User Manual

D-Link

DIR-410
M2M 3G VPN Router

Copyright

Trademarks

FCC Interference Statement

Federal Communication Commission 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 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 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: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

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.

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

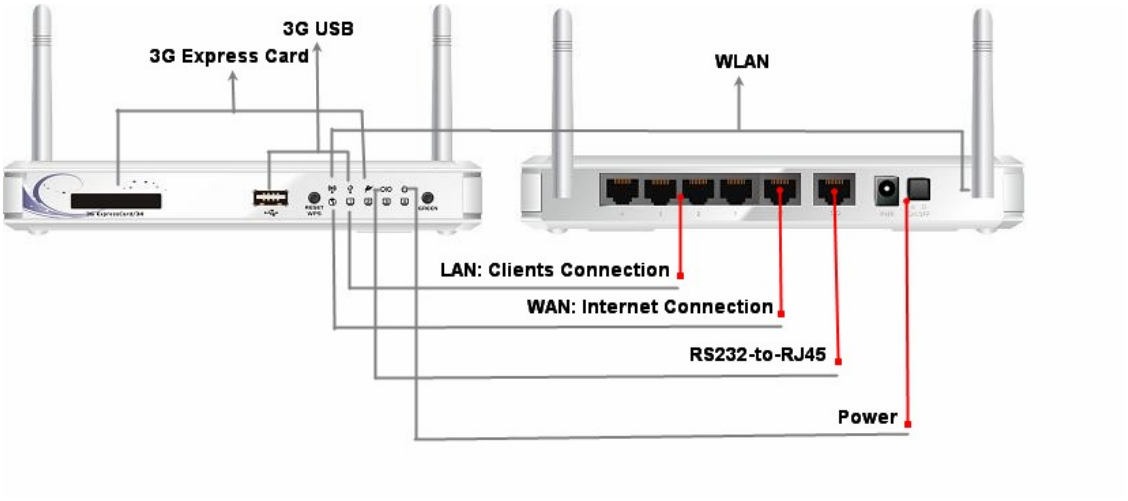
Congratulations on your purchase of this outstanding product: DIR-410 M2M 3G VPN Router. This product is specifically designed for Office needs. It provides a complete solution for Internet surfing, 3G backup, and VPN tunneling. Instructions for installing and configuring this product can be found in 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	M2M 3G VPN Router		1
2	Power adapter 12V 2A		1
3	CD		1

1.2 Hardware Installation

1.2.1 Hardware configuration



1.2.2 LED indicators

	LED color	Description
WAN	Green	It is connected to Internet.
	Green in flash	Data access
LAN	Green	RJ45 cable is plugged, and Ethernet connection is established.
	Green in flash	Data access
WLAN	Green	WiFi is on.
	Green in flash	Data access
3G USB	Amber	3G/3.5G is on.
	Amber in flash	Data access
3G Express Card	Amber	Connection established
	Amber in flash	Data access
RS232	Amber	Serial port connection established
	Amber in flash	Data access
Power	Green in flash	Normal mode (The power is on.)
	Green in fast flash	Reset mode

1.2.3 Installation Steps

Step 1. Attach the antenna:
Screw the antenna in a clockwise direction to the back panel of the unit.

DO NOT connect M2M 3G VPN Router to power before performing the installation steps below.

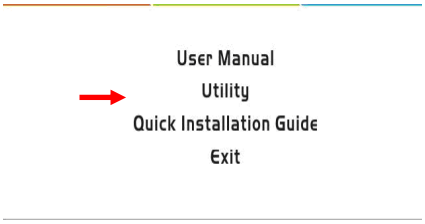
Step 2. Insert the 3G USB to the router:
Plug your USB modem which is with activated SIM card provided by your 3G service provider.
to the USB interface.

Step 3. Connect with the Ethernet patch 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. The LED of Internet connection will show green color if the Ethernet connection is normally connected.

Step 4. Connect the power adapter:
Plug the other end of the power adapter into a wall outlet.

Step 5. Press the power button

Step 6. Start to configure the device:
You can start to configure the device via the Easy Setup.
(see Easy Setup Utility)

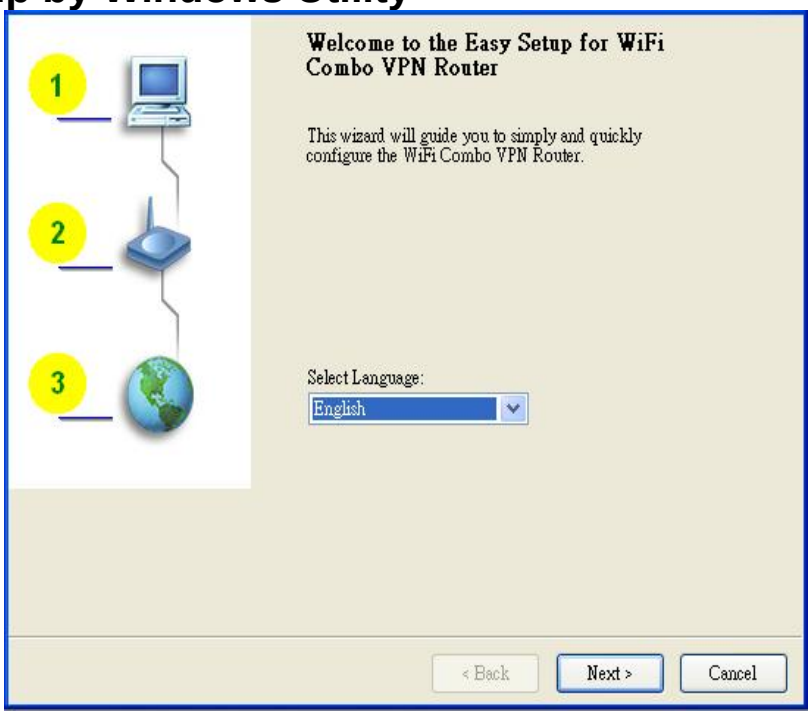


CHAPTER 2. Getting Started

2.1 Easy Setup by Windows Utility

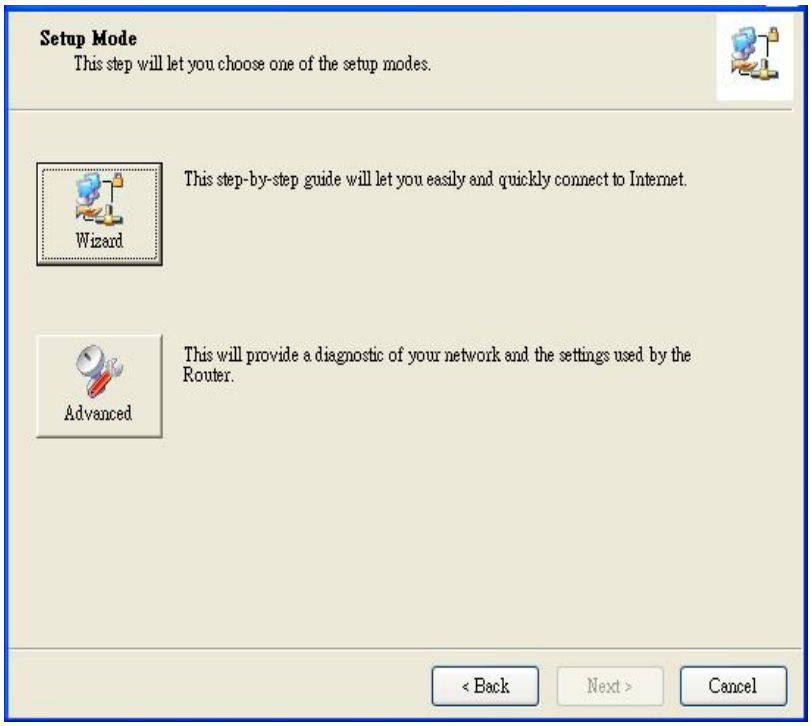
Step 1:
Install the Easy Setup Utility from CD then follow the steps to configure it.

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

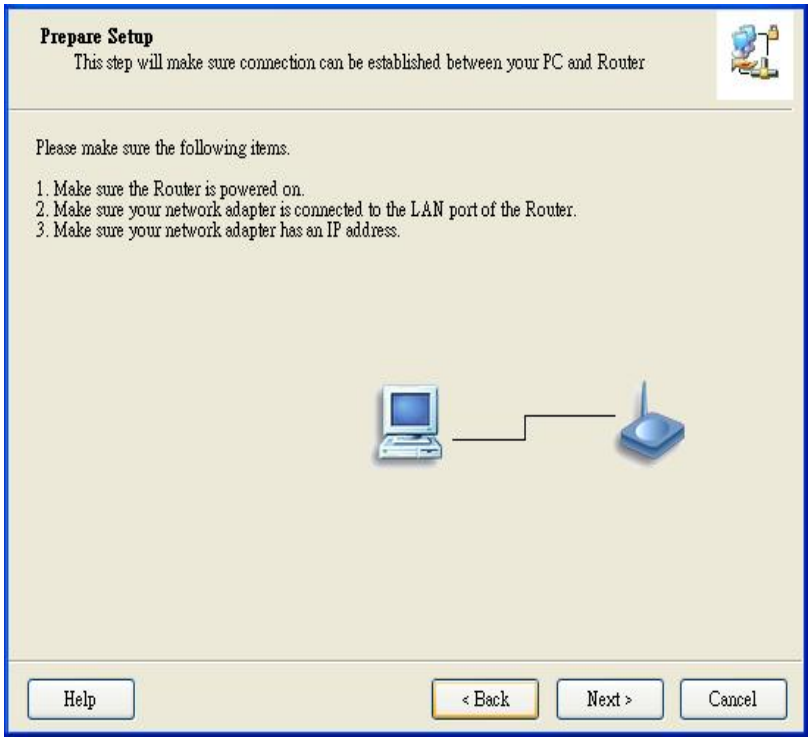


Step 3:
Then click the “Wizard” to continue.

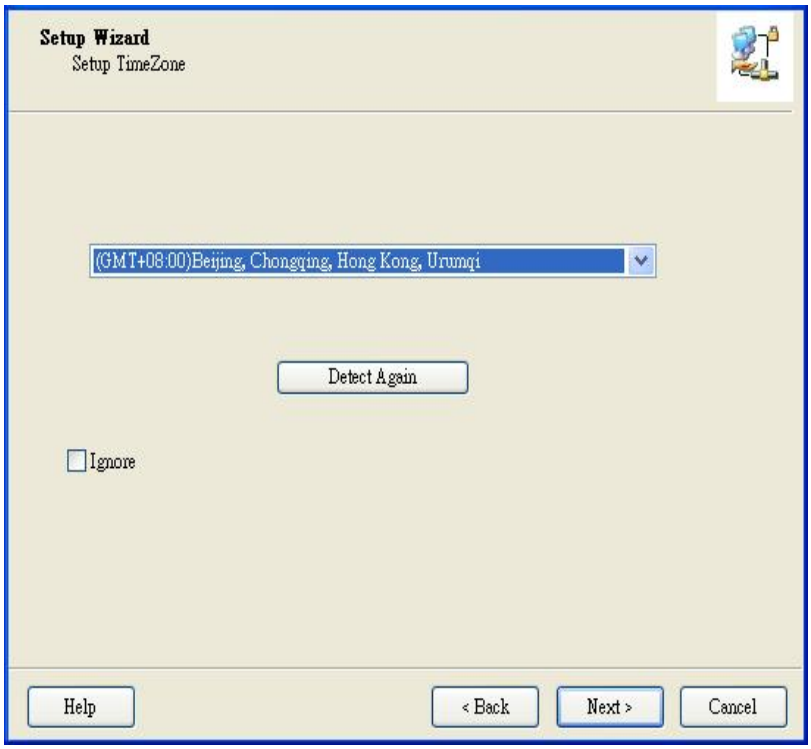
Or click “advanced” to run advanced mode for more detailed setting. (See User Manual)



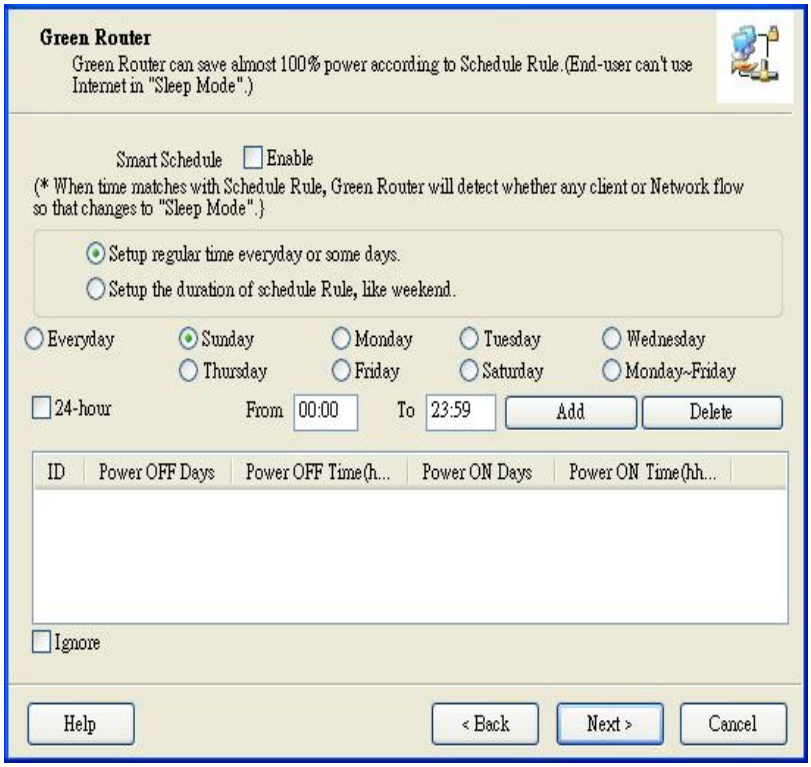
Step 4:
Click “Next” to continue.



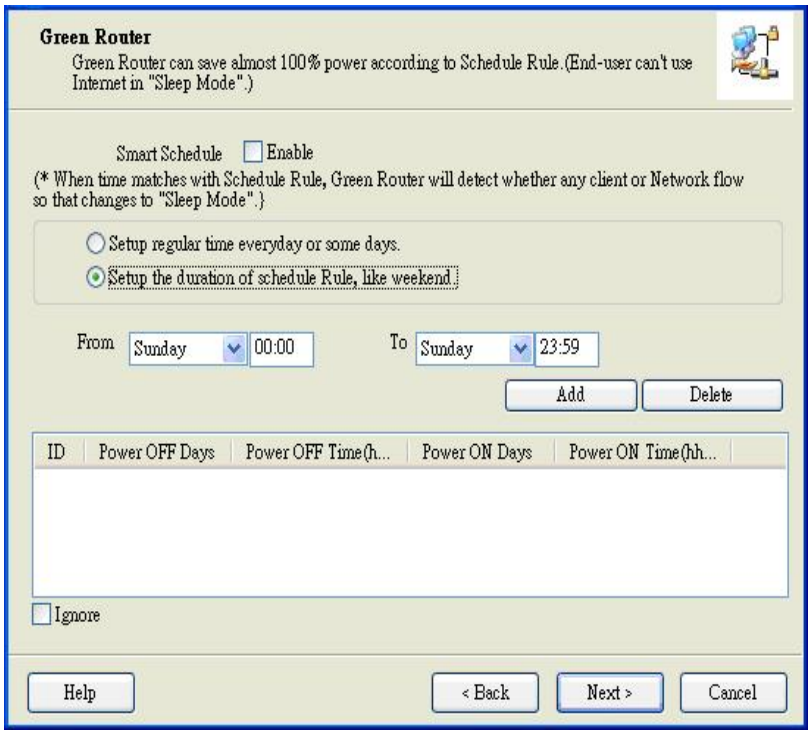
Step 5:
Select time zone. It can help us to synchronize the system time with network time server.



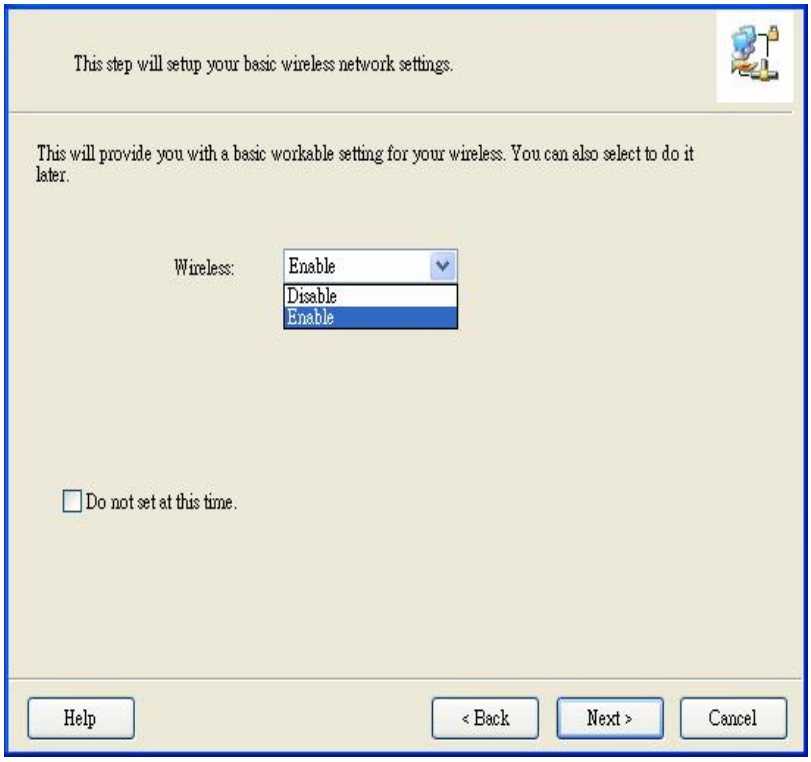
Step 6-1:
Configure the schedule setting for Green function. You can set the schedule for turning on or turning off this device automatically.



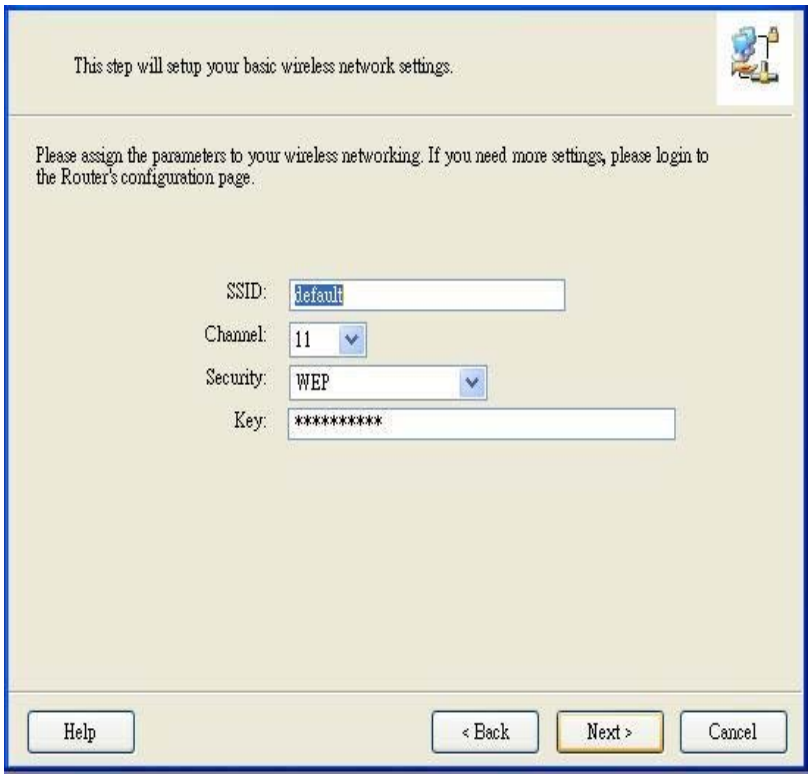
Step 6-2:
Click **SMART Schedule** setting for Green function. The device would check the packet flow before the power is turned off. For instance, if the router is on the sleeping mode, you could surf the Internet at that time. Afterwards, if there are not any packet flows, the router would be turned off automatically.



Step 7:
Configure your wireless interface.

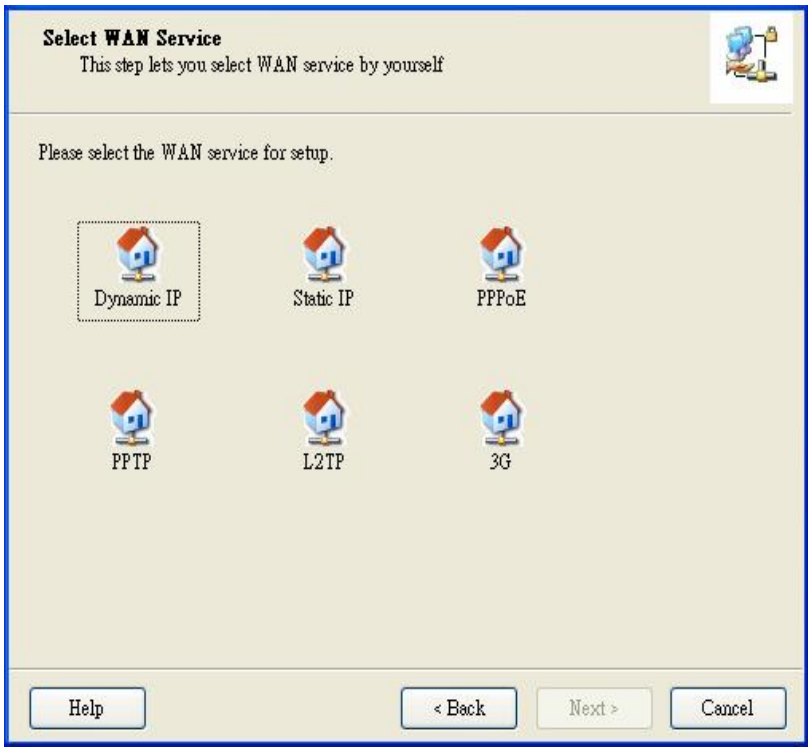


Step 8:
Insert SSID, Channel and Security options, and then click “Next” to continue.

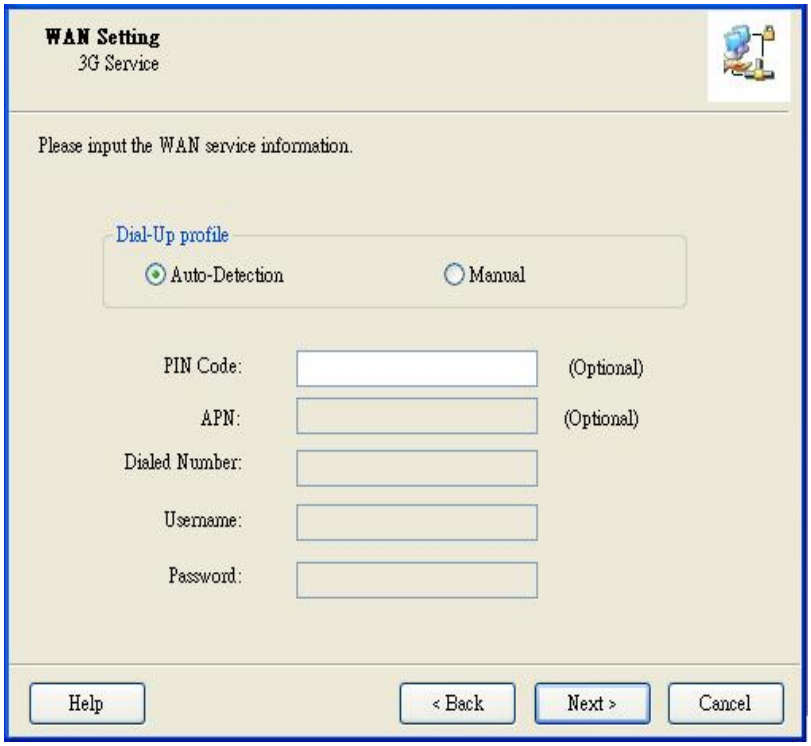


Step 9:
Auto detect the WAN service, just click the [Next] button.
Or you could select the WAN type by yourself via select the check box [Let me select WAN service by myself] → jump to Step 10.

Step 10:
Select the WAN type by yourself. You can get this information by asking your ISP.

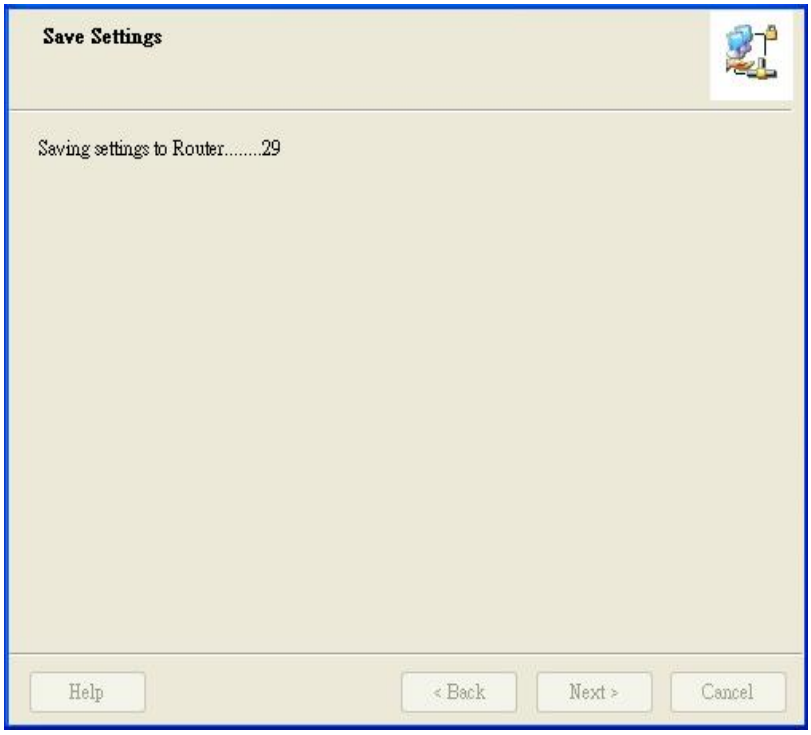


Step 11-1：
Select “Auto-Detection”, and the Utility will try to detect and configure the required 3G service settings automatically. Click “Next” to continue. Default PIN Code is empty, if you have PIN Code, you must enter it. For example “0000”. If no, just Click “Next” to continue.



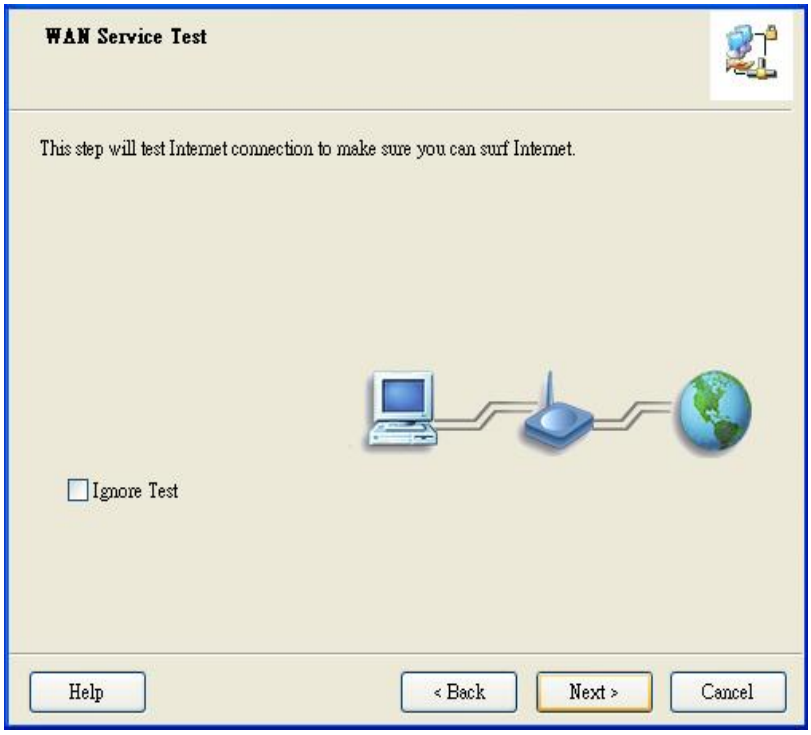
Step 11-2：
Or you can select “Manual” and manually fill in the required 3G service settings provided by your ISP. Click “Next” to continue.

Step 12：
The M2M 3G VPN Router is rebooted to make your entire configuration take effect.

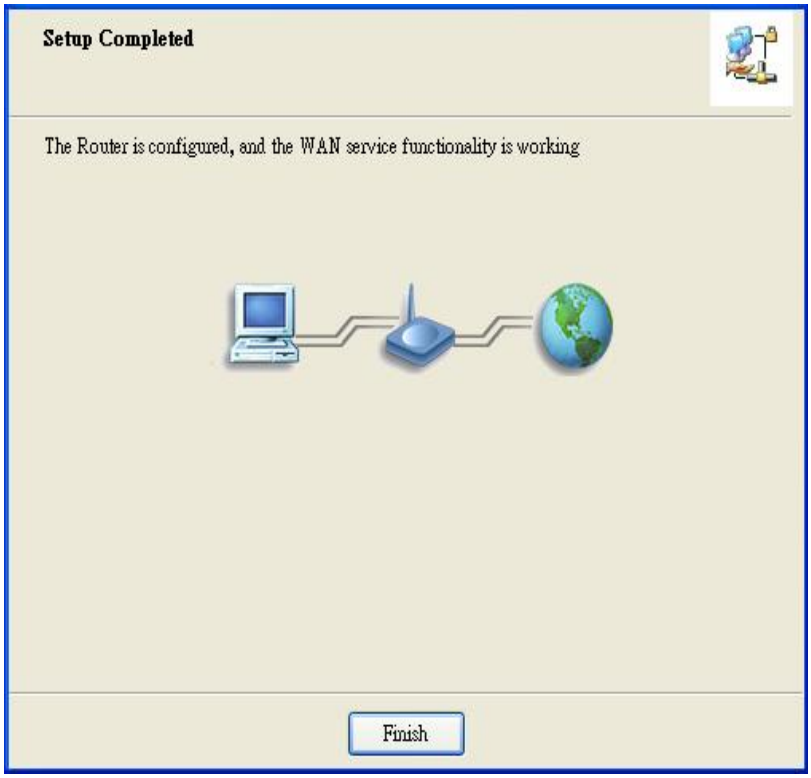


Step 13：
Click “Next” to test the Internet connection.

Step 14：
Click “Next” to test WAN Networking service or you can ignore test.



Step 15：
Congratulations! Setup is completed. Now you have already connected to Internet successfully.

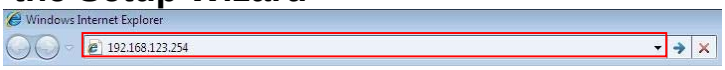


2.2 Easy Setup by Configuring Web Pages

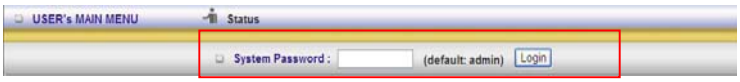
You can also browse UI of the web to configure the device.

Browse to Activate the Setup Wizard

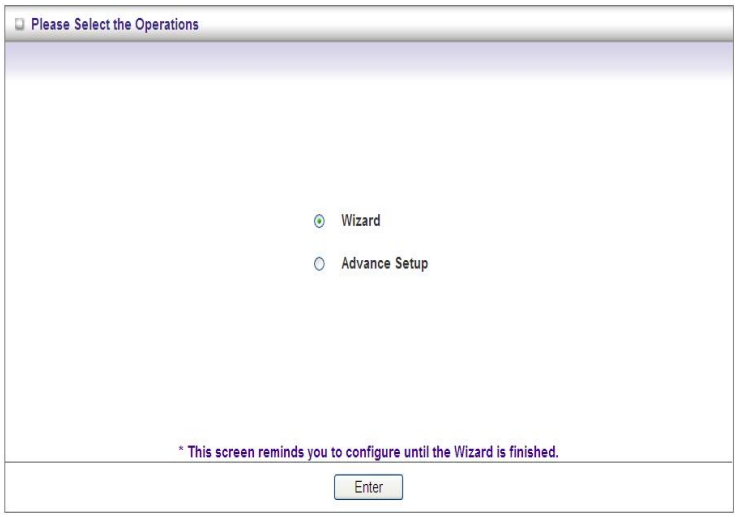
Type in the IP Address (http://192.168.123.254)



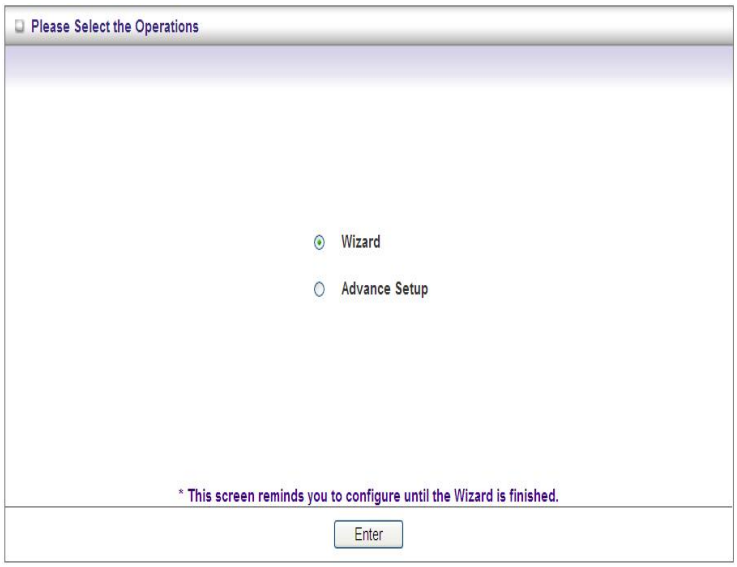
Type the default password ‘admin’ in the System Password and then click ‘login’ button.



Select “Wizard” for basic settings in simple way.

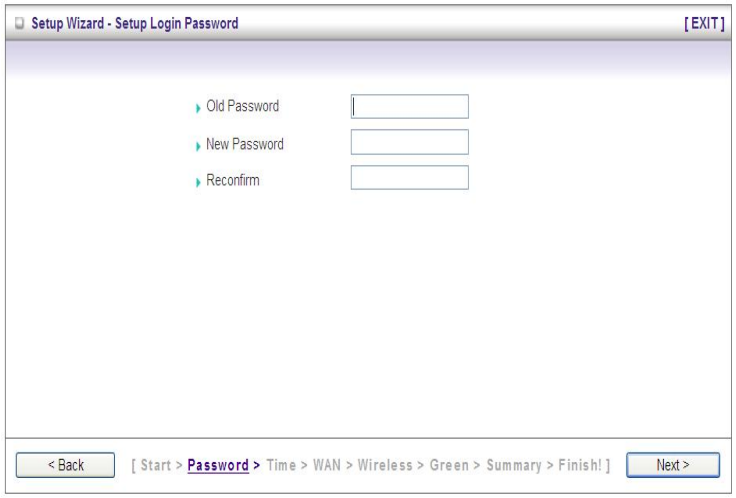


Press “Next” to start the Setup Wizard.

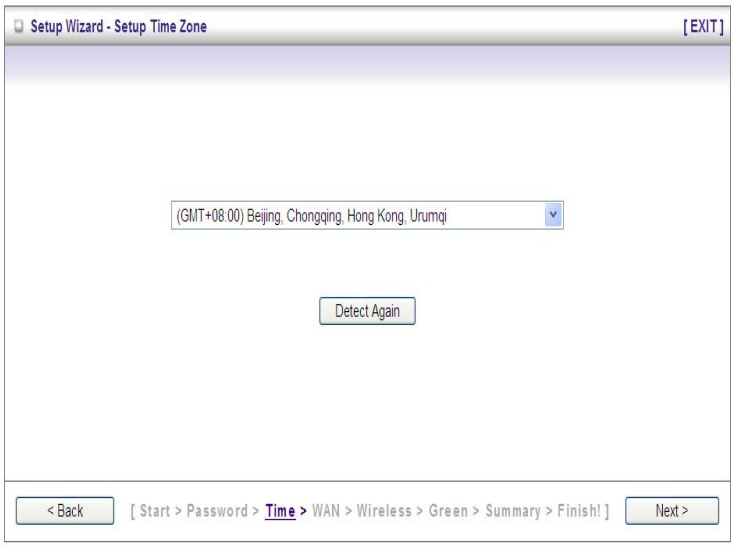


Configure with the Setup Wizard

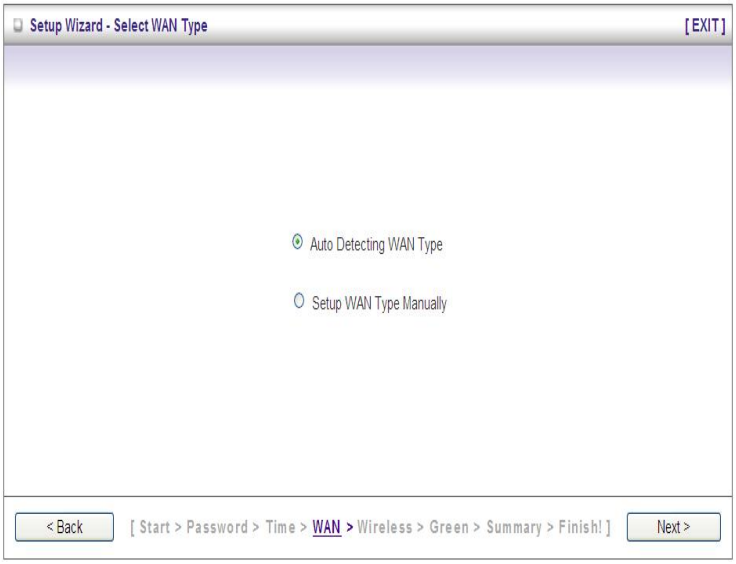
Step 1:
Setup login password.
Enter your system password.



Step 2:
Select Time Zone.

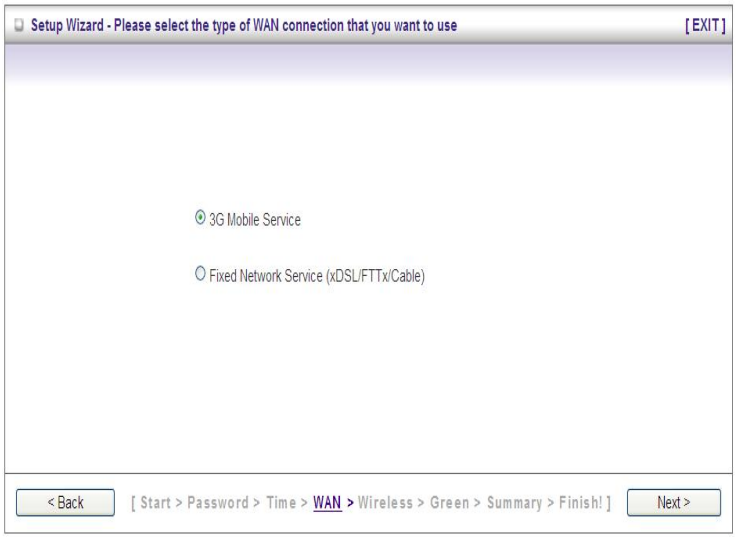


Step 3:
Setup Wan Type.

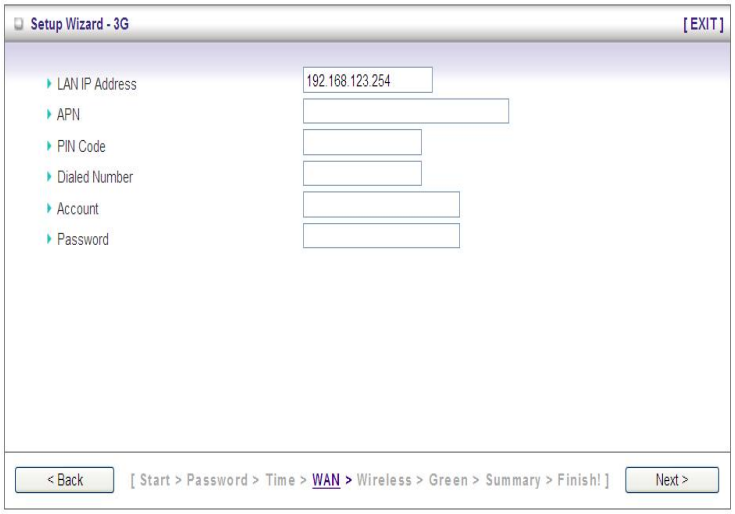


Step 4:
Select the WAN type you would like to use.

If you select “3G Mobile Service, please jump to **step 5-1**. However, if you click “Fixed Network Service, please jump to **step 5-2**.

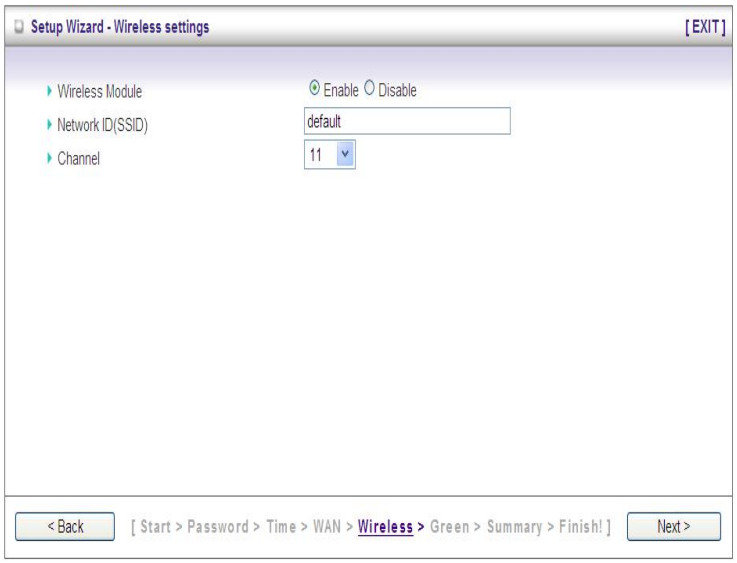


Step 5-1:
Set up 3G Dial-up profile.

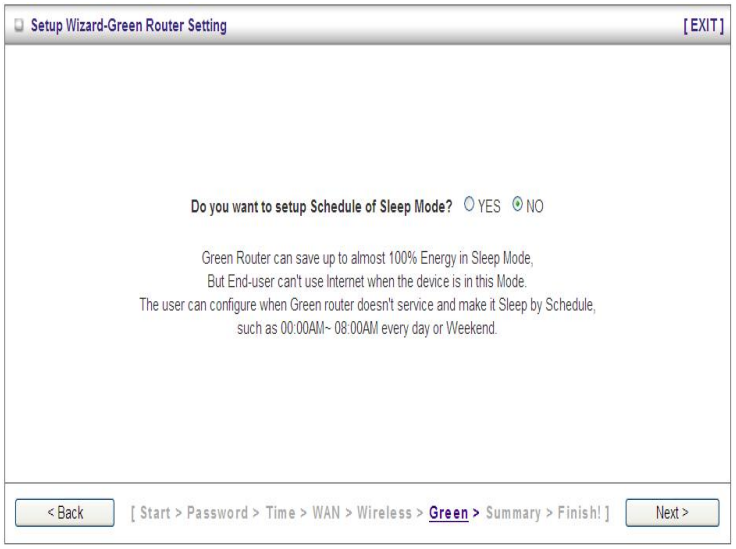


Step 5-2:
Select WAN type by yourself. Afterwards, please fill in necessary information.

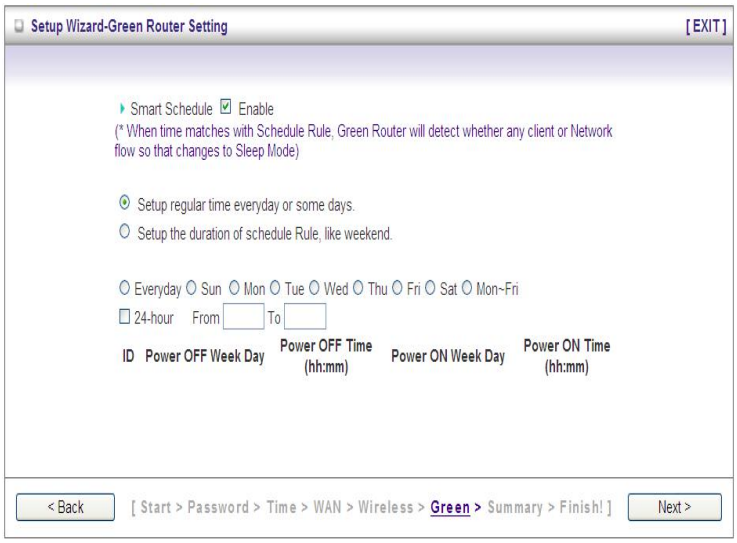
Step 6:
Set up your Wireless Settings.
Type your network ID in the blank of SSID.



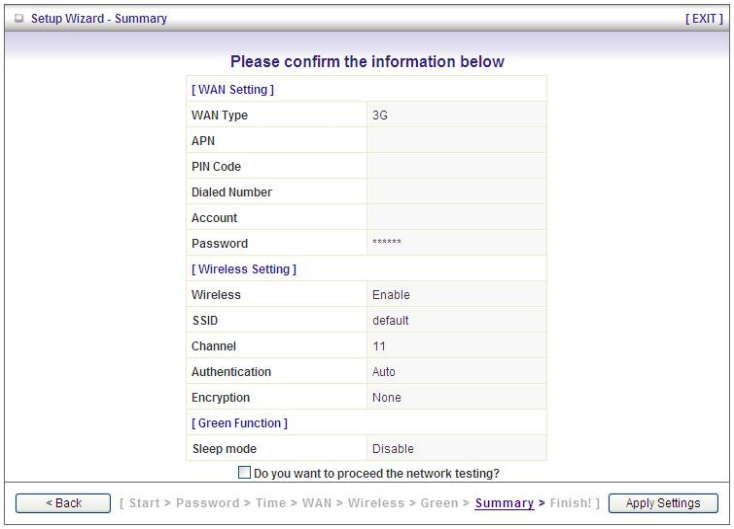
Step 7:
You could choose whether to configure Sleep Mode. If you would like to trigger the sleep mode, please click “YES”. If not, please click “NO” and jump to **step 8**.



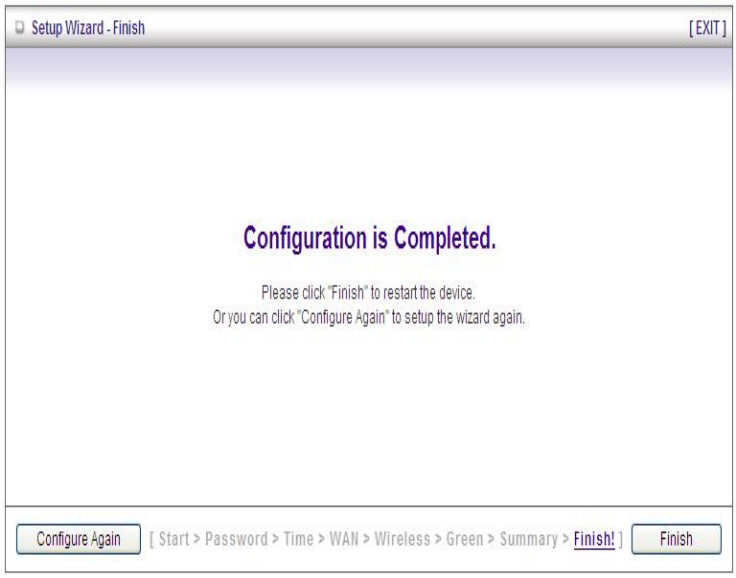
Step 8
Configure the schedule setting for Green function. You can set the schedule for turning on or turning off this device automatically.
As for the Smart Schedule, the device would check the packet flow before the power is turned off.
For instance, if the router is on the sleeping mode, you could surf the Internet at that time. Afterwards, if there are not any packet flows, the router would be turned off automatically.



Step 9:
Confirm the information you set up in User Interface. If it is correct, please click 'Apply settings'.



Step 10:
Click Finish to complete it.



Step 11:
The system is restarting to make sure your configuration take effect.

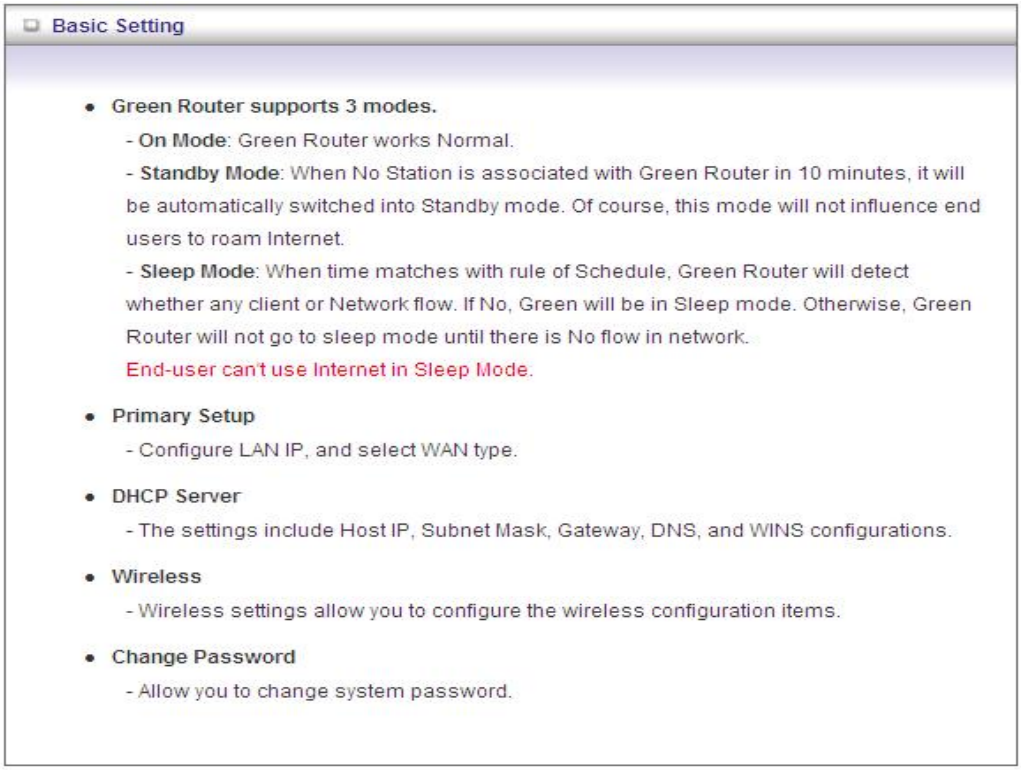
CHAPTER 3. Making Configuration

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

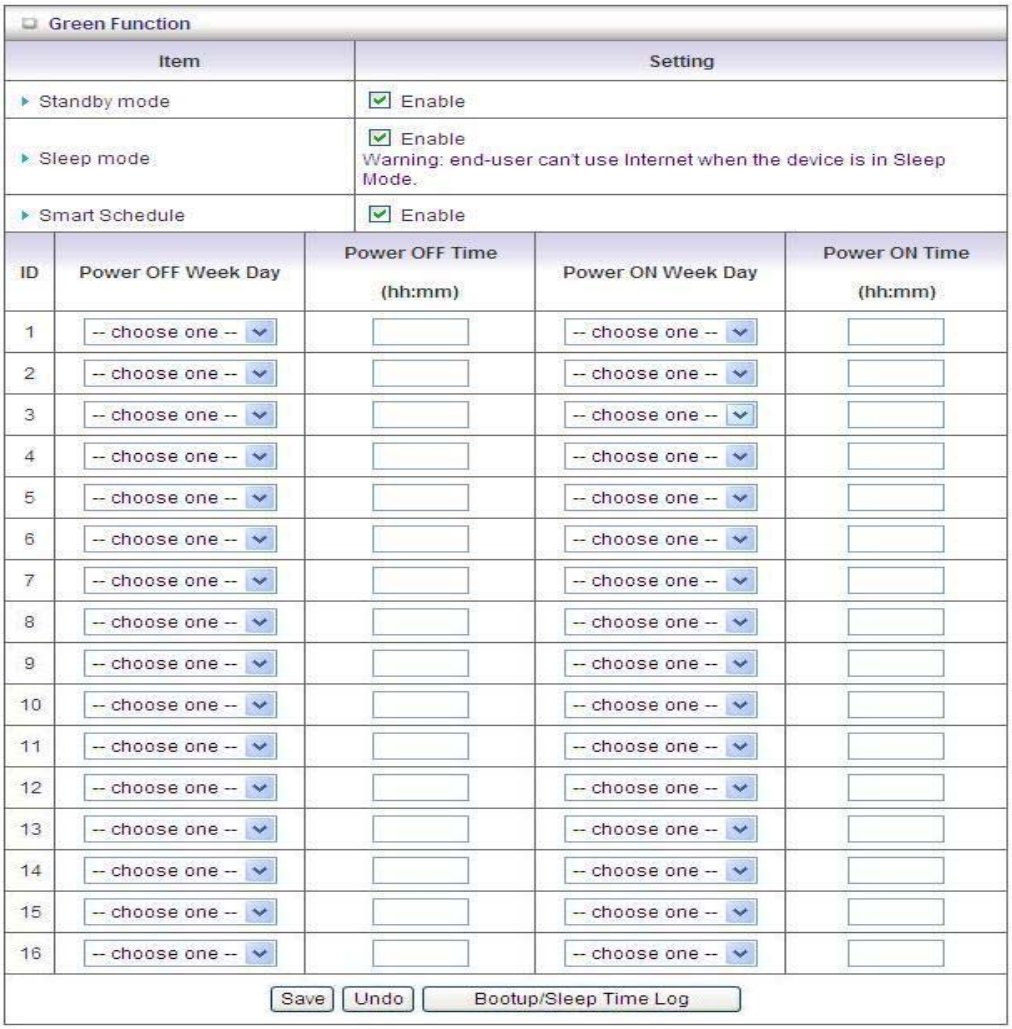
Enter the default password “admin” in the System Password and then click ‘login’ button.

Afterwards, select ‘Advanced’ indicated in the user interface for further configuring this device. In the “Advanced” page, it could be categorized four sections, respectively Basic Setting, Forwarding Rules, Security Setting, and Advanced Setting.

3.1 Basic Setting



3.1.1 Green Function

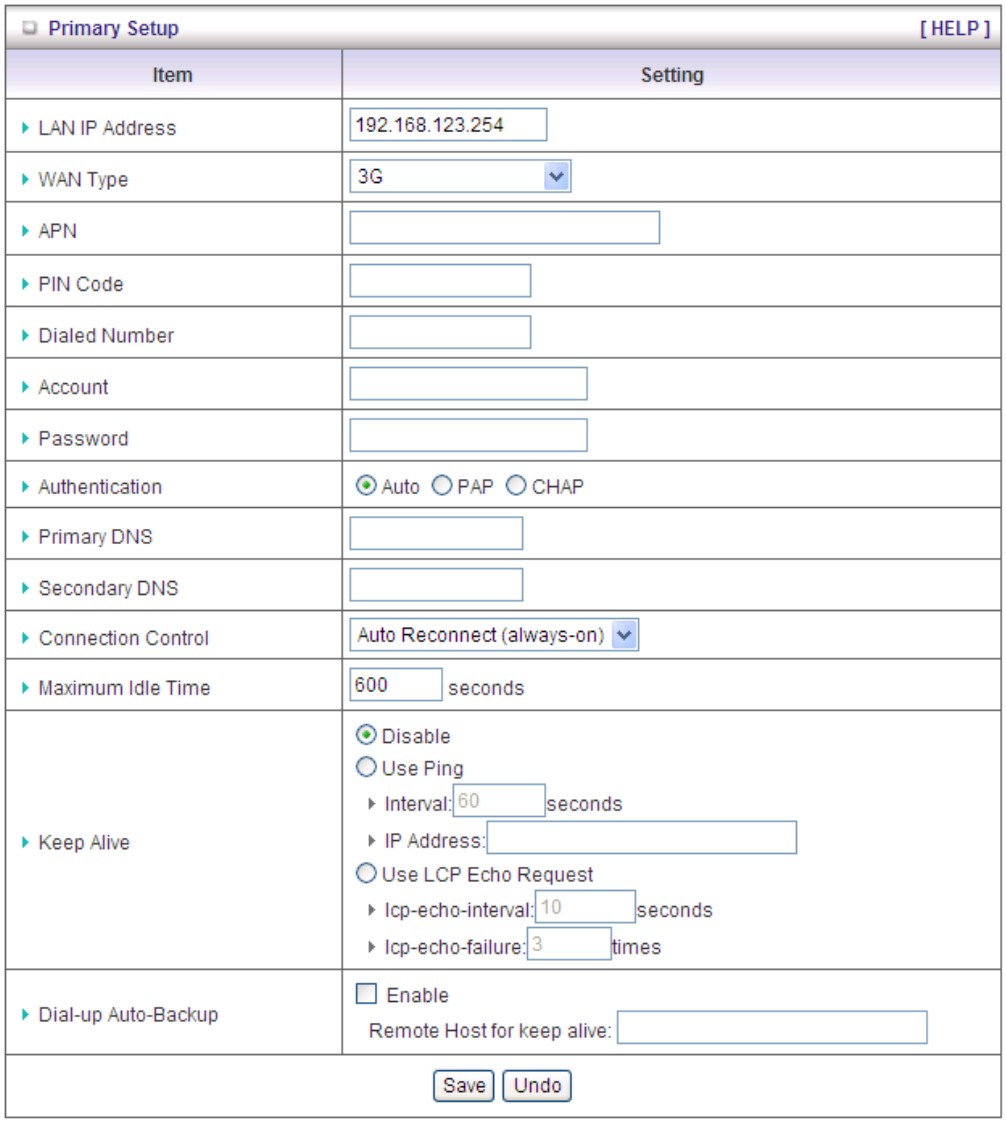


1. **Standby mode:** The device will be automatically switched into standby mode if there are no packets in ten minutes.
2. **Sleep mode:** End user can not use Internet when the device is in sleep mode.
3. **Smart Schedule:** The device would check the packet flow before the power is turned off. For instance, if the router is on the sleeping mode, you could surf the Internet at that time. Afterwards, if there are not any packet flows, the router would be turned off automatically.

3.1.2 Primary Setup

First of all, you are supposed to select the WAN type and then configure the setting.

A. 3G



For 3G WAN Networking. The WAN fields may not be necessary for your connection. The information on this page will only be used when your service provider requires you to enter a User Name and Password to connect with the 3G network.

Please refer to your documentation or service provider for additional information.

1. **LAN IP Address:** The local IP address of this device. The computer on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary.

2. **3G Failover:** When the 3G connection is interrupted, the connection of router would automatically shift to wired line.
3. **WAN Type:** WAN connection type of your ISP. You can click WAN Type combo button to choose a correct one from the following options:
4. **APN**: Enter the APN for your PC card here.(Optional)
5. **Pin Code**: Enter the Pin Code for your SIM card. (Optional)
6. **Dial-Number**: This field should not be altered except when required by your service provider.
7. **Account**: Enter the new User Name for your PC card here, you can contact to your ISP to get it. (Optional)
8. **Password**: Enter the new Password for your PC card here, you can contact to your ISP to get it. (Optional)
9. **Authentication**: Choose your authentication.
10. **Primary DNS**: This feature allows you to assign a Primary DNS Server, contact to your ISP to get it. (Optional)
11. **Secondary DNS**: This feature allows you to assign a Secondary DNS Server, you can contact to your ISP to get it. (Optional)
12. **Connection Control**: Select your connection control. There are 3 modes to select:

    Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

    Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

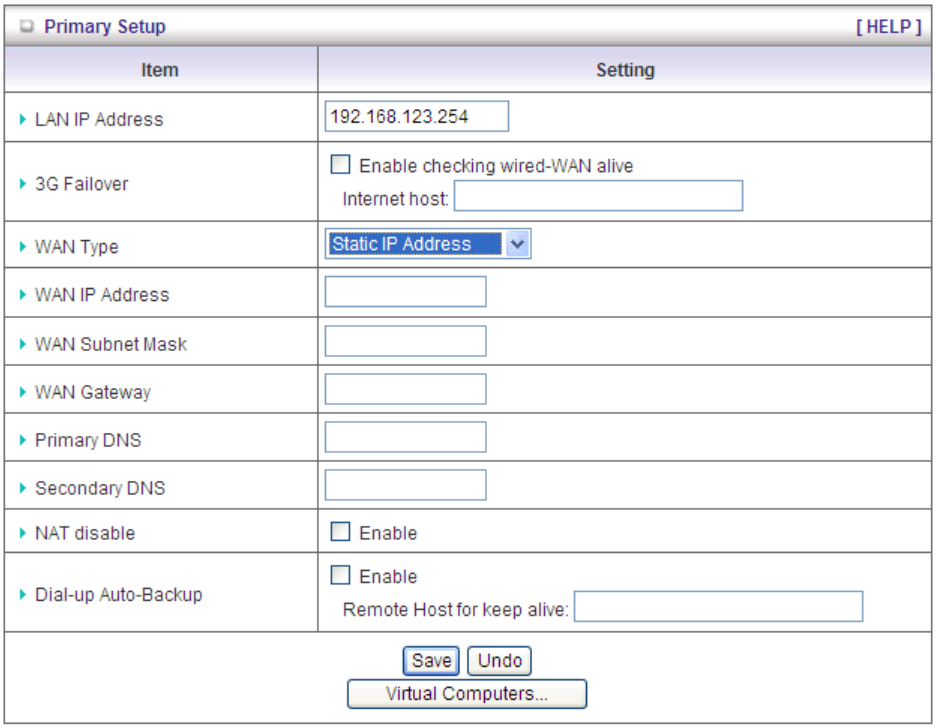
    Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

10. **Maximum Idle Time**: The time of no activity to disconnect your 3G session. Set it to zero or enable “Auto-reconnect” to disable this feature. If Auto-reconnect is enabled, this device will connect with ISP automatically after system is restarted or connection is dropped.
11. **Keep Alive**: This feature must collocate with the function "Auto" of "Auto Connect". Enable it to keep the connection always be established.

    Use Ping: Keep connection alive by sending ICMP ping request to specified IP address

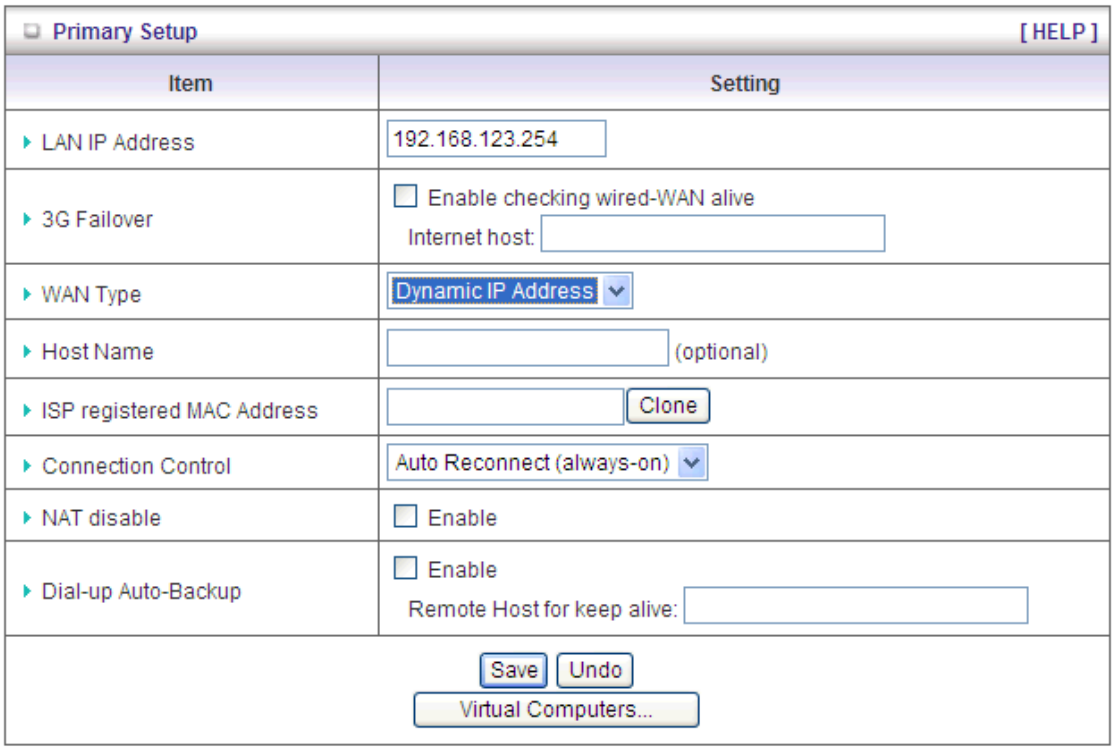
    Use LCP Echo Request: Keep connection alive by sending LCP echo request, unless you know the detailed or not change the default value.

B. Static IP Address



1. **LAN IP Address:** The local IP address of this device. The computer on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary.
2. **3G Failover:** When the 3G connection is interrupted, the connection of router would automatically shift to wired line.
3. **WAN IP Address, Subnet Mask, Gateway, Primary and Secondary DNS**:
   Enter the proper settings provided by your ISP.
4. **NAT disable:** The device would send private IP to other LAN PC if you select enable.

C. Dynamic IP Address



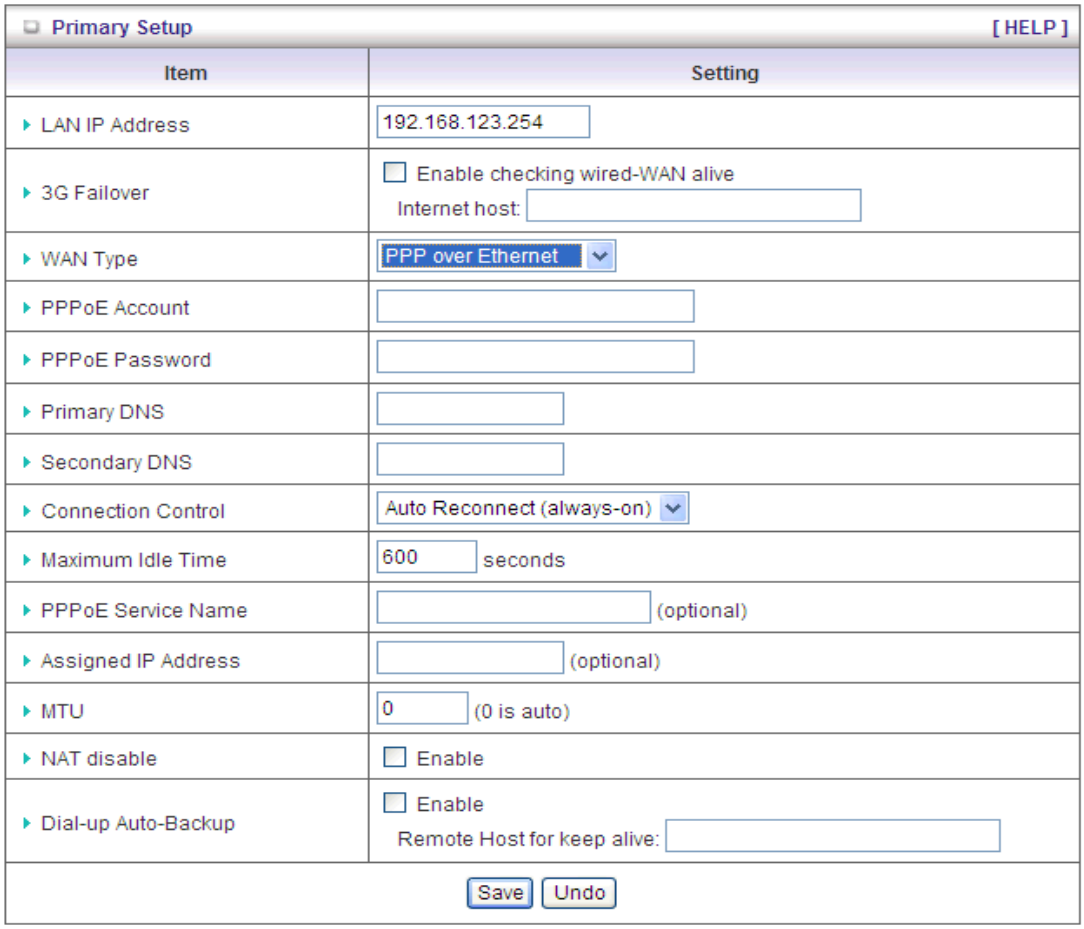
1. **LAN IP Address:** The local IP address of this device. The computer on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary.
2. **3G Failover:** When the 3G connection is interrupted, the connection of router would automatically shift to wired line.
3. **Host Name**: Optional, required by some ISPs, for example, @Home.
4. **ISP registered MAC Address:** Enter MAC address of your ISP. (Optional)
5. **Connection Control**: There are 3 modes to select:

   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

   Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

   Manually: The device will not make the link until someone clicks the connect-button in the Status-page.
6. **NAT disable:** The device would not send private IP to other LAN PC if you select disable.

D. PPP over Ethernet



1. **LAN IP Address:** The local IP address of this device. The computer on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary.
2. **3G Failover:** When the 3G connection is interrupted, the connection of router would automatically shift to wired line.
3. **PPPoE Account:** The account your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it blank.
4. **PPPoE Password:** The password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it blank.
5. **Primary DNS**: This feature allows you to assign a Primary DNS Server, contact to your ISP to get it. (Optional)
6. **Secondary DNS**: This feature allows you to assign a Secondary DNS Server, you can contact to your ISP to get it. (Optional)
7. **Connection Control**: There are 3 modes to select:

   Connect-on-demand: The device will link up with ISP when the clients send outgoing

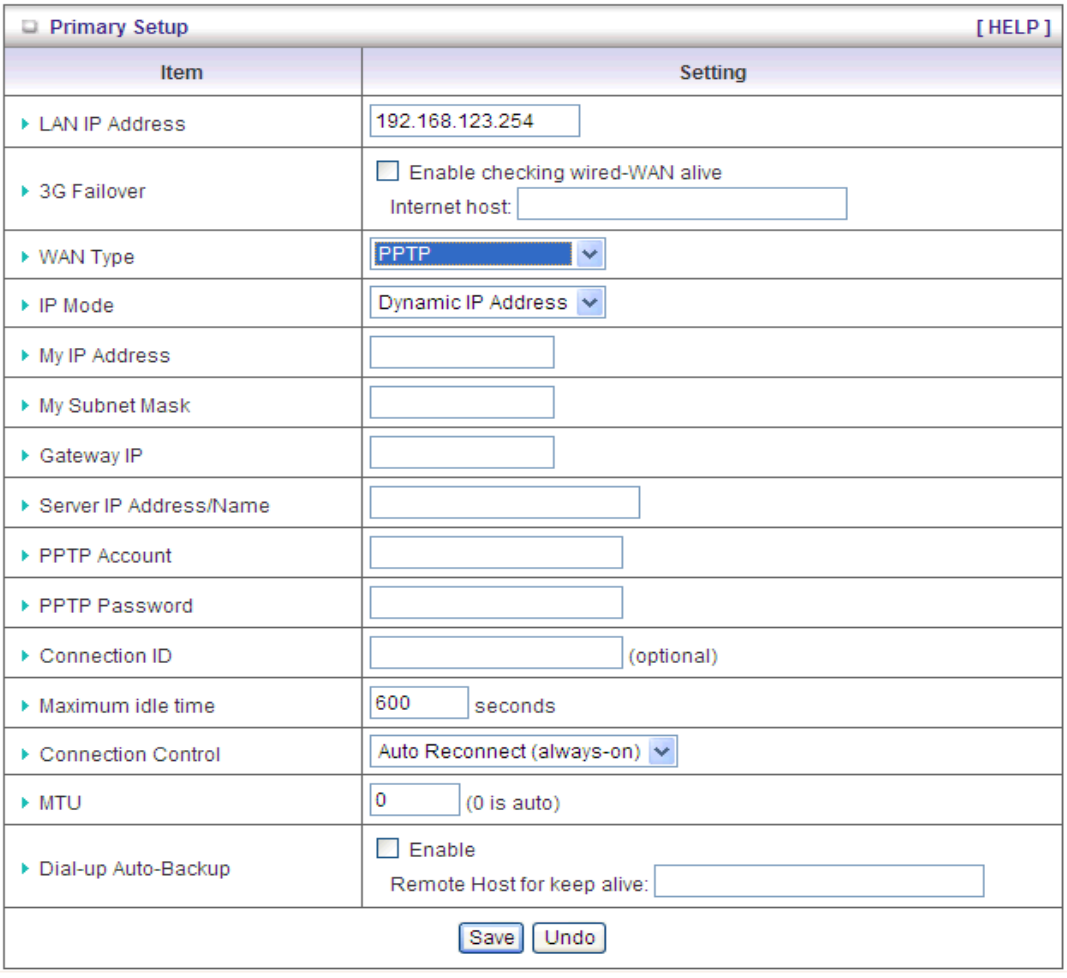
packets.

Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

8. **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.
9. **PPPoE Service Name**: Optional. Input the service name if your ISP requires it. Otherwise, leave it blank.
10. **Assigned IP Address:** It is required by some ISPs. (Optional)
11. **Maximum Transmission Unit (MTU):** Most ISP offers MTU value to users. The default MTU value is 0 (auto).
12. **NAT disable:** The device would not send private IP to other LAN PC if you select disable.

E. PPTP



1. **LAN IP Address:** The local IP address of this device. The computer on your network must

use the LAN IP address of this device as their Default Gateway. You can change it if necessary.

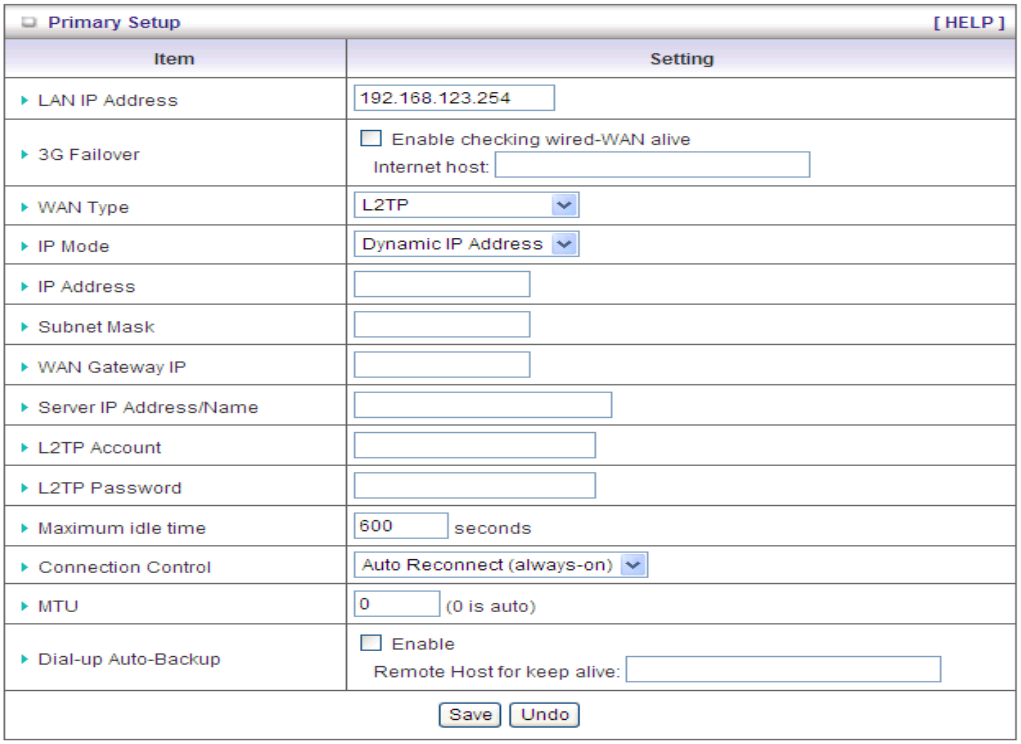
2. **3G Failover:** When the 3G connection is interrupted, the connection of router would automatically shift to wired line.
3. **IP Mode**: Please check the IP mode your ISP assigned, and select “Static IP Address” or “Dynamic IP Address”.
4. **My IP Address** and **My Subnet Mask**: The private IP address and subnet mask your ISP assigned to you.
5. **Gateway IP** and **Server IP Address/Name**: The IP address of the PPTP server and designated Gateway provided by your ISP.
6. **PPTP Account** and **Password**: The account and password your ISP assigned to you. If you don't want to change the password, keep it blank.
7. **Connection ID**: Optional. Input the connection ID if your ISP requires it.
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. If Auto-reconnect is enabled, this device will connect with ISP automatically after system is restarted or connection is dropped.
9. **Connection Control**: There are 3 modes to select:

   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

   Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

   Manually: The device will not make the link until someone clicks the connect-button in the Status-page.
10. **Maximum Transmission Unit (MTU)**: Most ISP offers MTU value to users. The default MTU value is 0 (auto).

F. L2TP



1. **LAN IP Address:** The local IP address of this device. The computer on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary.
2. **3G Failover:** When the 3G connection is interrupted, the connection of router would automatically shift to wired line.
3. **IP Mode**: Please check the IP mode your ISP assigned, and select “Static IP Address” or “Dynamic IP Address”.
4. **IP Address** and **Subnet Mask**: The private IP address and subnet mask your ISP assigned to you.
5. **WAN Gateway IP** and **Server IP Address/Name**: The IP address of the L2TP server and designated Gateway provided by your ISP.
6. **L2TP Account** and **Password**: The account and password your ISP assigned to you. If you don't want to change the password, keep it blank.
7. **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. If Auto-reconnect is enabled, this device will connect with ISP automatically, after system is restarted or connection is dropped.
8. **Connection Control**: There are 3 modes to select:

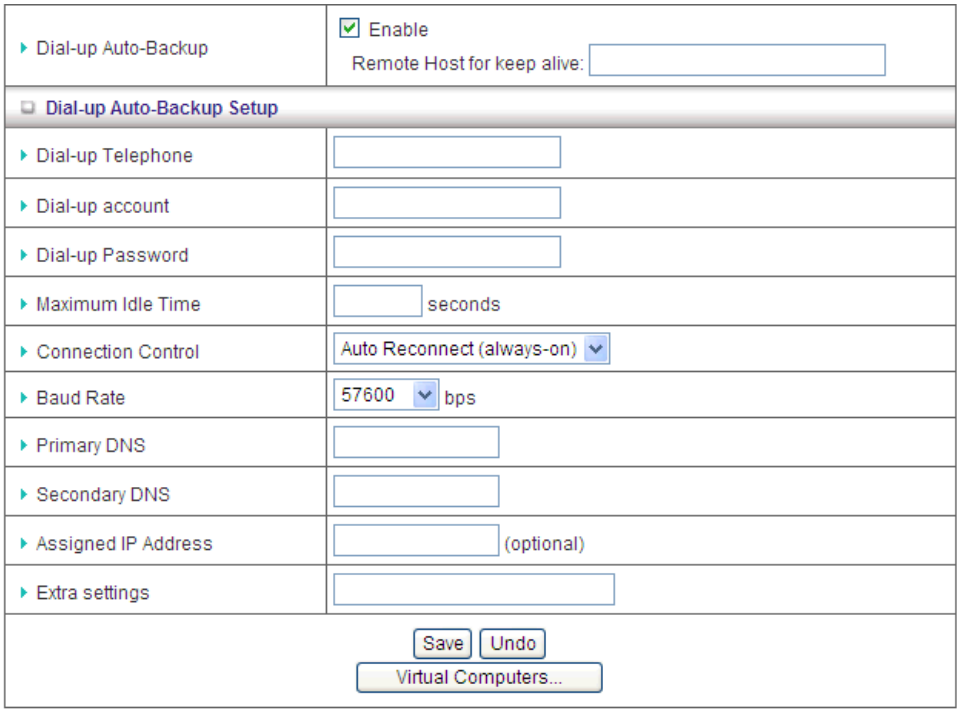
   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

9. **Maximum Transmission Unit (MTU)**: Most ISP offers MTU value to users. The default MTU value is 0 (auto).

Click to enable **"Dial-up Auto-Backup"** and you can find Dial-up Auto-Backup setting.



1. **Dial-up Telephone** Input the dial-up telephone provided by ISP.
2. **Dial-up account:** Input the account provided by your ISP.
3. **Dial-up Password:** Input the password provided by your ISP.
4. **Maximum Idle Time:** The time of no activity to disconnect your Dial-up Network session. Set it to zero or enable "Auto-reconnect" to disable this feature. If Auto-reconnect is enabled, this device will connect with ISP automatically, after system is restarted or connection is dropped.
5. **Connection Control**: There are 3 modes to select:

   Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

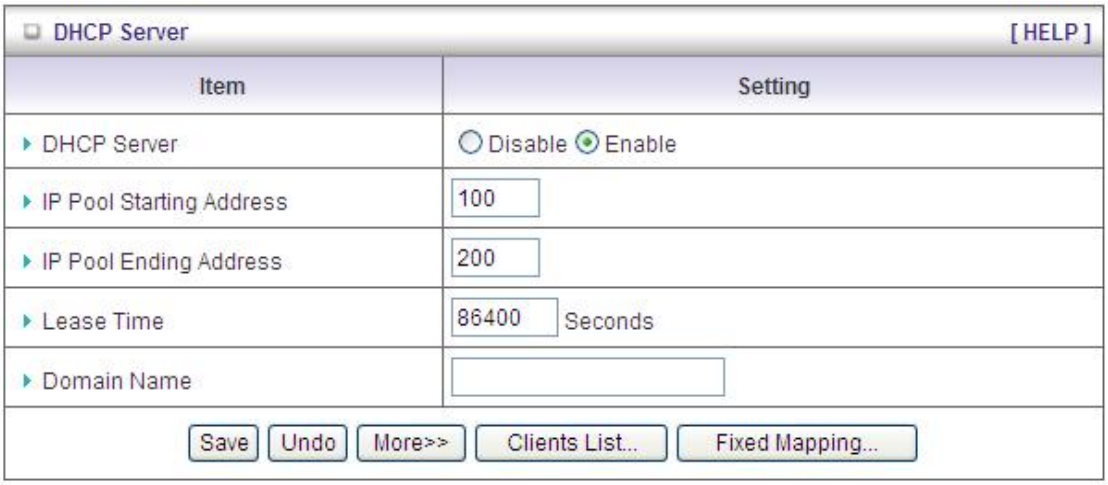
   Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

6. **Baud Rate:** The rate of packet transmitting.
7. **Primary DNS**: This feature allows you to assign a Primary DNS Server, contact to your ISP to get it. (Optional)
8. **Secondary DNS**: This feature allows you to assign a Secondary DNS Server, you can contact to your ISP to get it. (Optional)
9. **Assigned IP Address:** If your ISP gave you a specified IP address, fill it here.
10. **Extra Settings:** Sometimes you have to add some extra AT commands to improve your modem connection, fill it here.

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

3.1.3 DHCP Server

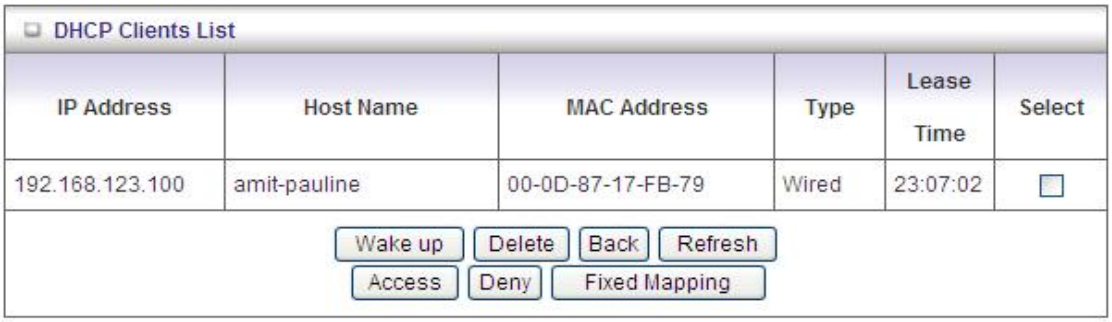


1. **DHCP Server:** Choose either **Disable** or **Enable**. If you enable the DHCP Server function, the following settings will be effective.
2. **IP Pool Starting/Ending Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool 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:** This information will be passed to the clients. **(**Optional)

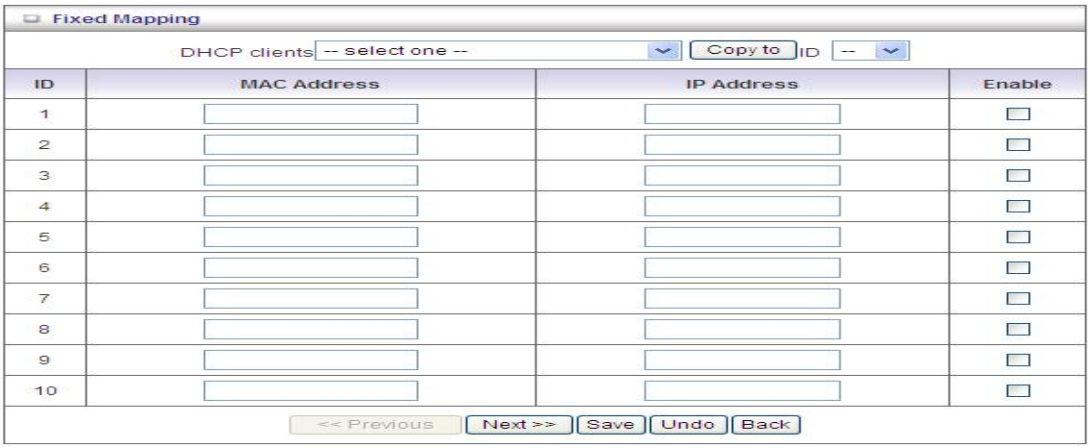
Press **“More>>”** and you can find more settings.

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

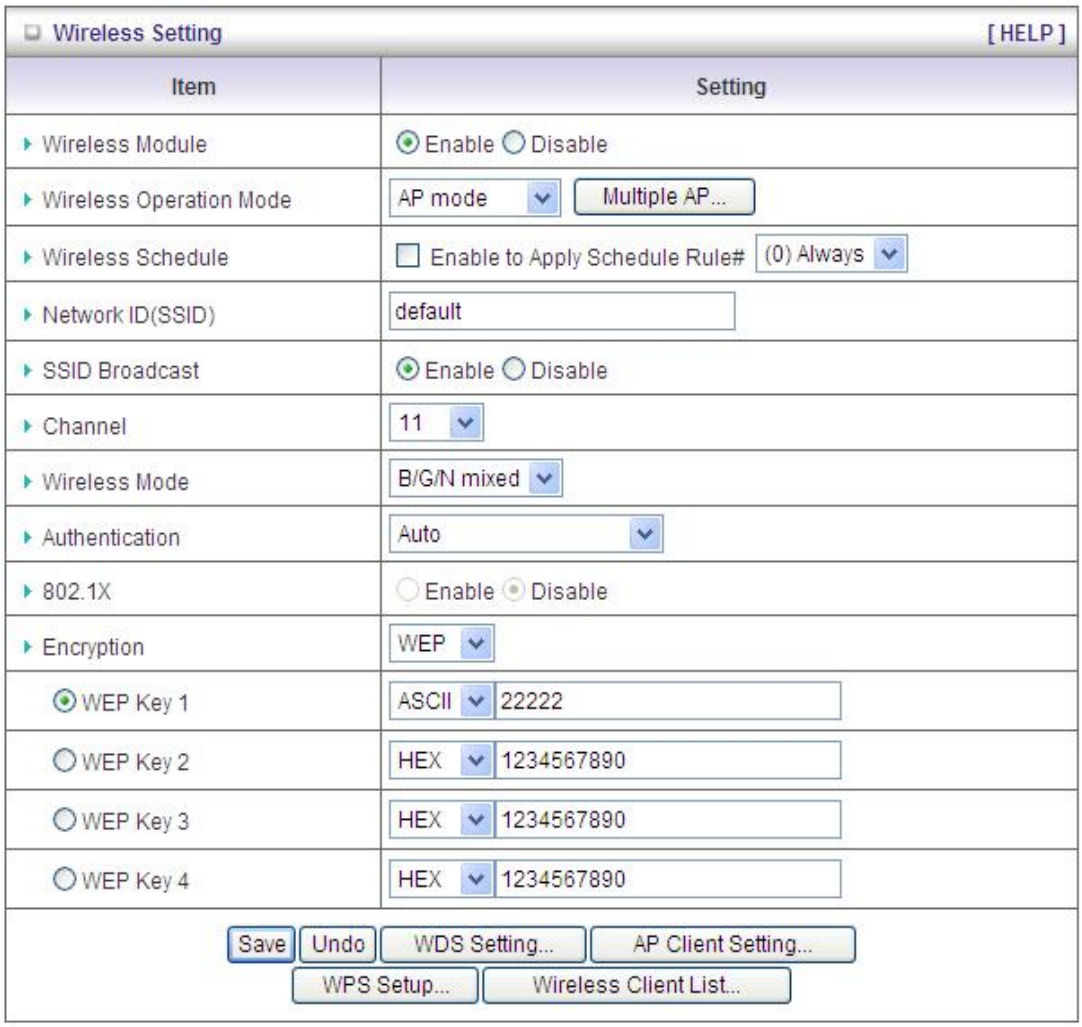
Press **“Clients List”** and the list of DHCP clients will be shown consequently.



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



3.1.4 Wireless Settings



Wireless settings allow you to set the wireless configuration items.

1. **Wireless Module:** You can enable or disable wireless function.
2. **Wireless Operation Mode:** Choose appropriate wireless operation mode.
3. **Wireless Schedule:** Click ‘’enable” to apply schedule rule.
4. **Network ID (SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is “default”)
5. **SSID Broadcast:** The 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.
6. **Channel:** The radio channel number. The permissible channels depend on the

Regulatory Domain. The factory default setting is as the following: channel 6 for North America; channel 7 for European (ETSI); channel 7 for Japan.

7. **Wireless Mode:** Choose “B/G mixed”, “B only”, “N only”, or “B/G/N mixed”. The factory default setting is “B/G/N mixed”.
8. **802. 1X:** Click “enable” to enable the function of 802.1X.
9. **Authentication mode:** You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.

- **Open**

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

- **Shared**

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

- **Auto**

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

- **WPA-PSK**

Select Encryption 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.

- **WPA2-PSK**

  WPA2-PSK user AES and TKIP for Same the encryption, the others are same as the WPA2-PSK.

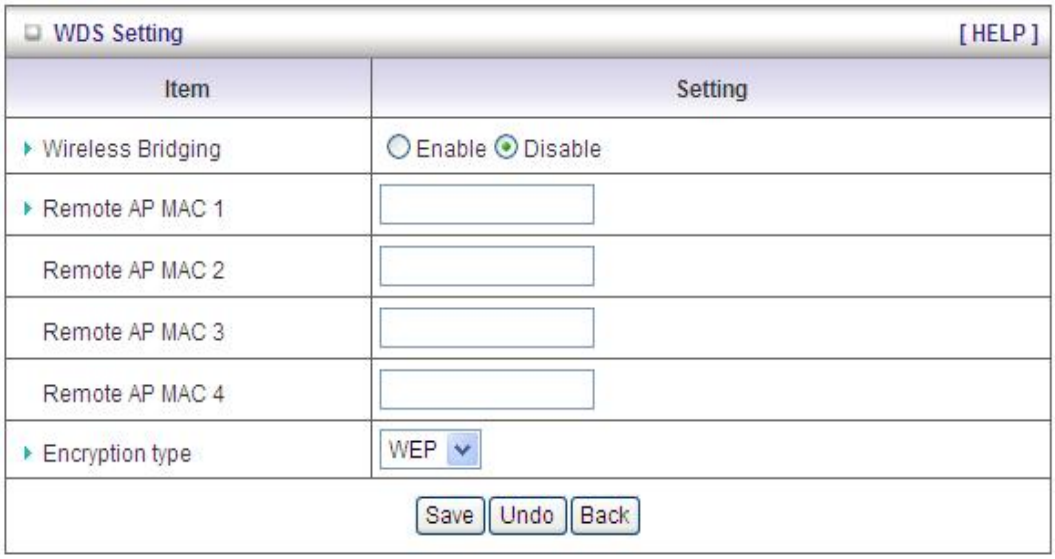
- **WPA-PSK/WPA2-PSK**

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

- **WPA/WPA2**

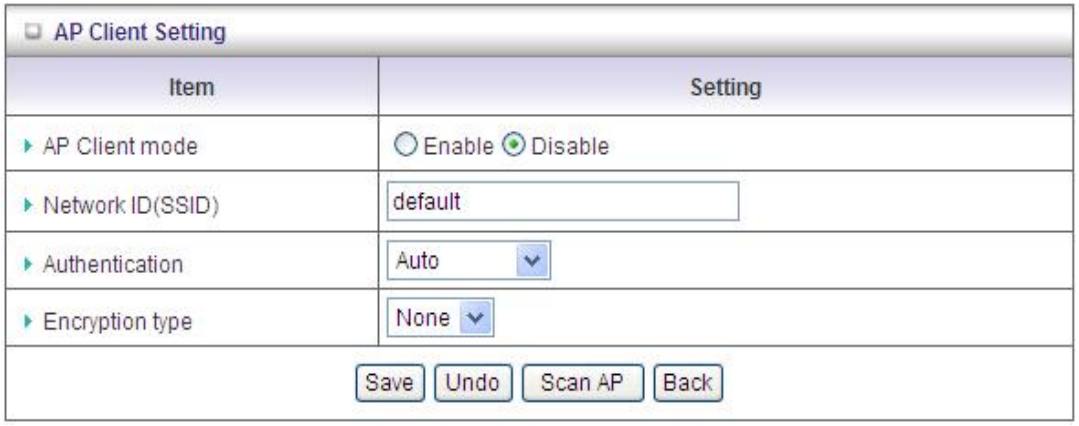
  Another encryption options for WPA-TKIP and WPA2-AES, the others are same the WPA.

Press **"WDS Setting" and** It allows PC to get connected to wireless network within the area.



1. **Wireless Bridging:** You could enable this function by selecting "Enable".
2. **Remote AP MAC 1~Remote AP MAC 4:** Enter the wireless MAC into the blank.
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.
4. **Encryption key:** Set up encryption key based on the rule of encryption type. Once you set up encryption, second LAN PC must enter the same encryption type as the first one.

Press **“AP Client Setting”**



1. **AP Client mode:** You could enable this function by selecting “Enable”.
2. **Network ID(SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is “default”)
3. **Authentication:** Choose your authentication.
4. **Encryption type:**

- **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

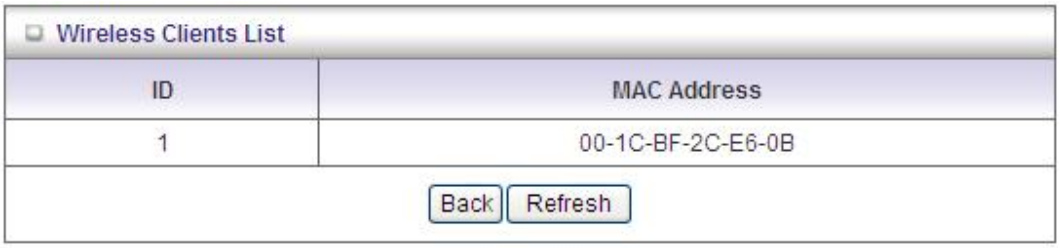
- **WPA2-PSK**

  WPA2-PSK user AES and TKIP for Same the encryption, the others are same as the WPA2-PSK.

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

1. **WPS:**.You can enable this function by selecting “Enable”. WPS offers a safe and easy way to allow the wireless clients connected to your wireless network.
2. **AP PIN**: You can press Generate New Pin to get an AP PIN.
3. **Config Mode**: Select your 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”.

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

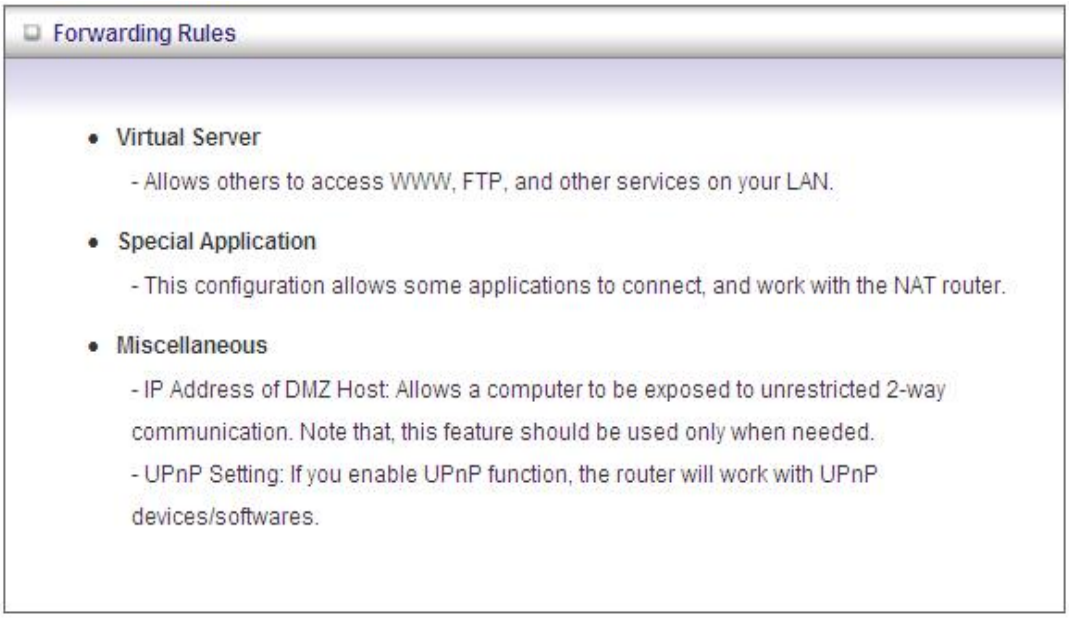


Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

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.

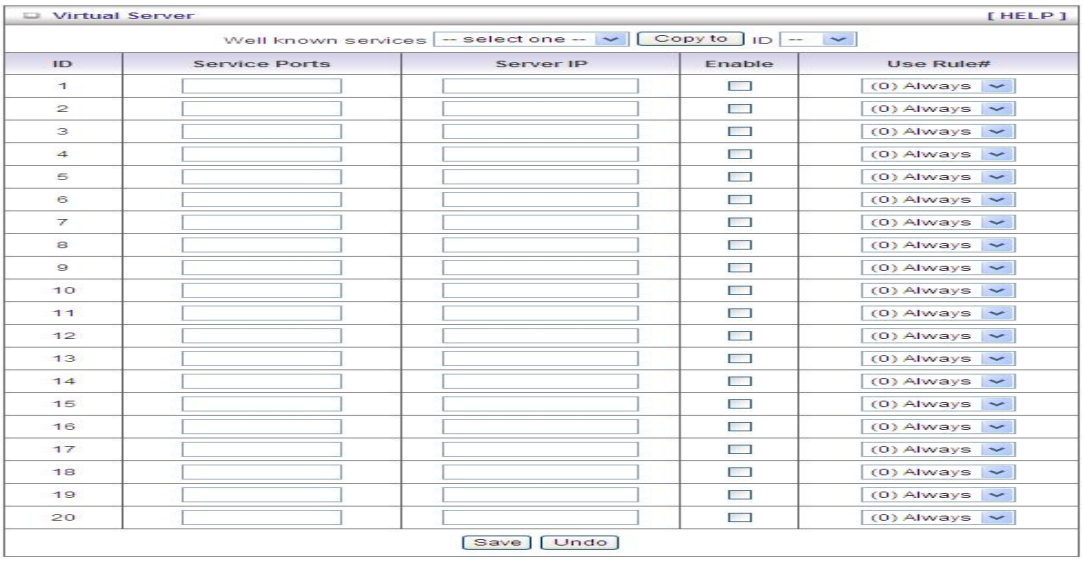
3.2 Forwarding Rules



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**.



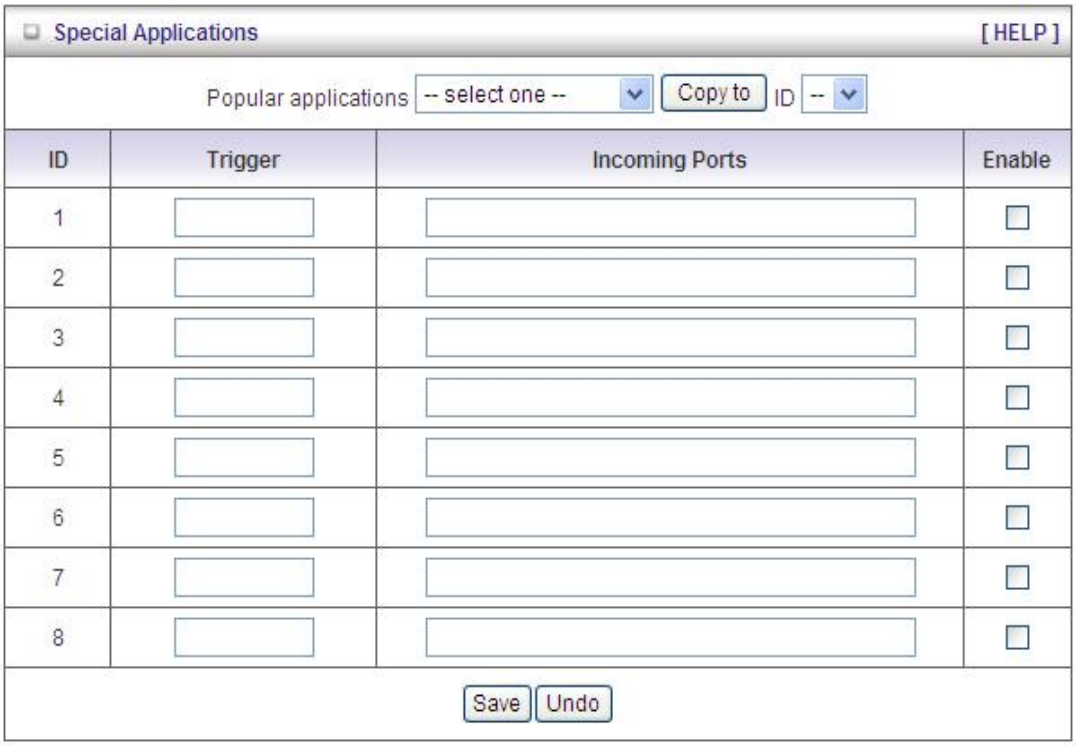
For example, if you have an FTP server (port 21) at 192.168.123.1, a Web server (port 80) at 192.168.123.2, and a VPN server at 192.168.123.6, then you need to specify the following virtual server mapping table:

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

Afterwards, 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.



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

1. **Trigger:** The outbound port number issued by the application.

2. **Incoming Ports**: When the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

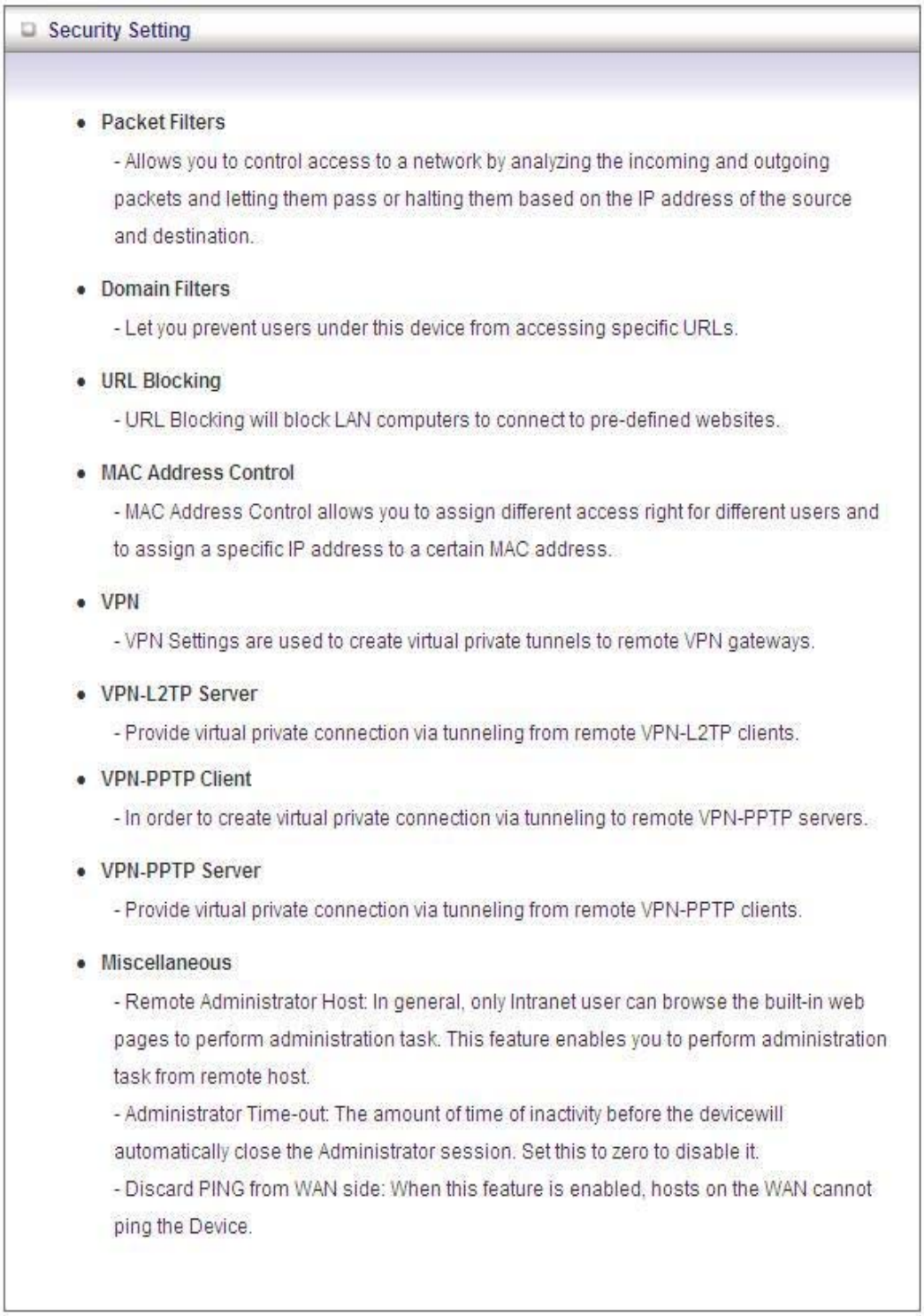
Afterwards, Click on “Save” to store your settings or click “Undo” to give up the changes.

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.
3. **IGMP setting:** IGMP is Internet Group Management Protocol. It could transmit message to groups of computers.

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

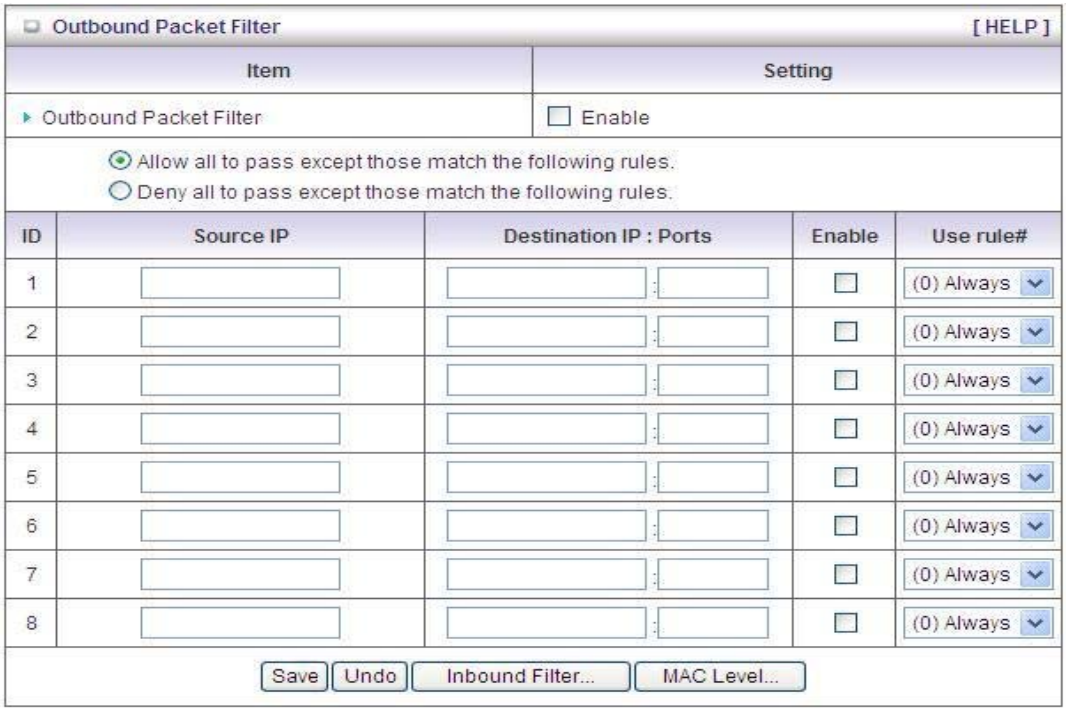
3.3 Security Setting



3.3.1 Packet Filters

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

1. Allow all to pass except those match the 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#

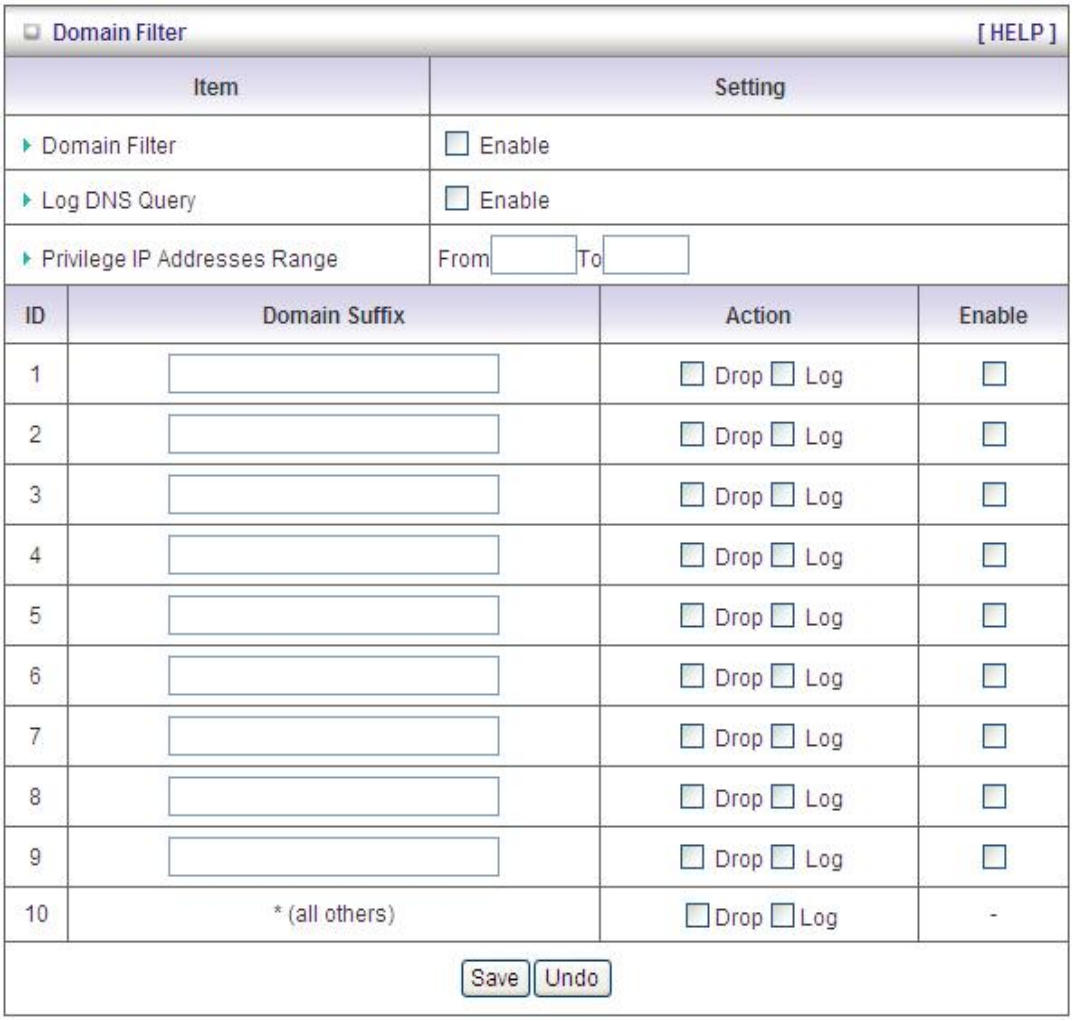
For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.

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.

Afterwards, 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.

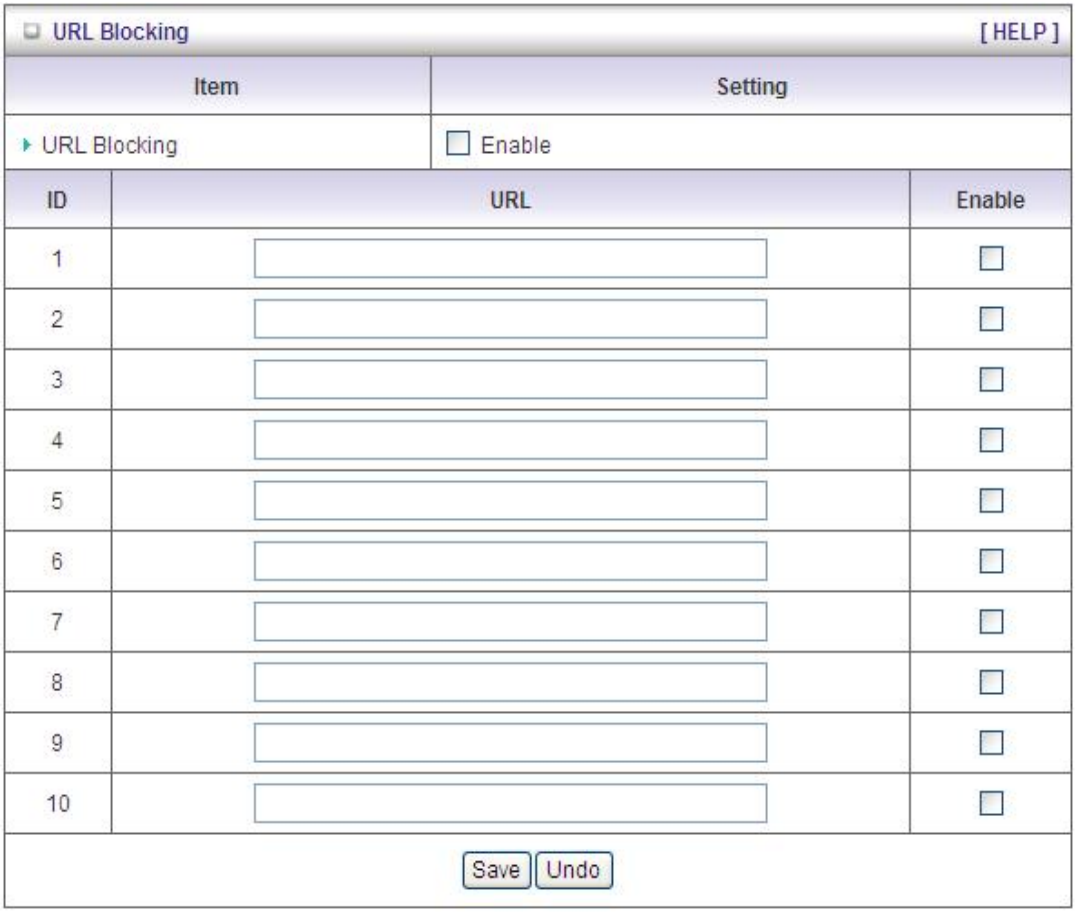
1. **Domain Filter**: Check if you want to enable Domain Filter.
2. **Log DNS Query**: Check if you want to log the action when someone accesses the specific URLs.
3. **Privilege IP Address Range**: Setting a group of hosts and privilege these hosts to access network without restriction.

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 these access.
6. **Enable**: Check to enable each rule.

Afterwards, 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 requires user to input suffix (like .com or .org, etc), while URL Blocking requires 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.



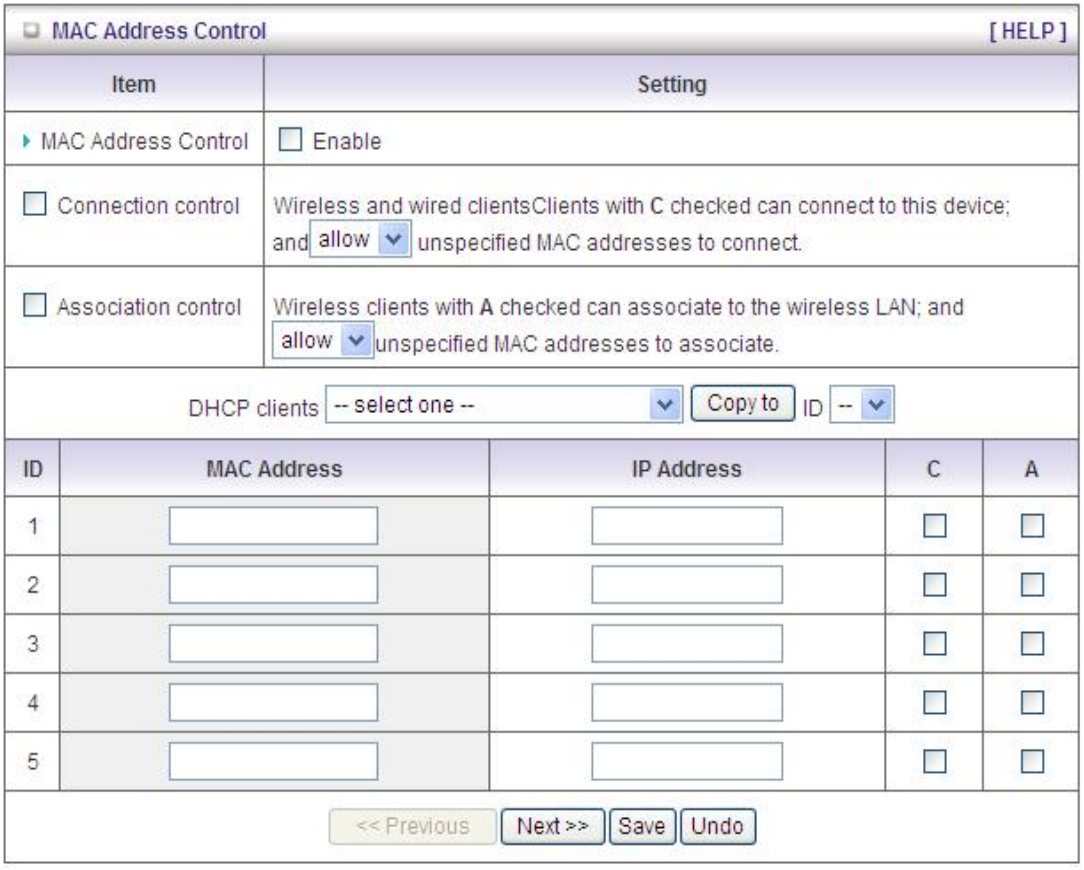
1. **URL Blocking**: Check if you want to enable URL Blocking.

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.

Afterwards, 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

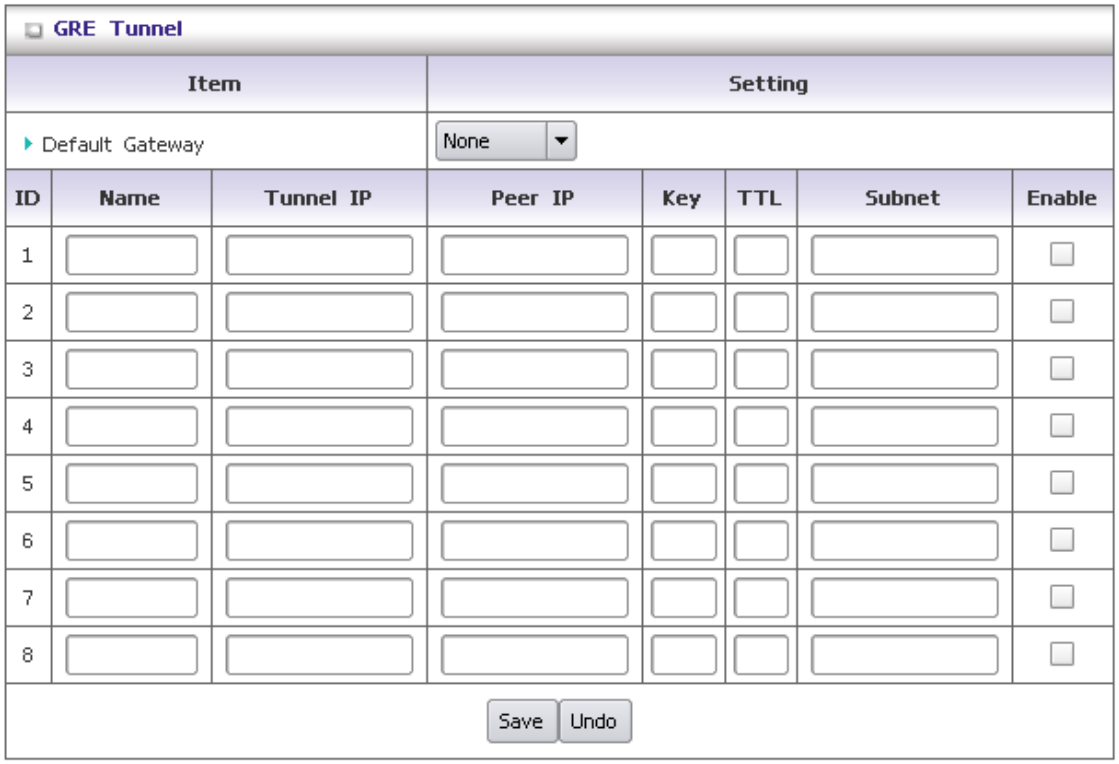
below), to connect with this device.

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.

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

3.3.5 GRE Tunnel

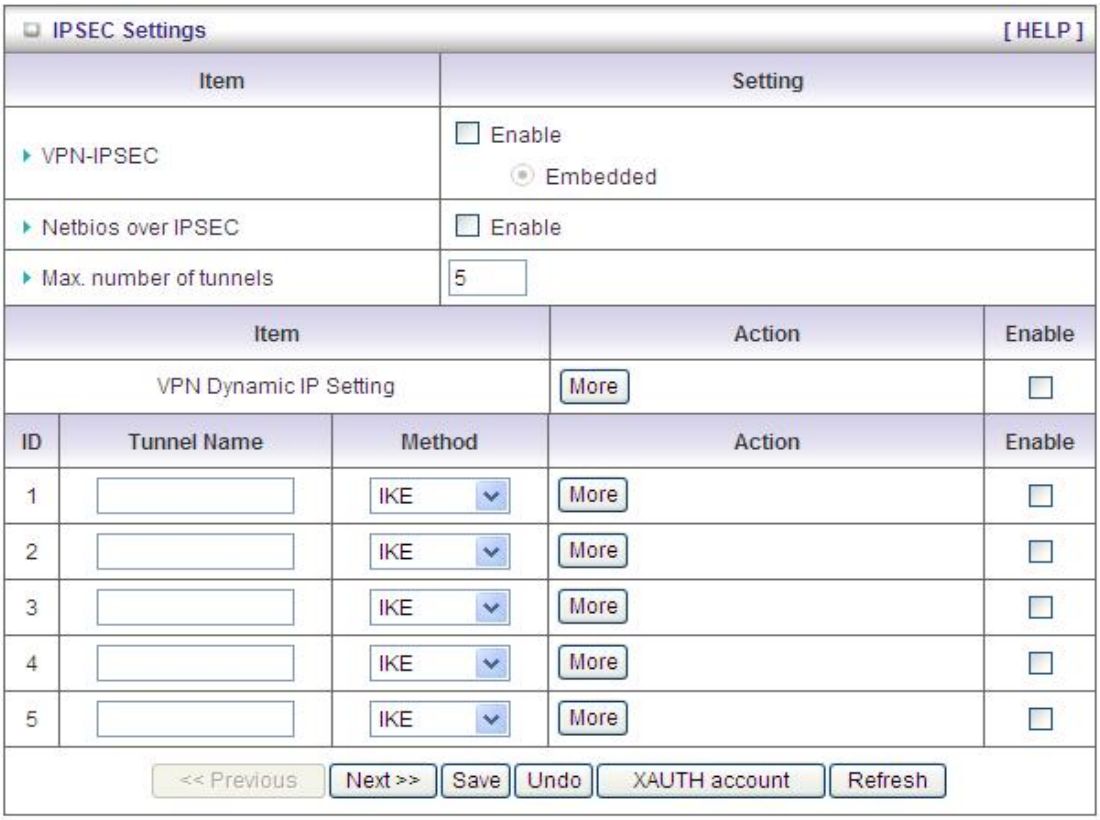
The GRE tunnel could bridge two LAN subnets, all packets with IP header could pass it, no matter it is unicast, broadcast, or multicast.



1. **Name**: Tunnel name, it is used for identifying each tunnel interface.
2. **Tunnel IP**: WAN side IP.
3. **Peer IP**: Remote Gateway IP.
4. **Key**: This value is used for tunnel priority. The tunnel with no key has the highest priority, and the priority is lower if the value is larger.
5. **TTL**: TTL for packets. Usually, we use the value 255.
6. **Subnet**: Remote subnet.

3.3.6 VPN-IPSEC

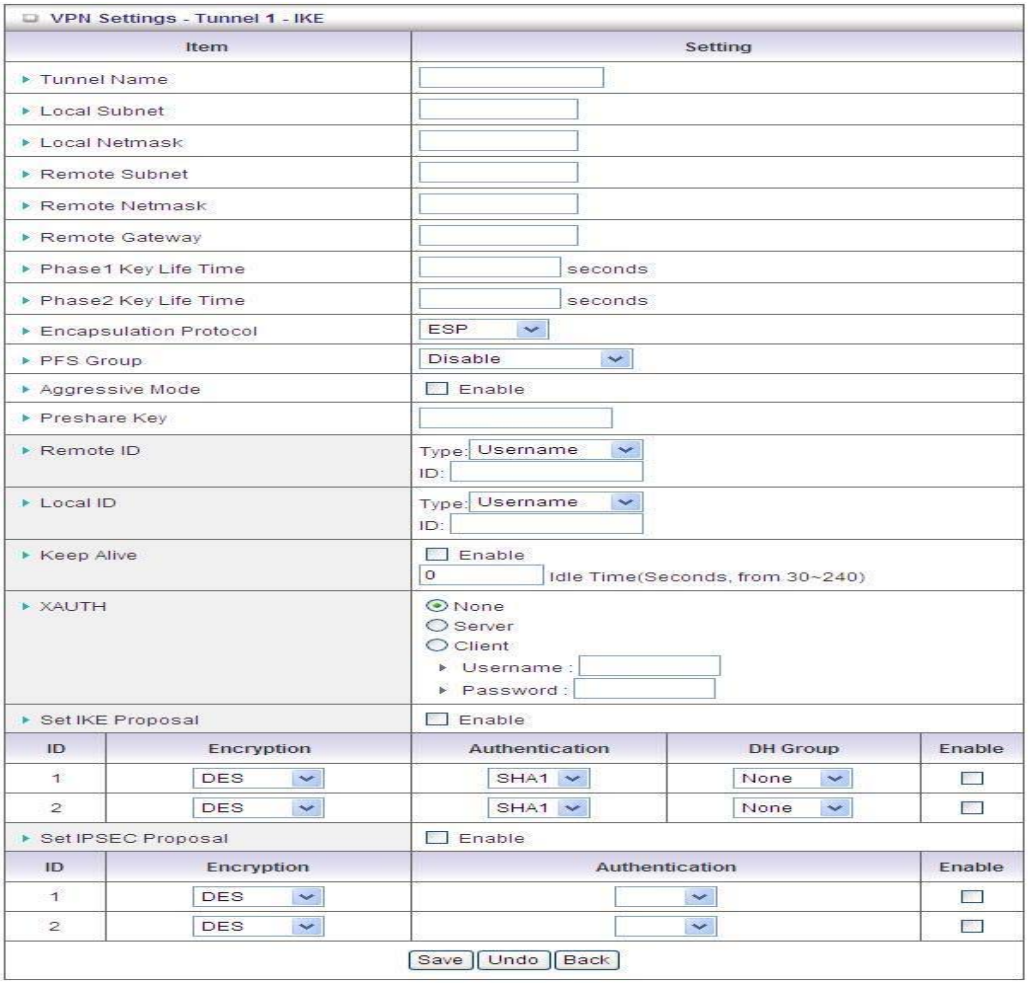
VPN Settings are used to create virtual private tunnels to remote VPN.



3.3.6.1 IPSEC Settings

1. **VPN-IPSEC:** You could trigger the function of VPN-IPSEC if you click “enable”.
2. **Netbios over IPSEC:** If you would like two LAN to receive the Netbios from Network Neighborhood, you have to click “enable”.
3. **Max. number of tunnels:** The device supports 1~20 tunnels.
4. **Tunnel Name:** Indicate which tunnel that is focused now.
5. **Method:** IPSec VPN supports two kinds of key-obtained methods: manual key and automatic key exchange. Manual key approach indicates that two end VPN router setup authenticator and encryption key by system managers manually. However, IKE approach will perform automatic Internet key exchange. System managers of both end gateways only need set the same pre-shared key. To setup more details configuration of IKE and manual key, please press **“more”**.

3.3.6.2 VPN Settings-IKE



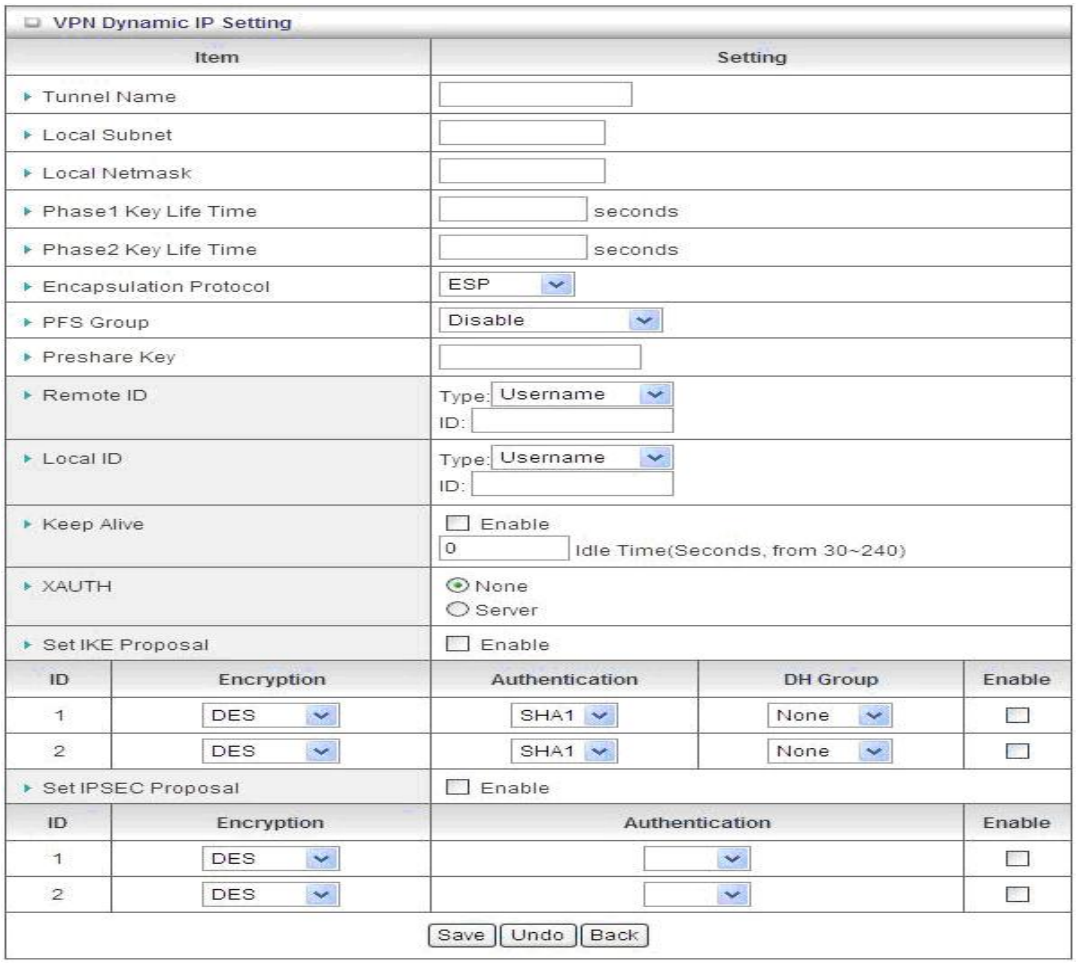
1. **Tunnel Name:** Indicate which tunnel that is focused now
2. **Local subnet:** The subnet of LAN site of local VPN router. It can be a host, a partial subnet, and the whole subnet of LAN site of local router.
3. **Local Netmask:** Local netmask combined with local subnet to form a subnet domain.
4. **Encapsulation Protocol:** There are three protocols to select : ESP, AH, ESP+AH.
5. **PFS Group:** There are five options can be selected: Disable, Group 1, Group 2, Group 5, and Same as phase 1. You can select a DH Group for Phase 2 Key exchanging, or use the same DH Group as Phase 1, or, disable PFS option.
6. **Aggressive Mode:** Enabling this mode will accelerate establishing tunnel, but the devicewill suffer from less security in the meanwhile. Hosts in both ends of the tunnel must support this mode so as to establish the tunnel properly.
7. **Preshare Key:** The first key that supports IKE mechanism of both VPN router and VPN client host for negotiating further security keys. The pre-shared key must be same for

both VPN router and client

8. **Remote ID:** The Type and the Value are the same as the Type and the Value of the Local ID of the remote VPN router.
9. **Local ID:** The Type and the Value are the same as the Type and the Value of the Remote ID of the remote VPN gateway.
10. **Keep Alive:** Click “enable” to keep VPN connection alive. Otherwise, if there are no packets transmitting, the VPN tunnel would disconnect.
11. **Xauth:** If you click “Xauth”. It means that it is without Extended Authentication(xAuth). If you. However, if you choose “Server”, it will verify the legality of user information from VPN client. The user information that is provided by VPN client needs to match to user information that is in local user database of VPN server.
12. **Set IKE Protocol:** Click “enable” to set IKE Protocol. The default value will be used if this option is disabled.
13. **Encryption/Authentication/DH Group:** Select appropriate encryption, authentication and DH Group

3.3.6.3 VPN Dynamic IP Setting

If client side could not receive the fixed IP and need to have connection established, please configure VPN Dynamic IP Setting. For instance, the business traveler would like to use laptop to get connected to the company’s internal website.

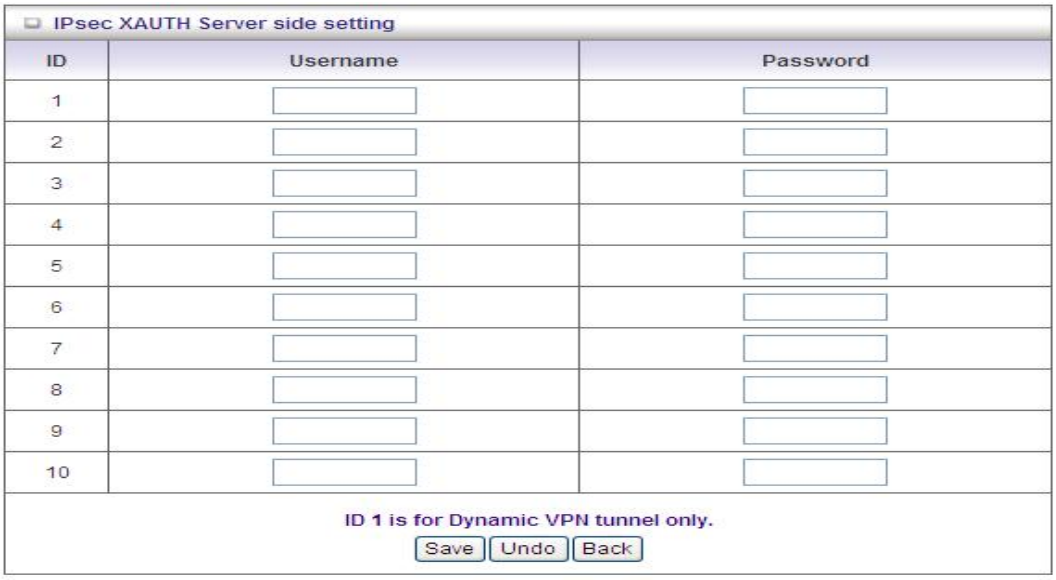


1. **Tunnel Name:** Indicate which tunnel that is focused now
2. **Local subnet:** The subnet of LAN site of local VPN router. It can be a host, a partial subnet, and the whole subnet of LAN site of local router.
3. **Local Netmask:** Local netmask combined with local subnet to form a subnet domain.
4. **Encapsulation Protocol:** There are three protocols to select : ESP, AH, ESP+AH.
5. **PFS Group:** There are five options can be selected: Disable, Group 1, Group 2, Group 5, and Same as phase 1. You can select a DH Group for Phase 2 Key exchanging, or use the same DH Group as Phase 1, or, disable PFS option.
6. **Preshare Key:** The first key that supports IKE mechanism of both VPN router and VPN client host for negotiating further security keys. The pre-shared key must be same for both VPN router and client.
7. **Remote ID:** The Type and the Value are the same as the Type and the Value of the Local ID of the remote VPN router.
8. **Local ID:** The Type and the Value are the same as the Type and the Value of the Remote ID of the remote VPN gateway.
9. **Keep Alive:** Click “enable” to keep VPN connection alive. Otherwise, if there are no

packets transmitting, the VPN tunnel would disconnect.

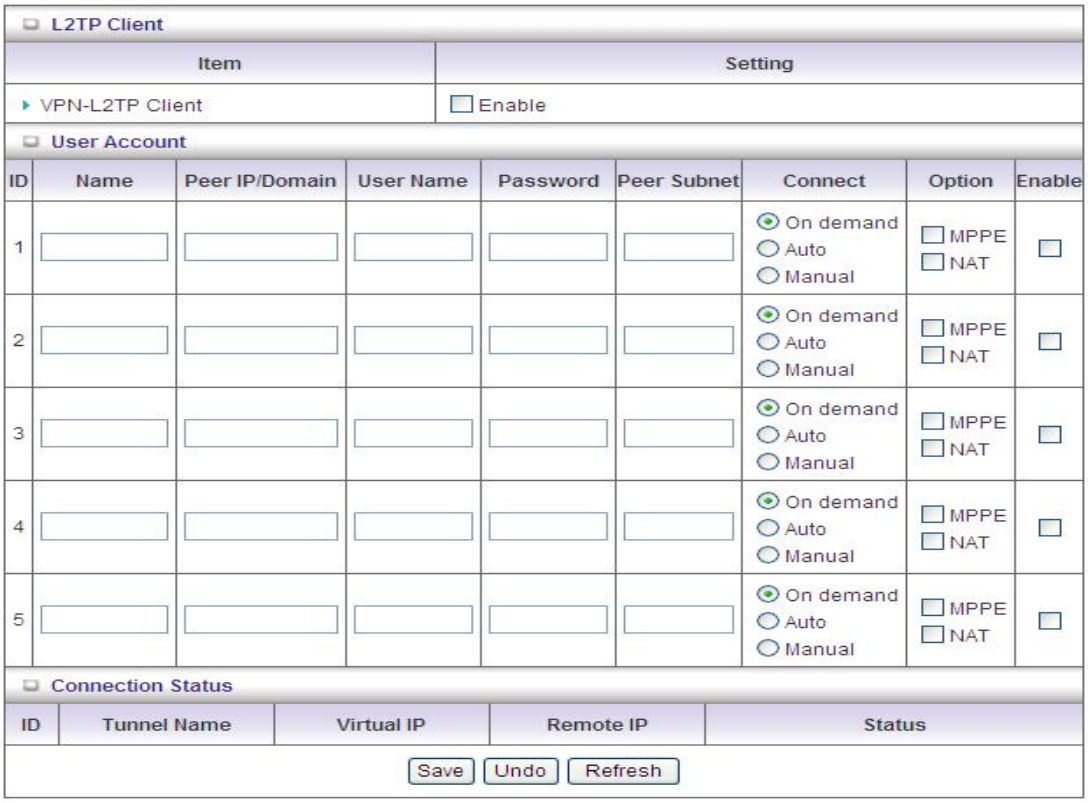
10. **Xauth:** If you click “Xauth”. It means that it is without Extended Authentication(xAuth). If you. However, if you choose “Server”, it will verify the legality of user information from VPN client. The user information that is provided by VPN client needs to match to user information that is in local user database of VPN server.
11. **Set IKE Protocol:** Click “enable” to set IKE Protocol. The default value will be used if this option is disabled.
12. **Encryption/Authentication/DH Group:** Select appropriate encryption, authentication and DH Group

Press **“XAUTH”** account and you could configure Xauth account and password in this section.



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

3.3.7 VPN-L2TP Client



1. **VPN-L2TP Client:** Click “enable” to enable VPN-L2TP Client function.
2. **Name:** The name of tunnel.
3. **Peer IP/Domain:** Input the L2TP Server IP or domain name.
4. **User Name:** The account your ISP assigns to you.
5. **Password:** The password your ISP assigns to you.
6. **Peer Subnet:** Enter peer subnet.
7. **Connect:** The way of triggering VPN connection. There are three modes to select:

   On-demand: The device will link up with ISP when the clients send outgoing packets.

   Auto (Always-on): The device will link with ISP until the connection is established.

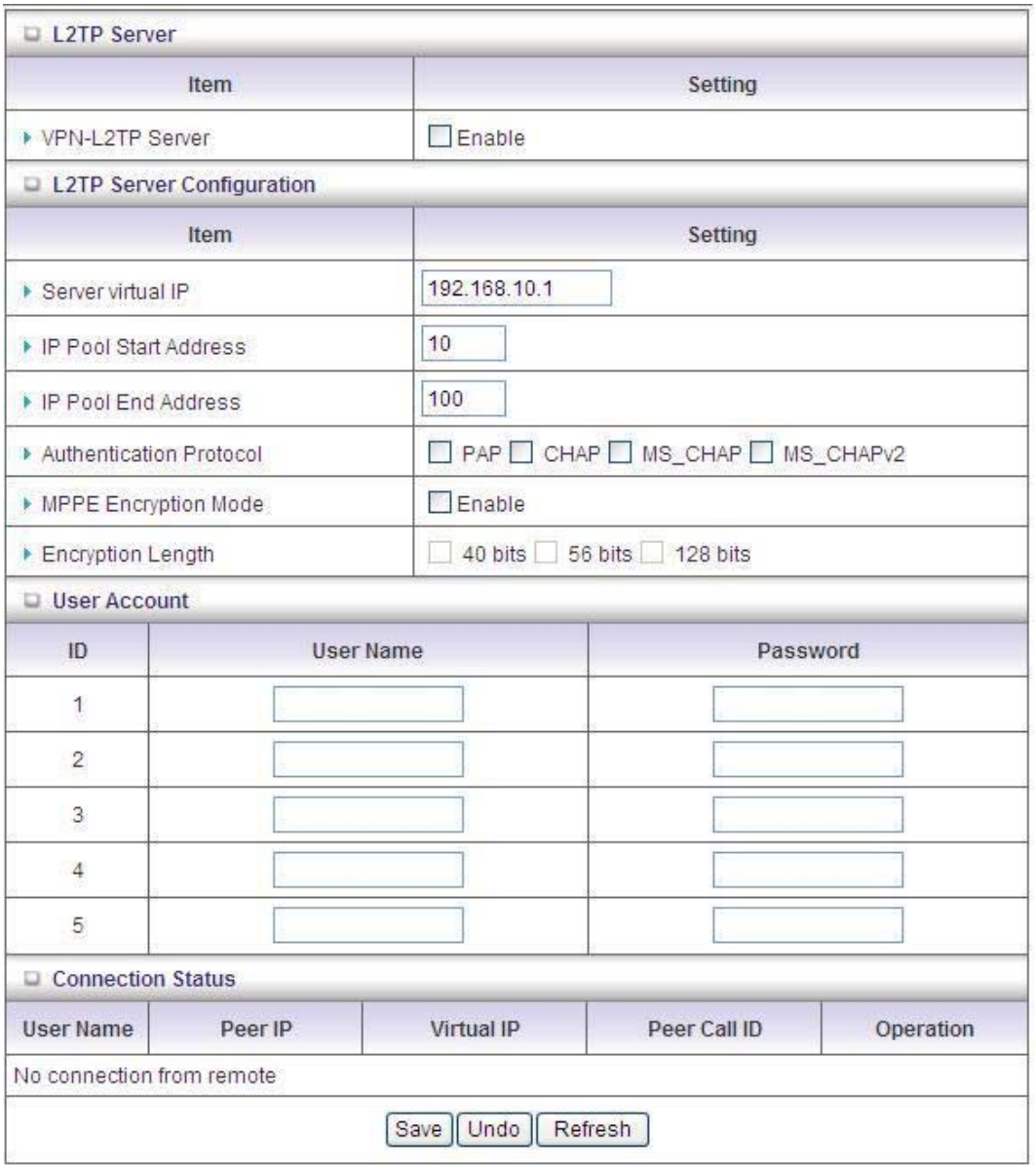
   Manually: The device will not make the link until someone clicks the connect-button in the Status-page.
8. **Option:**

   MPPE: The MPPE encryption supports.

   NAT: The Nat Traversal supports.

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

3.3.8 VPN-L2TP Server



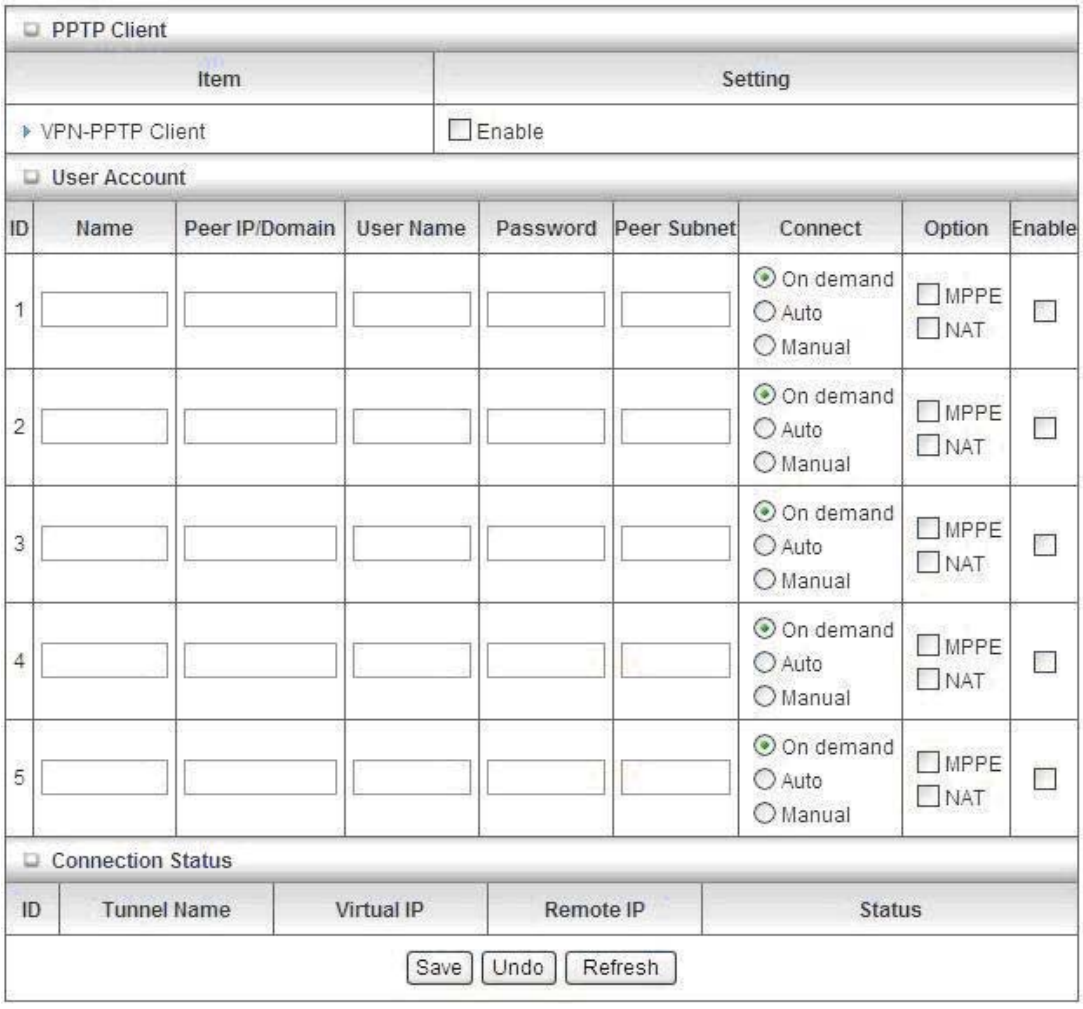
1. **VPN-L2TP Server:** Click “enable” to enable the function of VPN-L2TP Server.
2. **Server Virtual IP:** The IP address of L2TP server. This IP address should be different from IP address of PPTP server and LAN subnet of VPN gateway.
3. **IP Pool Start Address:** The start virtual IP Address that sends to the client.
4. **IP Pool End Address:** The end virtual IP Address that sends to the client.
5. **Authentication Protocal:** User can choose authentication protocol such as PAP, CHAP,MS_CHAP and MS_CHAPv2.
6. **MPPE Encryption Mode:** Click checkbox to enable MPPE Encryption Mode. Please note that MPPE needs to work with MSCHAP authentication method.
7. **Encryption length:** There are three kinds of encryption length, respectively 40 bits, 56 bits, and 128 bits.
8. **User Name:** Input the account of L2TP client.

9. **Password:** Input the password of L2TP password.

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

3.3.9 VPN-PPTP Client

It is different from L2TP.



1. **VPN-PPTP Client:** Click “enable” to enable the function of VPN-PPTP Client.
2. **Name:** The name of tunnel.
3. **Peer IP/Domain:** Input the PPTP Server IP or domain name.
4. **User Name:** The account your ISP assigns to you.
5. **Password:** The password your ISP assigns to you.
6. **Peer Subnet:** Enter the peer subnet.
7. **Connect:** The way of triggering VPN connection. There are three modes to select:
   On-demand: The device will link up with ISP when the clients send outgoing packets.
   Auto (Always-on): The device will link with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

8. **Option:**

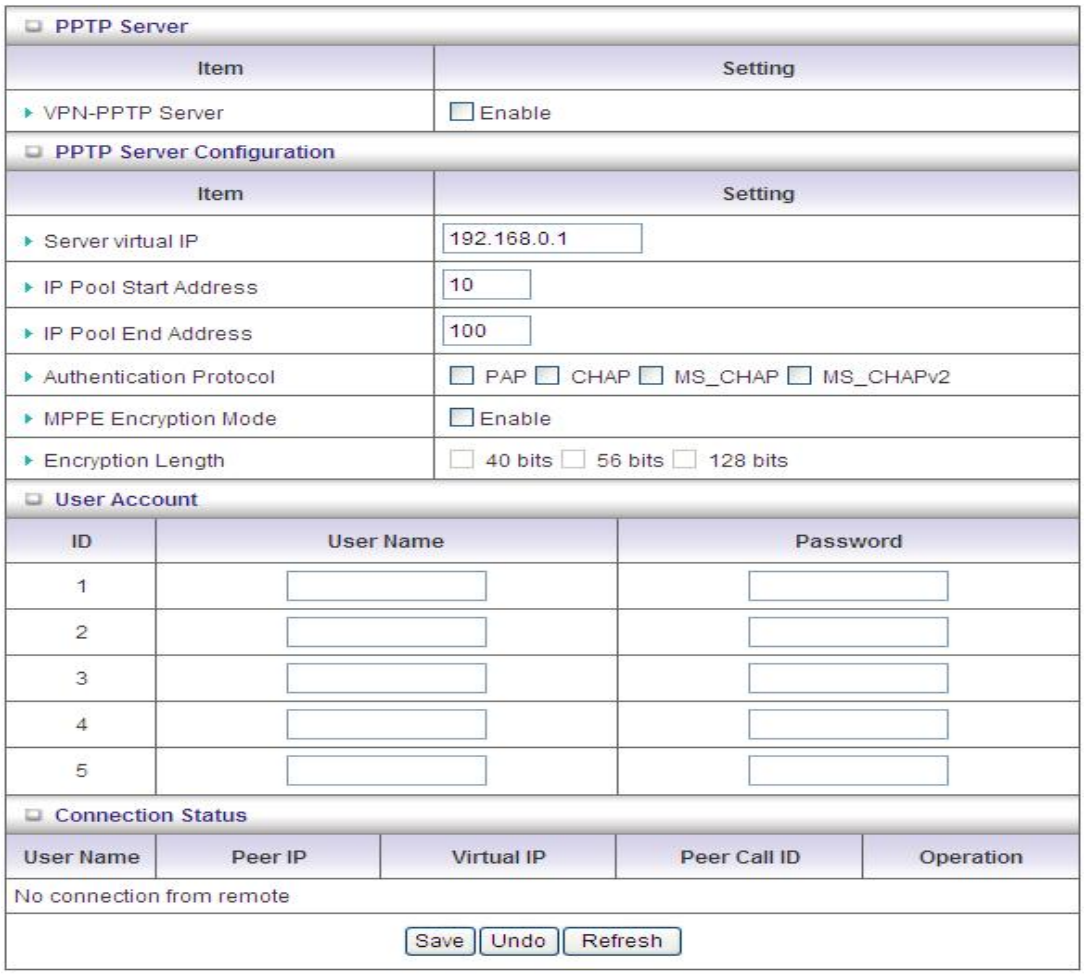
   MPPE: The MPPE encryption supports.

   NAT: The Nat Traversal supports.

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

3.3.10 VPN-PPTP Server

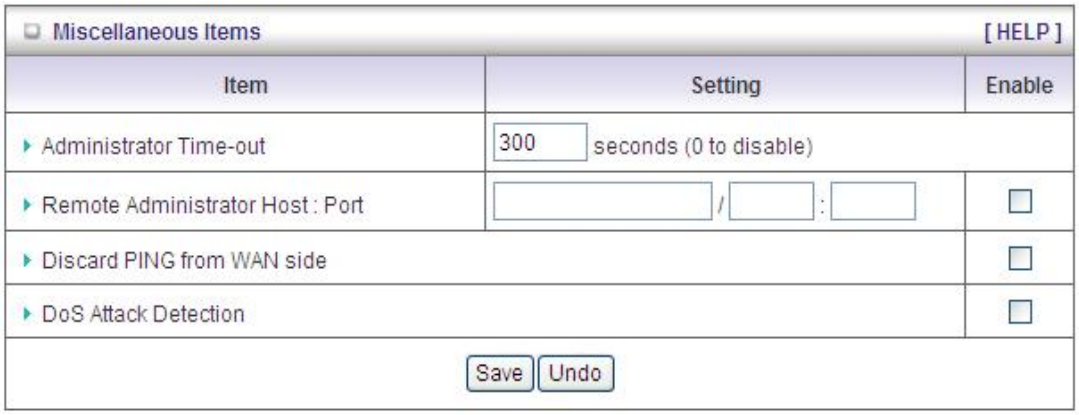
The configuration is the same as L2TP.



1. **VPN-PPTP Server:** Click “enable” to enable the function of VPN-PPTP Server.
2. **IP Pool Start Address:** The start virtual IP Address that sends to the client.
3. **IP Pool End Address:** The end virtual IP Address that sends to the client.
4. **Authentication Protocal:** User can choose authentication protocol such as PAP, CHAP,MS_CHAP and MS_CHAPv2.

5. **MPPE Encryption Mode:** Click ‘’enable” to enable MPPE Encryption Mode. Please note that MPPE needs to work with MSCHAP authentication method.
6. **Encryption length:** There are three kinds of encryption length, respectively 40 bits, 56 bits, and 128 bits.
7. **User Name:** Input the account of PPTP client.
8. **Password:** Input the password of PPTP password.

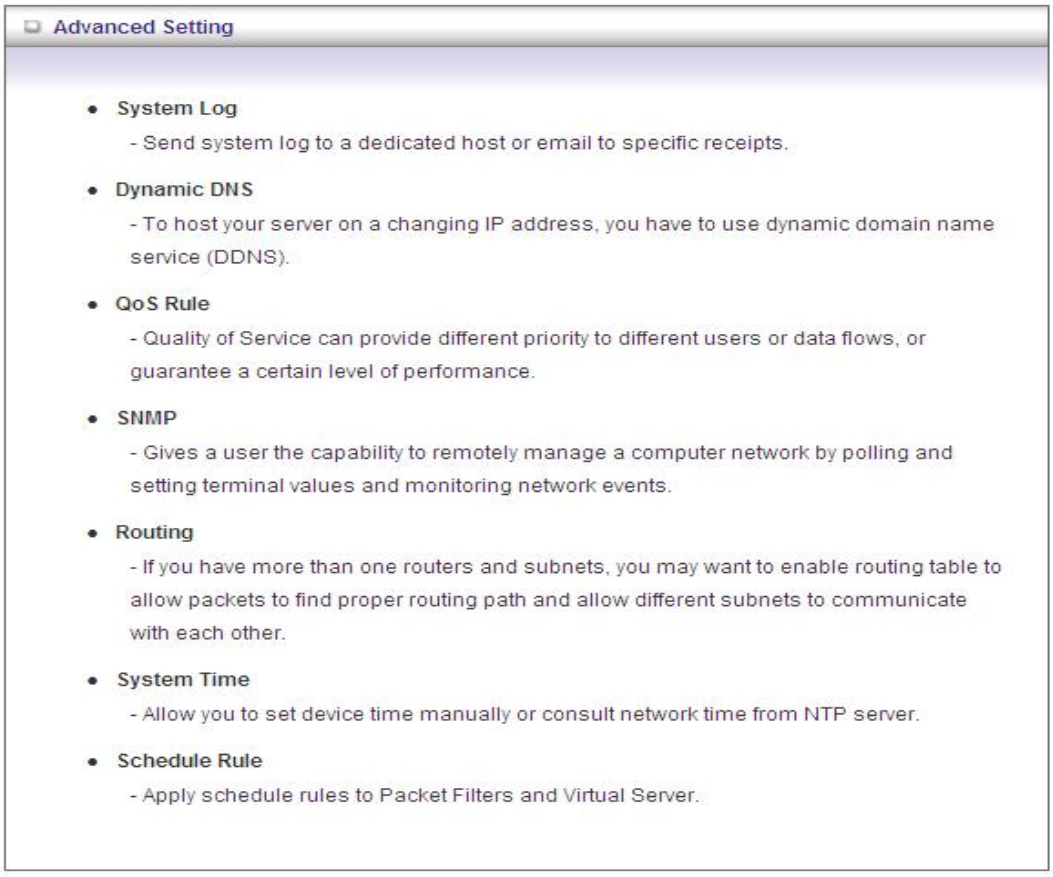
3.3.11 Miscellaneous Items



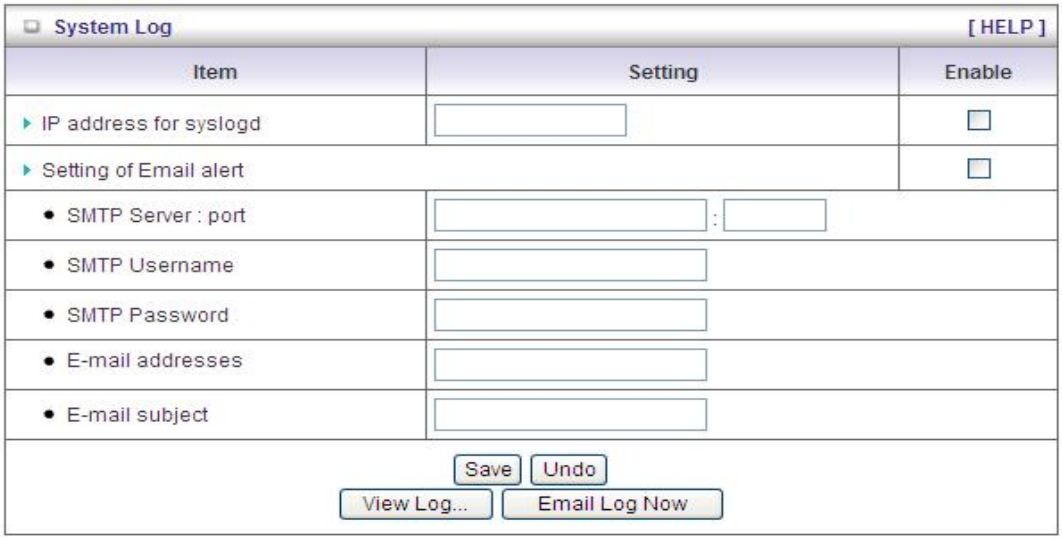
1. **Administrator Time-out**: The time of no activity to logout automatically, you may set it to zero to disable this feature.
2. **Remote Administrator Host/Port**
   In general, only Internet user can browse the built-in web pages to perform administration task. This feature enables you to perform 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 coming from the Internet. Currently, the router can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack etc.

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

3.4 Advanced Setting



3.4.1 System Log



This page supports two methods to export system logs to specific destination by means of

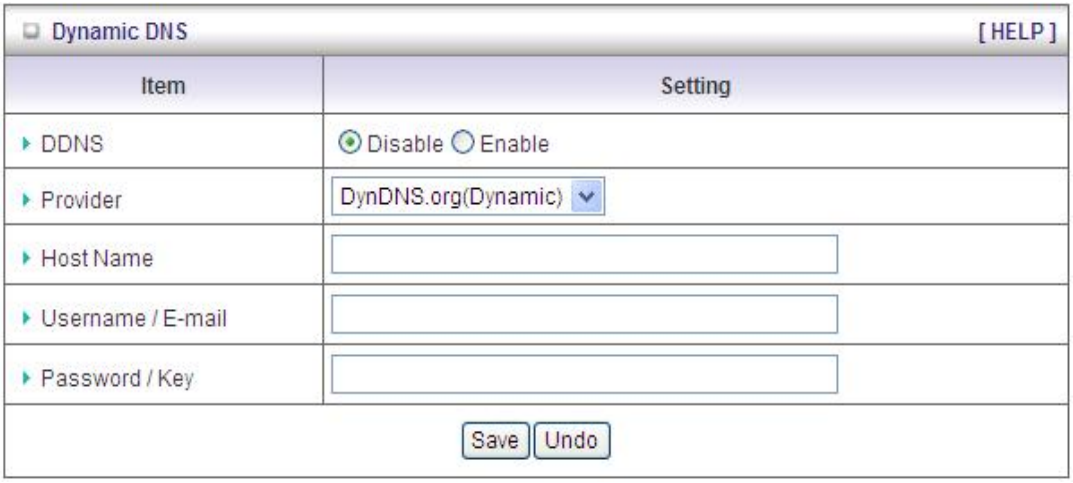
syslog (UDP) and SMTP(TCP). The items you have to setup include:

1. **IP Address for Syslog**: Host IP of destination where syslog will be sent to. Check **Enable** to enable this function.
2. **Setting of Email 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:** Enter the Username offered by your ISP.
5. **SMTP Password: Enter the User name offered by your ISP.**
6. **E-mail Addresses:** The recipients are the ones who will receive these logs. You can assign more than 1 recipient, using ';' or ',' to separate these email addresses.
7. **E-mail Subject**: The subject of email alert is optional.

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

3.4.2 Dynamic DNS

To host your server on a changing IP address, you have to use dynamic domain name service (DDNS). Therefore, anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.
Before you enable **Dynamic DNS**, you need to register an account on one of these Dynamic DNS servers that we list in **Provider** field.



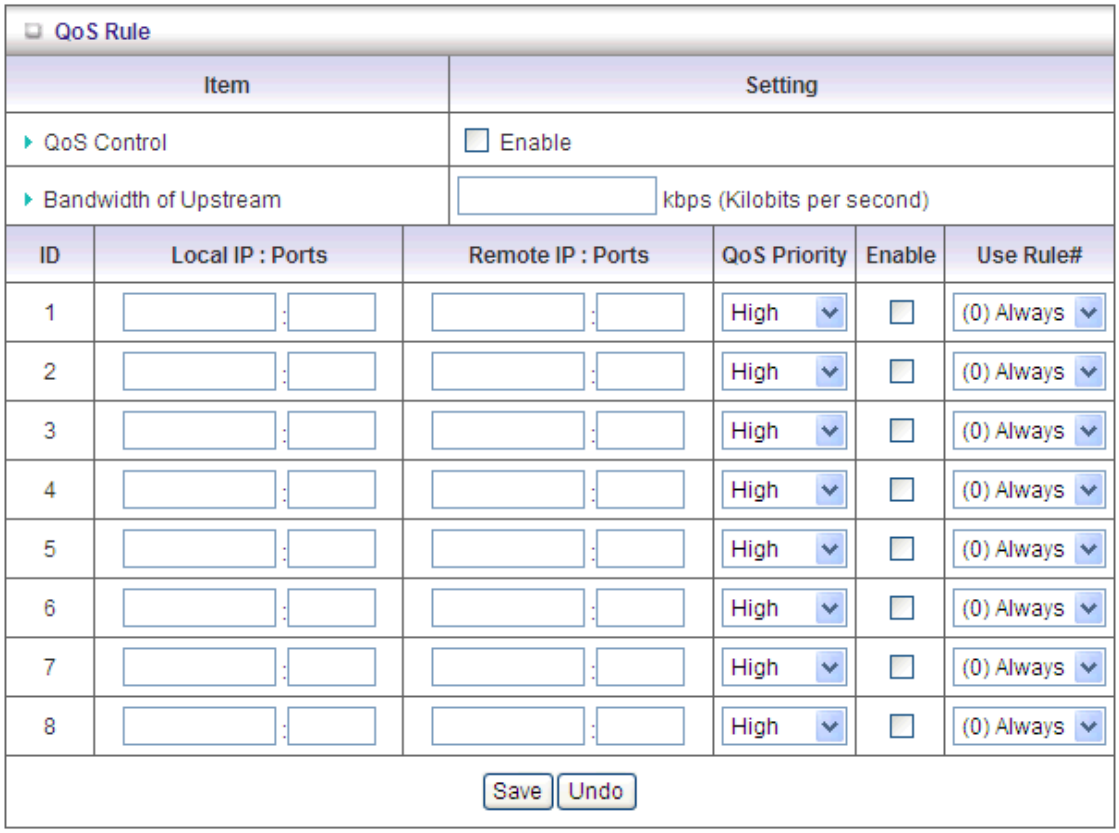
1. **DDNS:** Select enable if you would like to trigger this function.

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

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

3.4.3 QoS

This device supports QoS function. User could set specified upstream connection with different priority. There are three priorities could be selected. The packets with High priority would be processed first.

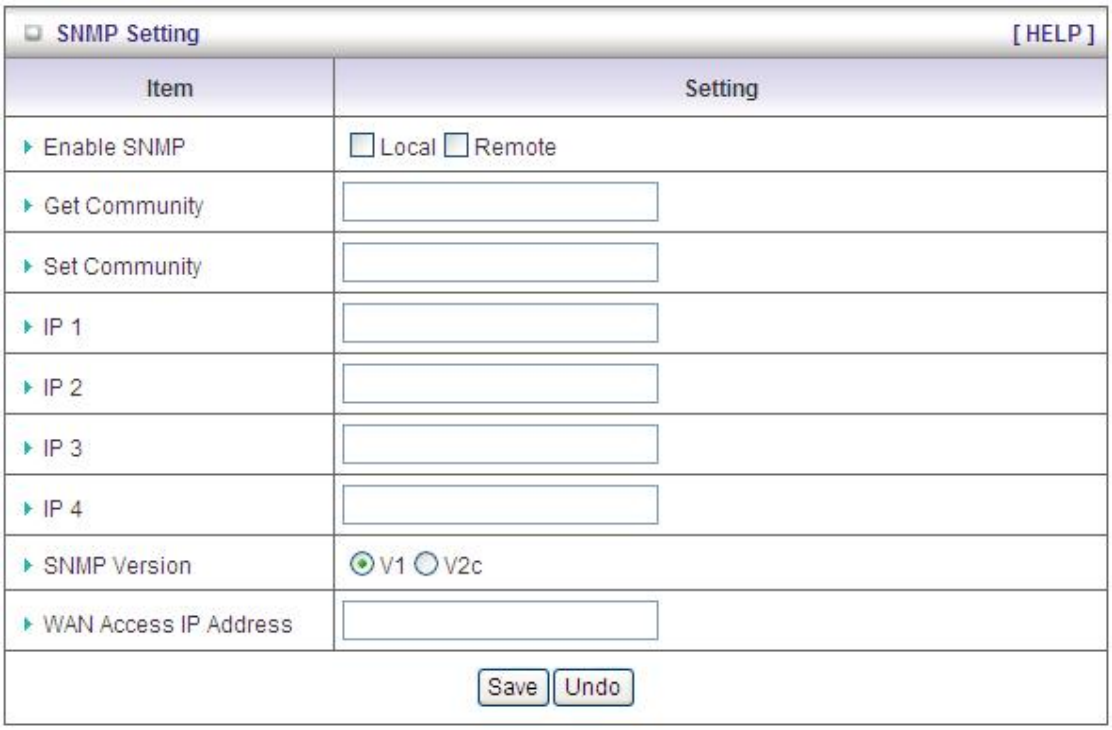


1. **QoS:** Quality of Service.
2. **Local IP/Ports:** The IP and ports that LAN side PC used. The value 0 means don’t care.
3. **Remote IP/Ports:** The IP and ports that Remote Server used. The value 0 means don’t care.

   For example, if you want to guarantee the HTTP bandwidth, you could keep Local IP/Port as 0/0, Remote IP/Port as 0/80.

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.

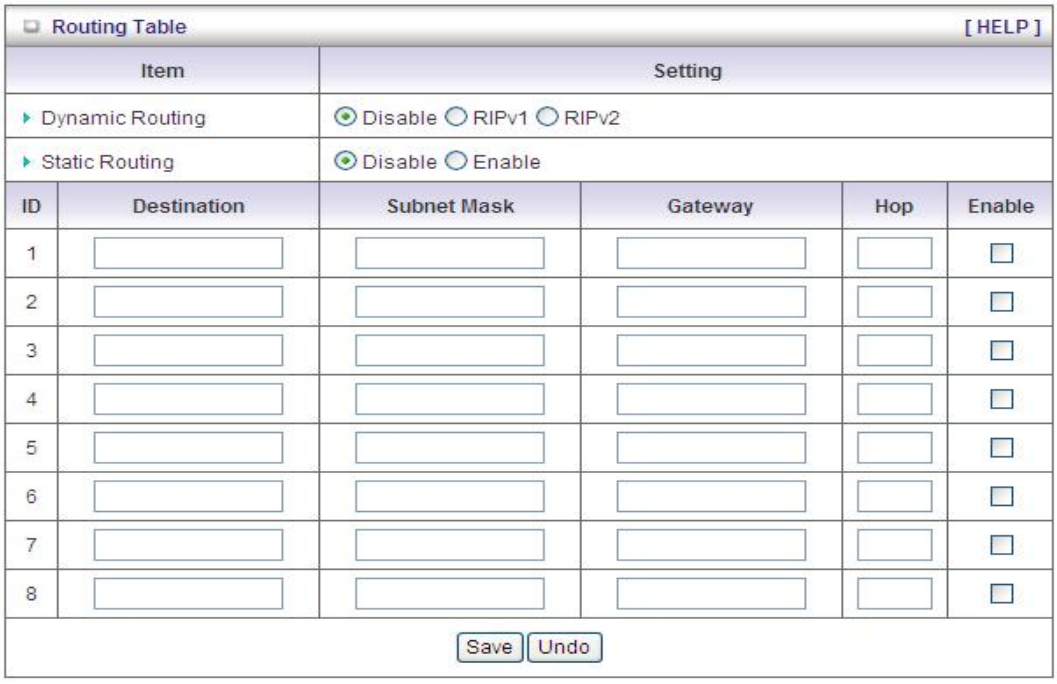


1. **Enable SNMP**: You must check “Local”, “Remote” or both to enable SNMP function. If “Local” is checked, this device will respond request from LAN. If “Remote” is checked, this device will respond request from WAN.
2. **Get Community**: The community of GetRequest is that this device will respond.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

Afterwards, 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 addresses are utilized 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 subnets 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.

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

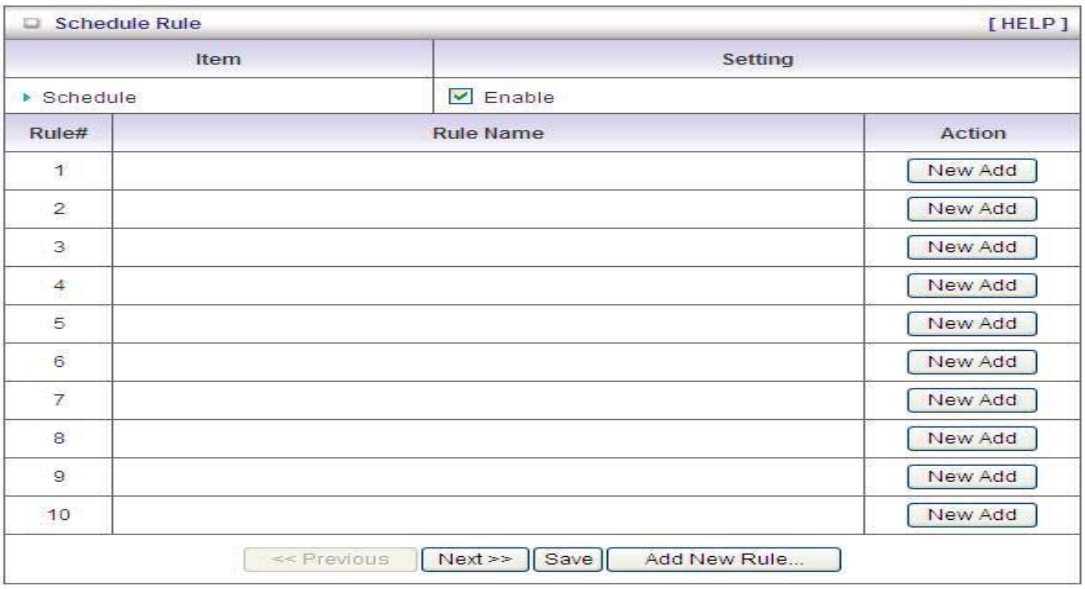
3.4.6 System Time

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 .
4. **Sync with my PC**: Click on the button if you want to set Date and Time using PC’s Date and Time.

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

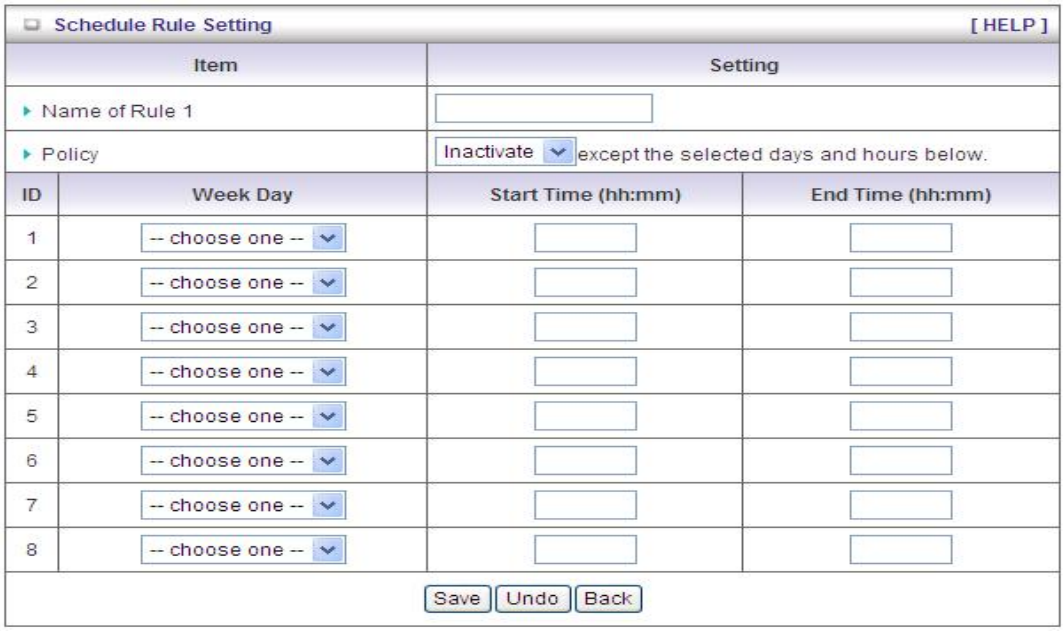
3.4.7 Scheduling

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



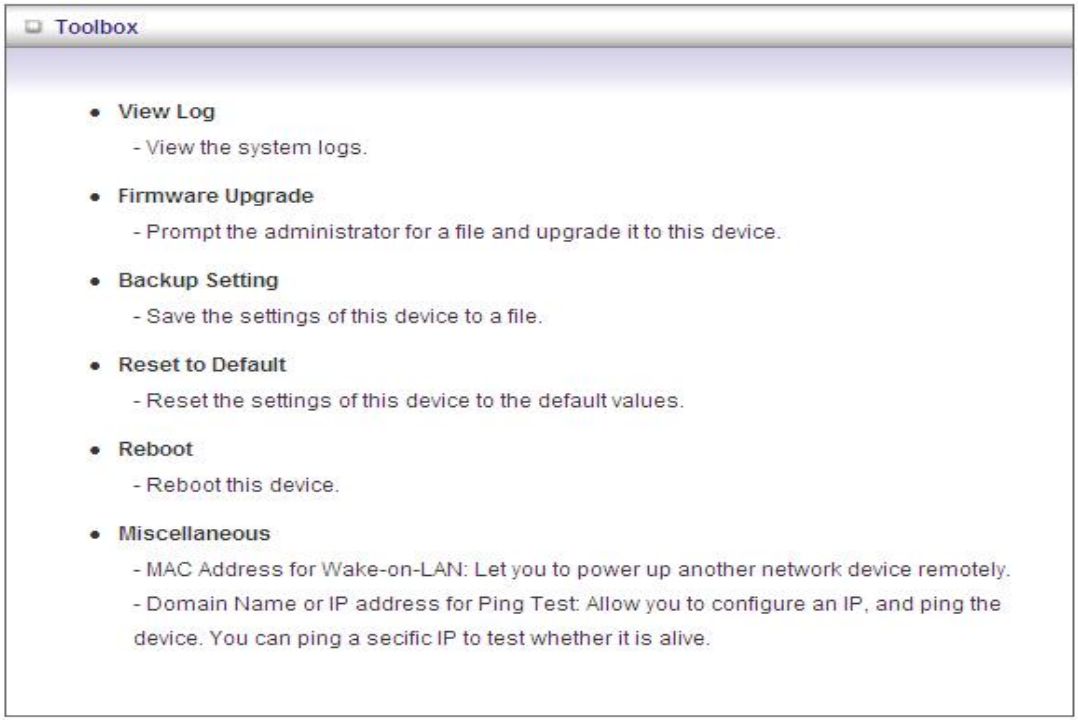
1. **Schedule**: Check to enable the schedule rule settings.

2. **Add New Rule**: To create a schedule rule, click the “New Add” 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 “wake-up time“ everyday from 06:00 to 07:00.

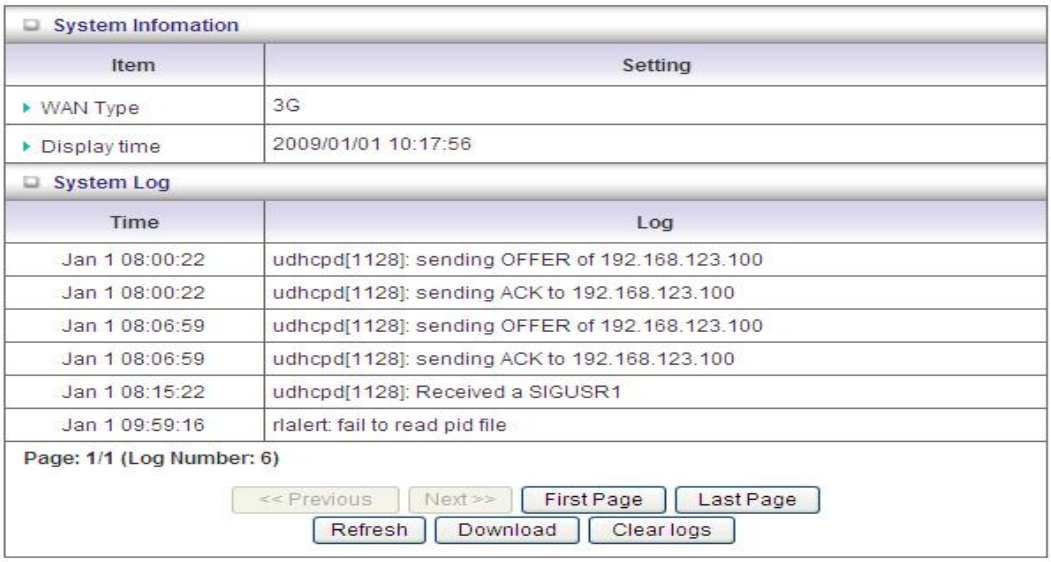


Afterwards, click save” to store your settings or click “Undo” to give up the changes.

3.5 Tool Box

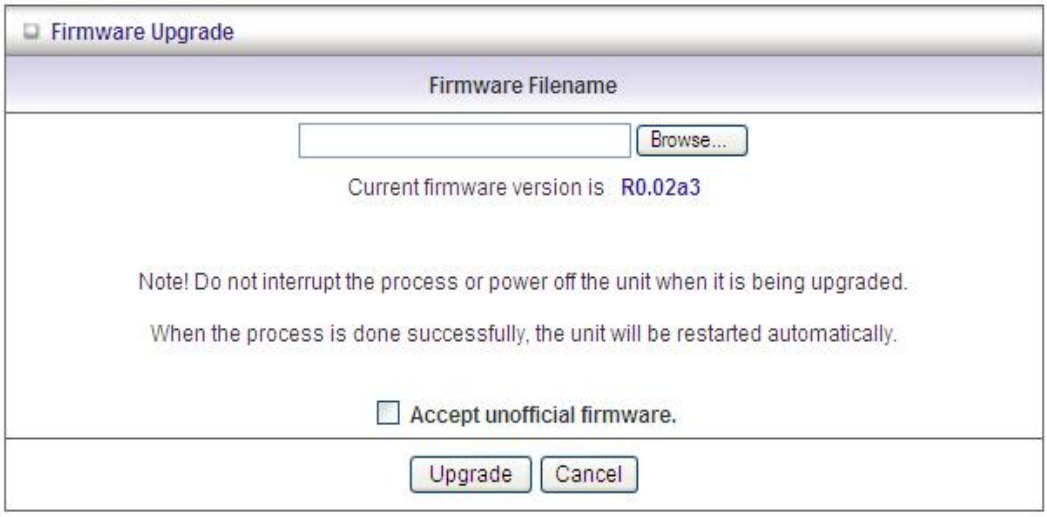


3.5.1 System Info



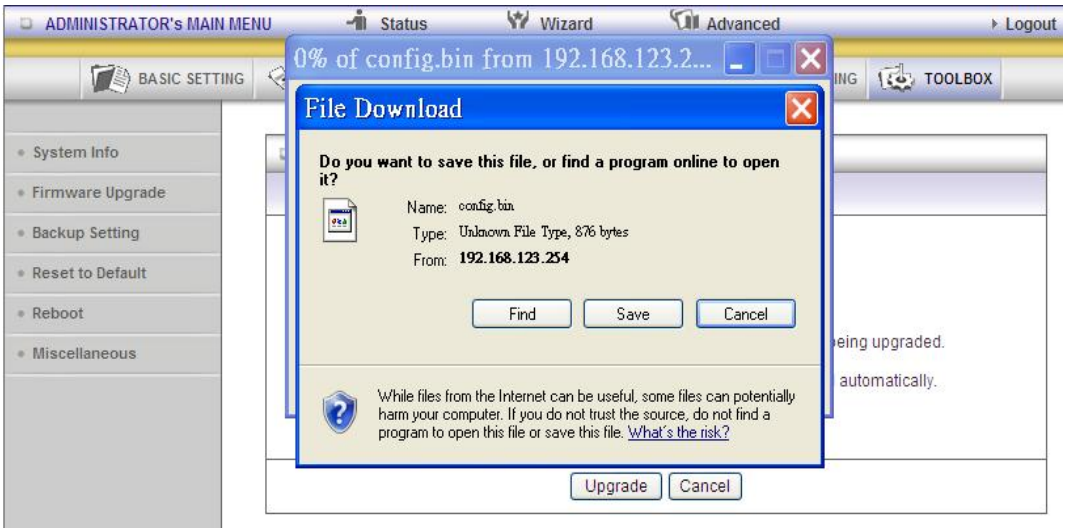
You can view the System Information and System log, and download/clear the System log, in this page.

3.5.2 Firmware Upgrade



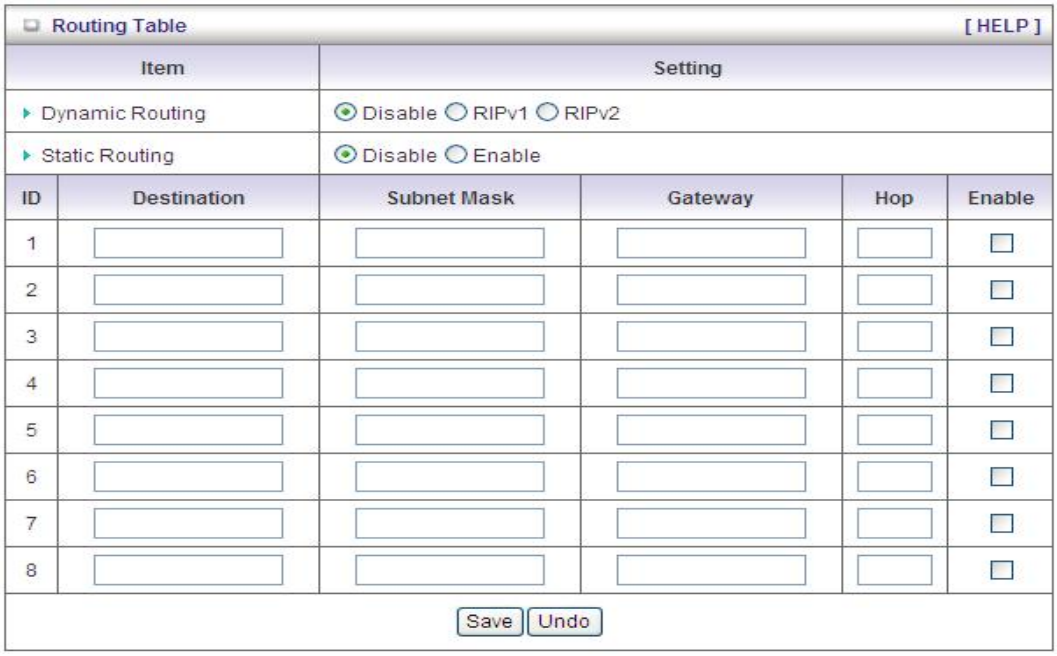
You can upgrade firmware by clicking “Upgrade” button.

3.5.3 Backup Setting



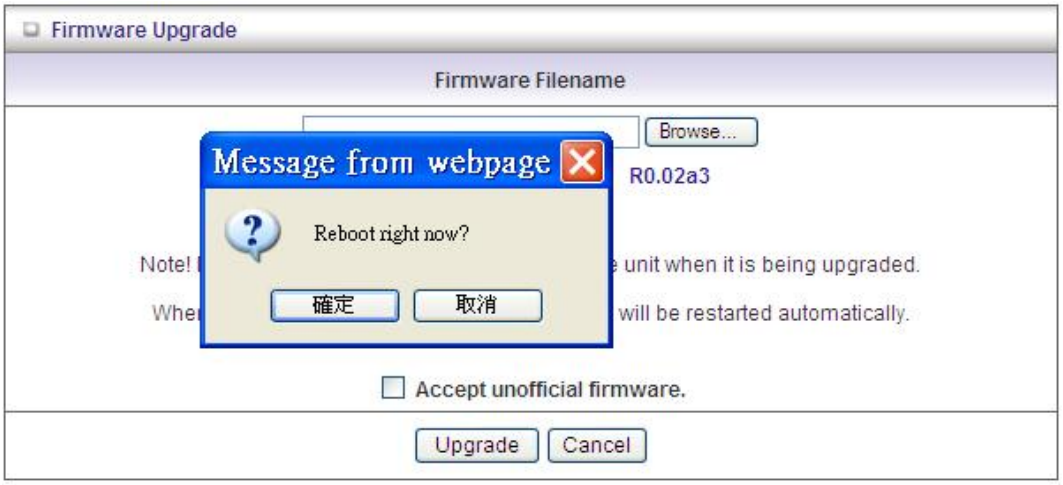
You can backup your settings by clicking the “**Backup Setting”** function item and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you saved.

3.5.4 Reset to Default



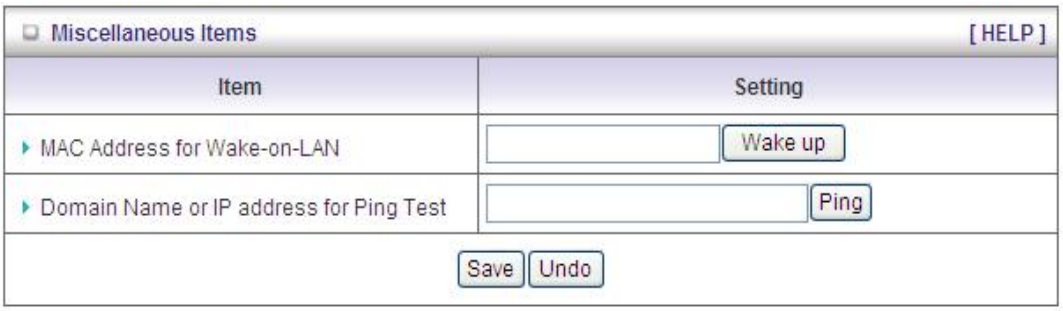
You can also reset this device to factory default settings by clicking the **Reset to default** function item.

3.5.5 Reboot



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

3.5.6 Miscellaneous



1. **MAC Address for Wake-on-LAN:** It enables you to power up a networked device remotely. If you would like to trigger this function, you have to know the MAC address of this device. For instance if the MAC address is 00-11-22-33-44-55, enter it into the blank of MAC Address for Wake-on-LAN. Afterwards. Afterwards, click "Wake up" button which makes the router to send the wake-up frame to the target device immediately.

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.

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

CHAPTER 4. Troubleshooting

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

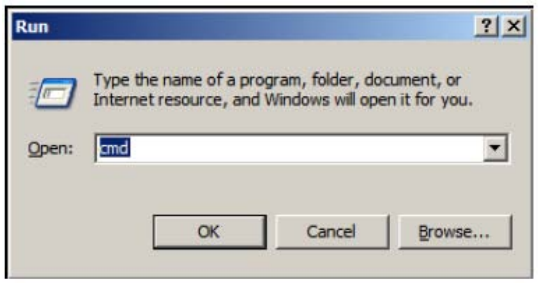
1 Why can't I configure the router even the cable is plugged and the LED is lit?

Do a **Ping test** to make sure that the WiFi Combo VPN 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 VPN 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"**.

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

A. Make sure the RJ45 cable connects 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 provider. Please check your ISP to know this information.

G. Why does my 3G connection 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 VPN 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 VPN Router and the client, then restart it and then turn on the client again.

V. Ensure that the LEDs are indicating normally. If not, make sure that the 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 VPN Router to default setting

C. Why does my wireless connection keep dropping?

I. Antenna Orientation.

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

Appendix A. Spec Summary Table

Device Interface		BDW463AM
Wireless WAN	USB 2.0 for external HSPA modem	1
	ExpressCard-34 for external HSPA modem	1
Ethernet WAN	RJ-45 port, 10/100Mbps, auto-MDI/MDIX	1
RS232 WAN	RJ-45 type RS-232 port for dial-up modem	1
Ethernet LAN	RJ-45 port, 10/100Mbps, auto-MDI/MDIX	4
Printer/Storage Port	USB 2.0 (shared with Wireless WAN) for external Printer / Storage sharing	1
SMA Connector	For 1.8 dBm di-pole antenna	2
WPS+Reset Button	For WPS connection & Restore to factory default.	1
Green Button	Standby & Sleep mode regulating (Option)	1
LED Indication	Power Status / WAN / LAN1 ~ LAN4/ WiFi / USB / ExpressCard / RS232	•
Power Button	For ON/OFF power modes	1
Power Jack	Powered via external DC 12V/2A switching adapter	1
Wireless LAN (WiFi)		
Standard	IEEE 802.11n Draft 2.0 compliance	•
SSID	SSID broadcast or in stealth mode	•
Channel	Auto-selection, manually	•
Security	WEP, WPA, WPA-PSK, WPA2, WPA2-PSK	•
WPS	WPS (Wi-Fi Protected Setup)	•
WDS	WDS (Wireless Distribution System)	•
WMM	WMM (Wi-Fi Multimedia)	•
Functionality		
Wireless WAN	GPRS/EDGE/WCDMA/HSDPA/HSUPA	•
	CDMA2000/EVDO	•
Ethernet WAN	PPPoE, DHCP client, Static IP, PPTP, L2TP	•
WAN Connection	Auto-reconnect, dial-on-demand, manually	•
VPN	IPSec, L2TP, PPTP, with Multiple Encryption	•
QoS, Bandwidth Mgmt.	Smart-QoS Select, WAN&WWAN Bandwidth Priority	•
Others	Application Layer Gateway (ALG) optimization	•
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 and protection	•
Routing Protocol	Static route, dynamic route (RIP v1/v2)	•
Management	SNMP, UPnP IGD, syslog	•
Administration	Web-based UI, remote login, backup/restore setting	•
Environment & Certification		
Package Information	Package dimension (mm)	
	Package weight (g)	
Operation Temp.	Temp.: 0~40°C, Humidity 10%~90% non-condensing	•
Storage Temp.	Temp.: -10~70°C, Humidity: 0~95% non-condensing	•
EMI Certification	CE/FCC compliance	•
RoHS	RoHS compliance	•

*Specifications are subject to change without 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