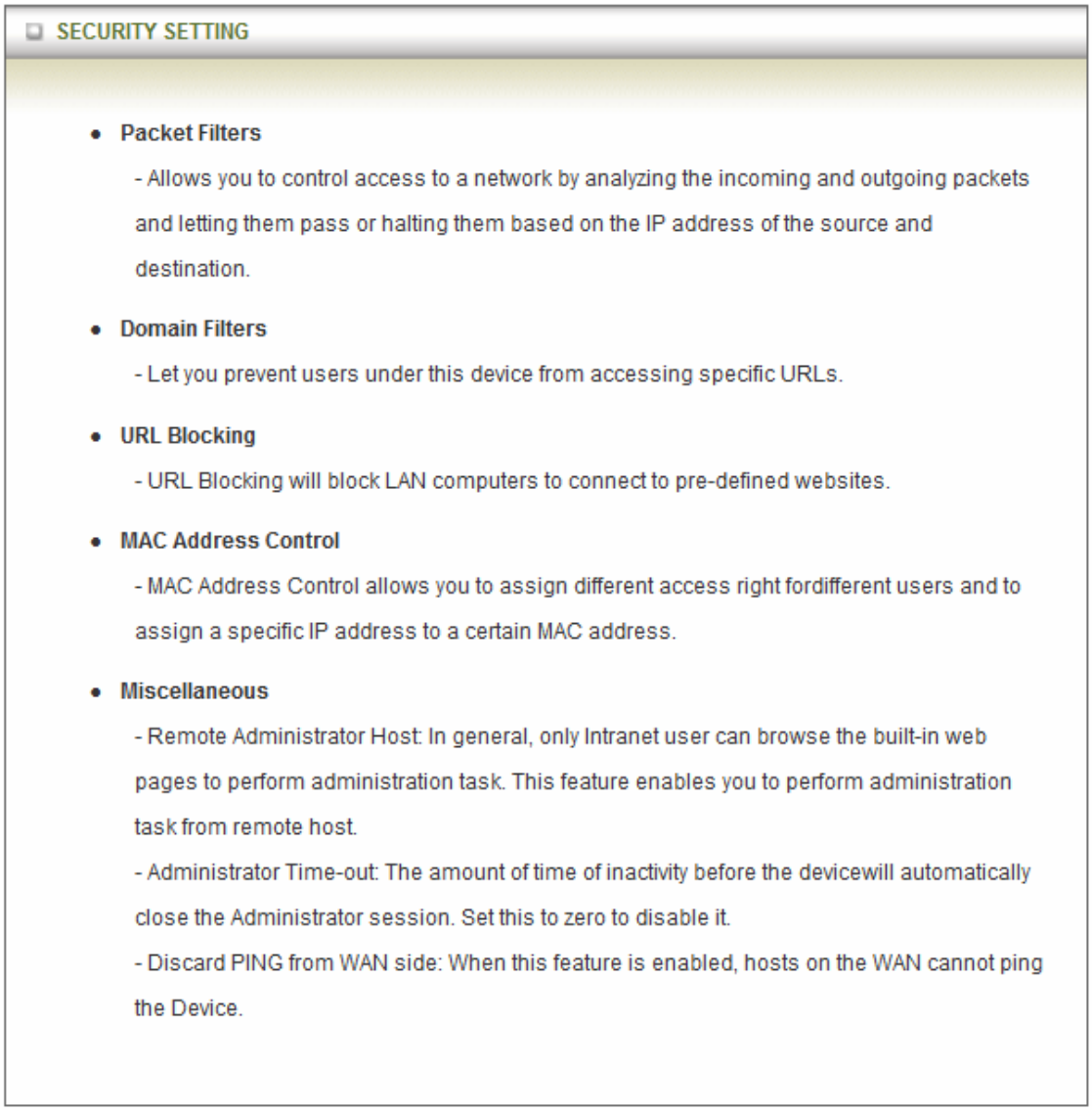
2. **UPnP Setting**

   The device supports the UPnP function. If the OS of your client computer supports this function, and you enabled it, like Windows XP, you can see the following icon when the client computer gets IP from the device.

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

3.3 Security Setting

The security setting includes Packet Filter, Domain Filter, URL Blocking, MAC Address Control, L2TP/PPTP Client, and miscellaneous.

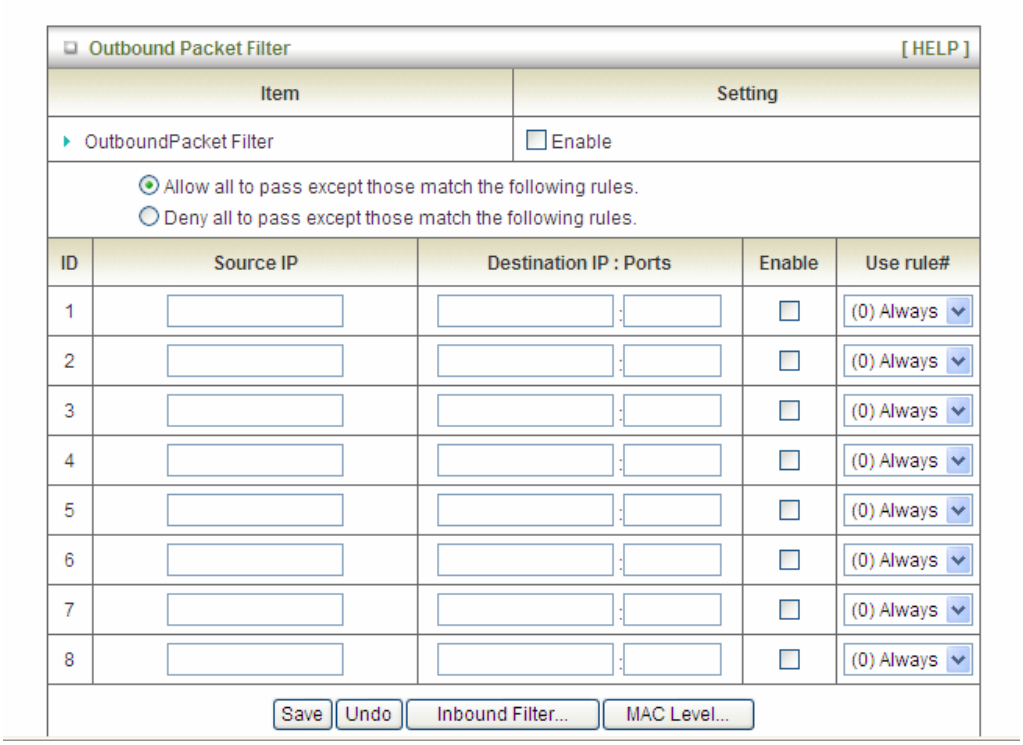


3.3.1 Packet Filters

Packet Filter includes both outbound filter and inbound filter. And they have same way to setting.

Packet Filter 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 specified rules
2. Deny all to pass except those match the specified rules



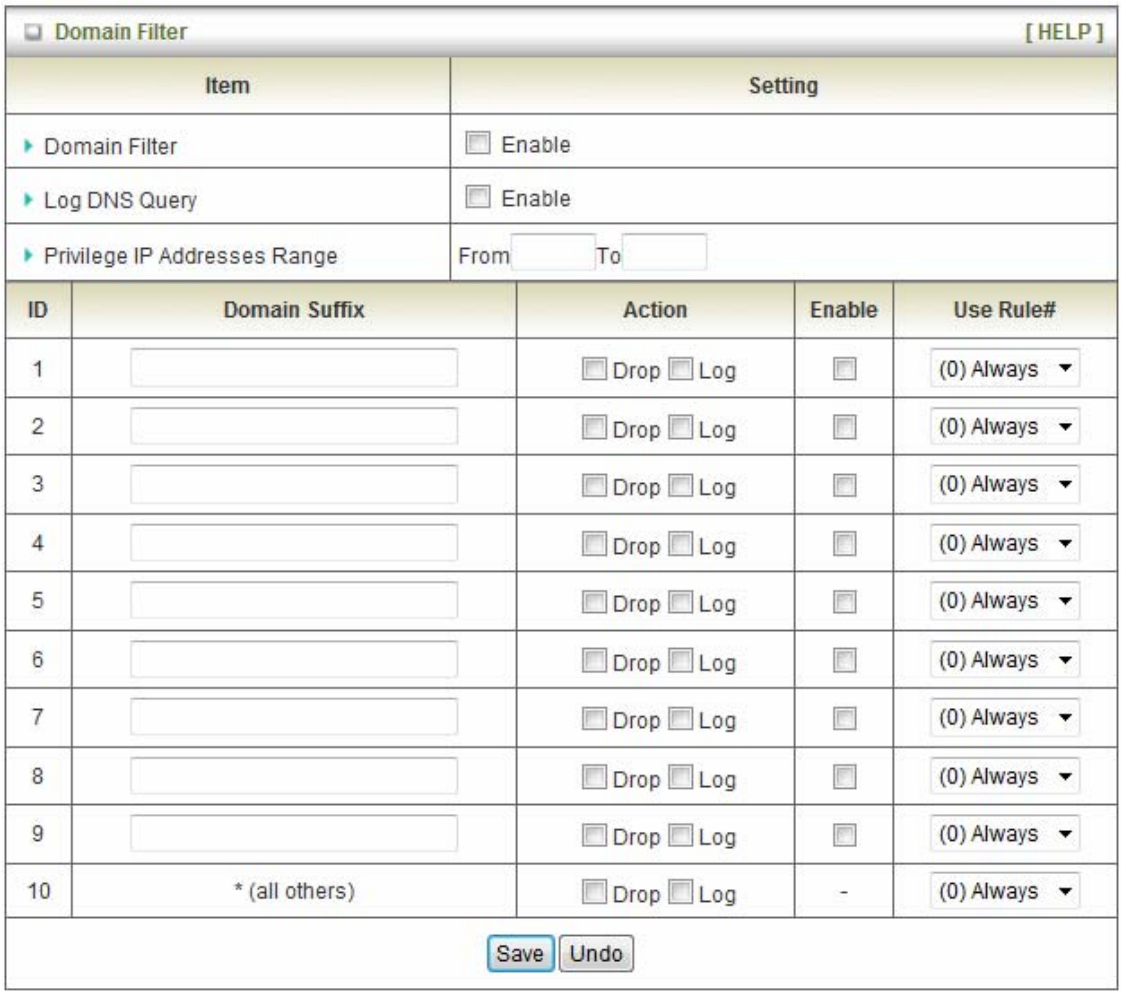
You can specify 8 rules for each direction: inbound or outbound. For each rule, you can define the following:

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

For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.
For source or 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 Detail, please refer to **Scheduling Rule.**
Each rule can be enabled or disabled individually.

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

3.3.2 Domain Filters



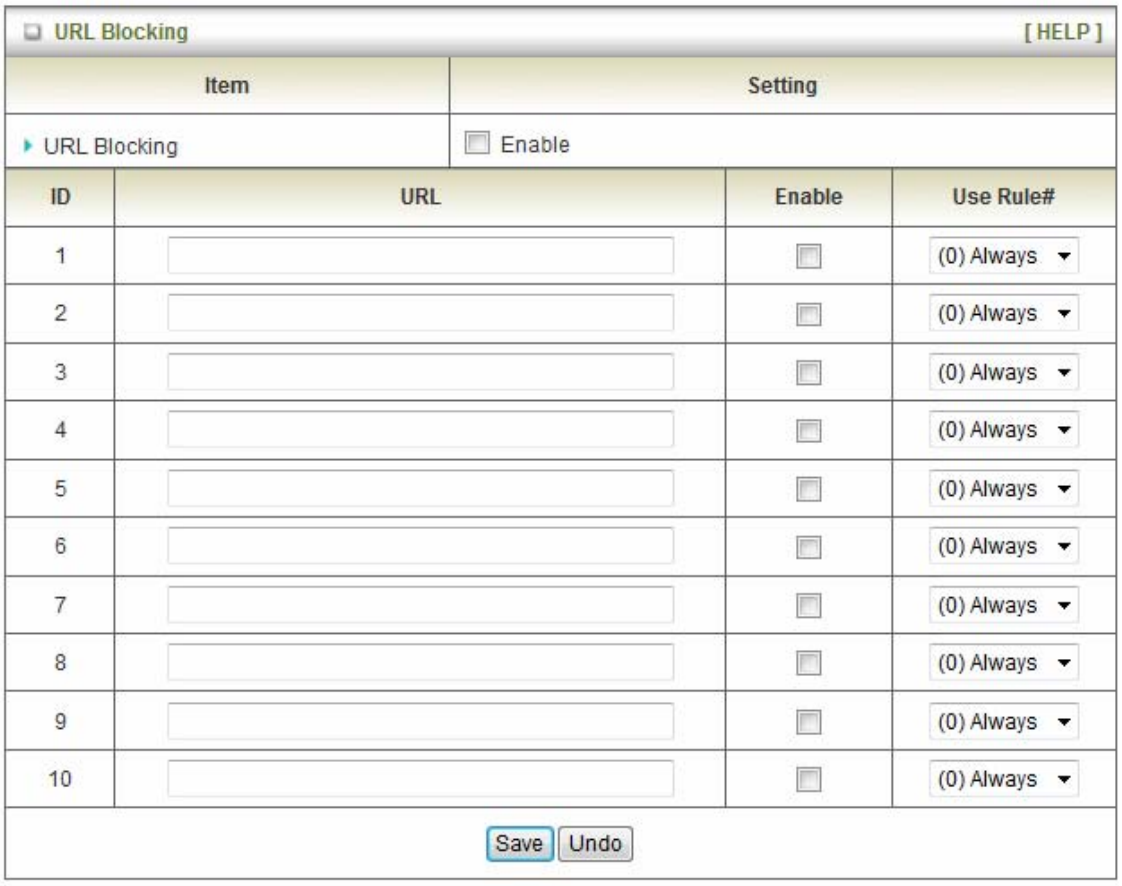
Domain Filter prevents users under this device from accessing specific URLs.

1. **Domain Filter**: Check if you want to enable Domain Filter.
2. **Log DNS Query**: Check if you want to log the action when someone accesses the specific URLs.
3. **Privilege IP Address Range**: Setting a group of hosts and privilege these hosts to access network without restriction.
4. **Domain Suffix**: A suffix of URL can be restricted, for example, ".com", "xxx.com".
5. **Action**: When someone is accessing the URL met the domain-suffix, what kind of action you want.
   Check “Drop” to block the access. Check “Log” to log this access.
6. **Enable**: Check to enable each rule.

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

3.3.3 URL Blocking

URL Blocking will block LAN computers to connect with pre-define Websites. The major difference between “Domain filter” and “URL Blocking” is Domain filter require user to input suffix (like .com or .org, etc), while URL Blocking require user to input a keyword only. In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a **keyword**.

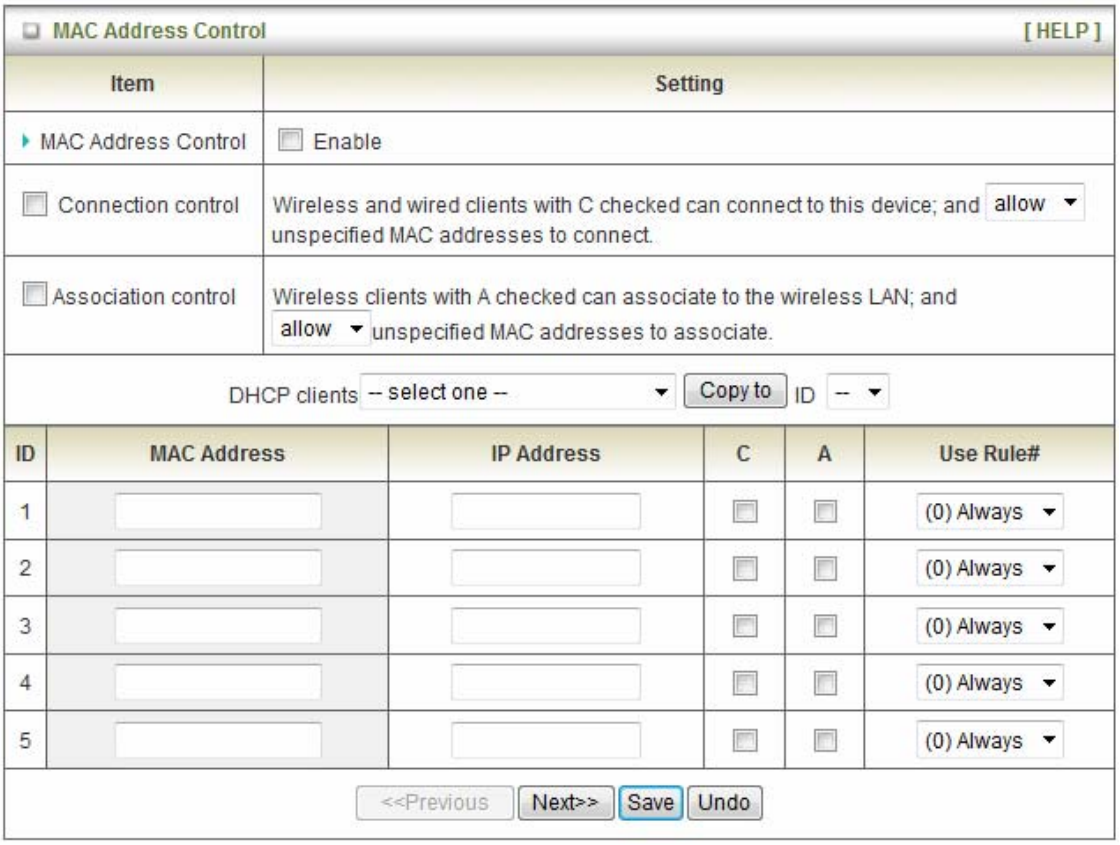


1. **URL Blocking**: Check if you want to enable URL Blocking.
2. **URL**: If any part of the Website's URL matches the pre-defined word, the connection will be blocked.
   For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".
3. **Enable**: Check to enable each rule.
4. **Use Rule#:** You can set a schedule rule for each of rule.

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

3.3.4 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.

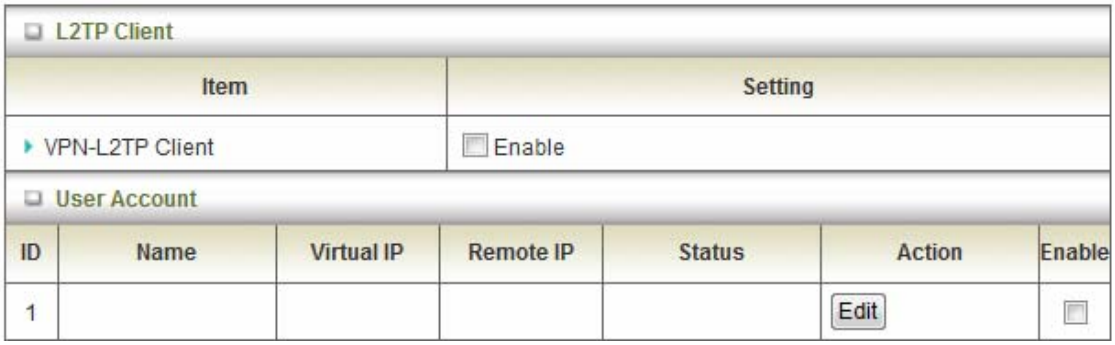


1. **MAC Address Control**: Check “Enable” to enable the “MAC Address Control”. All of the settings in this page will take effect only when “Enable” is checked.
2. **Connection control**: Check "Connection control" to enable the controlling of which wired and wireless clients can connect with this device. If a client is denied to connect with this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect with this device.
3. **Association control**: Check "Association control" to enable the controlling of which wireless client can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN.

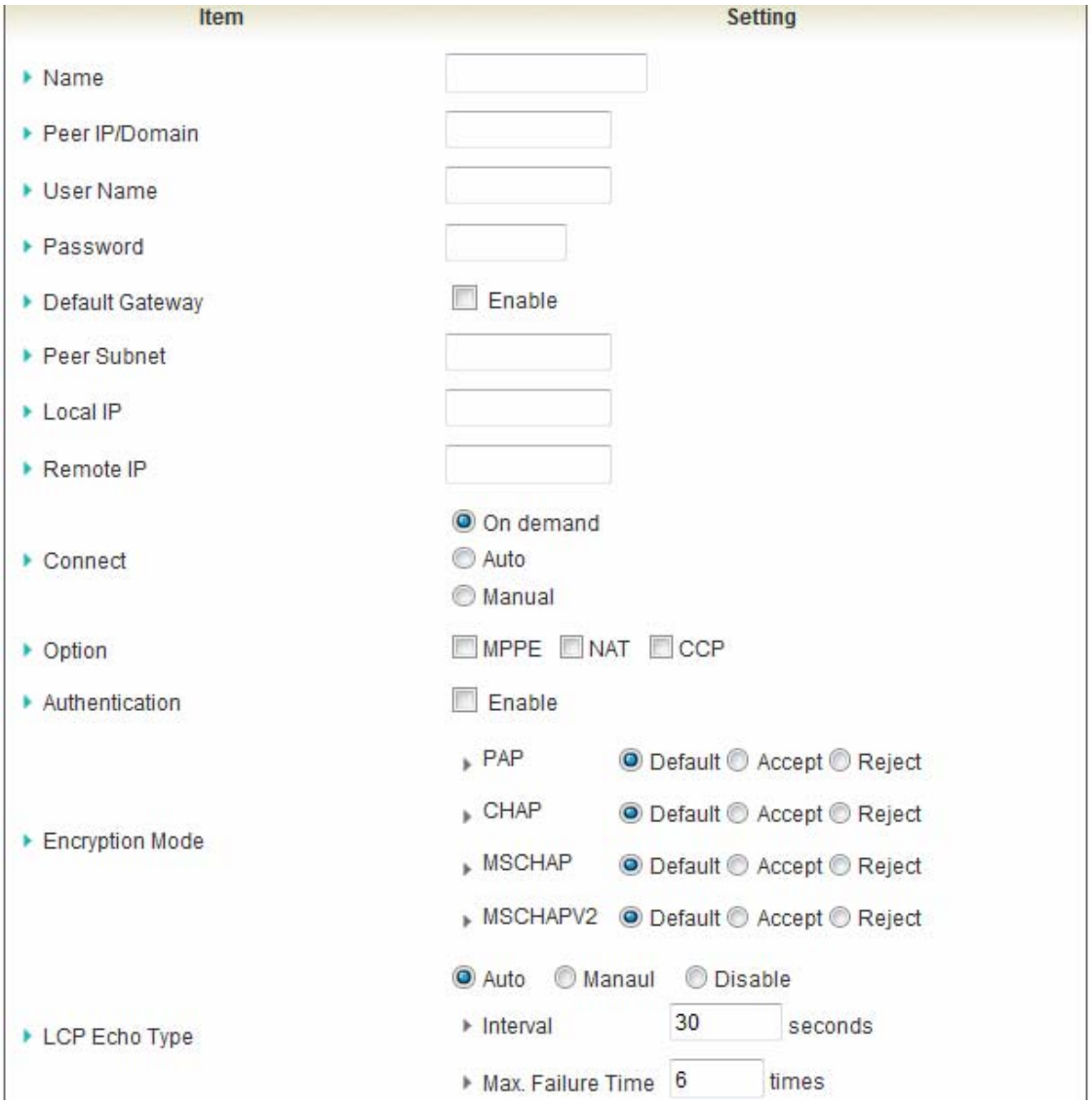
Click on “Save” to store your settings or click “Undo” to give up the changes.

3.3.5 VPN-L2TP Client

This router can connect to a remote L2TP server after WAN connection is established.



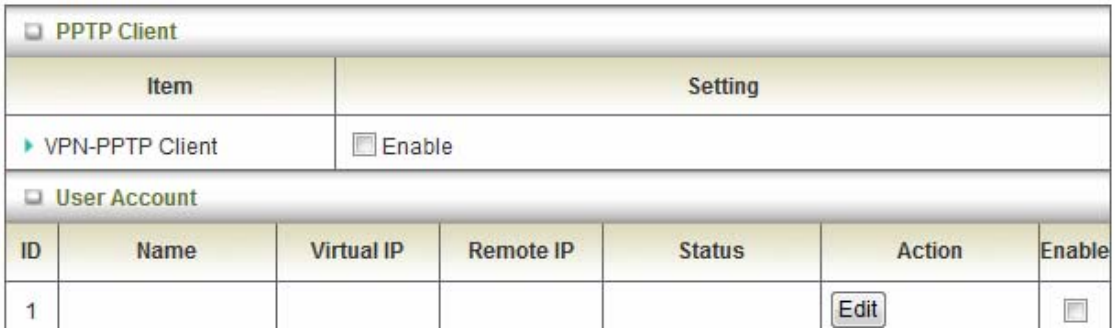
Enable **VPN-L2TP Client**, and press **"Edit"** button to add connection detail.



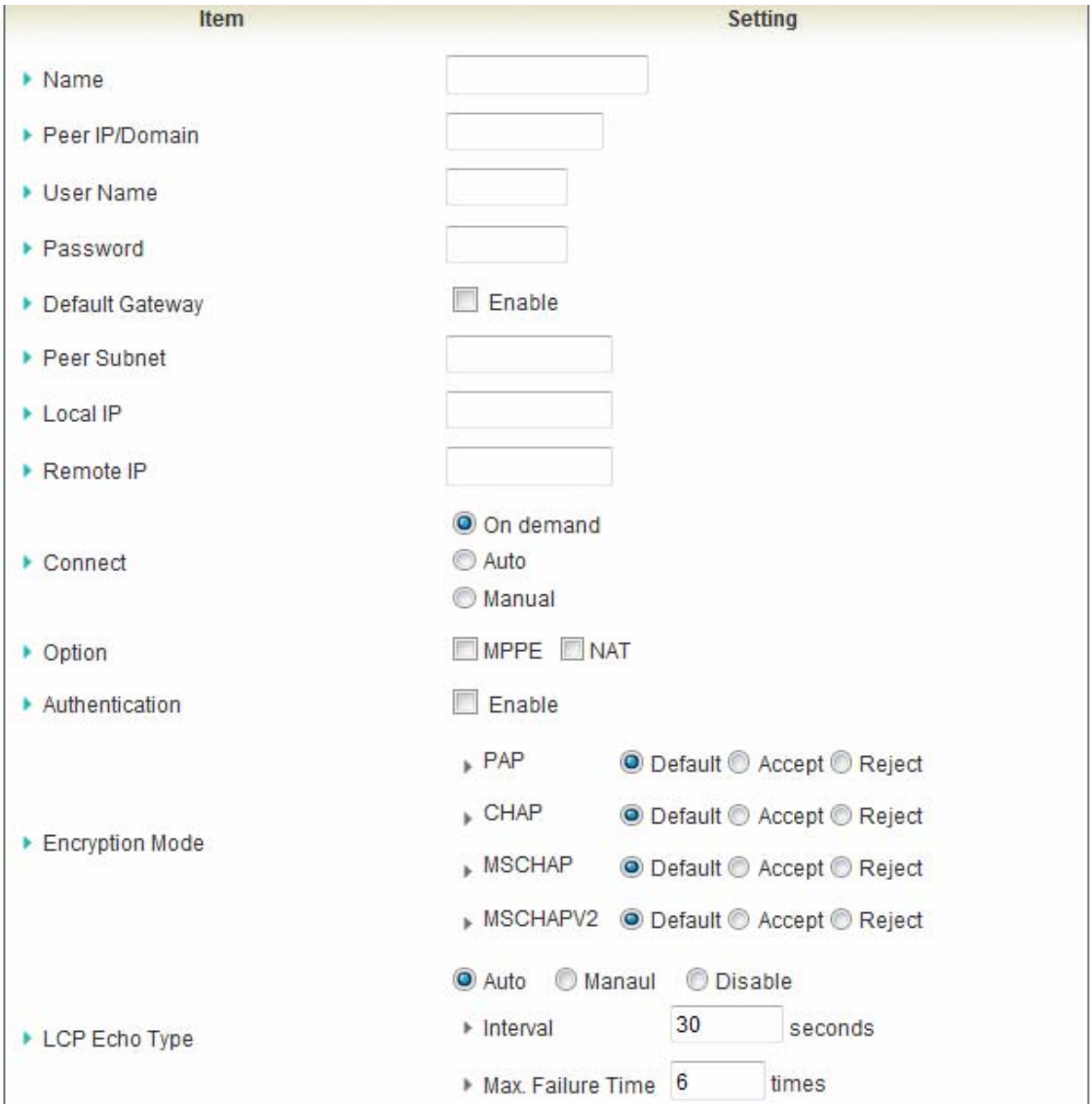
1. **Name:** Input a name of this profile.
2. **Peer IP/Domain:** Input the IP address or domain name of remote L2TP server.
3. **User name:** enter the user name to dial to remote L2TP server.
4. **Password:** enter the password to dial to remote L2TP server.
5. **Default Gateway:** If check this checkbox, all traffic will be routed to remote L2TP server.
6. **Peer Subnet:** Only the destination in this peer subnet will be routed to remote L2TP server.
7. **Local IP:** You can set a fixed IP address of this L2TP connection.
8. **Remote IP:** Indicate a peer IP address of L2TP connection.
9. **Connect:** You can choose on-demand, auto, or manual to trigger this connection.
10. **Option:** Options for connection.
11. **Authentication:** You need to enable this option if remote L2TP server requests it.
12. **Encryption Mode:** You can choose different ways for encryption. The encryption you choose must be supported by remote L2TP server.
13. **LCP Echo Type:** Choose the way to do connection keep alive.

3.3.6 VPN-PPTP Client

This router can connect to a remote PPTP server after WAN connection is established.

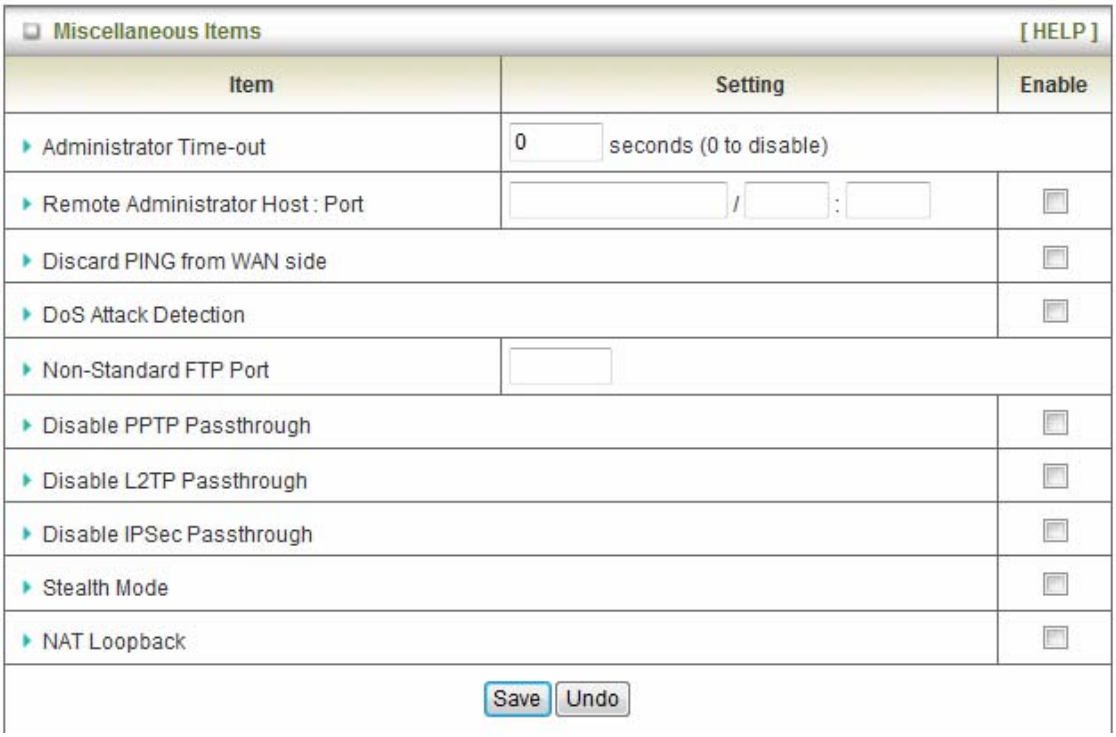


Enable **VPN-PPTP Client**, and press **"Edit"** button to add connection detail.



1. **Name:** Input a name of this profile.
2. **Peer IP/Domain:** Input the IP address or domain name of remote PPTP server.
3. **User name:** enter the user name to dial to remote PPTP server.
4. **Password:** enter the password to dial to remote PPTP server.
5. **Default Gateway:** If check this checkbox, all traffic will be routed to remote PPTP server.
6. **Peer Subnet:** Only the destination in this peer subnet will be routed to remote PPTP server.
7. **Local IP:** You can set a fixed IP address of this PPTP connection.
8. **Remote IP:** Indicate a peer IP address of PPTP connection.
9. **Connect:** You can choose on-demand, auto, or manual to trigger this connection.
10. **Option:** Options for connection.
11. **Authentication:** You need to enable this option if remote PPTP server requests it.
12. **Encryption Mode:** You can choose different ways for encryption. The encryption you choose must be supported by remote PPTP server.
13. **LCP Echo Type:** Choose the way to do connection keep alive.

3.3.7 Miscellaneous



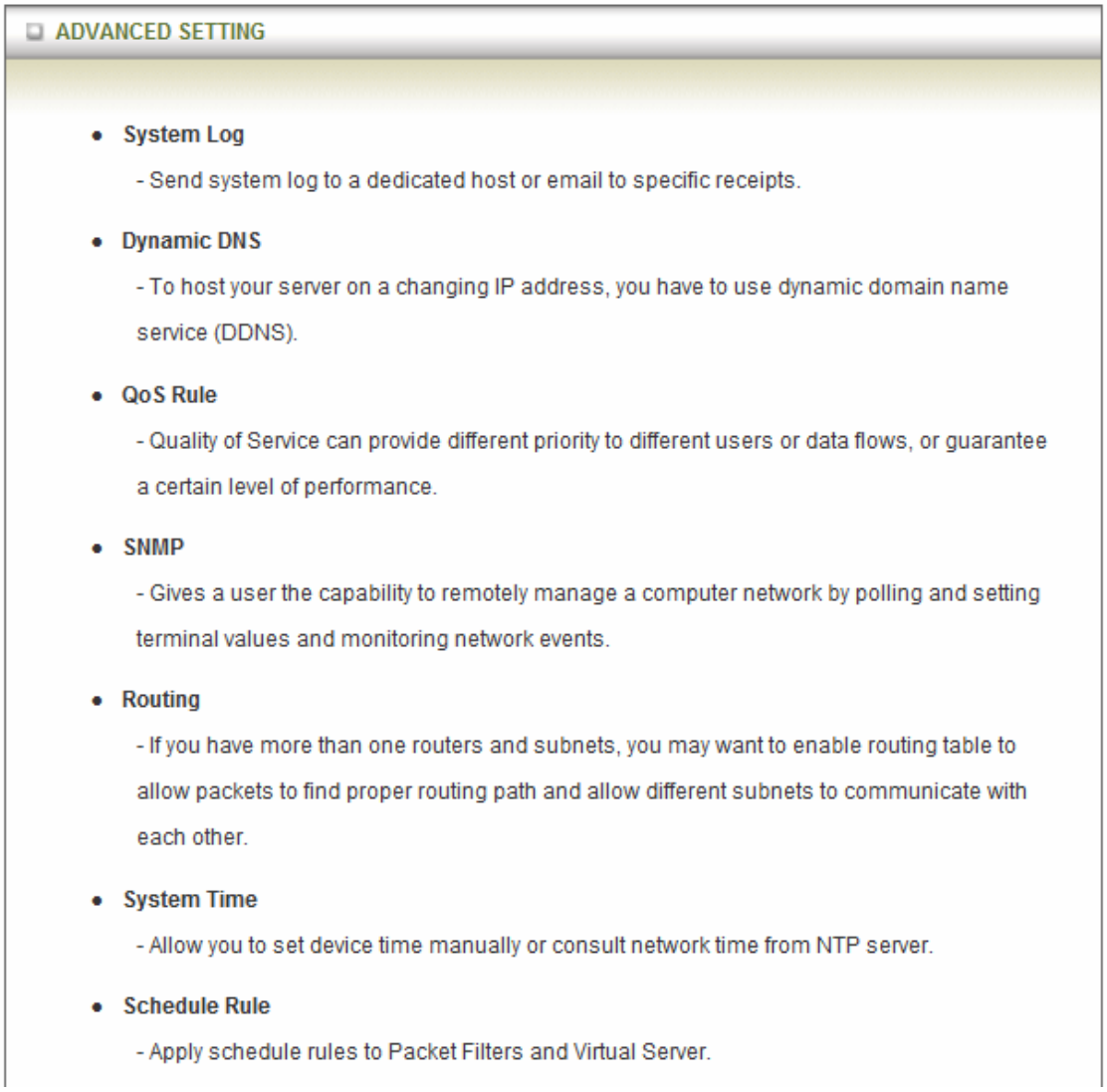
1. **Administrator Time-out**: The time of no activity to logout automatically, you may set it to zero to disable this feature.
2. **Remote Administrator Host/Port**
   In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect with this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses for example, "10.1.2.0/24".
   NOTE: When Remote Administration is enabled, the web server port will be shifted to 80. You can change web server port to other port, too.
3. **Discard PING from WAN side**: When this feature is enabled, any host on the WAN cannot ping this product.
4. **DoS Attack Detection**: When this feature is enabled, the router will detect and log the DoS attack comes from the Internet. Currently, the router can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack etc.
5. **Non-Standard FTP port:** If you want to access a WAN FTP server which doesn't use port 21, you need to indicate the port number that WAN FTP uses.

6. **Disable PPTP passthrough:** The PPTP passthrough is enabled by default. You can disable here.
7. **Disable L2TP passthrough:** The L2TP passthrough is enabled by default. You can disable here.
8. **Disable IPSec passthrough:** The IPSec passthrough is enabled by default. You can disable here.
9. **Stealth Mode:** If enable this option, router will become “hidden” if someone uses port scan utility to scan available ports on this router.
10. **NAT Loopback:** If enable this option, local hosts can access local virtual server via WAN IP address of this router.

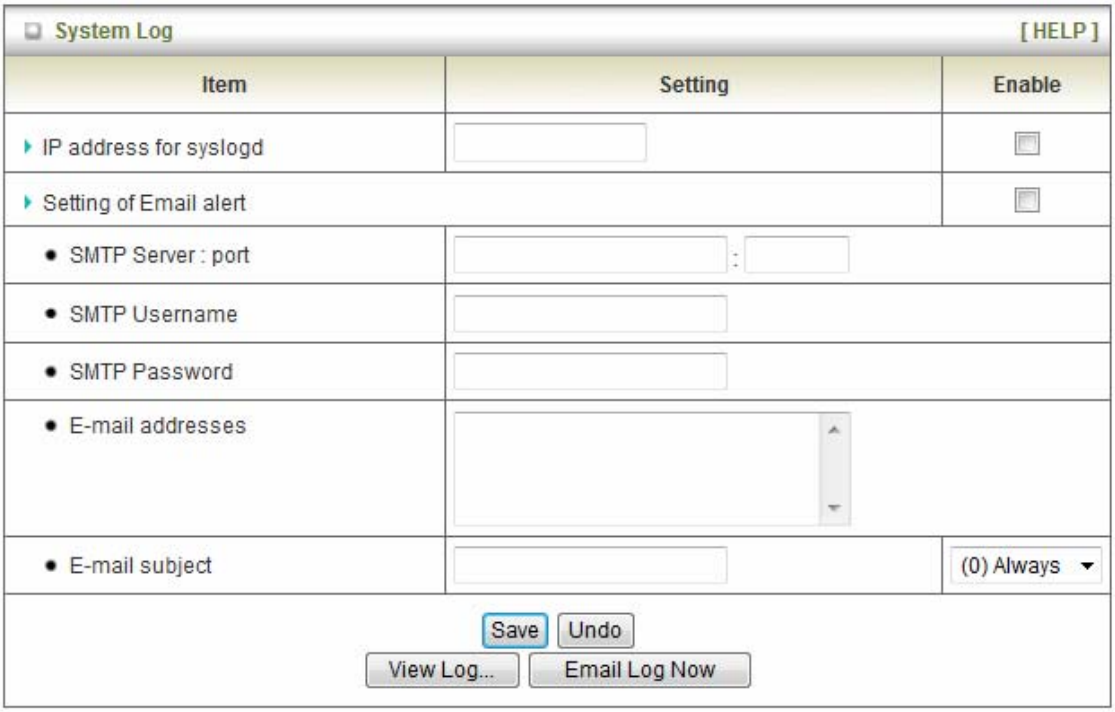
Click on “Save” to store your settings or click “Undo” to give up the changes.

3.4 Advanced Setting

The **Advanced Setting** includes System log, Dynamic DNS, QoS, SNMP, Routing, System Time, Schedule Rule, IPv6, and VLAN settings.



3.4.1 System Log



This page support two methods to export system logs to specific destination by means of syslog (UDP) and SMTP(TCP). The items you have to setup including:

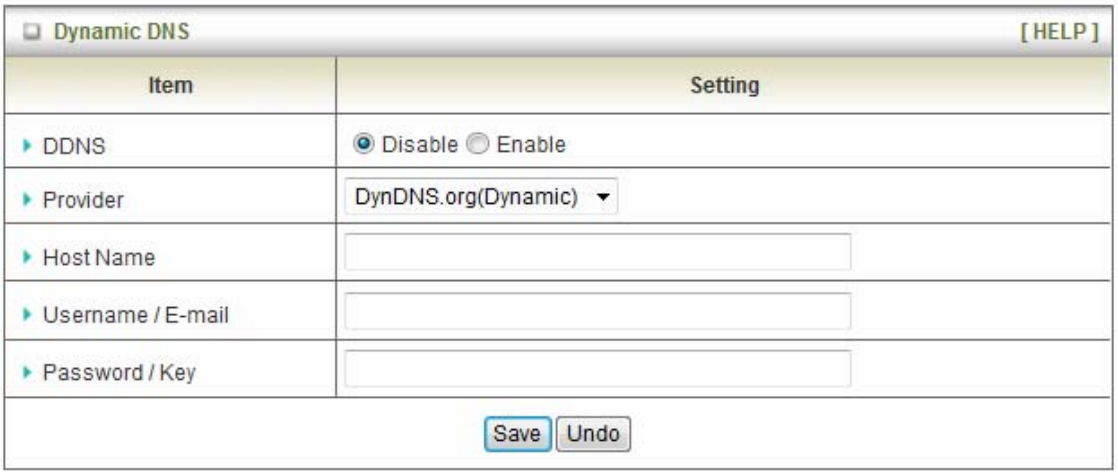
1. **IP Address for Sys log**: Host IP of destination where sys log will be sent to. Check **Enable** to enable this function.
2. **Setting of E-mail Alert**: Check if you want to enable Email alert (send syslog via email).
3. **SMTP Server:Port**: Input the SMTP server IP and port, which are connected 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".
4. **SMTP Username:** Input username of your account on this SMTP server.
5. **SMTP Password:** Input password of your account on this SMTP server.
6. **E-mail address:** The recipients who will receive these logs, you can assign more than 1 recipient, using ';' or ',' to separate these email addresses.
7. **E-mail Subject**: The subject of email alert, this setting is optional.

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

3.4.2 Dynamic DNS

To host your server on a changing IP address, you have to use dynamic domain name service (DDNS). So that 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.



To enable **Dynamic DNS** click the check box next to **Enable** in the **DDNS** field. Next you have to enter the appropriate information about your Dynamic DNS Serve .**Provider**, **Host Name**, **Username/E-mail**, and **Password/Key**. You can get this information when you register an account on a Dynamic DNS server.

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

3.4.3 QoS

Quality of Service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

3.4.3.1 Smart QoS

Item	Setting
Cross-layer QoS	Disable
QoS Mode	Smart-QoS
Bandwidth of Upstream	2000 kbyte
Bandwidth of Downstream	4000 kbyte
Flexible Bandwidth Management	Enable

1. **Cross-layer QoS :** you can select enable/disable the QoS control
2. **QoS Mode :** you can select Smart-QoS or User defined QoS rule for your own QoS control
3. **Bandwidth of upstream / bandwidth of Downstream** : you can input the value of maximize of upstream and downstream bandwidth from your ISP
4. **Enable Flexible Bandwidth management :** If you enable this management, system will share the bandwidth of those selected applications to other applications if user do not run those selected application, for example, If you select Game/ VoIP/ Video 3 applications for higher priority in your system, then the system will automatically reserve 10% of bandwidth to other application, and share the rest of bandwidth (100-10)/3=30% each to Game/VoIP/Video, so if user do not play a game, then the system will flexible share the 30% of bandwidth to other application.

Item	Select
Game	☑
Chat	☐
VoIP	☑
P2P	☐
Video	☑
Web	☐
Save	

Example for Smart-QoS with FBM enable : Mr. Wang selects Game/ VoIP/ Video 3

applications for higher priority in his system, the system will automatically reserve 10% of minimum rate of bandwidth to other application, and share the rest minimum rate of bandwidth (100-10)/3=30% each to Game/VoIP/Video. If Mr. Wang's son plays on-line game in the morning, the total bandwidth will all reserve to his son. By the evening, when Mr. Wang back home and wants to watch IPTV, then he will get the same priority with his son, and share the bandwidth.

5. **Disable Flexible Bandwidth Management :** If you disable this management, system will allow you to input percentage of bandwidth manually.

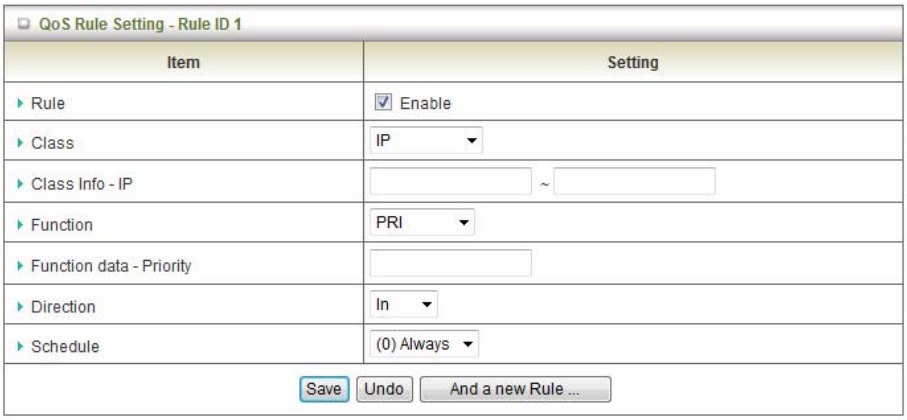
Item	Select	Setting
Game	☑	50 %
Chat	☐	0 %
VoIP	☑	30 %
P2P	☐	0 %
Video	☐	0 %
Web	☐	0 %
Save		

3.4.3.2 User defined QoS Rule

Item	Setting
Cross-layer QoS	Enable
QoS Mode	User define QoS rule
Bandwidth of Upstream	2000 kbyte
Bandwidth of Downstream	5000 kbyte
Flexible Bandwidth Management	Enable

1. Cross-layer QoS : you can enable/disable this QoS system.
2. **QoS Mode :** you can select User defined QoS rule for your own QoS control
3. **Bandwidth of upstream / bandwidth of Downstream** : you can input the value of maximize of upstream and downstream bandwidth from your ISP
4. **Advance setting :** you can press the button of 'Add New Rule' to create a new QoS rule.

5. **Create a QoS Rule** : you can enable the rule, and select QoS class type as below.



Class : You can create your own QoS rule by different classes as below.

Class	Description
IP	IP address base
N	TCP port
UDPPORT	UDP port
MAC	MAC base
DSCP	DSCP base

Function : you can set your own function value to enable your QoS rule as below.

Function	Description	Data
PRI	Priority	1~6
MAXR	Maximum bandwidth Rate	KBps/MBps
MINR	Minimum bandwidth Rate	KBps/MBps
SESSION	Connection session	number
DROP	Drop packet	None
LOG	Log event	None
ALERT	Alert event	None

Direction : you can select inbond/ outbond for your direction.

Direction	
IN	inbond
OUT	outbond
BOTH	inbond & outbond

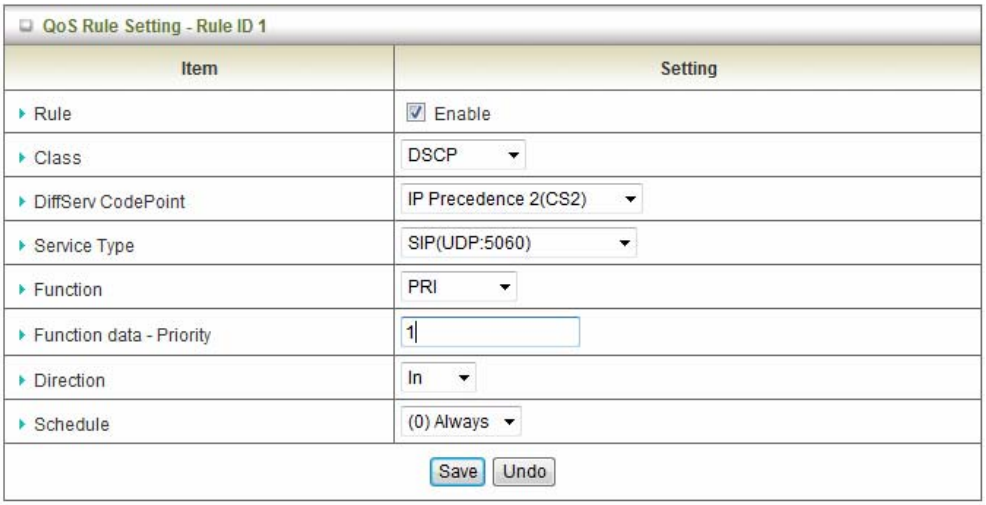
6. **DSCP setting** : you can set your own DSCP value here.

DiffServ Code Point : you can select code value.

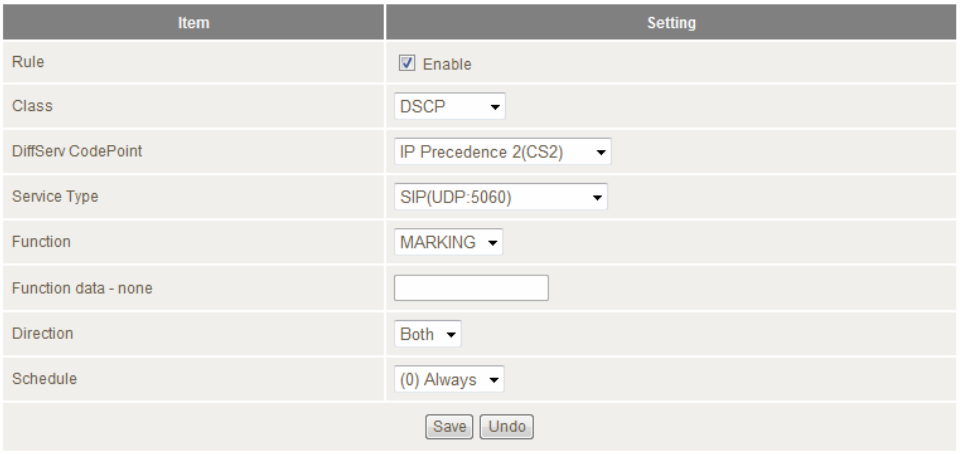
Service Type : you can select their service type.

Function : PRI

Function data- Priority : 1~6



DSCP marking : you can add your inbound / outbound packets a DCSP marking, please see one example as below.



Ex. Please mark CS3 when an packet in/ out via UDP port 5060.

Once you saved the QoS rule, system will show you the rule as below, you can add another new rule accordingly.

System will show you all your QoS rule as below

Note 1. : You can move up or down the priority of all rules by pointing the '↑'or '↓' if you want to change the priority.

Note 2. : You can unmark any rule if you do not want it enable now.

Provide different priority to different users or data flows, or guarantee a certain level of performance.

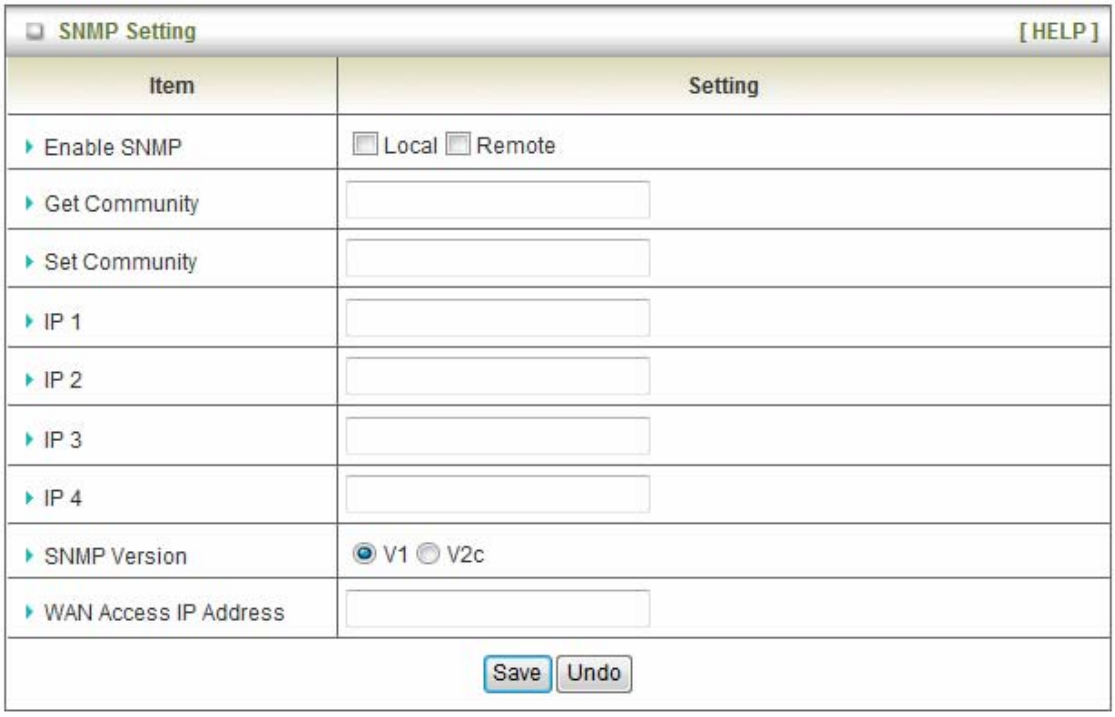
1. **QOS Control**: Check **Enable** to enable this function.
2. **Bandwidth of Upstream**: Set the limitation of upstream bandwidth
3. **Local IP : Ports**: Define the Local IP address and ports of packets
4. **Remote IP : Ports**: Define the Remote IP address and ports of packets

5. **QoS Priority:** This defines the priority level of the current Policy Configuration. Packets associated with this policy will be serviced based upon the priority level set. For critical applications High or Normal level is recommended. For non-critical applications select a Low level.
6. **Enable**: Check to enable the corresponding QOS rule.
7. **User Rule#**: The QoS rule can work with Scheduling Rule number#. Please refer to the Section 3.1.4.7 Schedule Rule.

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

3.4.4 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.

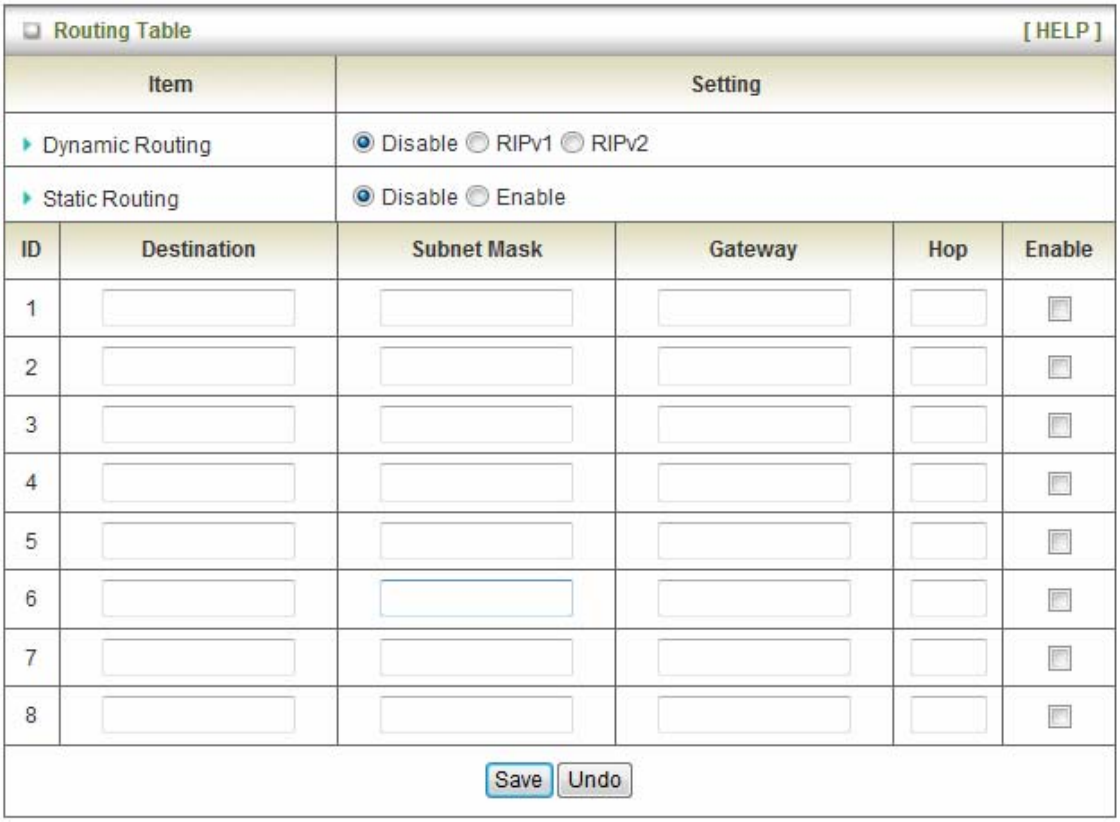


1. **Enable SNMP**: You must check “Local”, “Remote” or both to enable SNMP function. If “Local” is checked, this device will response request from LAN. If “Remote” is checked, this device will response request from WAN.
2. **Get Community**: The community of GetRequest that this device will respond.
3. **Set Community**: The community of SetRequest that this device will accept.
4. **IP 1, IP 2, IP 3, IP 4**: Enter the IP addresses of your SNMP Management PCs. User has to configure to where this device should send SNMP Trap message.
5. **SNMP Version**: Select proper SNMP Version that your SNMP Management software supports.
6. **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.

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

3.4.5 Routing

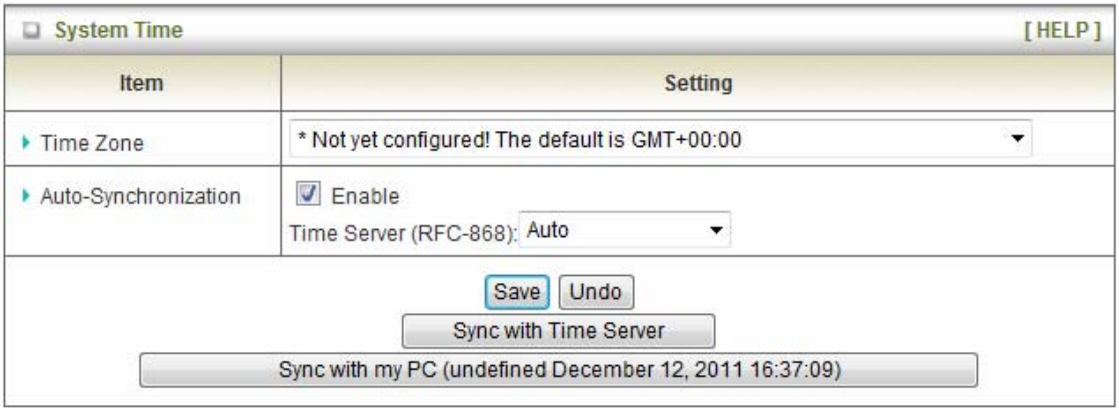
If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other. The routing table allows you to determine which physical interface address to use for outgoing IP data grams.



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 subnet in your network. Otherwise, please select RIPv1 if you need this protocol.
2. **Static Routing**: For static routing, you can specify up to 8 routing rules. 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.

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

3.4.6 System Time



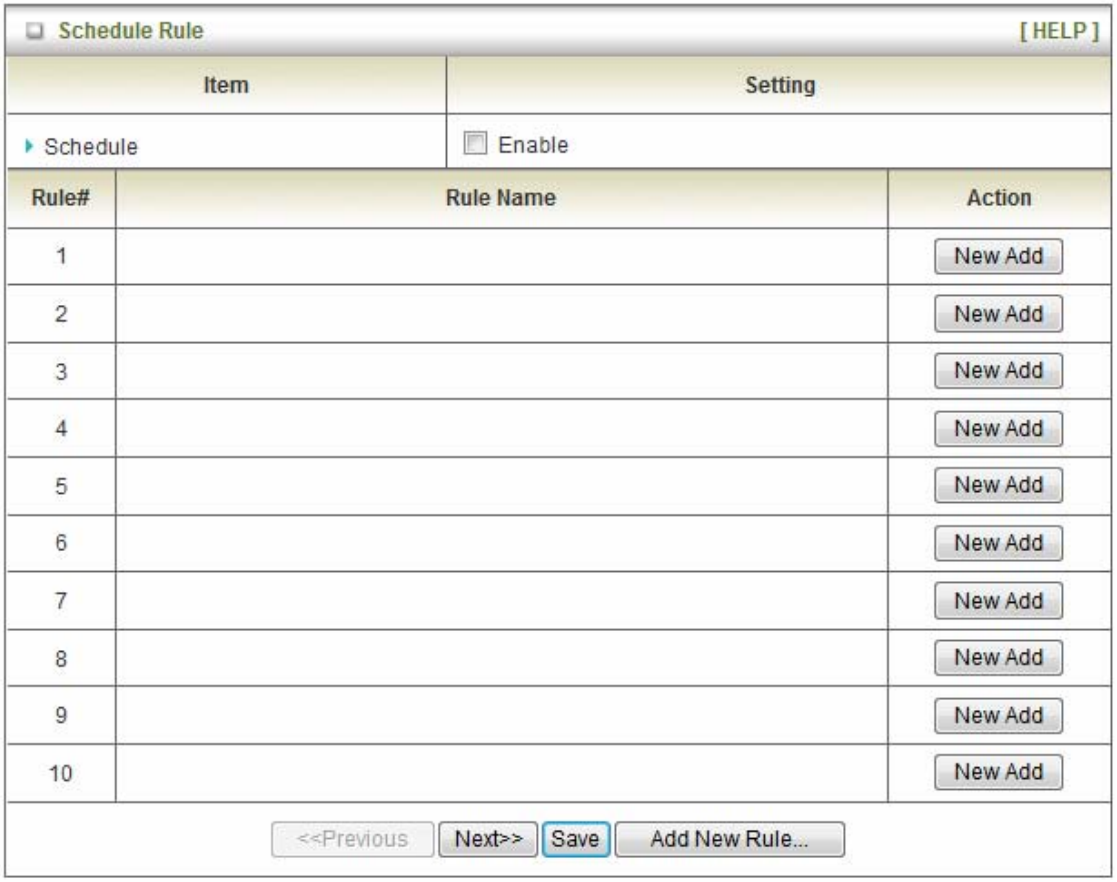
1. **Time Zone**: Select a time zone where this device locates.
2. **Auto-Synchronization**: Check the “Enable” checkbox to enable this function. Besides, you can select a NTP time server to consult UTC time.
3. **Sync with Time Server**: Click on the button if you want to set Date and Time by NTP Protocol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

.

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

3.4.7 Scheduling

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



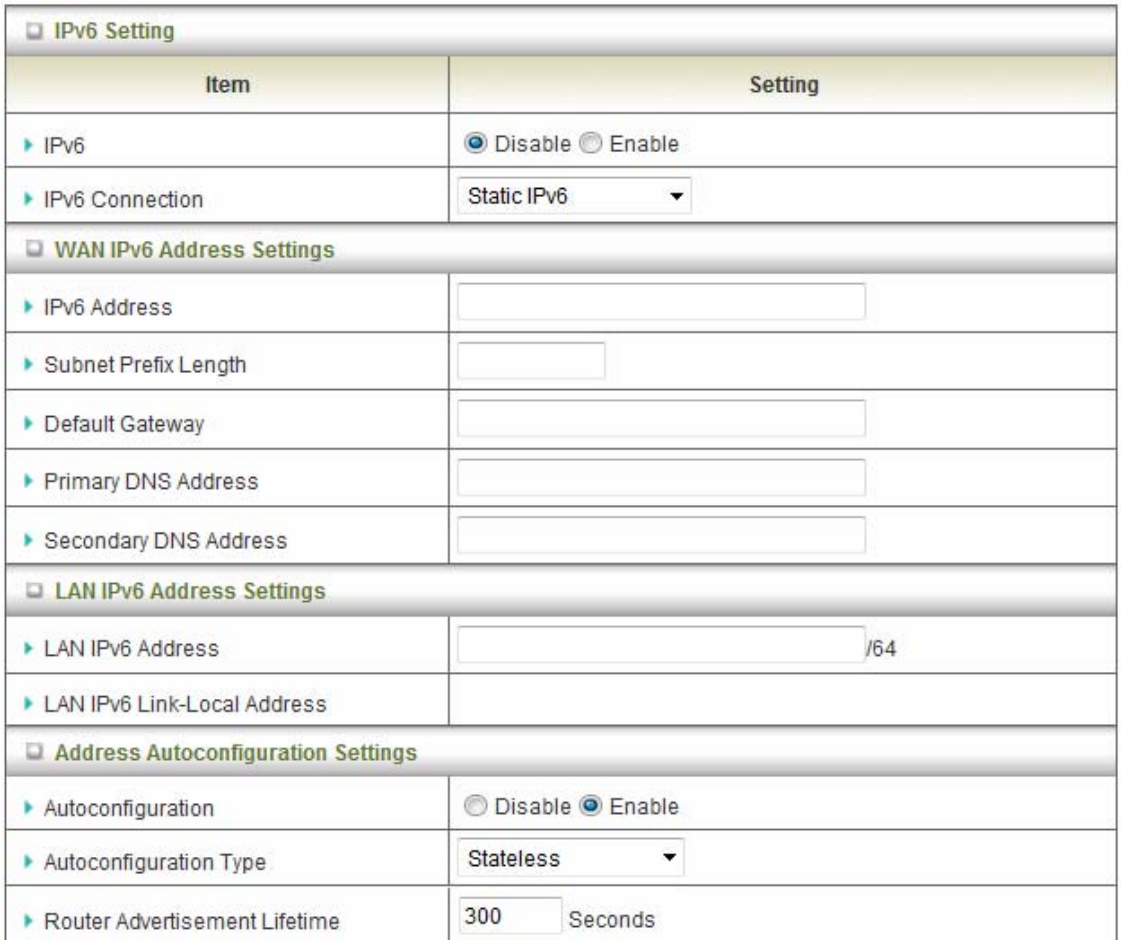
1. **Schedule**: Check to enable the schedule rule settings.
2. **Add New Rule**: To create a schedule rule, click the “Add New Rule” button. You can edit the **Name of Rule**, **Policy**, and set the schedule time (**Week day**, **Start Time**, and **End Time**). The following example configures “ftp time” as everyday 14:10 to 16:20.

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

3.4.8 IPv6

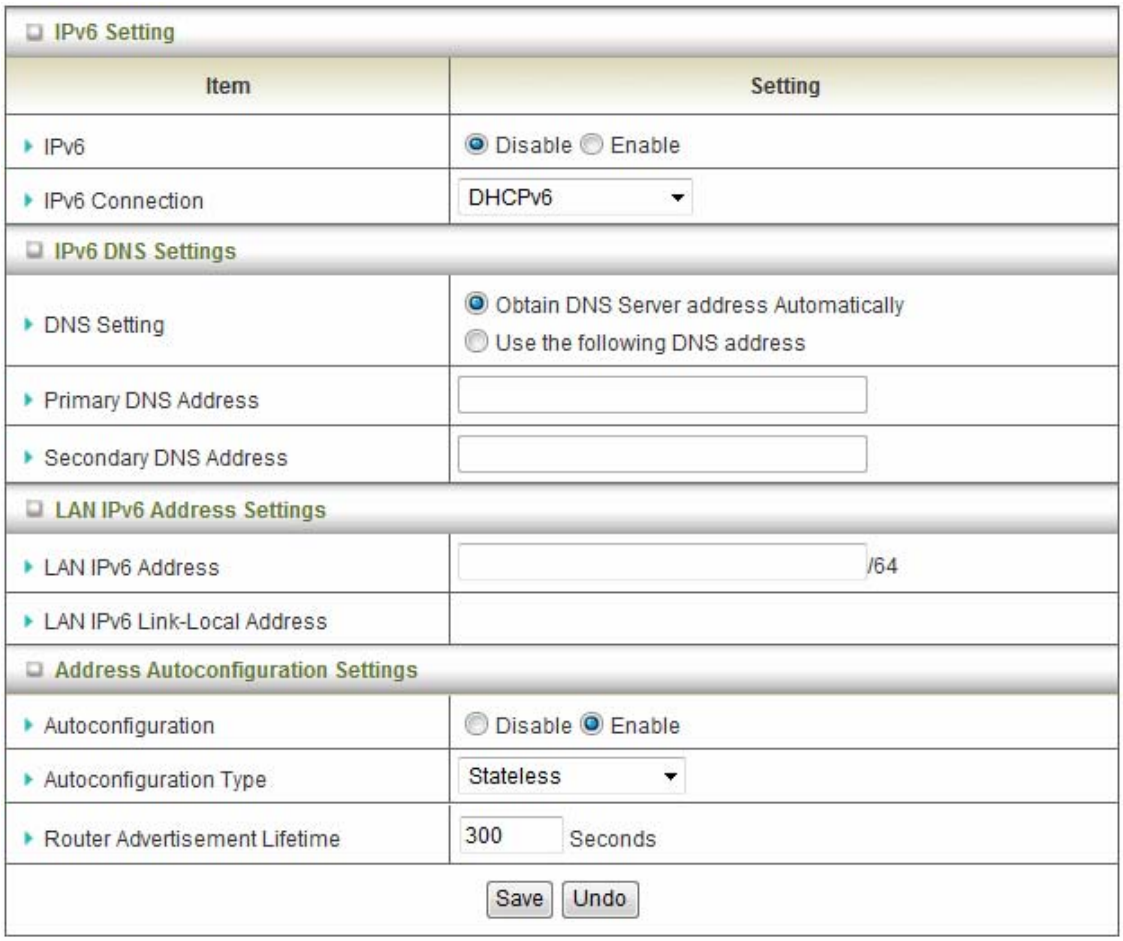
This device supports several IPv6 applications. You can choose Static IPv6, DHCPv6, PPPoEv6, 6to4, and IPv6 in IPv4 tunnel according to your requirements.

3.4.8.1 Static IPv6



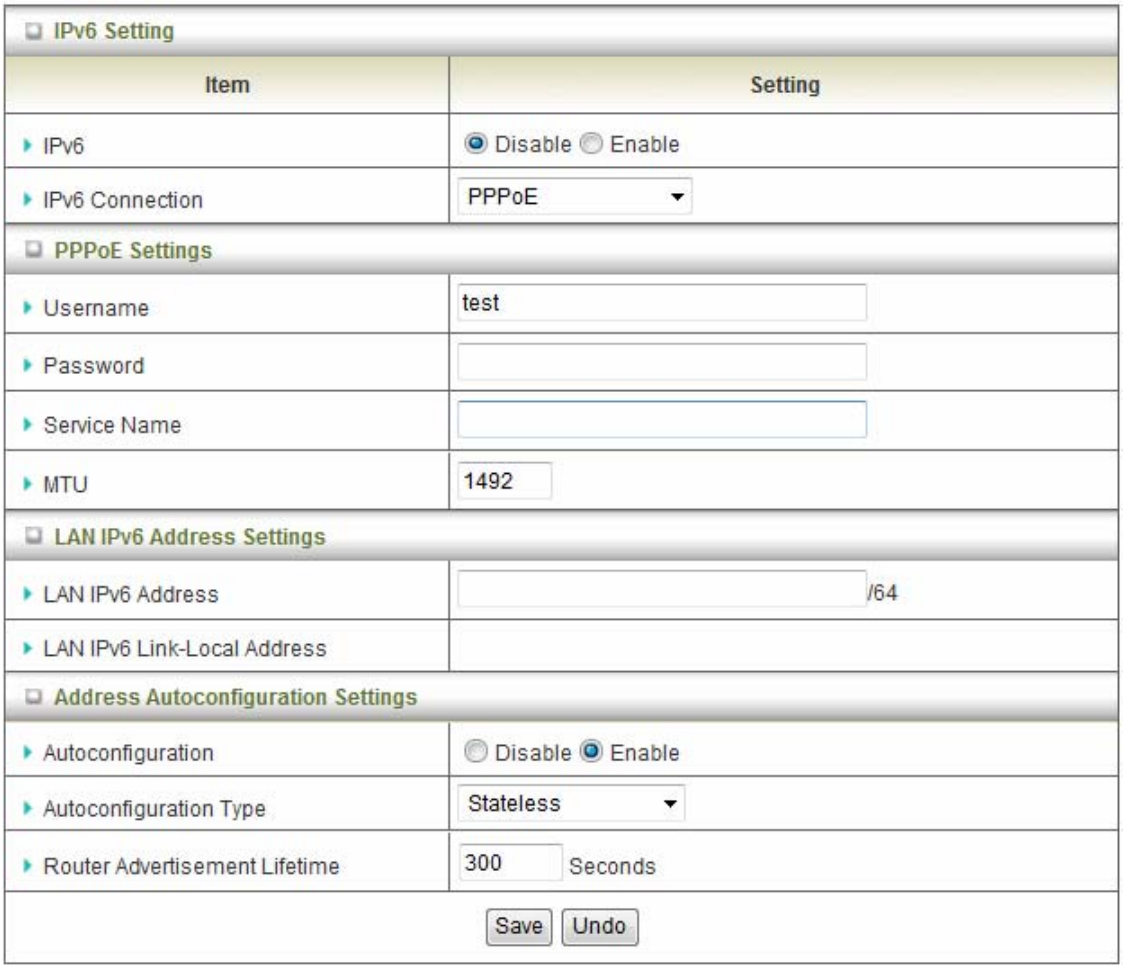
1. **IPv6**: Disable or enable the IPv6 functions.
2. **IPv6 Connection**: you can choose Static IPv6 from the list.
3. **WAN IPv6 address settings**: you can add IPv6 address / subnet prefix length / default Gateway / Primary DNS address and secondary DNS address.
4. **LAN IPv6 address settings**: you can add LAN IPv6 address, and IPv6 Link-Local address will be showed automatically.
5. **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.

3.4.8.2 DHCPv6



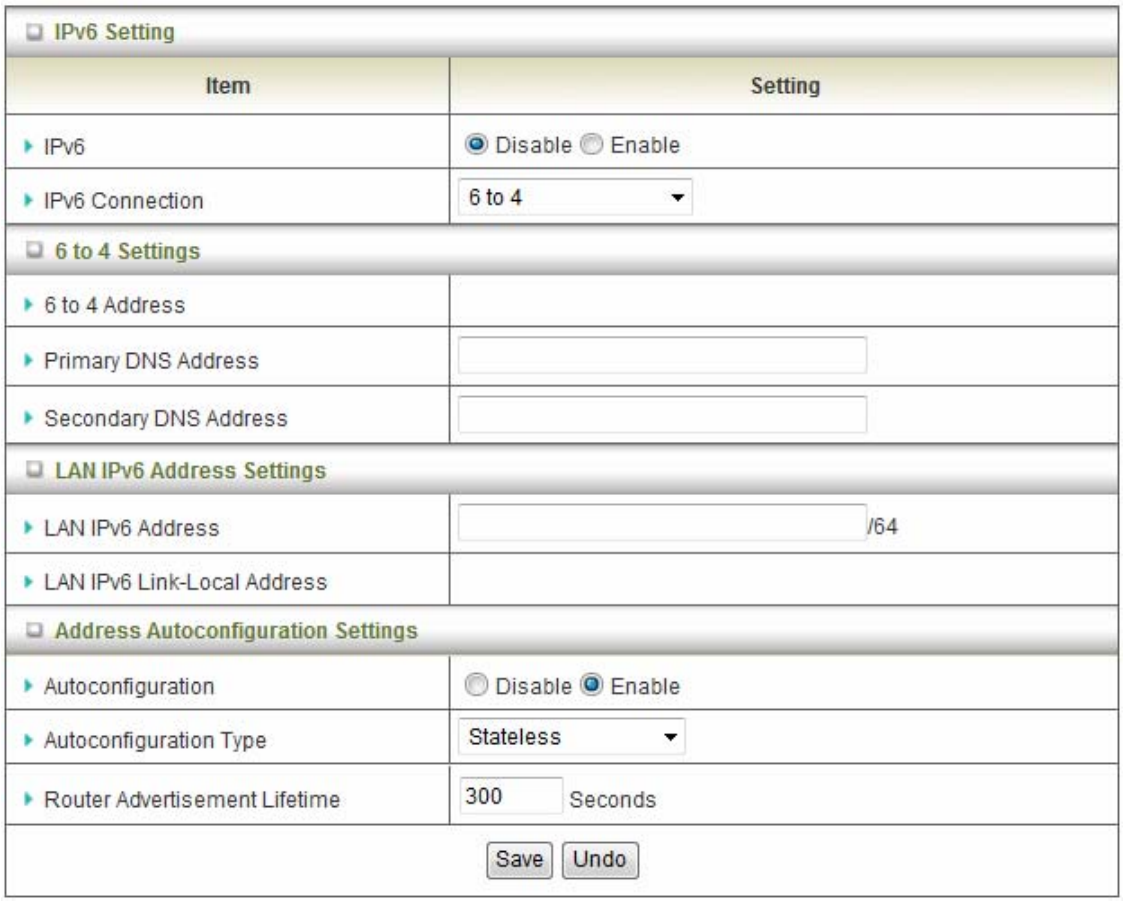
1. **IPv6 DNS settings**: you may obtain IPv6 DNS automatically or set DNS address manually for Primary DNS address and secondary DNS address.
2. **LAN IPv6 address settings**: you can add LAN IPv6 address, and IPv6 Link-Local address will be showed automatically.
3. **Address auto configuration setting:** 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.

3.4.8.3 PPPoEv6



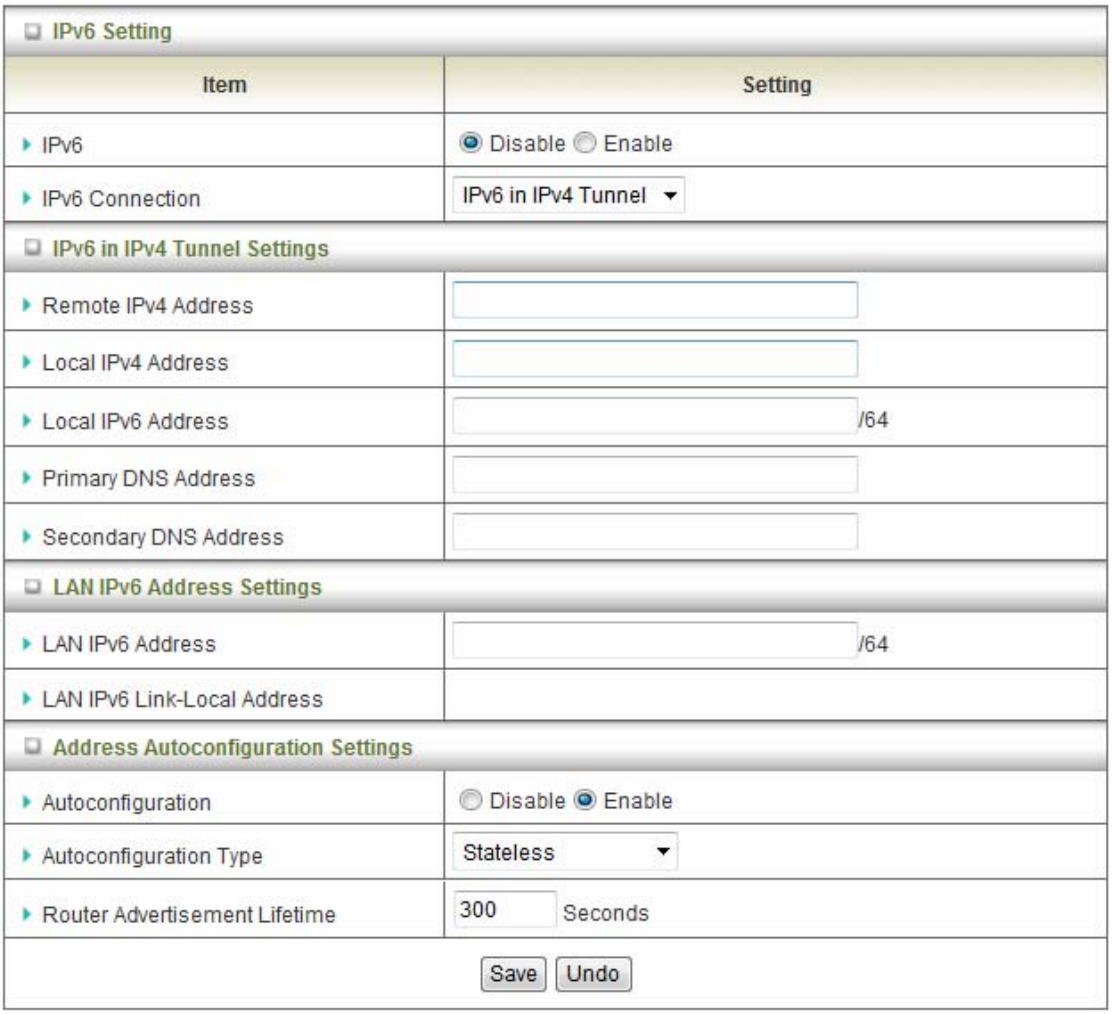
1. **PPPoE settings**: you need to type username and password of PPPoE connection. The service name is only required when ISP asks you to input it. MTU is 1492 by default.
2. **LAN IPv6 address settings**: you can add LAN IPv6 address, and IPv6 Link-Local address will be showed automatically.
3. **Address 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.

3.4.8.4 6 to 4



1. **IPv6 DNS settings**: The 6 to 4 address will be showed automatically when WAN gets a public IPv4 address. You may set DNS address manually for Primary DNS address and secondary DNS address.
2. **LAN IPv6 address settings**: you can add LAN IPv6 address, and IPv6 Link-Local address will be showed automatically.
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.

3.4.8.5 IPv6 in IPv4 Tunnel

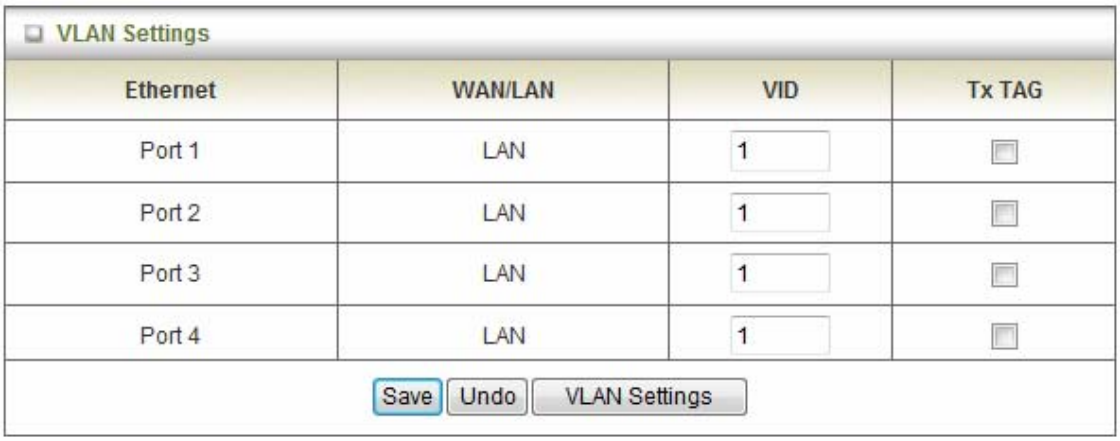


1. **IPv6 address in IPv4 Tunnel settings**: you may add remote / local IPv4 address and local IPv6 address, and then set DNS address manually for Primary DNS address and secondary DNS address.
2. **LAN IPv6 address settings**: you can add LAN IPv6 address, and IPv6 Link-Local address will be showed automatically.
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.

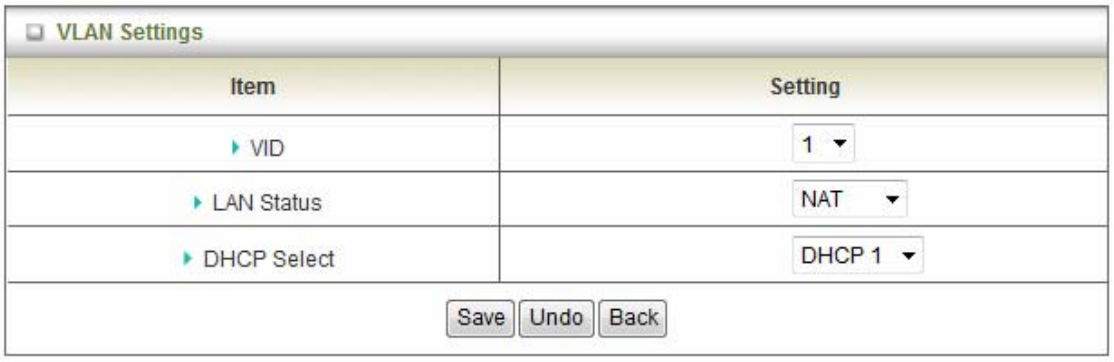
3.4.9 VLAN

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

There are four LAN ports with this router, so you can have up to 4 VLAN if required. Those four LAN ports belong to one VLAN by default. If you want to divide them into different VLAN, you just need to assign different “VID” for them. If ISP requests a “VLAN Tag” with your outgoing data, please remember to check the checkbox of “Tx TAG”.



For detailed configuration of VLAN, please press button **“VLAN Settings”** to continue.



1. **VID:** Select which VID you want to configure.
2. **LAN Status and DHCP Select:** there are two options: NAT or Bridge.

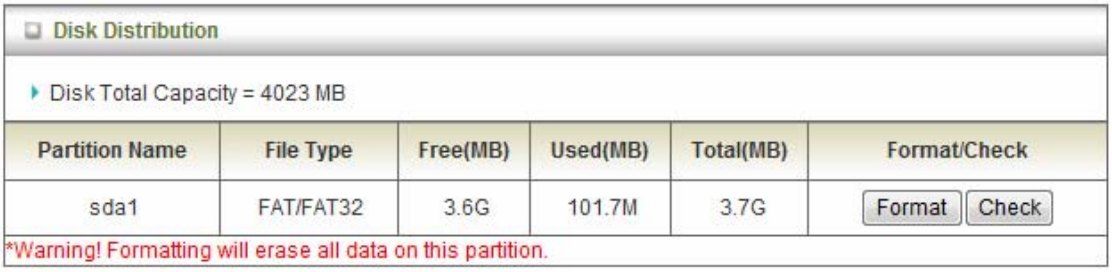
   If choose NAT: The NAT function is activated, and you can select one of DHCP server configurations to apply to this VID.

   If choose Bridge: The NAT function is deactivated, and WAN traffic will be transferred to local LAN port which has same VID.

3.5 NAS

With NAS function on this device, you can share your USB drive or USB HDD via network easily.

3.5.1 Disk Uility



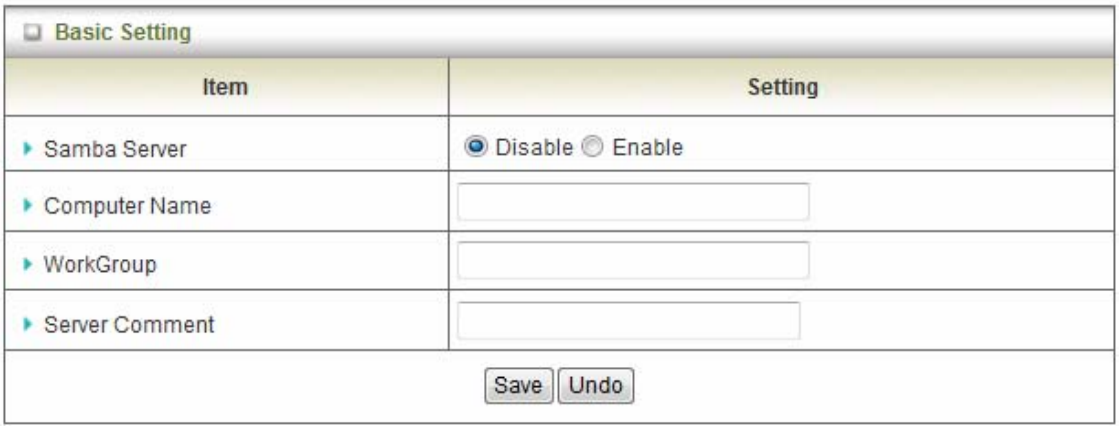
1. Format

This utility would format the certain partition.
Please be noted! This action will clear all your data in this partition. You will not be able to recover it any more.

2. Check

This utility could help you check the partition, find the lost files, try to fix some problems.

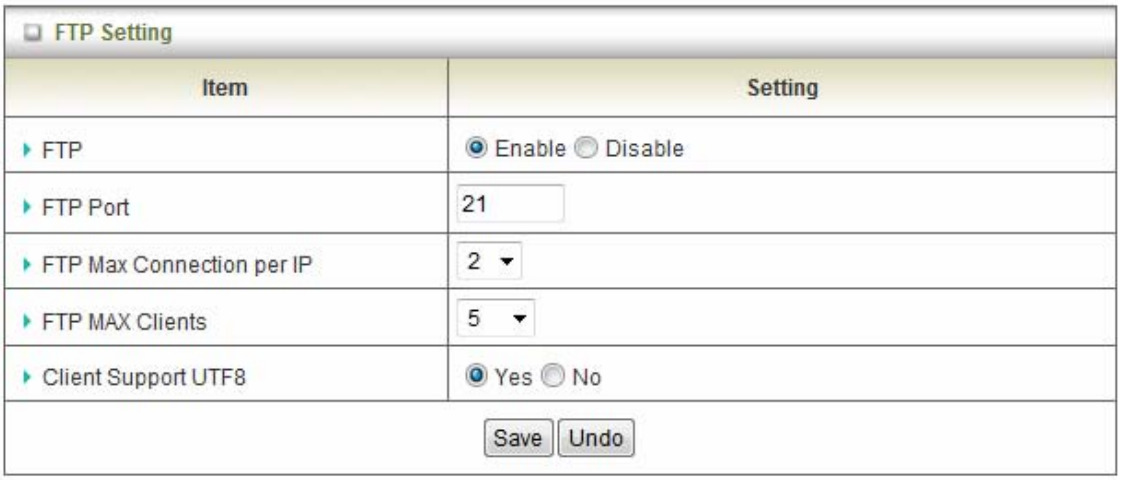
3.5.2 Samba Server



These settings are for Samba Server (Windows My Network Places).

1. **Samba Server:** Enable or Disable Samba server functions.
2. **Computer Name**
   The name that is showed on the windows network neighbors search result.
3. **WorkGroup**
   This name MUST be the same as your computer, or you could not search this device via windows.
4. **Server Comment**
   Just a comment for recognize.

3.5.3 FTP Service Configuration



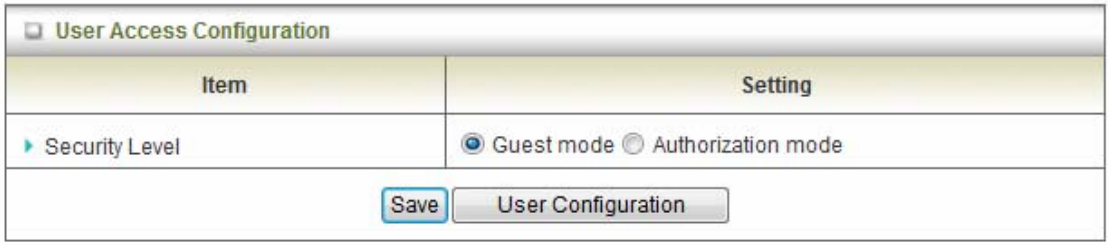
These settings are for FTP service.

1. **FTP:** Enable or disable functions of FTP server on this device.
2. **FTP Port:**
   The default port is 21, but sometimes you might want to hide your FTP service by changing it. We have the ability to receive the request on non-standard FTP port, but please be noted, some NAT router could not support non-standard FTP port, that means some of your clients might have to use passive mode to get file.
3. **FTP Max Connection per IP:** You can limit the maximum number of FTP connection for each client.
4. **FTP MAX Clients:** You can indicate how many FTP clients can access the FTP service on this device at the same time.
5. **Client Support UTF8:**
   This option is used when your FTP client could support UTF8. Usually, the default value "No" is okay for most clients.

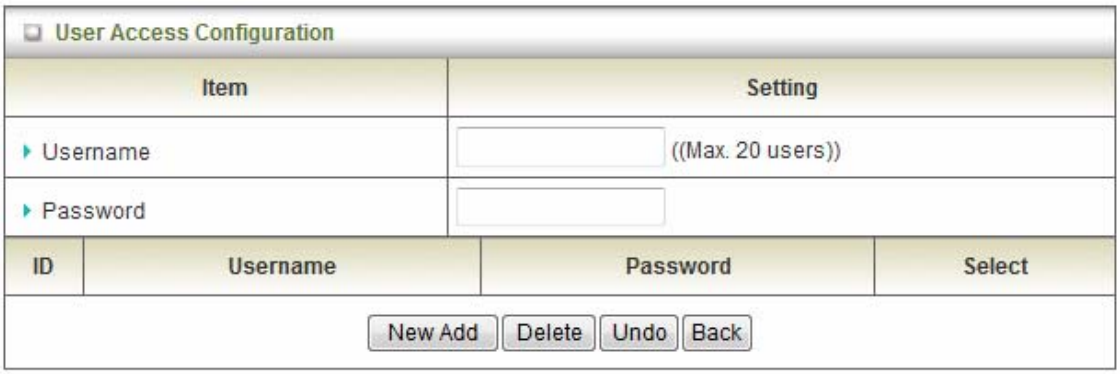
3.5.4 Access Control

The default setting is "Guest mode", all clients could access as anonymous users.

If you want to control the permission, change to "Authorization mode" and save it, then go to "User Configuration".



In this page, you can manage the user account.
Key in the user name and password then press “Add” could let you add a new user.
If you want to delete an account, select it and click “Delete” button.



3.5.5 iTunes Server

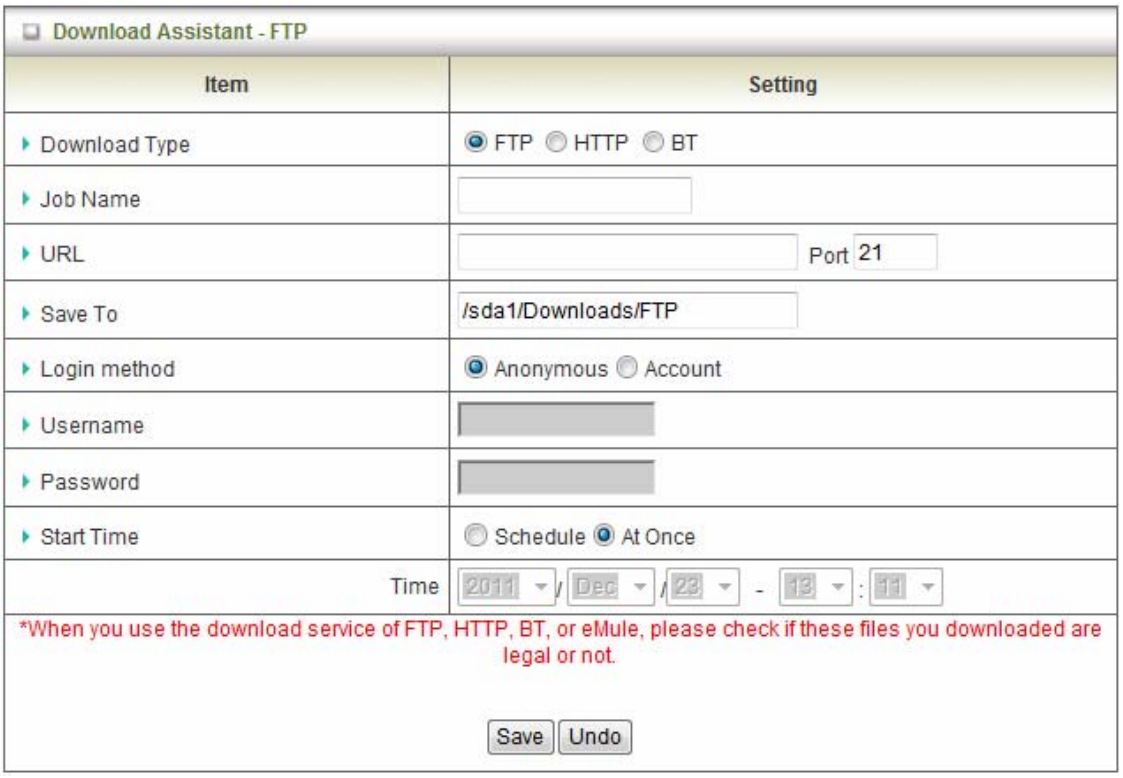
This function could enable the built-in iTunes Server to support iTunes which is a media player released by Apple.

1. **Service:** Enable or disable this function.
2. **Share Partition:** Select which partition on USB drive that you want to share.
3. **Server Name:**
   The name of this server, it will be shown on the iTunes.
4. **Service Port:**
   The TCP port for WEB management interface, for example, if the default value is 3689, then your iTunes server URL will be http://This_Device_IP:3689
5. **Access Password:**
   The password for iTunes Server WEB management interface.

3.5.6 Download Assistant

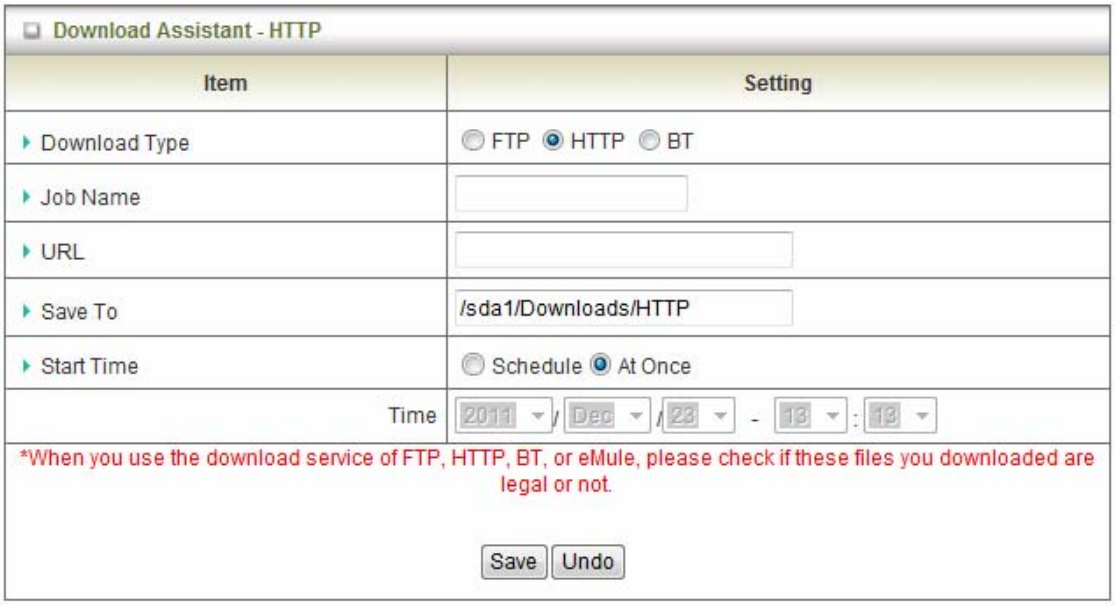
With Download Assistant, you don't need to turn the computer all day on to wait for download to be finished. This device will help you download files from remote FTP server or HTTP server automatically. You can also choose BT for P2P file download.

3.5.6.1 FTP



1. **Job Name:**
   It's for you to remember the job easily, and the device would use this name to info you when the job is done.
2. **URL:**
   The URL for the file you want to download.
   You have to use this format:
   IP/path/file, you don't have to add protocol part such like "ftp://".
3. **Save To:**
   The destination path on USB disk that you want to save files.
   Default value is /C/Download/FTP
4. **Login method:**
   Anonymous, you can access this site without any authentication
   Account, you have to enter the username and password to login.
5. **Start Time:**
   Schedule: this device will start FTP download on the time that you specified. The schedule job that is saved could be check on Status page by selecting "View Scheduled Download Status".
   At Once: the FTP download would be started immediately.

3.5.6.2 HTTP

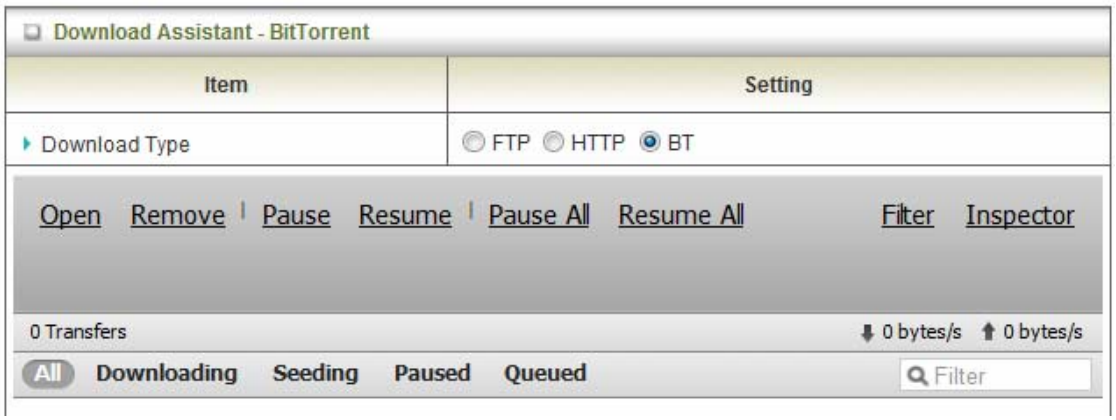


1. **Job Name:**
   It's for you to remember the job easily, and the device would use this name to info you when the job is done.
2. **URL:**
   The URL for the file you want to download.
   You have to use this format:
   IP/path/file, you don't have to add protocol part such like "http://".
3. **Save To:**
   The destination path on USB disk that you want to save files.
   Default value is /C/Download/HTTP
4. **Start Time:**
   Schedule: this device will start FTP download on the time that you specified. The schedule job that is saved could be check on Status page by selecting "View Scheduled Download Status".

   At Once: the FTP download would be started immediately.

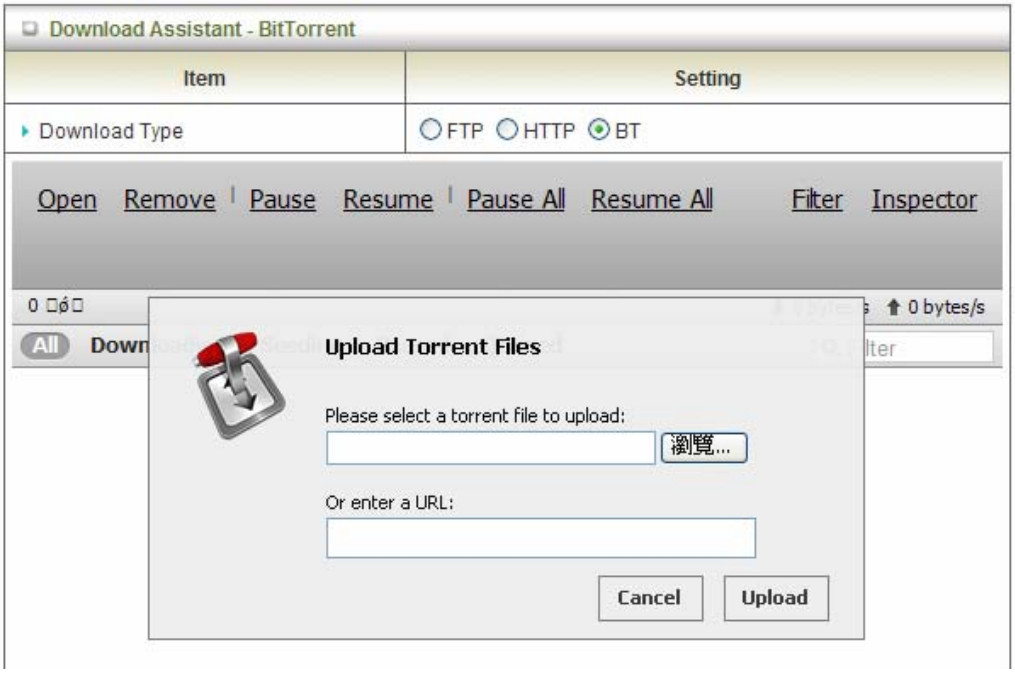
3.5.6.3 BT (Bit Torrent)

You can download file by using BT (Bit Torrent).



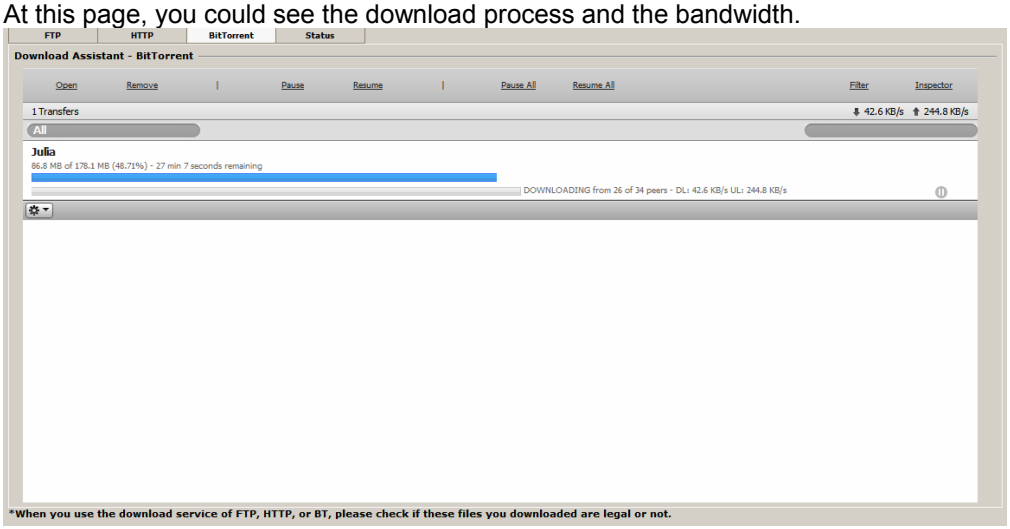
Start BT download

First, you have to get a seed file, which we called “torrent”. Then click the “Open” link on UI, it would pop up a sub menu to let you upload.
Or, if your torrent file could be download from network, you could just enter a URL.



BT download status

After you upload the torrent, download job would be started immediately.
The device could support 3 concurrent download jobs, other jobs would wait in job queue. If one of the three running job is done, the next new job would be started.
At this page, you could see the download process and the bandwidth.



Stop, Resume and Remove seed

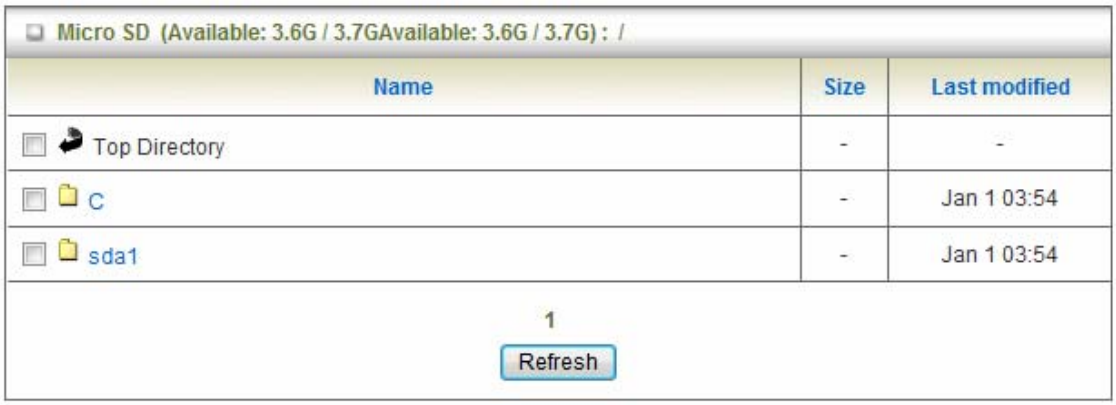
Select any job on the list, and click right button of mouse, you could see a menu with several actions you could do.
You could Stop (Pause), Resume, or Remove a job with this sub menu.

3.5.7 Download Status

Here shows all jobs for download assistant.

3.5.8 Web HDD

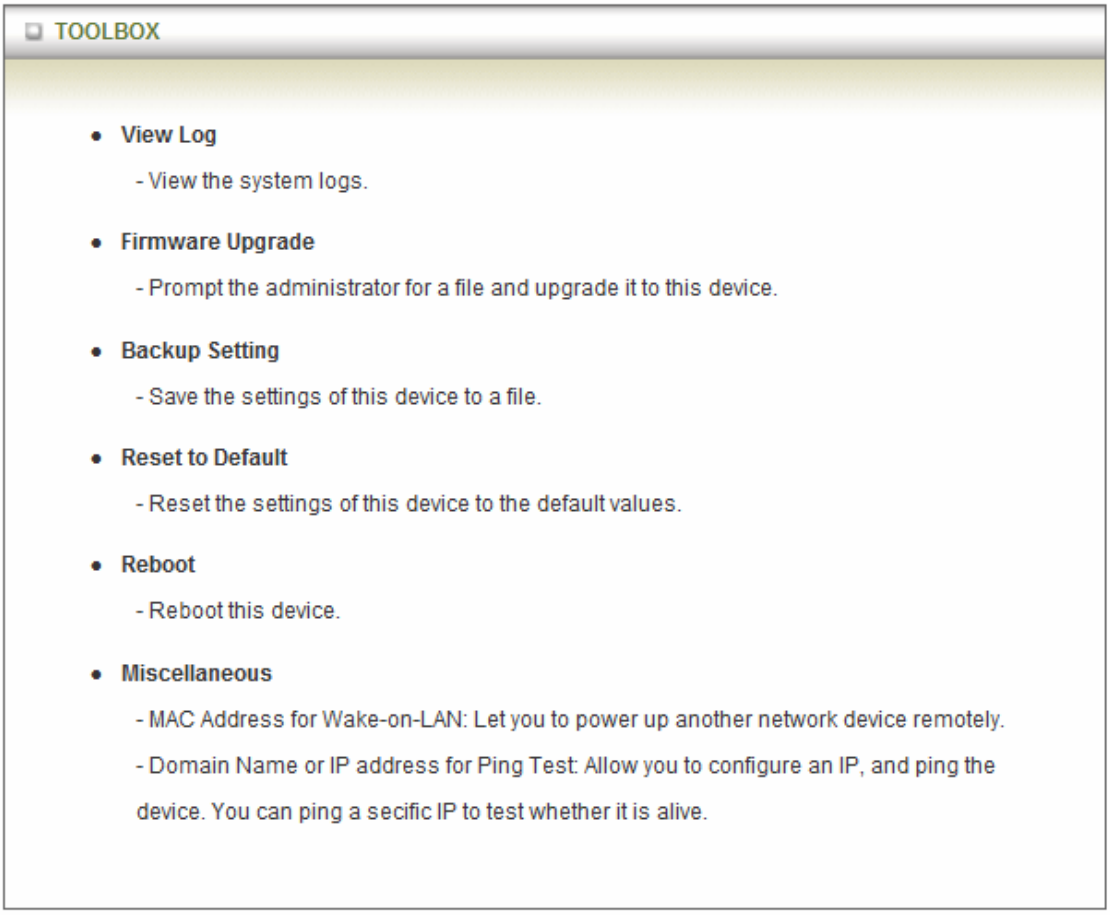
This Web HDD can allow you to enter HDD by web UI, and also can allow you to let ‘guest’ to enter the ‘public’ area only.



3.5.9 Miscellaneous

This setting is for UPnP AV media server service.

3.6 Tool Box

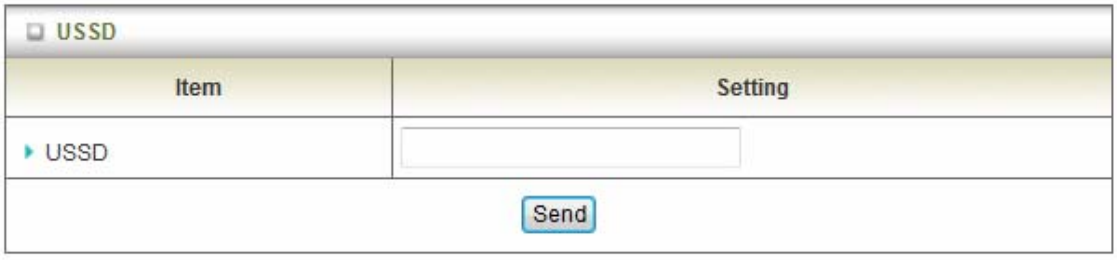

TOOLBOX
View Log
- View the system logs.
Firmware Upgrade
- Prompt the administrator for a file and upgrade it to this device.
Backup Setting
- Save the settings of this device to a file.
Reset to Default
- Reset the settings of this device to the default values.
Reboot
- Reboot this device.
Miscellaneous
- MAC Address for Wake-on-LAN: Let you to power up another network device remotely.
- Domain Name or IP address for Ping Test: Allow you to configure an IP, and ping the device. You can ping a secific IP to test whether it is alive.

3.6.1 System Info

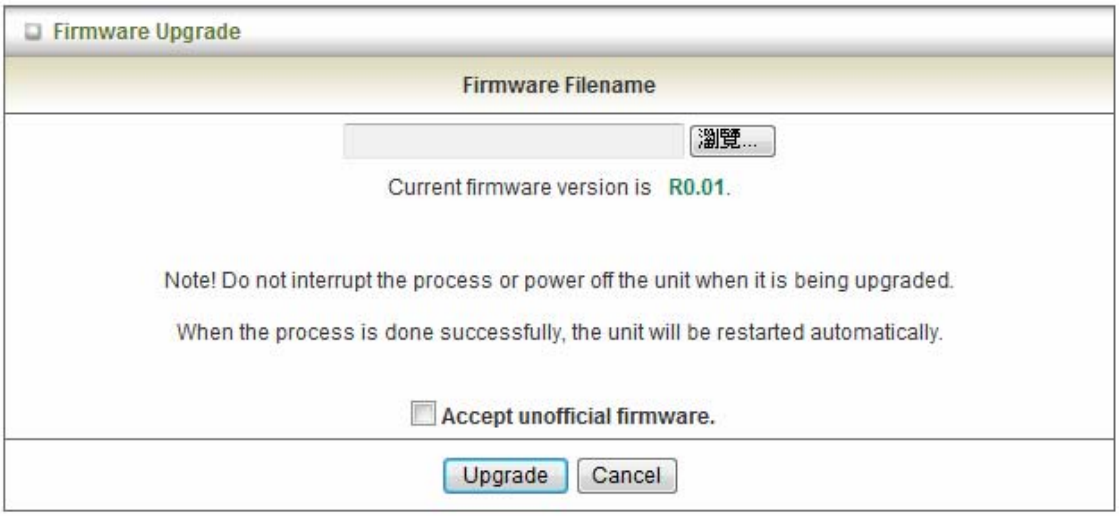
You can view the System Information and System log, and download/clear the System log.

3.6.2 USSD

USSD is a way to let subscribers finish some application on line, such as recharge SIM card.
Enter the USSD command you got from ISP or carrier, and press button “Send” to send this request to ISP or carrier. In most cases, ISP/Carrier will return a message regarding to your USSD command. The replied message will be showed at this page as well. Please note some replied message is sent back via SMS, and this device can’t deal with any SMS message. If you don’t get any response after sending the command, please call your ISP/carrier to confirm you request has been accepted.

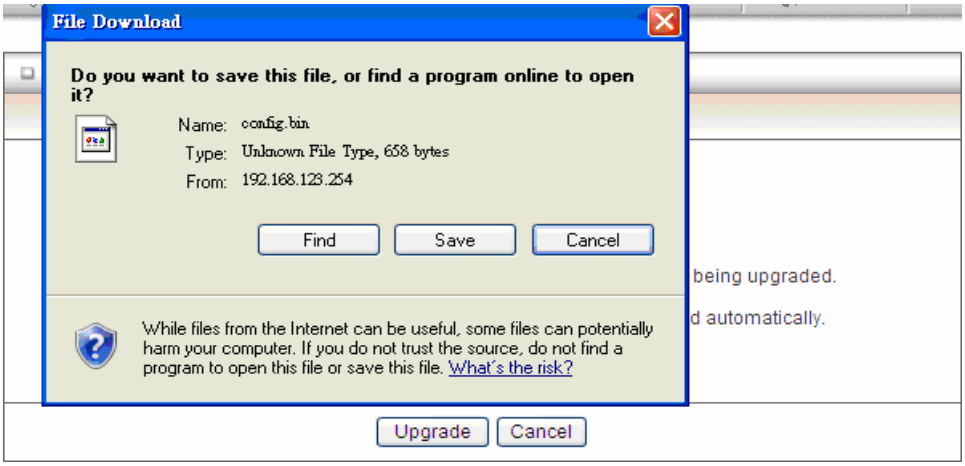


3.6.3 Firmware Upgrade



You can upgrade firmware by clicking “Upgrade” button.

3.6.4 Backup Setting

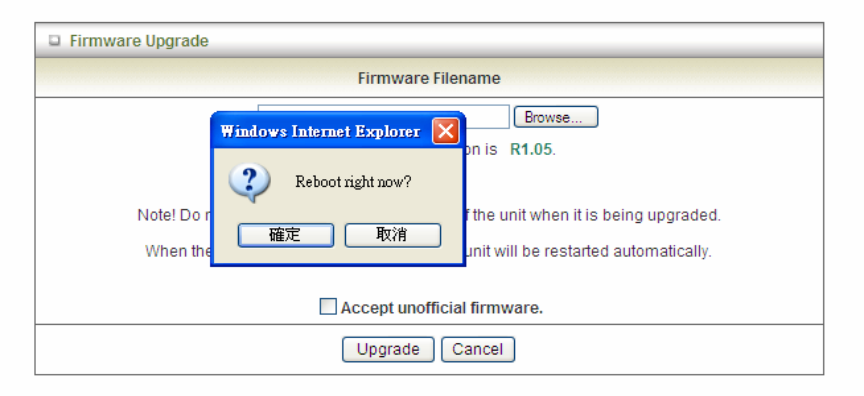


You can backup your settings by clicking the “**Backup Setting”** function item and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you saved.

3.6.5 Reset to Default

You can also reset this device to factory default settings by clicking the **Reset to default** function item.

3.6.6 Reboot



You can also reboot this device by clicking the **Reboot** function item.

3.6.7 Miscellaneous

1. **MAC Address for Wake-on-LAN:** Input MAC address of host that you want to use WOL.
2. **Domain Name or IP address for Ping Test:** Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

Chapter 4 . Troubleshooting

This Chapter provides solutions to problems for the installation and operation of the WiFi Combo Router. You can refer to the following if you are having problems.

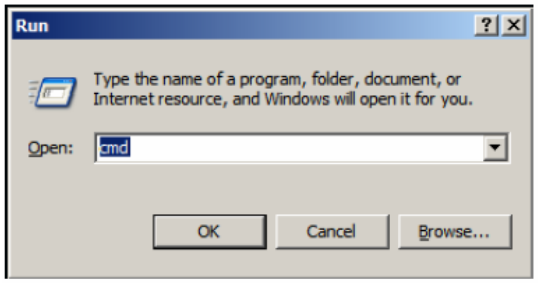
1 Why can't I configure the router even the cable is plugged and the LED is lit?

Do a **Ping test** to make sure that the WiFi Combo Router is responding.

Note: It is recommended that you use an Ethernet connection to configure it.

Go to **Start > Run**.

1. Type **cmd**.



2. Press **OK.**
3. Type **ipconfig** to get the IP of default gateway.
4. Type "**ping 192.168.123.254".** Assure that you ping the correct IP Address assigned to the WiFi Combo Router. It will show four replies if you ping correctly.

```
Pinging 192.168.123.254 with 32 bytes of data:

Reply from 192.168.123.254: bytes=32 time<1ms TTL=64
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64
```

Ensure that your Ethernet Adapter is working, and that all network drivers are installed properly. Network adapter names will vary depending on your specific adapter. The installation steps listed below are applicable for all network adapters.

1. Go to **Start > Right click on "My Computer" > Properties**.
2. **Select** the **Hardware Tab**.
3. Click **Device Manager**.
4. Double-click on "**Network Adapters"**.
5. Right-click on **Wireless Card bus Adapter** or **your specific network adapter**.

6. Select **Properties** to ensure that all drivers are installed properly.
7. Look under **Device Status** to see if the device is working properly.
8. Click "**OK"**.
9.

2 What can I do if my Ethernet connection does not work properly?

A. Make sure the RJ45 cable connect with the router.

B. Ensure that the setting on your Network Interface Card adapter is "Enabled".

C. If settings are correct, ensure that you are not using a crossover Ethernet cable, not all Network Interface Cards are MDI/MDIX compatible, and use a patch cable is recommended.

D. If the connection still doesn't work properly, then you can reset it to default.

3 Problems with 3G connection?

A. What can I do if the 3G connection is failed by Auto detection?

Maybe the device can't recognize your ISP automatically. Please select "Manual" mode, and filling in dial-up settings manually.

B. What can I do if my country and ISP are not in the list?

Please choose "Others" item from the list, and filling in dial-up settings manually.

C. What can I do if my 3G connection is failed even the dongle is plugged?

Please check the following items:

I. Make sure you have inserted a validated SIM card in the 3G data card, and the subscription from ISP is still available

II. If you activate PIN code check feature in SIM card, making sure the PIN code you fill in dial-up page is correct

III. Checking with your ISP to see all dial-up settings are correct

IV. Make sure 3G signal from your ISP is available in your environment

D. What can I do if my router can't recognize my 3G data card even it is plugged?

There might be compatibility issue with some certain 3G cards. Please check the latest compatibility list to see if your 3G card is already supported.

E. What should I insert in APN, PIN Code, Account, Password, Primary DNS, and Secondary DNS?

The device will show this information after you choose country and Telcom. You can also check these values with your ISP.

F. Which 3G network should I select?

It depends on what service your ISP provide. Please check your ISP to know this information.

G. Why my 3G connection is keep dropping?

Please check 3G signal strength from your ISP in your environment is above middle level.

4 Something wrong with the wireless connection?

A. Can't setup a wireless connection?

I. Ensure that the SSID and the encryption settings are exactly the same to the Clients.

II. Move the WiFi Combo Router and the wireless client into the same room, and then test the wireless connection.

III. Disable all security settings such as **WEP**, and **MAC Address Control**.

IV. Turn off the WiFi Combo Router and the client, then restart it and then turn on the client again.

V. Ensure that the LEDs are indicating normally. If no, make sure that the AC power and Ethernet cables are firmly connected.

VI. Ensure that the IP Address, subnet mask, gateway and DNS settings are correctly entered for the network.

VII. If you are using other wireless device, home security systems or ceiling fans, lights in your home, your wireless connection may degrade dramatically. Keep your product away from electrical devices that generate RF noise such as microwaves, monitors, electric motors…

B. What can I do if my wireless client can not access the Internet?

I. Out of range: Put the router closer to your client.

II. Wrong SSID or Encryption Key: Check the SSID or Encryption setting.

III. Connect with wrong AP: Ensure that the client is connected with the correct Access Point.

i. **Right-click** on the **Local Area Connection icon** in the taskbar.

ii. Select **View Available Wireless Networks in Wireless Configure**. Ensure you have selected the correct available network.

iii. Reset the WiFi Combo Router to default setting

C. Why does my wireless connection keep dropping?

I. Antenna Orientation.

i. Try different antenna orientations for the WiFi Combo Router.

ii. Try to keep the antenna at least 6 inches away from the wall or other objects.

II. Try changing the channel on the WiFi Combo Router, and your Access Point and Wireless adapter to a different channel to avoid interference.

III. Keep your product away from electrical devices that generate RF noise, like microwaves, monitors, electric motors, etc.

5 What to do if I forgot my encryption key?

1. Go back to advanced setting to set up your Encryption key again.
2. Reset the WiFi Combo Router to default setting

6 How to reset to default?

1. Ensure the WiFi Combo Router is powered on
2. Find the **Reset** button on the right side
3. Press the **Reset** button for 8 seconds and then release.
4. After the WiFi Combo Router reboots, it has back to the factory **default** settings.

Appendix A. Spec Summary Table

Hardware & Port Configuration		CDW68AAM-U01
Wireless WAN	USB 2.0 for external 3G/3.75G modem	1
Ethernet WAN	RJ-45 port, 10/1000Mbps, auto-MDI/MDIX	1
Ethernet LAN	RJ-45 port, 10/1000Mbps, auto-MDI/MDIX	4
USB Sharing	USB 2.0 for file sharing (shared USB port)	1
Antenna	Fixed antenna	3
WPS Button	WPS connection for 2.4G or 5G wireless	●
Wi-Fi On/Off Button	Enable/disable 2.4G or 5G wireless	●
Reset Button	Reset setting to factory default	●
LED Indication	Status/3G/NAS/2.4G WLAN/5G WLAN/WAN/LAN1~4	●
Wireless LAN (WiFi)		
Standard	IEEE 802.11a/b/g/n compliance	●
SSID	SSID broadcast or in stealth mode	●
Security	WEP, WPA, WPA2, WPA-PSK, WPA2-PSK	●
WPS/ WIfi On-Off	WPS (Wi-Fi Protected Setup) / WIfi On-Off	●
WMM	WMM (Wi-Fi Multimedia)	●
Functionality		
Wireless WAN	PPP (for WCDMA/HSPA)	●
	PPPoE (for iBurst)	●
Ethernet WAN	PPPoE/DHCP client/Static IP/PPTP/L2TP	●
Combo WAN	Auto-Failover, Load Sharing	●
IPv6 support	Dual Stack, 6-in-4, 6-to-4, Static IPv6	●
One-to-Many NAT	Virtual server, special application, DMZ	●
SPI Firewall	IP/Service filter, URL blocking, MAC control	●
DoS Protection	DoS (Deny of Service) detection	●
Routing Protocol	Static route, dynamic route (RIP v1/v2)	●
Storage/File Sharing	FAT16/FAT32, EXT2, NTFS (Read only) Samba server, FTP server	●
Media server	UPnP AV media server, iTunes server	●
Management	SNMP, UPnP IGD, syslog	●
Administration	Web-based UI, remote login, backup/restore setting	●
Environment & Certification		
Package Content	CDW68AAM-U01 , DC 12V/1.5A power adapter, CD (Manual, Utility)	●
Operation Temp.	Temp.: 0~40°C, Humidity 10%~90% non-condensing	●
Storage Temp.	Temp.: -10~70°C, Humidity: 0~95% non-condensing	●
CE, FCC, RoHS	CE/FCC, RoHS compliance	●

*Specifications are subject to change without prior notice

Appendix B. Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please refer to the GNU General Public License below to check the detailed terms of this license.

The following parts of this product are subject to the GNU GPL, and those software packages are copyright by their respective authors.

- Linux-2.4.28 system kernel
- busybox_1_00_rc2
- bridge-utils 0.9.5
- dhcpcd-1.3
- ISC DHCP V2 P5
- util-linux 2.12b for fdisk application
- e2fsprogs 1.27
- mini-lpd
- samba 2.2.7a
- syslogd spread from busybox
- wireless tools
- ntpclient of NTP client implementation
- RT61apd for 802.1X application
- vsftpd-2.0.3
- quota-tools 3.13
- GNU Wget

Availability of source code
Please visit our web site or contact us to obtain more information.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.
You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.
Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.
In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.
3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the

integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS