Air Live®
Powered by OvisLink Corp.

N450R

3T3R Wireless-N Dual Band Gigabit Router

User's Manual

www.airlive.com

Copyright & Disclaimer

OvisLink Corp. has made the best effort to ensure the accuracy of the information in this user's guide. However, we are not liable for the inaccuracies or errors in this guide. Please use with caution. All information is subject to change without notice

This product requires professional installation. Please do not attemp to install the device without the necessary knowledge in regards to your country's wireless regulations.

FCC 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.

Table of Contents

1 Introduction

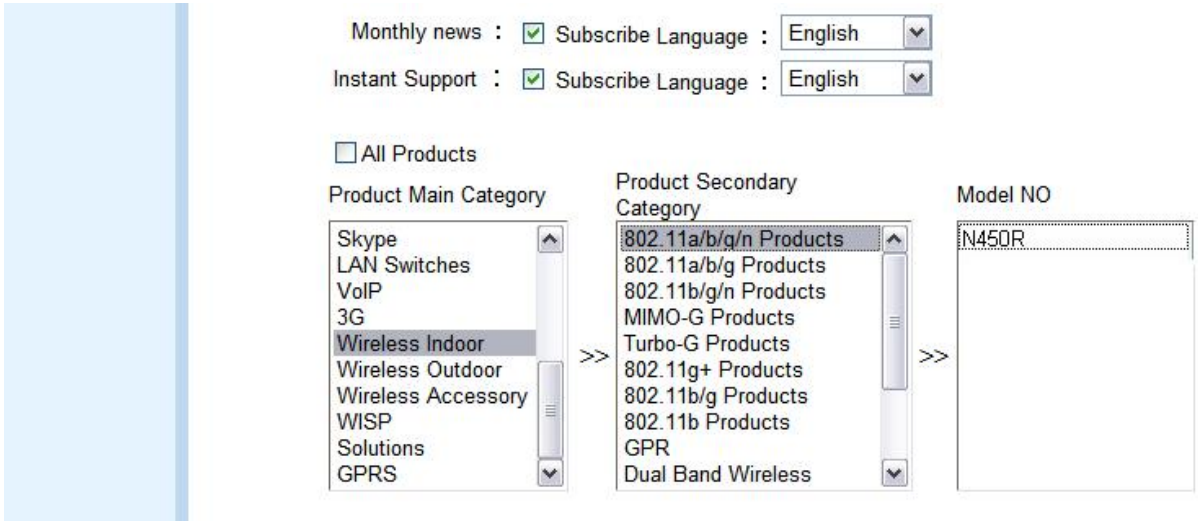
Thank you for purchase of this AirLive product. **AirLive N450R** is a 802.11n concurrent dual band broadband router with USB slots for USB storage and 3G USB modem support. It features Gigabit LAN and WAN ports that can work with 10/100Mbps devices also. In this guide, you will learn how to configure N450R's extensive functions.

1.1 Firmware Upgrade and Tech Support

If you encounter a technical issue that can not be resolved by information on this guide, we recommend that you visit our comprehensive website support at www.airlive.com. The tech support FAQ are frequently updated with latest information.

In addition, you might find new firmwares that either increase software functions or provide bug fixes for N450R. You can reach our on-line support center at the following link: http://www.airlive.com/support/support_2.jsp

Since 2009, AirLive has added the “Newsletter Instant Support System” on our website. AirLive Newsletter subscribers receives instant email notifications when there are new download or tech support FAQ updates for their subscribed airlive models. To become an AirLive newsletter member, please visit: http://www.airlive.com/member/member_3.jsp



1.2 Package List

Items	Description	Contents	Quantity
1	N450R main unit		1
2	Antenna		3
3	Power adapter (12V ,1.5A)		1
4	CD		1
5	Quick Start Guide		1

1.3 Features

- Supports Wireless a/b/g/n Dual Band Standard
- 450Mbps at 5GHz and 300Mbps at 2.4GHz
- 5GHz and 2.4GHz at the same time
- 3T3R Beam Forming radio, smart antenna technology
- Multi-Wall and Multi-Level environment
- 4 x Gigabit LAN and 1 x Gigabit WAN Ports
- Support WAN and 3G Failover or Load Sharing
- 2 x USB 2.0 port for external storage and 3G dongle
- Wireless Encryption: WEP, WPA/WPA2, WPA-PSK/WPA2-PSK
- Support WPS Button
- Supports QoS bandwidth, Web HDD, Internet scheduling
- Supports Smartphone tethering to share 3G bandwidth
- Supports UPnP Media server, iTunes Server
- AirLive IPCAM Plug-and-Play
- IPv6, SNMP, Static Route, RIP
- UPnP, Virtual Sever, ALG, DMZ and SPI Firewall etc
- Supports IPSec, L2TP and PPTP VPN Pass-Through

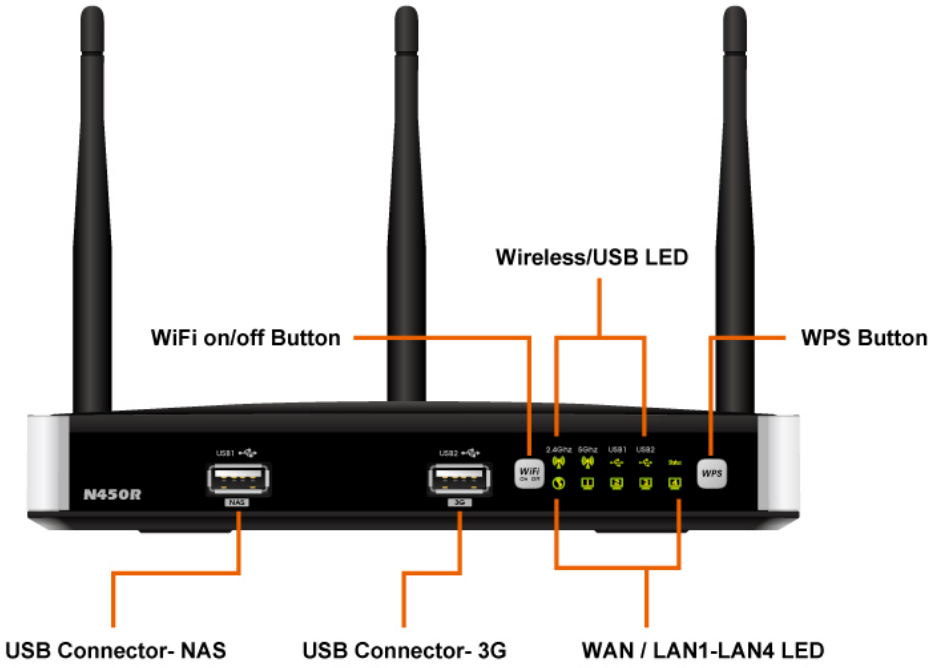
1.4 Specification Table

Device Interface	
Ethernet WAN	RJ-45 port,10/100/1000Mbps, auto-MDI/MDIX
Ethernet LAN	RJ-45 port, 10/100/1000Mbps, auto-MDI/MDIX x 4
USB WAN	USB 2.0 for 3G/3.5G/4G USB dongle
USB Sharing	USB 2.0 for file sharing
Antenna	External antenna x 3
WPS Button	For WPS connection
Wireless On/Off Button	Enable /Disable Wireless Radio
Reset Button	Reset router setting to factory default
LED Indication	Status / 2.4GHz/5GHz/ USB1/USB2/ WAN / LAN1 ~ LAN4
Power	DC 12V/1.5A switching power adapter
Wireless LAN (WiFi)	
Standard	IEEE 802.11n 2.4GHz(2x2) /5GHz (3x3) 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)
WMM	WMM (Wi-Fi Multimedia)
Functionality	
Ethernet WAN	PPPoE, DHCP client, Static IP, PPTP, L2TP
WAN Connection	Auto-reconnect, dial-on-demand, manually
IPv6 support	Dual stack IPv6 support
One-to-Many NAT	Virtual server, special application, DMZ
NAT Session	Support NAT session up to 20,000 sessions
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)
Storage/File Sharing	FAT16/FAT32, EXT2, NTFS (Read only) Samba server, FTP server
Media server	UPnP AV media server, iTunes server
Scheduling Download management	FTP, HTTP , BitTorrent
Management	SNMP, UPnP IGD, syslog, DDNS
Administration	Web-based UI, remote login, backup/restore setting

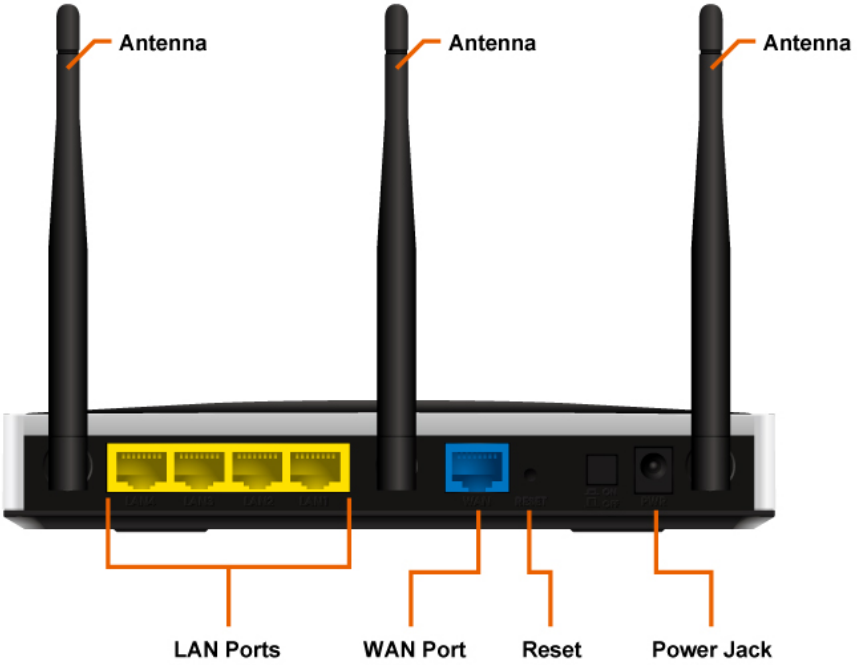
Environment & Certification	
Package Information	Package dimension (mm)
	Package weight (g)
Operation Temp.	Temp.: 0~40oC, Humidity 10%~90% non-condensing
	Temp.: -10~70oC, Humidity: 0~95% non-condensing
EMI Certification	CE/FCC compliance
RoHS	RoHS compliance

1.5 Hardware Installation

1.5.1 Front View



1.5.2 Rear View



1.5.3 LED Indicators

LED	Indicator	Description
Status	Green and flash once per second	This device is working
	Green and Steady On	An error occurred
	OFF	Device is powered off or an error occurred
Ethernet WAN	Green and Steady On	Ethernet WAN connection is established
	Green and Blinking	Data packet transferred via Ethernet WAN
Ethernet LAN 1~4	Green and Steady On	Ethernet LAN connection is established
	Green and Blinking	Data packet transferred via Ethernet LAN
2.4GHz	Green and Blinking	Data packet transferred via 2.4G WiFi
	Green and Fast Blinking	In WPS PBC mode
	OFF	2.4GHz wireless radio is disabled

5GHz	Green and Blinking	Data packet transferred via 5G WiFi
	Green and Fast Blinking	In WPS PBC mode
	OFF	5GHz wireless radio is disabled
NAS	Green and Steady On	An external USB storage is attached
	Green and Blinking	Data packet transferred via attached USB storage device (e.g. USB drive)
	OFF	No USB storage is attached
3G	Green and Steady On	3G connection is established
	Green and Blinking	Data packet transferred via 3G WAN
	OFF	3G connection is not established

1.5.4 Button Definition

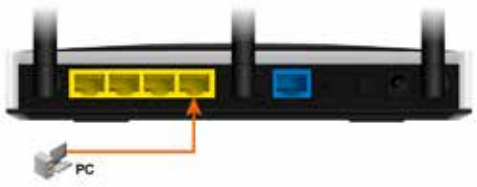
Button	Description
WPS	Continually press 3 seconds to enter WPS PBC mode for 2.4G wireless
	Continually press 8 seconds to enter WPS PBC mode for 5G wireless
WiFi on/off	Continually press 3 seconds to switch on/off for 2.4G wireless radio
	Continually press 8 seconds to switch on/off for 5G wireless radio
Reset	Continually press 6 seconds to reset device settings to factory default
Power	Push down the button to turn on the power

1.5.5 How to Operate

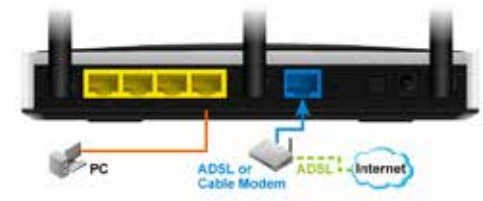
DO NOT connect the router to power before performing the installation steps below.

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

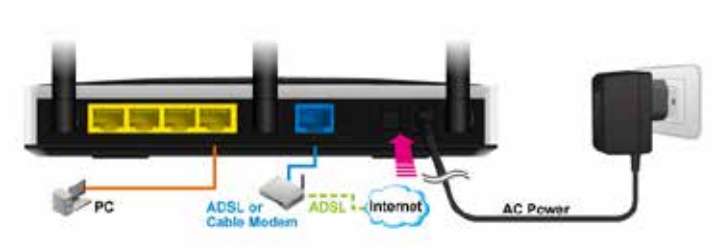
Step 2: Plug the RJ45 cable into LAN port 1~4 and connect with your PC or NB.



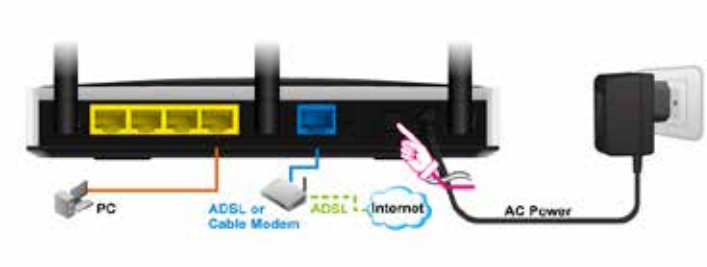
Step 3: Plug your RJ-45 into the WAN port and connect with your xDSL modem.



Step 4: Plug the power jack into it.



Step 5: Power ON.



Step 6: Prepare a USB Storage and then plug into the USB port.

1.6 Wireless Operation Modes

1.6.1 AP Router (Default Setting)

In this mode, you can share your 3G Internet connection and/or broadband connection. If you do not have a 3G USB dongle, you can still share your ADSL modem, xDSL mdoem, or Cable Modem connections. If you have both 3G and Broadband, you can use both for connection backup.

1.6.2 AP Only

When operating in the Access Point mode, the N450R becomes the center hub of the wireless network. All wireless cards and clients connect and communicate through N450R. This type of network is known as "**Infrastructure Network**". Other N450R can connect to AP mode through "**Adapter Mode**".

1.6.3 WDS Repeater

In WDS Repeater mode, the N450R functions as a repeater that extends the range of remote wireless LAN. In this mode, the remote Access Point must have WDS (Wireless Distribution System) capability. If you require the PC's MAC addresses to be preserved when the data pass through the Repeater, it is necessary to use the WDS Repeater mode. Because the radio is divided into WDS + AP mode, the Repeater mode will have less performance and distance.

1.6.4 WDS Only

This mode is also known as “WDS Pure MAC Bridge mode”. When configured to operate in the Wireless Distribution System (WDS) Mode, the N450R provides bridging functions with remote LAN networks in the WDS system. Each bridge can only associate with maximum of 4 other bridges in the WDS configuration. This mode is best used when you want to connect LAN networks together wirelessly. This mode usually delivers faster performance than infrastructure mode.

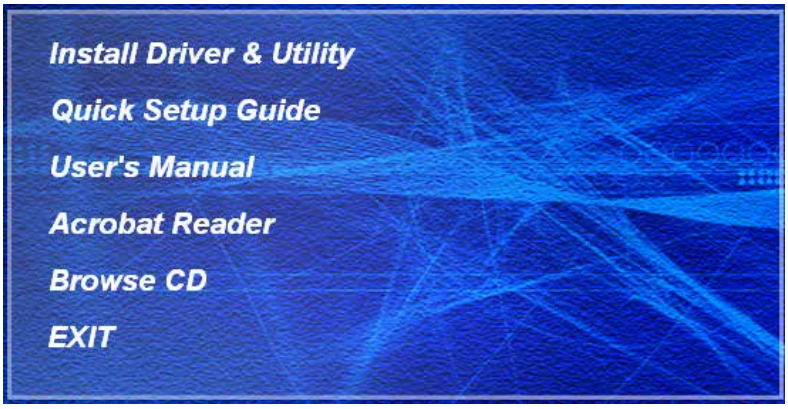
1.6.5 Adapter Mode

This mode is also known as “**Client**” mode. N450r acts as if it is a wireless adapter to connect with a remote Access Point. Users can attach a computer or a router to the LAN port of N450R to get network access. This mode is often used by WISP on the subscriber’s side.

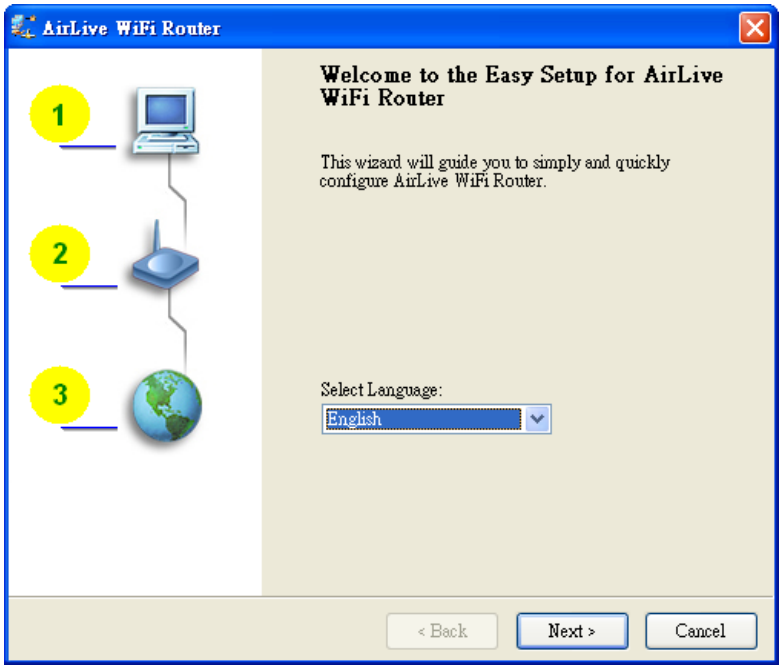
2 Getting Start

2.1 Easy Setup by Windows Utility

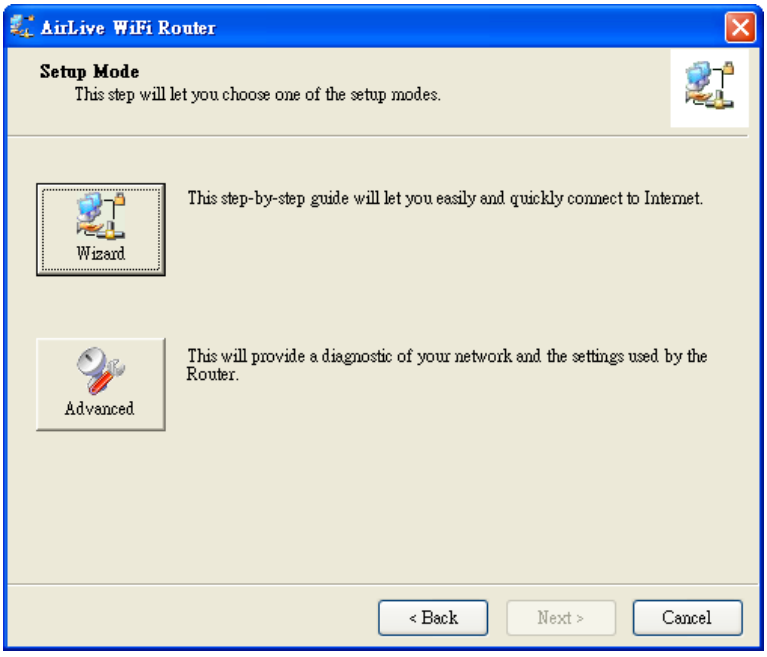
Step 1
Install the Easy Setup Utility from the provided CD. Click the “Install Driver & Utility” and then follow the steps to configure the device.



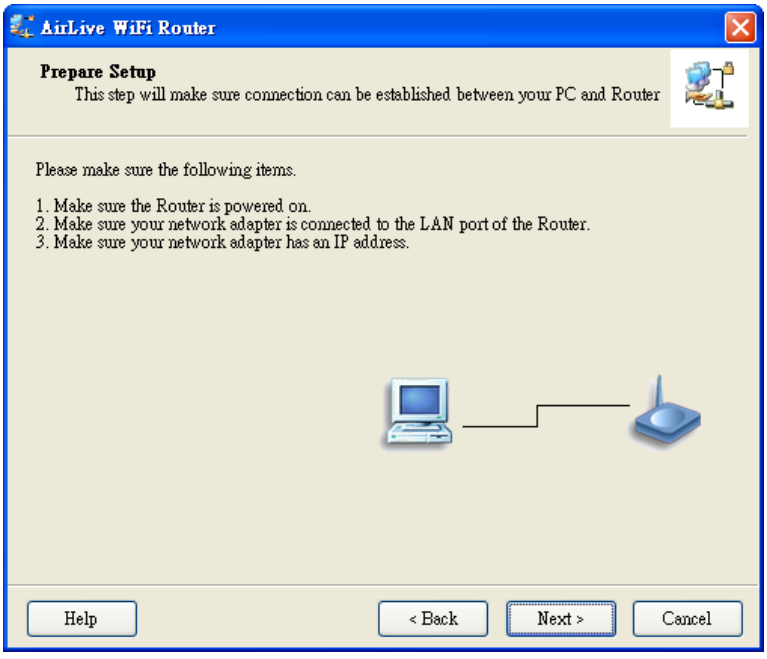
Step 2
Select Language then click “**Next**” to continue.



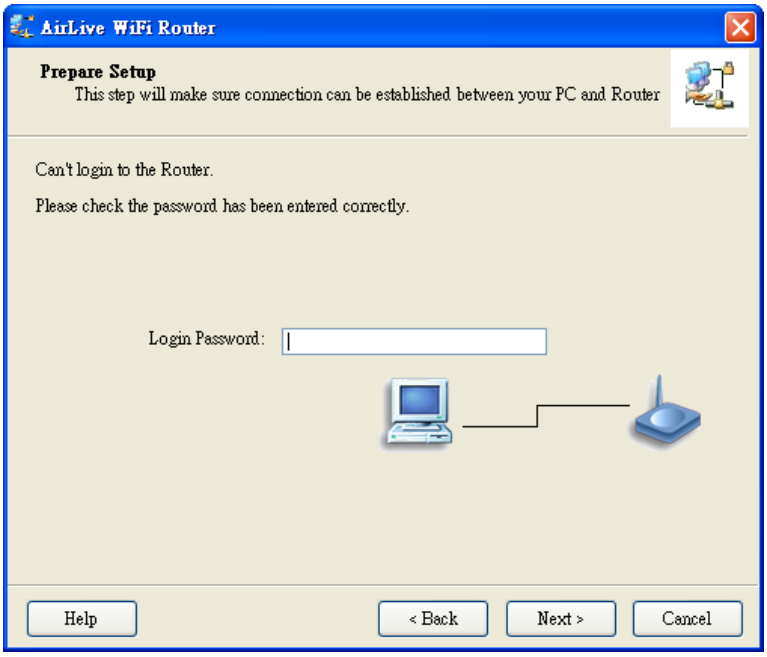
Step 3
Then, click the "**Wizard**" to continue.



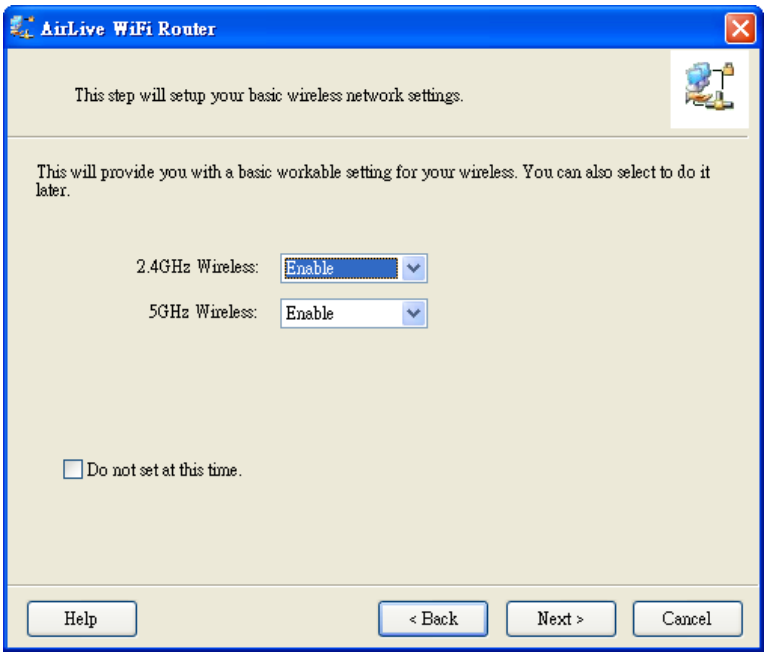
Step 4
Click "**Next**" to continue.



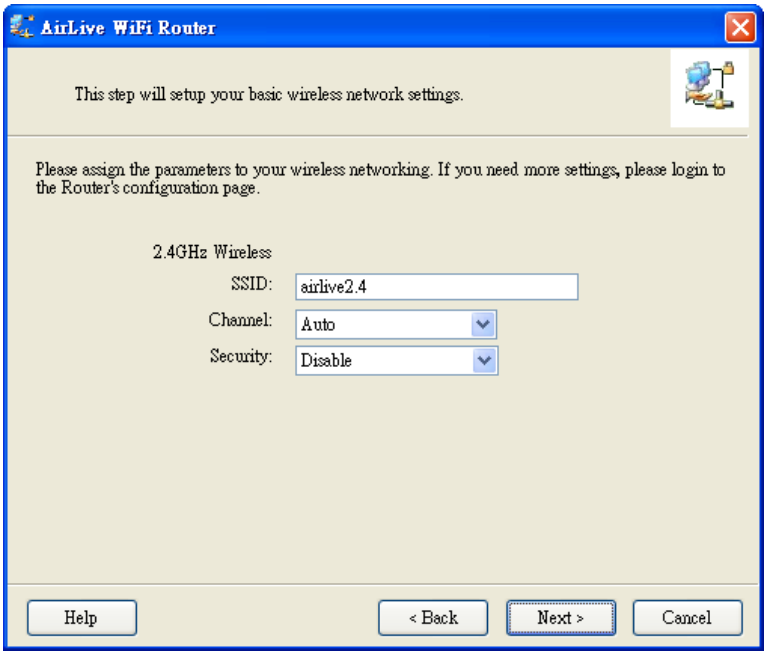
Step 5
Type-in password and then click “Next”. Default password is airlive.



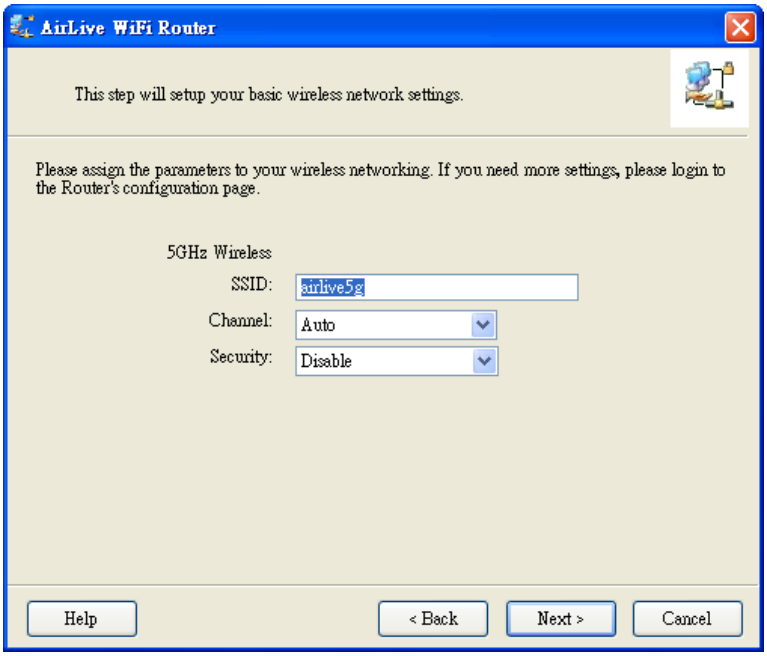
Step 6
Configure the wireless interface and then click “Next”.



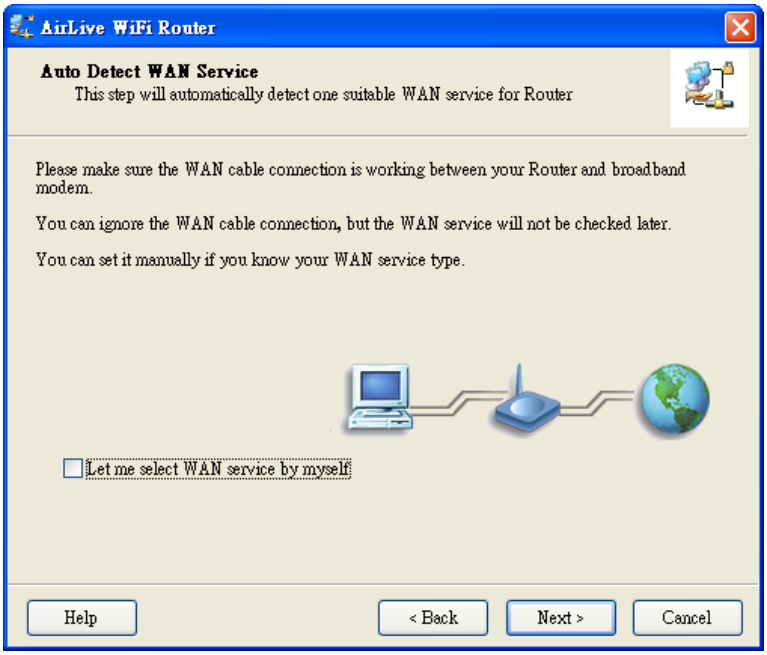
Step 7
Configure 2.4GHz wireless interface **SSID**, **Channel** and **Security**, and then click "**Next**".



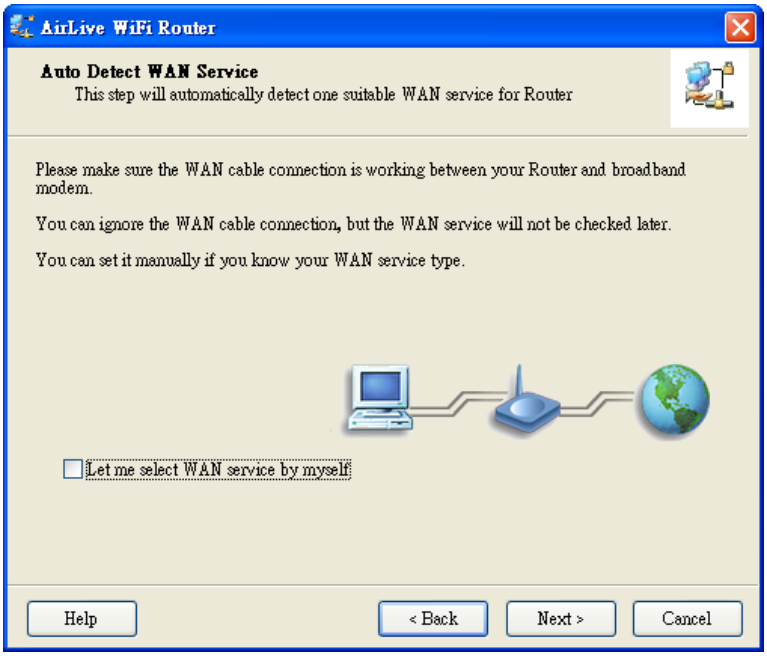
Step 8
Configure 5GHz wireless interface **SSID**, **Channel** and **Security**, and then click "**Next**"



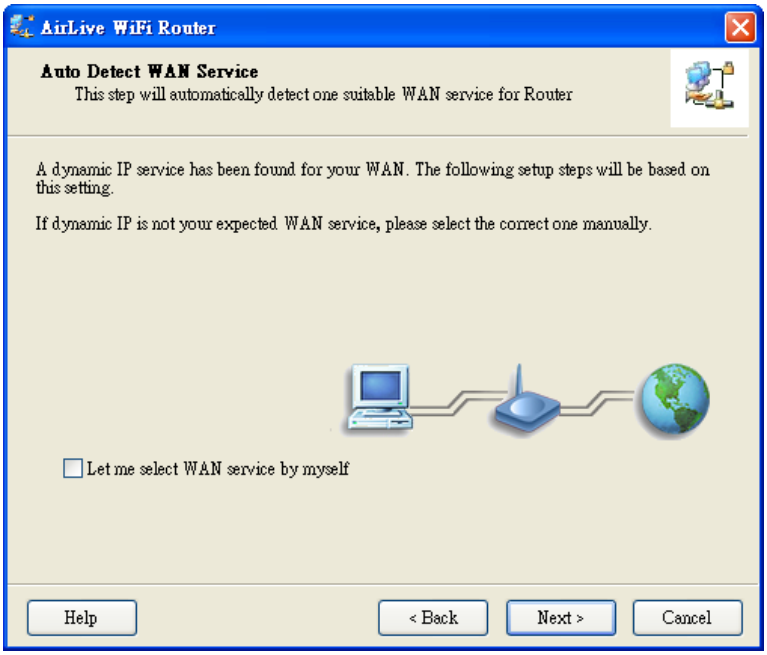
Step 9
Click **Next**.



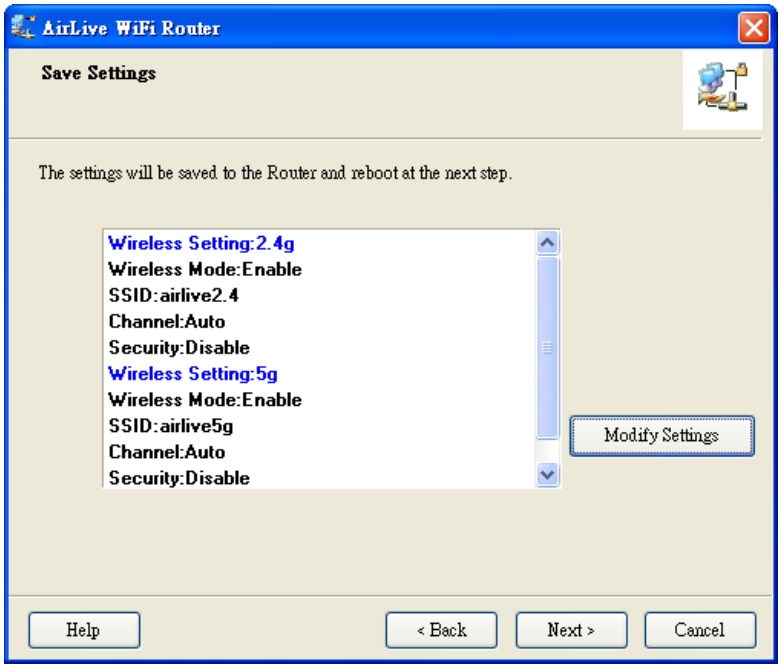
Step 10
Click “Next” to detect the WAN automatically.



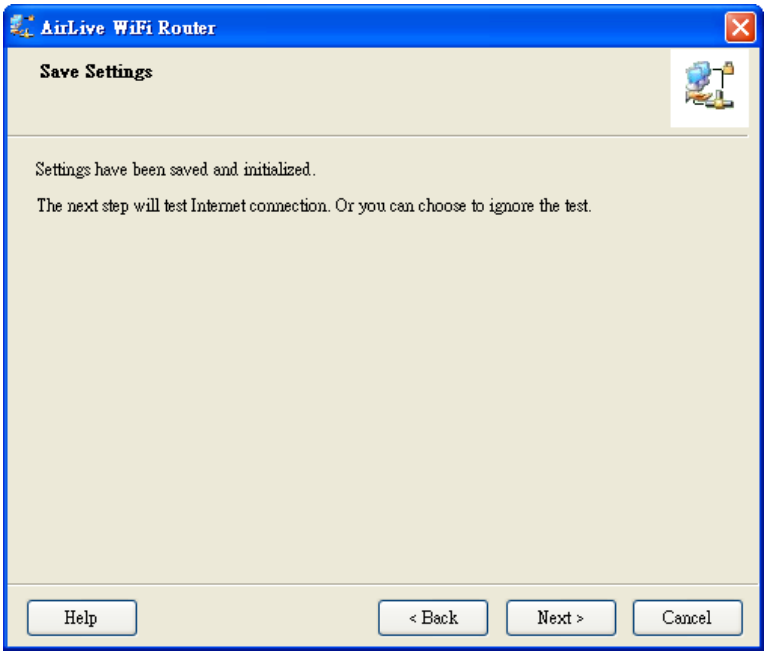
Step 11
Click “Next”.



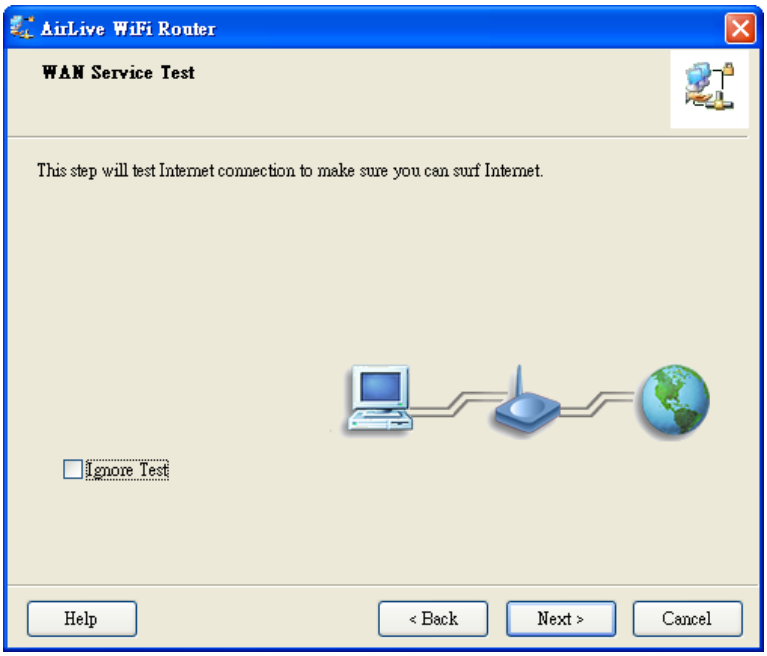
Step 12
Click “Next”.



Step 13
Click “Next”.

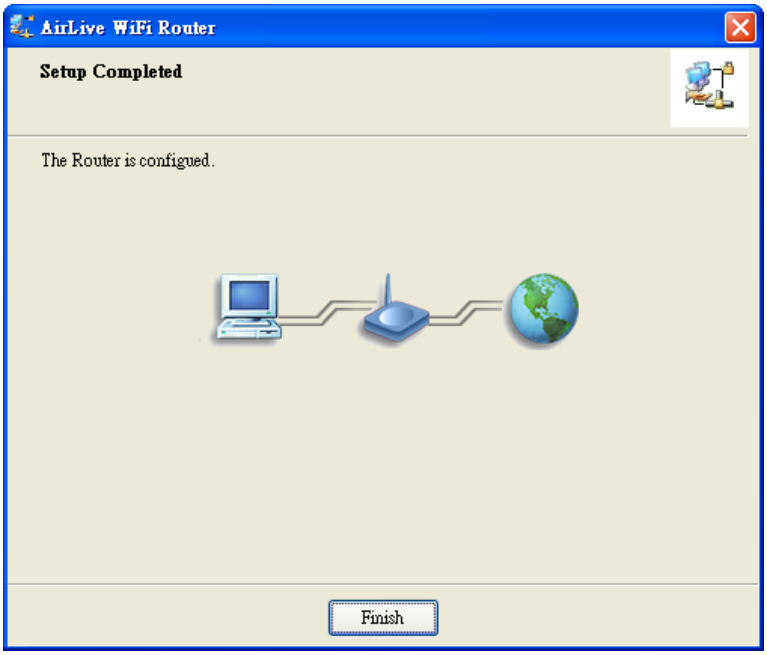


Step 14
Click “Next” to test the internet connection.



Step 15

You have completed the configuration. Click “Finish” and you can surf on the internet now.

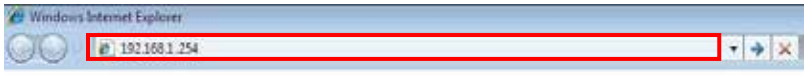


2.2 Easy Setup by Configuring Web UI

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

2.2.1 Browse to Activate the Setup Wizard

n Type in the IP Address (http://192.168.1.254)



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

n Select “Wizard” and then “Enter” for basic settings in simple way.

n Press “Next” to start the Setup Wizard.

2.3 Configure with Setup Wizard

Step 1: Setup Login Password
You can change the admin password here, clicks "**Next**" to continue.

Step 2: Setup Time Zone
Select **Time Zone**, clicks "**Next**" to continue.

Step 3: Select WAN Type
Choose "**Auto Detecting**" or "**Manually**" Setup WAN Type.

Step 4: Select WAN Type
If you want to use 3G service as the main Internet access, please set the WAN interface as **Wireless WAN** and the WAN type as "**3G**", and then click **Next** to continue.

Step 5: For 3G Mode
Select **Auto-Detection**, and then click **Next** to continue.

Step6: Wireless Settings
Set up your Wireless Network, select which wireless band you want to configure.
(e.g. Wireless 2.4G)

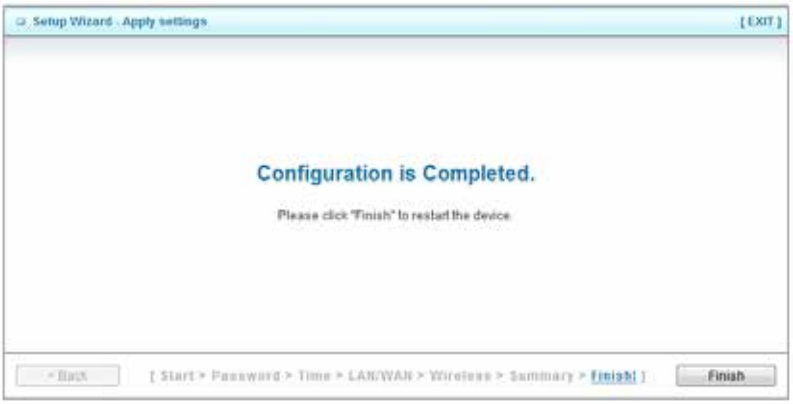
Step 7: Wireless 2.4G Settings
Setup your **SSID** and **Wireless Channel**.

Step 8
Setup **Wireless Authentication** and **Encryption**, then click **Next** to continue.

Step 9
Apply your Setting.
Clicks **Apply Setting** if finished, or click **Back** to previous settings.

Step 10
Check the information again, click "**Apply Setting**" to finish all settings or "**Back**" to the previous settings.

Step 11
Click "**Finish**" to complete it.



3 Configuration

3.1 Login Web UI

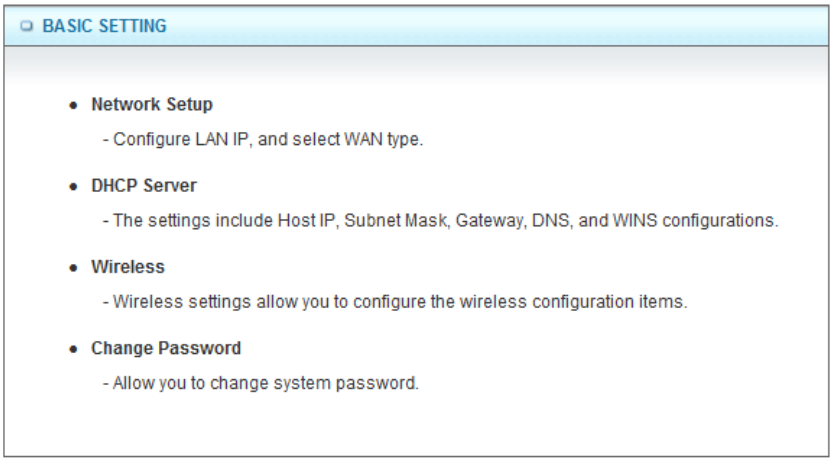
Whenever you want to configure your network or this device, you can access the Configuration Menu by opening the web-browser and typing in the IP Address of the device. The default IP Address is: **192.168.1.254**.

Enter the default password "**airlive**" in the System Password and then click '**login'** button.

Then, you can browse the "**Advanced**" configuration pages for configuring this device.

3.2 Basic Setting

There are four options: **Network Setup**, **DHCP Server**, **Wireless** and **Change Password**.



3.2.1 Network Setup

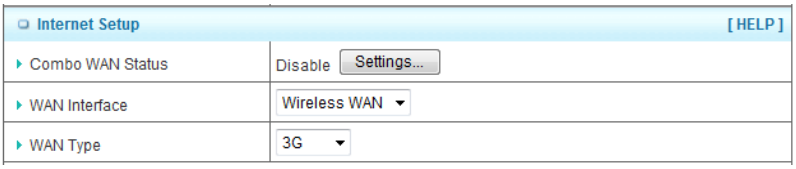
There are two ways to configure the network, respectively **LAN Setup** and **Internet setup**.

n **LAN Setup**

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

2. **Subnet Mask**
   Input your Subnet mask. (All devices in the network must have the same subnet mask.) The default subnet mask is **255.255.255.0**.

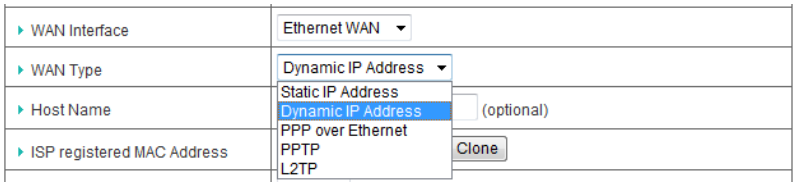
n **Internet Setup**



1. **Combo WAN Status**
   Display status of combo WANS. With Combo WAN feature, you can choose one primary WAN connection, and set another WAN connection for backup. Otherwise, you can also choose "**Load Sharing**" to use Ethernet WAN and 3G WAN simultaneously. The combo WAN status will be showed here. Press "**Settings**" button to configure this feature.

2. **WAN Interface**
   Select **Ethernet WAN** or **Wireless WAN t**o continue.

n **Ethernet WAN**



n Wireless WAN

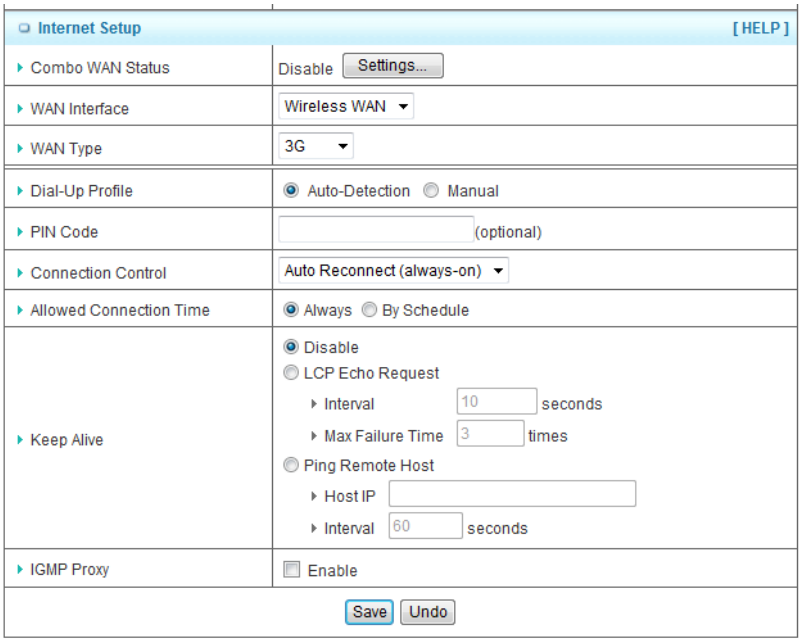
1. **WAN Type**
   WAN type of your Internet connection, select **3G** and **iBurst**. You can choose a correct one from the following options.

(A) 3G

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

*For 3G/Smarphone Tethering compatibility list, please visit the N450R product page on www.airlive.com.

NOTE: You need to insert USB modem card for 3G WAN connections.



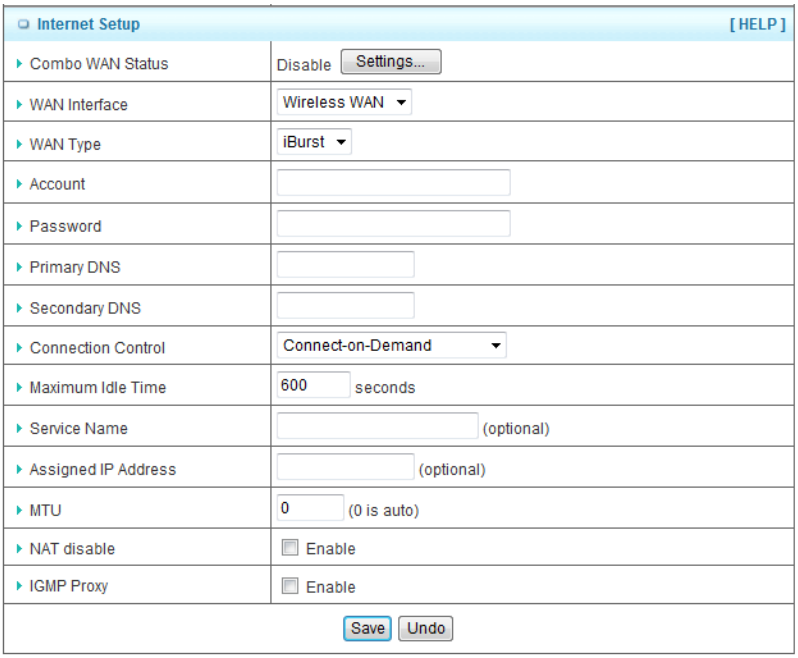
1. **WAN Type**
   Choose 3G for WAN connection.
2. **Dial-Up Profile**
   Please select Auto-Detection or Manual. You can choose "**Auto-Detection**", and the router will try to detect and configure the required 3G service settings automatically. Otherwise, you can select "**Manual**", and manually fill in the required 3G service settings provided by your carrier or ISP.

3. **Connection Control**
   There are 3 options to start connection:
   - **Auto Reconnect (Always-on)**
     The device will always try to link to Internet.
   - **Connect-on-demand**
     The device won't try to connect to Internet until LAN PCs or devices try to go to Internet. Once Internet connection is established, this device will drop the connection if maximum idle time is reached.
   - **Manually**
     The device won't try to connect to Internet until users press "connect" button at Status page. Once Internet connection is established, this device will drop the connection if maximum idle time is reached.
4. **Allowed Connection Time**
   You can limit WAN connection in a period of time if required.
5. **Keep Alive**
   There are three options for keep alive feature as below.
   - **Disable**
     Disable keep alive feature.
   - **LCP Echo Request**
     The device will constantly send LCP packets for keeping alive. Enter the time interval and the maximum failure count.
   - **Ping Remote Host**
     Enter the Remote host IP address and the time interval to send the ping packets for keeping alive.
6. **NAT Disable**
   You can disable NAT feature if required.
7. **IGMP Proxy**
   Enable this feature allows multicast stream (e.g. IPTV stream) to pass-through this device.

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

(B) iBurst

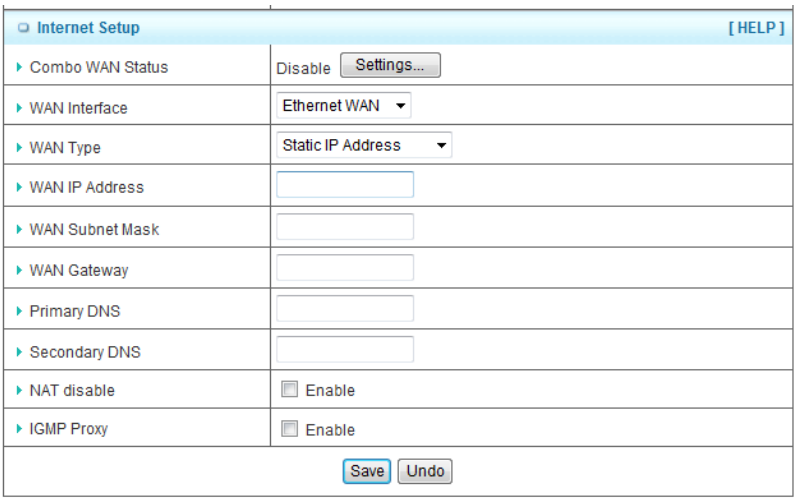
NOTE: You need to insert USB modem card for iBurst WAN connections.



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

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

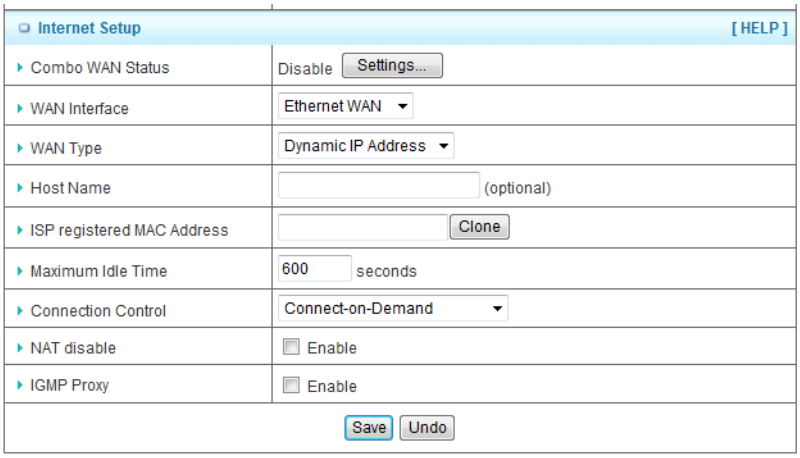
(C) Static IP Address



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

7. **NAT disable**
   You can disable NAT feature if required.
8. **IGMP Proxy**
   Enable this feature allows multicast stream (e.g. IPTV stream) to pass-through this device.

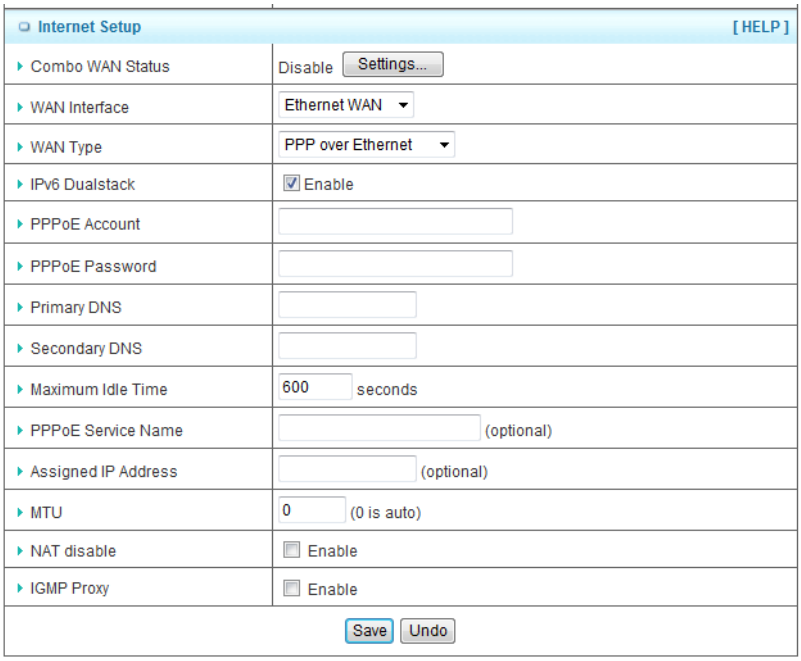
(D) Dynamic IP Address



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

6. **NAT disable**
   You can disable NAT feature if required.
7. **IGMP Proxy**
   Enable this feature allows multicast stream (e.g. IPTV stream) to pass-through this device.

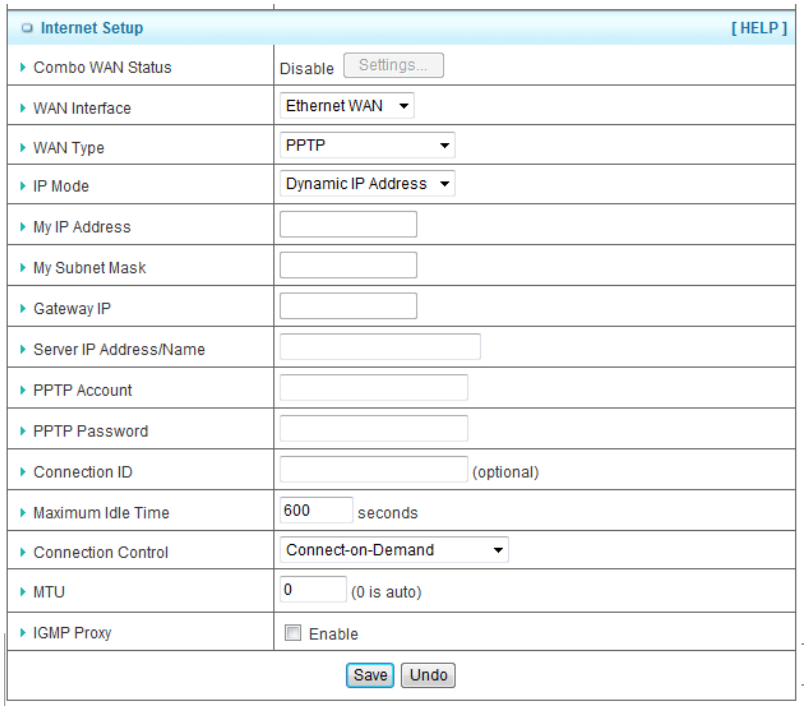
(E) PPP over Ethernet



1. **WAN Type**
   Choose PPP over Ethernet.
2. **IPv6 Dual Stack**
   If your ISP supports IPv6 dual stack, you can check this check box to get an IPv4 address and an IPv6 address via one PPPoE connection. After you check this check box, you also need to enable IPv6 function at **Advanced Setting->IPv6** setting page.
3. **PPPoE Account** and **Password**
   The account and password your ISP assigned to you.
4. **Primary DNS**
   You can indicate IP address of primary DNS if required.
5. **Secondary DNS**
   You can indicate IP address of secondary DNS if required.
6. **Maximum Idle Time**
   The amount of time of inactivity before disconnecting your PPPoE session. Set it to zero or enable “Auto-reconnect” to disable this feature.

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

(F) PPTP

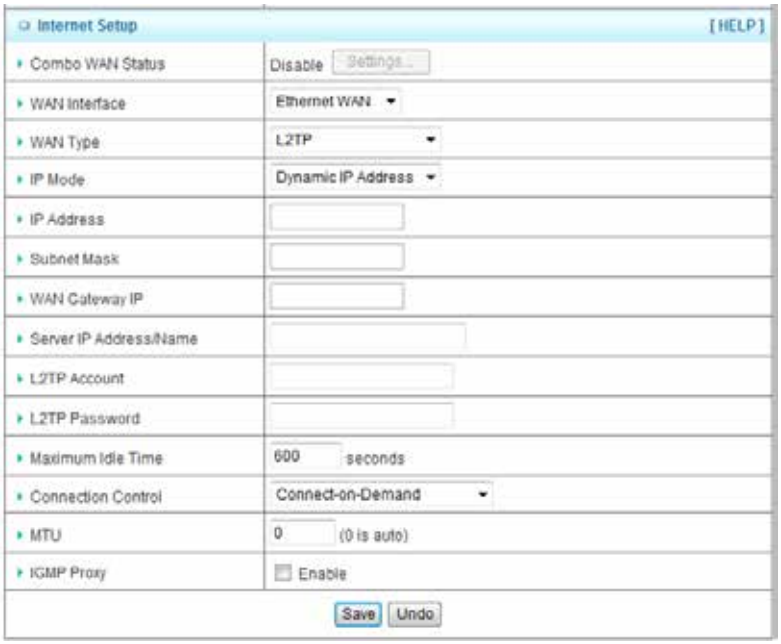


1. **WAN Type**
   Choose PPTP.
2. **IP Mode**
   You can select "**Static IP Address**" or "**Dynamic IP Address**".
3. **My IP Address***, **My Subnet Mask*, and Gateway IP***
   The IP address, subnet mask, and IP address of gateway your ISP assigned to you.
4. **Server IP Address/Name**
   The IP address of the PPTP server.
5. **PPTP Account** and **Password**
   The account and password your ISP assigned to you.

6. **Connection ID**
   Optional. Input the connection ID if your ISP requires it.
7. **Maximum Idle Time**
   The amount of time of inactivity before disconnecting your PPTP session. Set it to zero or enable “Auto-reconnect” to disable this feature.
8. **Connection Control**
   There are 3 options to start connection:
   - **Auto Reconnect (Always-on)**
     The device will always try to link to Internet.
   - **Connect-on-demand**
     The device won’t try to connect to Internet until LAN PCs or devices try to go to Internet. Once Internet connection is established, this device will drop the connection if maximum idle time is reached.
   - **Manually**
     The device won’t try to connect to Internet until users press “connect” button at Status page. Once Internet connection is established, this device will drop the connection if maximum idle time is reached.
9. **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.
10. **Maximum Transmission Unit (MTU)**
    Most ISP offers MTU value to users. The default MTU value is 0 (auto).
11. **IGMP Proxy**
    Enable this feature allows multicast stream (e.g. IPTV stream) to pass-through this device.

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

(G) L2TP



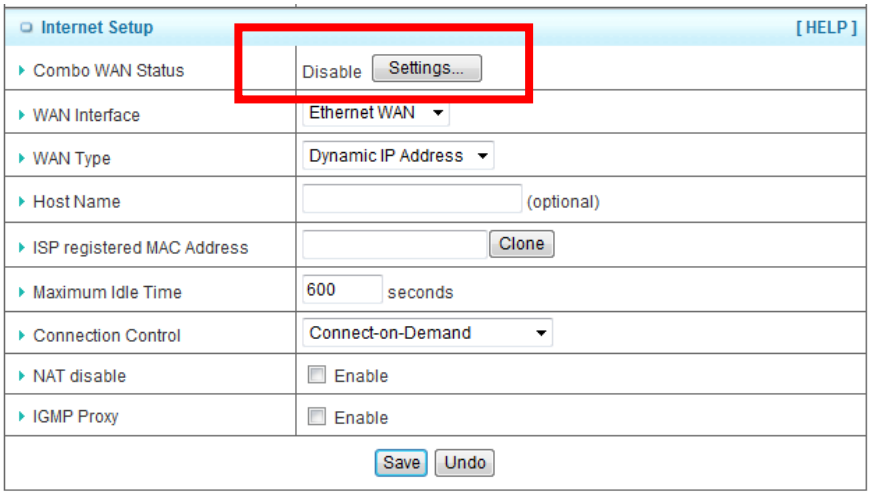
1. **WAN Type**
   Choose L2TP.
2. **IP Mode**
   You can select "**Static IP Address**" or "**Dynamic IP Address**".
3. **My IP Address***, **My Subnet Mask*, and Gateway IP***
   The IP address, subnet mask, and IP address of gateway your ISP assigned to you.
4. **Server IP Address/Name**
   The IP address of the L2TP server.
5. **L2TP Account** and **Password**
   The account and password your ISP assigned to you.
6. **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.
7. **Connection Control**
   There are 3 options to start connection:
   - **Auto Reconnect (Always-on)**
     The device will always try to link to Internet.
   - **Connect-on-demand**
     The device won't try to connect to Internet until LAN PCs or devices try to go to Internet. Once Internet connection is established, this device will drop the connection if maximum idle time is reached.
   - **Manually**
     The device won't try to connect to Internet until users press "connect" button at Status page. Once Internet connection is established, this device will drop the connection if maximum idle time is reached.

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

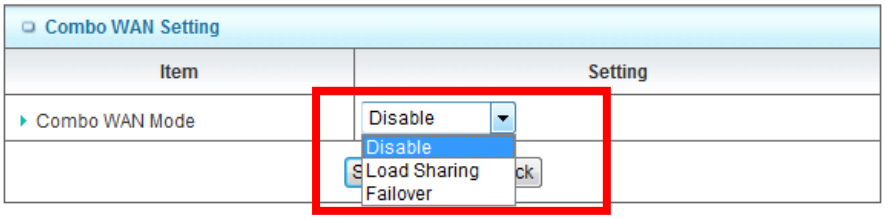
Note: The items with * above are only available when choosing Static IP Address in IP mode.

(H) Combo WAN Setting

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

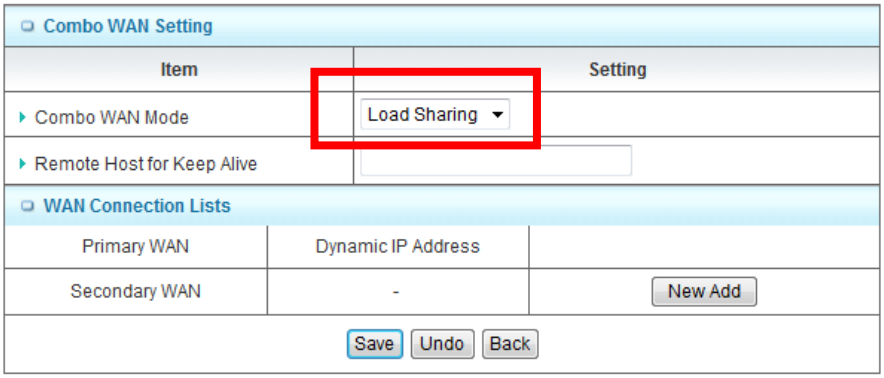


At Combo WAN setting page, you can choose **Disable**, **Load Sharing**, or **Failover** options. This Combo WAN feature will be deactivated if you select "**Disable**" from the list.

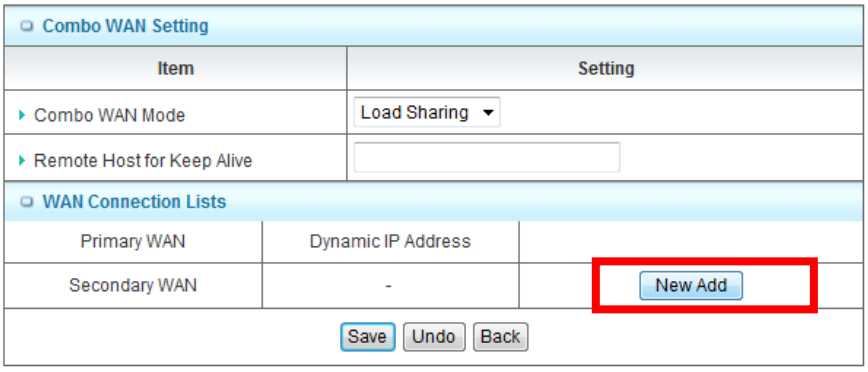


(a) Load Sharing

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

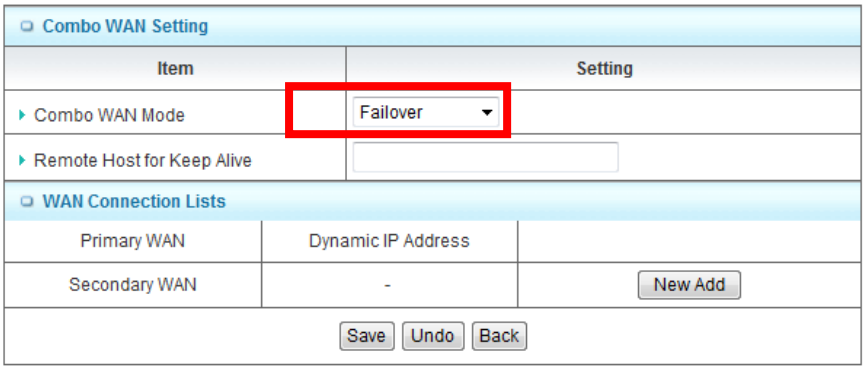


1. **Combo WAN Mode**
   Choose Load Sharing mode.
2. **Remote Host for Keep Alive**
   Type an IP address or domain name of remote host to detect if Internet connection is alive.
3. **Primary WAN**
   The primary WAN is the WAN type you set at Internet Setup page.
4. **Secondary WAN**
   Press "**New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



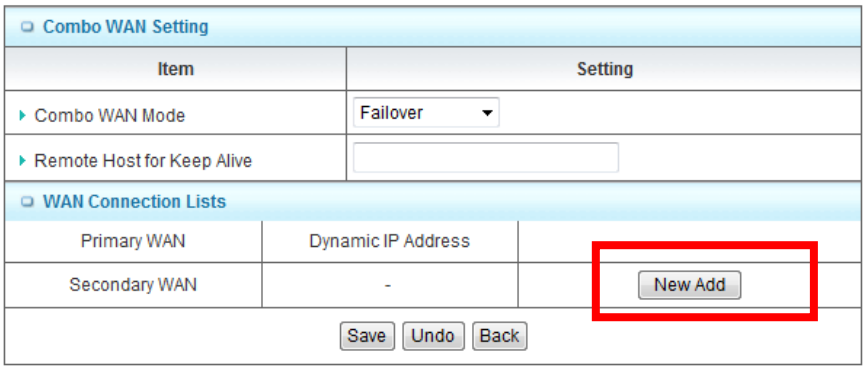
(b) Failover

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

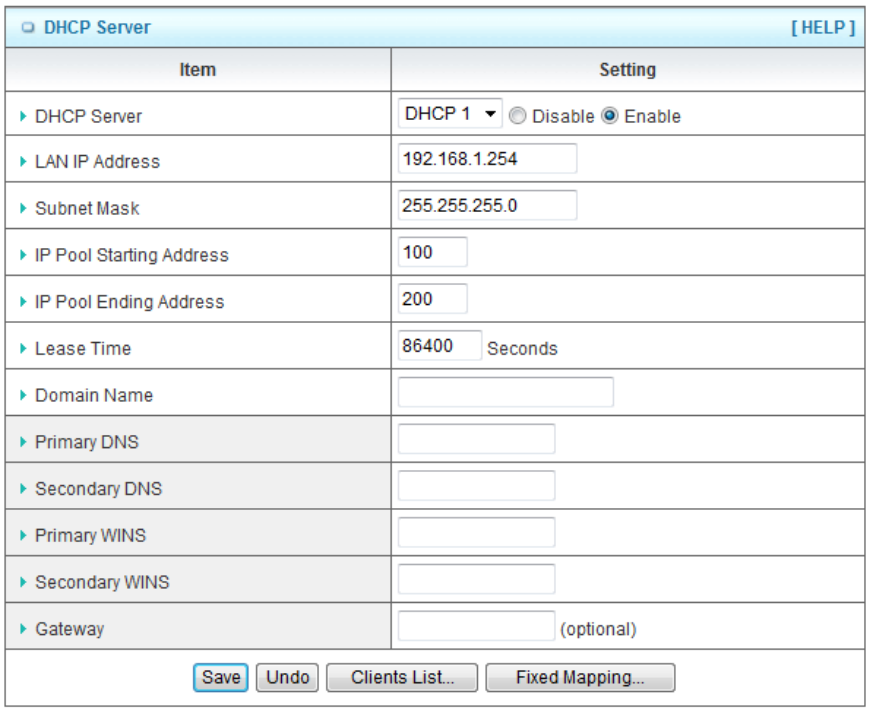


Internet connection will be switched from secondary WAN back to primary WAN.

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



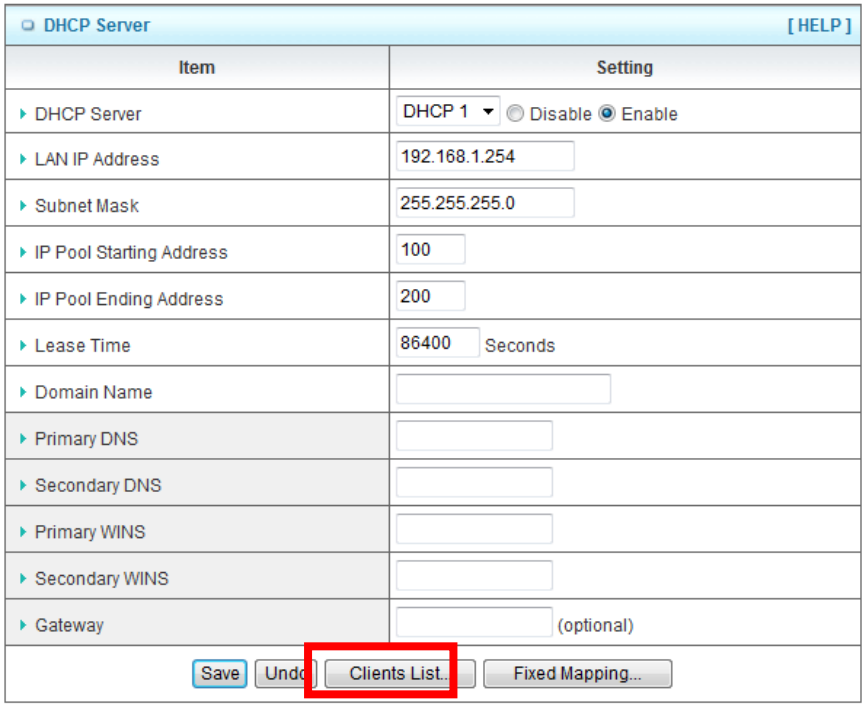
3.2.2 DHCP Server



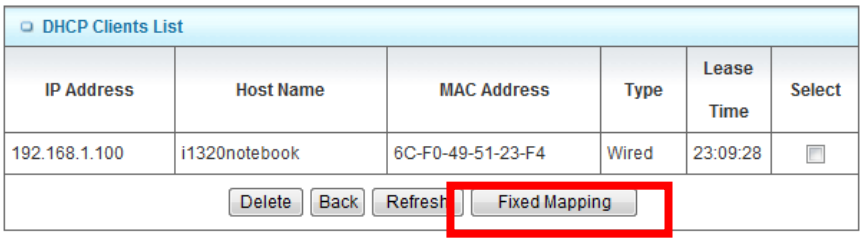
1. **DHCP Server**
   You can have total four (DHCP1~DHCP4) different settings of DHCP server configurations on this device. If you divide LAN network into different groups via VLAN ID (Please refer to **Advanced Setting->VLAN** for detail), you can have different DHCP server settings for each of them.
2. **IP Pool Starting/Ending Address**
   Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool.
3. **Lease Time**
   DHCP lease time to the DHCP client.
4. **Domain Name**
   Optional, this information will be passed to the clients.
5. **Primary DNS/Secondary DNS**
   Optional. This feature allows you to assign a DNS Servers
6. **Primary WINS/Secondary WINS**
   Optional. This feature allows you to assign a WINS Servers
7. **Gateway**
   Optional. Gateway Address would be the IP address of an alternate Gateway. This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.

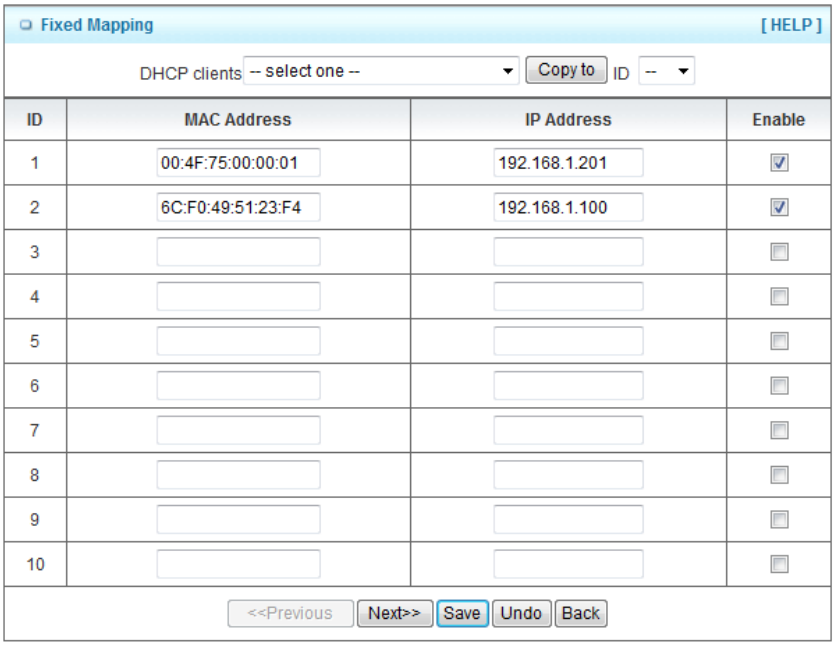
Click on "Save" to store your settings or click "Undo" to give up the changes.

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



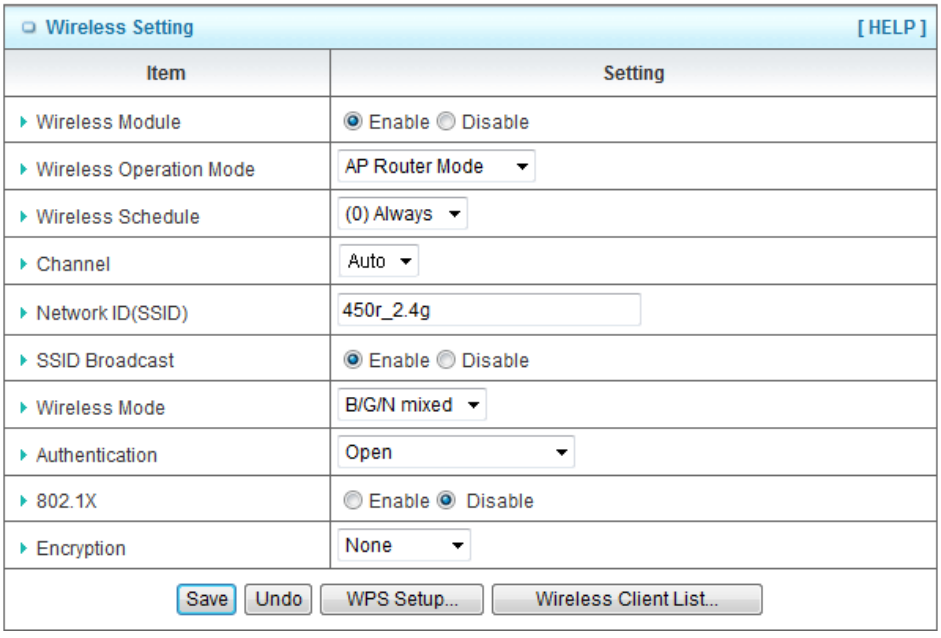
Press **"Fixed Mapping**" and the DHCP Server will reserve the special IP for designated MAC Address.





3.2.3 Wireless 2.4G Settings

Here you can configure settings for 2.4GHz wireless functions.



Wireless settings allow you to set the wireless configuration items.

1. **Wireless Module**
   You can enable or disable wireless function.

2. **Wireless Operation Mode**
   You can select the wireless operation mode such as AP Router, AP Only, and WDS Hybrid and WDS Only..etc.
3. **Wireless Schedule**
   You can limit Wi-Fi functions in a period of time if required.
4. **Channel**
   The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is Auto, channel 1~11 for North America, Channel 1~13 for European (ETSI) and channel1~ 14 for Japan.
5. **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 "**airlive2.4g**")
6. **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 cannot find the device from beacons.
7. **Wireless Mode**
   Choose "**B/G mixed**", "**B only**", "**G only**", "**N only**", "**G/N mixed**" or "**B/G/N mixed**". The factory default setting is "**B/G/N mixed**".
8. **Authentication**
   You may select one of authentication to secure your wireless network: **Open**, **Shared**, **Auto**, **WPA-PSK**, **WPA**, **WPA2-PSK**, **WPA2**, **WPA-PSK/WPA2-PSK**, or **WPA /WPA2**.

(A) 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.

(B) 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.

(C) Auto

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

(D) 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 (e.g. 12345678)

(E) 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.

(F) WPA-PSK2

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

(G) WPA2

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

(H) WPA-PSK/WPA-PSK2

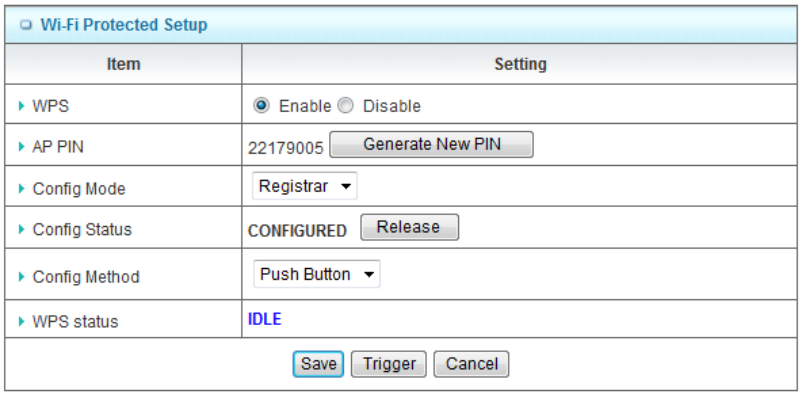
Another encryption options for WPA-PSK-TKIP and WPA-PSK2-AES, the others are same the WPA-PSK.

(I) WPA/WPA2

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

1. **802.1X**
   You can enable or disable 802.X function.
2. **Encryption**
   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.

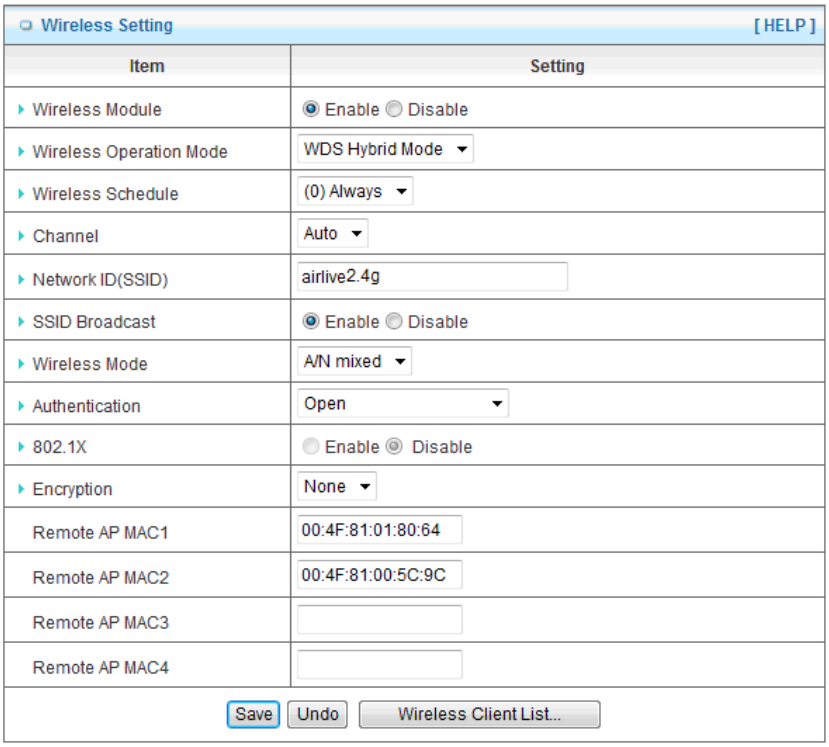
By pressing **"WPS Setup"**, you can configure and enable the easy setup feature WPS (Wi-Fi Protection Setup) for your wireless network.



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

By pressing **"WDS Hybrid Mode"** and **"WDS Only Mode"**, you can connect this device to another AP via WDS connection.

WDS Hybrid Mode



1. **Wireless Operation Mode W**
   Choose WDS Hybrid mode.
2. **Wireless Schedule**
   You can limit Wi-Fi functions in a period of time if required.
3. **Channel**
   The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is Auto, channel 1~11 for North America, channel 1~13 for European (ETSI) and channel1~ 14 for Japan.
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 "**airlive2.4g**")
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 cannot find the device from beacons.
6. **Wireless Mode**
   Choose "**B/G mixed**", "**B only**", "**G only**", "**N only**", "**G/N mixed**" or "**B/G/N mixed**". The factory default setting is "**B/G/N mixed**".

7. Authentication

You may select one of authentication to secure your wireless network: **Open**, **Shared**, **Auto**, **WPA-PSK**, **WPA**, **WPA2-PSK**, **WPA2**, **WPA-PSK/WPA2-PSK**, or **WPA /WPA2**.

(A) 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.

(B) 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.

(C) Auto

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

(D) 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 (e.g. 12345678)

(E) 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.

(F) WPA-PSK2

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

(G) WPA2

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

(H) WPA-PSK/WPA-PSK2

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

(I) WPA/WPA2

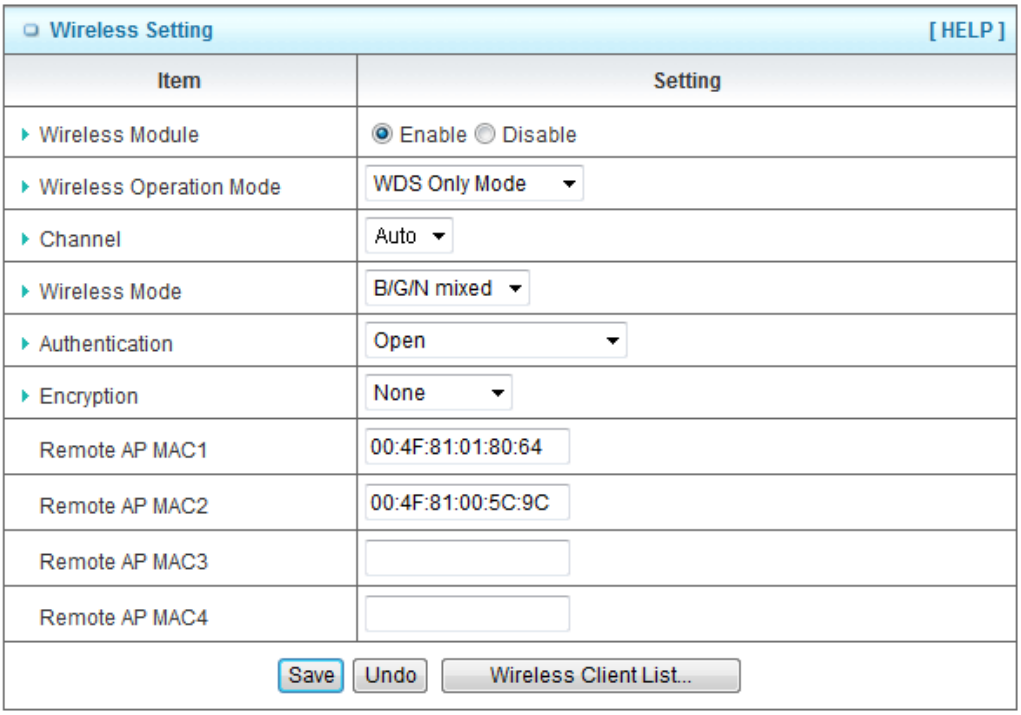
Another encryption options for WPA-TKIP and WPA2-AES, the others are same the WPA.

8. Encryption

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.

9. **Remote AP MAC 1~4**
   Enter the MAC address for remote AP that you want to connect via WDS.

WDS Only Mode



1. **Wireless Operation Mode W**
   Choose WDS Only mode.
2. **Wireless Schedule**
   You can limit Wi-Fi functions in a period of time if required.
3. **Channel**
   The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is Auto, channel 1~11 for North America, channel 1~13 for European (ETSI) and channel1~ 14 for Japan.
4. **Wireless Mode**
   Choose "**B/G mixed**", "**B only**", "**G only**", "**N only**", "**G/N mixed**" or "**B/G/N mixed**". The factory default setting is "**B/G/N mixed**".
5. **Authentication**
   You may select one of authentication to secure your wireless network: **Open**, **Shared**, **Auto**, **WPA-PSK**, **WPA**, **WPA2-PSK**, **WPA2**, **WPA-PSK/WPA2-PSK**, or **WPA /WPA2**.

(A) 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.

(B) 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.

(C) Auto
The AP will Select the Open or Shared by the client's request automatically.

(D) 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 (e.g. 12345678)

(E) 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.

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

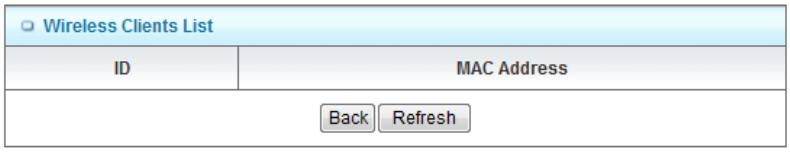
(G) WPA2
WPA2 add uses AES and TKIP for encryption, the others are same the WPA.

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

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

6. Encryption
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.

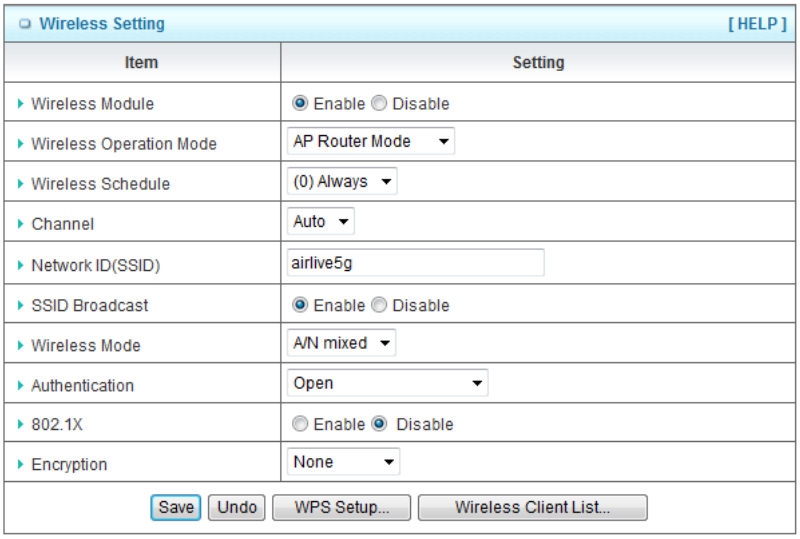
7. Remote AP MAC 1~4
Enter the MAC address for remote AP that you want to connect via WDS.



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

3.2.4 Wireless 5G Settings

Here you can configure settings for 5GHz wireless functions.



Wireless settings allow you to set the wireless configuration items.

1. **Wireless Module**
   You can enable or disable wireless function.
2. **Wireless Operation Mode**
   You can select the wireless operation mode such as AP Router, AP Only, and WDS Hybrid and WDS Only ..etc.
3. **Wireless Schedule**
   You can limit Wi-Fi functions in a period of time if required.
4. **Channel**
   The radio channel number. The permissible channels depend on the Regulatory Domain.
5. **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 "**airlive5g**")

6. **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.
7. **Wireless Mode**
   Choose “**A/N mixed**”, “**A only**”, “**N only**”. The factory default setting is “**A/N mixed**”.
8. **Authentication**
   You may select one of authentication to secure your wireless network: **Open Shared**, **Auto**, **WPA-PSK**, **WPA**, **WPA2-PSK**, **WPA2**, **WPA-PSK/WPA2-PSK**, or **WPA /WPA2**.

(A) 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.

(B) 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.

(C) Auto
The AP will Select the Open or Shared by the client’s request automatically.

(D) 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 (e.g. 12345678)

(E) 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.

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

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

(H) WPA-PSK/WPA-PSK2

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

(I) WPA/WPA2

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

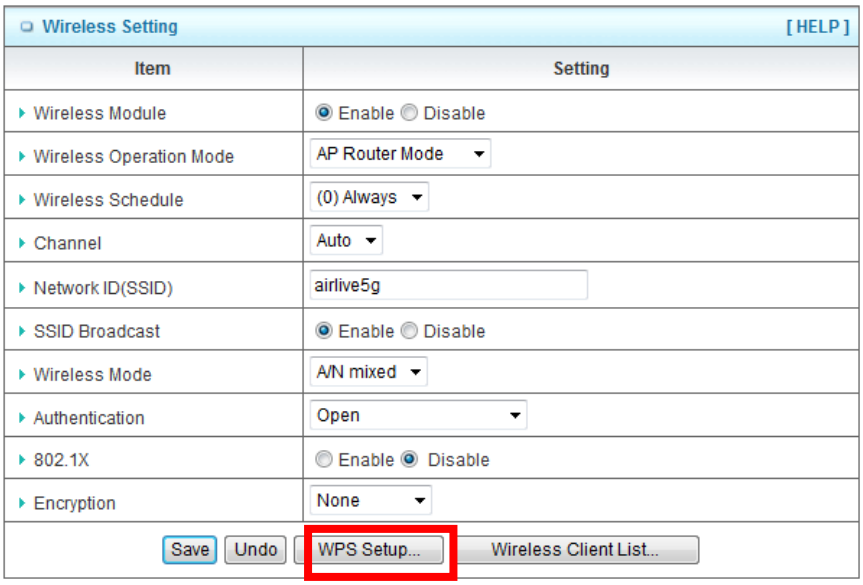
9. 802.1X

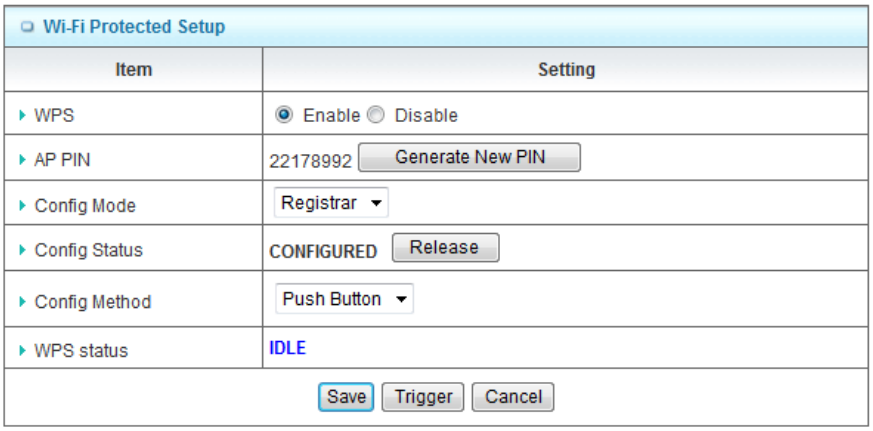
You can enable or disable 802.1X function.

10. 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.

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

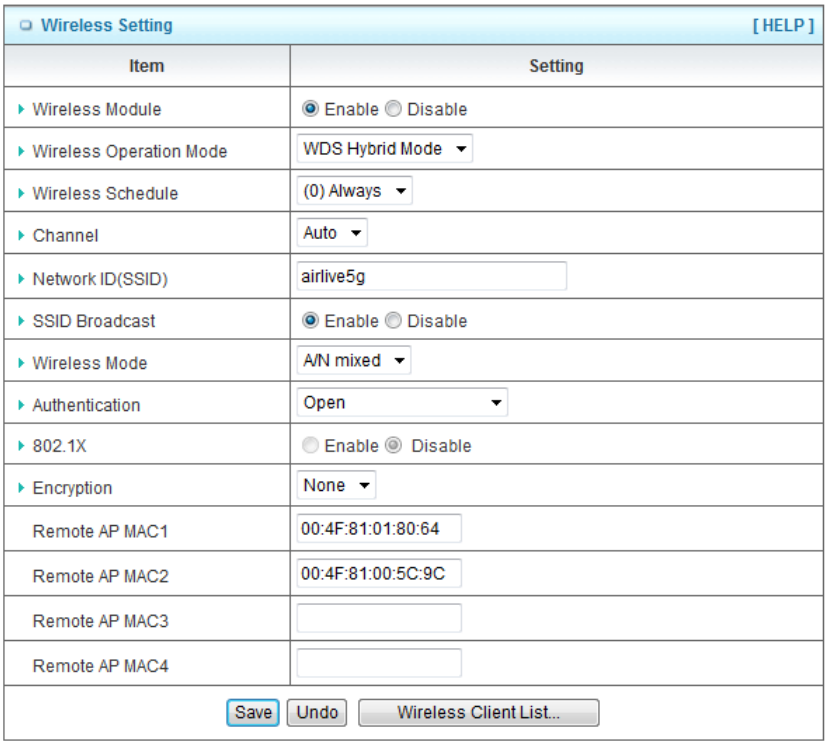




1. **WPS**
   You can enable this function by selecting “Enable”. WPS offers a safe and easy way to allow the wireless clients connected to your wireless network.
2. **AP PIN**
   You can press Generate New Pin to get an AP PIN.
3. **Config Mode**
   Select your config Mode from “Registrar” or “Enrollee”.
4. **Config Status**
   It shows the status of your configuration.
5. **Config Method**
   You can select the Config Method here from “**Pin Code**” or “**Push** Button”.
6. **WPS status**
   According to your setting, the status will show “**Start Process**” or “N**o used**”.

By pressing **“WDS Hybrid Mode”** and **“WDS Only Mode”**, you can connect this device to another AP via WDS connection.

WDS Hybrid Mode



1. **Wireless Operation Mode W**
   Choose WDS Hybrid mode.
2. **Wireless Schedule**
   You can limit Wi-Fi functions in a period of time if required.

3. **Channel**
   The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is Auto, channel 1~11 for North America, channel 1~13 for European (ETSI) and channel1~ 14 for Japan.

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 "**airlive2.4g**")

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 cannot find the device from beacons.

6. **Wireless Mode**
   Choose "**B/G mixed**", "**B only**", "**G only**", "**N only**", "**G/N mixed**" or "**B/G/N mixed**". The factory default setting is "**B/G/N mixed**".

7. **Authentication**
   You may select one of authentication to secure your wireless network: **Open**, **Shared**, **Auto**, **WPA-PSK**, **WPA**, **WPA2-PSK**, **WPA2**, **WPA-PSK/WPA2-PSK**, or **WPA /WPA2**.

(A) 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.

(B) 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.

(C) Auto
The AP will Select the Open or Shared by the client's request automatically.

(D) 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 (e.g. 12345678)

(E) 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.

(F) WPA-PSK2

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

(G) WPA2

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

(H) WPA-PSK/WPA-PSK2

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

(I) WPA/WPA2

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

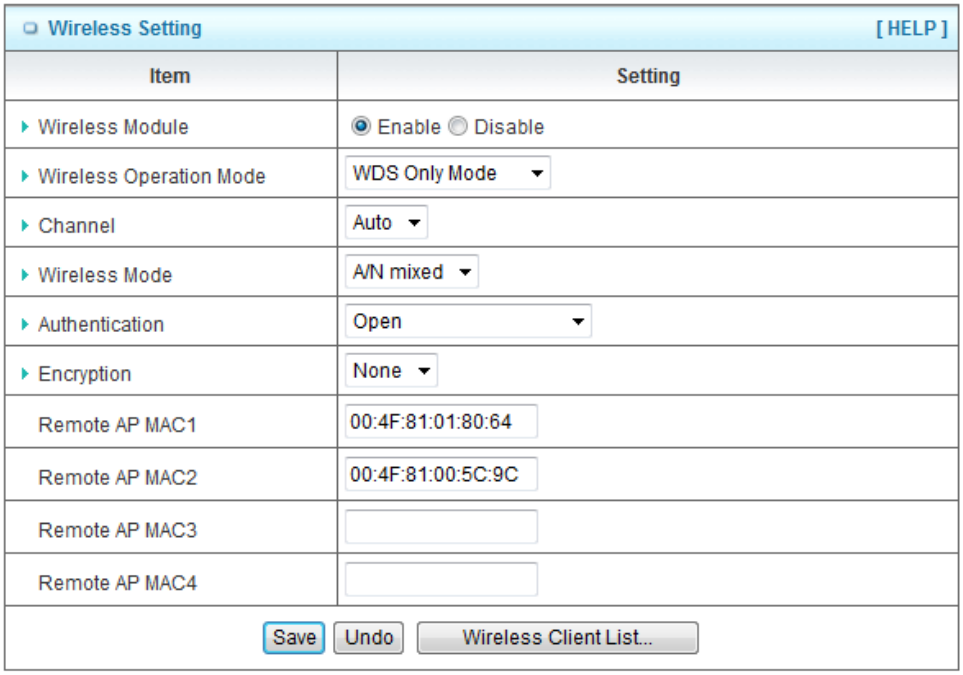
8. Encryption

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.

9. Remote AP MAC 1~4

Enter the MAC address for remote AP that you want to connect via WDS.

WDS Only Mode



1. Wireless Operation Mode W

Choose WDS Hybrid mode.

2. Wireless Schedule

You can limit Wi-Fi functions in a period of time if required.

3. **Channel**
   The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is Auto., channel 1~11 for North America, channel 1~13 for European (ETSI) and channel1~ 14 for Japan.

4. **Wireless Mode**
   Choose "**B/G mixed**", "**B only**", "**G only**", "**N only**", "**G/N mixed**" or "**B/G/N mixed**". The factory default setting is "**B/G/N mixed**".

5. **Authentication**
   You may select one of authentication to secure your wireless network: **Open**, **Shared**, **Auto**, **WPA-PSK**, **WPA**, **WPA2-PSK**, **WPA2**, **WPA-PSK/WPA2-PSK**, or **WPA /WPA2**.

(A) 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.

(B) 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.

(C) Auto
The AP will Select the Open or Shared by the client's request automatically.

(D) 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 (e.g. 12345678)

(E) 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.

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

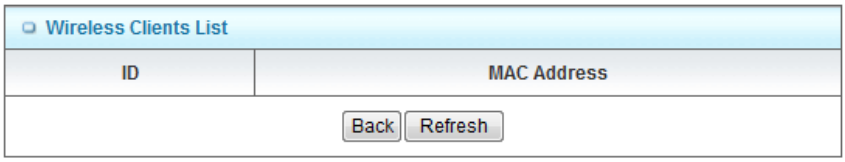
(G) WPA2
WPA2 add uses AES and TKIP for encryption, the others are same the WPA.

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

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

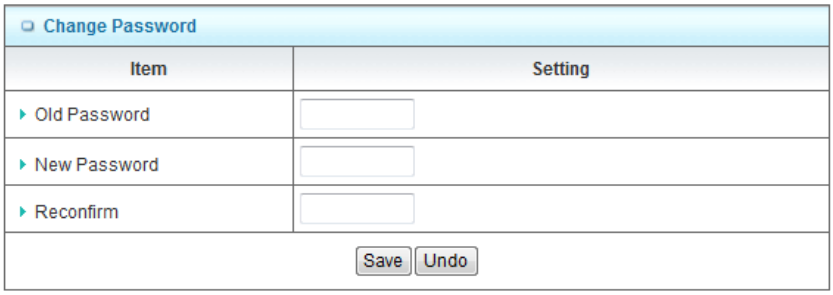
6. **Encryption**
   Select the appropriate category. Once you set up that type of encryption, second LAN PC must enter the same encryption type as the first one.
7. **Remote AP MAC 1~4**
   Enter the MAC address for remote AP that you want to connect via WDS.

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



3.2.5 Change Password

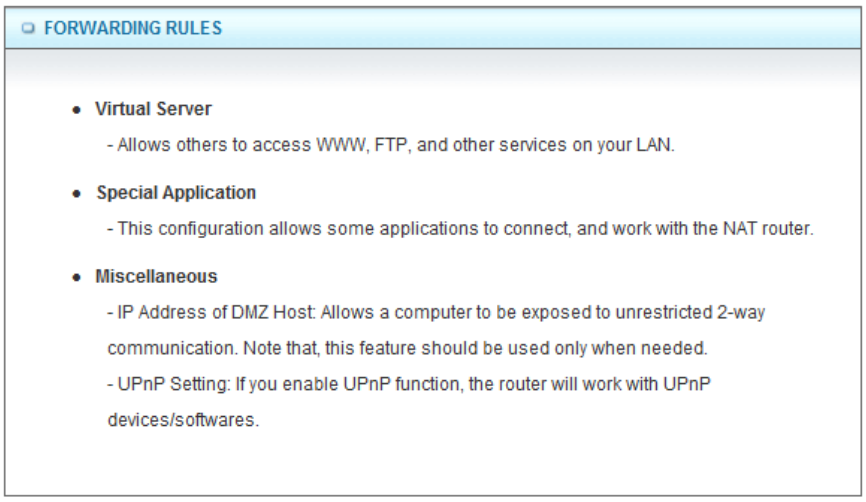
You can change the System Password here. We strongly recommend you to change the system password for security reason.



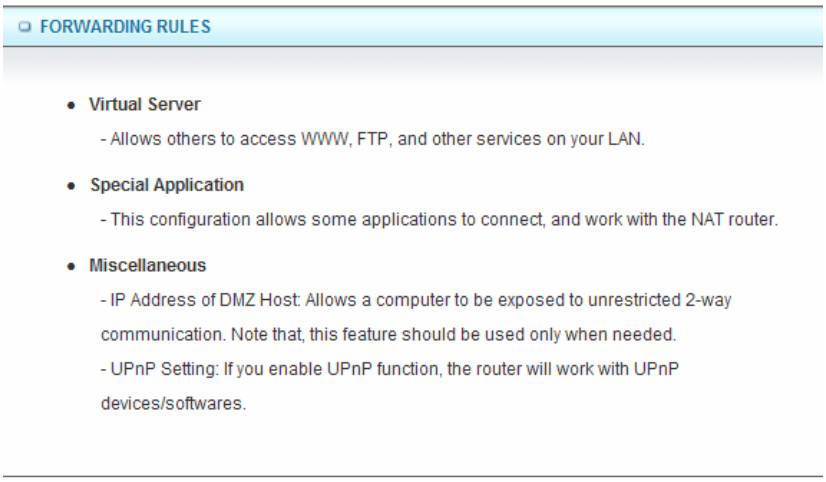
Click on "**Save**" to store your settings or click "**Undo**" to give up the changes.

3.3 Forwarding Rules

There are three options: **Virtual Server**, **Special Application** and **Miscellaneous**.

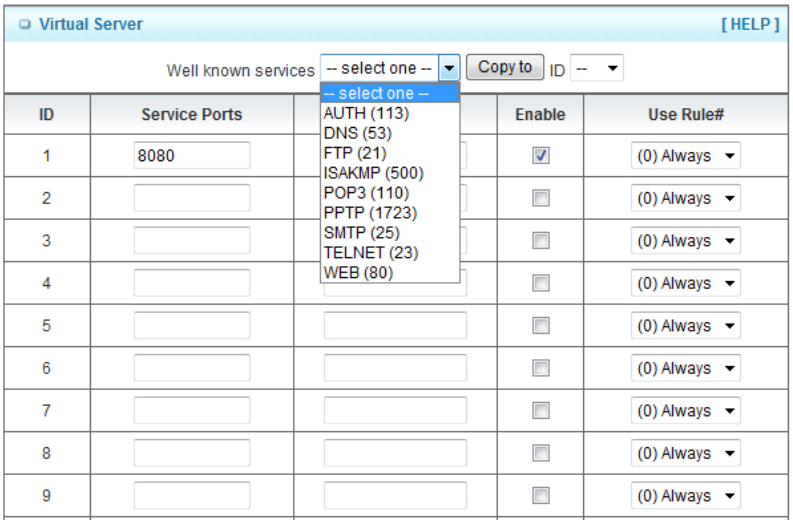


3.3.1 Virtual Server



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**.



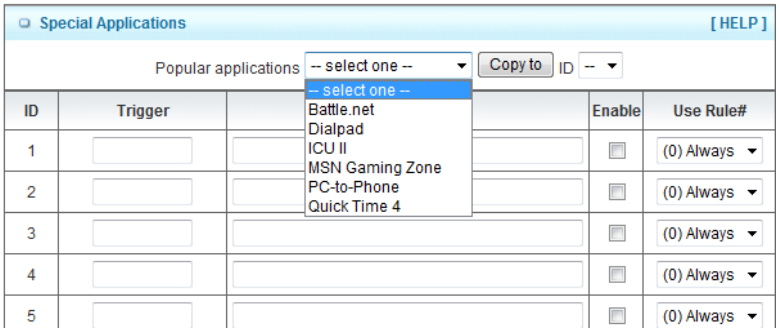
For example, if you have an FTP server (port 21) at 192.168.1.1, a Web server (port 80) at 192.168.1.2, and a VPN server at 192.168.1.6, then you need to specify the following virtual server mapping table: Service Port

	Server IP	Enable
21	192.168.1.1	V
80	192.168.1.2	V
1723	192.168.1.6	V

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

3.3.2 Special AP

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

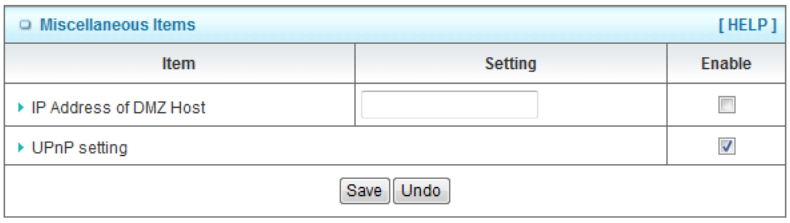


1. **Trigger**
   The outbound port number issued by the application.
2. **Incoming Ports**
   When the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.
3. **Enable**
   Check the checkbox to activate each of rule. This device provides some predefined settings. Select your application and click "**Copy to"** to add the predefined setting to your list. Click on "**Save**" to store your settings or click "**Undo**" to give up the changes.

3.3.3 IP CAM

After you plug AirLive IP Camera into PnP Router, please check the IP CAM table list as following.

3.3.4 Miscellaneous



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

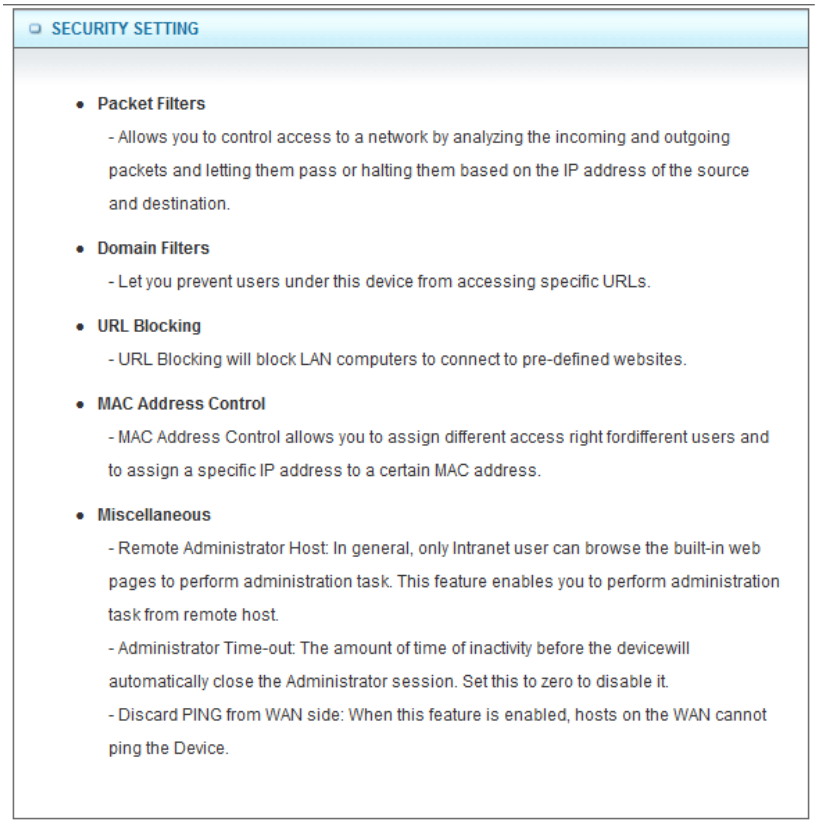
2. UPnP Setting

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

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

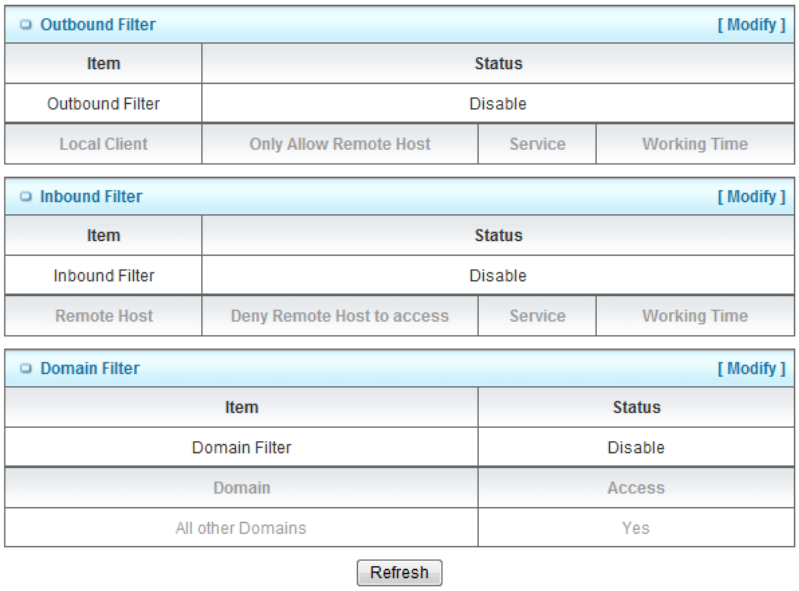
3.4 Security Setting

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



3.4.1 Status

You can see the security log on the status page as following,

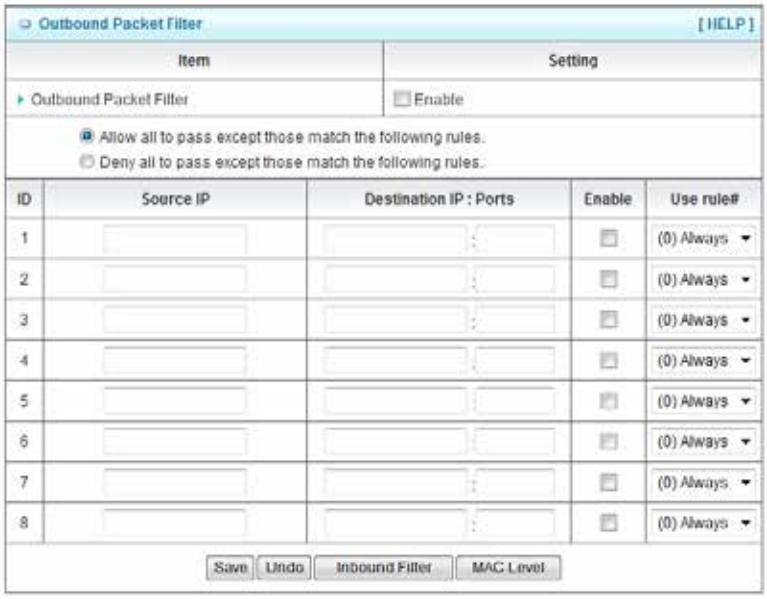


3.4.2 Packet Filters

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

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

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



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

- Source IP address
- Destination IP address
- Destination port
- Enable or Disable
- Use Rule#

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

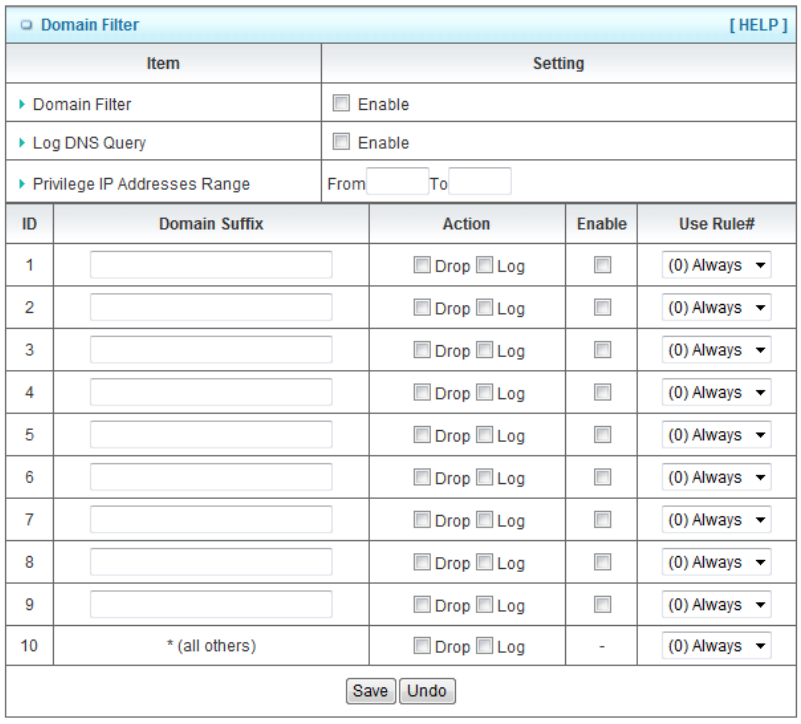
For source or destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999, No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. Packet Filter can work with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

Each rule can be enabled or disabled individually.

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

3.4.3 Domain Fitters

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



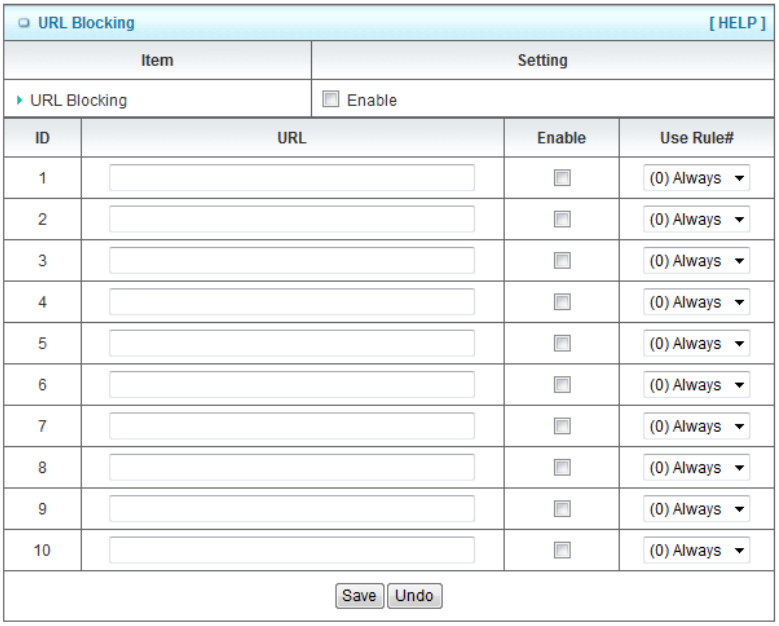
1. **Domain Filter**
   Check if you want to enable Domain Filter.
2. **Log DNS Query**
   Check if you want to log the action when someone accesses the specific URLs.

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

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

3.4.4 URL Blocking

URL Blocking will block LAN computers to connect with pre-define Websites. The major difference between "**Domain filter**" and "**URL Blocking**" is Domain filter 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".

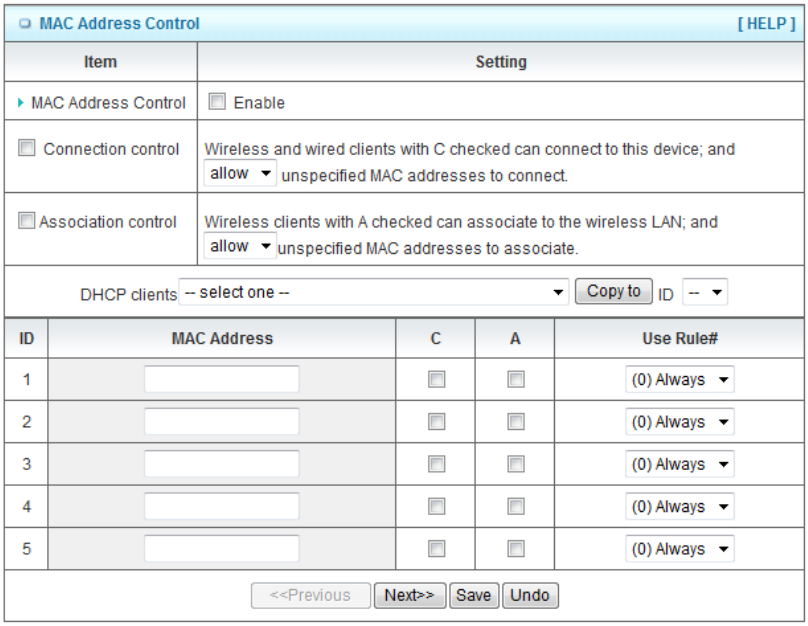
3. **Enable**
   Check to enable each rule.

4. **Use Rule#**
   You can set a schedule rule for each of rule.

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

3.4.5 MAC Control

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

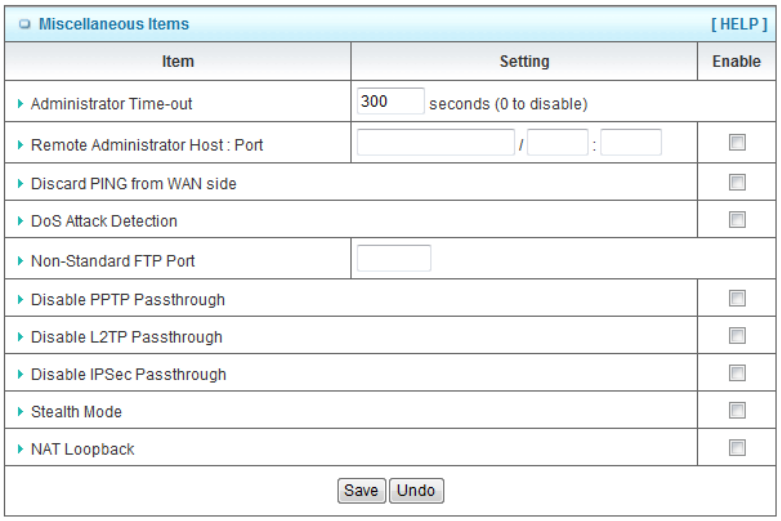


1. **MAC Address Control**
   Check "Enable" to enable the "**MAC Address Control**". All of the settings in this page will take effect only when "Enable" is checked.

2. **Connection control**
   Check "**Connection control**" to enable the controlling of which wired and wireless clients can connect with this device. If a client is denied to connect with this device, it means the client can't access to the Internet either. Choose "**allow**" or "**deny**" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect with this device.

3. **Association control**
   Check "Association control" to enable the controlling of which wireless client can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "**allow**" or "**deny**" to allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN.

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



3.4.6 Miscellaneous

1. **Administrator Time-out**
   The time of no activity to logout automatically, you may set it to zero to disable this feature.

2. **Remote Administrator Host/Port**
   In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect with this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses for example, "10.1.2.0/24".

NOTE: When Remote Administration is enabled, the web server port will be shifted to 80. You can change web server port to other port, too.

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

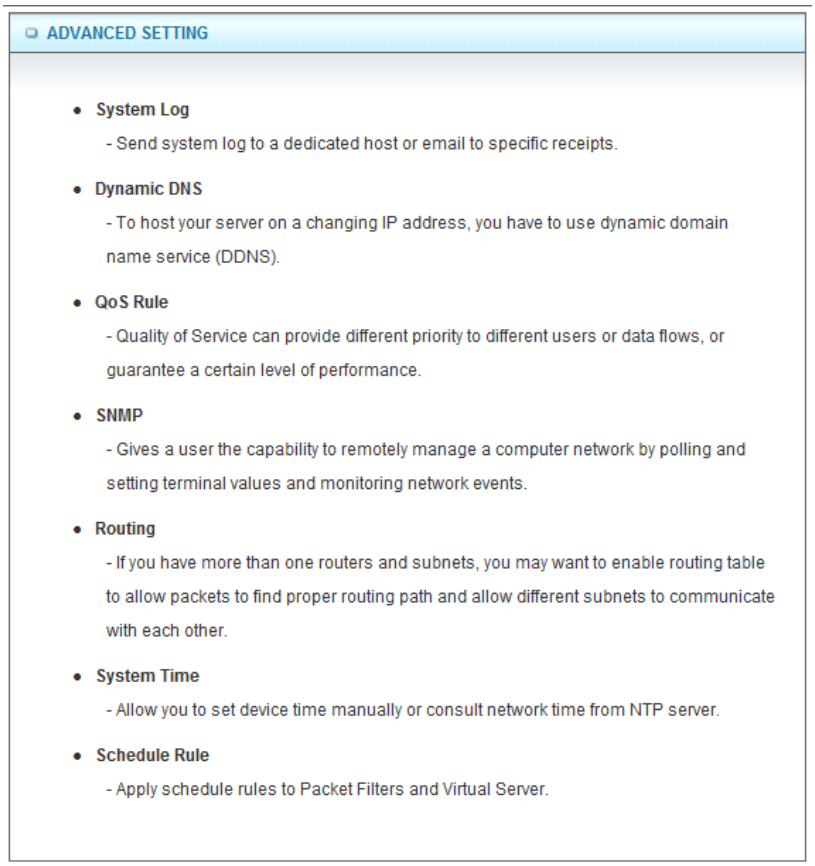
4. **DoS Attack Detection**
   When this feature is enabled, the router will detect and log the DoS attack comes from the Internet. Currently, the router can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack etc.

5. **Non-Standard FTP port**
   If you want to access a WAN FTP server which doesn't use port 21, you need to indicate the port number that WAN FTP uses.
6. **Disable PPTP passthrough**
   The PPTP passthrough is enabled by default. You can disable here.
7. **Disable L2TP passthrough**
   The L2TP passthrough is enabled by default. You can disable here.
8. **Disable IPSec passthrough**
   The IPSec passthrough is enabled by default. You can disable here.
9. **Stealth Mode**
   If enable this option, router will become "hidden" if someone uses port scan utility to scan available ports on this router.
10. **NAT Loopback**
    If enable this option, local hosts can access local virtual server via WAN IP address of this router.

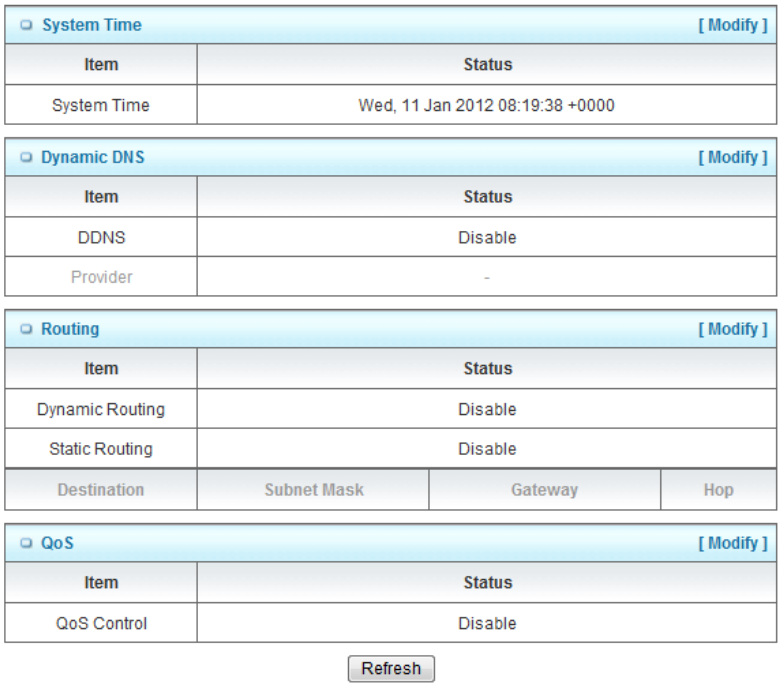
Click on "**Save**" to store your settings or click "**Undo**" to give up the changes.

3.5 Advanced Setting

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

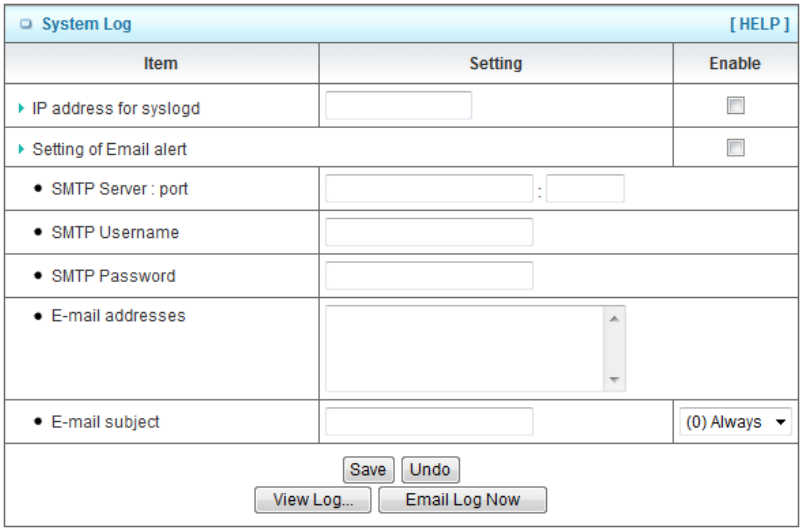


3.5.1 Status



3.5.2 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 including:



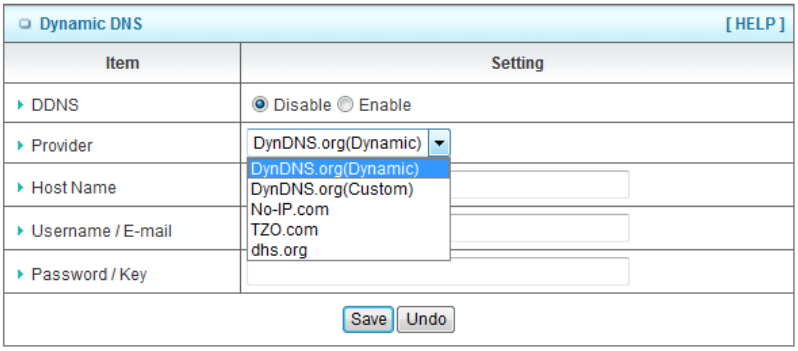
1. **IP Address for Sys log**
   Host IP of destination where sys log will be sent to. Check **Enable** to enable this function.
2. **Setting of E-mail Alert**
   Check if you want to enable Email alert (send syslog via email).

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

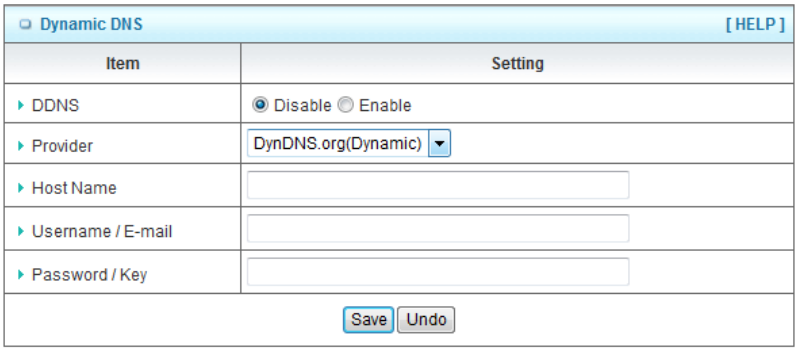
Click on "**Save**" to store your settings or click "**Undo**" to give up the changes.

3.5.2 Dynamic DNS

To host your server on a changing IP address, you have to use dynamic domain name service (DDNS). So that anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.



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

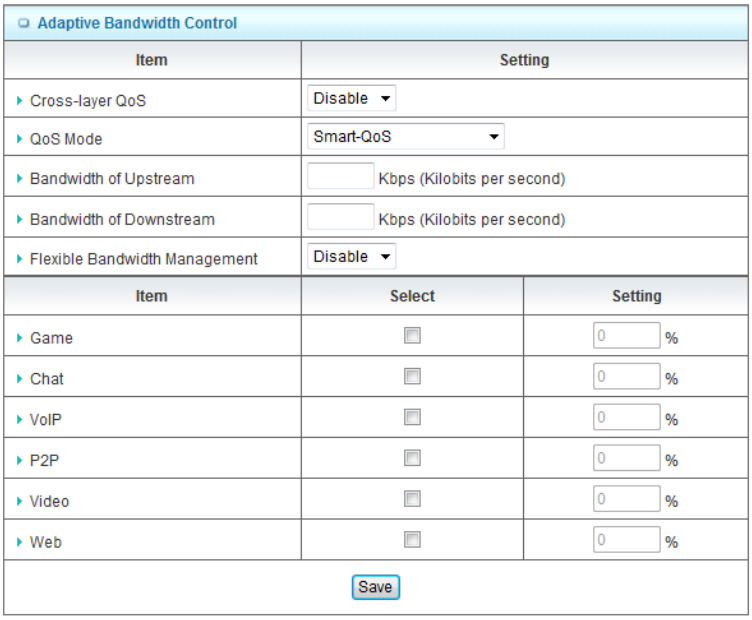


To enable **Dynamic DNS** click the check box next to **Enable** in the **DDNS** field. Next you have to enter the appropriate information about your Dynamic DNS Serve .**Provider**, **Host Name**, **Username/E-mail**, and **Password/Key**. You can get this information when you register an account on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

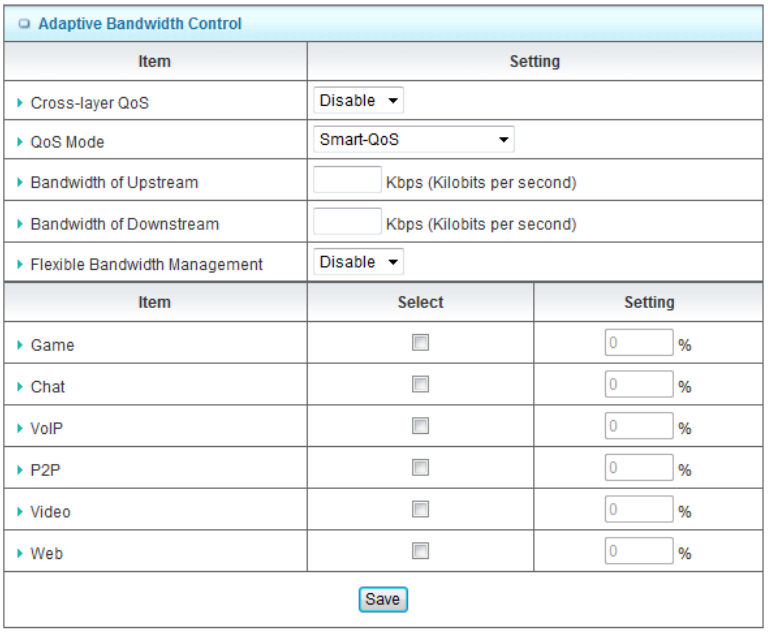
Click on "**Save**" to store your settings or click "**Undo**" to give up the changes.

3.5.3 QoS

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

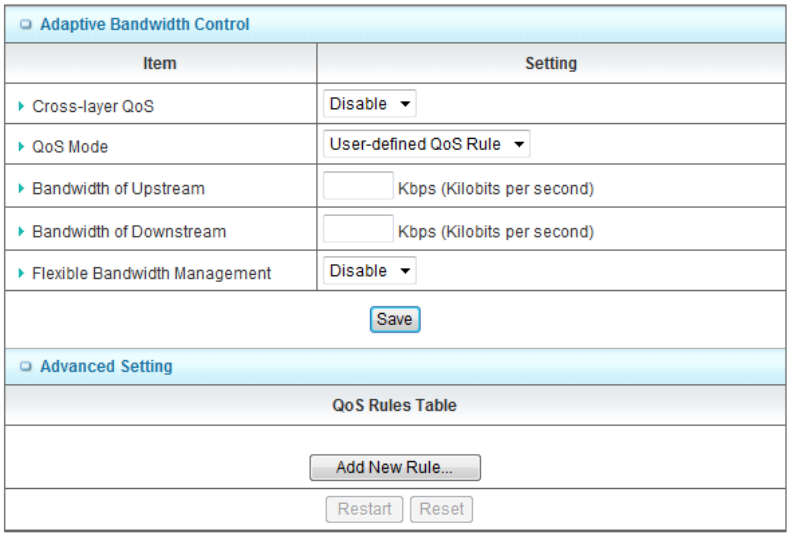


(A) Smart QoS

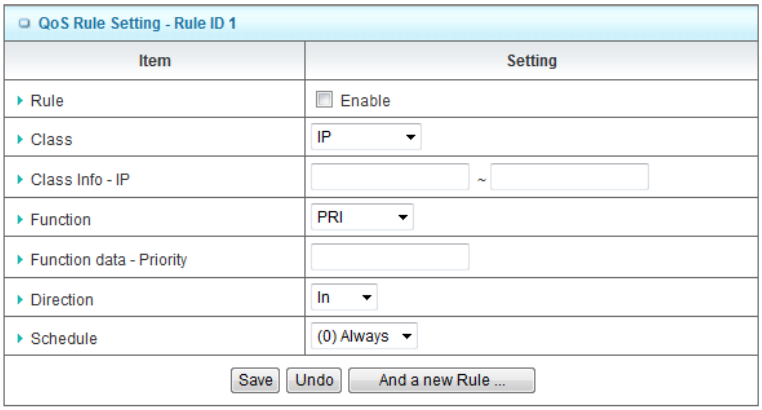


1. **Cross-layer QoS**
   You can select enable/disable the QoS control
2. **QoS Mode**
   You can select Smart-QoS or User defined QoS rule for your own QoS control
3. **Bandwidth of upstream / bandwidth of Downstream**
   You can input the value of maximize of upstream and downstream bandwidth from your ISP
4. **Enable Flexible Bandwidth management**
   If you enable this management, system will share the bandwidth of those selected applications to other applications if user do not run those selected application, for example, If you select Game/ VoIP/ Video 3 applications for higher priority in your system, then the system will automatically reserve 10% of bandwidth to other application, and share the rest of bandwidth (100-10)/3=30% each to Game/VoIP/Video, so if user do not play a game, then the system will flexible share the 30% of bandwidth to other application.
5. **Example for Smart-QoS with FBM enable**
   Mr. Wang selects Game/ VoIP/ Video 3 applications for higher priority in his system, the system will automatically reserve 10% of minimum rate of bandwidth to other application, and share the rest minimum rate of bandwidth (100-10)/3=30% each to Game/VoIP/Video. If Mr. Wang's son plays on-line game in the morning, the total bandwidth will all reserve to his son. By the evening, when Mr. Wang back home and wants to watch IPTV, then he will get the same priority with his son, and share the bandwidth.
6. **Disable Flexible Bandwidth Management**
   If you disable this management, system will allow you to input percentage of bandwidth manually.

(B) User defined QoS Rule



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



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

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

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

n **Function:** You can set your own function value to enable your QoS rule as below.

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

n **Direction:** You can select inbound/ outbound for your direction.

Direction	
IN	inbond
OUT	outbond
BOTH	inbond & outbond

6. DSCP setting: You can set your own DSCP value here.
DiffServ Code Point: you can select code value.
Service Type: You can select their service type.
Function: PRI
Function data- Priority: 1~6

DSCP marking

You can add your inbound / outbound packets a DCSP marking,

For example

Please mark CS3 when an packet in/ out via UDP port 5060.Once you saved the QoS rule, system will show you the rule as below, you can add another new rule accordingly.

System will show you all your QoS rule as below

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

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

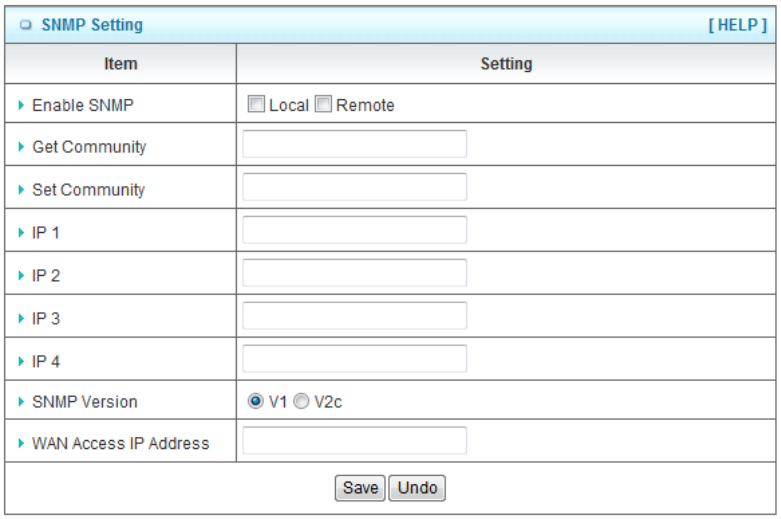
Provide different priority to different users or data flows, or guarantee a certain level of performance.

1. **QOS Control**
   Check **Enable** to enable this function.
2. **Bandwidth of Upstream**
   Set the limitation of upstream bandwidth
3. **Local IP : Ports**
   Define the Local IP address and ports of packets
4. **Remote IP : Ports**
   Define the Remote IP address and ports of packets
5. **QoS Priority**
   This defines the priority level of the current Policy Configuration. Packets associated with this policy will be serviced based upon the priority level set. For critical applications High or Normal level is recommended. For non-critical applications select a Low level.
6. **Enable**
   Check to enable the corresponding QOS rule.
7. **User Rule#**
   The QoS rule can work with Scheduling Rule number#. Please refer to the Section 3.1.4.7 Schedule Rule.

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

3.5.4 SNMP

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

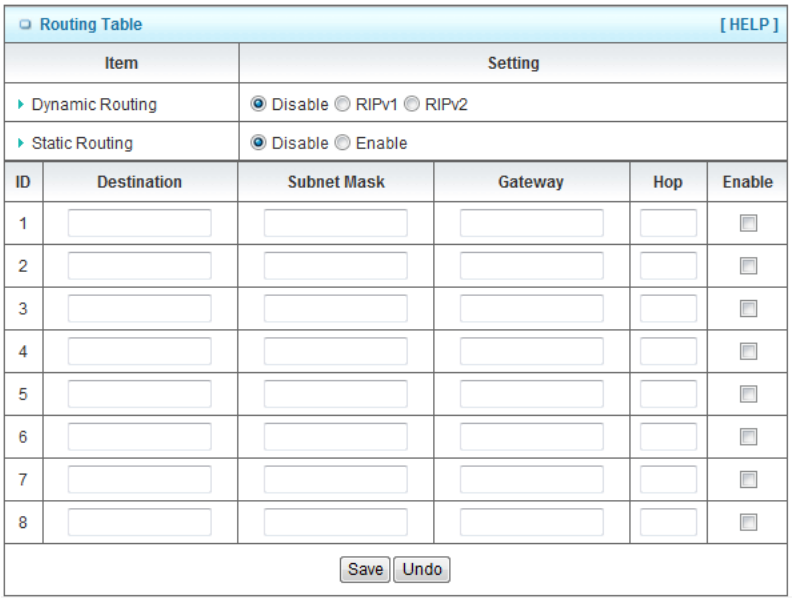


1. **Enable SNMP**
   You must check "**Local**", "**Remote**" or both to enable SNMP function. If "**Local**" is checked, this device will response request from LAN. If "Remote" is checked, this device will response request from WAN.
2. **Get Community**
   The community of GetRequest that this device will respond.
3. **Set Community**
   The community of SetRequest that this device will accept.
4. **IP 1, IP 2, IP 3, IP 4**
   Enter the IP addresses of your SNMP Management PCs. User has to configure to where this device should send SNMP Trap message.
5. **SNMP Version**
   Select proper SNMP Version that your SNMP Management software supports.
6. **WAN Access IP Address**
   If you want to limit the remote SNMP access to specific computer, please enter the PC's IP address. The default value is 0.0.0.0, and it means that any internet connected computer can get some information of the device with SNMP protocol.

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

3.5.5 Routing

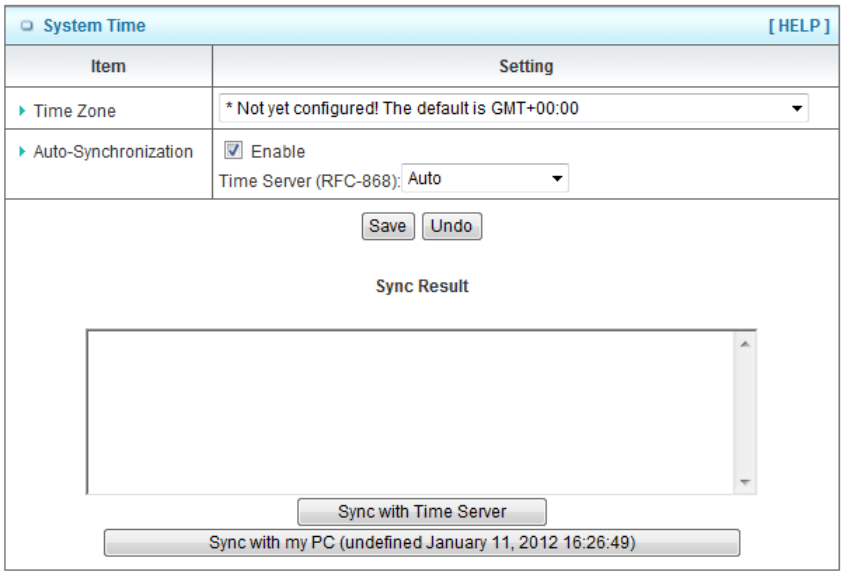
If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other. The routing table allows you to determine which physical interface address to use for outgoing IP data grams.



1. **Dynamic Routing**
   Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnet in your network. Otherwise, please select RIPv1 if you need this protocol.
2. **Static Routing**
   For static routing, you can specify up to 8 routing rules. You can enter the **destination IP address**, **subnet mask**, **gateway**, and **hop** for each routing rule, and then enable or disable the rule by checking or un-checking the Enable checkbox.

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

3.5.6 System Time

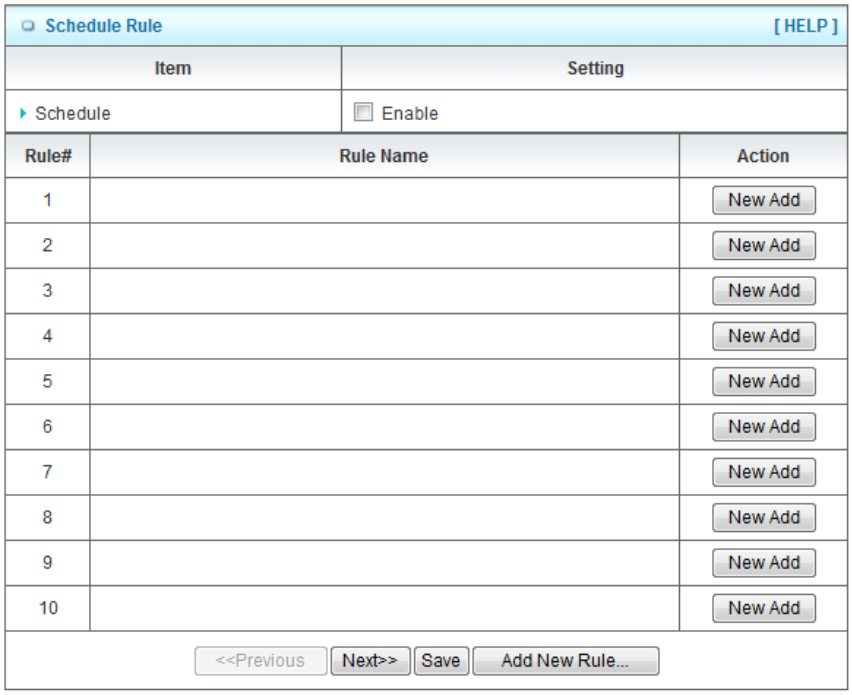


1. **Time Zone**
   Select a time zone where this device locates.
2. **Auto-Synchronization**
   Check the "**Enable**" checkbox to enable this function. Besides, you can select a NTP time server to consult UTC time.
3. **Sync with Time Server**
   Click on the button if you want to set Date and Time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

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

3.5.7 Scheduling

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

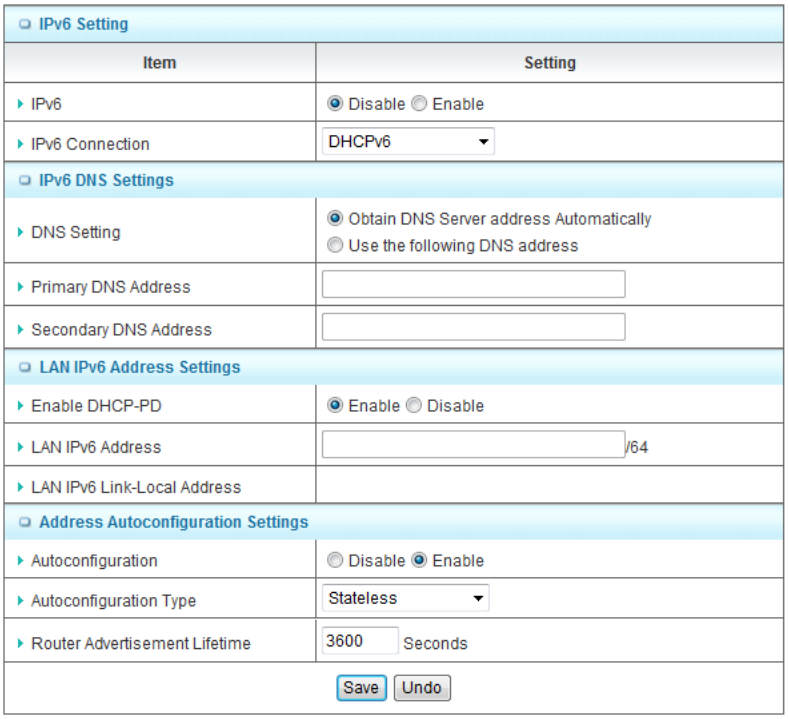


1. **Schedule**
   Check to enable the schedule rule settings.
2. **Add New Rule**
   To create a schedule rule, click the "**Add New Rule"** button. You can edit the **Name of Rule**, **Policy**, and set the schedule time (**Week day**, **Start Time**, and **End Time**). The following example configures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

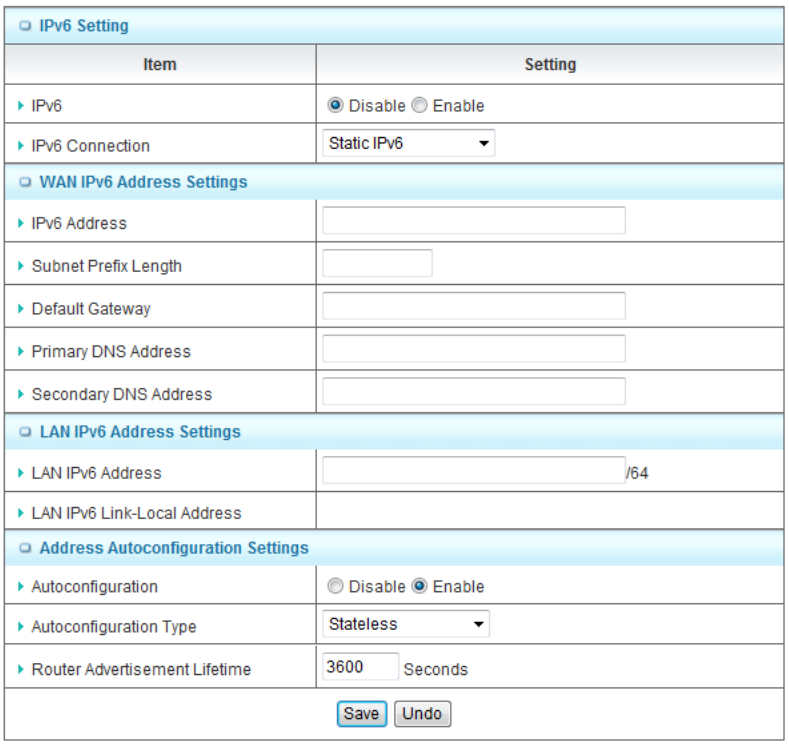
Click on "**Save**" to store your settings or click "**Undo**" to give up the changes.

3.5.8 IPv6

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

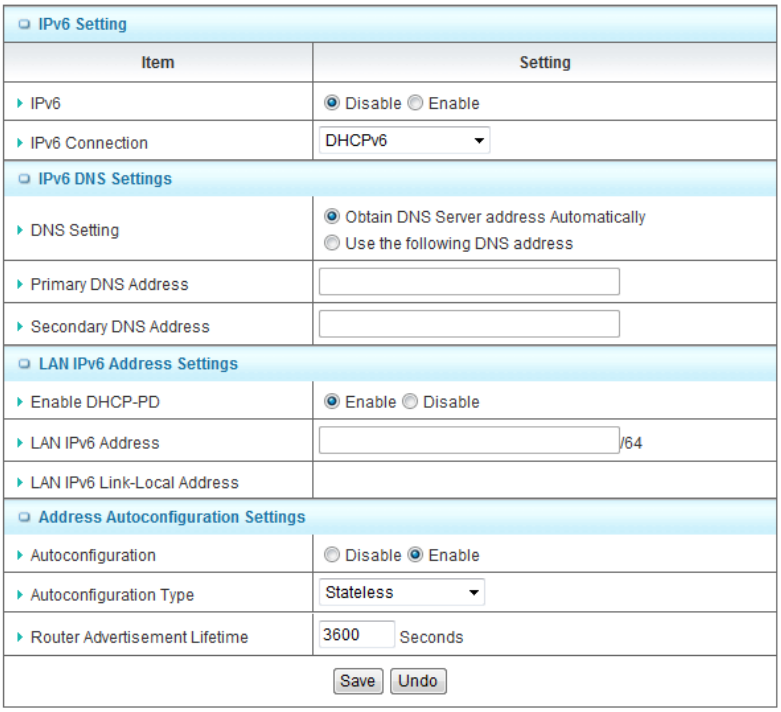


(A) Static IPv6



1. **IPv6**
   Disable or enable the IPv6 functions.
2. **IPv6 Connection**
   You can choose Static IPv6 from the list.
3. **WAN IPv6 address settings**
   You can add IPv6 address / subnet prefix length / default Gateway / Primary DNS address and secondary DNS address.
4. **LAN IPv6 address settings**
   You can add LAN IPv6 address, and IPv6 Link-Local address will be showed automatically.
5. **Address auto configuration setting**
   Disable or enable this auto configuration setting. You may set stateless or stateful(Dynamic IPv6), and also check if need to send Router advertisement messages periodically.

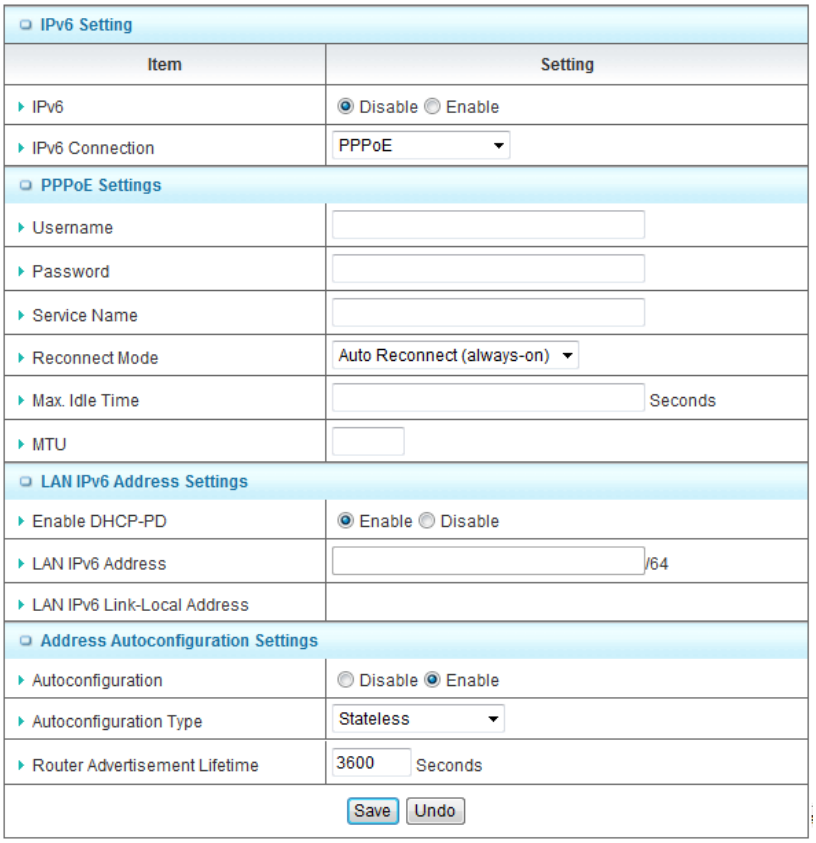
(B) DHCPv6



1. **IPv6 DNS settings**
   You may obtain IPv6 DNS automatically or set DNS address manually for Primary DNS address and secondary DNS address.
2. **LAN IPv6 address settings**
   You can add LAN IPv6 address, and IPv6 Link-Local address will be showed automatically.

3. Address auto configuration setting
Disable or enable this auto configuration setting. You may set stateless or stateful (Dynamic IPv6), and also check if need to send Router advertisement messages periodically.

(C) PPPoEv6

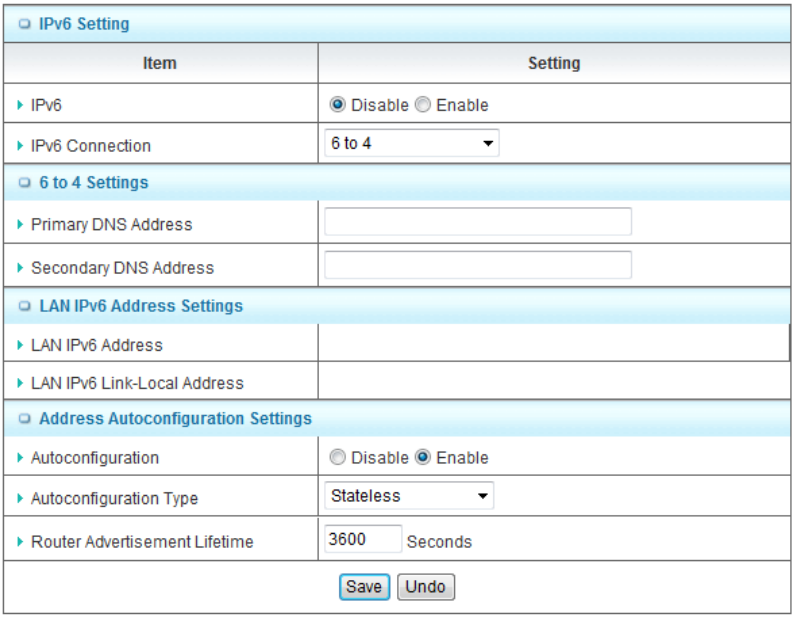


1. PPPoE settings
You need to type username and password of PPPoE connection. The service name is only required when ISP asks you to input it. MTU is 1492 by default.

2. LAN IPv6 address settings
You can add LAN IPv6 address, and IPv6 Link-Local address will be showed automatically.

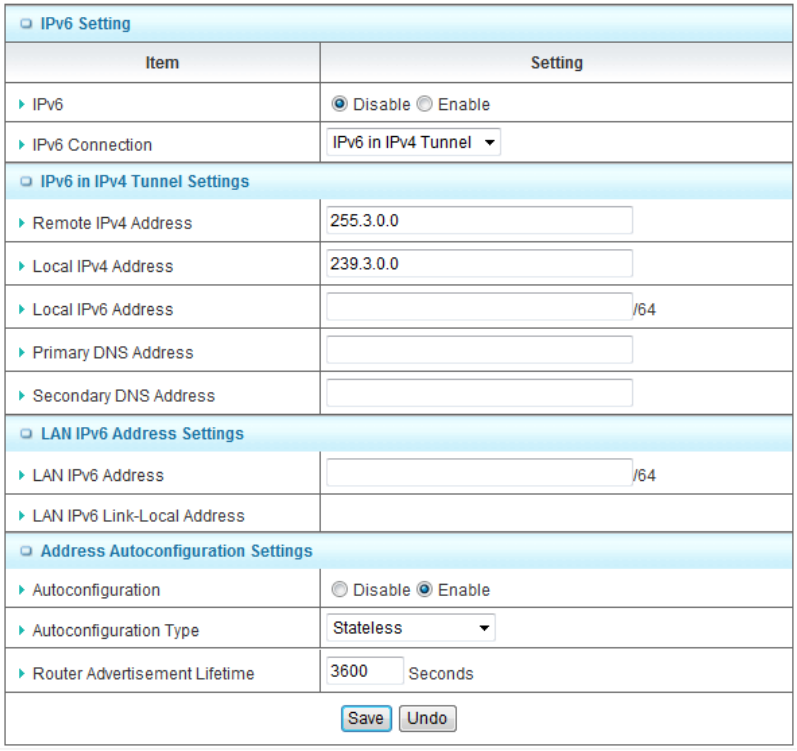
3. Address auto configuration setting
Disable or enable this auto configuration setting. You may set stateless or stateful (Dynamic IPv6), and also check if need to send Router advertisement messages periodically.

(D) 6 to 4



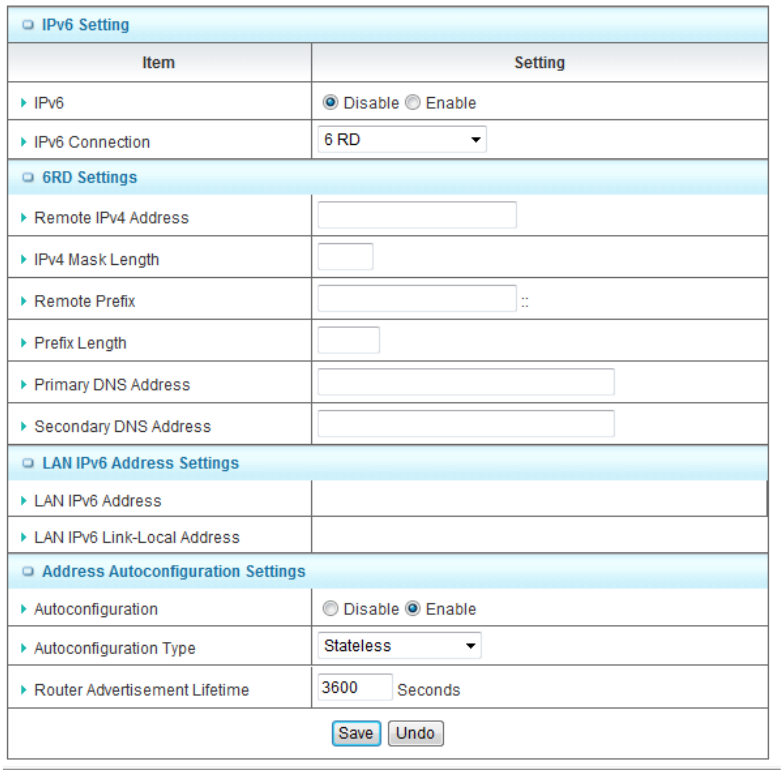
1. **IPv6 DNS settings**
   The 6 to 4 address will be showed automatically when WAN gets a public IPv4 address. You may set DNS address manually for Primary DNS address and secondary DNS address.
2. **LAN IPv6 address settings**
   You can add LAN IPv6 address, and IPv6 Link-Local address will be showed automatically.
3. **Address auto configuration setting**
   Disable or enable this auto configuration setting. You may set stateless or stateful (Dynamic IPv6), and also check if need to send Router advertisement messages periodically.

(E) IPv6 in IPv4 Tunnel



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

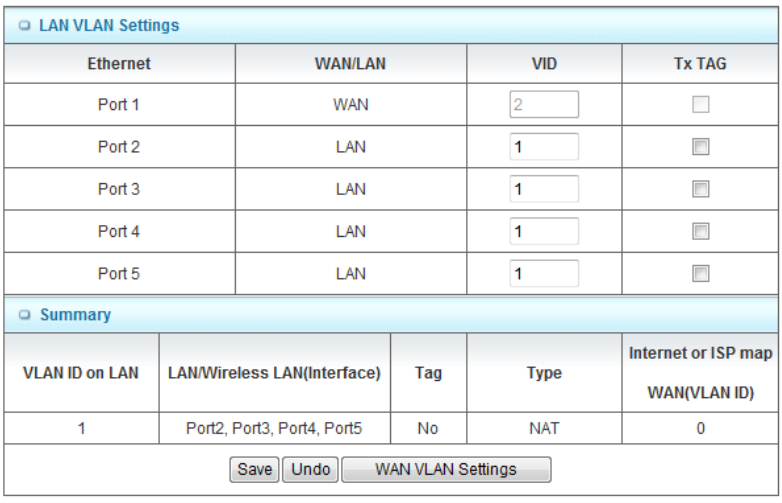
(F) 6 RD



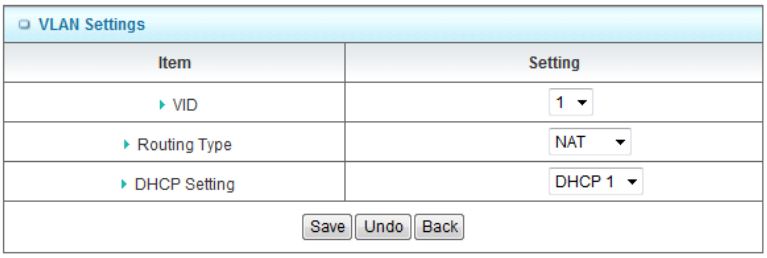
3.5.9 VLAN

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

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



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

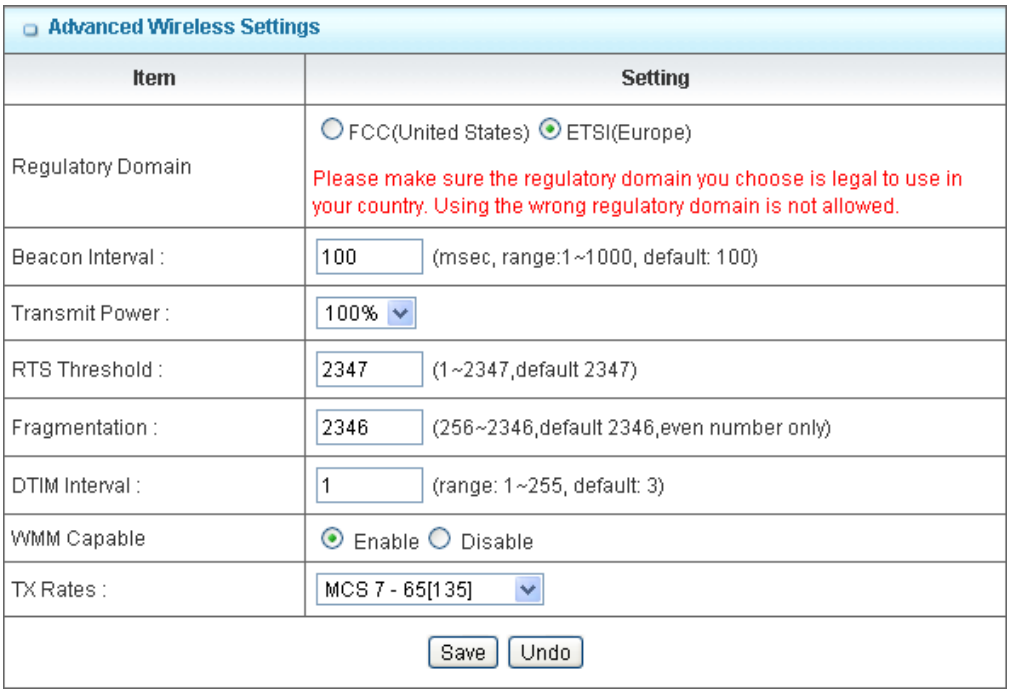


1. **VID**
   Select which VID you want to configure.
2. **LAN Status and DHCP Select**
   Tthere are two options: NAT or Bridge.

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

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

3.5.10 Advanced Wireless Settings

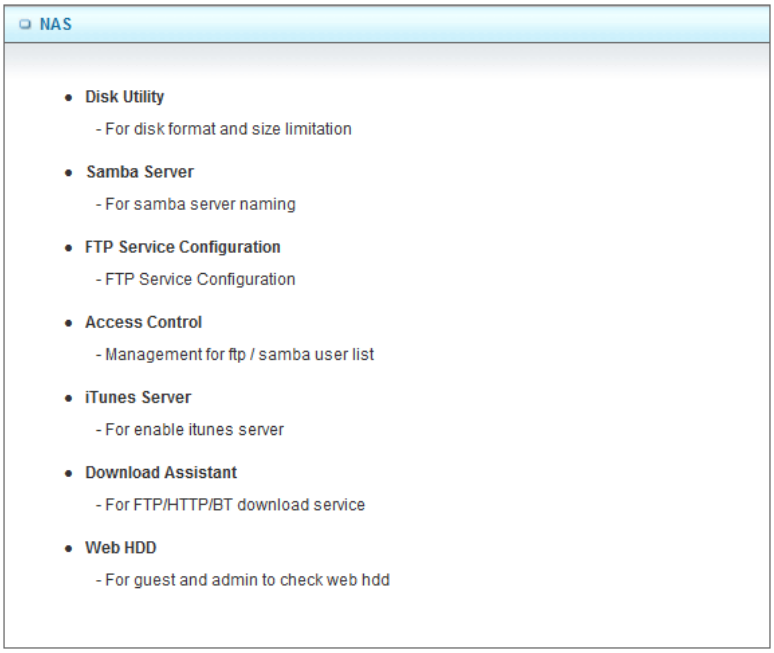


1. **Regulatory Domains**
   The legal frequency and channels varies between countries. Please select one which is allowed in your country.

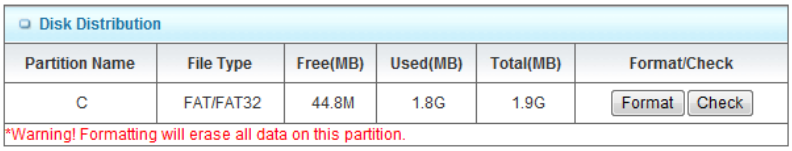
2. **Beacon Interval**
   The device broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 1000.
3. **Transmit Power**
4. **RTS Threshold**
   RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.
5. **Fragmentation**
   When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of 2346. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.
6. **DTIM interval**
   The AIRMAX5 buffers packets for stations that operate in the power-saving mode. The Delivery Traffic Indication Message (DTIM) informs such power-conserving stations that there are packets waiting to be received by them. The DTIM interval specifies how often the beacon frame should contain DTIMs. It should have a value between 1 to 255, with a default value of 3.
7. **WMM Capable**
   Enable or disable WMM Capable.
8. **TX Rates**
   You can adjust the transmit output power of the N450R. The higher the output power, the larger coverage N450R can deliver. However, it is advised that you use just enough output power so it will not create excessive interference for the environment. Also, using too much power at close distance can create serious performance drop due to signal distortion.

3.6 NAS

With NAS function on this device, you can share your USB drive or USB HDD via network easily. There are **Disk Utility**, **Samba Server**, **FTP Service Configuration**, **Access Control**, **iTunes Server**, **Download Assistant** and **Web HDD** options.



3.6.1 Disk Utility



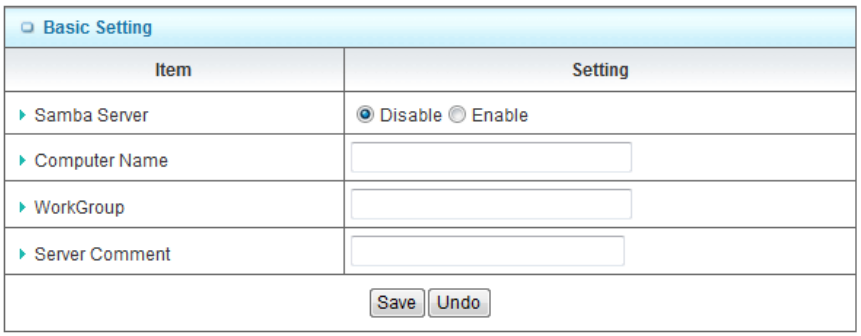
1. Format

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

2. Check

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

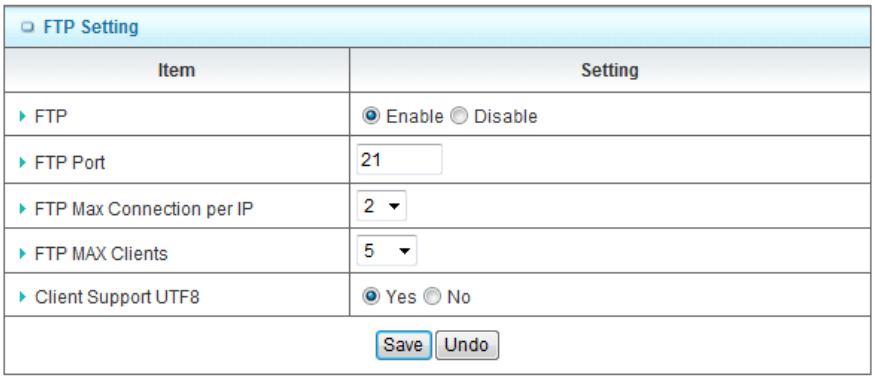
3.6.2 Samba Server



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

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

3.6.3 FTP Service Configuration

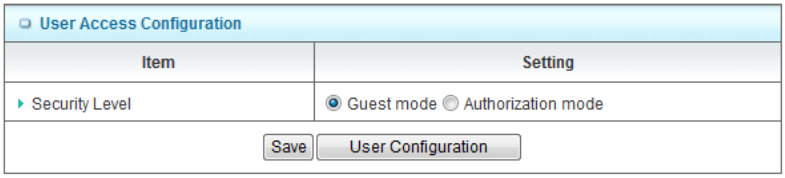


These settings are for FTP service.

1. **FTP**
   Enable or disable functions of FTP server on this device.
2. **FTP Port**
   The default port is 21, but sometimes you might want to hide your FTP service by changing it. We have the ability to receive the request on non-standard FTP port, but please be noted, some NAT router could not support non-standard FTP port, that means some of your clients might have to use passive mode to get file.

3. **FTP Max Connection per IP**
   You can limit the maximum number of FTP connection for each client.
4. **FTP MAX Clients**
   You can indicate how many FTP clients can access the FTP service on this device at the same time.
5. **Client Support UTF8**
   This option is used when your FTP client could support UTF8. Usually, the default value “No” is okay for most clients.

3.6.4 Access Control

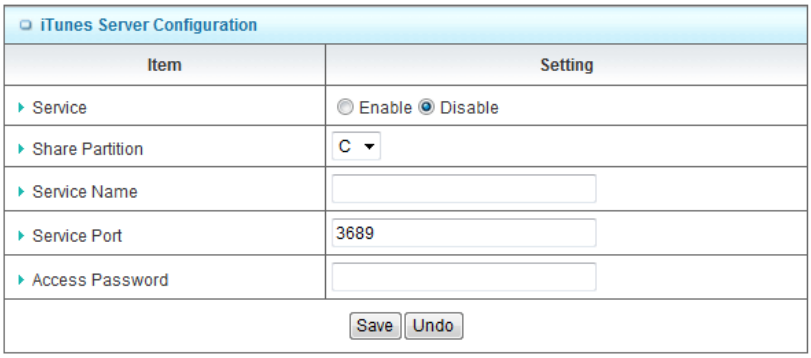


The default setting is “**Guest mode**”, all clients could access as anonymous users. If you want to control the permission, change to “Authorization mode” and save it, then go to “**User Configuration**”.

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

3.6.5 iTunes Server

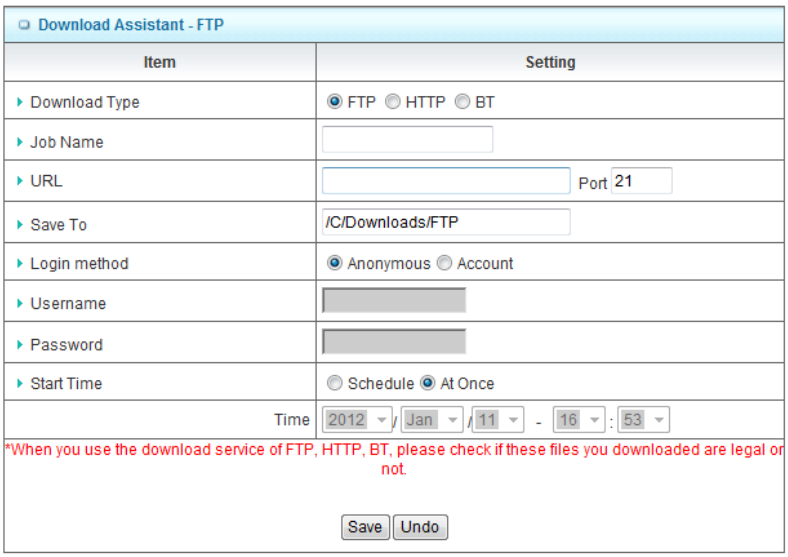
This function could enable the built-in iTunes Server to support iTunes which is a media player released by Apple.



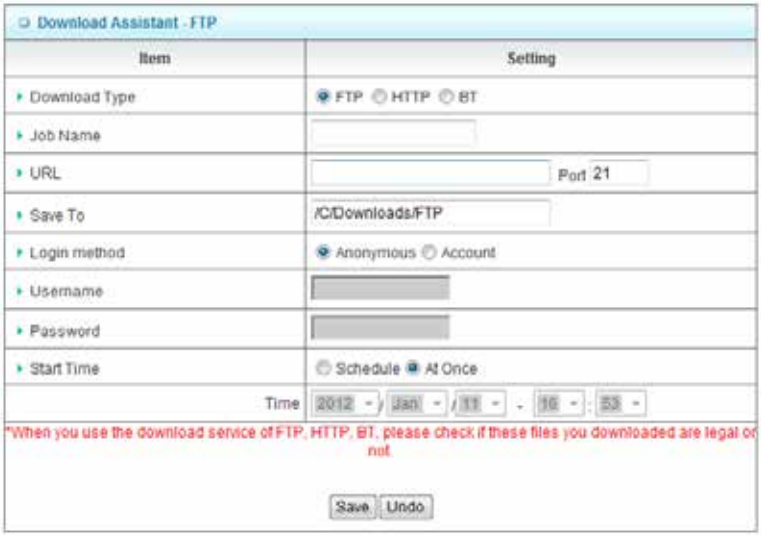
1. **Service**
   Enable or disable this function.
2. **Share Partition**
   Select which partition on USB drive that you want to share.
3. **Server Name**
   The name of this server, it will be shown on the iTunes.
4. **Service Port**
   The TCP port for WEB management interface, for example, if the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

3.6.6 Download Assistant

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



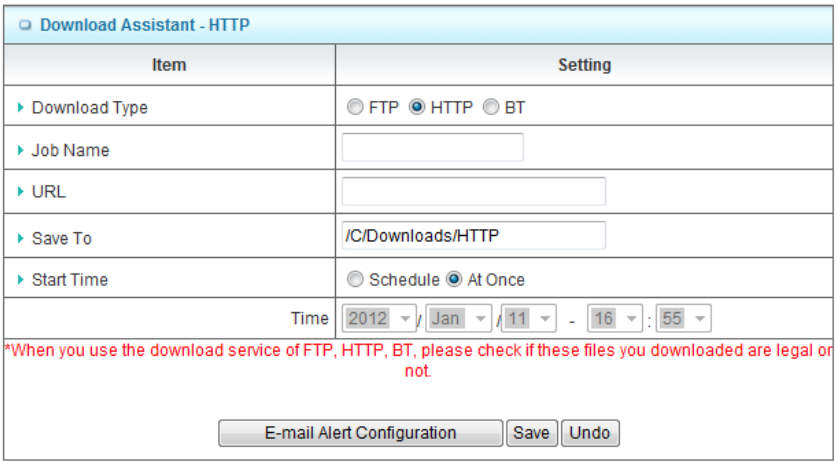
(A) FTP



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

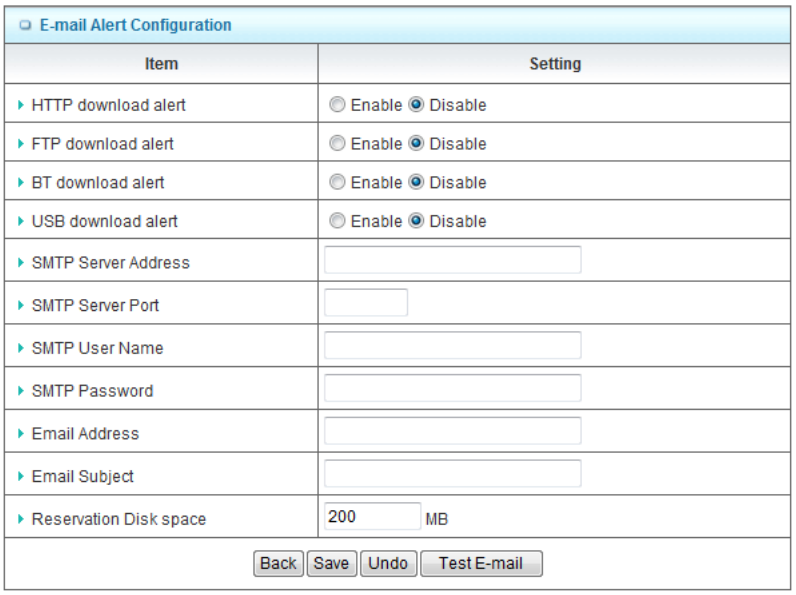
At Once: the FTP download would be started immediately.

(B) HTTP



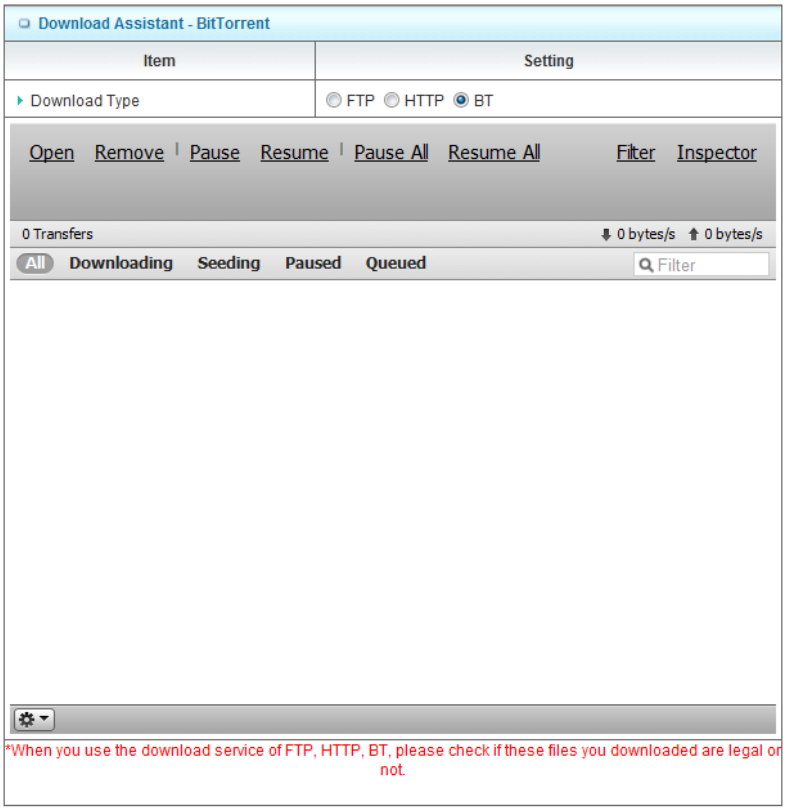
1. **Job Name**
   It's for you to remember the job easily, and the device would use this name to info you when the job is done.
2. **URL**
   The URL for the file you want to download.
   You have to use this format:
   IP/path/file, you don't have to add protocol part such like "http://".
3. **Save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

By pressing **"E-mail Alert Configuration"**,



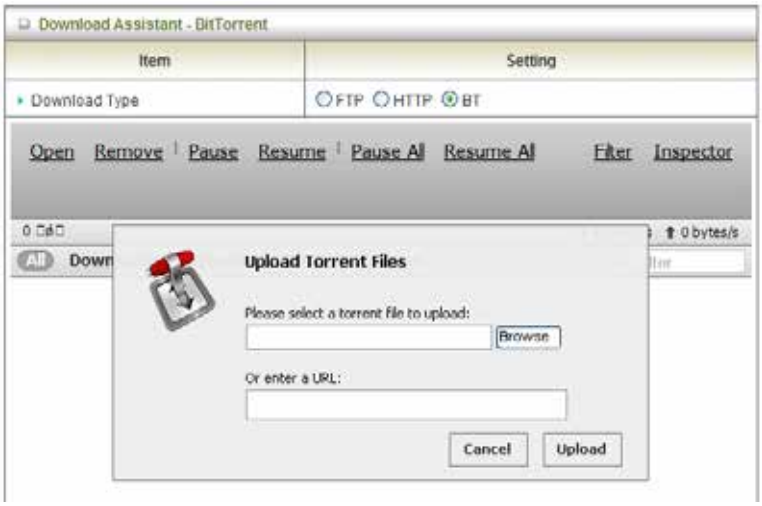
(C) BT (Bit Torrent)

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



n **Start BT download**

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



n **BT download status**

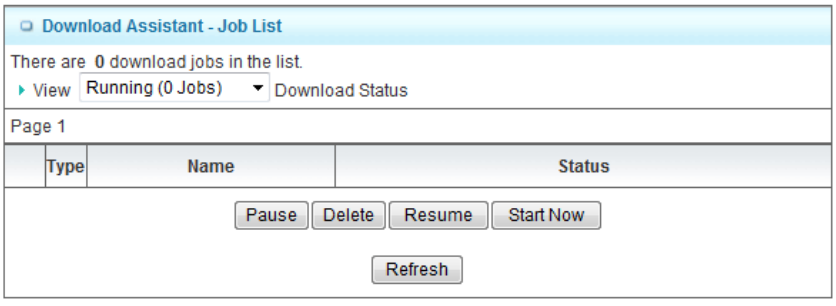
After you upload the torrent, download job would be started immediately.
The device could support 3 concurrent download jobs, other jobs would wait in job queue. If one of the three running job is done, the next new job would be started.
At this page, you could see the download process and the bandwidth.

n **Stop, Resume and Remove seed**

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

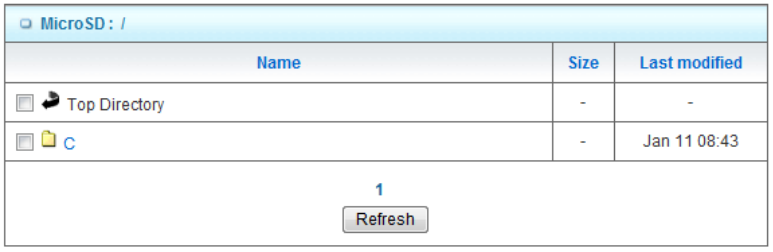
3.6.7 Download Status

Here shows all jobs for download assistant.



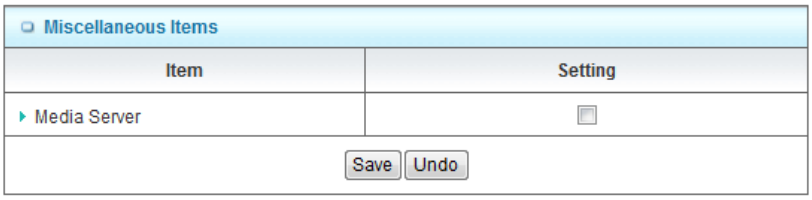
3.6.8 Web HDD

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



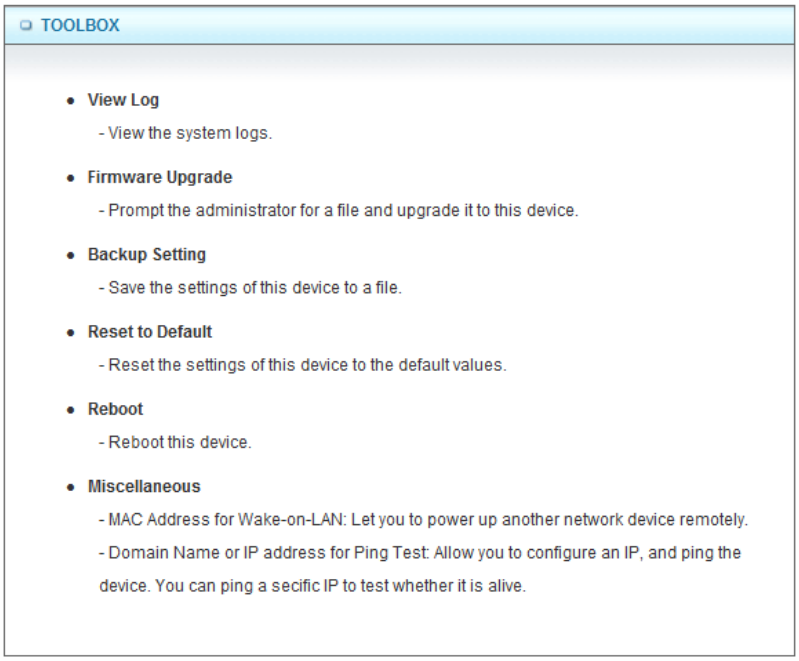
(A) Miscellaneous

This setting is for Media Server service.



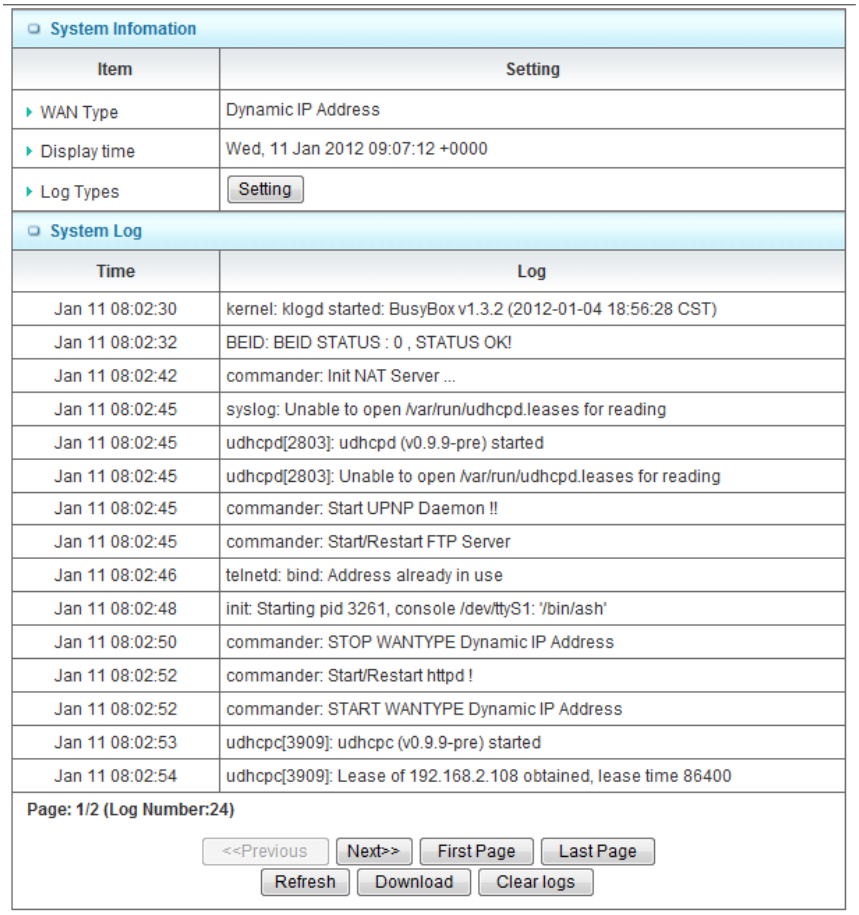
3.7 Tool Box

There are seven options: **System Log**, **Firmware Upgrade**, **Backup Setting**, and **Reset to Default**, **Reboot** and **Miscellaneous**.

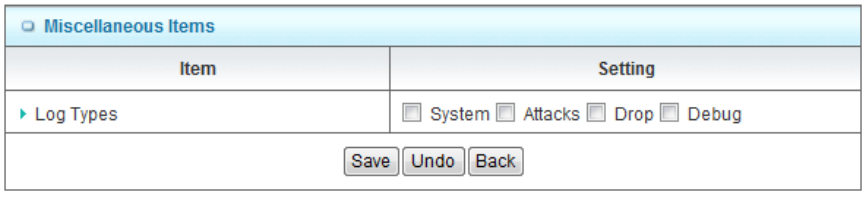


3.7.1 System Info

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



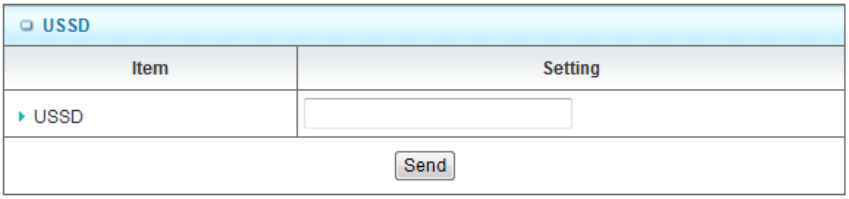
Press “**Setting**” button.



3.7.2 USSD

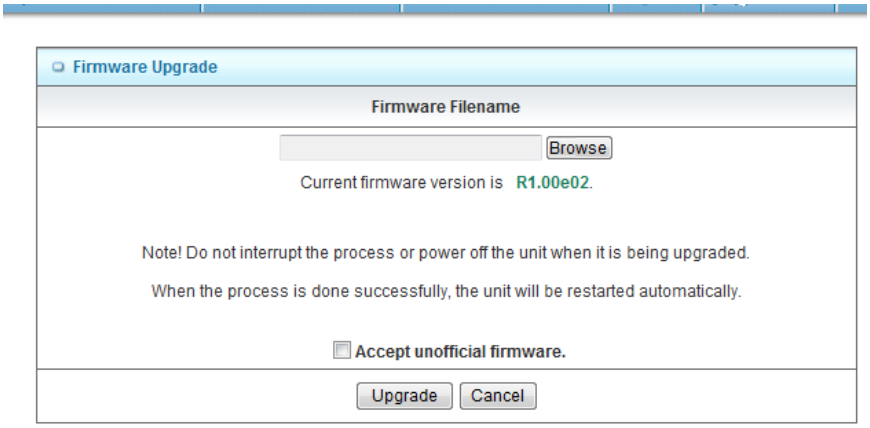
USSD is a way to let subscribers finish some application on line, such as recharge SIM card.

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

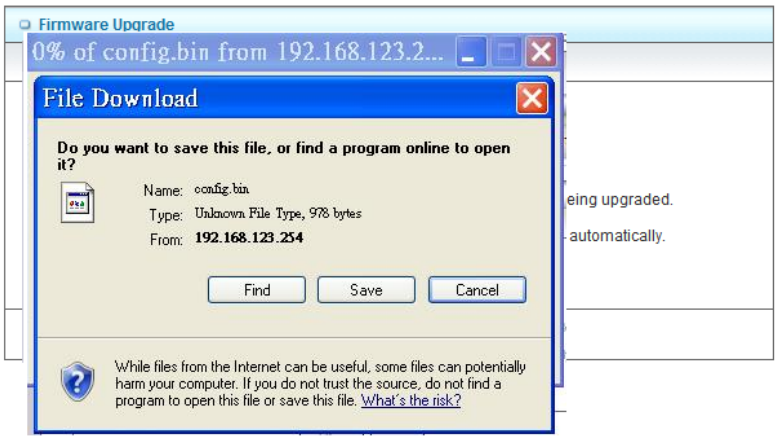


3.7.3 Firmware Upgrade

You can upgrade firmware by clicking “**Upgrade**” button.



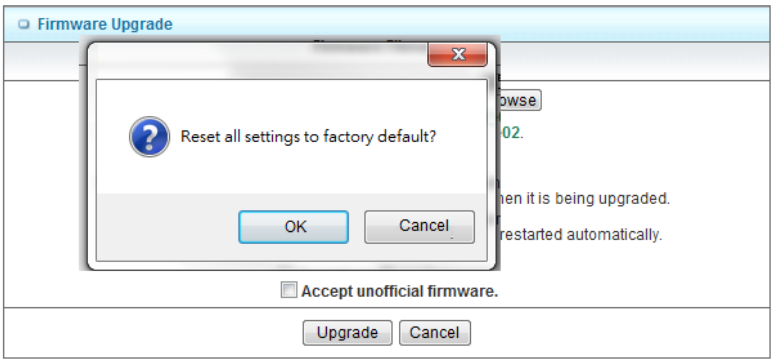
3.7.4 Backup Setting



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

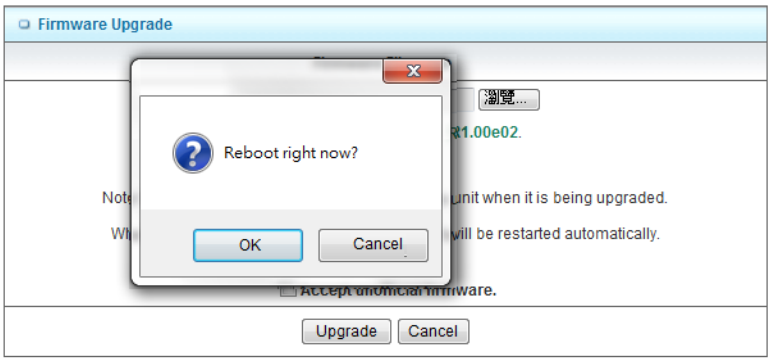
3.7.5 Reset to Default

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

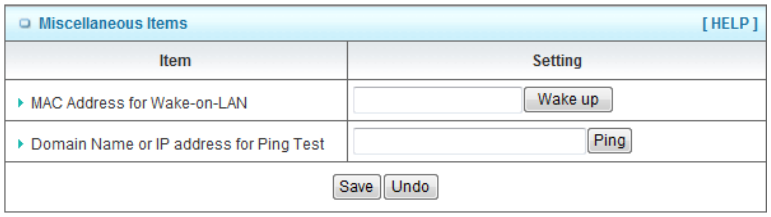


3.7.6 Reboot

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



3.7.7 Miscellaneous – Wake on LAN & Ping



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, 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.

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

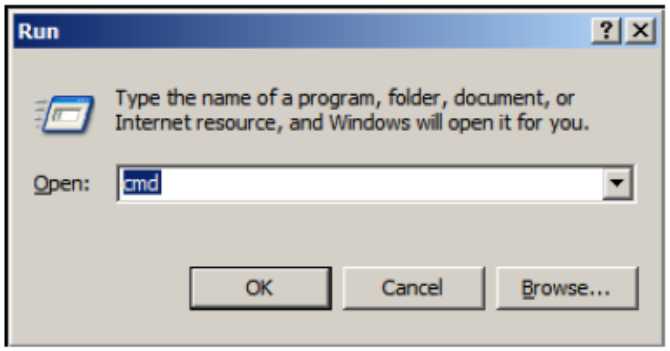
A Appendix A: Troubleshooting

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

A:

Do a **Ping test** to make sure that the router is responding.

1. Go to Start > Run.
2. Type **cmd**.



3. Press **OK.**
4. Type **ipconfig** to get the IP of default gateway.
5. Type "**ping 192.168.1.254".** Assure that you ping the correct IP Address assigned to the router. It will show four replies if you ping correctly.

```
Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
```

6. 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.
7. Go to **Start** > Right click on "**My Computer**" > **Properties**.
8. Select the **Hardware** Tab.
9. Click **Device Manager**.
10. Double-click on "**Network Adapters"**.
11. Right-click on Wireless Card bus Adapter or your specific network adapter.
12. Select **Properties** to ensure that all drivers are installed properly.

13. Look under **Device Status** to see if the device is working properly.
14. Click "**OK"**.

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

A:

Make sure the RJ45 cable connects with the router.

1. Ensure that the setting on your Network Interface Card adapter is "**Enabled**".
2. 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.
3. If the connection still doesn't work properly, then you can reset it to default.

Q: Something wrong with the wireless connection?

A:

1. **Can't setup a wireless connection?**
   - Ensure that the SSID and the encryption settings are exactly the same to the Clients.
   - Move the WiFi Combo Router and the wireless client into the same room, and then test the wireless connection.
   - Disable all security settings such as **WEP**, and **MAC Address Control**.
   - Turn off the WiFi Combo Router and the client, then restart it and then turn on the client again.
   - Ensure that the LEDs are indicating normally. If no, make sure that the AC power and Ethernet cables are firmly connected.
   - Ensure that the IP Address, subnet mask, gateway and DNS settings are correctly entered for the network.
   - 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.
2. **What can I do if my wireless client can not access the Internet?**
   - Out of range: Put the router closer to your client.
   - Wrong SSID or Encryption Key: Check the SSID or Encryption setting.
   - Connect with wrong AP: Ensure that the client is connected with the correct Access Point.

(A) **Right-click** on the **Local Area Connection icon** in the taskbar.
(B) Select **View Available Wireless Networks in Wireless Configure**. Ensure you have selected the correct available network.
(C) Reset the WiFi Combo Router to default setting

3. **Why does my wireless connection keep dropping?**
   - Antenna Orientation.

(A) Try different antenna orientations for the WiFi Combo Router.
(B) Try to keep the antenna at least 6 inches away from the wall or other objects.
(C) Try changing the channel on the WiFi Combo Router, and your Access Point and Wireless adapter to a different channel to avoid interference.

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

Q: What to do if I forgot my encryption key?

A:

1. **Go to the Wireless Advanced setting to setup the encryption key again.**
2. Reset the router to default setting

Q: How to reset to default?

A:

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

Q: Problems with 3G connection?

A:

1. **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.
2. **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.
3. **What can I do if my 3G connection is failed even the dongle is plugged?**
   Please check the following items:
4. Make sure you have inserted a validated SIM card in the 3G data card, and the subscription from ISP is still available
5. If you activate PIN code check feature in SIM card, making sure the PIN code you fill in dial-up page is correct
6. Checking with your ISP to see all dial-up settings are correct
7. Make sure 3G signal from your ISP is available in your environment
8. **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.
9. **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.
10. **Which 3G network should I select?**
    It depends on what service your ISP provide. Please check your ISP to know this information.
11. **Why my 3G connection is keep dropping?**
    Please check 3G signal strength from your ISP in your environment is above middle level.

Q: How to configure the iTunes Server?

A:

Step1

Please check the USB HDD has installed to N450R properly.

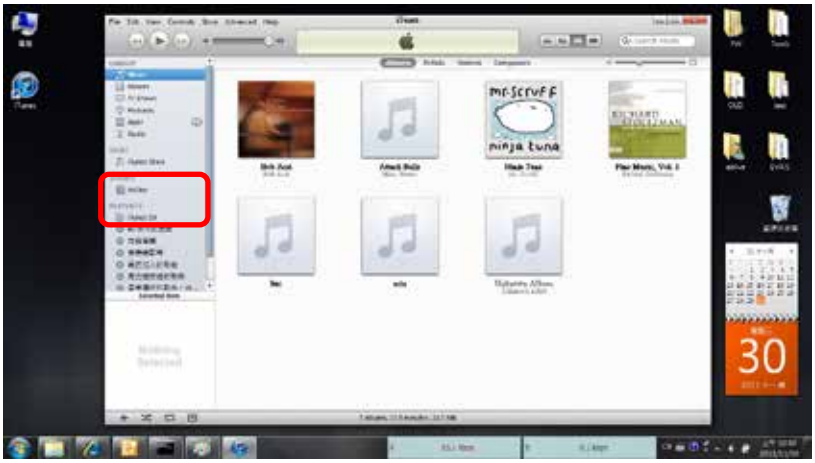
Step2

Click iTunes Server, then enable iTunes Sever, type-in Service Name, Service Port and Access password. Click “Save” to apply settings.

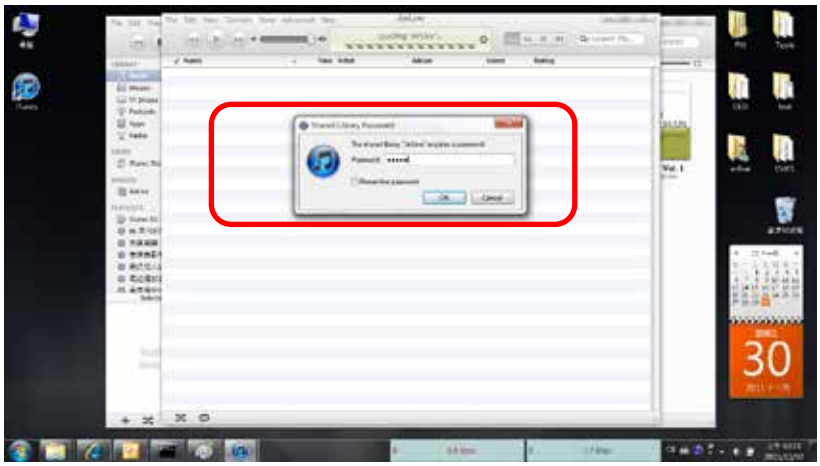
Step3: Click Web HDD, and then click “C” to check whether music file in the folder.

Step4: Start iTunes player on your PC.

Step5: There will appear a shared folder: AirLive, which you create



Step6: Please type the login password.



Step7: The music files will appear, click on the song to start to play.