Air Live®
Powered by OvisLink Corp.

WN-220ARM

Wireless 11N 150Mbps ADSL2+M Router

User's Manual

www.airlive.com

Copyright

Trademarks

All products, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior not

FCC Interference Statement

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

CE Declaration of Conformity

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

Table of Contents

1 Introduction

1.1 Overview

AirLive WN-220ARM is the center of your home or office network, you can share a high –speed Internet connection, files, and multi - player games with the flexibility, speed, security and simplicity! The WN-220ARM ties functions All-in-one of wireless 150Mbps 11n-lite networking technology.

AirLive WN-220ARM also a built - in 4- port full - duplex 10/100Mbps Switch to connect you're wired - Ethernet devices together. Finally, the Router function ties it all up and lets your whole network shares a high – speed cable or DSL Internet connection.

Wireless High-Speed 150Mbps and high speed DSL lead you to enjoy various applications. Seamlessly work with X-Box360, online game and download application or IPTV streaming.

The QoS (Quality of Service) feature allows prioritizing the different package according the 802.11e WMM protocol and triple play (Voice, Video and Data) automatically. The AirLive WN-220ARM also provides the capability to control total bandwidth or limit the bandwidth by application. Therefore, the administrator can setup different class of connection speeds for different applications.

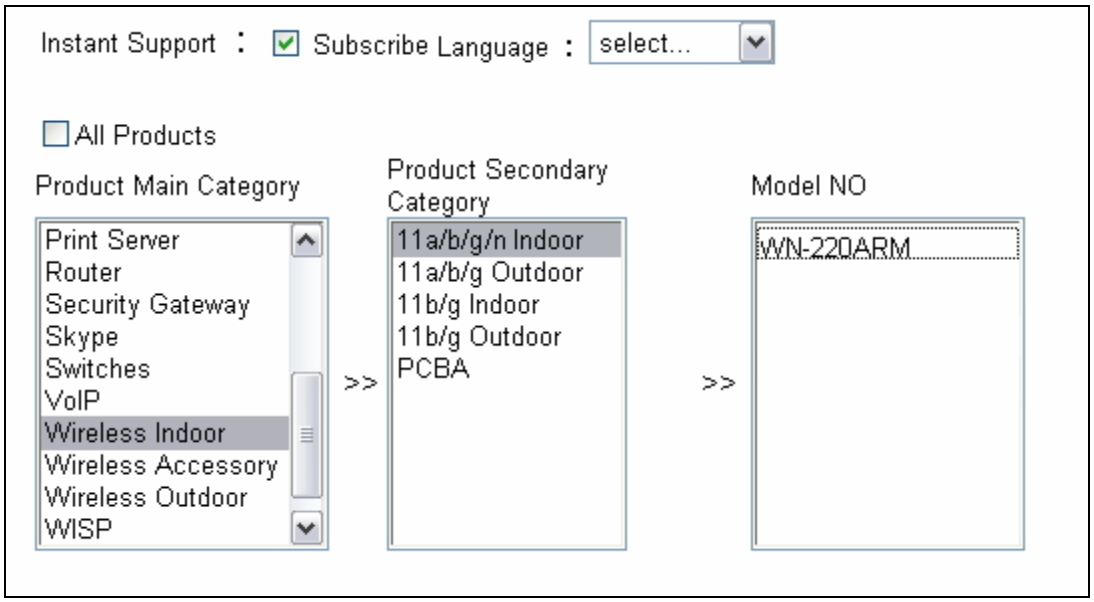
1.2 Features

If you encounter a technical issue that cannot 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 firmware that either increase software functions or provide bug fixes for WN-220ARM. 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



1.3 Product Overview

- Enjoy Your AirLive Wireless
- Compatible with AirLive Wireless IP Camera
- Green WLAN for Smart Power Saving
- Support Easy Setup Wizard
- TR069 Remote Management
- IPv6 support

1.4 Packing List

- WN-220ARM
- 2dbi antenna
- Power Adapter
- CD
- QIG

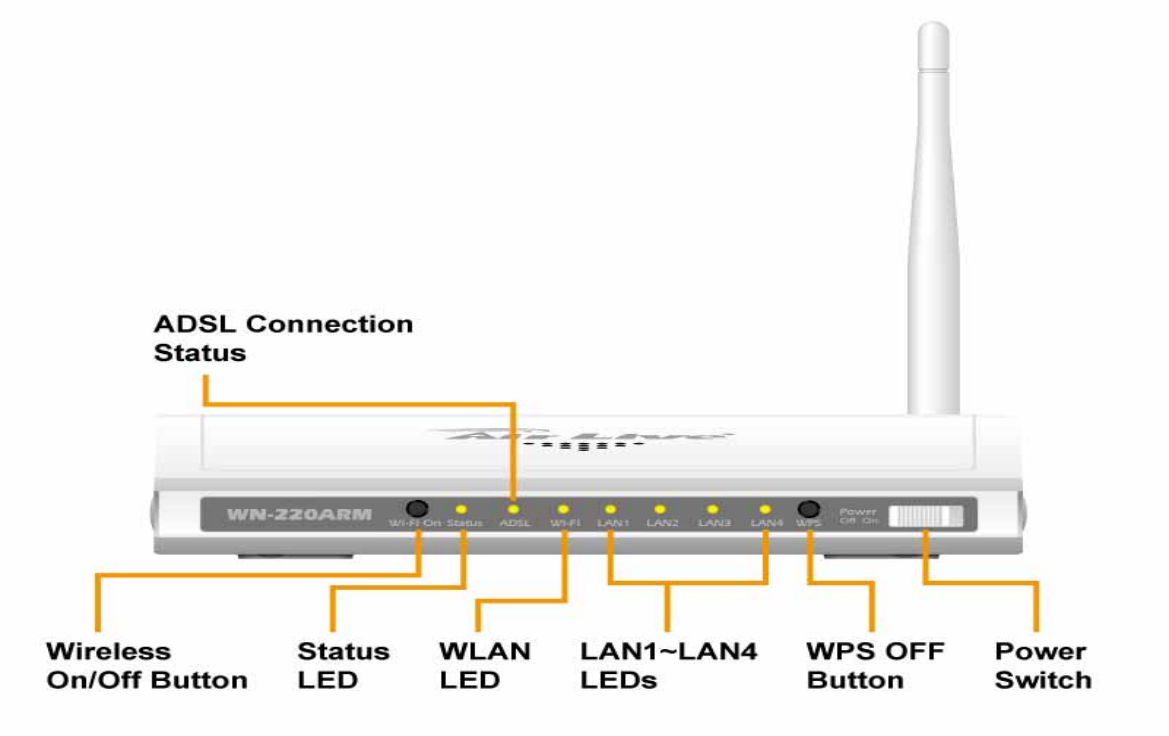
1.5 Specification Table

Device Interface		
ADSL Line	ADSL port (Annex A)	1
ADSL2 /2+ Standard Module	1-port ADSL2+ connector ITU 992.1 (G.dmt) Annex A, ITU 992.2 (G.lite), ITU 992.3 ADSL2 (G.dmt.bis), ITU 992.5 ADSL2+	●
Ethernet LAN	RJ-45 port, 10/100Mbps, auto-MDI/MDIX	4
Antenna	For 2.0 dBi Fixed antenna	1
WPS Button	For WPS connection	1
Wireless On/Off Button	Enable /Disable Wireless Radio	1
LED Indication	Status/ ADSL/ LAN1 ~ LAN4/ WiFi	●
Power Jack	DC Power Jack and switch, powered via external DC 12V/0.6A switching power adapter	1

Wireless LAN (WiFi)		
Standard	IEEE 802.11b/g/n (1x1) 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		
ADSL WAN	PPPoE / PPPoA / IPoA / Static IP / Dynamic IP	●
WAN Connection	Auto-reconnect, dial-on-demand, manually	●
IPv6 support	Dual stack IPv6 support	●
One-to-Many NAT	Virtual server, special application, DMZ, Super DMZ (IP pass through) And IPTV IGMP V1 V2 Pass through	●
NAT Session	Support NAT session	8000
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)	●
Ovislink IPcam support	Ovislink IPcam support	●
Remote management	TR069 (2-wire/ Motive)	●
Management	SNMP, UPnP IGD, syslog	●
Administration	Web-based UI, remote login, backup/restore setting	●
Environment & Certification		
Package Information	Package dimension (mm)	
	Package weight (g)	
Operation Temp.	Temp.: 0~40oC, Humidity 10%~90% non-condensing	●
Storage Temp.	Temp.: -10~70oC, Humidity: 0~95% non-condensing	●
EMI Certification	CE/FCC compliance	●
RoHS	RoHS compliance	●

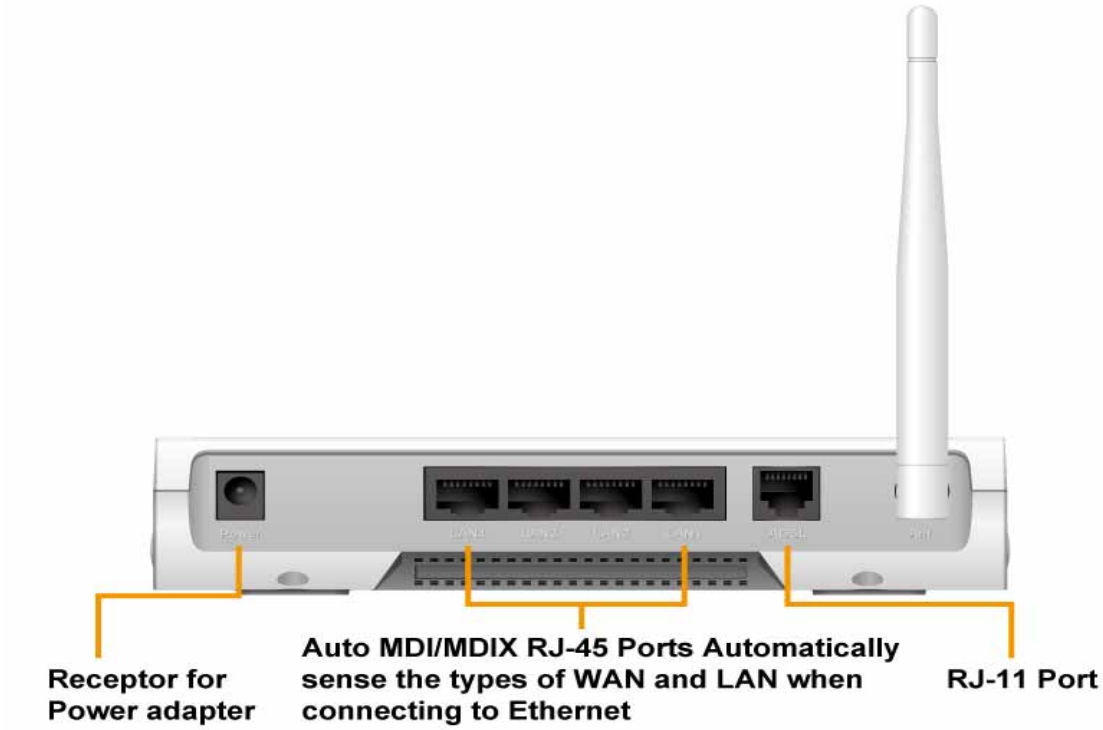
1.6 Hardware Installation

1.6.1 Front View



※ **Reset**: Press “Wireless on/off” and “WPS” button for 5 sec simultaneously.

1.6.2 Rear View



1.6.3 LED Indicators

	LED Status	Description
ADSL	Green in flash	xDSL connection is established
	Green in fast flash	Data packet transferred via DSL Line
WLAN	Green	WiFi is on.
	Green in flash	Data access
LAN	Green	RJ45 cable is plugged, and Ethernet connection is established.
	Green in flash	Data access

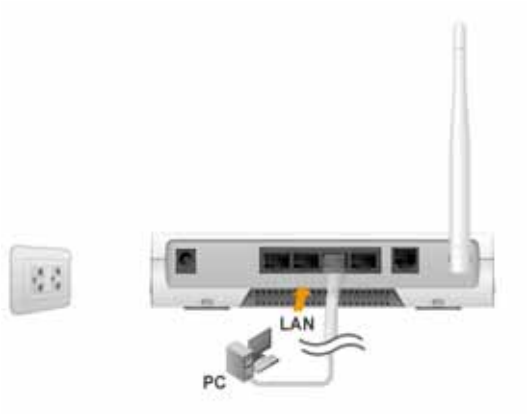
1.6.4 Button Definition

	Description
Enable "Wireless" and WPS	1. When Wireless is off, press this button (about 1 sec) to enable "Wireless Radio". 2. When Wireless is On, press this button (about 1 sec) to execute WPS function.
Reset	Press "Wireless on/off" and "WPS" button for 5 sec simultaneously.

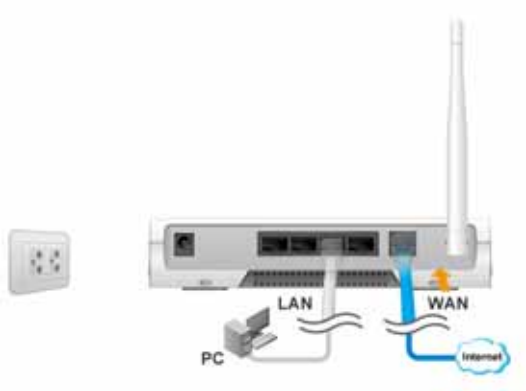
1.6.5 How to Operate

DO NOT connect WiFi Broadband Router to power before performing the installation steps below.

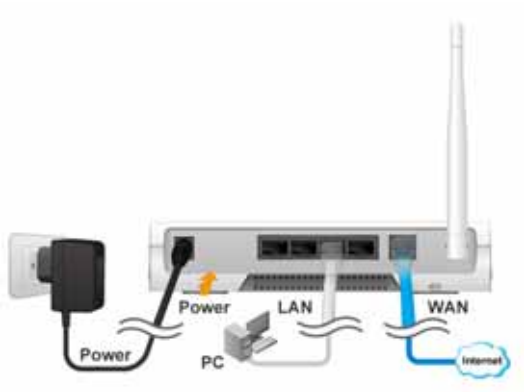
Step 1.
Plug the RJ45 cable into LAN port 1~4 and connect with your PC or NB.



Step 2.
Plug your RJ-11 into the DSL port and connect with your xDSL modem.



Step 3.
Plug the power jack into it.



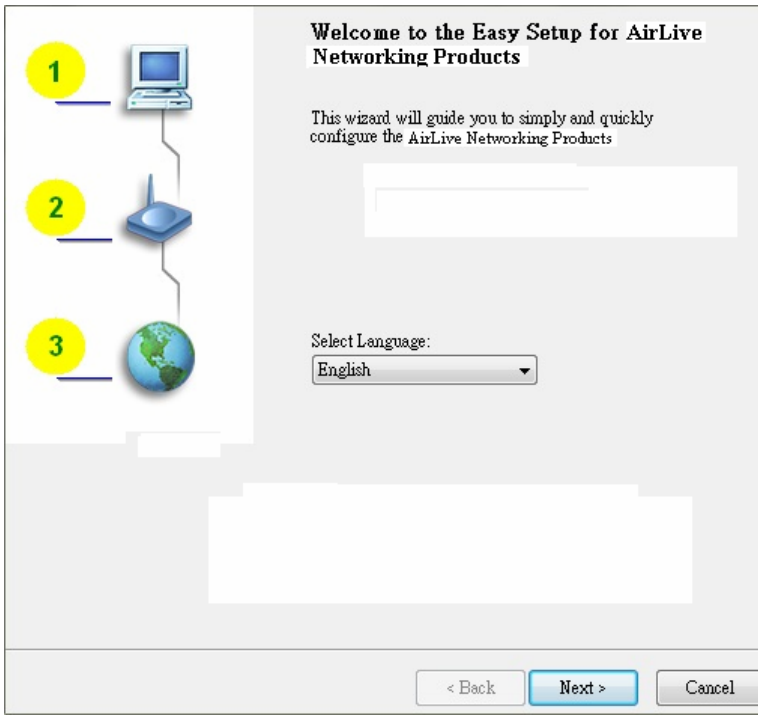
Step 4
Power ON.

2 Getting Started

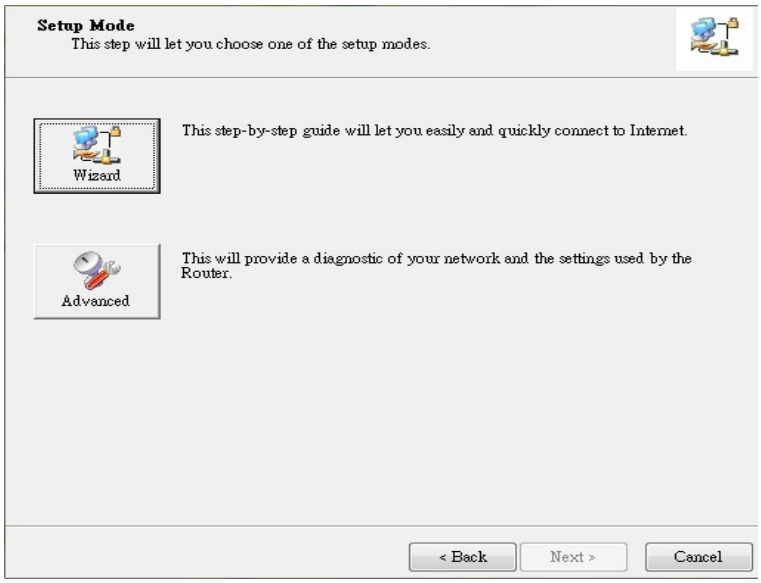
2.1 Easy Setup by Windows Utility

Step 1.
Install the Easy Setup Utility from the provided CD click the "**Start**" then follow the steps to configure the device.

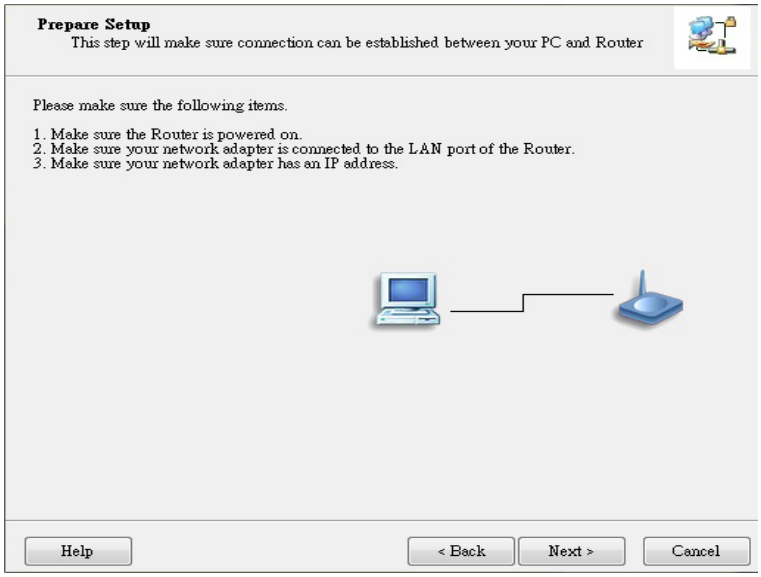
Step 2.
Select Language then click "Next" to continue.



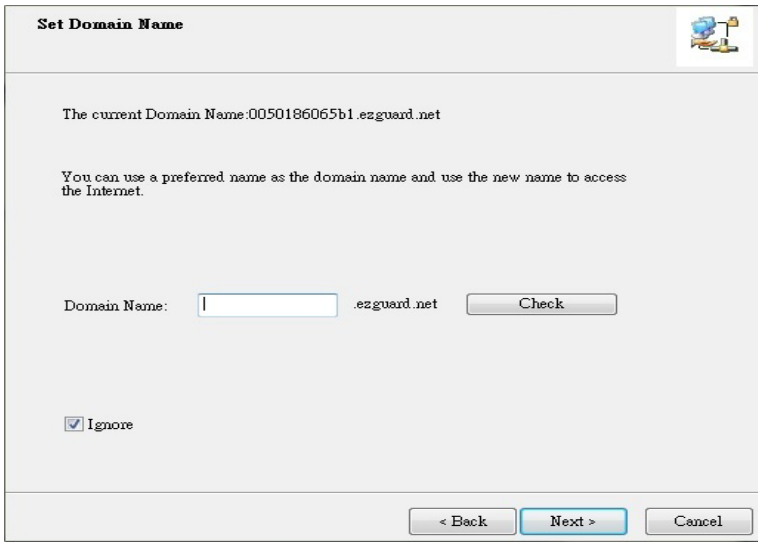
Step 3.
Then click the “Wizard” to continue.



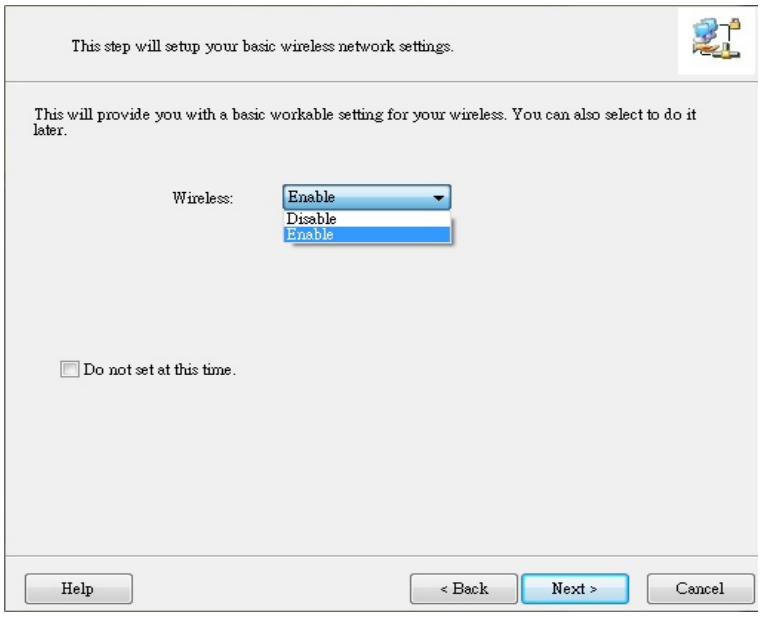
Step 4.
Click “Next” to continue.



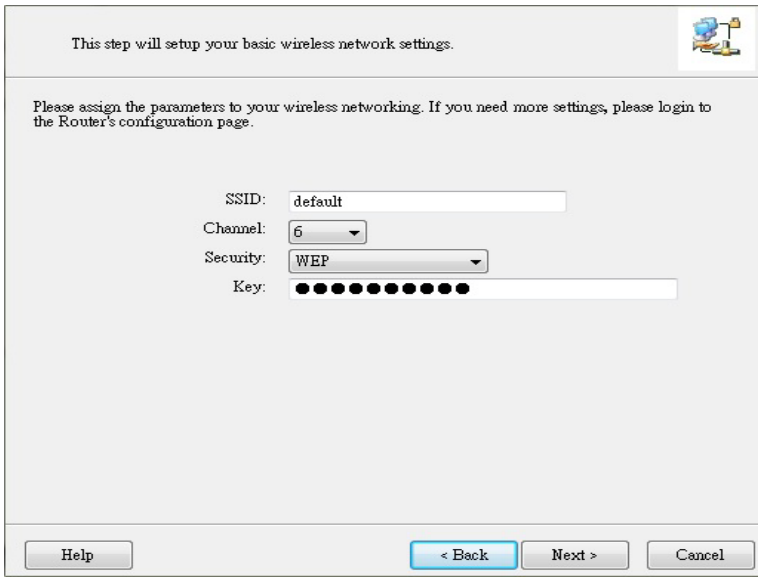
Step 5.
One free DDNS account 'MAC address.ezguard .net' for end user to access the NAS router remotely, you can rename an alias name to remember it easily. Once you type in a name, you can click 'check' to see if the name server accepts it or not. You also can click 'Ignore' to pass it.



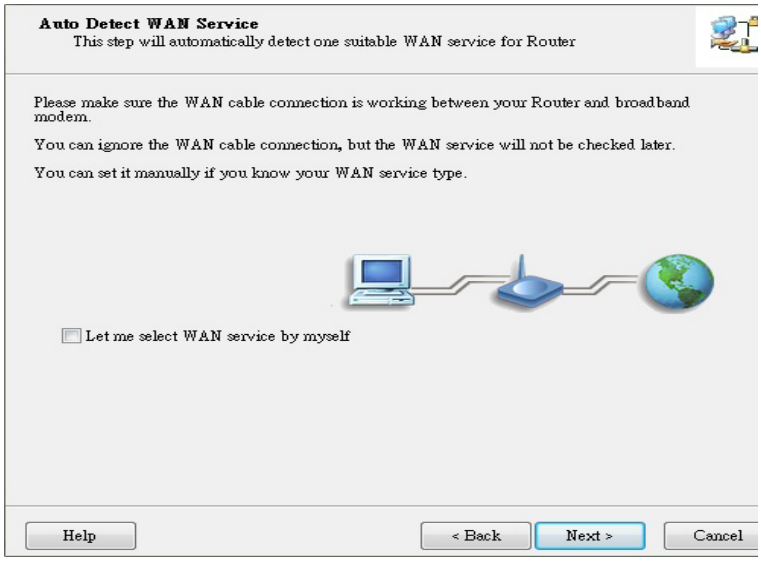
Step 6.
Select Wireless Enable, and then click "Next" to continue.



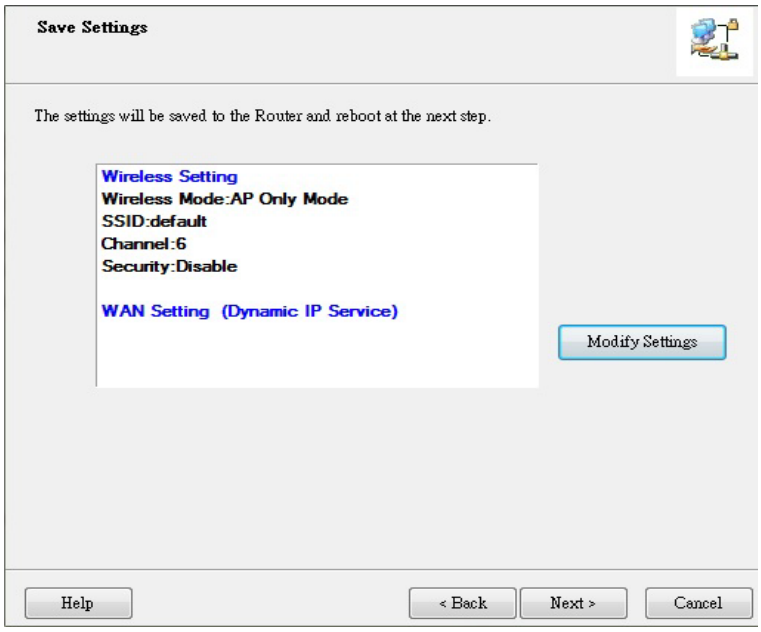
Step 7.
Enter SSID, Channel and Security options, and then click “Next” to continue.



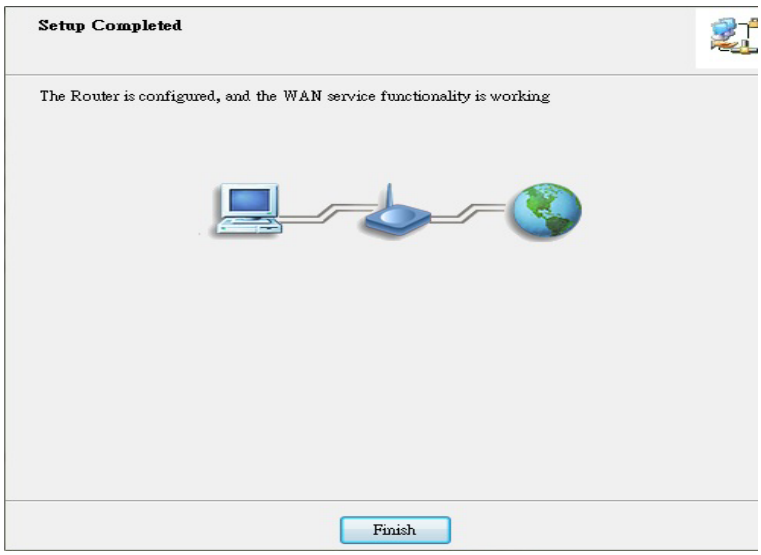
Step 8.
Select Auto Detect WAN service.



Step 9.
Save the setting.



Step 10.
Congratulations!
Setup is completed.
Now you have already connected to Internet successfully.



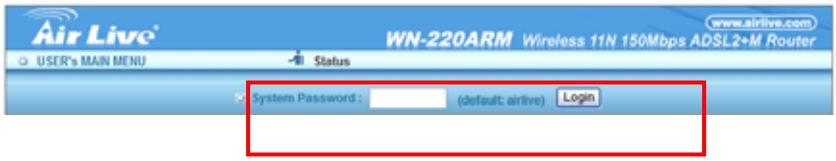
2.2 Easy Setup by Web UI

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

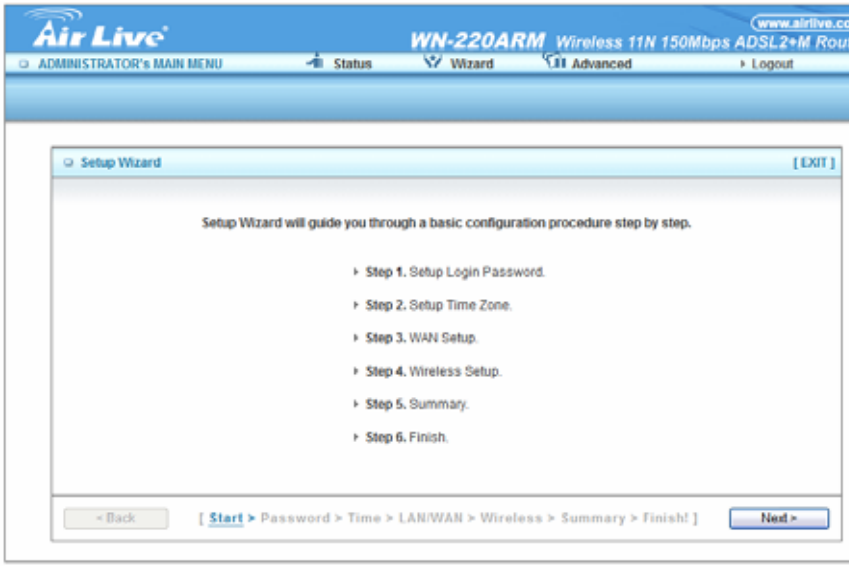
2.2.1 Browse to Activate the Setup Wizard

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

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

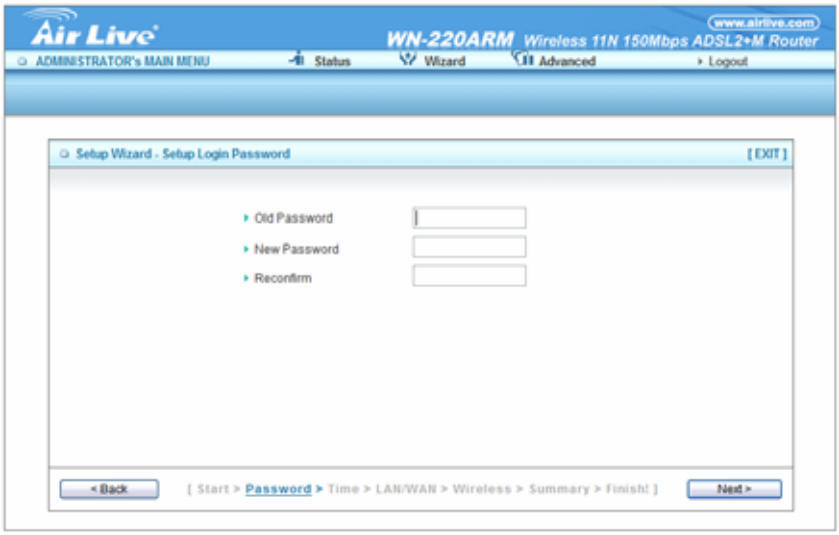


Select "Wizard" for basic settings in simple way. Press "Next" to start the Setup Wizard.

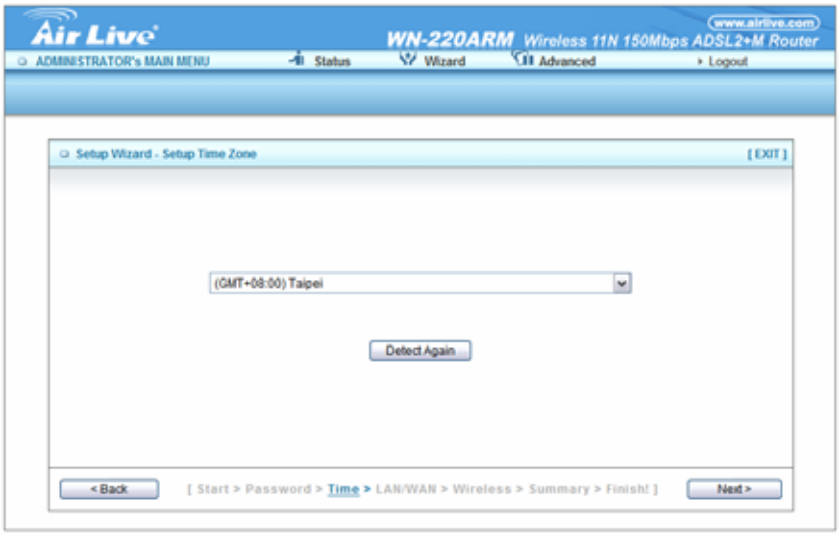


2.3 Setup Wizard

Step 1
You can change the password of administrator here.



Step 2
Select Time Zone.

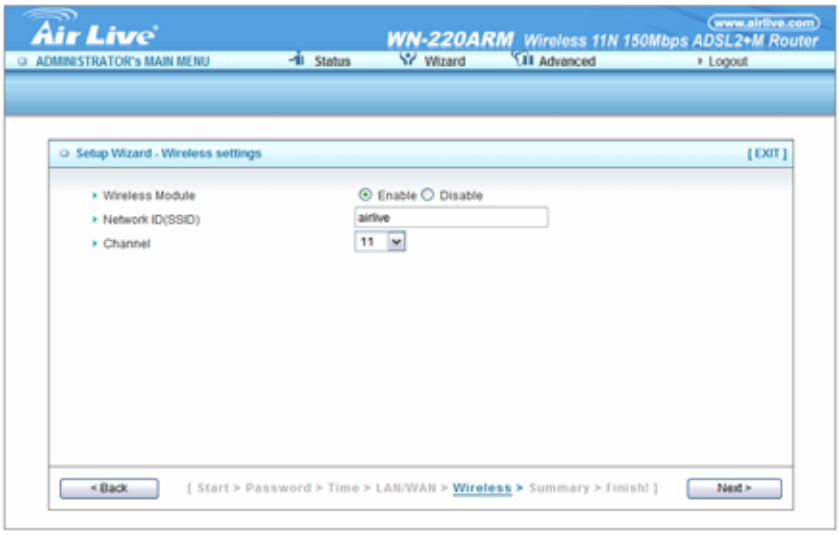


Step 3
You can select Auto detecting WAN type or setup WAN type manually.

Step 4
The system will detect the WAN type if you choose to let the system detect automatically.

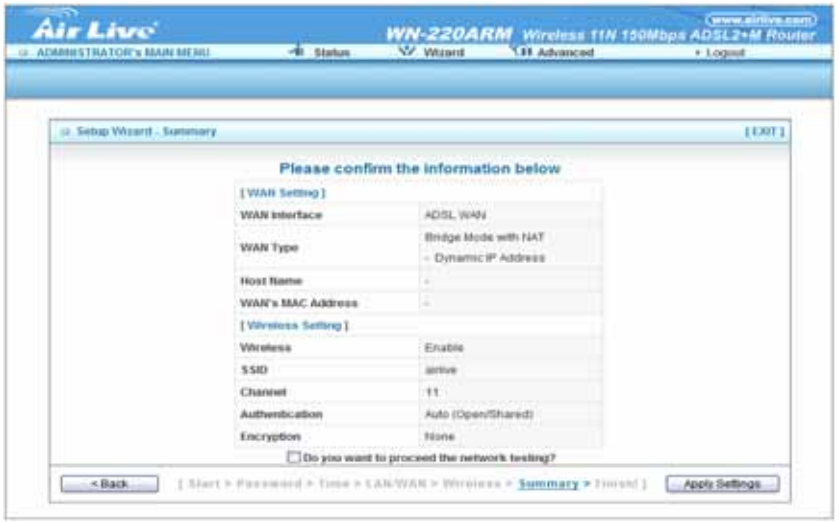
Step 5
Type in Host name and ISP registered MAC address. (if no such information, you can go next)

Step 5-1
Wireless setting.

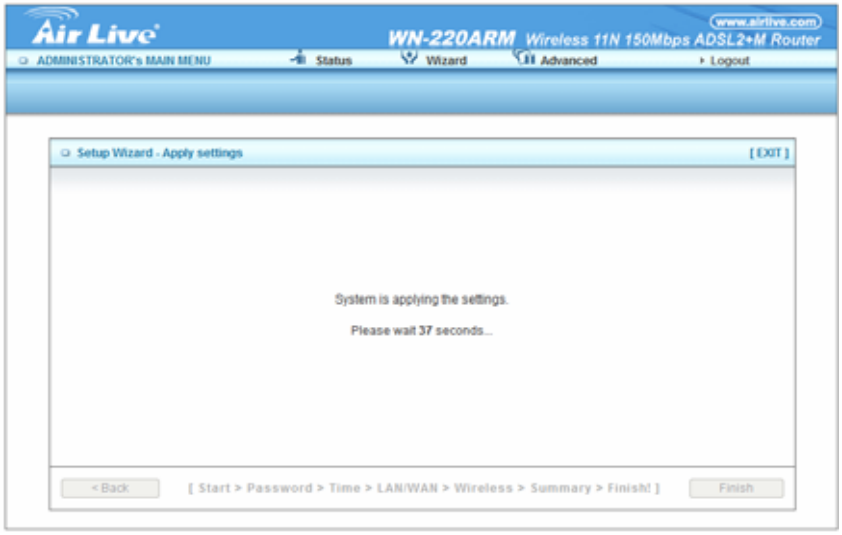


Step 5-2
Wireless authentication and encryption.

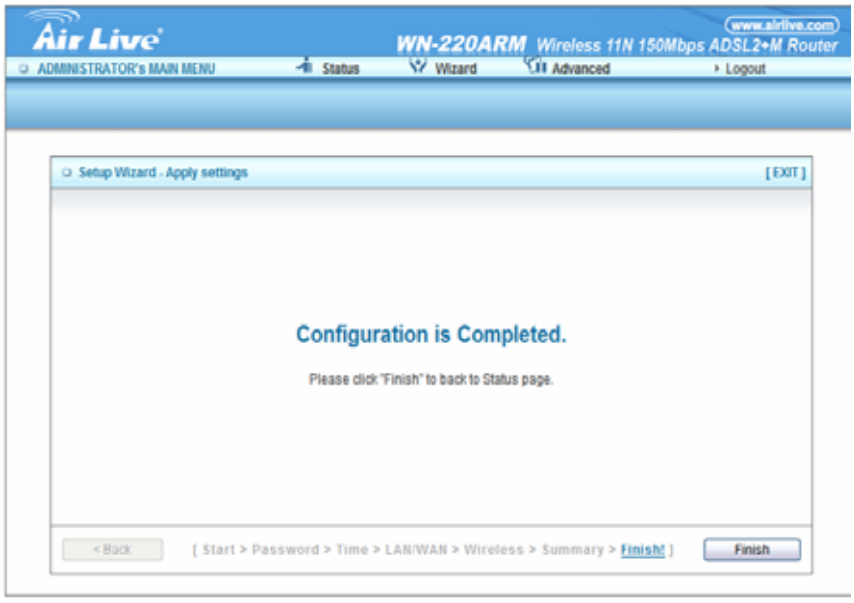
Step 6
Check the information again.



Step 7
System is applying the setting.



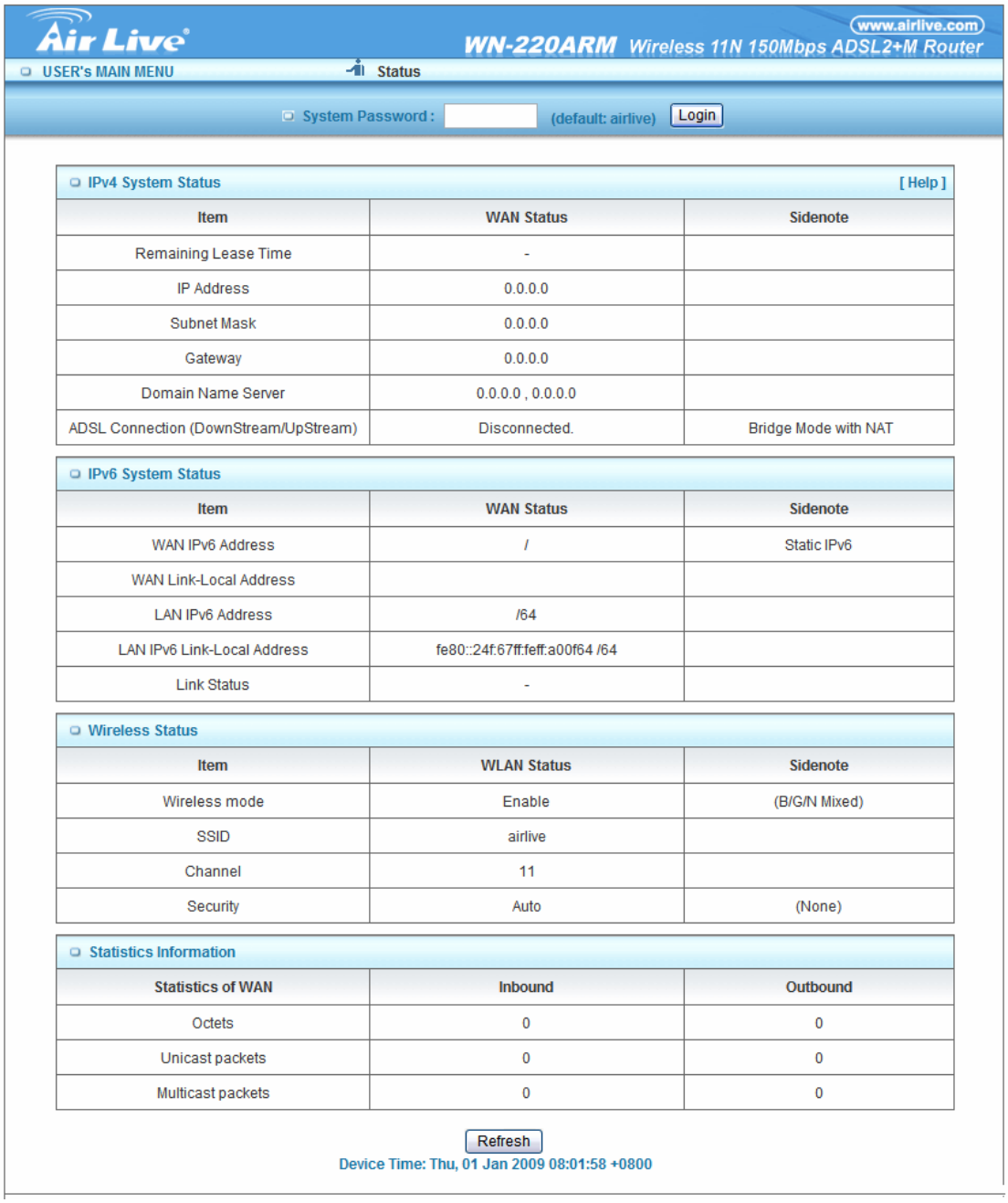
Step 8
Click finish to complete it.



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.

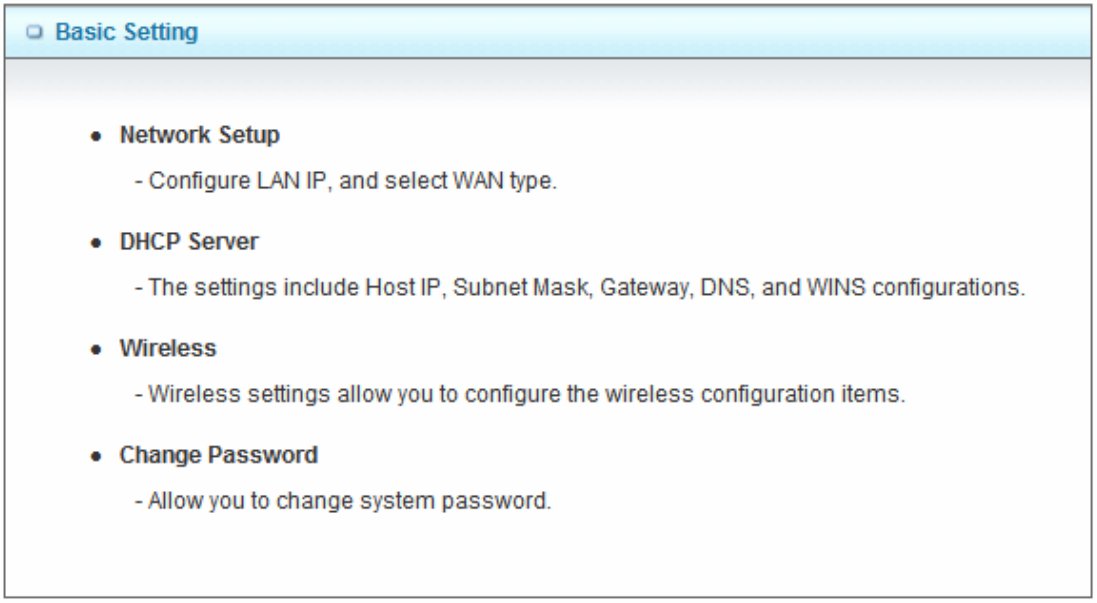


Enter the default password "**airlive**" in the System Password and then click 'login' button.

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

3.2 Basic Setting

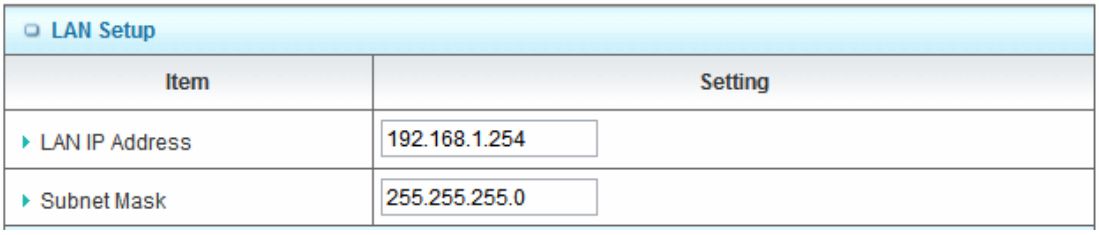
There are four options: Network Setup, DHCP Server, Wireless and Change Password.



3.2.1 Network Setup

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

3.2.2 LAN Type



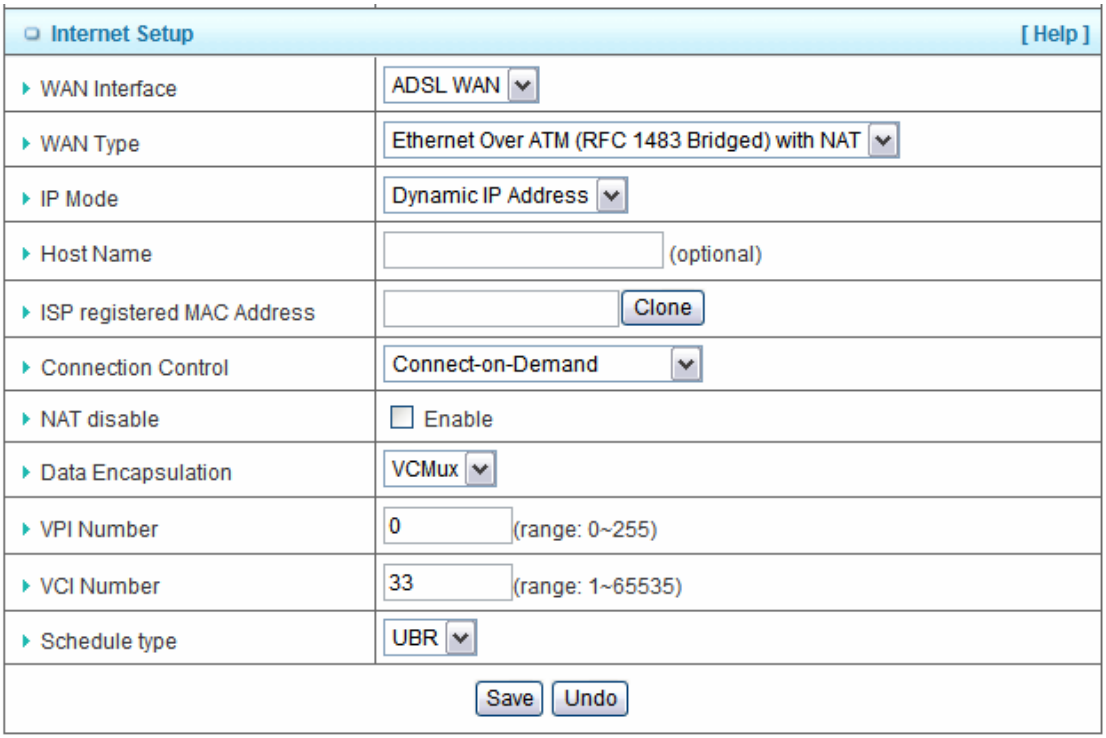
1. **LAN IP Address:** The local IP address of this device. The computer on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary.

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.

3.2.2.1 Internet Setup

1. **WAN Interface:** Select ADSL WAN or Wireless WAN to continue.

A. Ethernet Over ATM with Static IP

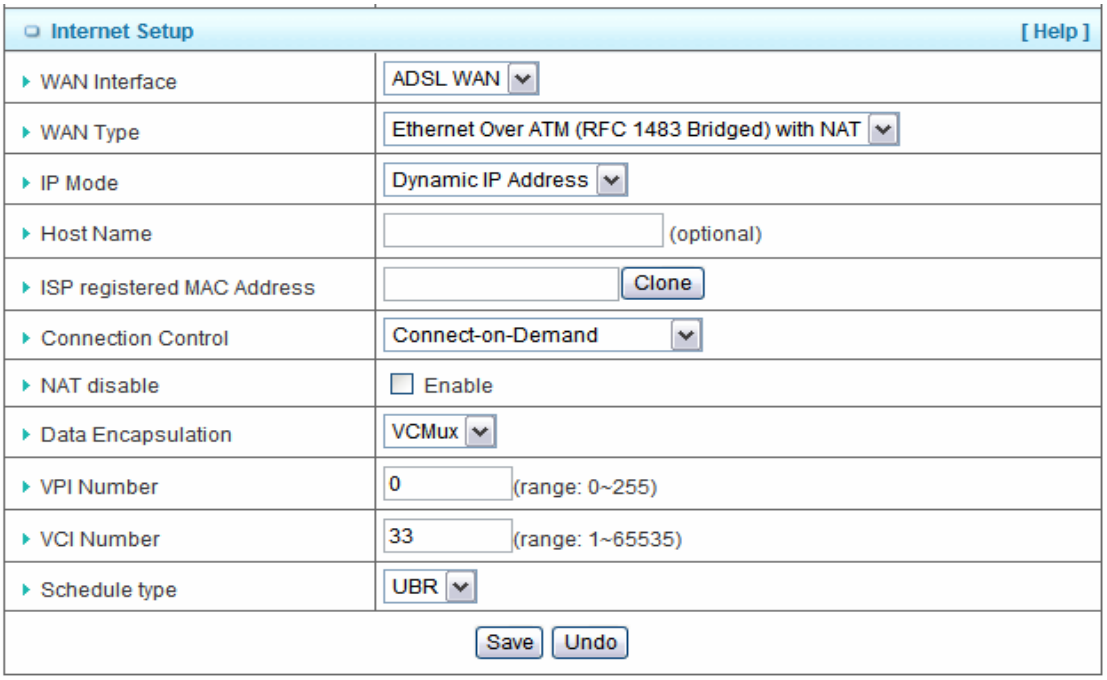


2. **WAN Type**: WAN connection type of your ISP. You can click WAN Type combo button to choose a correct one from the following options:

- Ethernet Over ATM(RFC1483 Bridged) with NAT
- IP over ATM(RFC 1483 Routed)
- PPP over Ethernet
- PPP over ATM

3. **Activate WWAN for Auto-failover** : Once you enable this function, you have to input WWAN information for 3G Auto-Backups (see as WWAN 3G portion). Host Name : ISP host name
4. **PPPoA Account**: input your account
5. **PPPoA Password**: input your password
6. Primary DNS and Secondary DNS
7. ISP registered MAC Address
8. **Connection Control:** you can choose Connect-on-demand, Auto Reconnect (always-on) and Manually.
9. **Maximum idle time** : 600 seconds
10. **NAT disable:** If you enable this option, the device would not transfer the LAN IP to WAN IP, it will behave like a pure router.
11. **Data Encapsulation:** Vc-MUX and LLC, these two options depend on your ISP setting.
12. **VPI and VCI, Schedule Type:** these values depend on your ISP setting.

B. Dynamic IP Address



1. **Activate WWAN for Auto-Failover**: With this function enabled, when the Ethernet WAN connection is broken, the device will automatically activate the WWAN connection and keep you connected to internet with the alternative WWAN broadband service. Meanwhile, if the device detected that the Ethernet WAN connection is recovered, your broadband connection will be switched to use the Ethernet WAN service.

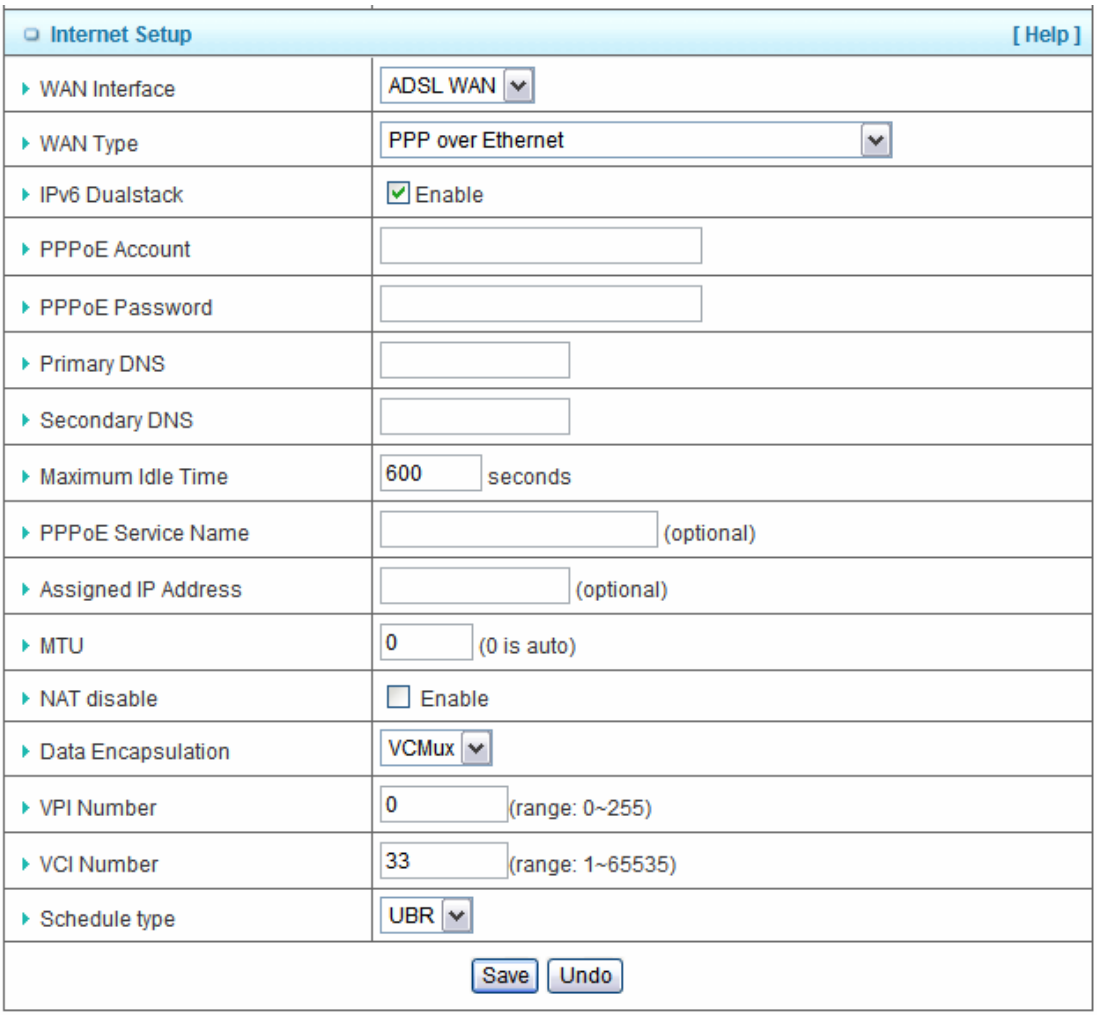
2. **Host Name**: Optional, required by some ISPs, for example, @Home.

3. **ISP registered MAC Address:** Enter MAC address of your ISP. (Optional)

4. **Connection Control**: There are 3 modes to select:
   (1) **Connect-on-demand:** The device will link up with ISP when the clients send outgoing packets.
   (2) **Auto Reconnect (Always-on)**: The device will link with ISP until the connection is established.
   (3) **Manually:** The device will not make the link until someone clicks the connect-button in the Status-page.

5. **NAT disable:** The device would not send private IP to other LAN PC if you select disable.

C. PPP over Ethernet



1. **Activate WWAN for Auto-Failover**: With this function enabled, when the Ethernet WAN connection is broken, the device will automatically activate the WWAN connection and keep you connected to internet with the alternative WWAN broadband service. Meanwhile, if the device detected that the Ethernet WAN connection is recovered, your broadband connection will be switched to use the Ethernet WAN service.
2. **PPPoE Account** and **Password**: The account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it blank.

3. **Connection Control**: There are 3 modes to select:

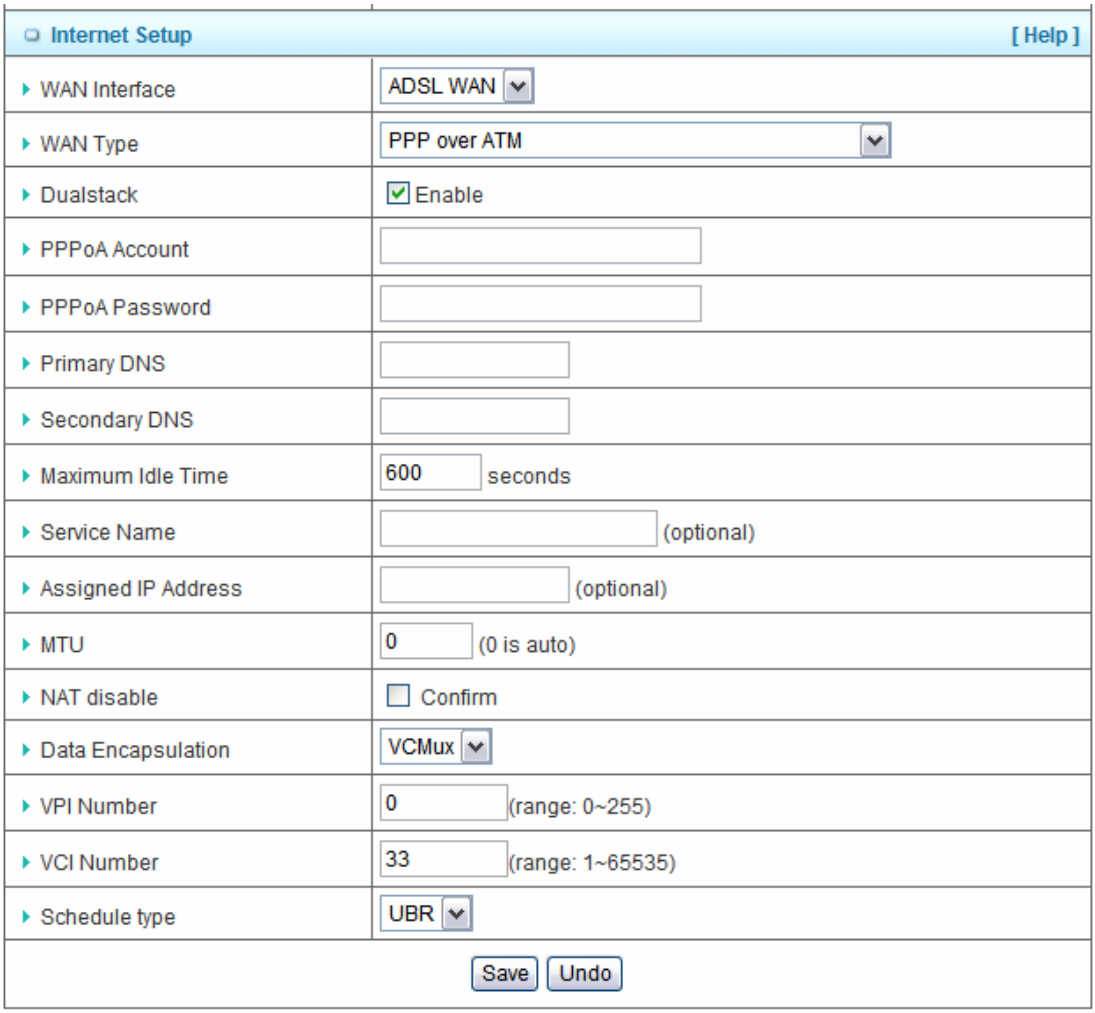
(1) **Connect-on-demand**: The device will link up with ISP when the clients send outgoing packets.

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

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

4. **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.
5. **PPPoE Service Name**: Optional. Input the service name if your ISP requires it. Otherwise, leave it blank.
6. Assigned IP Address: It is required by some ISPs. (Optional)
7. **Maximum Transmission Unit (MTU):** Most ISP offers MTU value to users. The default MTU value is 0 (auto).
8. **NAT disable:** The device would not send private IP to other LAN PC if you select disable.

D. PPPoA



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. **PPPoA Account ,Password, Primary and Secondary DNS**:
   Enter the proper settings provided by your ISP.
3. **Connection Control**: There are 3 modes to select:

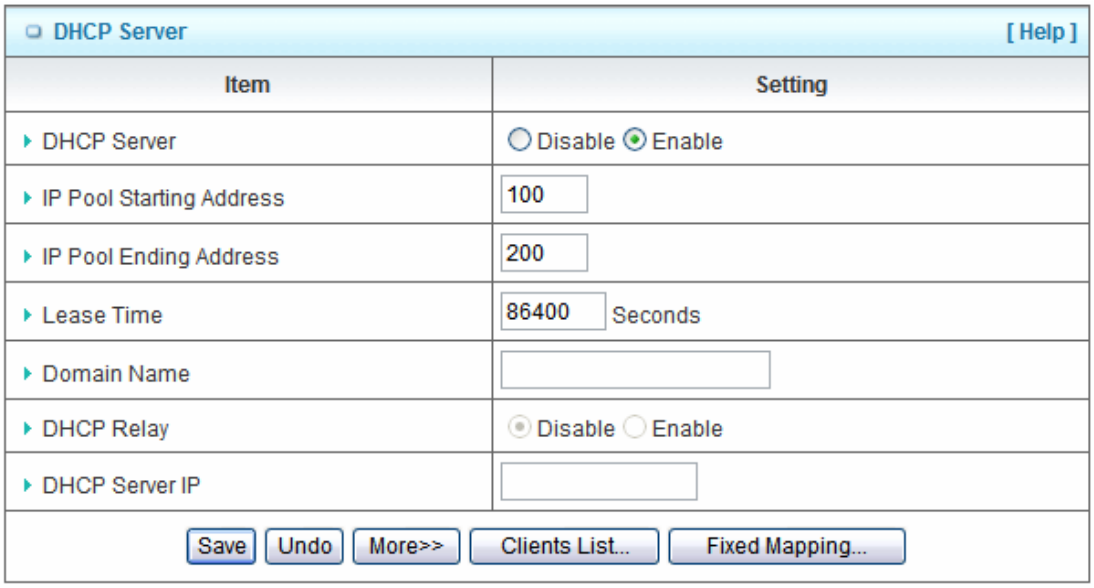
(1) **Connect-on-demand**: The device will link up with ISP when the clients send outgoing packets.

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

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

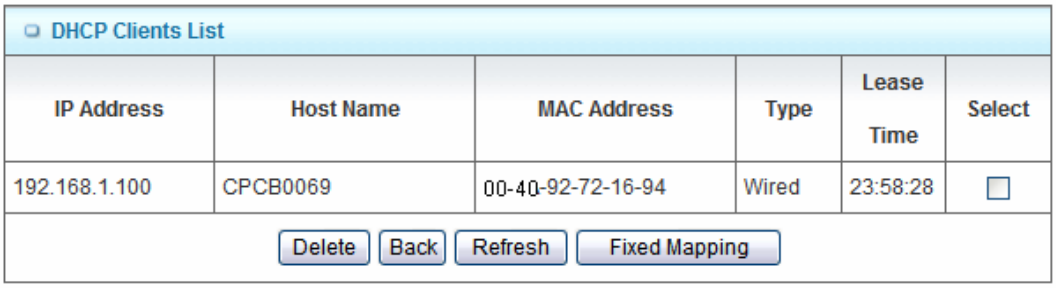
4. **Maximum Idle Time**: the time of no activity to disconnect your PPTP session. Set it to zero or enable “Auto-reconnect” to disable this feature. If Auto-reconnect is enabled, this device will connect with ISP automatically after system is restarted or connection is dropped.
5. **Service Name:** Sometimes your ISP would give you a specified service name to dial-up.
6. **Assigned IP Address:** If your ISP give you a specified IP address, fill it here.
7. **Maximum Transmission Unit (MTU)**: Most ISP offers MTU value to users. The default MTU value is 0 (auto).
8. **NAT disable:** If you enable this option, the device would not transfer the LAN IP to WAN IP, it will behave like a pure router.
9. **Data Encapsulation:** Vc-MUX and LLC, these two options depend on your ISP setting.
10. **VPI and VCI, Schedule Type:** these values depend on your ISP setting.

3.2.2 DHCP Server



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

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

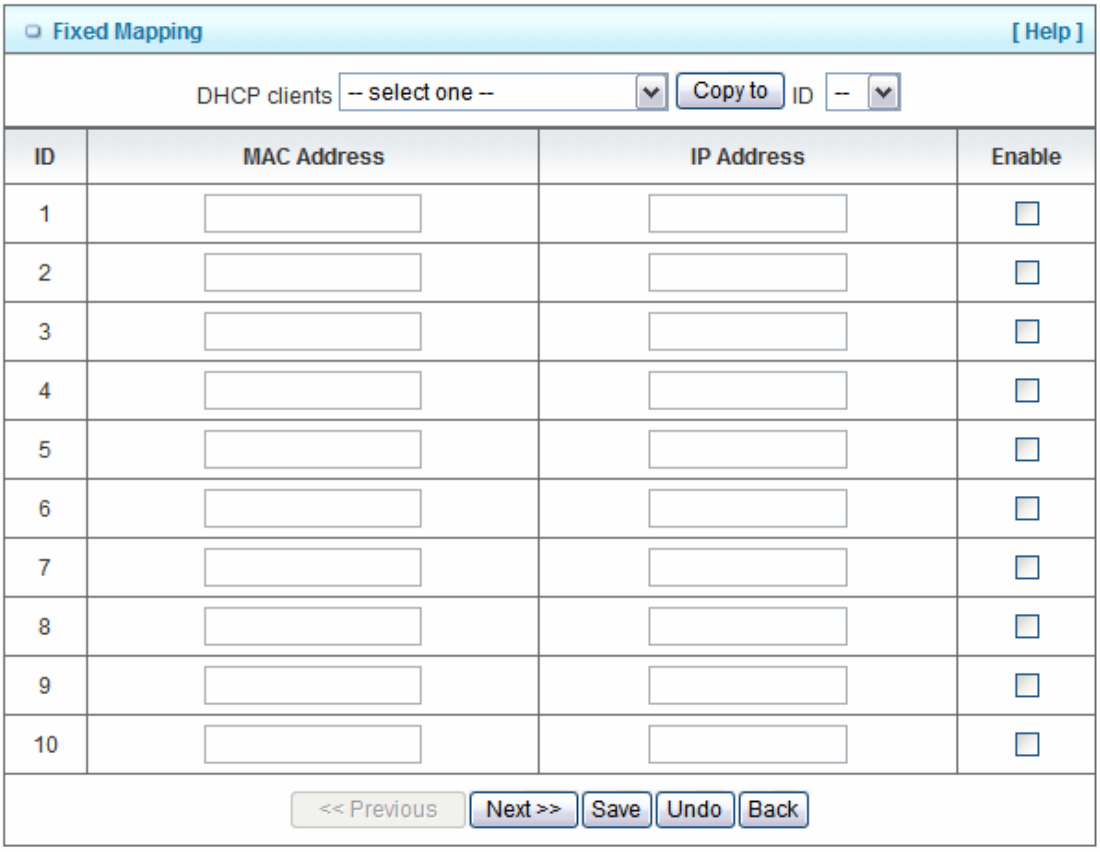


DHCP Clients List

IP Address	Host Name	MAC Address	Type	Lease Time	Select
192.168.1.100	CPCB0069	00-40-92-72-16-94	Wired	23:58:28	☐

Delete | Back | Refresh | Fixed Mapping

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



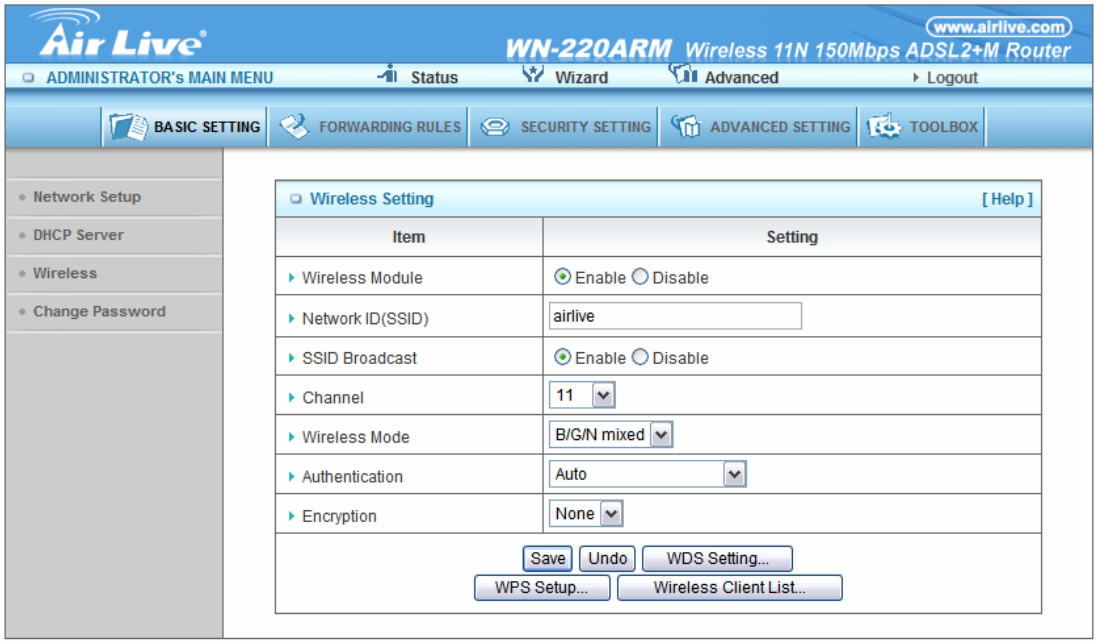
Fixed Mapping [Help]

DHCP clients -- select one -- Copy to ID --

ID	MAC Address	IP Address	Enable
1			☐
2			☐
3			☐
4			☐
5			☐
6			☐
7			☐
8			☐
9			☐
10			☐

<< Previous | Next >> | Save | Undo | Back

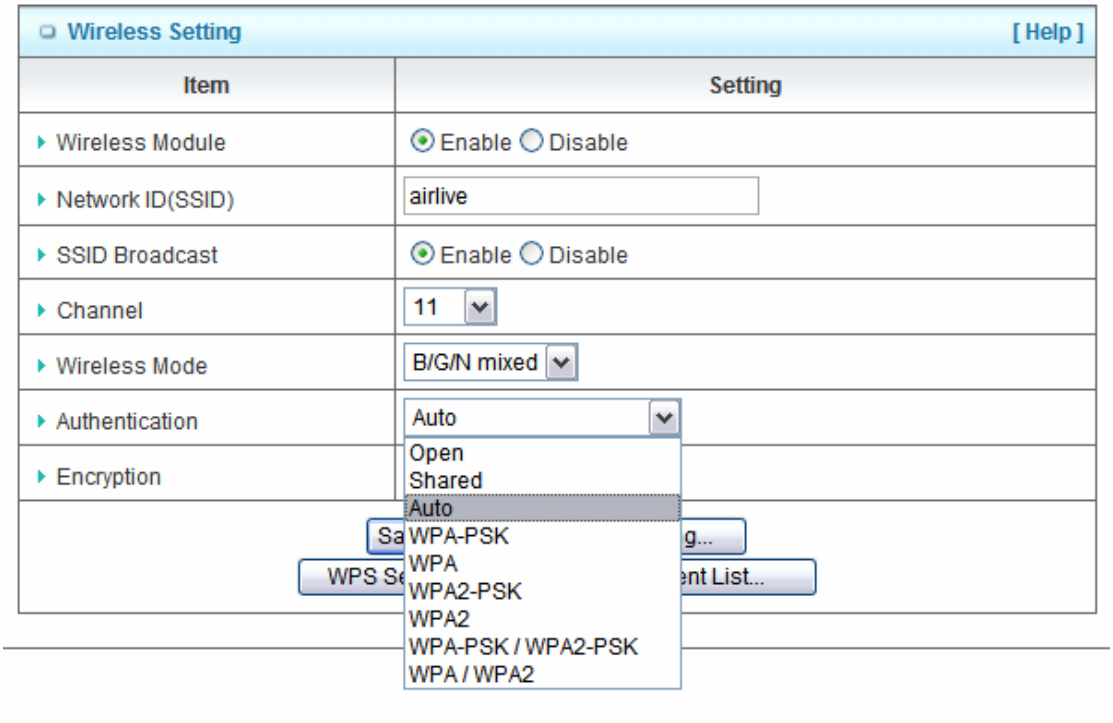
3.2.3 Wireless Setting



Wireless settings allow you to set the wireless configuration items.

1. **Wireless Module:** You can enable or disable wireless function.
2. **Network ID (SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is “default”)
3. **SSID Broadcast:** The 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.
4. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is as the following: channel 6 for North America; channel 7 for European (ETSI); channel 7 for Japan.
5. **Wireless Mode:** Choose “B/G mixed”, “B only”, “G only”, “N only”, “G/N mixed” or “B/G/N mixed”. The factory default setting is “B/G/N mixed”.
6. **Authentication mode:** You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2,

WPA-PSK/WPA2-PSK, or WPA /WPA2.



- **Open**

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

- **Shared**

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

- **Auto**

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

- **WPA-PSK**

  Select Encryption and Pre-share Key Mode

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

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

  Fill in the key, Ex 12345678

- **WPA**

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

  Select Encryption and RADIUS Shared Key.

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

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

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

- **WPA2-PSK**

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

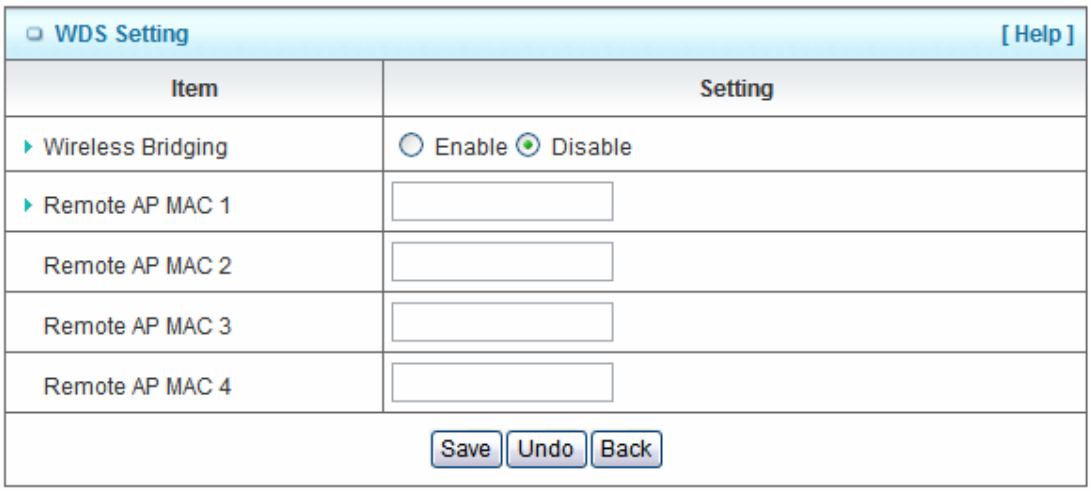
- **WPA-PSK/WPA2-PSK**

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

- **WPA/WPA2**

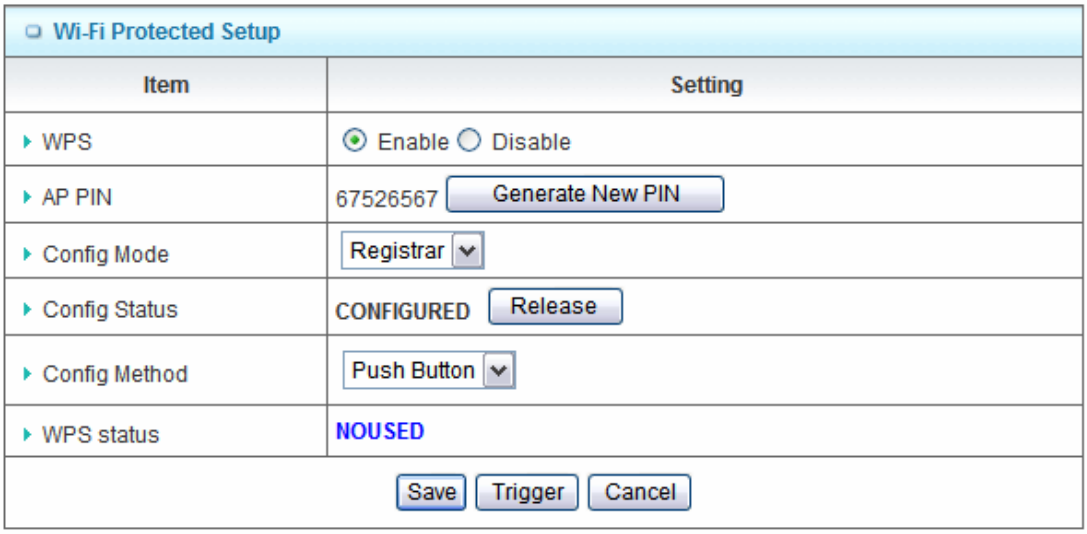
  Another encryption options for WPA-TKIP and WPA2-AES, the others are same the WPA.

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

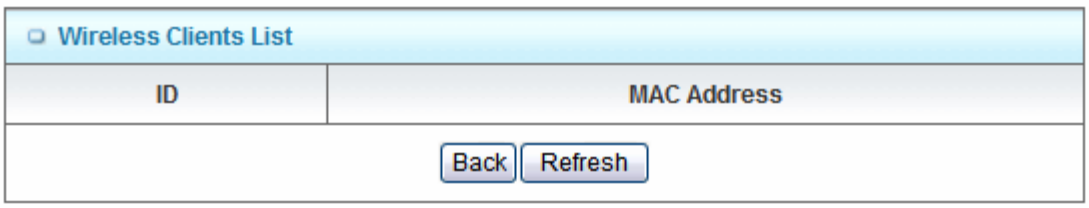


1. **Wireless Bridging:** You could enable this function by selecting “Enable”.
2. **Remote AP MAC 1~Remote AP MAC 2:** Enter the wireless MAC into the blank.
3. **Encryption type:** Select the appropriate category. Once you set up that type of encryption, second LAN PC must enter the same encryption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

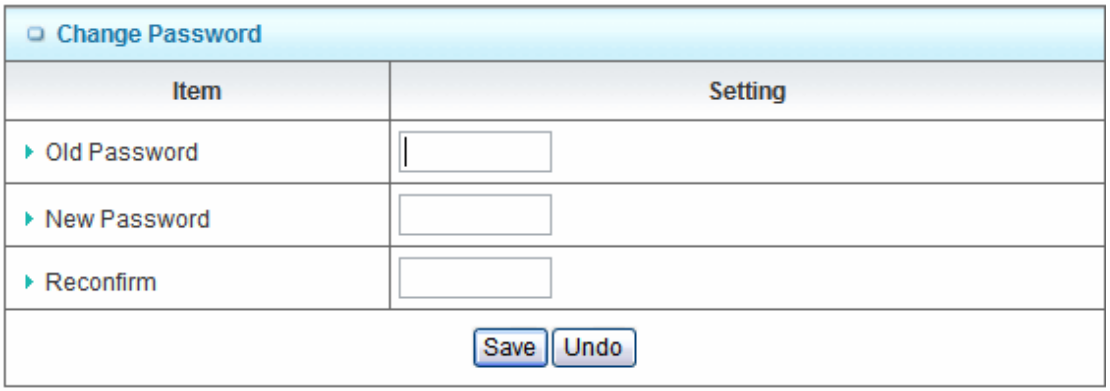
Press **“WPS Setup”**, you can configure and enable the easy setup feature WPS (Wi-Fi Protection Setup) for your wireless network.



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



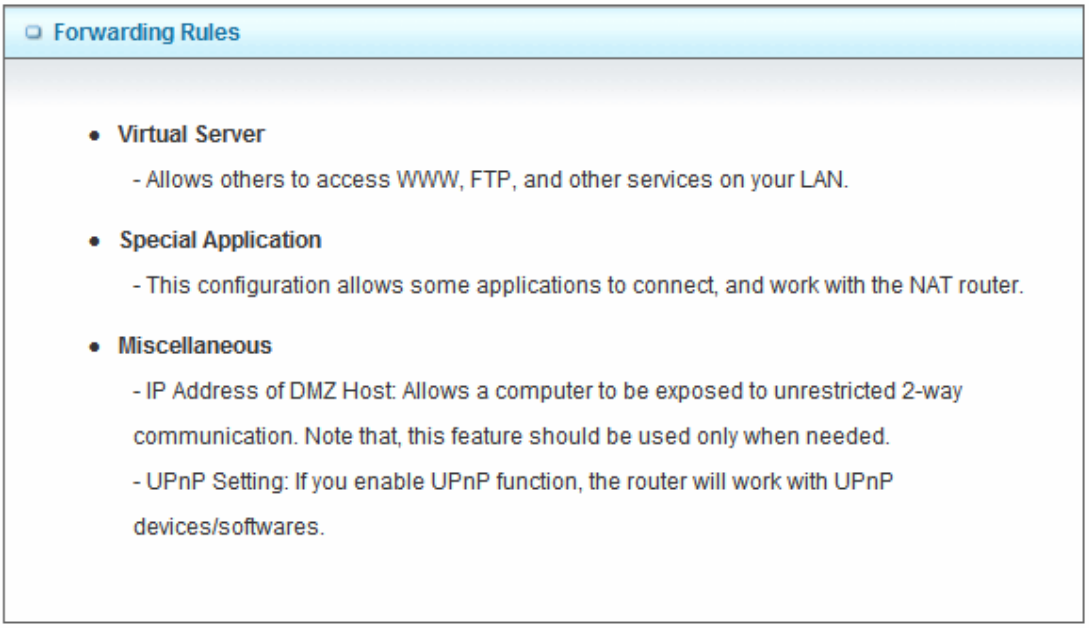
3.2.4 Change Password



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

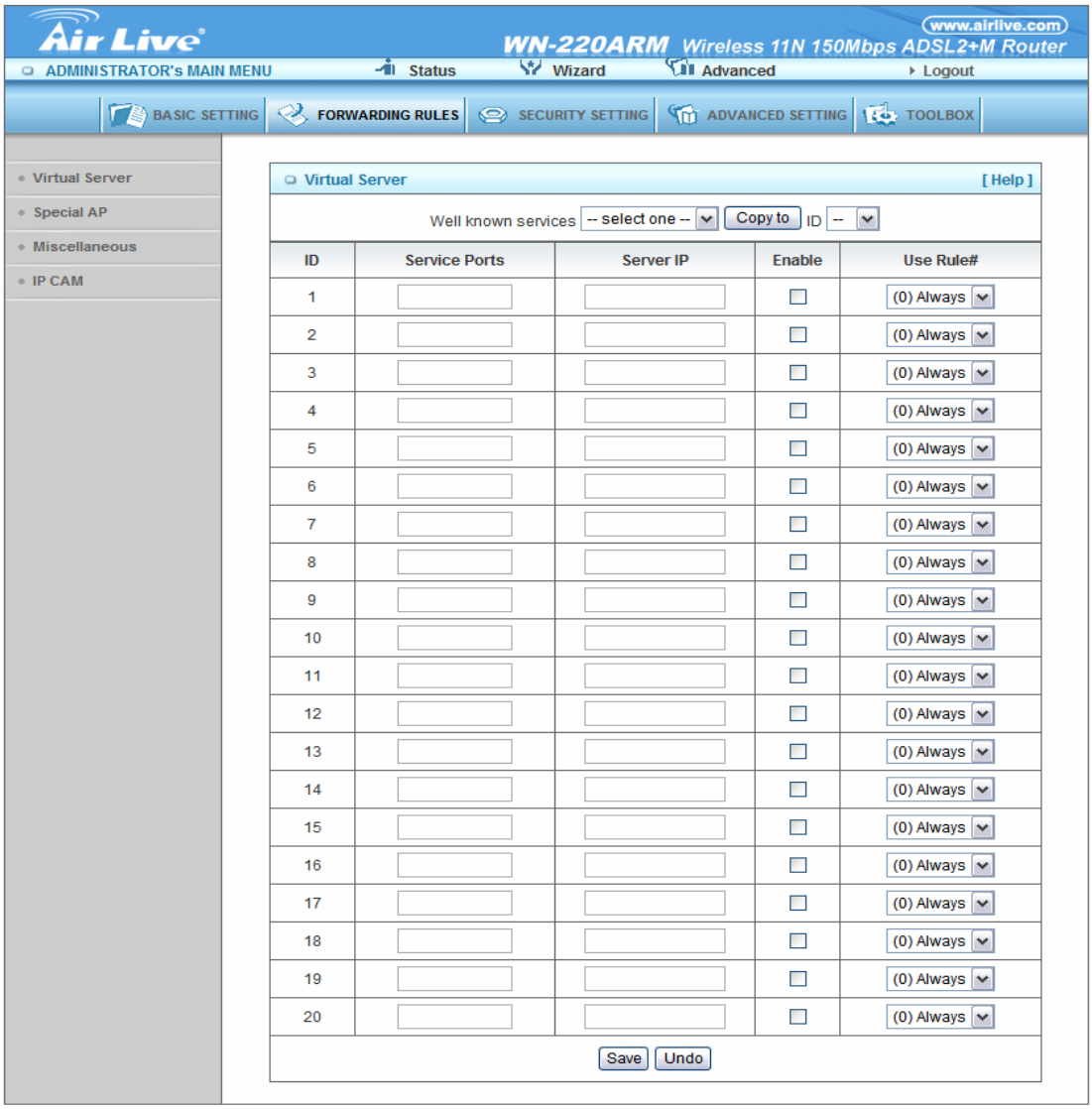
There are three options: Virtual Sever, Special Application and Miscellaneous.



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**.



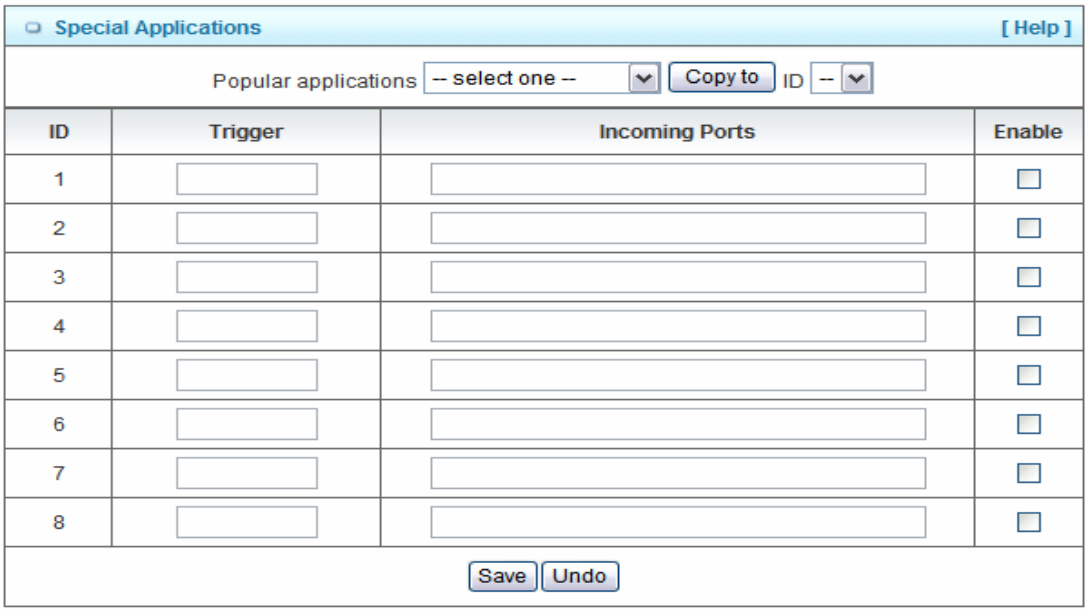
For example, if you have an FTP server (port 21) at 192.168.1.1, a Web server (port 80) at 192.168.1.2, and a VPN server at 192.168.1.6, then you need to specify the following virtual server mapping table:

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 Application

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

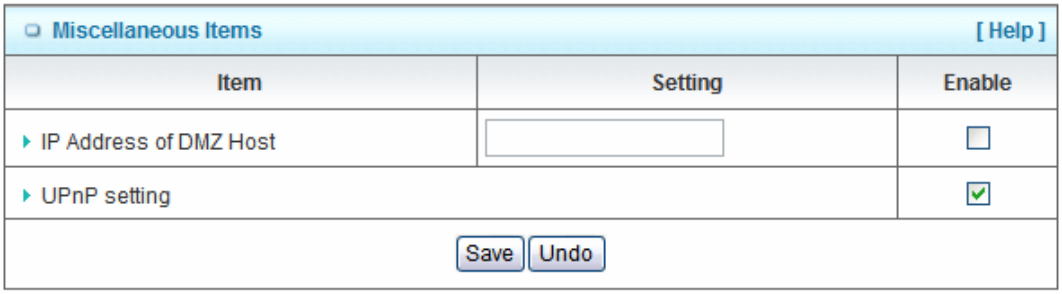


This device provides some predefined settings. Select your application and click "**Copy to"** to add the predefined setting to your list.

1. **Trigger:** The outbound port number issued by the application.
2. **Incoming Ports**: When the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

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

3.3.3 Miscellaneous – DMZ Host & UPnP



1. **IP Address of DMZ Host**

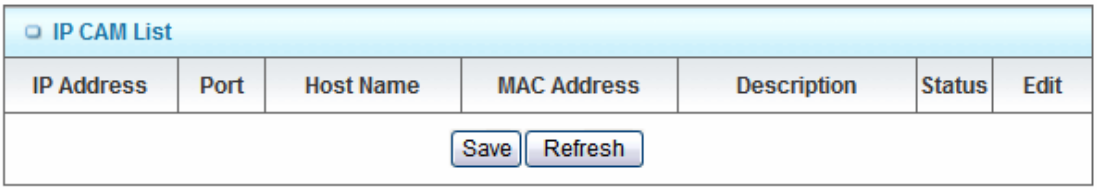
   DMZ (Demilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

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.

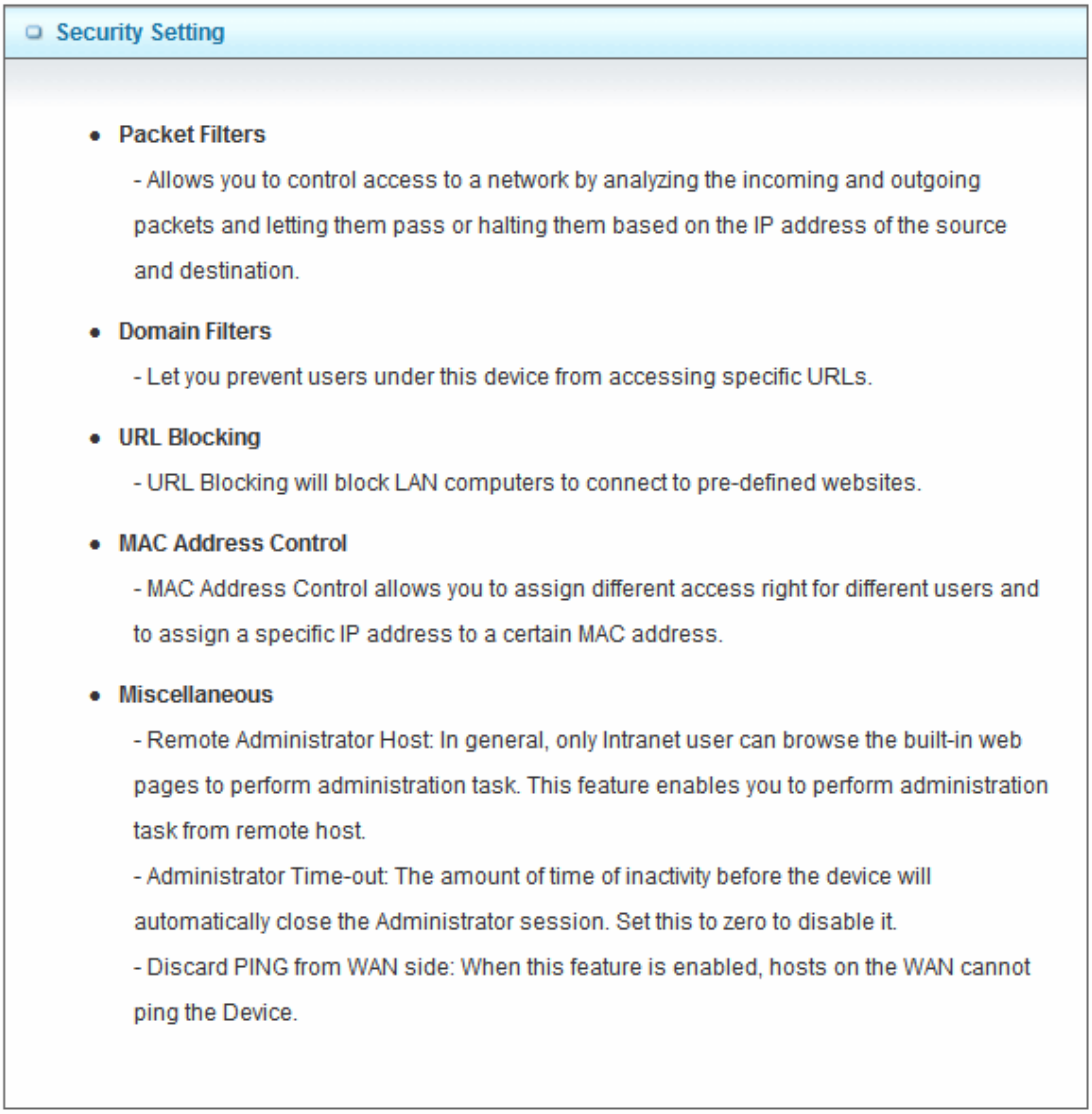
Afterwards, click on "Save" to store your settings or click "Undo" to give up th**e changes.**

3.3.4 IP CAM List



3.4 Security Setting

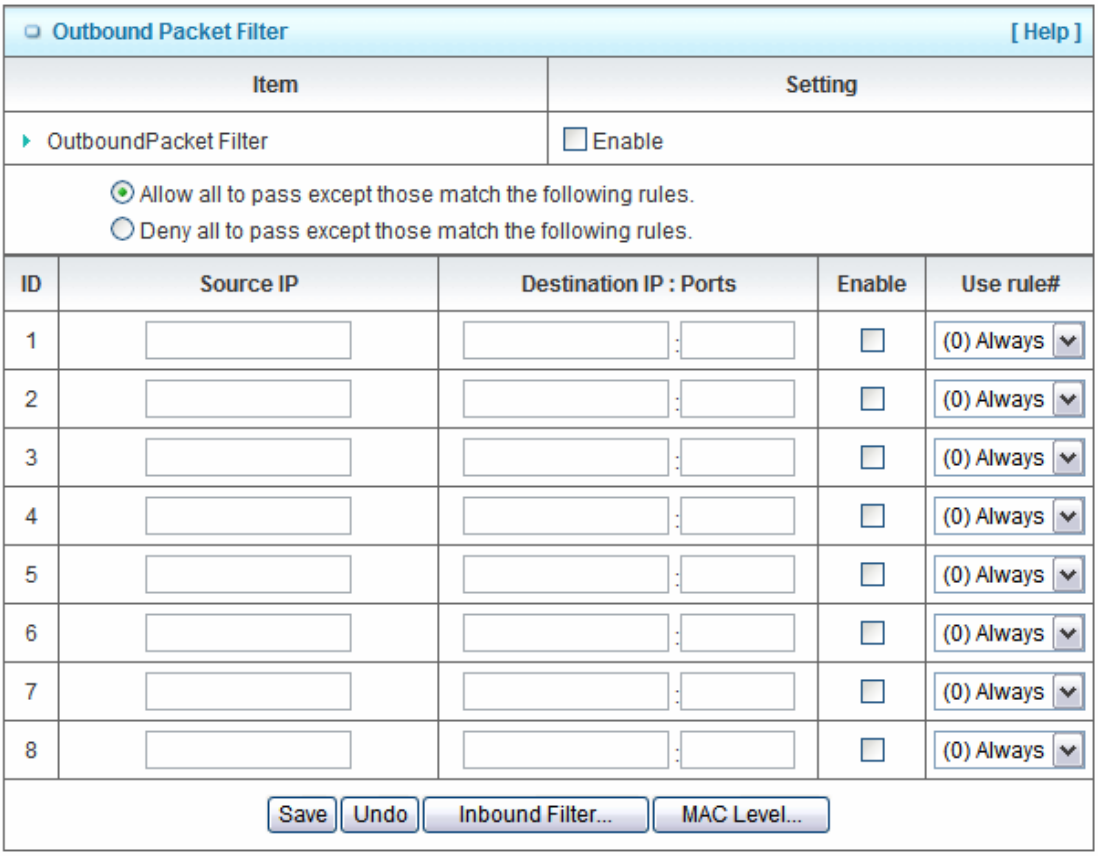
There are five options: Packet Filters, Domain, URL Blocking, MAC Address Control and Miscellaneous.



3.4.1 Packet Filters

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

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



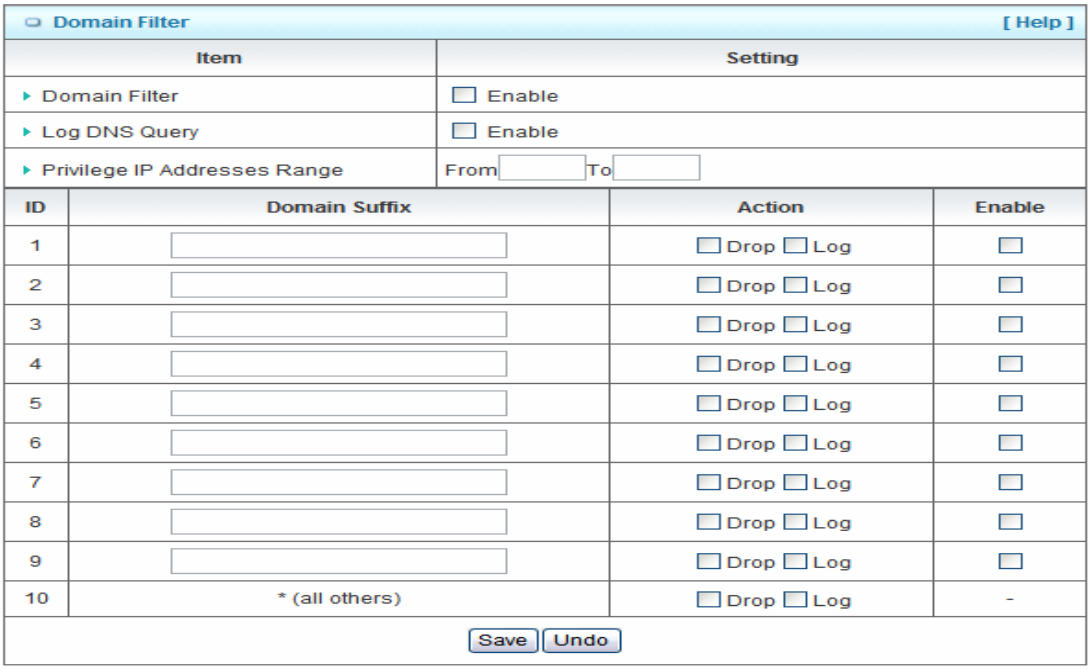
You can specify 8 rules for each direction: inbound or outbound. For each rule, you can define the following:

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

For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.
For source or destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999, No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. Packet Filter can work with **Scheduling Rules,** and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule.**
Each rule can be enabled or disabled individually.

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

3.4.2 Domain Filters



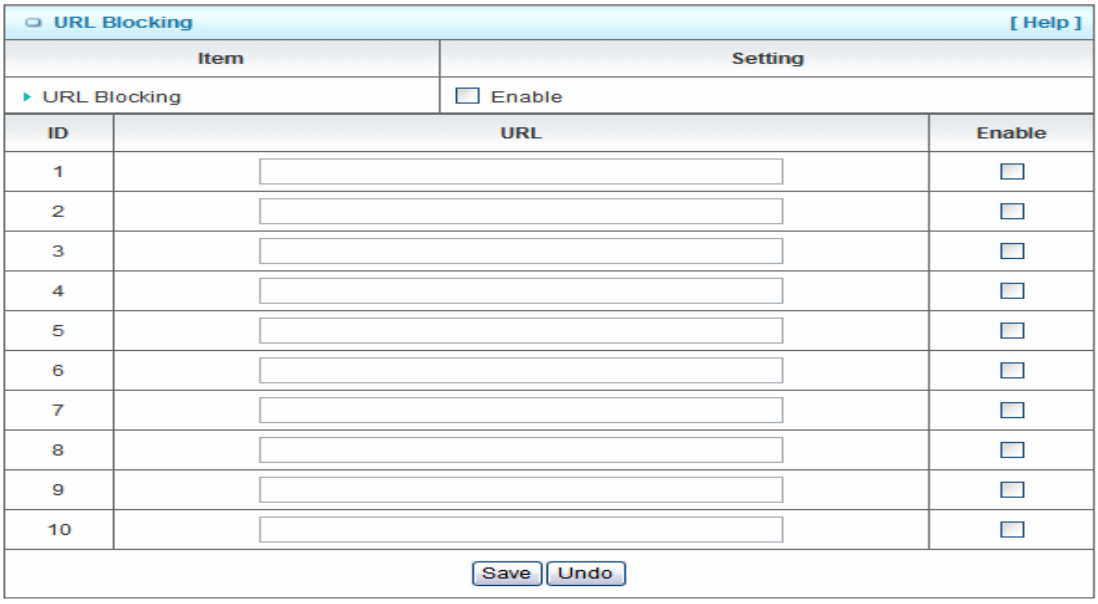
Domain Filter prevents users under this device from accessing specific URLs.

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

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

3.4.3 URL Blocking

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



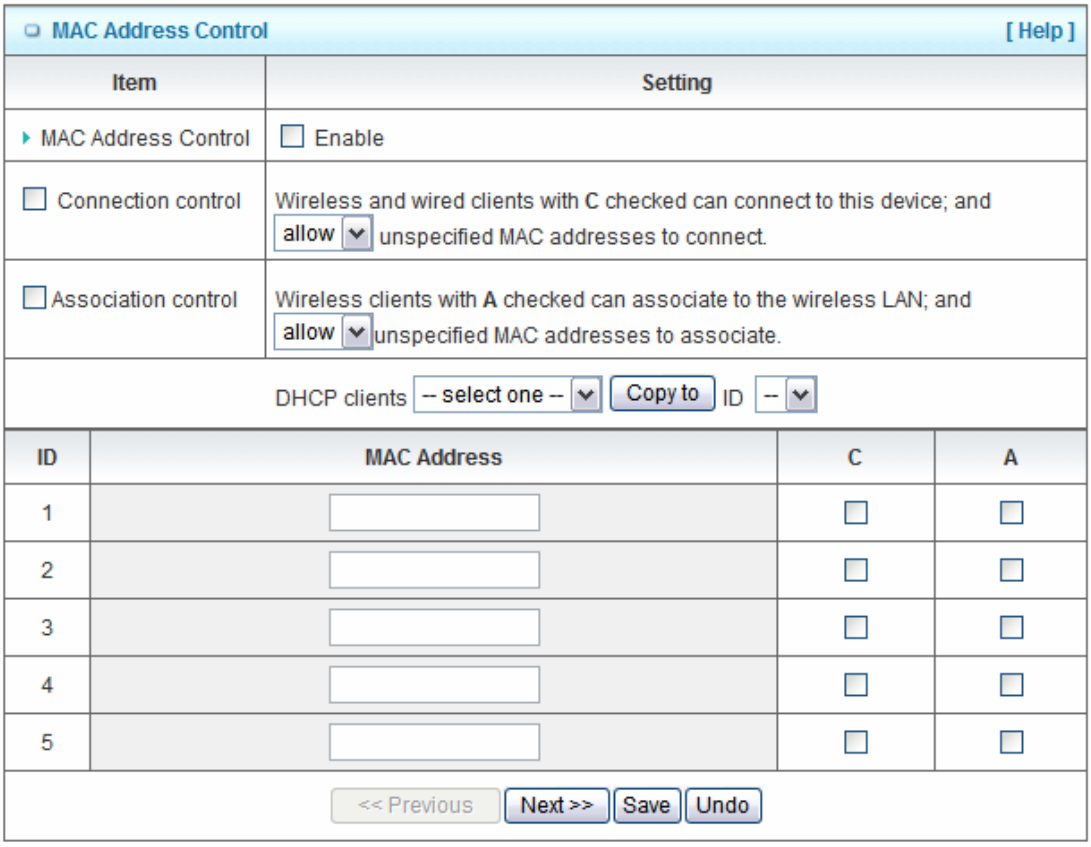
1. **URL Blocking**: Check if you want to enable URL Blocking.

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

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

3.4.4 MAC Control

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

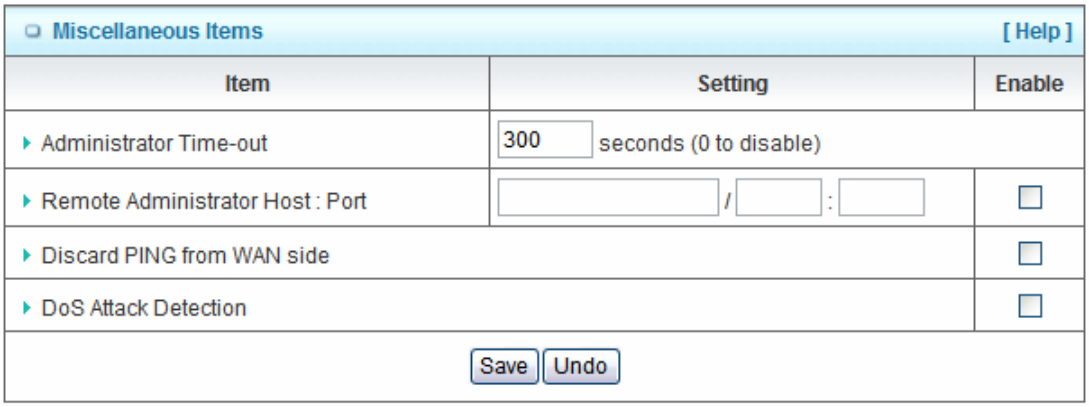


1. **MAC Address Control**: Check “Enable” to enable the “MAC Address Control”. All of the settings in this page will take effect only when “Enable” is checked.

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

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

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

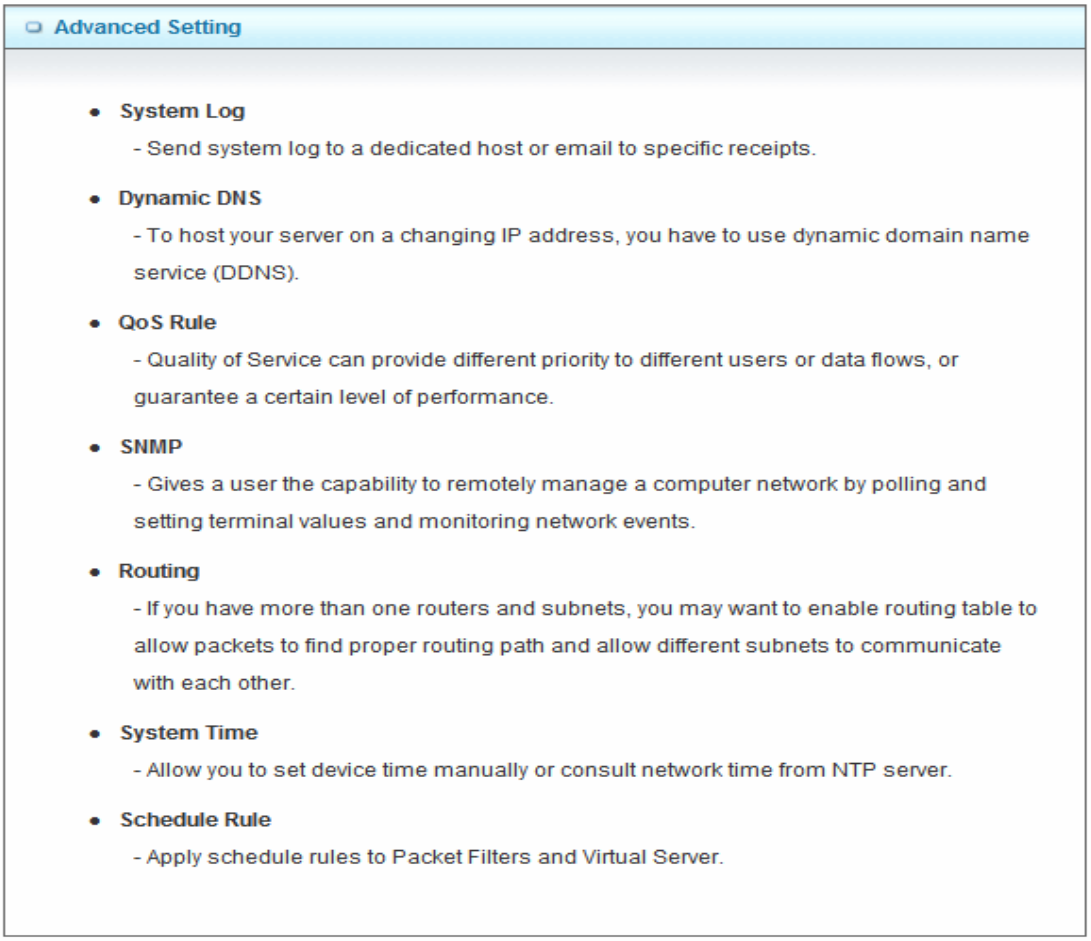
NOTE: When Remote Administration is enabled, the web server port will be shifted to 80. You can change web server port to other port, too.

3. **Discard PING from WAN side**: When this feature is enabled, any host on the WAN cannot ping this product.
4. **DoS Attack Detection**: When this feature is enabled, the router will detect and log the DoS attack coming from the Internet. Currently, the router can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack etc.

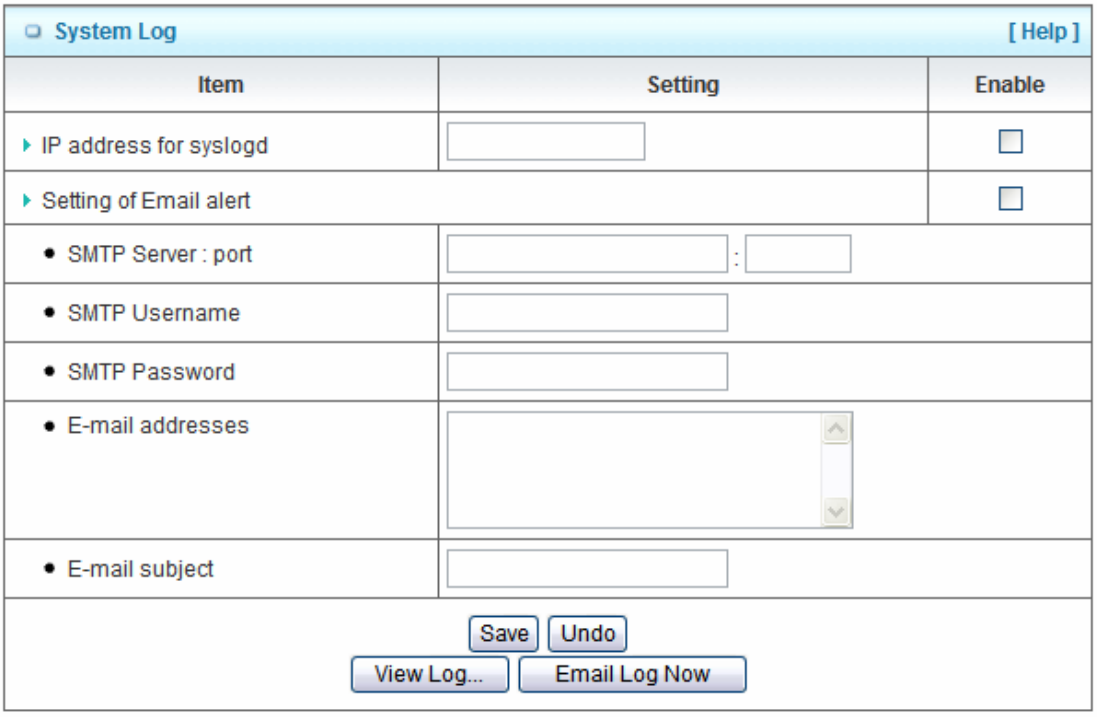
Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.5 Advanced Setting

There are seven options: System Log, Dynamic DNS, QoS Rule, SNMP, Routing, System Time and Schedule Rule.



3.5.1 System Log



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

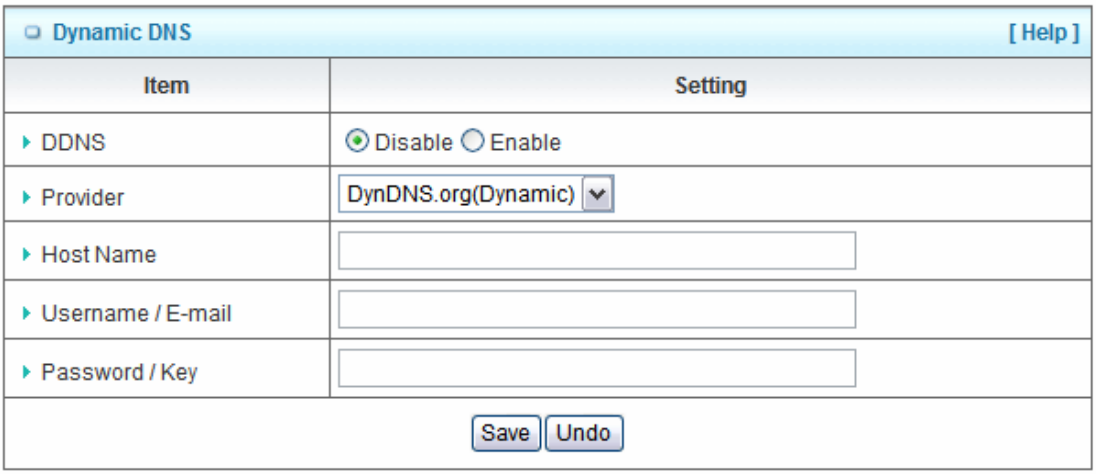
1. **IP Address for Syslog**: Host IP of destination where syslog will be sent to. Check **Enable** to enable this function.
2. **Setting of Email alert**: Check if you want to enable Email alert (send syslog via email).
3. **SMTP Server: Port**: Input the SMTP server IP and port, which are connected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

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

3.5.2 Dynamic DNS

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

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

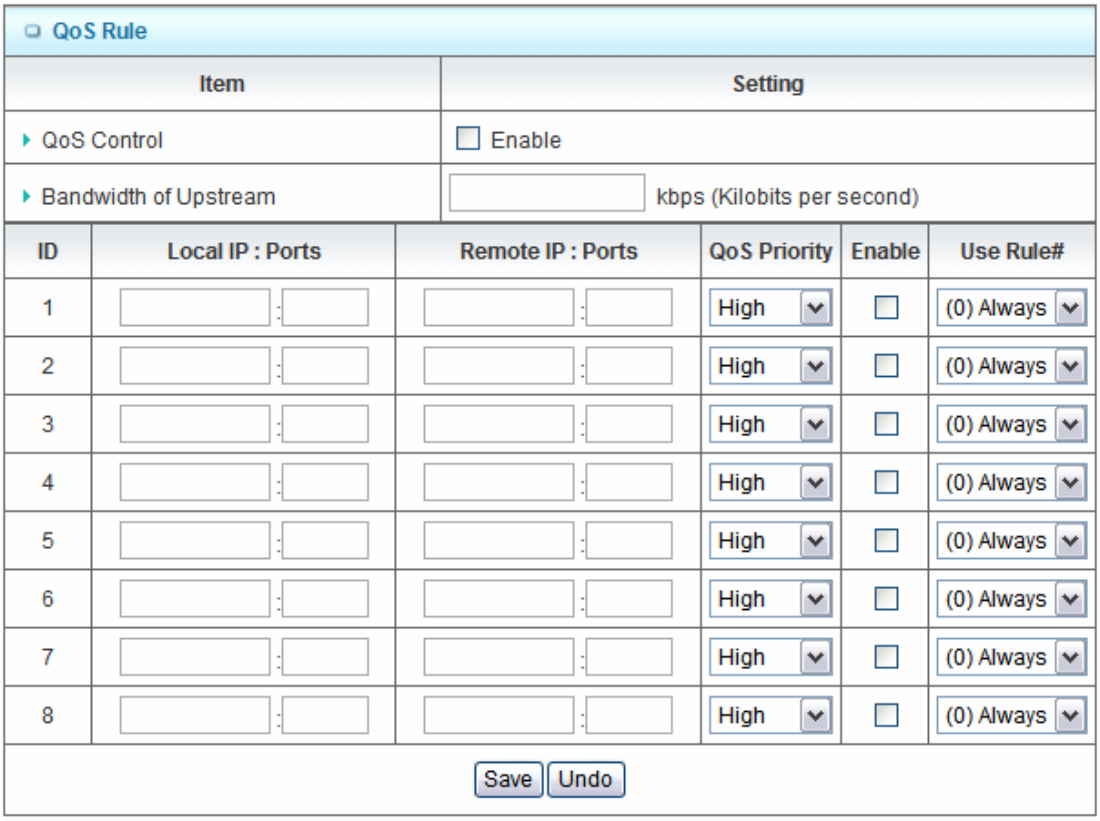


1. **DDNS:** Select enable if you would like to trigger this function.
2. **Provider:** The DDNS provider supports service for you to bind your IP(even private IP) with a certain Domain name. You could choose your favorite provider.
3. **Host Name:** Register a domain name to the DDNS provider. The fully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

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

3.5.3 QoS

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



QoS Rule

Item	Setting
QoS Control	Enable
Bandwidth of Upstream	kbps (Kilobits per second)

ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use Rule#
1	:	:	High		(0) Always
2	:	:	High		(0) Always
3	:	:	High		(0) Always
4	:	:	High		(0) Always
5	:	:	High		(0) Always
6	:	:	High		(0) Always
7	:	:	High		(0) Always
8	:	:	High		(0) Always

Save Undo

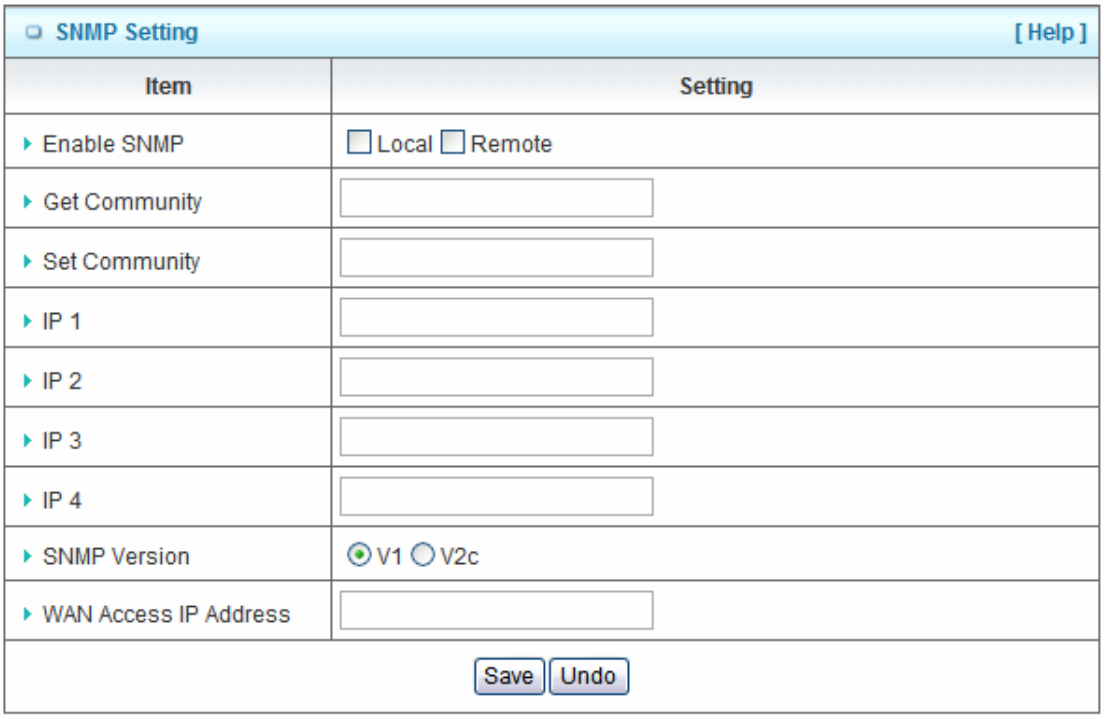
1. **QoS Control**: Check Enable to enable this function.
2. **Bandwidth of Upstream**: Set the limitation of upstream bandwidth.
3. **Local IP: Ports**: Define the Local IP address and ports of packets.
4. **Remote IP: Ports**: Define the Remote IP address and ports of packets.
5. **QoS Priority:** 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 3.4.1.7 Schedule Rule.

Afterwards, 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 respond request from LAN. If “Remote” is checked, this device will respond request from WAN.
2. **Get Community**: The community of GetRequest is that this device will respond.
3. **Set Community**: The community of SetRequest is that this device will accept.
4. **IP 1, IP 2, IP 3, IP 4**: Enter the IP addresses of your SNMP Management PCs. User has to configure where this device should send SNMP Trap message.

5. **SNMP Version**: Select proper SNMP Version that your SNMP Management software supports.
6. **WAN Access IP Address**: If you want to limit the remote SNMP access to specific computer, please enter the PC's IP address. The default value is 0.0.0.0, and it means that any Internet connected computer can get some information of the device with SNMP protocol.

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

3.5.5 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 addresses are utilized for outgoing IP data grams.

Routing Table [Help]

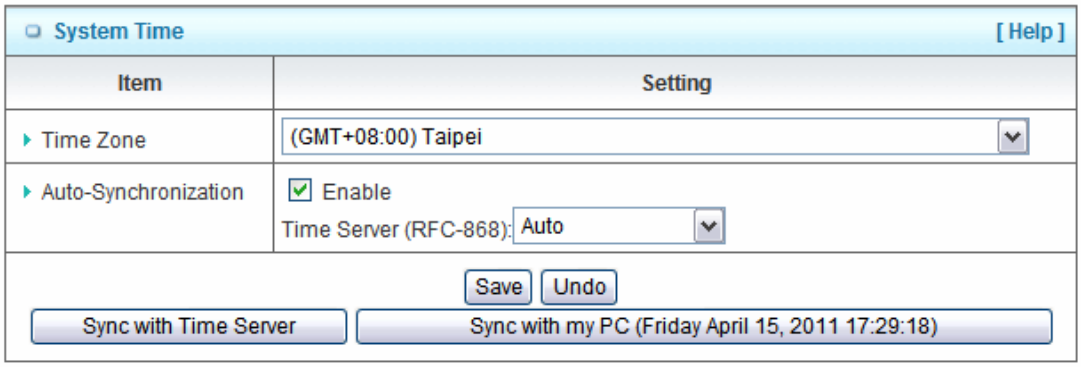
Item	Setting
Dynamic Routing	◉ Disable ○ RIPv1 ○ RIPv2
Static Routing	◉ Disable ○ Enable

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1					☐
2					☐
3					☐
4					☐
5					☐
6					☐
7					☐
8					☐

Save Undo

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

3.5.6 System Time

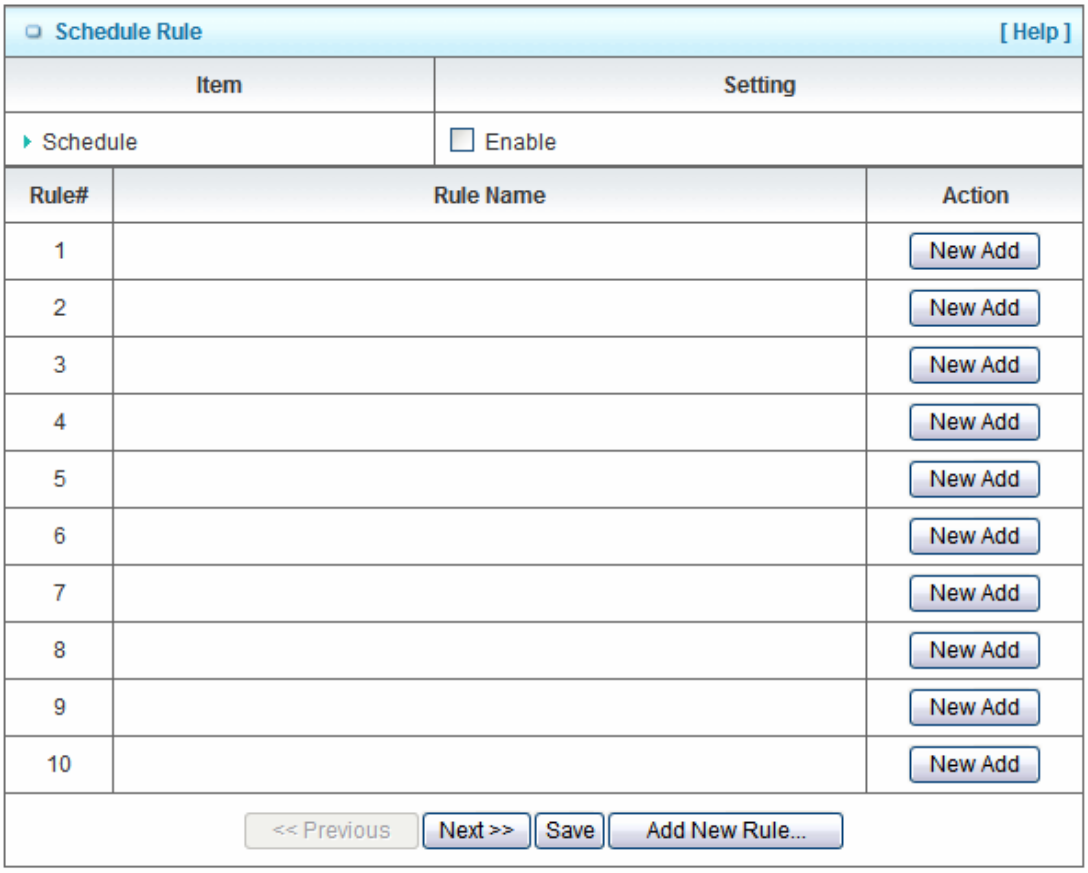


1. **Time Zone**: Select a time zone where this device locates.
2. **Auto-Synchronization**: Check the “Enable” checkbox to enable this function. Besides, you can select a NTP time server to consult UTC time.
3. **Sync with Time Server**: Click on the button if you want to set Date and Time by NTP Protocol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

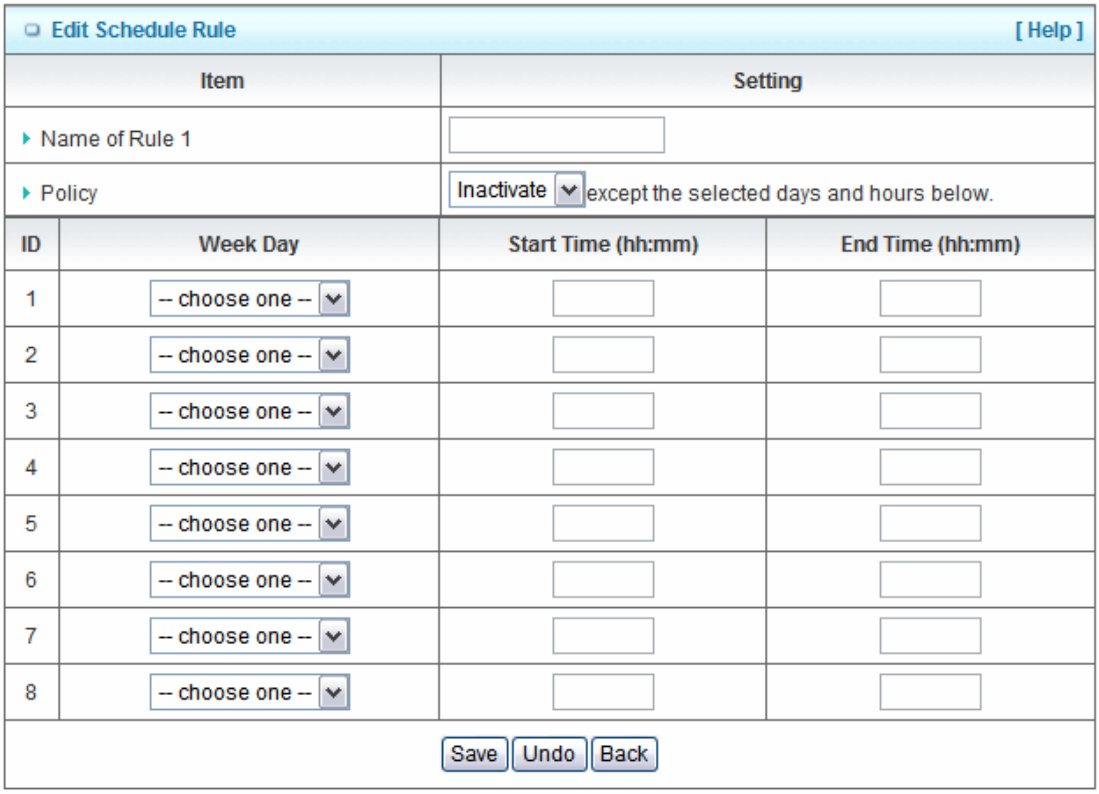
Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.5.7 Scheduling

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

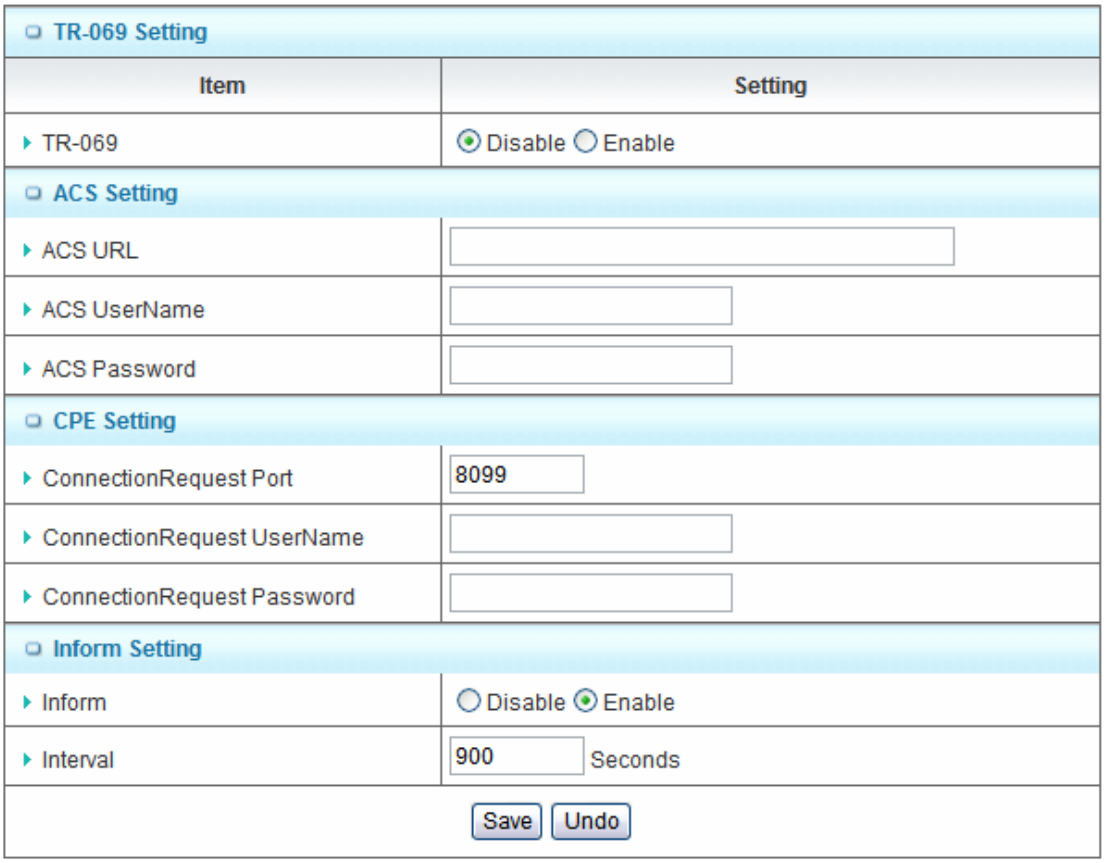


1. **Schedule**: Check to enable the schedule rule settings.
2. **Add New Rule**: To create a schedule rule, click the “New Add” button. You can edit the **Name of Rule**, **Policy**, and set the schedule time (**Week day**, **Start Time**, and **End Time**). The following example configures “wake-up time“ everyday from 06:00 to 07:00.



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

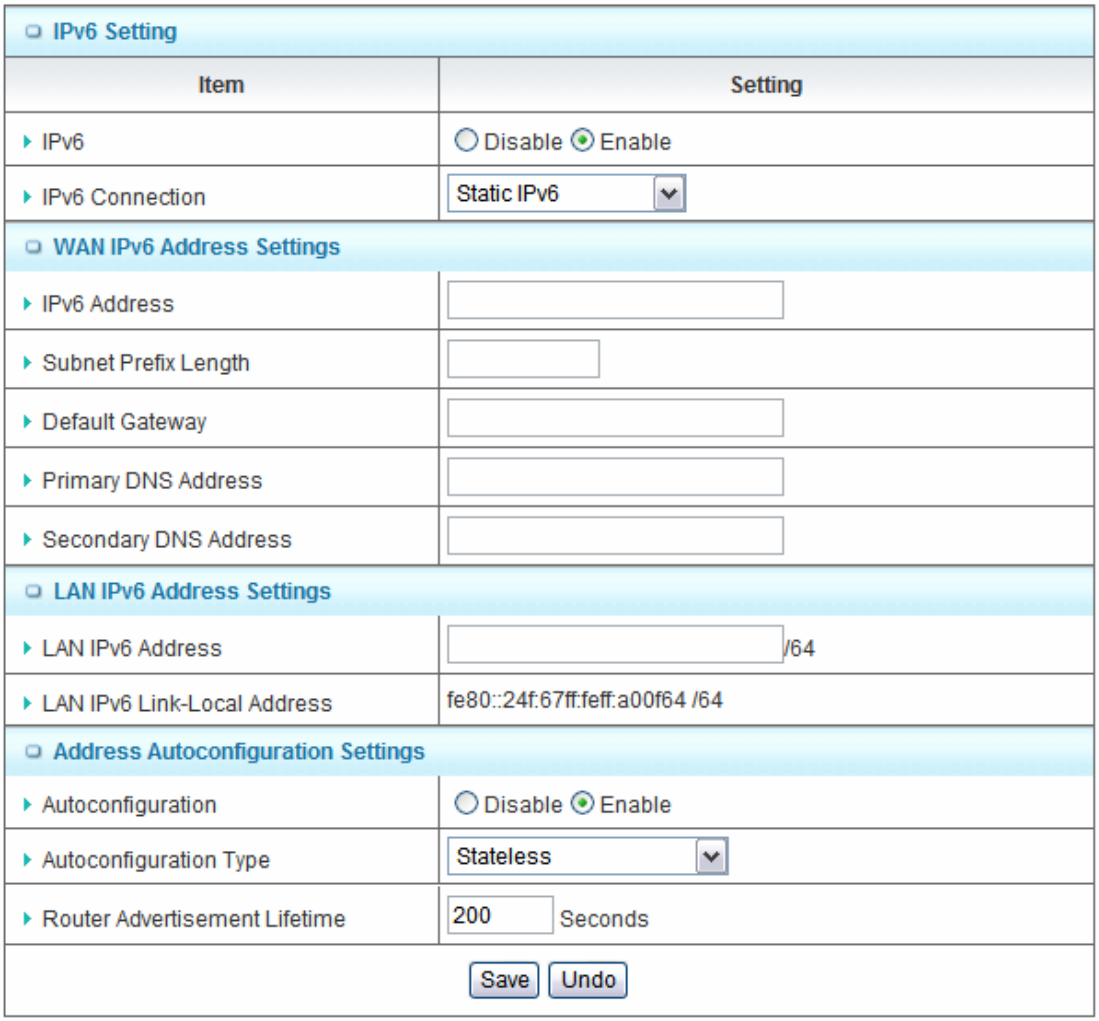
3.5.8 TR-069



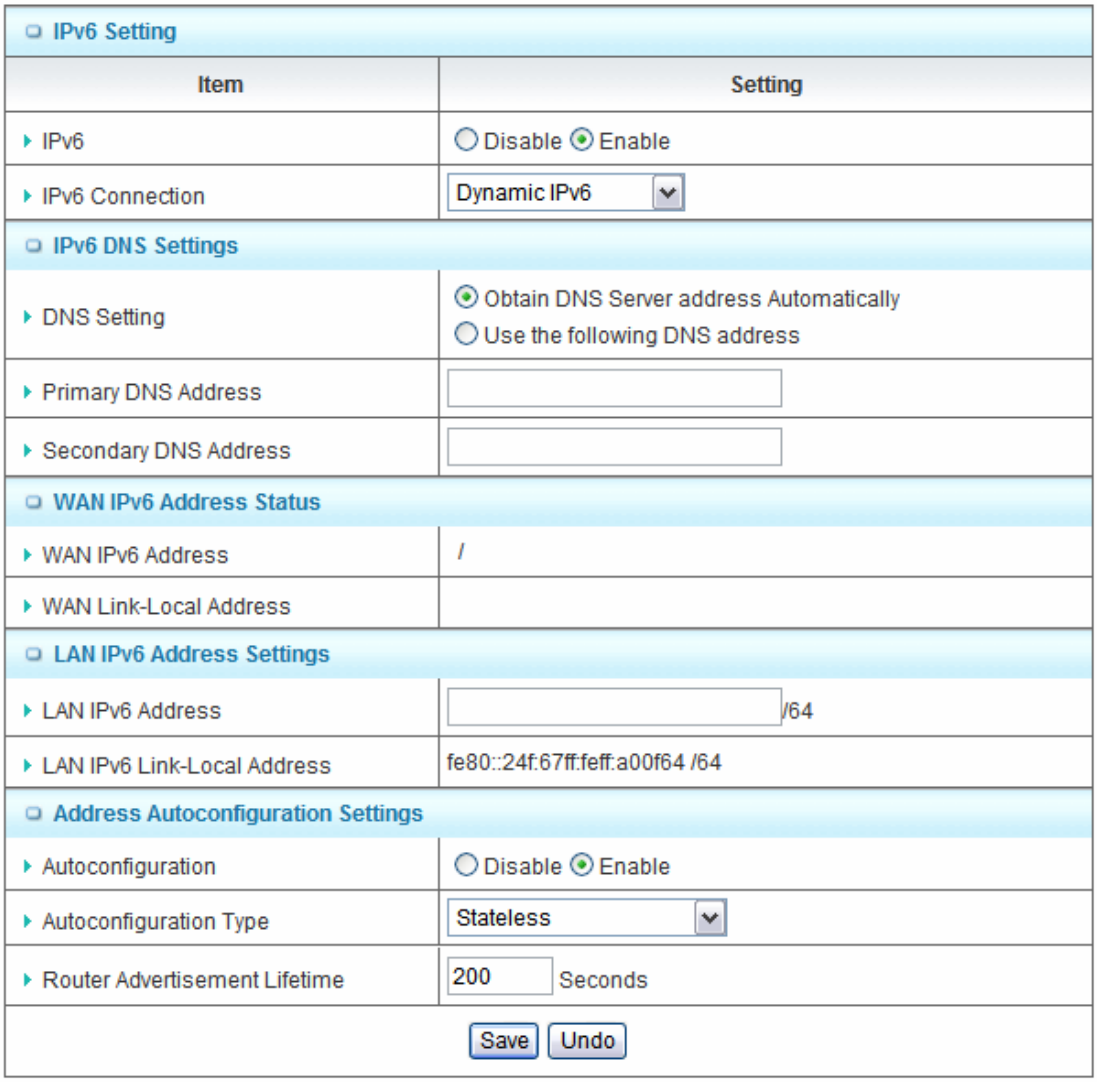
1. **TR-069**: Disable or enable the TR-069 settings.
2. **ACS setting**: you may add ACS URL/ Username/ Password.
3. **CPE setting**: you may add CPE connection request port/ username /password.
4. **Inform setting**: you may enable/disable the interval of informing CPE.

Note: TR-069 is a customized feature with ISP, please contact with us once you get any question.

3.5.9 IPv6 Setting



1. **IPv6 setting**: Disable or enable the IPv6 settings.
2. **IPv6 Connection**: you may select the connection of Static IPv6/ Dynamic IPv6 / 6to4/ 6 in IPv4 tunel.
3. **WAN IPv6 address setting**: you may add IPv6 address /subnet prefix length / default Gateway / Primary DNS address and secondary DNS address.
4. **LAN IPv6 address setting**: LAN IPv6 address and LAN IPv6 Link-Local address.
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.

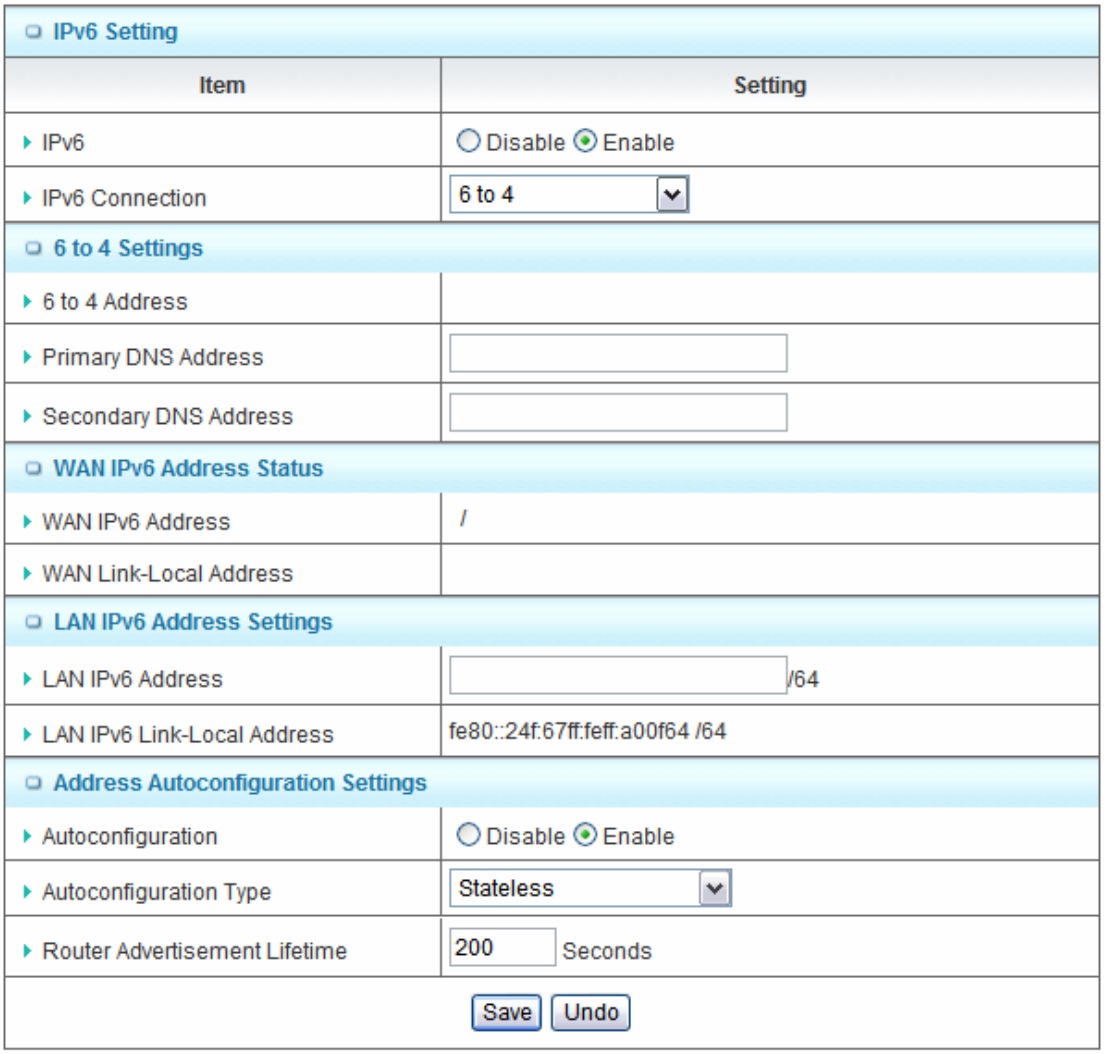


IPv6 Setting

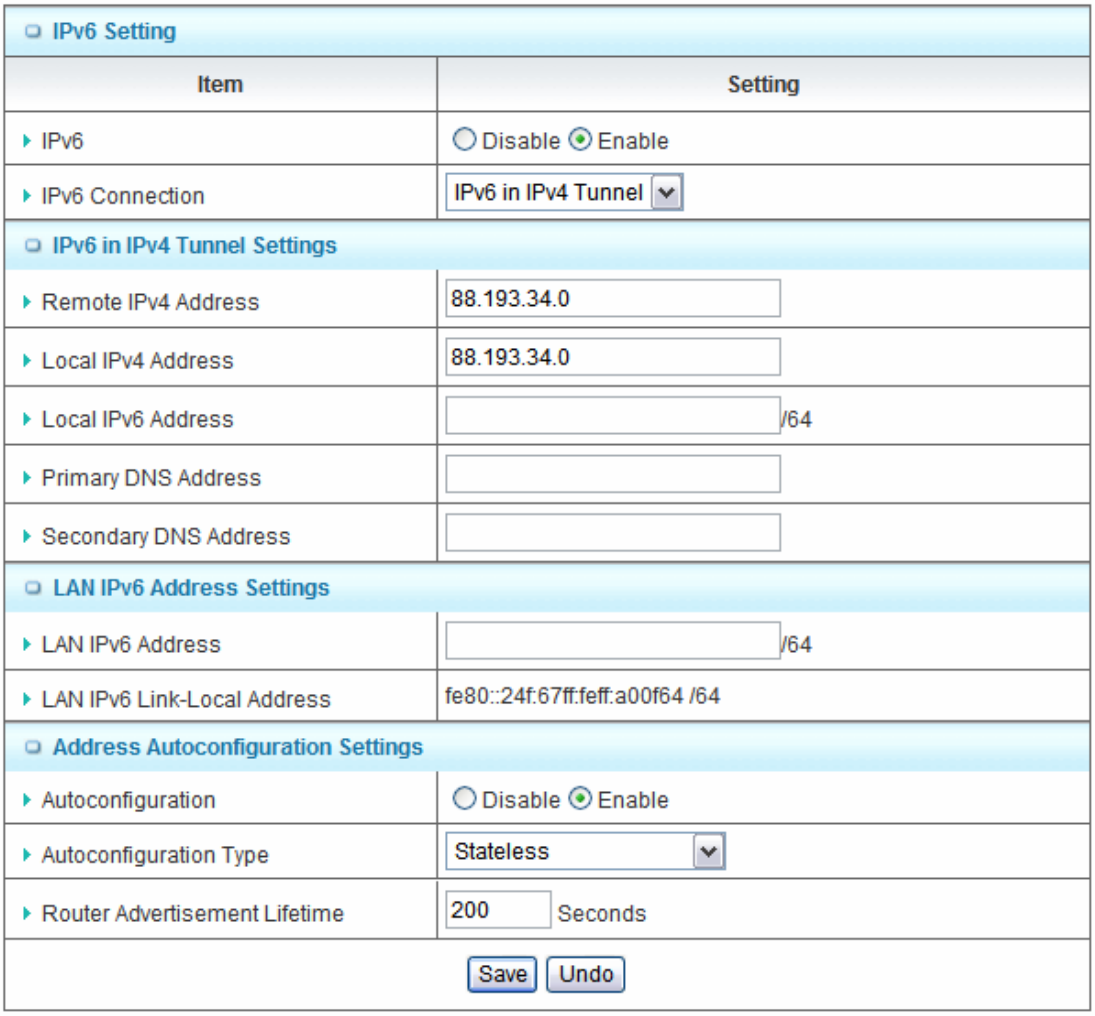
Item	Setting
IPv6	Disable Enable
IPv6 Connection	Dynamic IPv6
IPv6 DNS Settings	
DNS Setting	Obtain DNS Server address Automatically Use the following DNS address
Primary DNS Address	
Secondary DNS Address	
WAN IPv6 Address Status	
WAN IPv6 Address	/
WAN Link-Local Address	
LAN IPv6 Address Settings	
LAN IPv6 Address	/64
LAN IPv6 Link-Local Address	fe80::24f:67ff:feff:a00f64 /64
Address Autoconfiguration Settings	
Autoconfiguration	Disable Enable
Autoconfiguration Type	Stateless
Router Advertisement Lifetime	200 Seconds

Save Undo

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



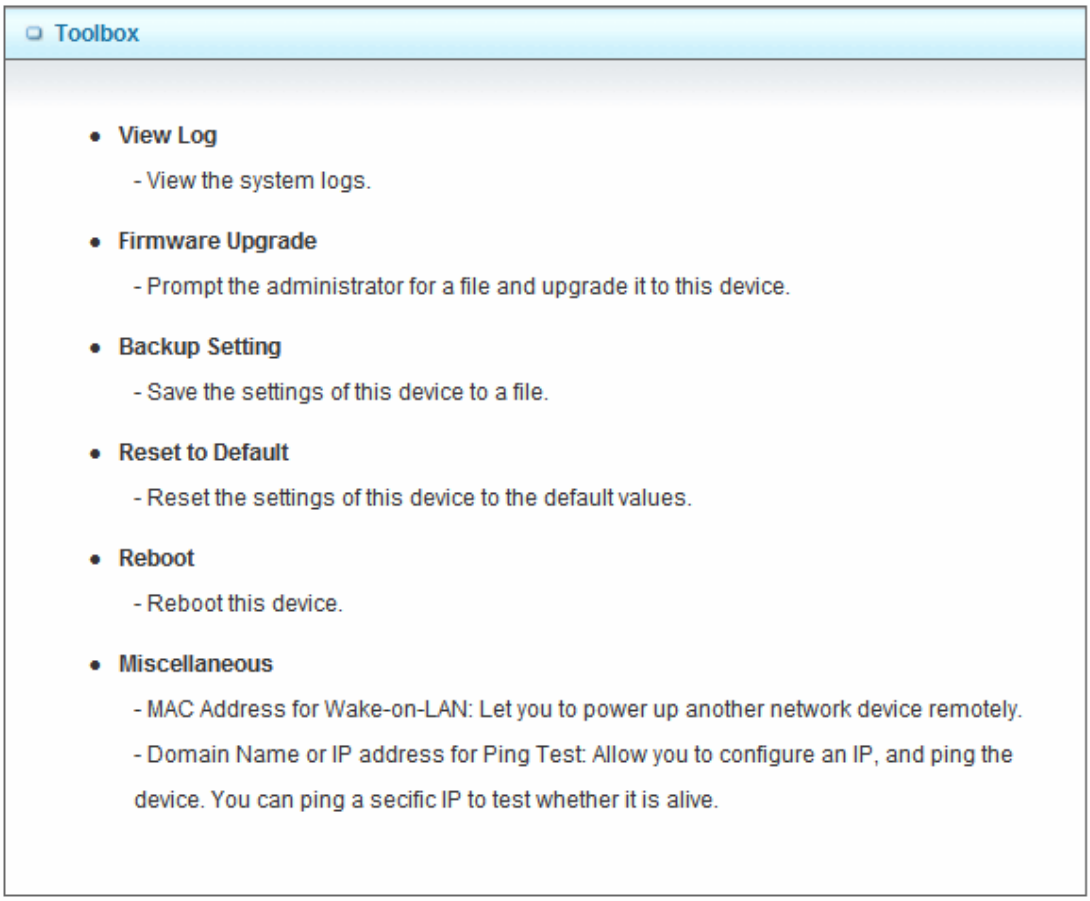
1. **WAN IPv6 address setting for 6to4**: you may obtain IPv6 DNS automatically or set DNS address manually for Primary DNS address and secondary DNS address.
2. **LAN IPv6 address setting**: LAN IPv6 address and LAN IPv6 Link-Local address.
3. **Address auto configuration setting:** Disable or enable this auto configuration setting. You may set stateless or stateful (Dynamic IPv6), and also check if need to send Router advertisement messages periodically.



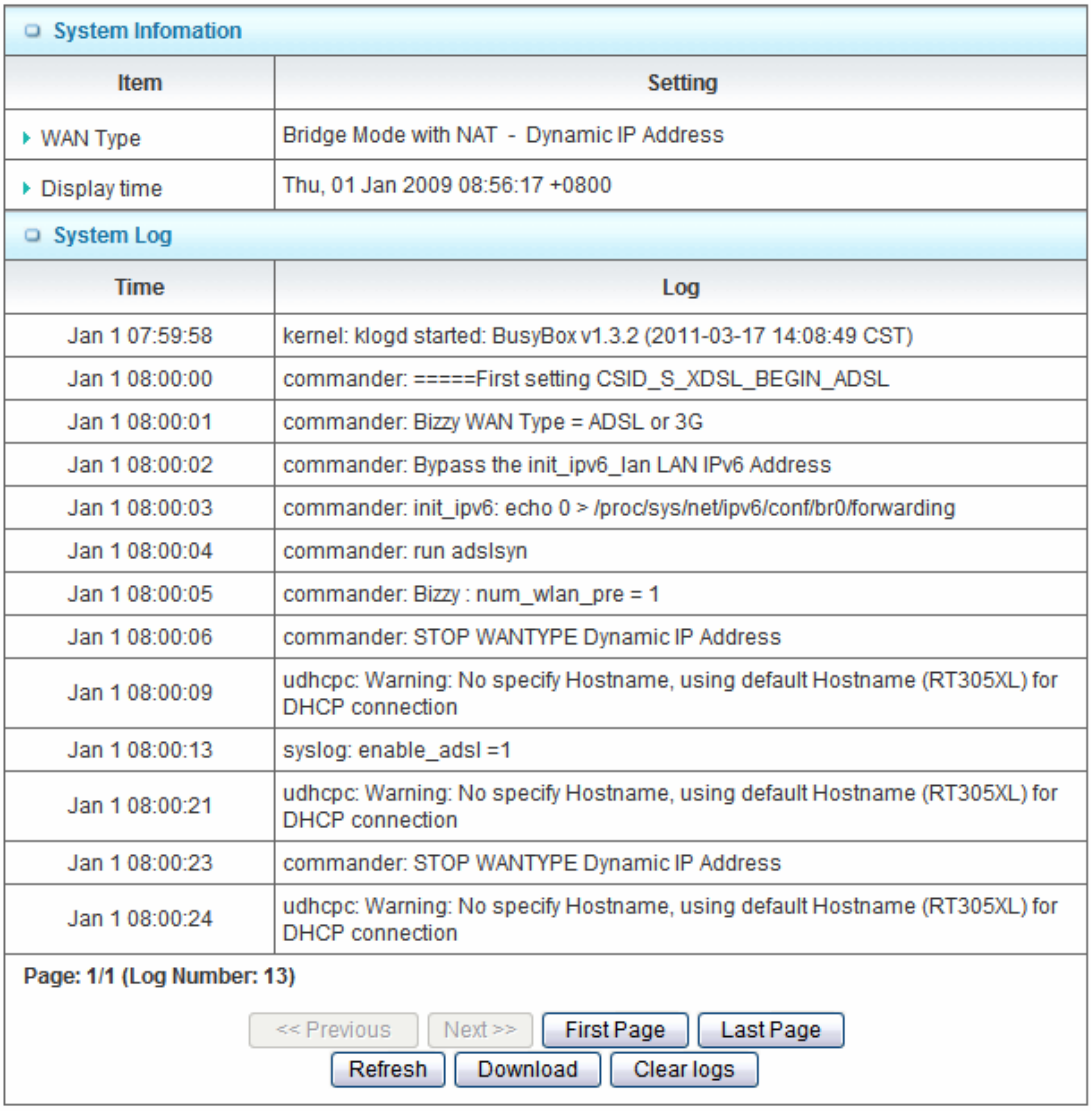
1. **WAN IPv6 address setting forIPv6 in IPv4 Tunnel**: you may add remote / local IPv4 address and local IPv6 address, then set DNS address manually for Primary DNS address and secondary DNS address.
2. **LAN IPv6 address setting**: LAN IPv6 address and LAN IPv6 Link-Local address.
3. **Address auto configuration setting:** Disable or enable this auto configuration setting. You may set stateless or stateful (Dynamic IPv6), and also check if need to send Router advertisement messages periodically.

3.6 Tool Box

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



3.6.1 System Information



System Infomation

Item	Setting
WAN Type	Bridge Mode with NAT - Dynamic IP Address
Display time	Thu, 01 Jan 2009 08:56:17 +0800

System Log

Time	Log
Jan 1 07:59:58	kernel: klogd started: BusyBox v1.3.2 (2011-03-17 14:08:49 CST)
Jan 1 08:00:00	commander: =====First setting CSID_S_XDSL_BEGIN_ADSL
Jan 1 08:00:01	commander: Bizzy WAN Type = ADSL or 3G
Jan 1 08:00:02	commander: Bypass the init_ipv6_lan LAN IPv6 Address
Jan 1 08:00:03	commander: init_ipv6: echo 0 > /proc/sys/net/ipv6/conf/br0/forwarding
Jan 1 08:00:04	commander: run adslsyn
Jan 1 08:00:05	commander: Bizzy : num_wlan_pre = 1
Jan 1 08:00:06	commander: STOP WANTYPE Dynamic IP Address
Jan 1 08:00:09	udhcpc: Warning: No specify Hostname, using default Hostname (RT305XL) for DHCP connection
Jan 1 08:00:13	syslog: enable_adsl =1
Jan 1 08:00:21	udhcpc: Warning: No specify Hostname, using default Hostname (RT305XL) for DHCP connection
Jan 1 08:00:23	commander: STOP WANTYPE Dynamic IP Address
Jan 1 08:00:24	udhcpc: Warning: No specify Hostname, using default Hostname (RT305XL) for DHCP connection

Page: 1/1 (Log Number: 13)

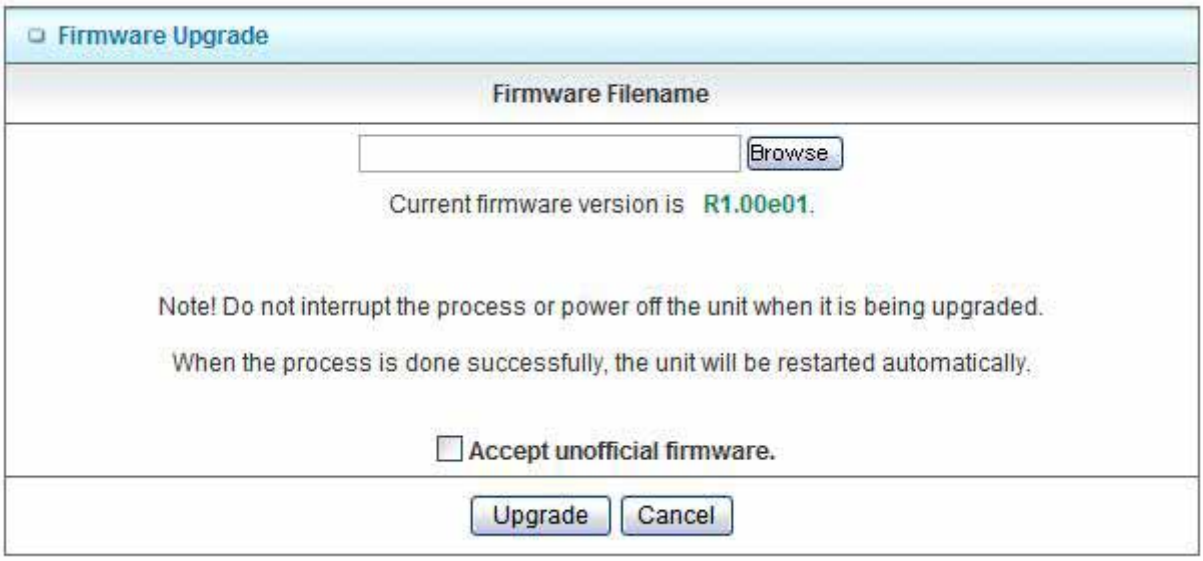
<< Previous | Next >> | First Page | Last Page

Refresh | Download | Clear logs

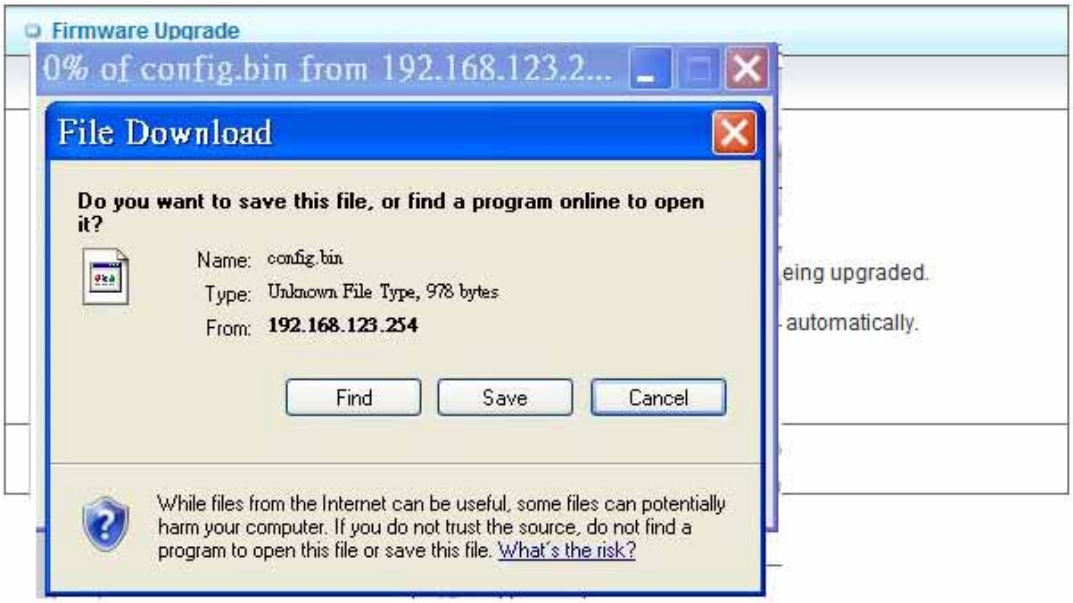
You can view the System Information and System log, and download/clear the System log, in this page.

3.6.2 Firmware Upgrade

You can upgrade firmware by clicking “Upgrade” button.

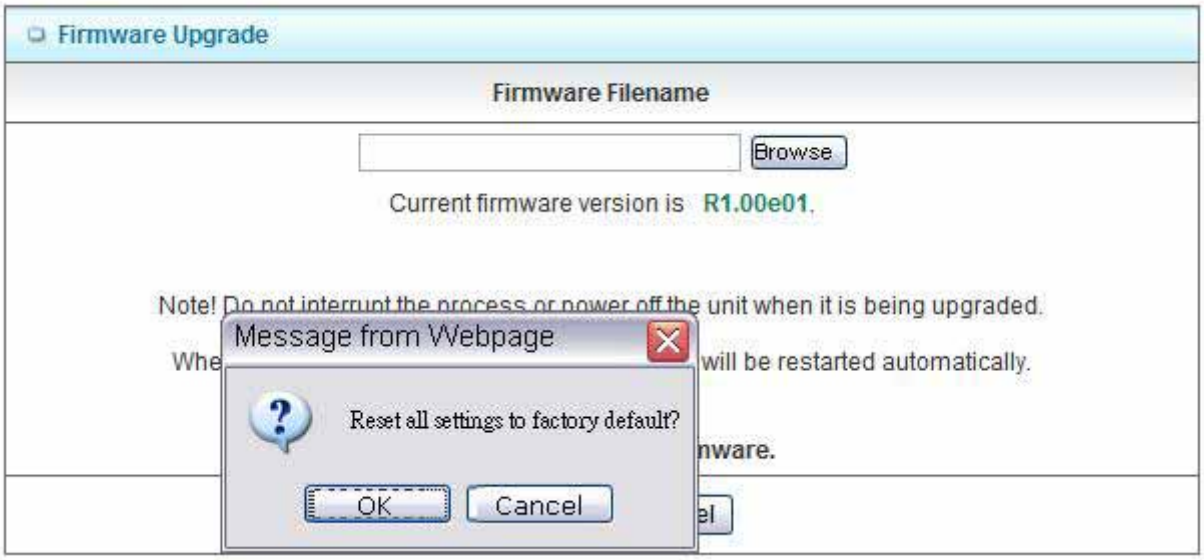


3.6.3 Backup Setting



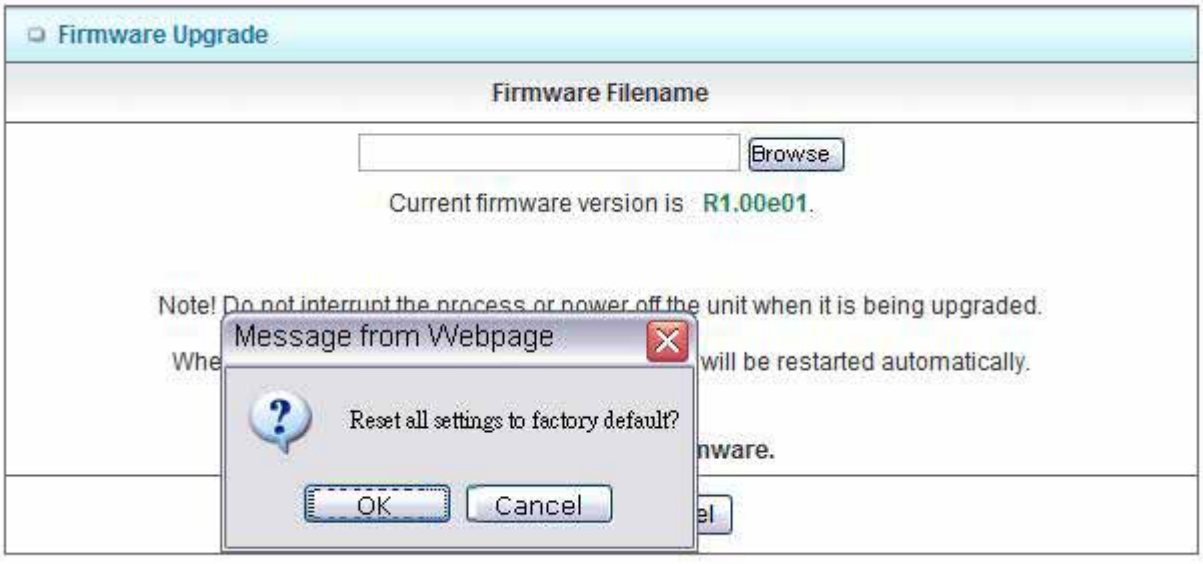
You can backup your settings by clicking the “**Backup Setting”** function item and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you saved.

3.6.4 Reset to Default



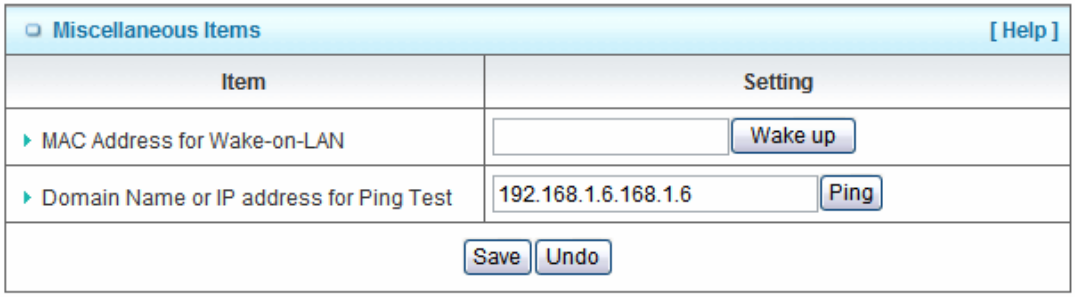
You can also reset this device to factory default settings by clicking the **Reset to default** function item.

3.6.5 Reboot



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

3.6.6 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. Afterwards, click "Wake up" button which makes the router to send the wake-up frame to the target device immediately.

2. **Domain Name or IP address for Ping Test**: Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

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

4 Appendix

4.1 Troubleshooting

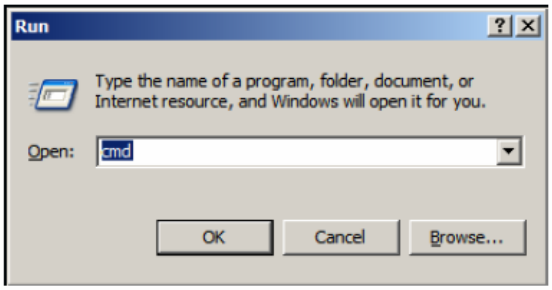
Q: Why can't I configure the router even the cable is plugged and the LED is lit?

A:

Do a **Ping test** to make sure that the WN-220ARM is responding.

Go to **Start > Run**.

1. Type **cmd**.



2. Press **OK.**
3. Type **ipconfig** to get the IP of default gateway.
4. Type "**ping 192.168.1.254".** Assure that you ping the correct IP Address assigned to the WiFi Broadband 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
```

Ensure that your Ethernet Adapter is working, and that all network drivers are installed properly. Network adapter names will vary depending on your

specific adapter. The installation steps listed below are applicable for all network adapters.

1. Go to **Start > Right click on "My Computer" > Properties**.
2. **Select** the **Hardware Tab**.
3. Click **Device Manager**.
4. Double-click on "**Network Adapters"**.
5. Right-click on **Wireless Card bus Adapter** or **your specific network adapter**.
6. Select **Properties** to ensure that all drivers are installed properly.
7. Look under **Device Status** to see if the device is working properly.
8. Click "**OK"**.

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

A:

1. Make sure the RJ45 cable connects with the router.
2. Ensure that the setting on your Network Interface Card adapter is "Enabled".
3. 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.
4. If the connection still doesn't work properly, then you can reset it to default.

Q: Something wrong with the wireless connection?

A:

A. Can't setup a wireless connection?

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

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

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

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

V. Ensure that the LEDs are indicating normally. If not, make sure that the power and Ethernet cables are firmly connected.

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

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

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

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

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

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

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

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

iii. Reset the WiFi Broadband Router to default setting

C. Why does my wireless connection keep dropping?

I. Antenna Orientation.

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

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

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

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

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

A:

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

Q: How to reset to default?

A:

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