User Manual

CDM532AM-001
WiFi Mobile Router

Trademarks

All products, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

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.

Table of contents

Chapter 1 Introduction

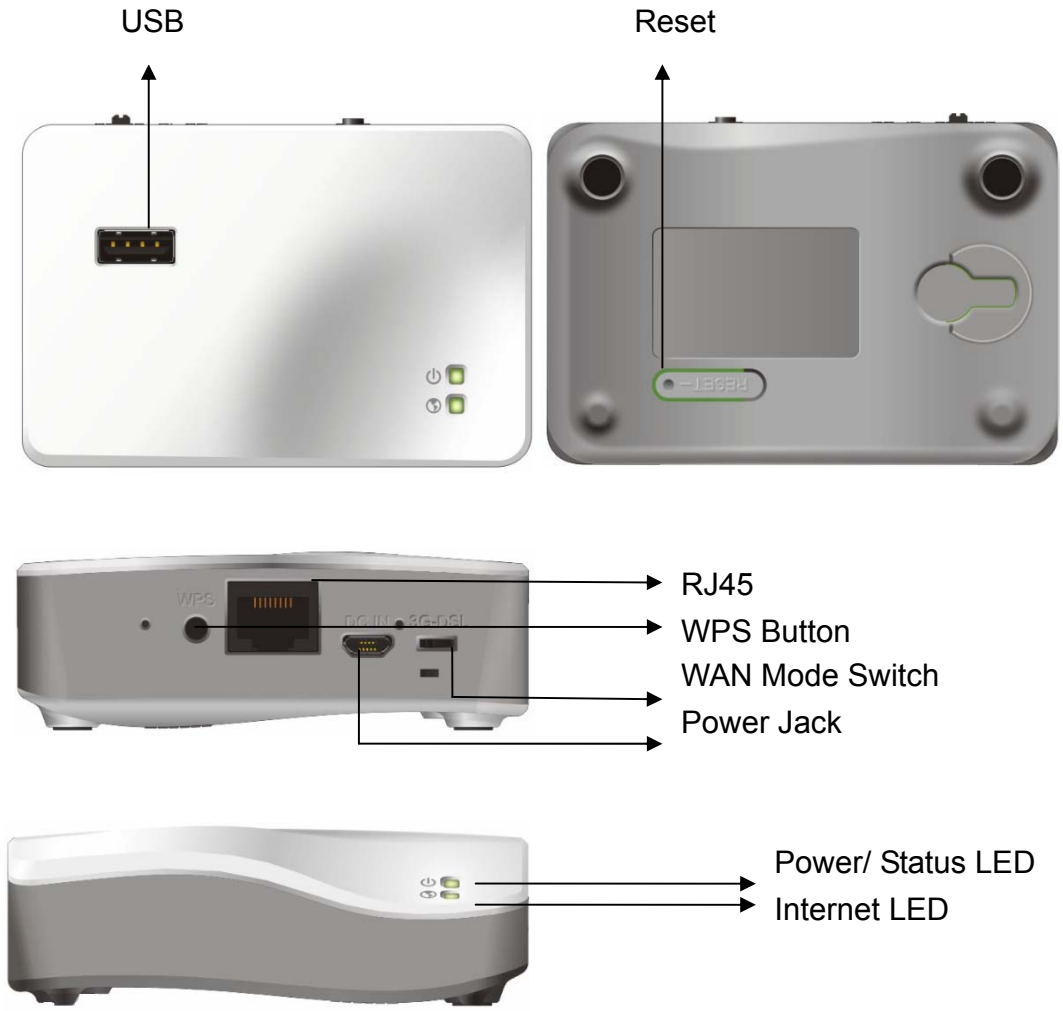
Congratulations on your purchase of this outstanding product: CDM532AM, WiFi Mobile Router. This product is specifically designed for mobile user who needs to have the Internet access beyond his/her home and office. It provides a complete solution for Internet surfing and broadband sharing. Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read this manual carefully for fully exploiting the functions of this product.

1.1 Package List

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

1.2 Hardware Installation

A. Hardware configuration



B. LED indicators

Power/ Status LED

Color	Status	Blinking Speed	Description
Green	Blinking	Slow	Device is on and system is working
Green	Blinking	Quick	Device is in Wi-Fi WPS mode
None	OFF	-	Device is powered off

Internet LED

Color	Status	Blinking Speed	Description
Red	Solid	-	Problems with Internet connection
Green	Solid	-	Internet connection is established
None	Off	-	Internet connection is dropped

C. Installation Steps for 3G Connection

Step 1. Plug in power:
Connect with the power adapter to the receptor on the back panel of it. Then the device will be powered on.

Step 2. Set WAN mode switch:
Set WAN mode switch at “3G” side.

Step 3. Connect with a USB 3G modem:
Plug your USB modem which is with activated SIM card provided by your 3G service provider.

Step 4. Connect with Ethernet Cable
Insert the Ethernet cable into RJ45 Ethernet Port on the back panel. And then plug the other end of RJ45 into the computer or Laptop computer.

Step 5. Start to configure the device:
You can start to configure the device via the Easy Setup Utility.
(see Easy Setup Utility in CD)

Note. If you set WAN mode switch at “DSL” side, the Ethernet port will became WAN port for you connect to xDSL modem. Your PC or laptop can only connect to it via WLAN at this condition.

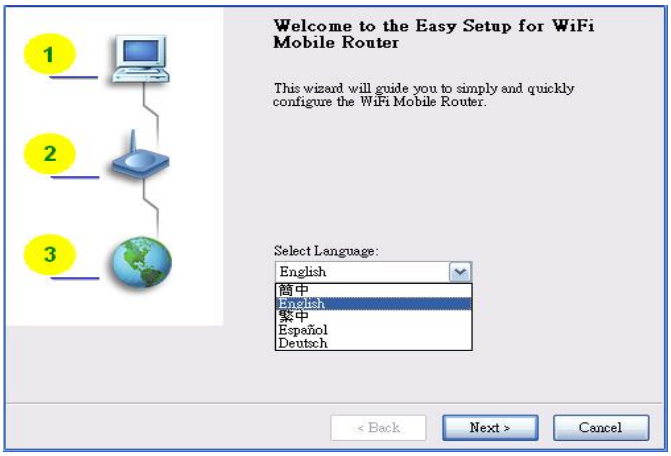
Chapter 2 Getting Started with Easy Setup

There are two approaches for you to set up the WiFi Mobile 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.

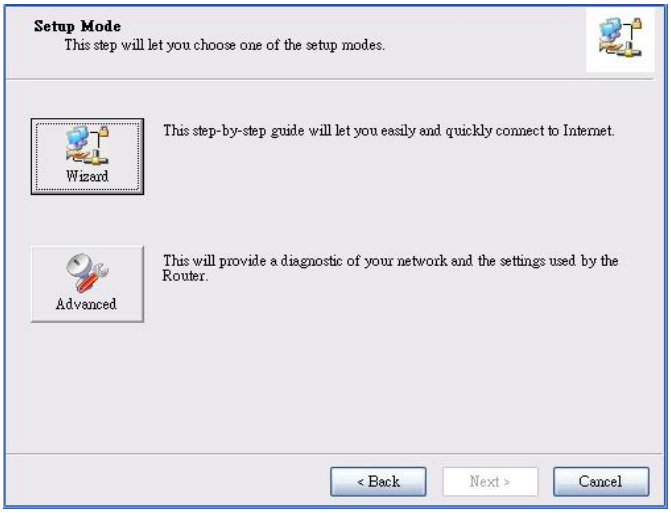
2.1 Easy Setup by Windows Utility

Step 1：
Install the Easy Setup Utility from the provided CD then follow the steps to configure the device.

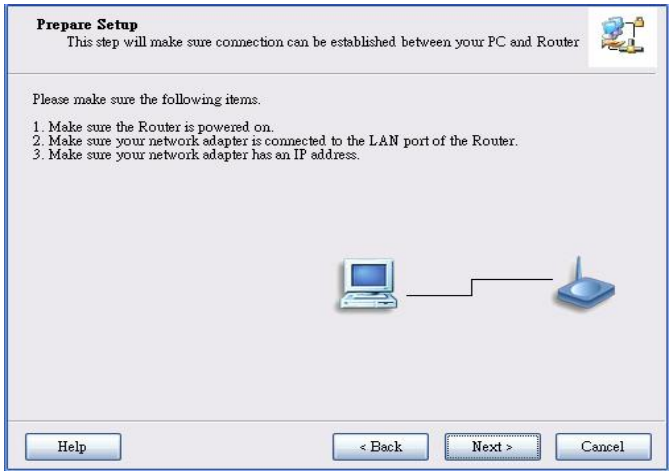
Step 2：
Select Language then click “Next” to continue.



Step 3：
Then click the “Wizard” to continue.

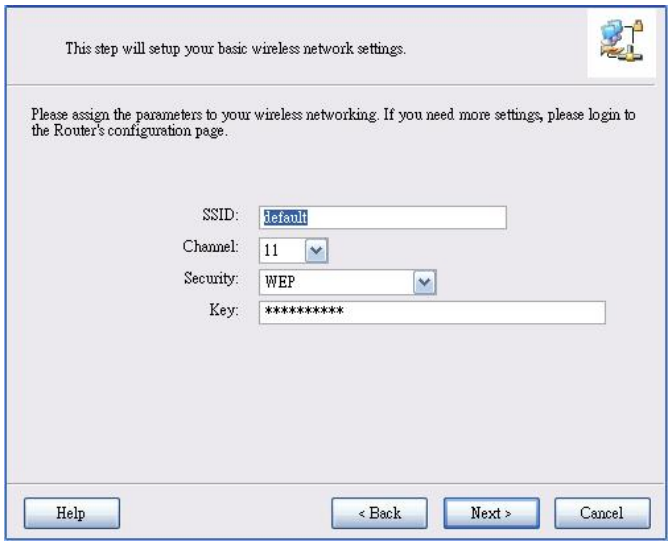


Step 4：
Click “Next” to continue.



Step 5：
Select Enable for Wireless if you want to setup WLAN configurations. Then click “Next” to continue.

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



Step 7：

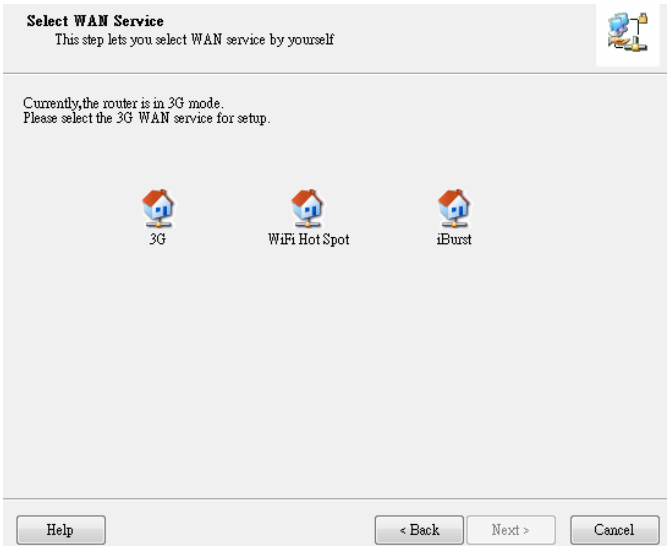
This utility will detect your WAN service automatically, or you can choose it by yourself.

Here we check “Let me select WAN service by myself”.

Step 8：

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

Note. If you set WAN switch to “DSL” mode, you can see other WAN options here.

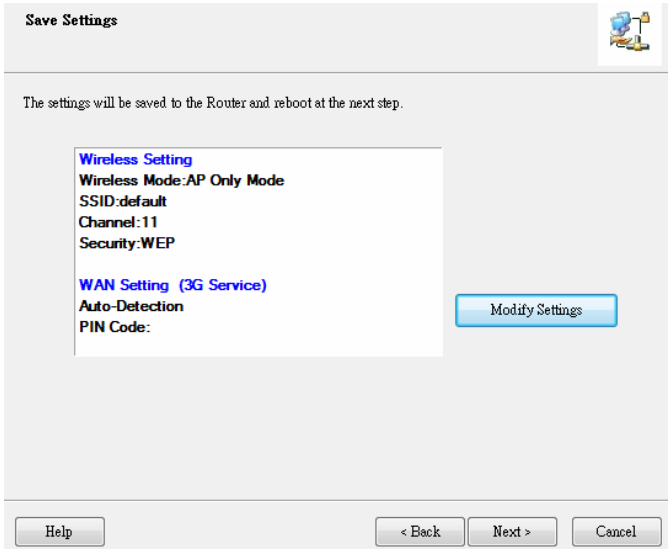


Step 9-1：

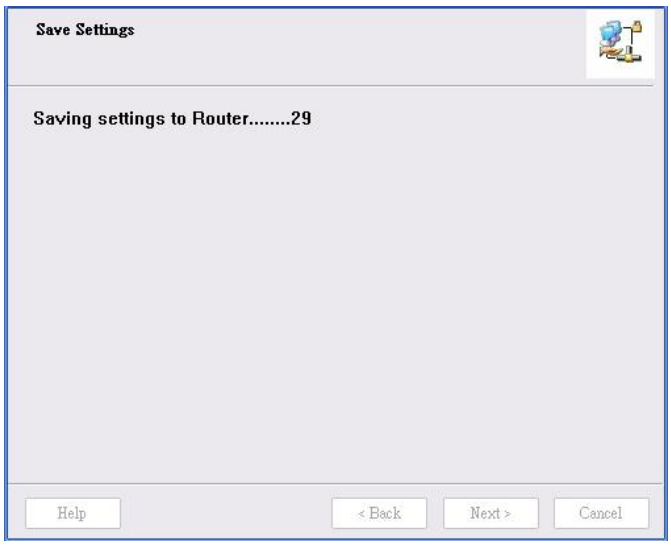
Select “Auto-Detection”, and the Utility will try to detect and configure the required 3G service settings automatically. Click “Next” to continue.

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：
This page will show new configurations you have set.
Click “Next” to continue.



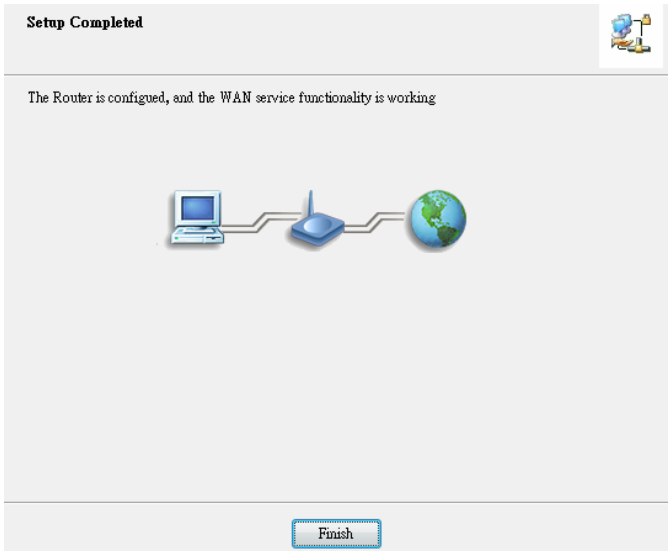
Step 11：
The WiFi Mobile Router is rebooted to make your entire configuration take effect.



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：
WAN connection is tested successfully. Clink “Finish” button to quit this utility.

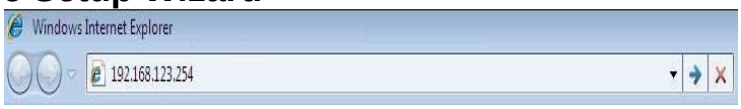


2.2 Easy Setup by Configuring Web Pages

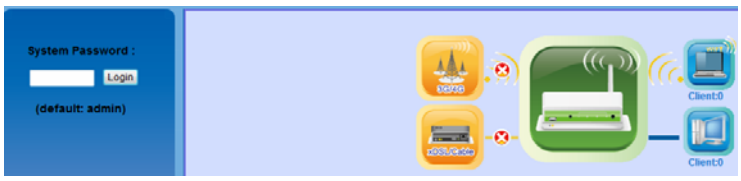
You can also browse web UI to configure the device.

Browse to Activate the Setup Wizard

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



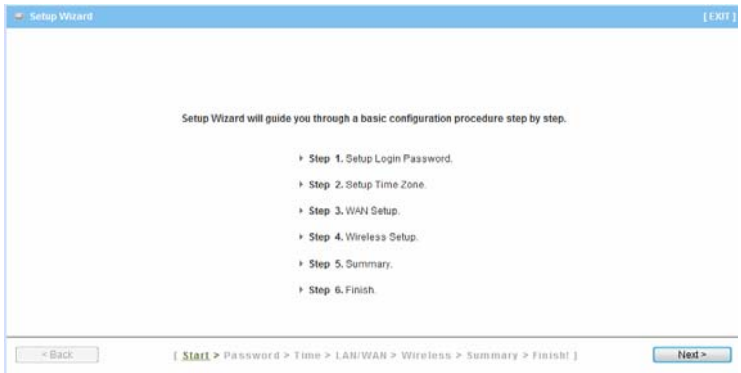
Type in the default password “admin” in the System Password and then click ‘login’ button.



Select your language.

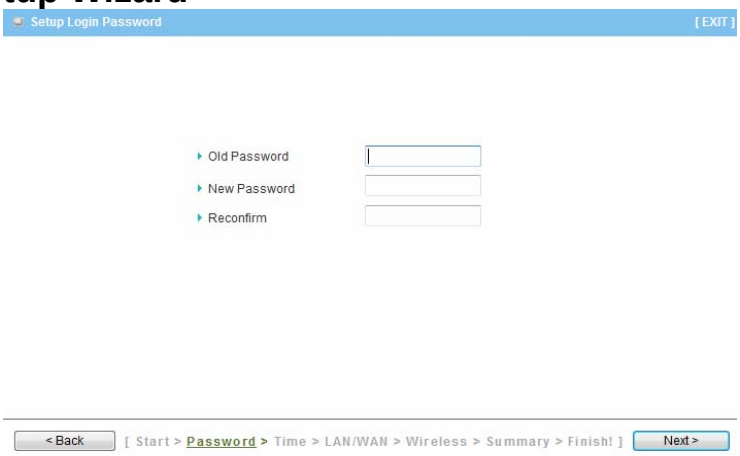
Select “Wizard” to proceed basic settings.

Click “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.

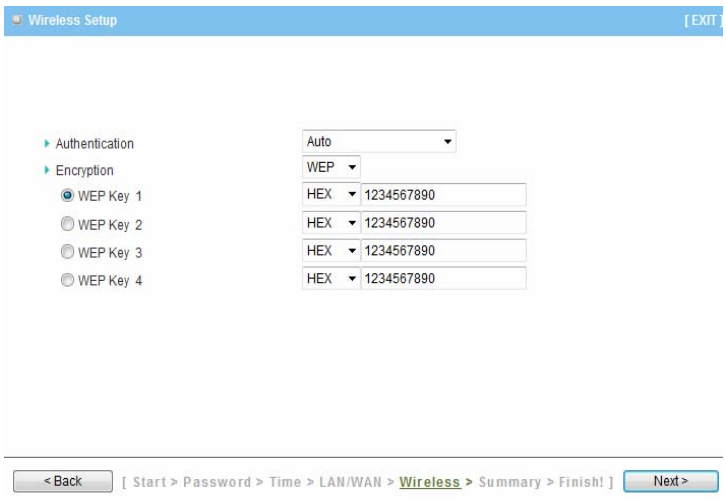
Step 3:
Select Wan Type.
Please set LAN IP address of this device. If you want to use 3G service as the main Internet access, please choose WAN type as “3G”.

Note. If you set WAN switch to “DSL” mode, you can see other WAN options here.

Step 4:
Setup 3G profile.
Select “Auto Detection”.

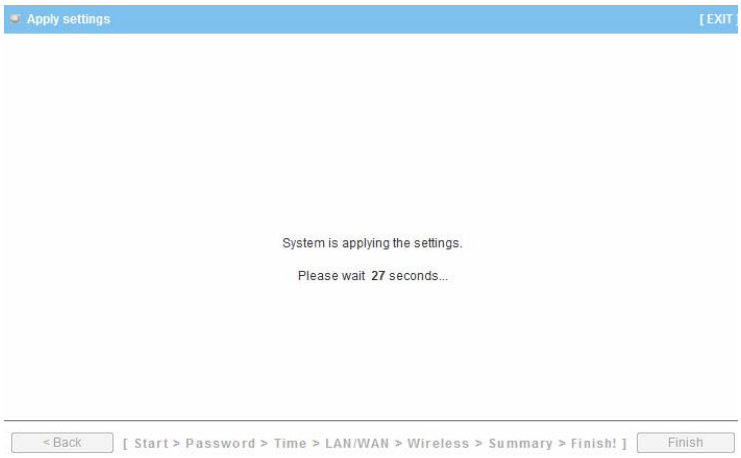
Step 5:
Setup your Wireless Network and SSID.

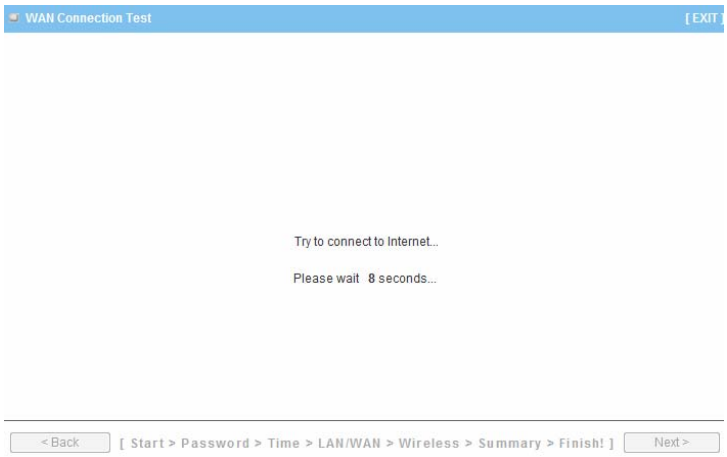
Step 6:
Setup Wireless Security configurations.



Step 7:
Applying new configurations you have set. Click “Next” to continue.

Step 8:
The device will save all new settings, and reboot automatically. After reboot, it will try to connect to Internet according to new settings.

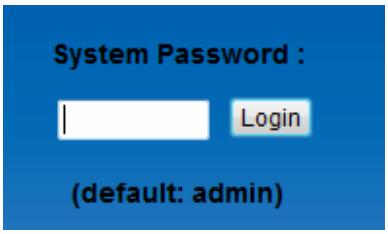




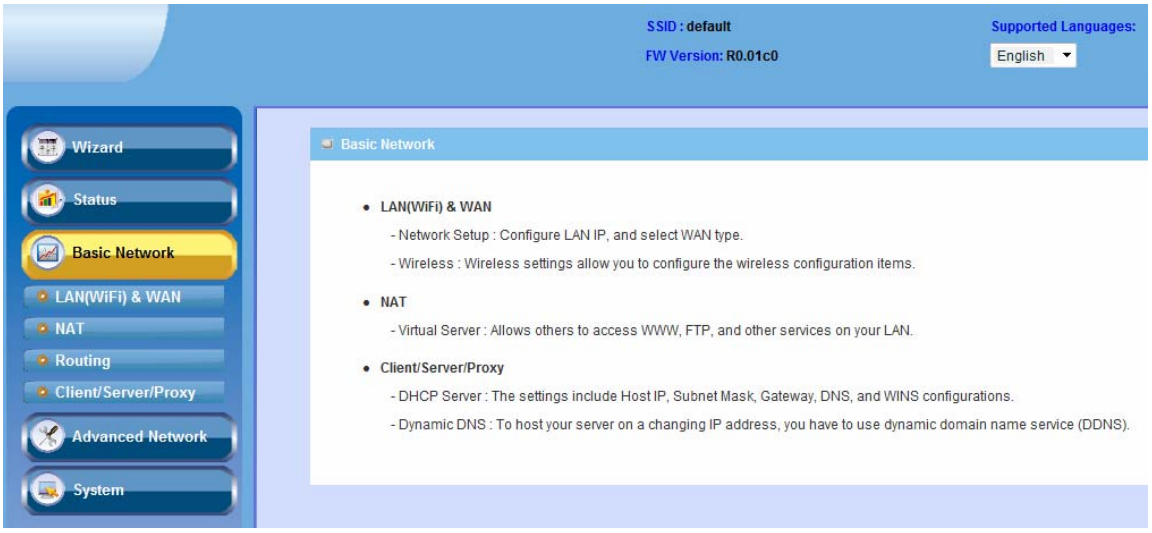
Chapter 3 Making Configuration

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.

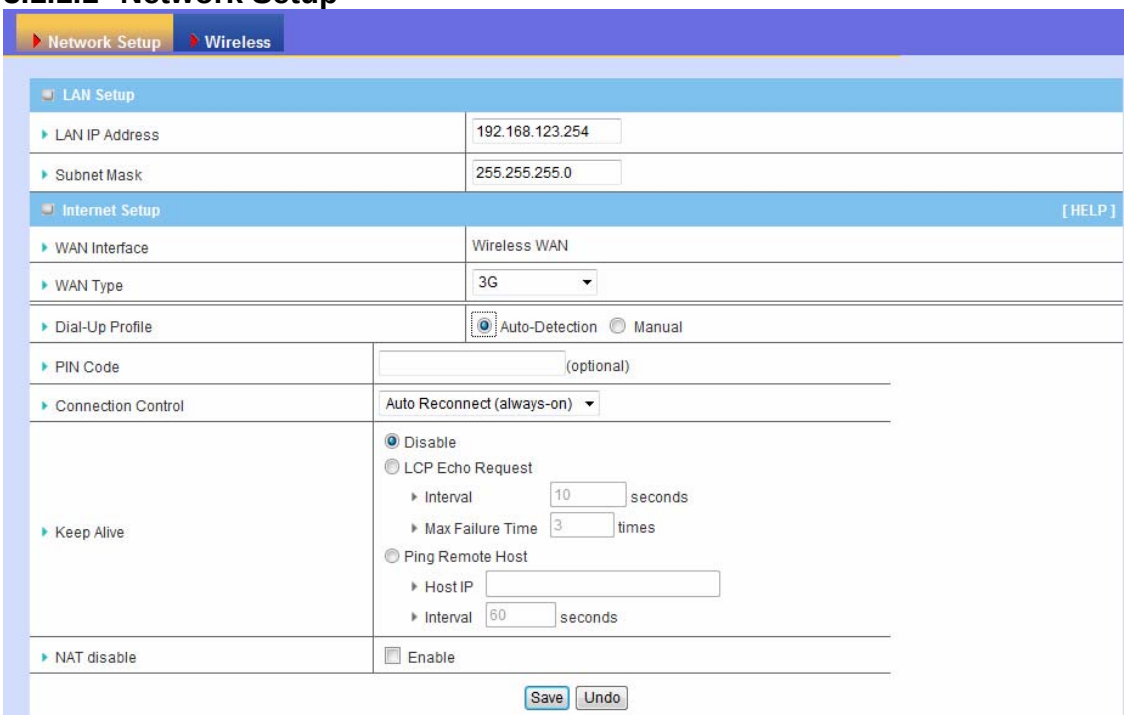


3.1 Basic Network Setting



3.1.1. LAN(WiFi) & WAN

3.1.1.1 Network Setup

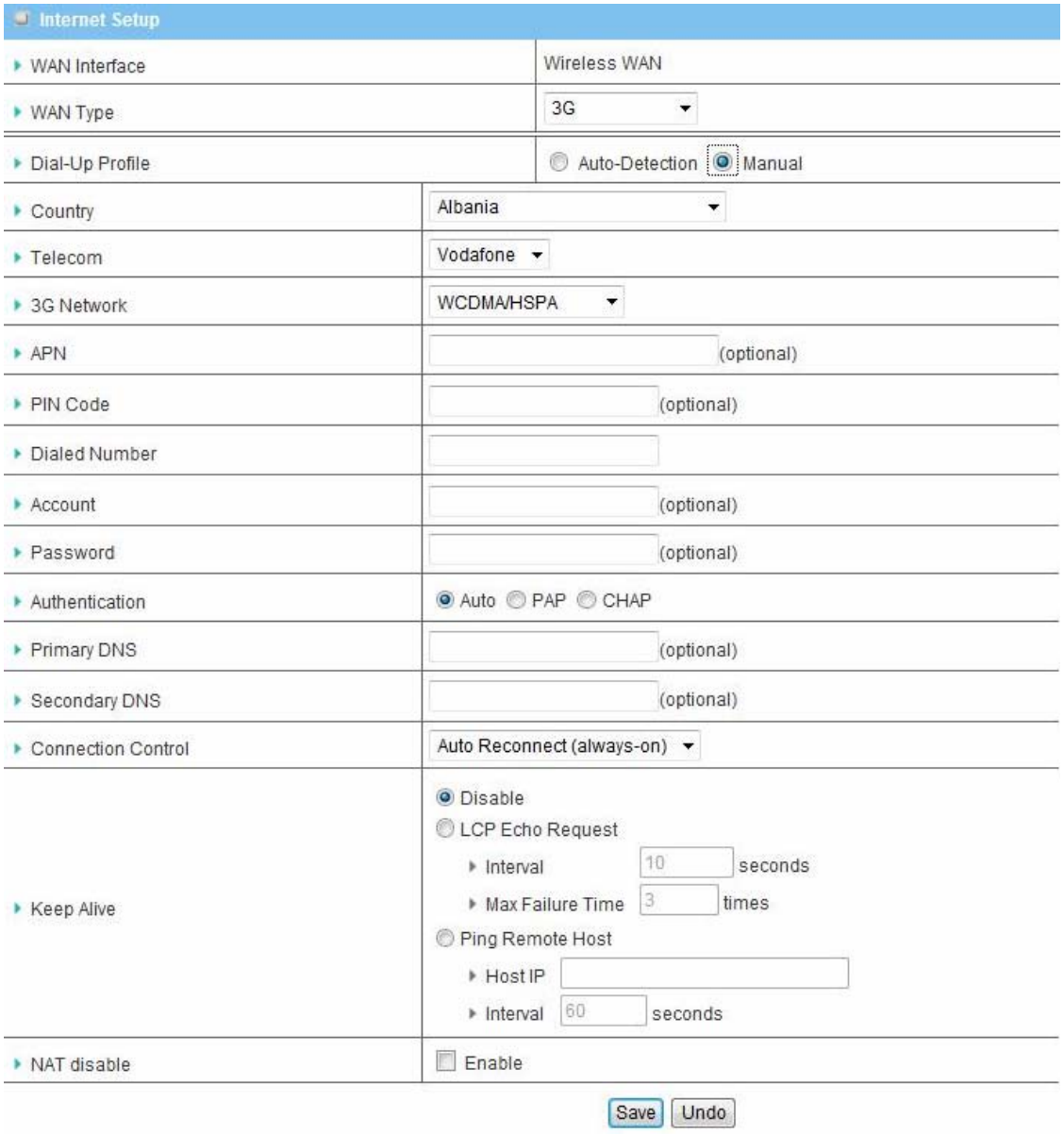


1. **LAN IP Address:** The local IP address of this device. The computers on your network must use the LAN IP address of this device as their default gateway. You can change it if necessary.
2. **Subnet Mask:** Input your Subnet mask. (All devices in the network must have the same subnet mask.) The default subnet mask is 255.255.255.0.
3. **WAN Interface:** This shows Ethernet WAN or Wireless WAN according to WAN mode switch on the device.
4. **WAN Type**: If WAN mode switch is set to “3G”, you can see 3G, iBurst, Wi-Fi HotSpot options from the drop-down list. Otherwise, if WAN mode switch is set to “DSL”, there will be Dynamic IP address, Static IP address, PPP over Ethernet(PPPoE), PPTP, and L2TP for WAN 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 and iBurst WAN connections.

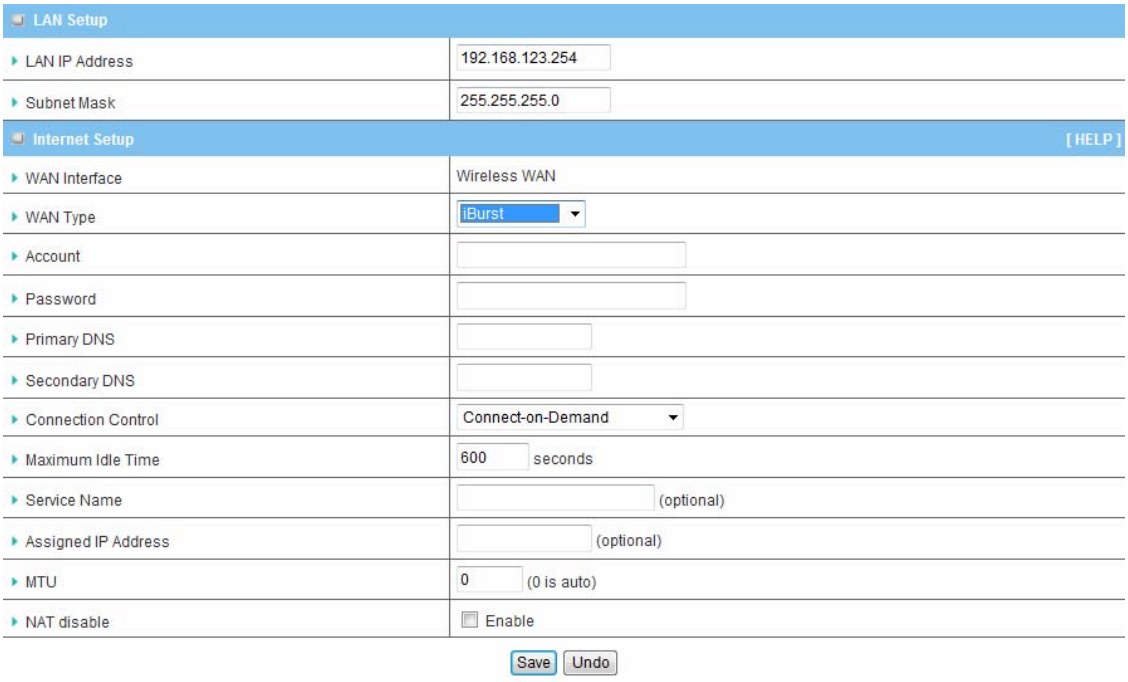


1. **WAN Type:** Choose 3G for WAN connection.
2. **Dial-Up Profile:** Please select Auto-Detection or Manual. You can choose “Auto-Detection”, and the router will try to detect and configure the required 3G service settings automatically. Otherwise, you can select “Manual”, and manually fill in the 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. **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.
16. **NAT Disable:** You can disable NAT feature if required.

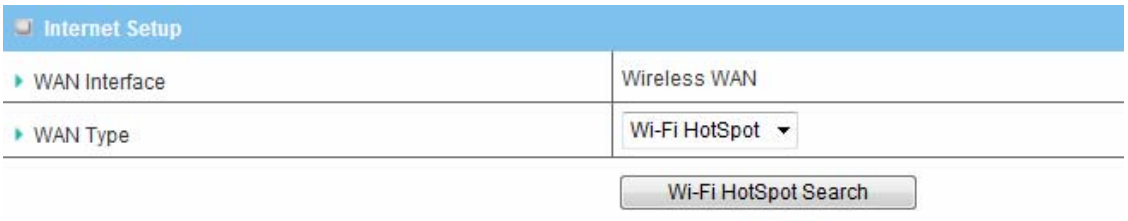
Note. The items with * above are only available when choosing Manual for Dial-up Profile.

B. iBurst



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.

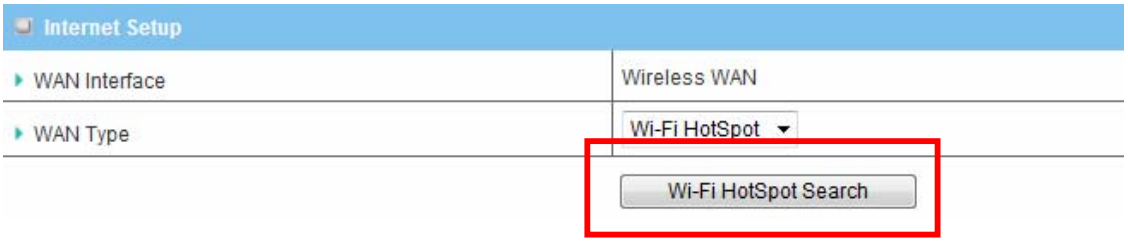
C. Wi-Fi HotSpot



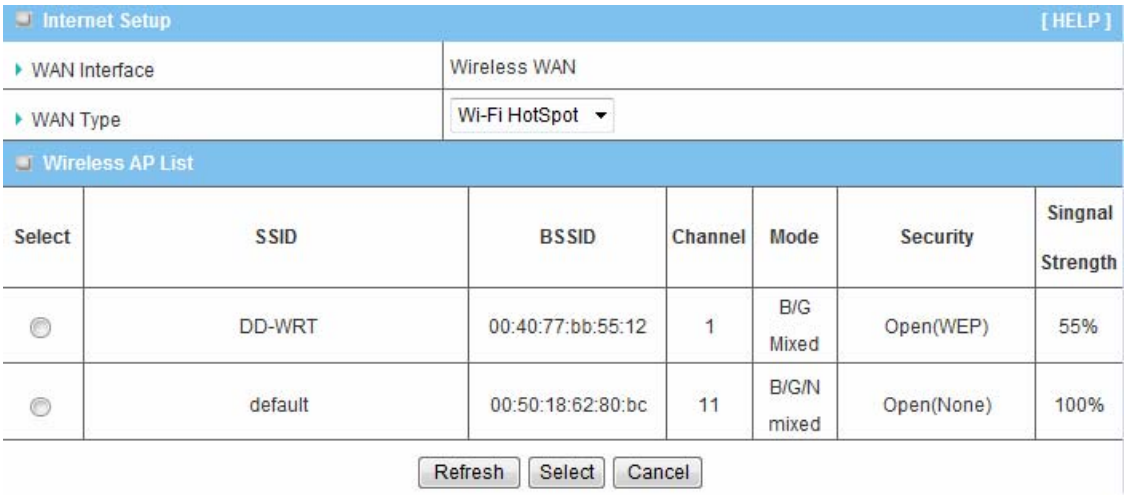
WAN Type: Choose Wi-Fi HotSpot. This WAN type allows you to share one Wi-Fi Hotspot account with your friends or colleagues. Local clients connect to this device via Wi-Fi connection, and surfing Internet by connecting to remote Wi-Fi Hotspot. Just follow a few steps below to connect to remote Wi-Fi HotSpot.

Note. If choosing Wi-Fi HotSpot WAN type, the wireless channel of WLAN will be set to as same as wireless channel of remote Wi-Fi HotSpot.

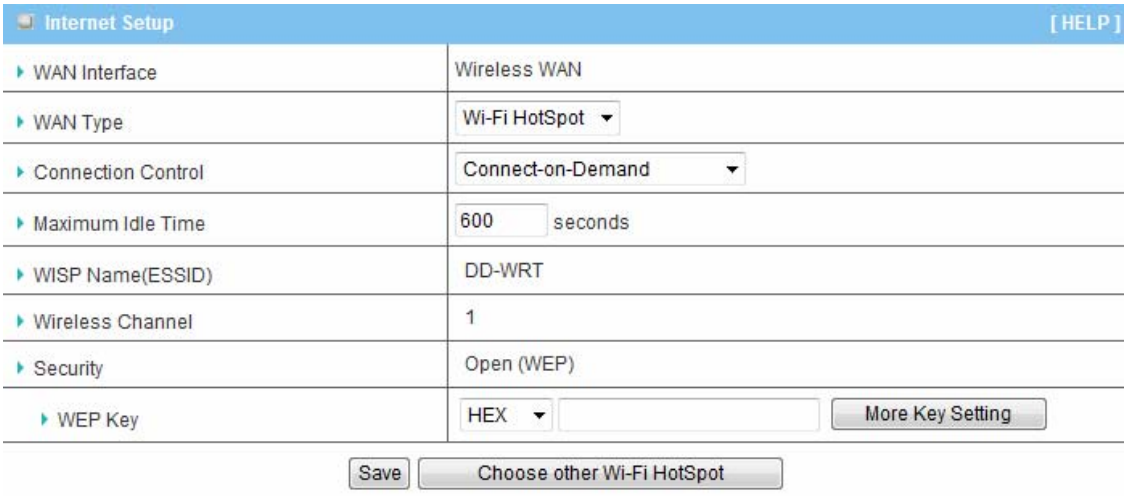
Step 1: Click "Wi-Fi HotSpot" Search" button to search any available Wi-Fi Hotspot or Wi-Fi AP (Access Point) in your environment.



Step 2: After finish searching, it will list all available Wi-Fi APs in your environment. You can select one of the lists to start to connect, or press "Refresh" button to search again.

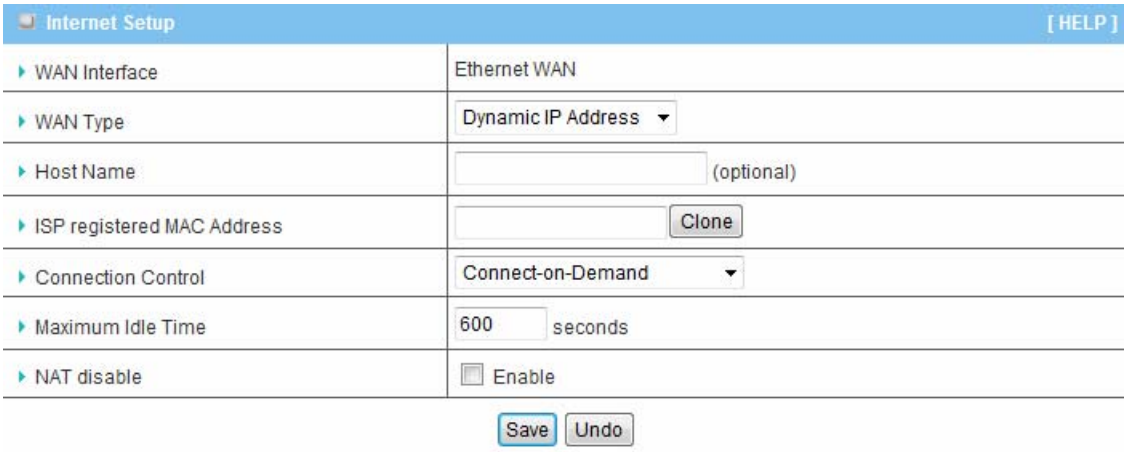


Step 3: Click “Save” button to save settings after selecting. There will be a field here for you to input encryption key if remote Wi-Fi Hotspot or Wi-Fi AP requires.



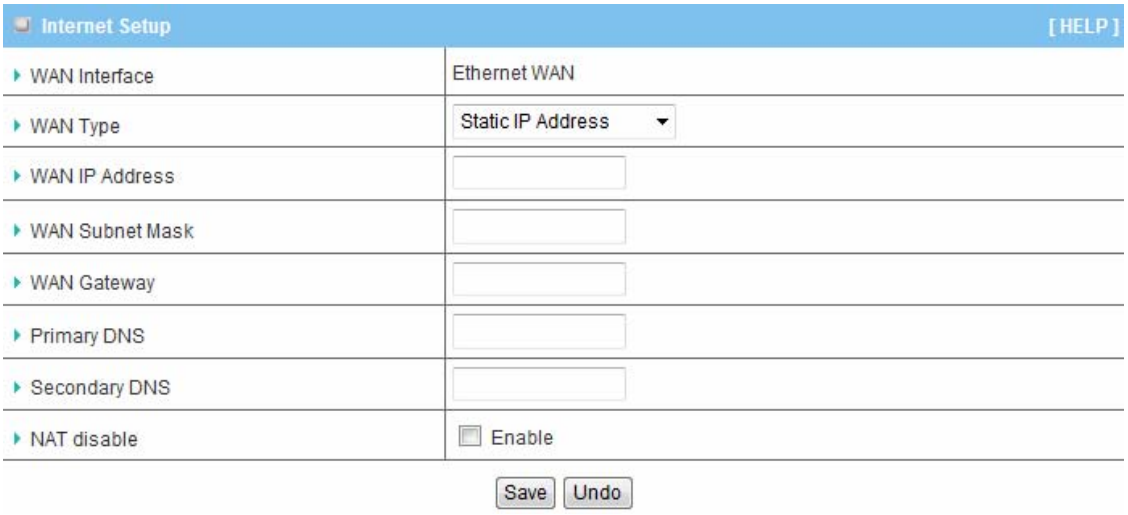
Step 4: Click “Reboot” button to restart device to take new settings effective.

D. Dynamic IP Address



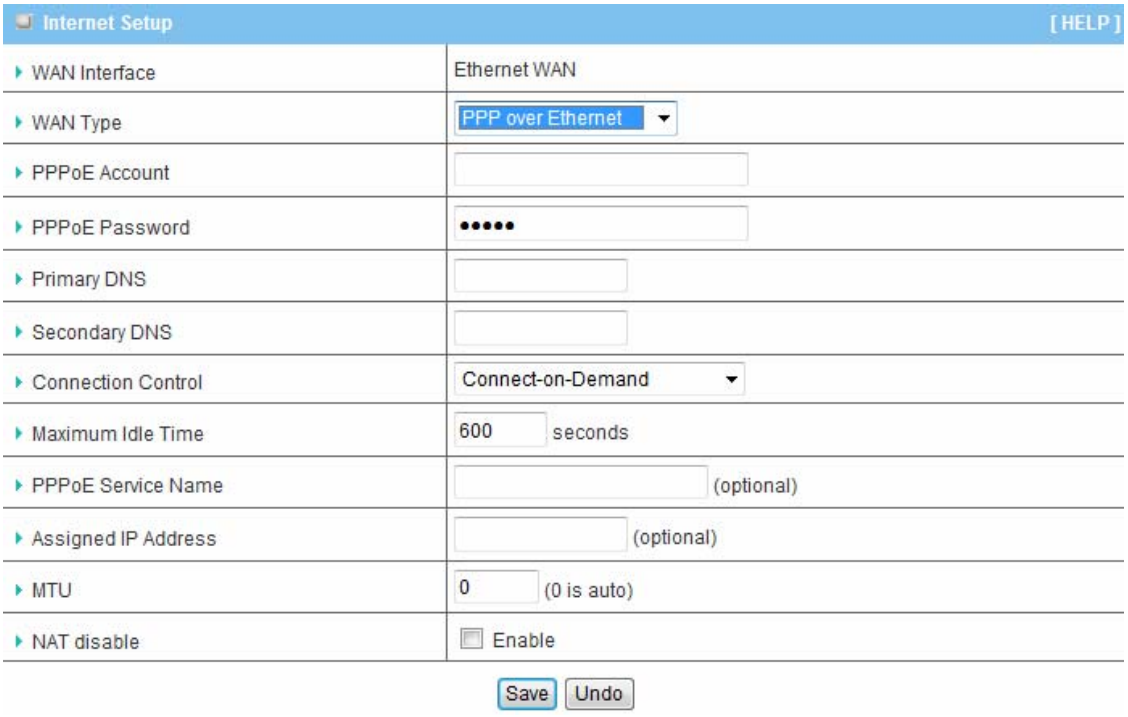
1. **WAN Type:** Choose Dynamic IP Address.
2. **Host Name**: Optional, required by some ISPs, for example, @Home.
3. **ISP registered MAC Address**: Some ISP (Cable company) will record your MAC address on PC. You can press “Clone” button to copy the MAC address on your PC here, or you can input it manually.
4. **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.
5. **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.
6. **NAT disable:** You can disable NAT feature if required.

E. Static IP Address



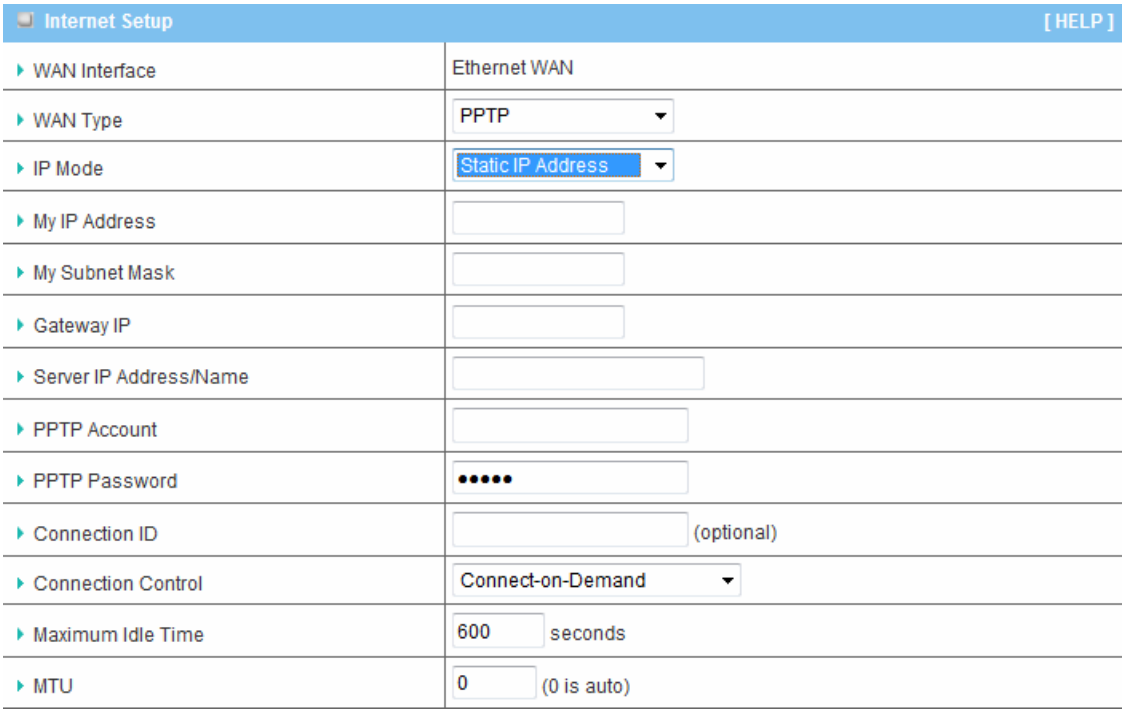
1. **WAN Type:** Choose Static IP Address.
2. **WAN IP Address:** Input the IP address you got from ISP.
3. **Subnet Mask:** Input the subnet mask of IP address you got from ISP.
4. **WAN Gateway:** Input the IP address of WAN gateway you got from ISP.
5. **Primary DNS:** Input the IP address of primary 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.

F. PPP over Ethernet (PPPoE)



1. **WAN Type:** Choose PPP over Ethernet.
2. **PPPoE Account** and **Password**: The account and password your ISP assigned to you.
3. **Primary DNS:** You can indicate IP address of primary DNS if required.
4. **Secondary DNS:** You can indicate IP address of secondary DNS if required.
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. **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.
7. **PPPoE Service Name**: Optional. Input the service name if your ISP requires it.
8. **Assigned IP Address:** You can input a IP address if you got a fix IP address from ISP.
9. **Maximum Transmission Unit (MTU):** Most ISP offers MTU value to users. The default MTU value is 0 (auto).
10. **NAT disable:** You can disable NAT feature if required.

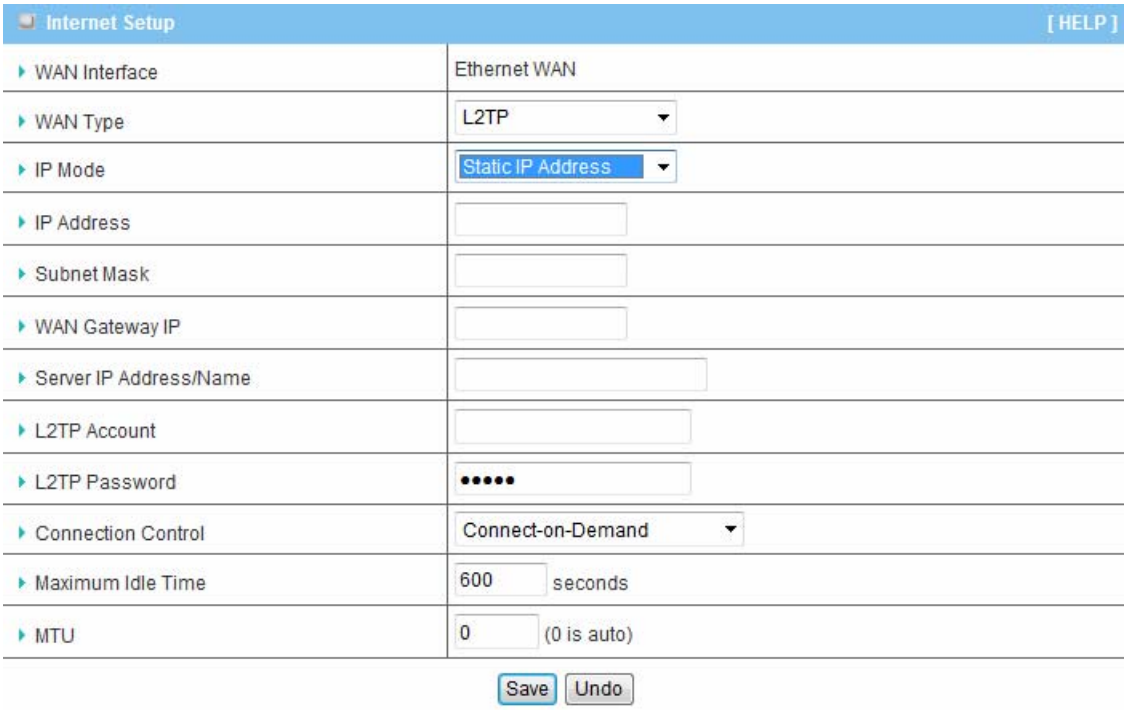
G. PPTP



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).

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

H. L2TP

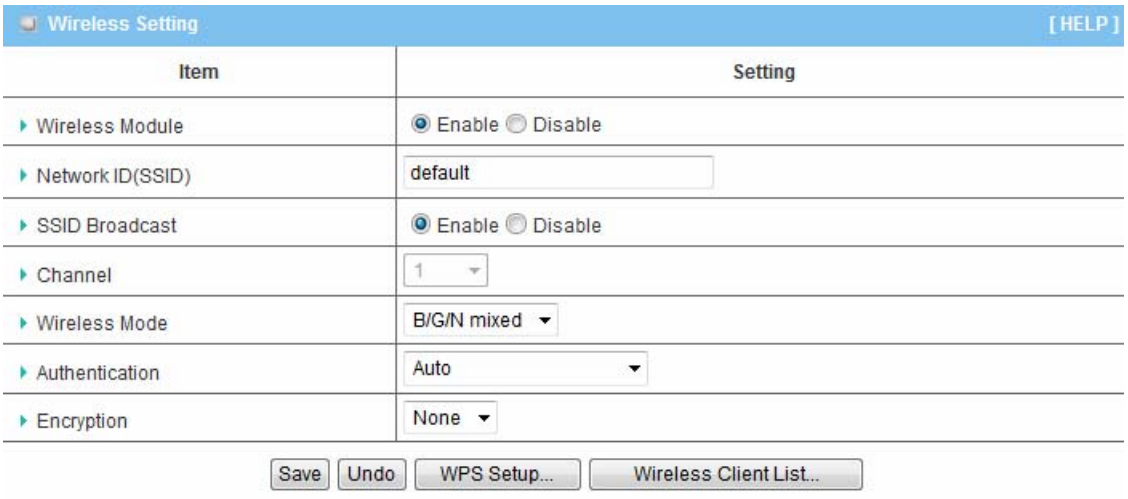


1. **WAN Type:** Choose L2TP.
2. **IP Mode**: You can select “Static IP Address” or “Dynamic IP Address”.
3. **My IP Address***, **My Subnet Mask*, and Gateway IP***: The IP address, subnet mask, and IP address of gateway your ISP assigned to you.
4. **Server IP Address/Name**: The IP address of the 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).

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

3.1.1.2 Wireless

Wireless settings allow you to set the WLAN (WiFi) configuration items.



1. **Wireless Module:** You can enable or disable WLAN function.
2. **Network ID (SSID):** Network ID is used for identifying the Wireless LAN (WLAN). (The factory default setting is “default”)
3. **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 this device.
4. **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).
5. **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”.
6. **Authentication & Encryption:** You may select one of authentication to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK.

   ■ **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. In this mode, you can choose no encryption or WEP encryption.

- **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. In this mode, WEP encryption is required.

- **Auto**

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

- **WPA-PSK**

Select TKIP or AES 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

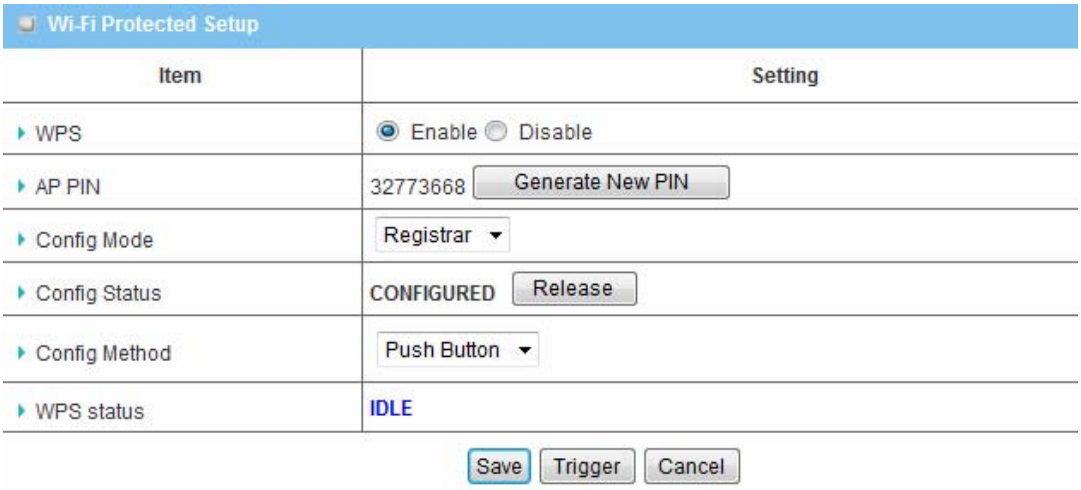
- **WPA2-PSK**

Select TKIP or AES 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-PSK/WPA2-PSK**

If selecting WPA-PSK/WPA2-PSK mixed mode, wireless clients can connect to this router via WPA-PSK or WPA2-PSK.

By pressing **"WPS Setup"**, you can configure and enable the easy setup feature WPS (Wi-Fi Protected 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 a new 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 "IDLE"

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

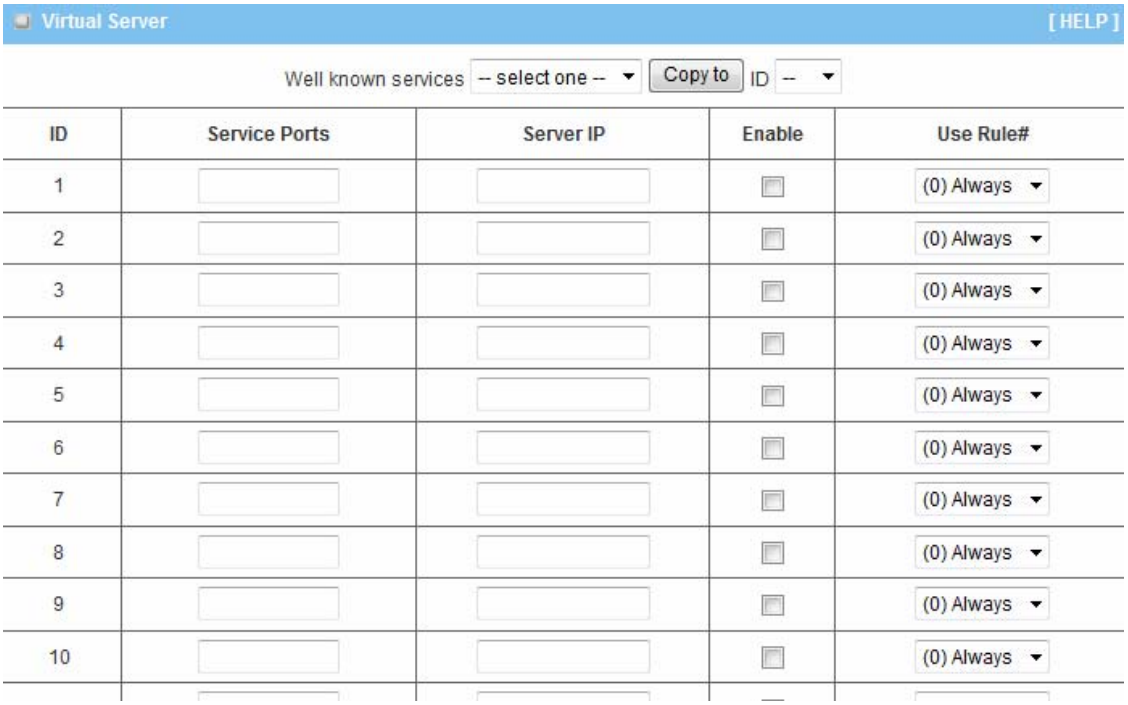
3.1.2. NAT

In this section, you can configure Virtual Server, Special AP, and DMZ settings.

3.1.2.1 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**.



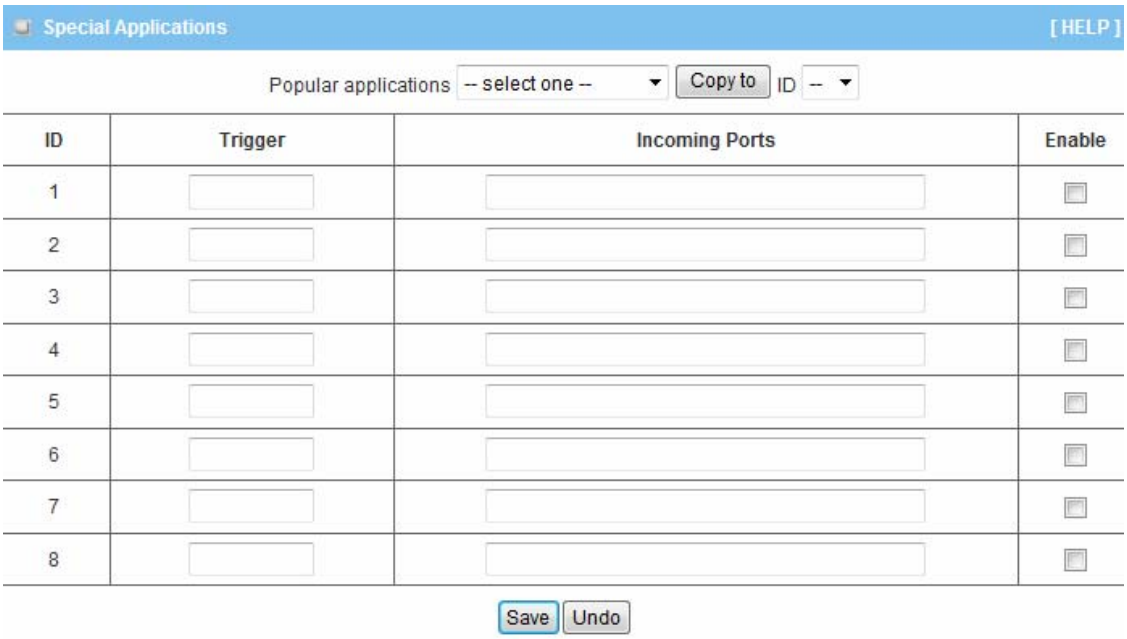
For an example, if you have an FTP server (port 21) at 192.168.123.1, a Web server (port 80) at 192.168.123.2, and a VPN server at 192.168.123.6, then you need to specify the following virtual server mapping table:

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.

3.1.2.2 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.

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.

3.1.2.3 DMZ

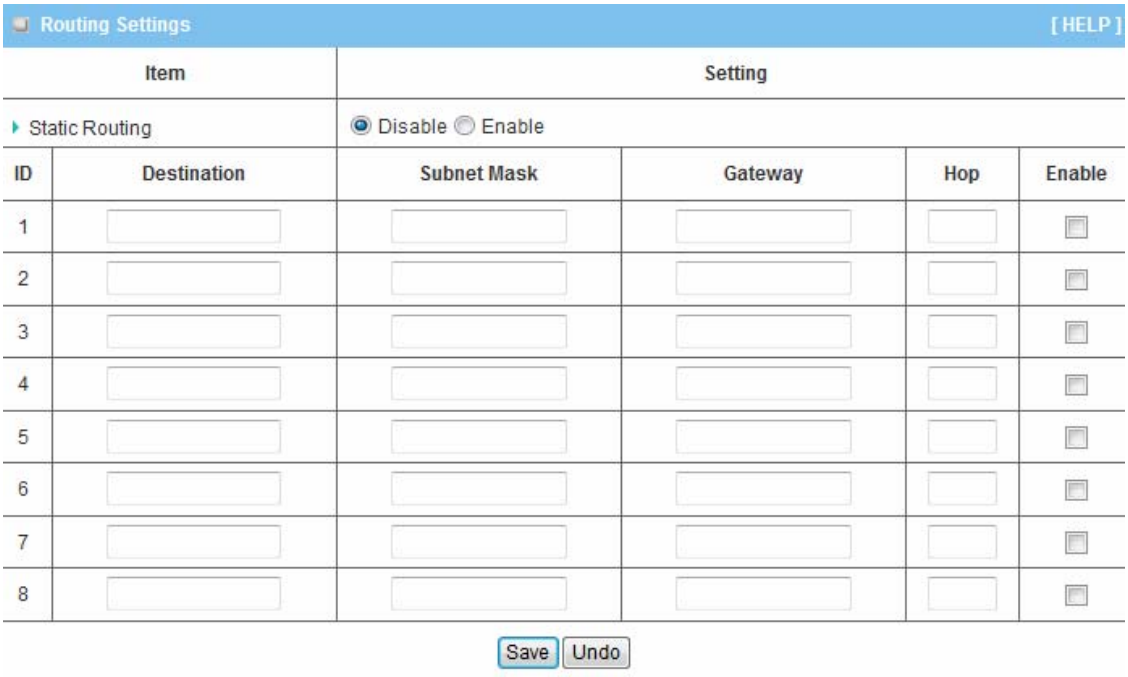
IP Address of DMZ Host:

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.

3.1.3. 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.

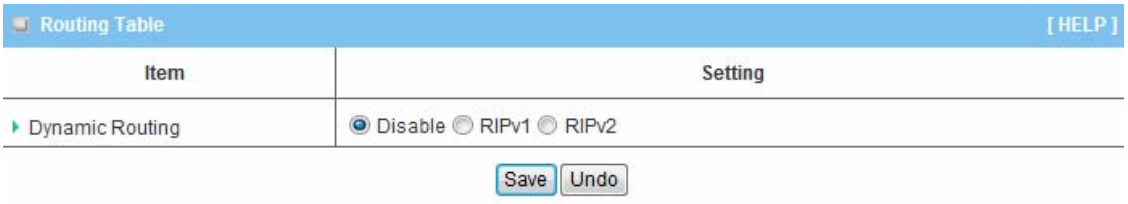
3.1.3.1 Static Routing



Static Routing: For static routing, you can specify up to 8 routing rules. You can enter the **destination IP address**, **subnet mask**, **Router**, 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.

3.1.3.2 Dynamic Routing



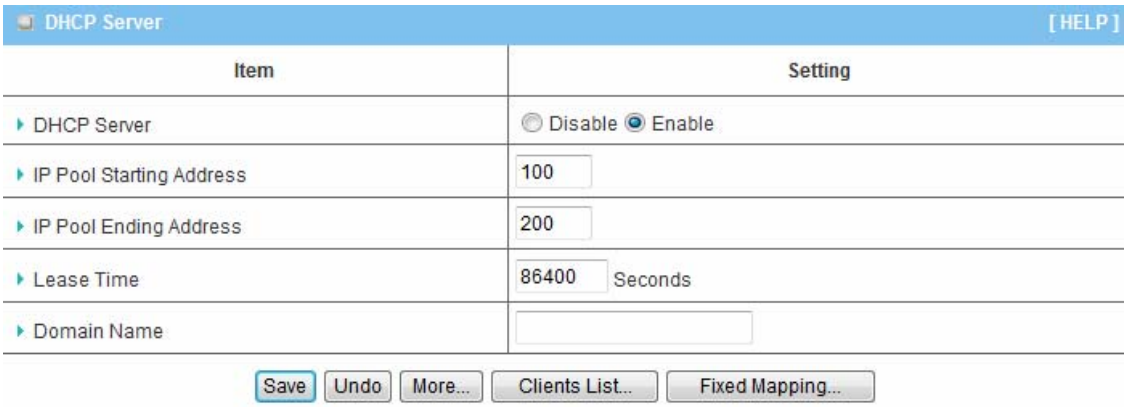
Dynamic Routing: Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnet in your network. Otherwise, please select RIPv1 if you need this protocol.

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

3.1.4. Client/Server/Proxy

In this section, you can configure DHCP Server and DDNS settings.

3.1.4.1 DHCP Server

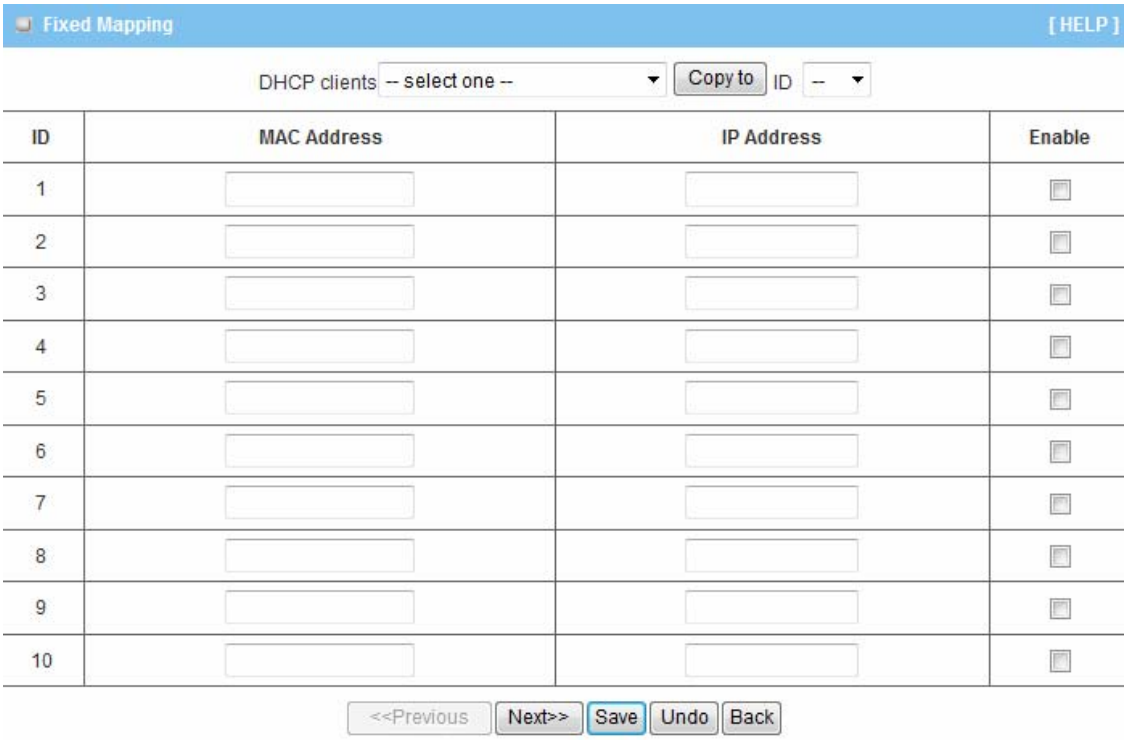


1. **DHCP Server:** Choose either **Disable** or **Enable**. If you enable the DHCP Server function, the following settings will be effective.
2. **IP Pool Starting/Ending Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool.
3. **Lease Time:** DHCP lease time to the DHCP client.
4. **Domain Name:** Optional, this information will be passed to the clients.
   Press **"More>>"** and you can find more settings
5. **Primary DNS/Secondary DNS:** Optional. This feature allows you to assign a DNS Servers
6. **Primary WINS/Secondary WINS:** Optional. This feature allows you to assign a WINS Servers
7. **Gateway:** Optional. Router Address would be the IP address of an alternate Router. This function enables you to assign another Router to your PC as default gateway, when DHCP server offers an IP to your PC.

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

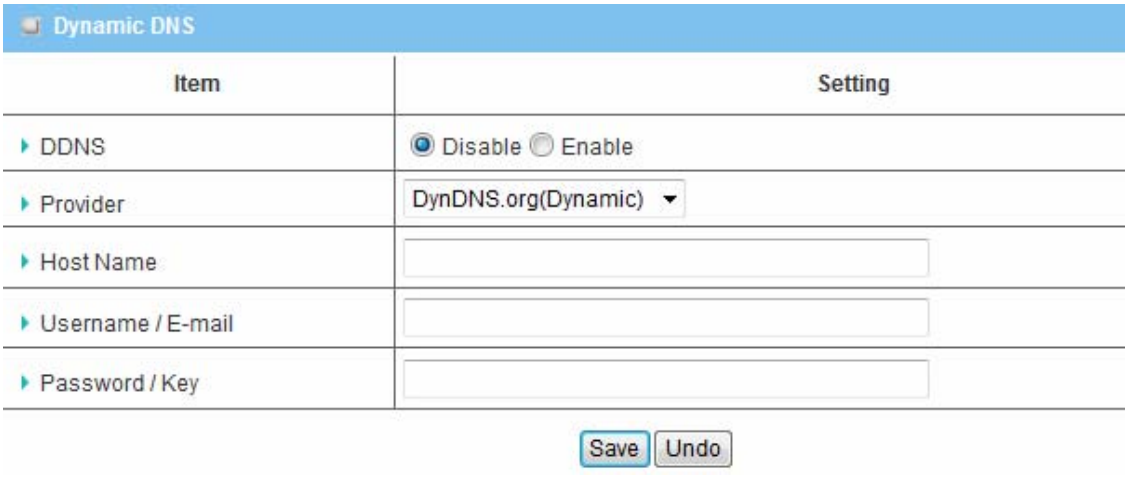
Press "Clients List" and the list of DHCP clients will be shown consequently.

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



3.1.4.2 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.

3.2 Advanced Network Setting

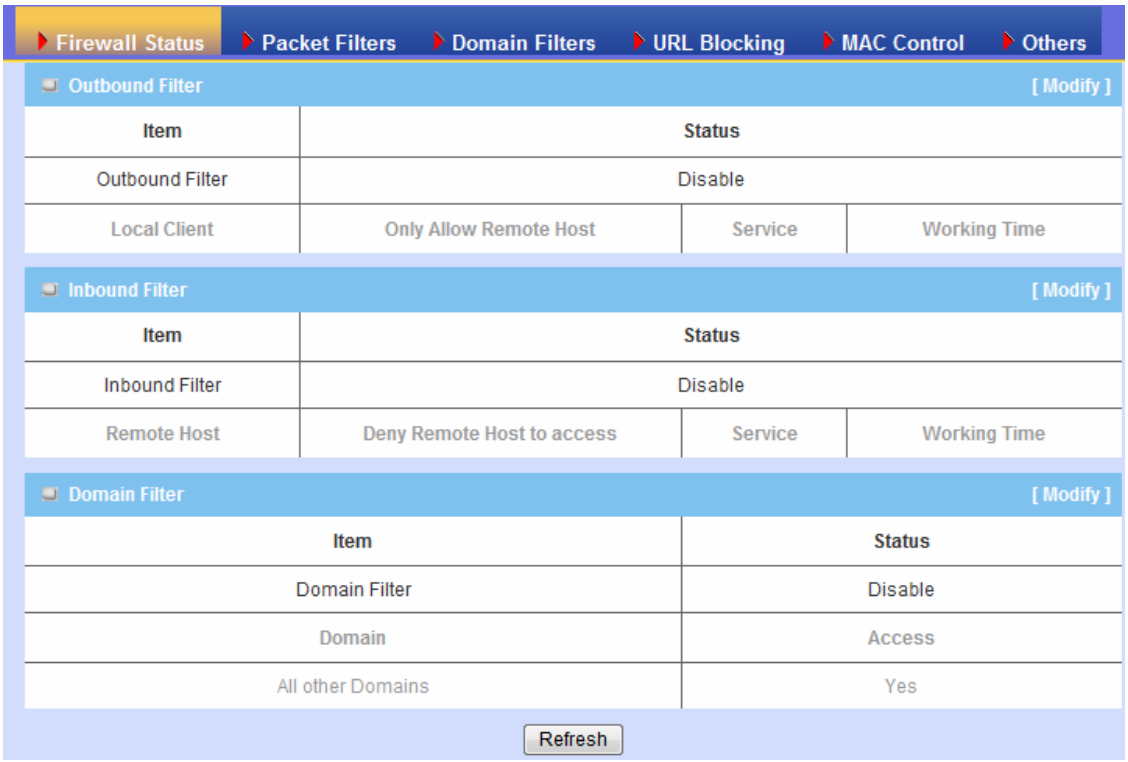
This router also support many advanced network features, such as firewall, QoS, and UPnP. You can finish those configurations in this section.

3.2.1 Firewall

The firewall functions include Packet Filters, Domain Filters, URL Blocking, and MAC Control.

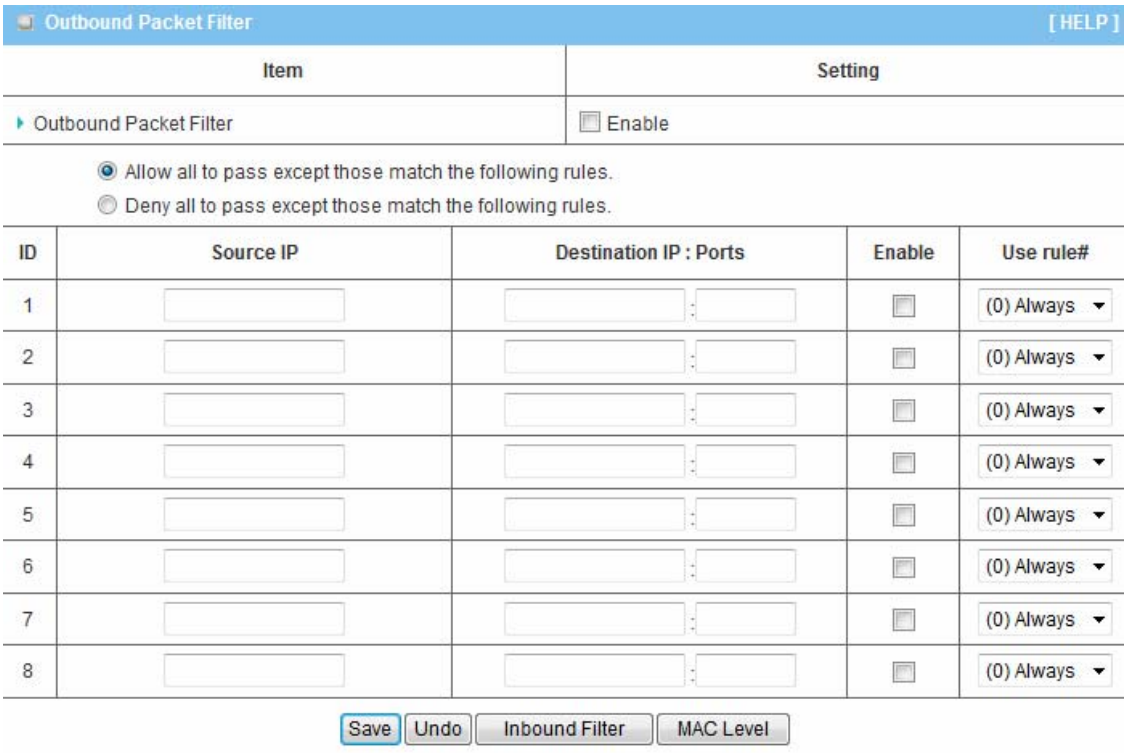
3.2.1.1 Firewall Status

This page shows all firewall rules that you have set.



3.2.1.2 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
- Destination IP address
- Destination port
- Protocol: TCP or UDP or both.
- Use Rule#

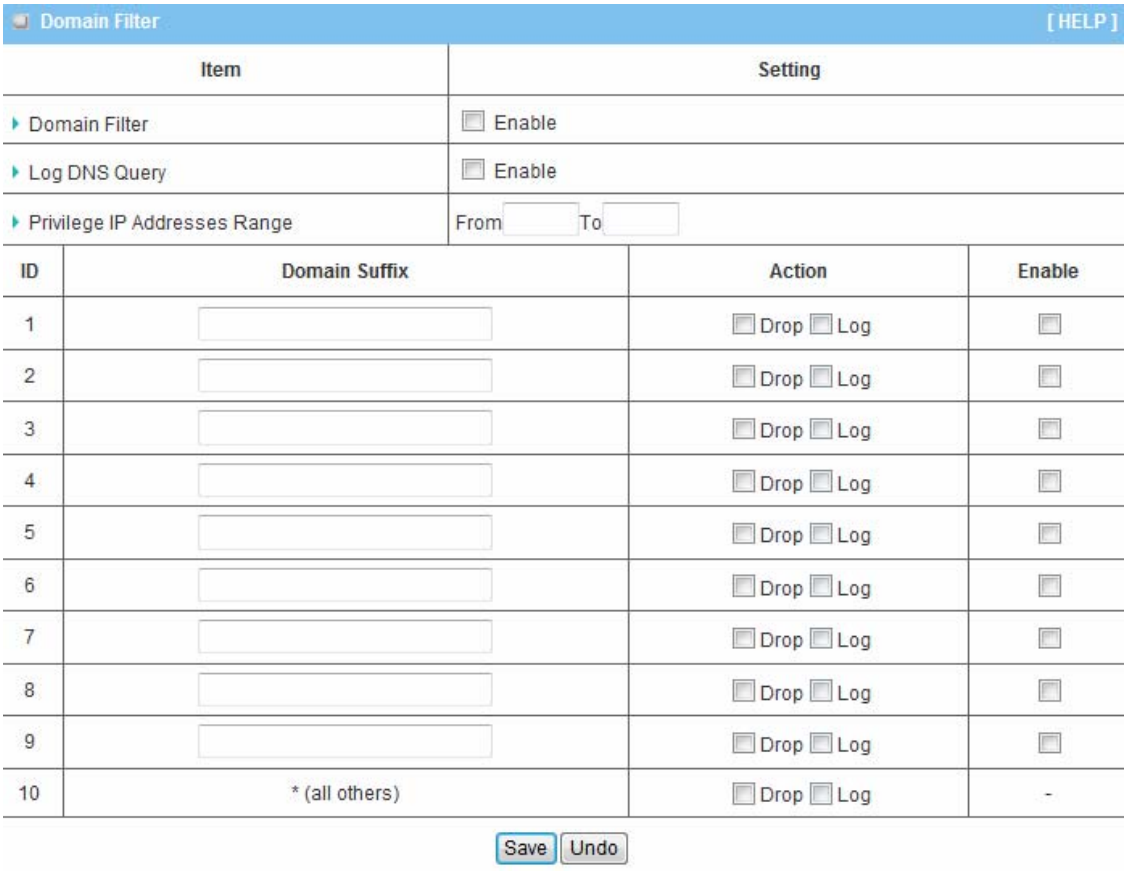
For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.
For destination port, you can define a single port (80) or a range of ports (1000-1999). An empty implies all port addresses. Packet Filter 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.

For MAC Level settings, please refer to MAC Control for details.

3.2.1.3 Domain Filters

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

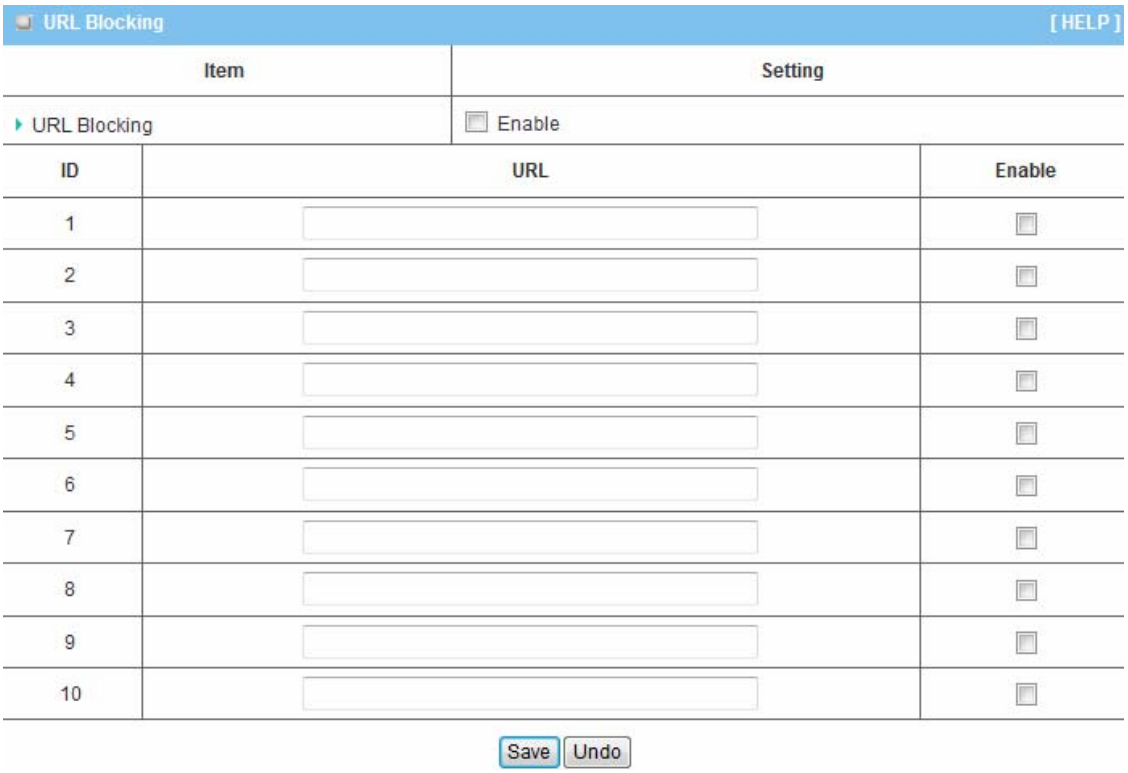


1. **Domain Filter**: Check if you want to enable Domain Filter.
2. **Log DNS Query**: Check if you want to log the action when someone accesses the specific Internet domains.
3. **Privilege IP Address Range**: Setting a group of hosts and privilege these hosts to access network without restriction.
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 record this access.
6. **Enable**: Check to enable each rule.

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

3.2.1.4 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**.

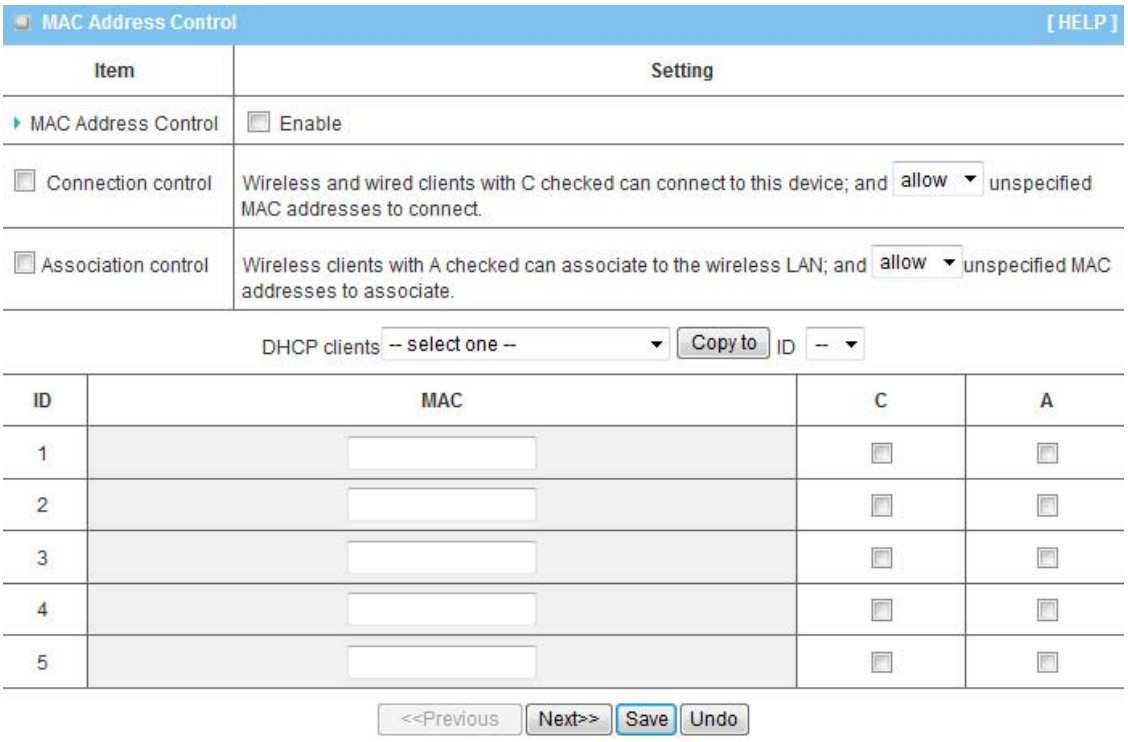


1. **URL Blocking**: Check if you want to enable URL Blocking.
2. **URL**: If any part of the Website's URL matches the pre-defined word, the connection will be blocked.
   For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".
3. **Enable**: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

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

3.2.1.5 MAC Address 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.

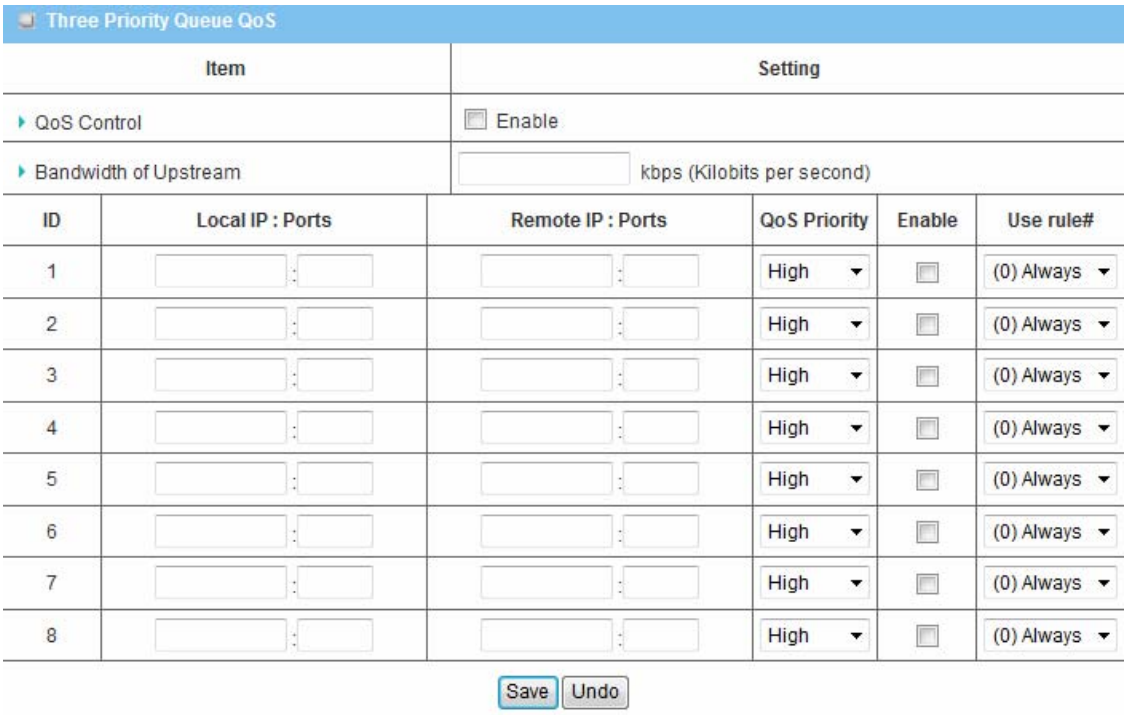
3.2.1.6 Others

1. **Discard PING from WAN side**: When this feature is enabled, any host on the WAN cannot ping this product.
2. **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.

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

3.2.2 QoS

Provide different priorities 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#.

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

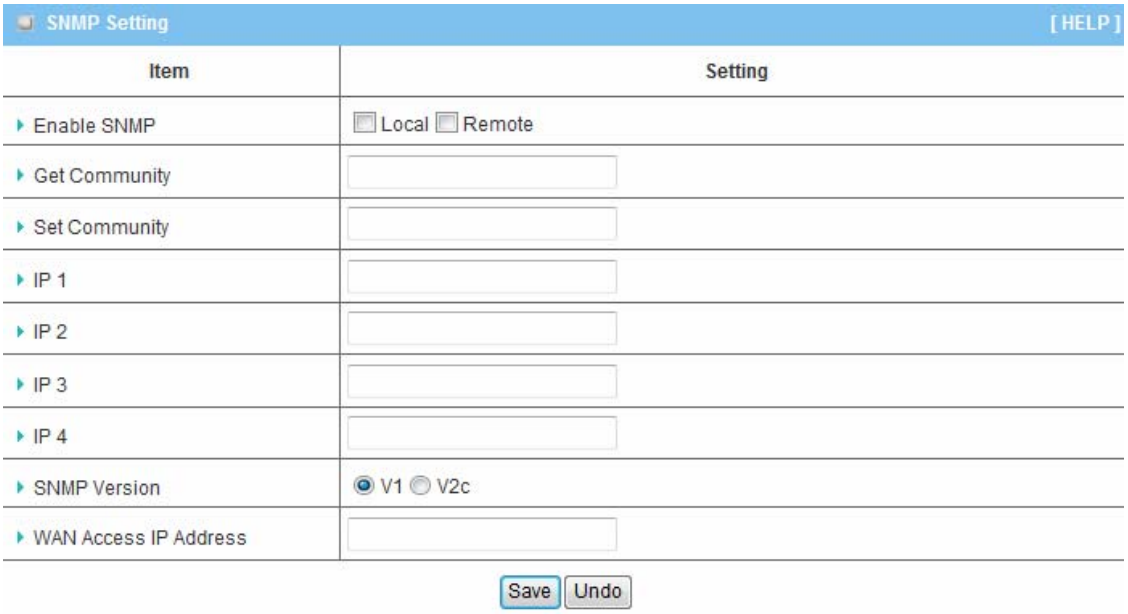
3.2.3 Management

3.2.3.1 UPnP

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.

3.2.3.2 SNMP

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. This device can support SNMP v1 and v2c



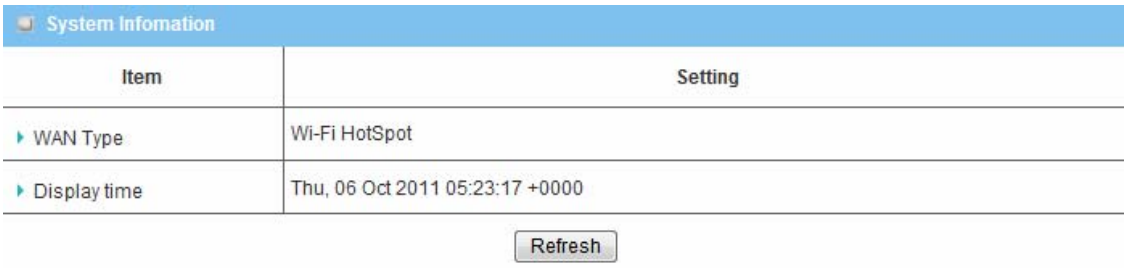
1. **Enable SNMP**: You must check “Local”, “Remote” or both to enable SNMP function. If “Local” is checked, this device will response request from LAN. If “Remote” is checked, this device will response request from WAN.
2. **Get Community**: The community of GetRequest that this device will respond.
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.

3.3 System

3.3.1 System Information

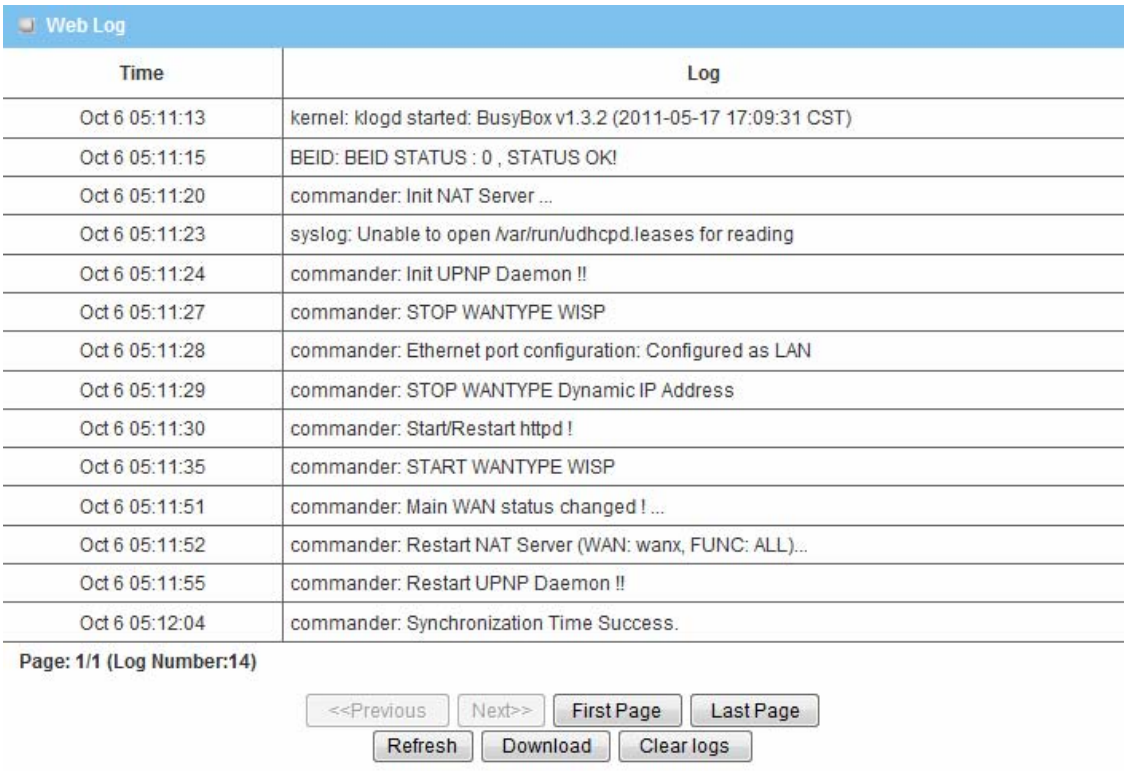
This page will show current WAN type, and system time.



3.3.2 System Status

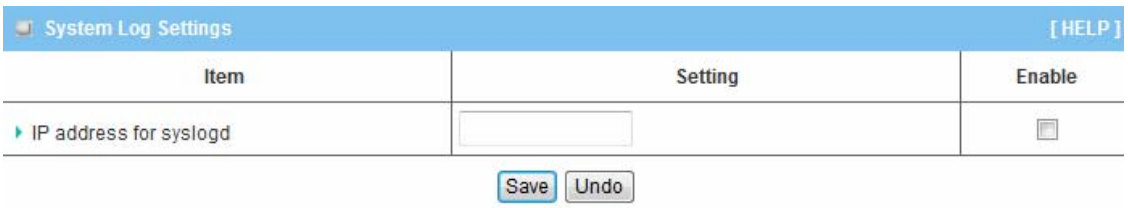
3.3.2.1 Web Log

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



3.3.2.2 Syslog

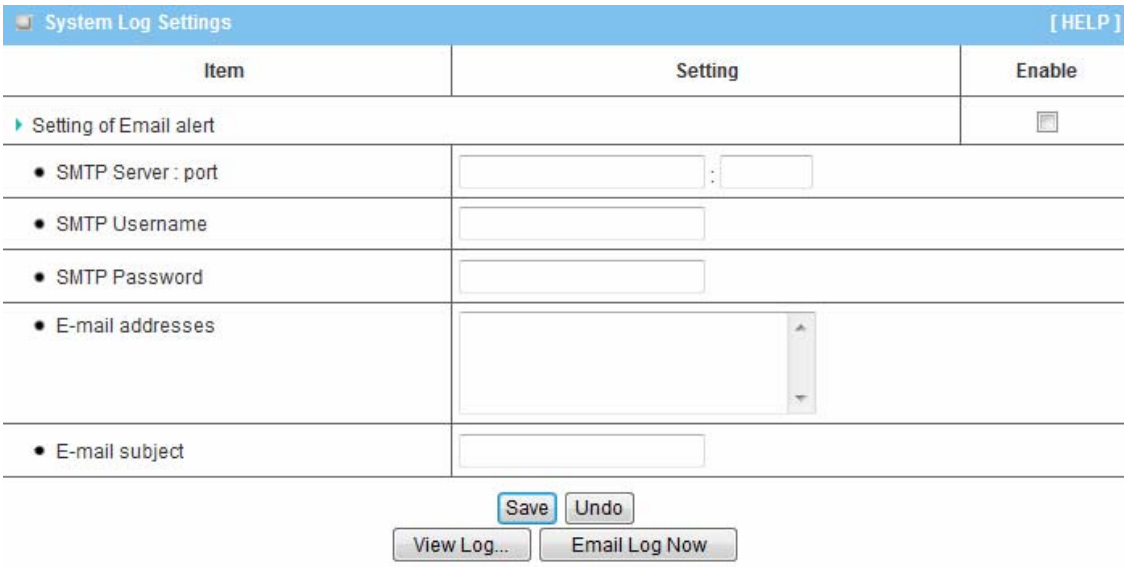
With enabling Syslog function, this device will send log to certain host periodically. You need to install a syslog utility on a host to receive syslogs.



IP Address for Sys log: Host IP of destination where sys log will be sent to. Check **Enable** to enable this function.

3.3.2.3 E-mail Alert

This page support two methods to export system logs to specific destination by means of syslog (UDP) and SMTP(TCP).

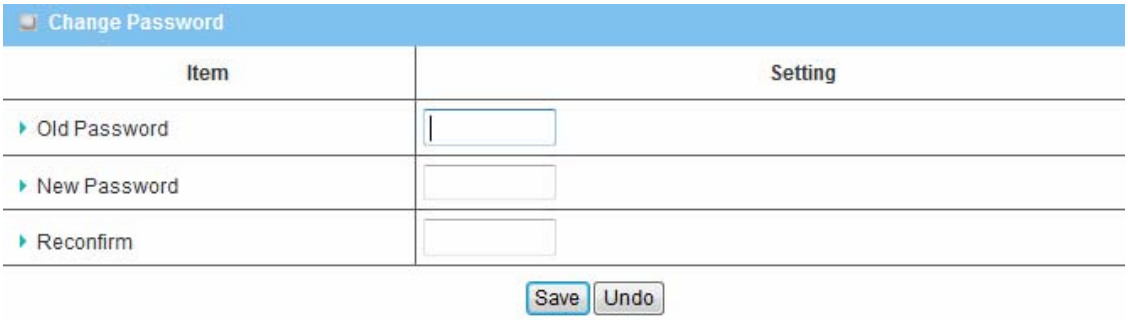


1. **Setting of E-mail Alert**: Check if you want to enable Email alert (send syslog via email).
2. **SMTP Server:Port**: Input the SMTP server IP and port, which are connected with ':'. If you do not specify port number, the default value is 25.
   For example, "mail.your_url.com" or "192.168.1.100:26".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

3.3.3 System Tools

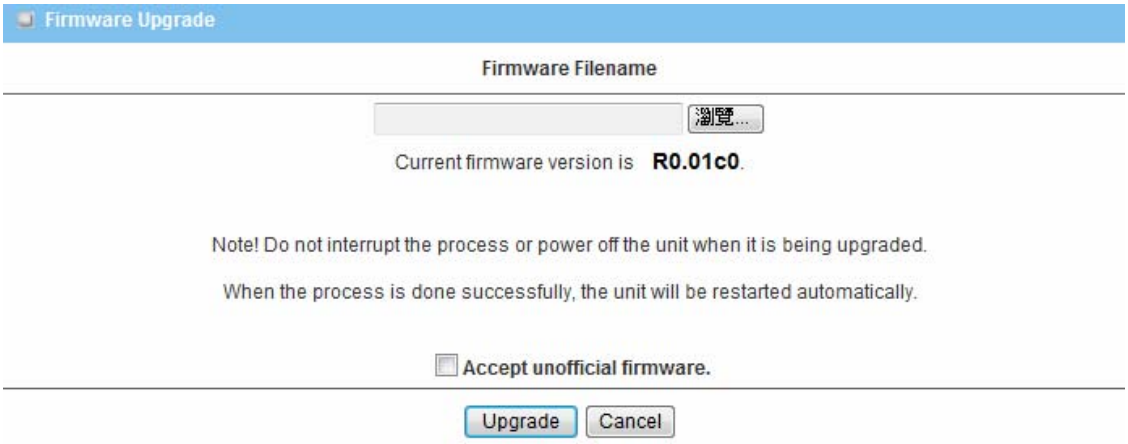
3.3.3.1 Account & Password

You can change the System Password here. We **strongly** recommend you to change the system password after you receive this device.



3.3.3.2 Firmware Upgrade

If new firmware is available, you can upgrade router firmware here.

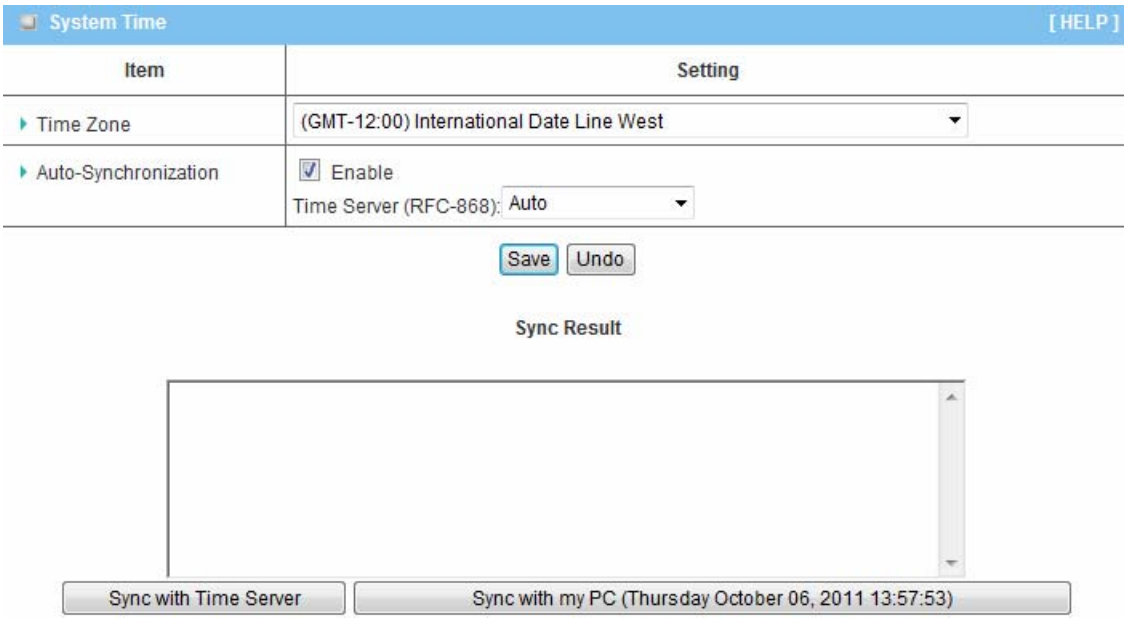


Press “browse” button to indicate the file name of new firmware, and then press Upgrade button to start to upgrade new firmware on this device. If you want to upgrade a firmware which is from GPL policy, please check “Accept unofficial firmware”.

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

3.3.3.3 System Time

You can set system time of this router here.

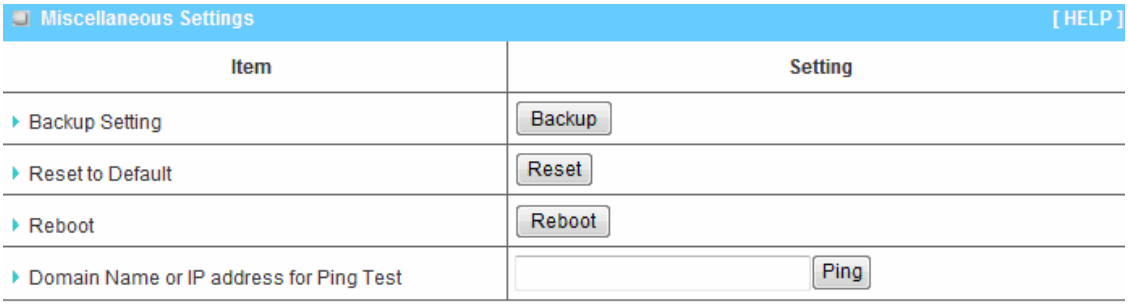


1. **Time Zone**: Select a time zone where this device locates.
2. **Auto-Synchronization**: Check the “Enable” checkbox to enable this function. Besides, you can select a NTP time server to consult UTC time.
3. **Sync with Time Server**: Click on the button if you want to set Date and Time by NTP Protocol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

3.3.3.4 Others

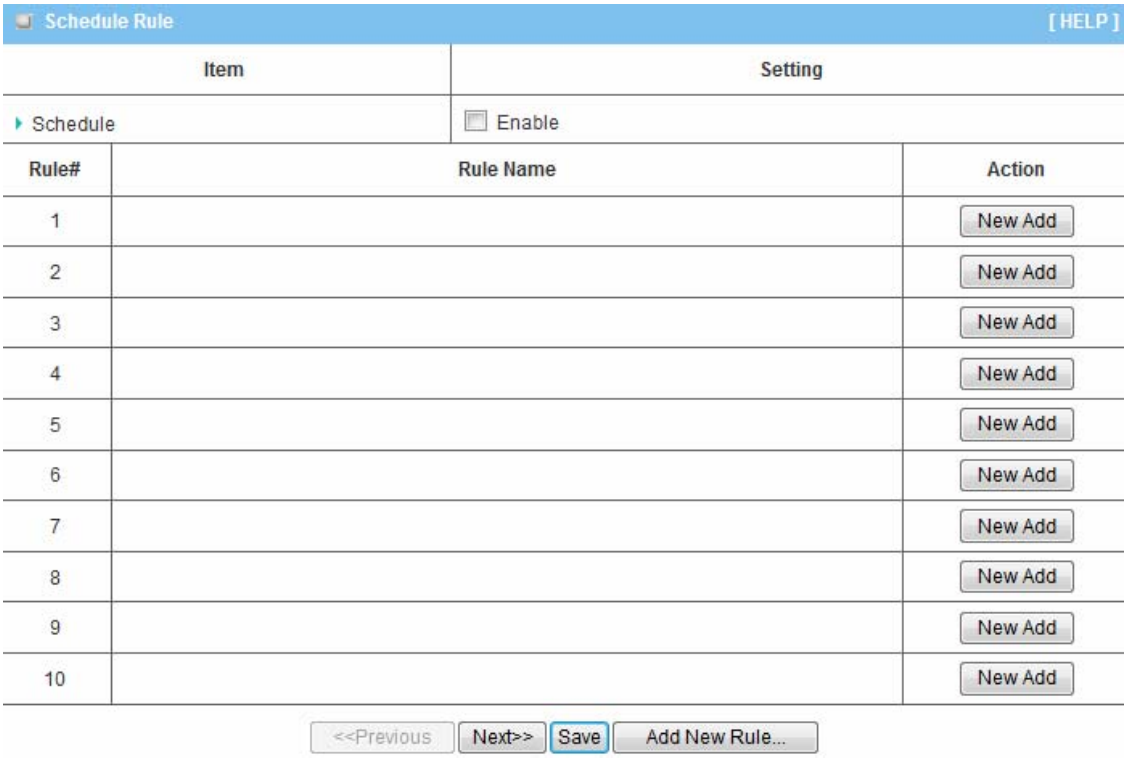


1. **Backup Setting:** You can backup your settings by clicking the "**Backup"** button, and save it as a bin file. Once you want to restore these settings, please follow the same instructions for Firmware Upgrade.
2. **Reset to Default:** You can reset this device to factory default settings by clicking the **Reset** button.
3. **Reboot:** Press Reboot button to restart the device immediately.
4. **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.

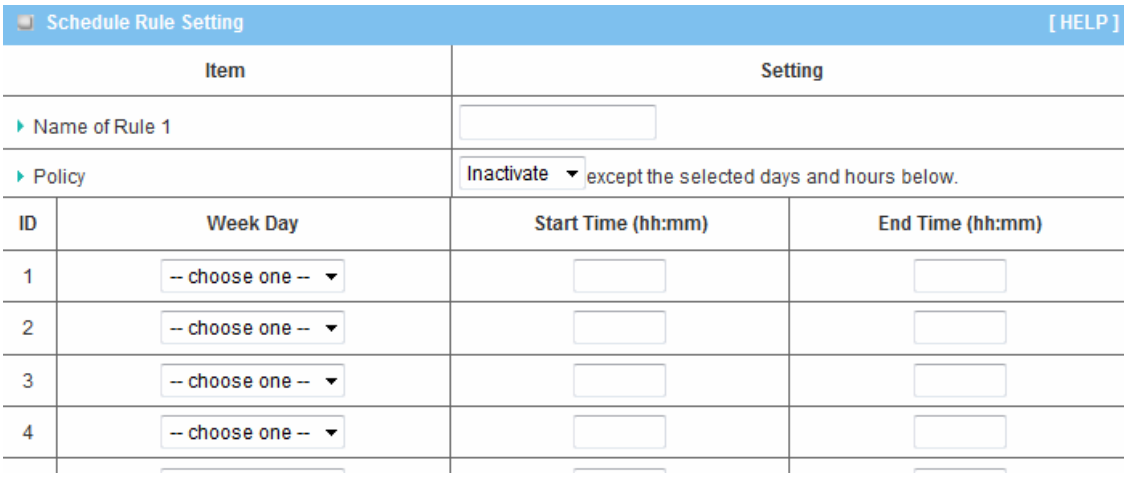
.

3.3.4 Scheduling

You can set the schedule time to decide when service will be activated.



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.

3.3.5 MMI

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".

Chapter 4 . Troubleshooting

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

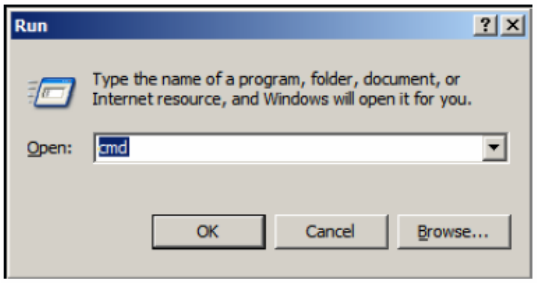
1 Why can't I configure the router even the cable is plugged and the LED is lit?

Do a **Ping test** to make sure that the WiFi Mobile 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 Router.
4. Type "**ping 192.168.123.254".** Assure that you ping the correct IP Address assigned to the WiFi Mobile 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 Mobile 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 Mobile 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, Router 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 Mobile Router to default setting

C. Why does my wireless connection keep dropping?

I. Antenna Orientation.

i. Try different antenna orientations for the WiFi Mobile 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 Mobile 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 Mobile Router to default setting

6 How to reset to default?

1. Ensure the WiFi Mobile 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 Mobile Router reboots, it has back to the factory **default** settings.

Appendix A. Spec Summary Table

Wireless WAN	USB 2.0 for external 3G/3.75G modem	1
Ethernet WAN/LAN	RJ-45 port, 10/100Mbps, WAN/LAN Configurable	1
Antenna	PIFA internal antenna	1
WPS Button	For WPS connection	1
Reset Button	Reset router setting to factory default	1
LED Indication	Status/ Internet	●
Mode Switch	Slide 3G/ Ethernet WAN Mode switch (3G/DSL)	1
Power Jack	Micro USB, DC 5V/1A	1
Wireless LAN (WiFi)		
Standard	IEEE 802.11n-lite compliance	●
SSID	SSID broadcast or in stealth mode	●
Channel	Auto-selection, manually	●
Security	WEP, WPA-PSK, WPA2-PSK	●
WPS	WPS (Wi-Fi Protected Setup)	●
WMM	WMM (Wi-Fi Multimedia)	●
Functionality		
Wireless WAN	PPP (for WCDMA/HSPA/ EVDO)	●
	Wifi Hotspot	●
	PPPoE (for iBurst)	●
Ethernet WAN	PPPoE, DHCP client, Static IP, PPTP, L2TP	●
WAN Connection	Auto-reconnect, dial-on-demand, manually	●
One-to-Many NAT	Virtual server, special application	●
SPI Firewall	IP/Service filter, URL blocking, MAC control	●
DoS Protection	DoS (Deny of Service) detection and protection	●
Routing Protocol	Static route, dynamic route (RIP v1/v2)	●
Management	UPnP IGD, syslog	●
Administration	Web-based UI, remote login, backup/restore setting	●
Environment & Certification		
Operation Temp.	Temp.: 0~40°C, Humidity 10%~90% non-condensing	●
Storage Temp.	Temp.: -10~70°C, Humidity: 0~95% non-condensing	●
CE, FCC	CE/FCC compliance	●
RoHS	RoHS compliance	●

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-2.6.21 system kernel
- busybox_1_00_rc2
- bridge-utils 0.9.5
- dhcpcd-1.3
- ISC DHCP V2 P5
- syslogd spread from busybox
- wireless tools
- ntpclient of NTP client implementation
- RT5350 for 802.1X application
- 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

FCC statement in User's Manual (for class B)

"Federal Communications Commission (FCC) 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 harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

1.The 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.