



WN-220R

150Mbps SOHO Wireless Router

User's Manual





Copyright & Disclaimer

No part of this publication may be reproduced in any form or by any means, whether electronic, mechanical, photocopying, or recording without the written consent of OvisLink Corp.

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

All Trademarks are properties of their respective holders.



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.



© 2009 OvisLink Corporation, All Rights Reserved



Table of Contents

1. Introduction	1
1.1 Overview	1
1.2 Support	2
1.3 Features	2
1.4 Packing List	3
1.5 Specification Table	3
1.6 Hardware Configuration	5
1.6.1 Front View	5
1.6.2 Rear View	5
1.6.3 LED Indicator	6
1.6.4 Button Definition	6
1.6.5 Hardware Installation	7
2. Getting Start	8
3. Making Configuration	14
3.1 Login to Configure from Wizard	15
3.2 System Status	19
3.3 Advanced	20
3.3.1 Basic Setting	20
3.3.2 Forwarding Rules	41
3.3.3 Security Settings	45
3.3.4 Advanced Settings	59
3.3.5 Toolbox	69
Appendix: FAQ and Troubleshooting	73



1

Introduction



1.1 Overview

AirLive WN-220R is the center of your home or office network, you can share a high-speed Internet connection with the flexibility, speed, security and simplicity! The WN-220R conforms to wireless 802.11b/g/n demand, and provides up to 150Mbps wireless speed. Its additional 4 Ethernet cable ports let the user connect your whole wired and wireless devices together.

WN-220R also supports various ways for connecting to your Internet Service Provider, such as static IP, dynamic IP (DHCP), or PPPoE. More over, with the Setup Wizard provided in the bundle CD, you can simply connect your network-able device to the world in few minutes.

If not specify, “Router” means WN-220R in the following paragraph.



1.2 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 firmware that either increase software functions or provide bug fixes for WN-220R. 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

Instant Support : Subscribe Language :

All Products

Product Main Category	Product Secondary Category	Model NO
Print Server	11a/b/g/n Indoor	WN-220R
Router	11a/b/g Outdoor	
Security Gateway	11b/g Indoor	
Skype	11b/g Outdoor	
Switches	PCBA	
VoIP		
Wireless Indoor		
Wireless Accessory		
Wireless Outdoor		
WISP		

Figure 1.4: AirLive Newsletter Support System

1.3 Features

- Enjoy Your AirLive Wireless
- Compatible with AirLive Wireless IP Camera
- Green WLAN for Smart Power Saving
- Support Easy Setup Wizard



1.4 Packing List

- WN-220R + Antenna
- Power adapter 5V 1A
- CD
- Quick Setup Guide

1.5 Specification Table

Hardware	
Ethernet WAN	RJ-45 port, 10/100Mbps, auto-MDI/MDIX
Ethernet LAN	RJ-45 port, 10/100Mbps, auto-MDI/MDIX
WPS Button	For WPS connection
Reset Button	Reset router setting to factory default
LED Indication	Status / WAN / LAN1 ~ LAN4/ Wireless
Power Jack	DC Power Jack, powered via external DC 5V/1A switching power adapter
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 (WiFi Protected Setup)
WMM	WMM (WiFi Multimedia)
Functionality	
Ethernet WAN	PPPoE, DHCP client, Static IP
WAN Connection	Auto-reconnect, dial-on-demand, manually
One-to-Many NAT	Virtual server, special application, DMZ

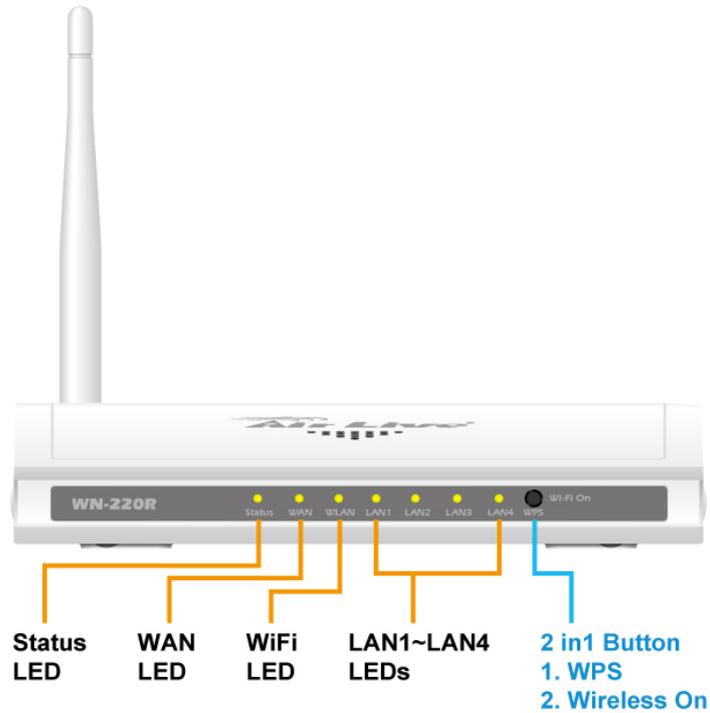


NAT Session	Support NAT session: 10000
SPI Firewall	IP/Service filter, URL blocking, MAC Control
DoS Protection	DoS (Deny of Service) detection and protection
Routing Protocol	Static route, dynamic route (RIP v1/v2)
Management	SNMP, UPnP IGD, syslog, DDNS
Administration	Web-based UI, remote login, backup/restore setting
Performance	NAT up to 90Mbps and Wireless up to 70Mbps
Environment & Certification	
Package Information	WN-220R, DC 5V/1A power adapter, Quick Installation Guide
Operation Temp.	Temp.: 0~40°C, Humidity 10%~90% non-condensing
Storage Temp.	Temp.: -10~70°C, Humidity: 0~95% non-condensing
EMI Certification	CE/FCC compliance
RoHS	RoHS compliance

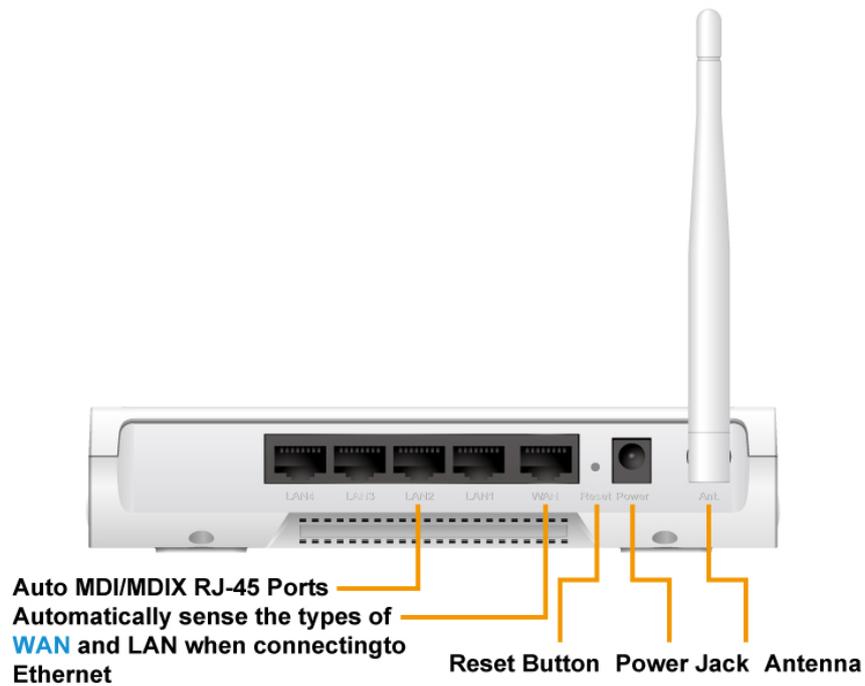


1.6 Hardware Configuration

1.6.1 Front View



1.6.2 Rear View





1.6.3 LED Indicator

	LED status	Description
Status	Green in flash	Device status is working.
WAN LED	Green	RJ45 cable is plugged
	Green in flash	Data access
LAN LED	Green	RJ45 cable is plugged
	Green in flash	Data access
WiFi LED	Green	WLAN is on
	Green in flash	Data access
	Green in fast flash	Device is in WPS PBC mode
	Green in dark	WiFi Radio is disabled

1.6.4 Button Definition

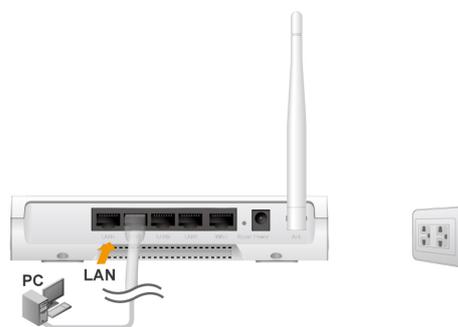
	Description
Enable "Wireless" and WPS	<ol style="list-style-type: none"> 1. When Wireless is off, press this button (about 1 sec) to enable "Wireless Radio". 2. When Wireless is On, press this button (about 1 sec) to execute WPS function.
Reset	Press (6) sec to reset to default when the device works simultaneously.



1.6.5 Hardware Installation

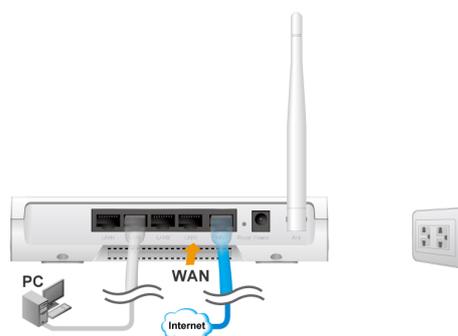
Step 1. Insert the Ethernet cable into LAN Port:

Insert the Ethernet patch cable into LAN port on the back panel of Router, and an available Ethernet port on the network adapter in the computer you will use to configure the unit.



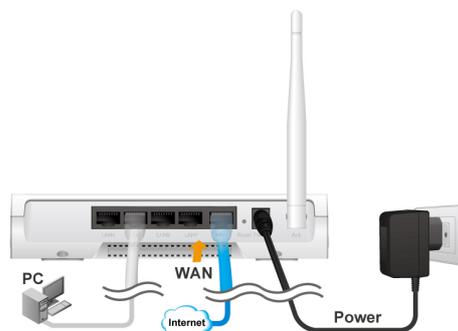
Step 2. Insert the Ethernet patch cable into Wired WAN port:

Insert the Ethernet patch cable from DSL Modem into Wired WAN port on the back panel of Router.



Step 3. Power on Router:

Connect the power adapter to the receptor on the back panel of your Router.



Step 4. Complete the setup.

When complete, the Status LED will flash.





2

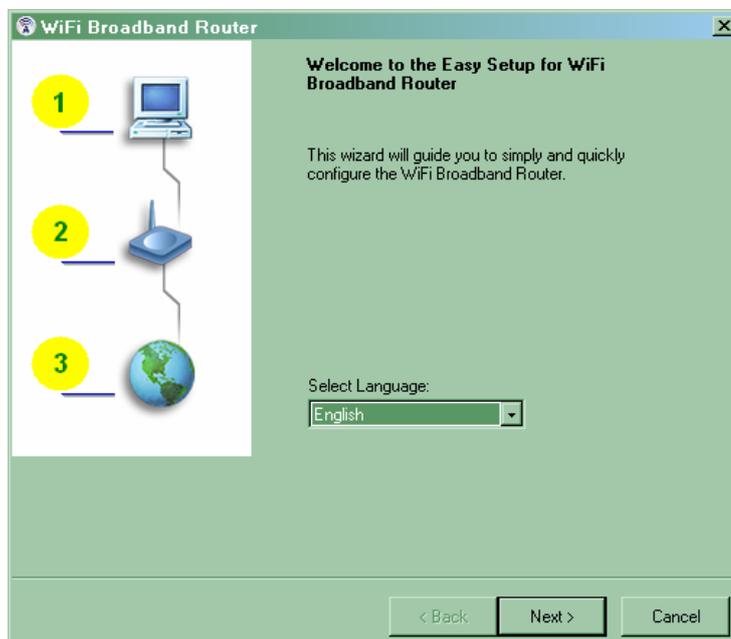
Getting Start

With the wizard utility, you might configure your Router in just few steps. Please insert the bundle CD into your CD drive and follow the description below for configuring your Router.

Select the “Install Driver & Utility” on the menu.



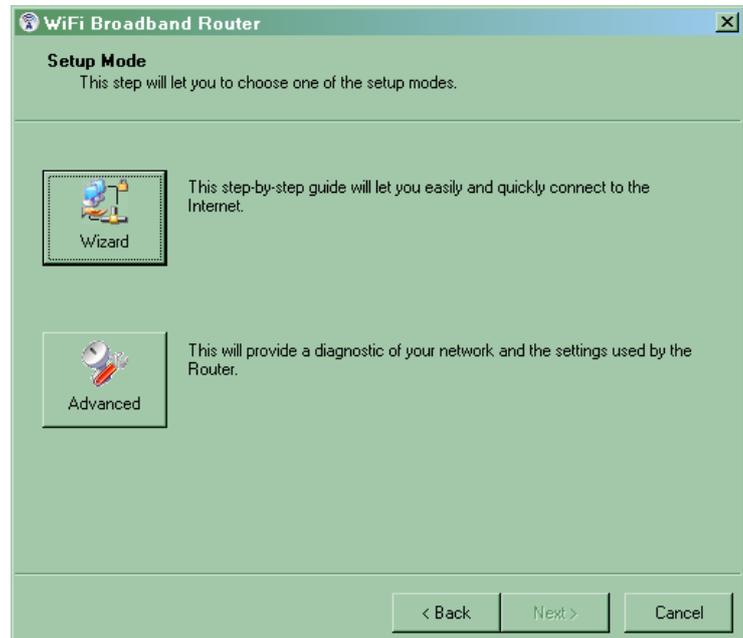
After the Utility shows up, please select Language then click “Next” for continues.





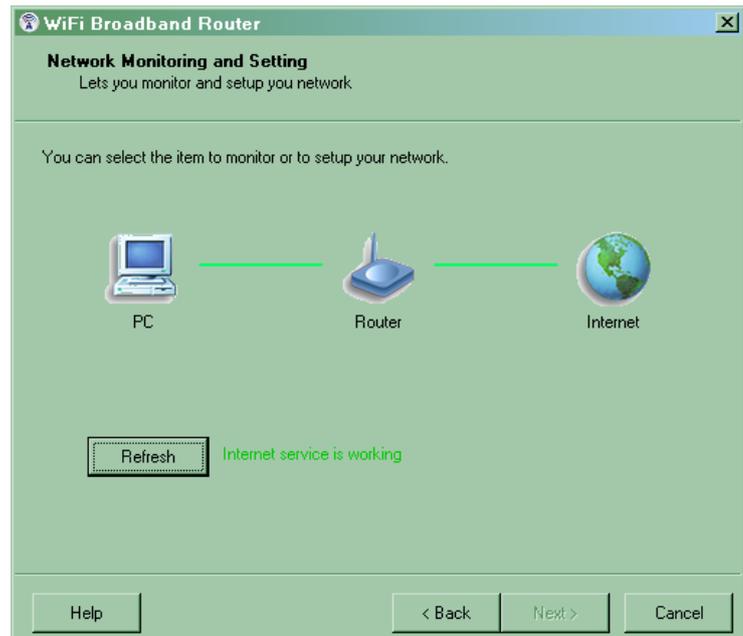
Setup mode

You can select Wizard mode to run the setup step-by-step or run advanced mode to diagnose the network settings of the router.



Advanced mode Setup

Check the PC, Router or Internet icons for the Status of PC, Router or Internet.

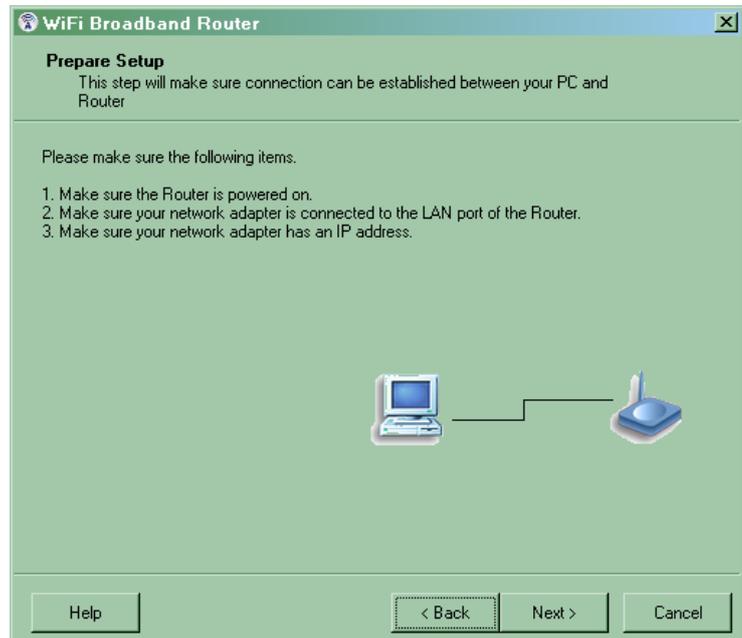




Quick Wizard Install mode Setup

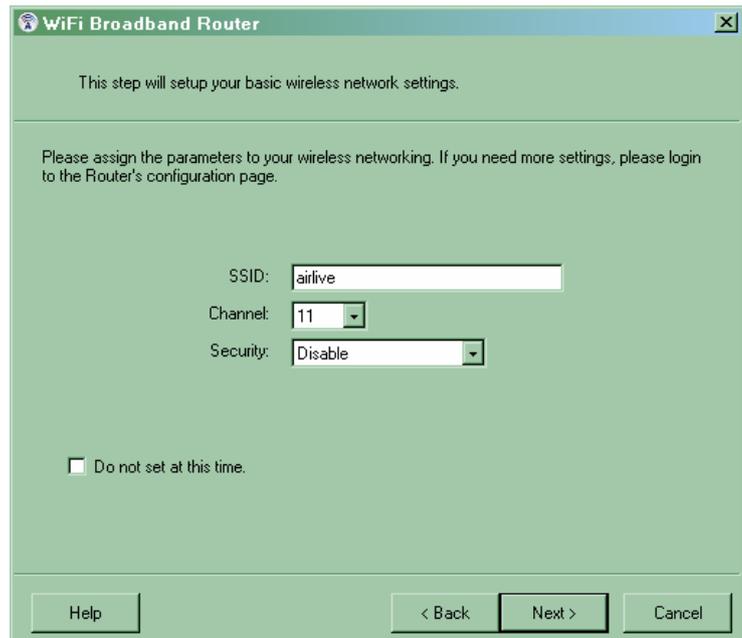
1. Make sure the router is powered on.
2. Make sure your network adapter is connected to the LAN port of the router
3. Make sure your network adapter has an IP address.

Click “Next” for continues



Wireless Setting

Key in the SSID, Channel and Security options, and then click “Next” for continues.



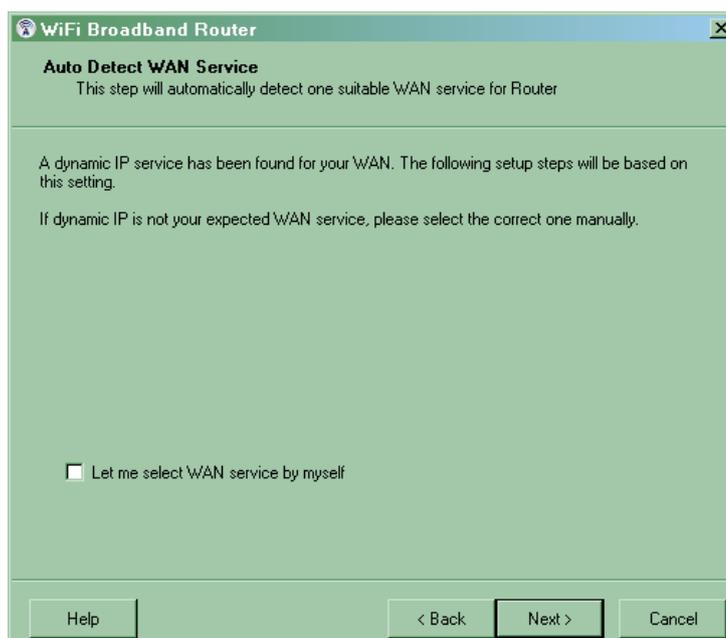
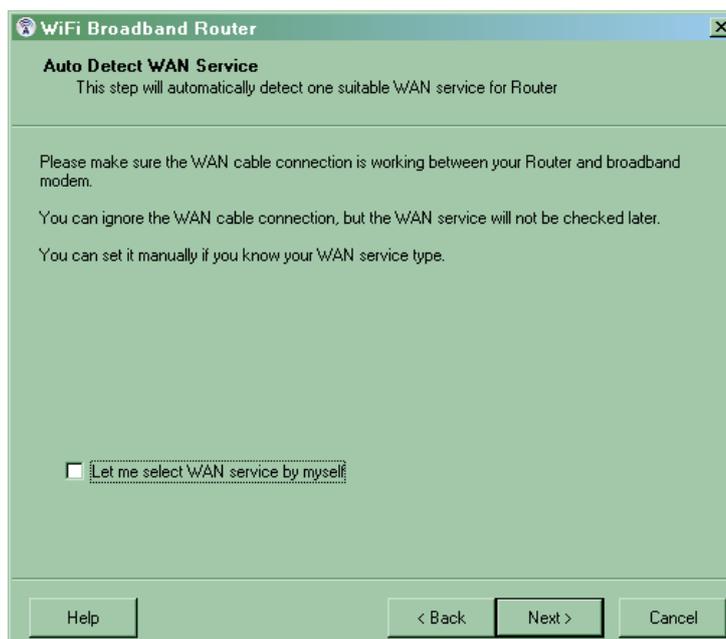


Auto Detect WAN Service

Click “Next” for continue.

Click the button, “Let me select WAN service by myself”, to disable this function.

Note: The Item supports to detect the Dynamic and PPPoE WAN Services only



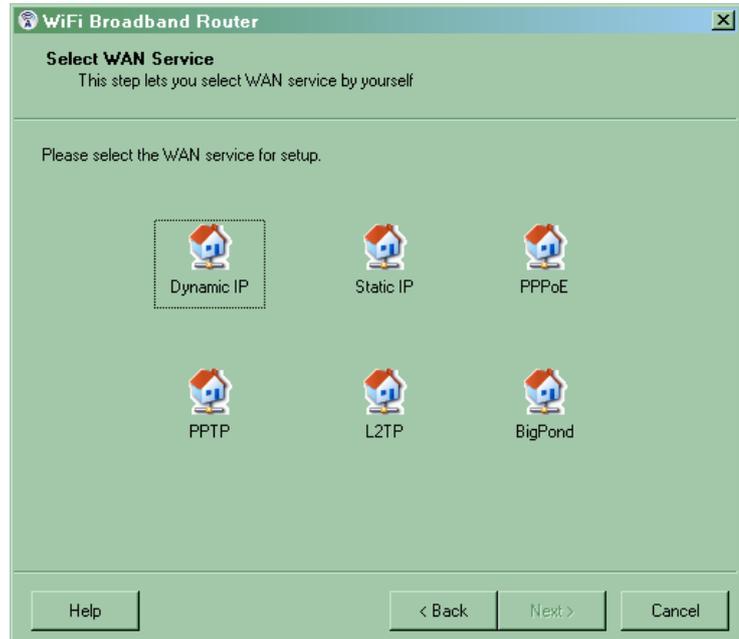
Example, the Dynamic WAN type is detected.

Manual select WAN Service

In the manual mode, Click the any icons for continues.

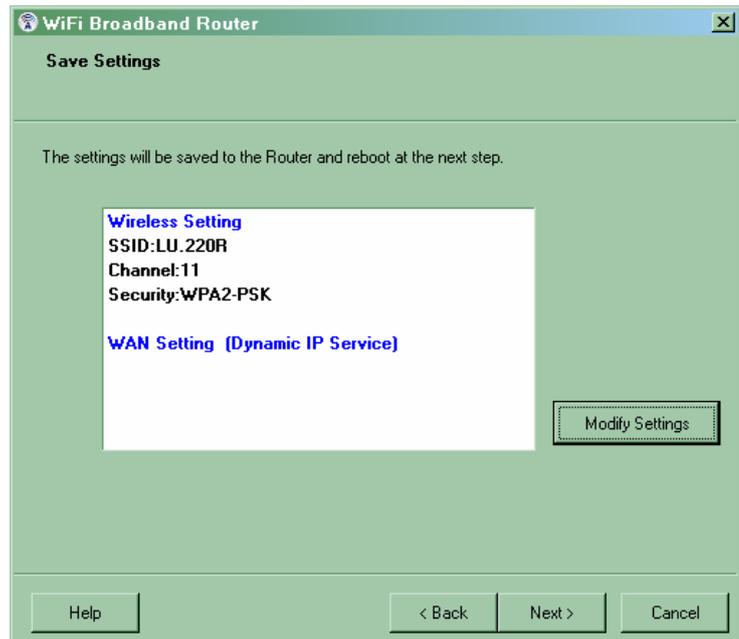
Summary of the settings and Next to “Reboot”

Click “Next” for continue.



Apply the Settings or Modify

Click “Next” for continue.

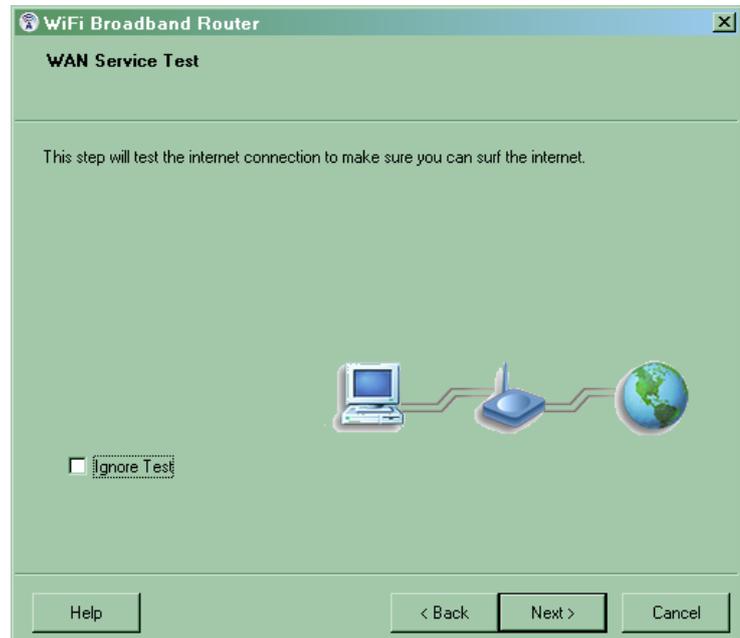




Test the Internet connection

Test WAN Networking service. Click “Next” for continue.

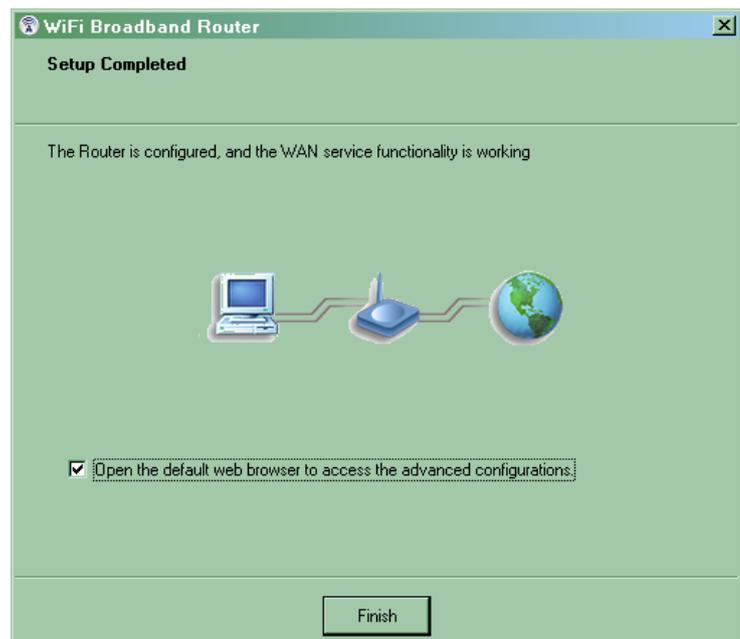
You can ignore the by select the “Ignore Test”.



Setup Completed

The EzSetup is finish; you can open the default web browser to configure advanced settings of the Router.

Click “Finish” to complete the installation.

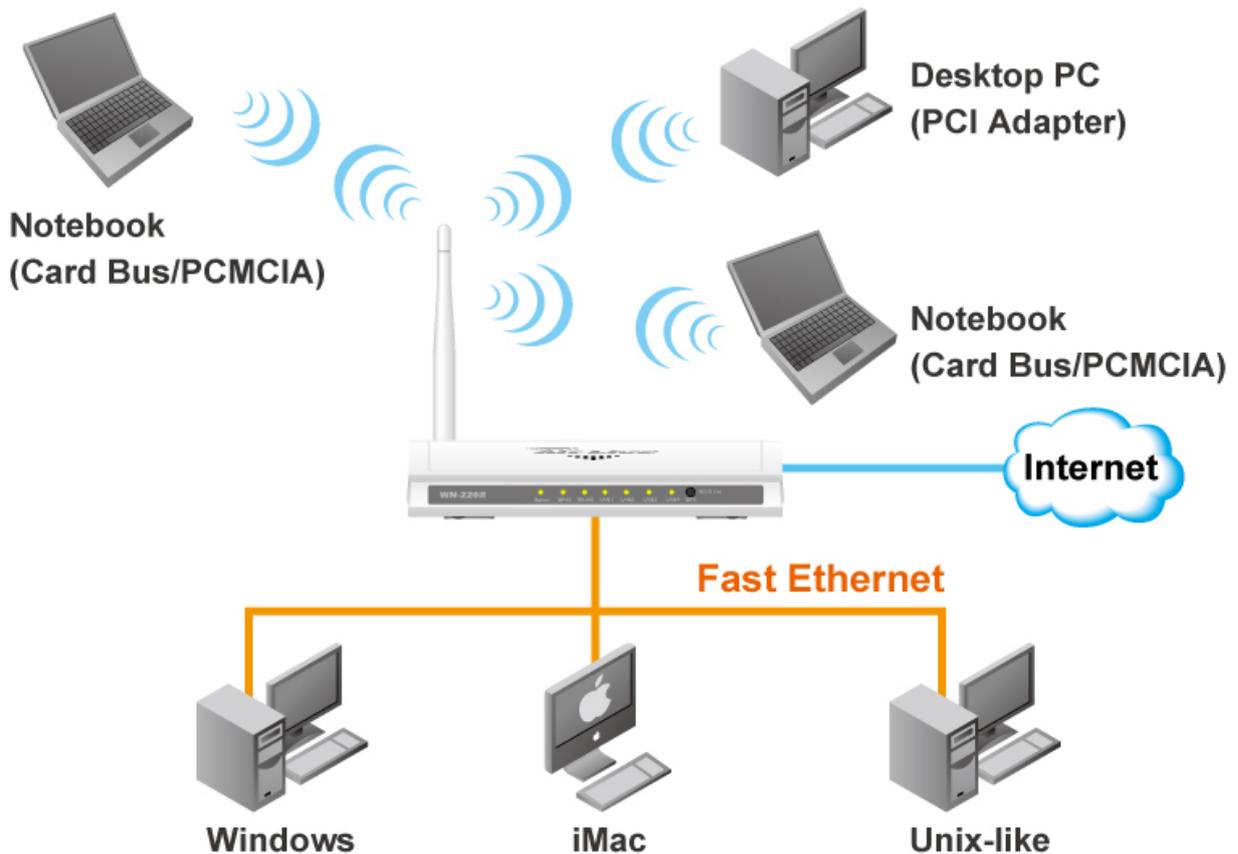




3

Making Configuration

WN-220R provides Web based configuration scheme that is, configuring by your Web browser, such as Mozilla Firefox or Internet Explorer. This approach can be adopted in any MS Windows, Macintosh or UNIX based platforms.



3.1 Login to Configure from Wizard

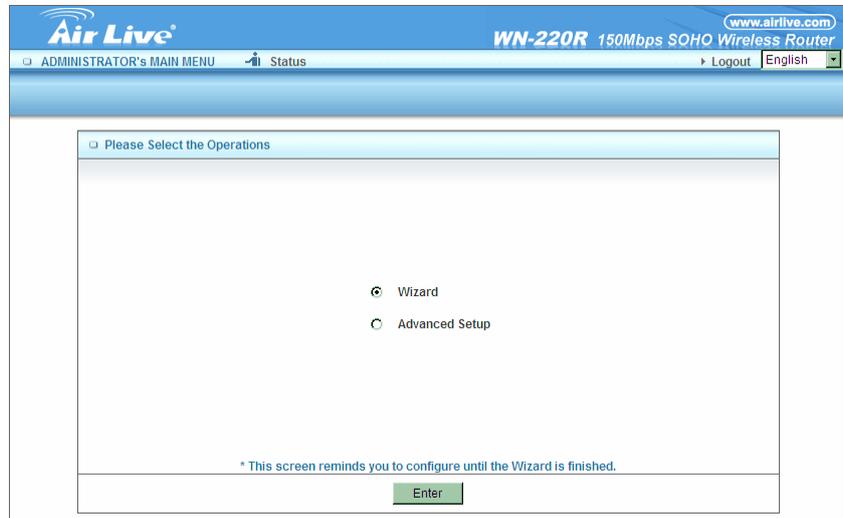
Type in the IP Address
(<http://192.168.1.254>)



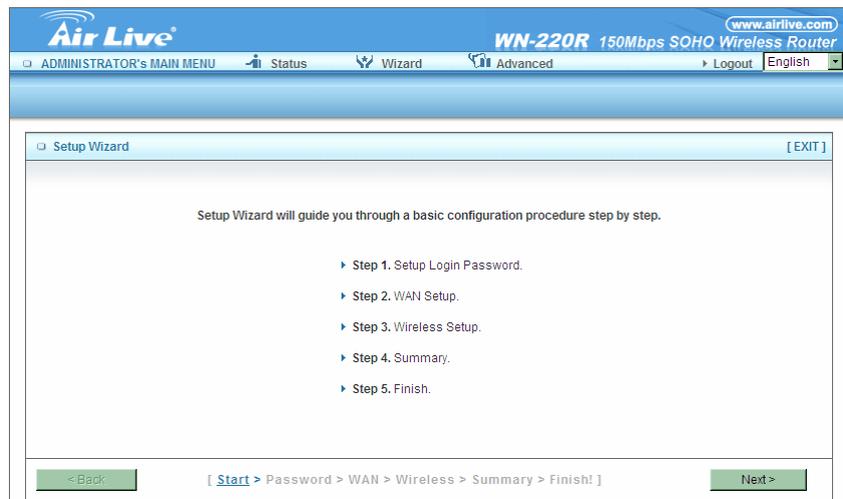
Type password, the default is “airlive” and click ‘login’ button.



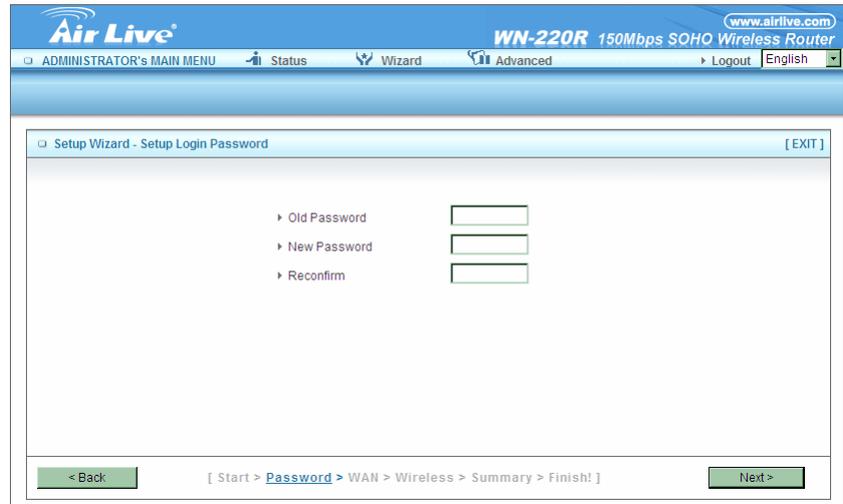
Press “Wizard” for basic settings with simple way.



Press “Next” to start wizard.

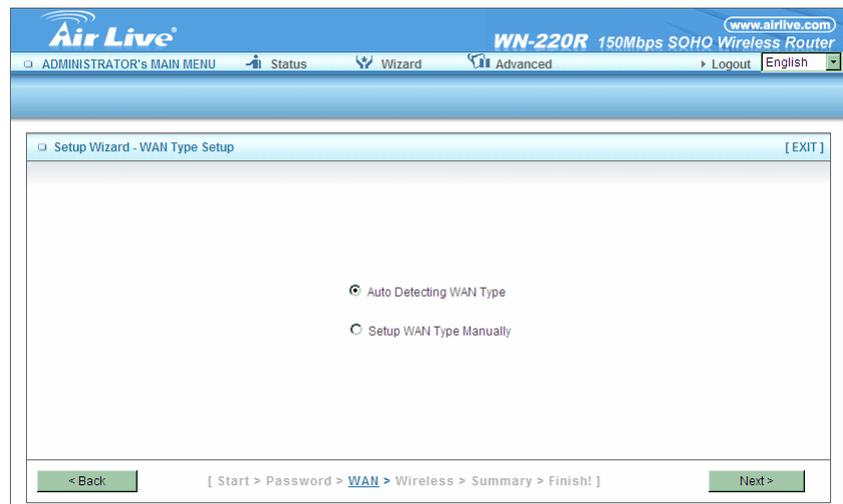
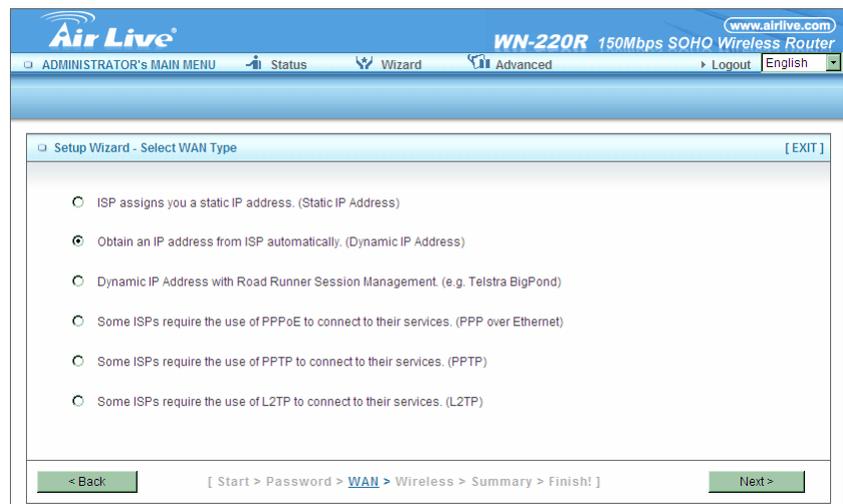


Step 1:
Set up your system password.



Step 2:
Select Wan Type.

Auto Detecting or
Setup Manually.

Step 3:
Setup the LAN IP and WAN Type.



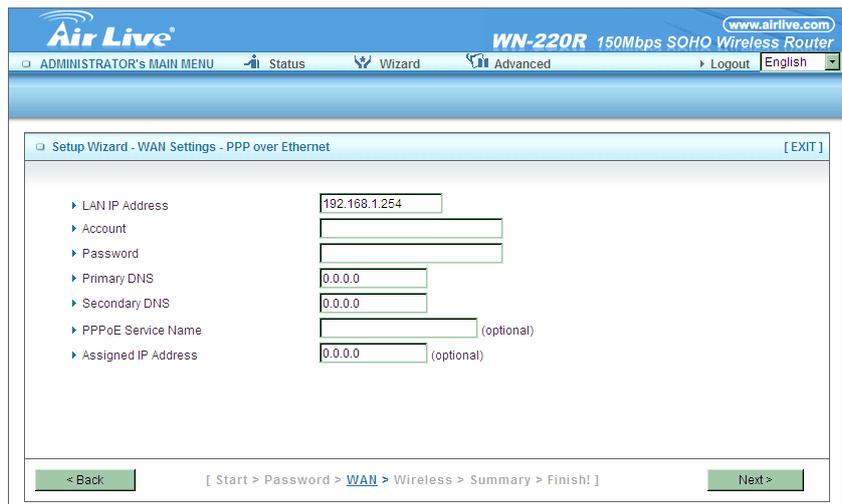
The screenshot shows the 'Setup Wizard - WAN Settings - Dynamic IP Address' page. The interface includes a navigation bar at the top with 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', 'Logout', and 'English'. The main content area has the following fields:

- LAN IP Address: 192.168.1.254
- Host Name: My Host (optional)
- WAN's MAC Address: 00-4F-67-00-02-03 with a 'Clone MAC' button

At the bottom, there are '< Back' and 'Next >' buttons, and a breadcrumb trail: [Start > Password > WAN > Wireless > Summary > Finish!]

Step 4:
Please fill in PPPoE service information which is provided by your ISP.

Example:



The screenshot shows the 'Setup Wizard - WAN Settings - PPP over Ethernet' page. The interface is similar to the previous step. The main content area has the following fields:

- LAN IP Address: 192.168.1.254
- Account: [Empty text box]
- Password: [Empty text box]
- Primary DNS: 0.0.0.0
- Secondary DNS: 0.0.0.0
- PPPoE Service Name: [Empty text box] (optional)
- Assigned IP Address: 0.0.0.0 (optional)

At the bottom, there are '< Back' and 'Next >' buttons, and a breadcrumb trail: [Start > Password > WAN > Wireless > Summary > Finish!]

Step 5:
Set up your Wireless.



The screenshot shows the 'Setup Wizard - Wireless settings' page. The interface is similar to the previous steps. The main content area has the following fields:

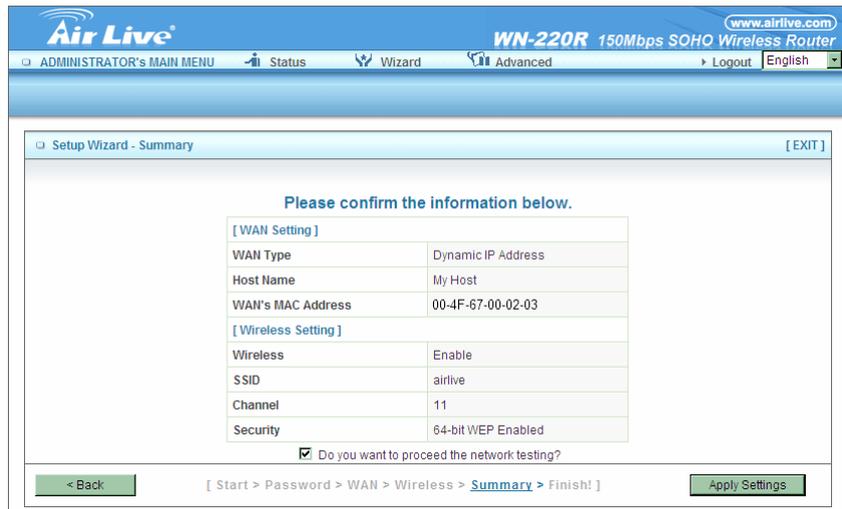
- Wireless function: Enable Disable
- Network ID(SSID): airlive
- Channel: 11

At the bottom, there are '< Back' and 'Next >' buttons, and a breadcrumb trail: [Start > Password > WAN > Wireless > Summary > Finish!]

Set up your Authentication and Encryption.



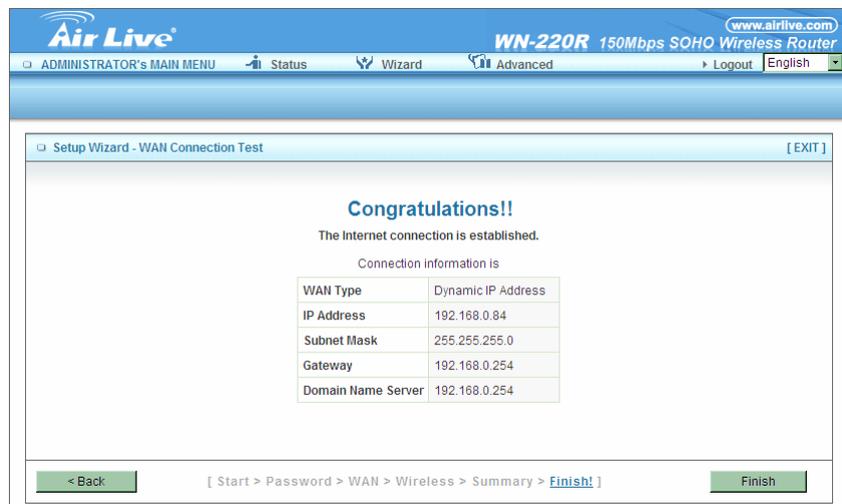
Step 6:
Then click Apply Setting.
And then the device will reboot.



[WAN Setting]	
WAN Type	Dynamic IP Address
Host Name	My Host
WAN's MAC Address	00-4F-67-00-02-03

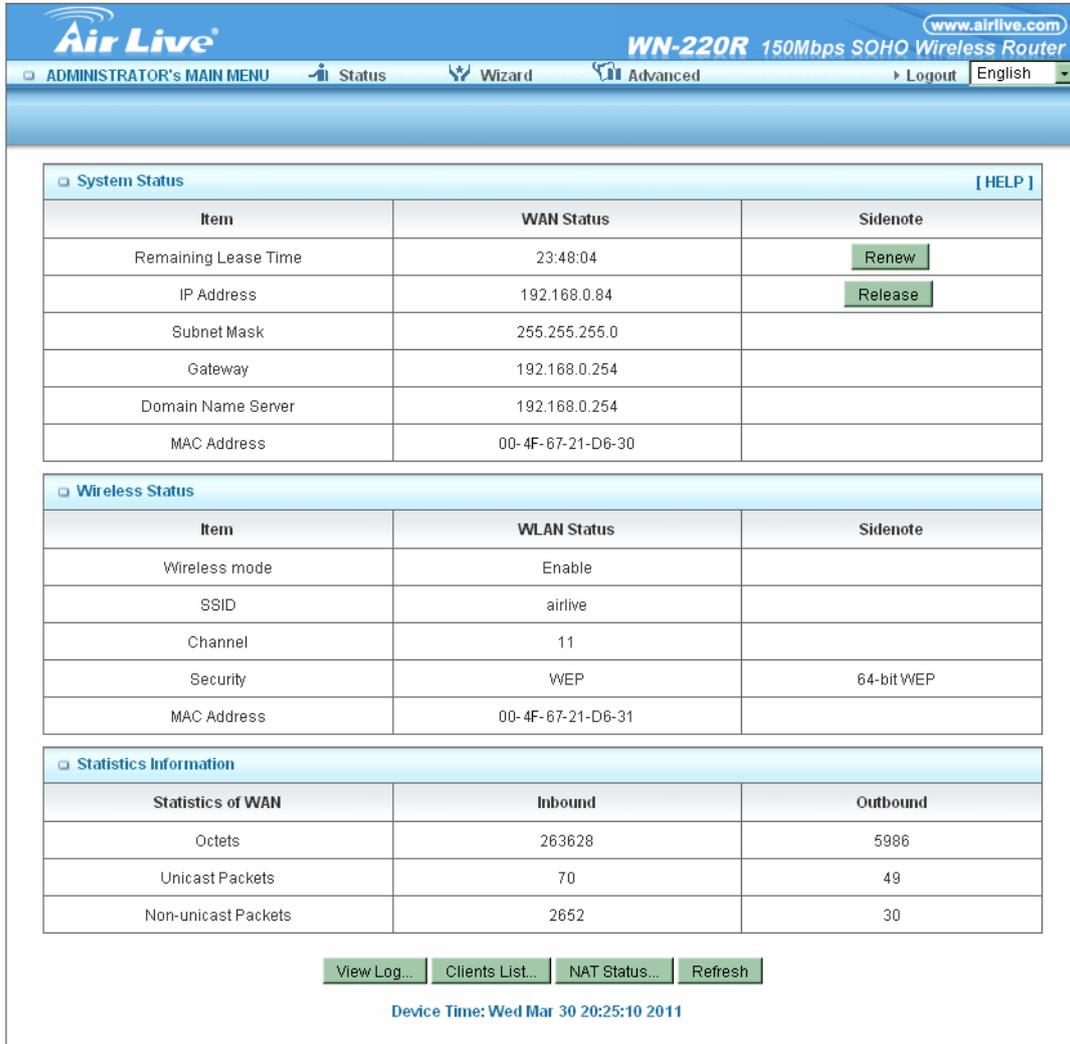
[Wireless Setting]	
Wireless	Enable
SSID	airlive
Channel	11
Security	64-bit WEP Enabled

Step 7:
Click Finish to complete it.



Connection information is	
WAN Type	Dynamic IP Address
IP Address	192.168.0.84
Subnet Mask	255.255.255.0
Gateway	192.168.0.254
Domain Name Server	192.168.0.254

3.2 System Status



The screenshot shows the 'System Status' page of the Air Live WN-220R 150Mbps SOHO Wireless Router. The page includes a navigation bar with 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', and 'Advanced' options. The main content area is divided into three sections: System Status, Wireless Status, and Statistics Information.

System Status

Item	WAN Status	Sidenote
Remaining Lease Time	23:48:04	Renew
IP Address	192.168.0.84	Release
Subnet Mask	255.255.255.0	
Gateway	192.168.0.254	
Domain Name Server	192.168.0.254	
MAC Address	00-4F-67-21-D6-30	

Wireless Status

Item	WLAN Status	Sidenote
Wireless mode	Enable	
SSID	airlive	
Channel	11	
Security	WEP	64-bit WEP
MAC Address	00-4F-67-21-D6-31	

Statistics Information

Statistics of WAN	Inbound	Outbound
Octets	263628	5988
Unicast Packets	70	49
Non-unicast Packets	2652	30

At the bottom of the page, there are buttons for 'View Log...', 'Clients List...', 'NAT Status...', and 'Refresh'. The device time is displayed as 'Wed Mar 30 20:25:10 2011'.

This option provides the function for observing this product's working status.

WAN Port Status:

If the WAN port is assigned a dynamic IP, there may appear a "Renew" or "Release" button on the Sidenote column. You can click this button to renew or release IP manually.

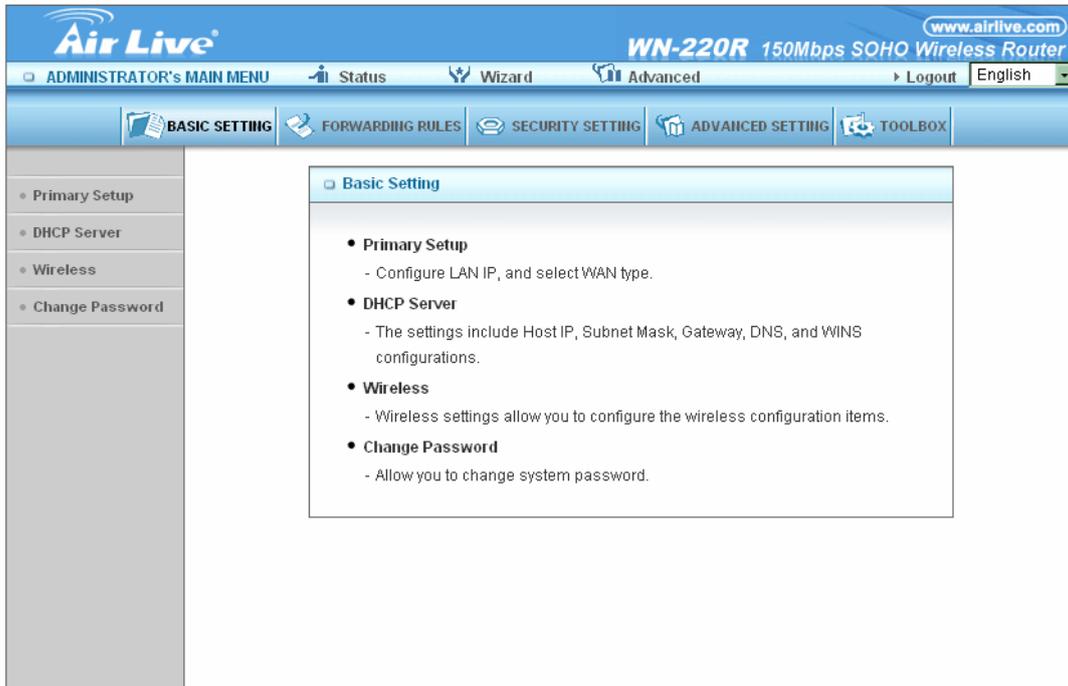
Statistics of Information:

Enables you to monitor inbound and outbound packets

3.3 Advanced

3.3.1 Basic Setting

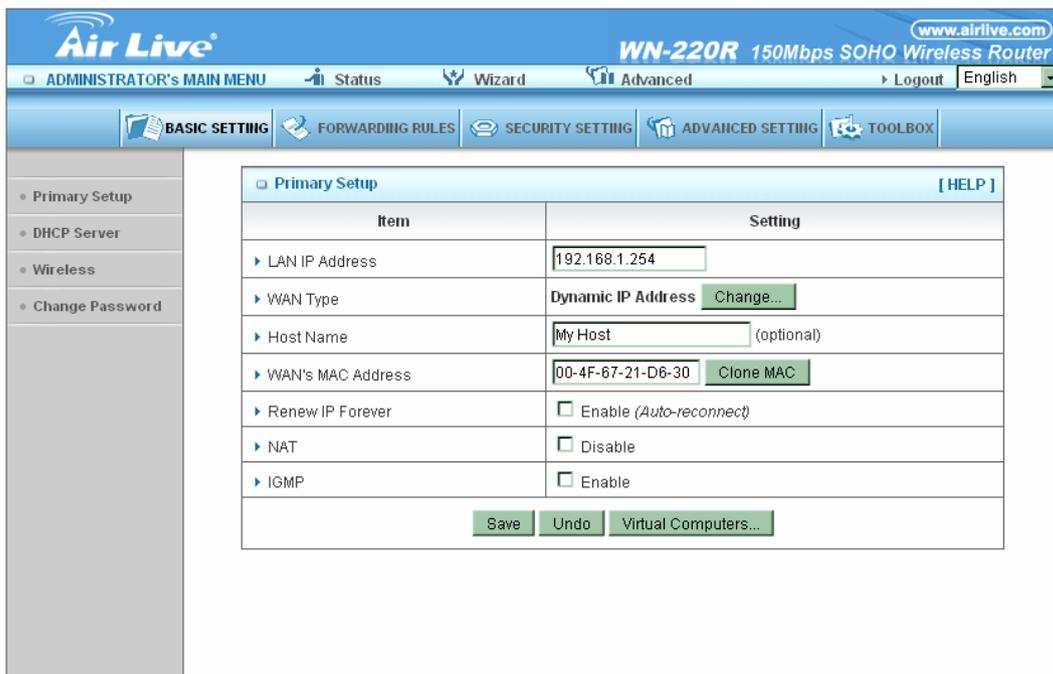
Please Select “Advanced Setup” to Setup



The screenshot shows the AirLive WN-220R web interface. The top navigation bar includes 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', 'Logout', and 'English'. Below this, there are tabs for 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. On the left, a sidebar lists 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area displays a 'Basic Setting' box with the following items:

- Primary Setup** - Configure LAN IP, and select WAN type.
- DHCP Server** - The settings include Host IP, Subnet Mask, Gateway, DNS, and WINS configurations.
- Wireless** - Wireless settings allow you to configure the wireless configuration items.
- Change Password** - Allow you to change system password.

3.3.1.1 Primary Setup – WAN Type, Virtual Computers

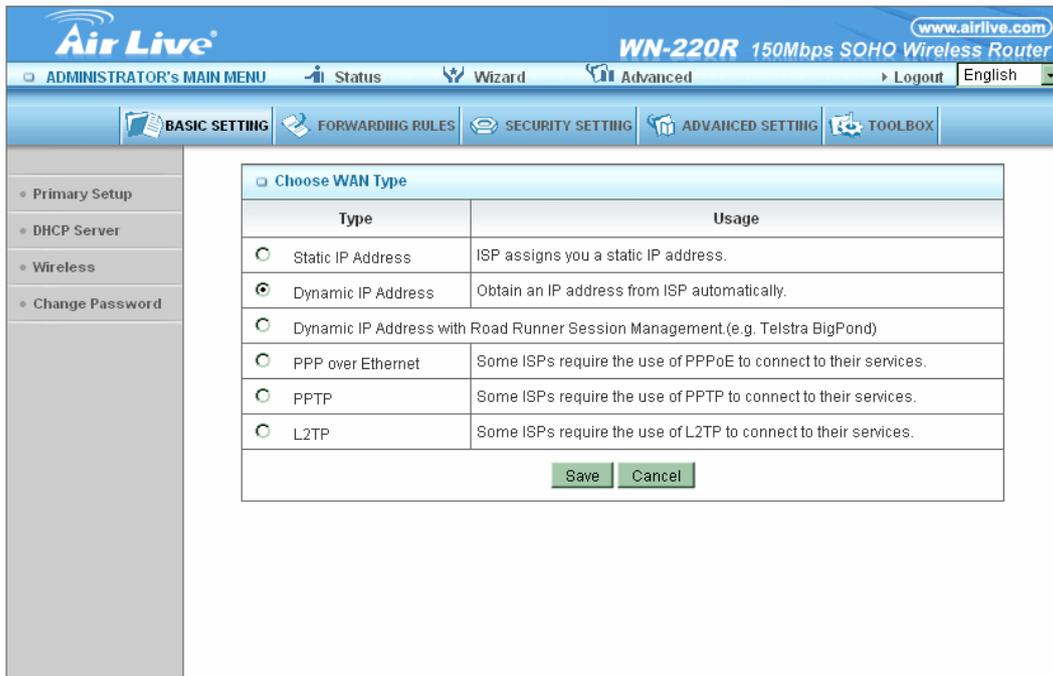


The screenshot shows the 'Primary Setup' configuration page in the AirLive WN-220R web interface. The page includes a sidebar with 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is a table with the following settings:

Item	Setting
▶ LAN IP Address	192.168.1.254
▶ WAN Type	Dynamic IP Address Change...
▶ Host Name	My Host (optional)
▶ WAN's MAC Address	00-4F-67-21-D6-30 Clone MAC
▶ Renew IP Forever	<input type="checkbox"/> Enable (Auto-reconnect)
▶ NAT	<input type="checkbox"/> Disable
▶ IGMP	<input type="checkbox"/> Enable

At the bottom of the table, there are buttons for 'Save', 'Undo', and 'Virtual Computers...'.

Press “Change”



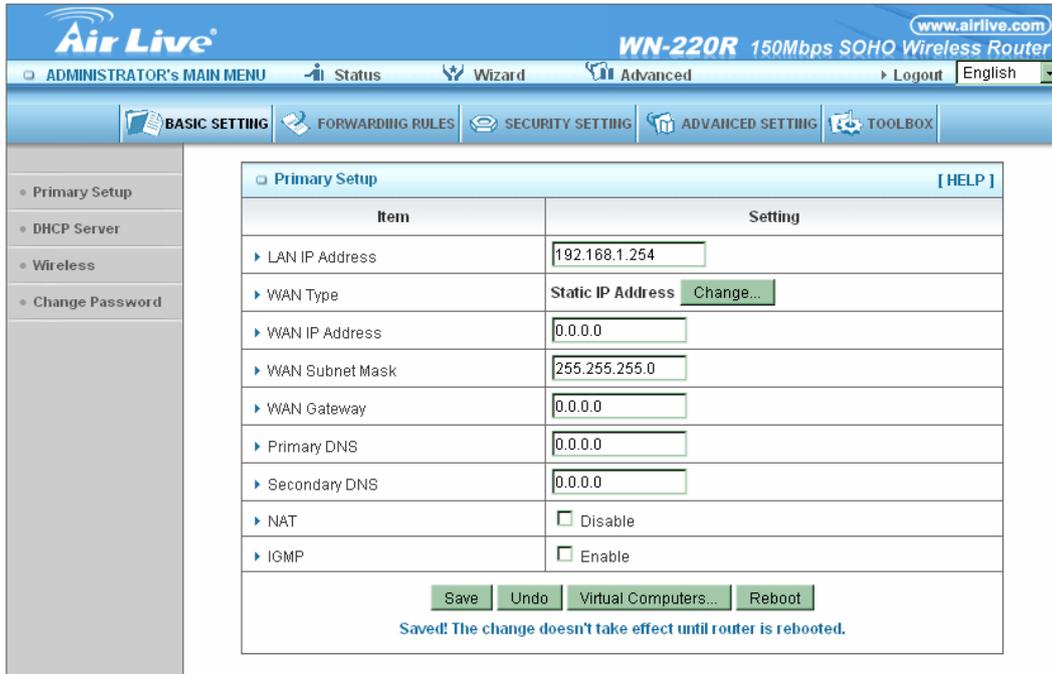
This option is primary to enable this product to work properly. The setting items and the web appearance depend on the WAN type. Choose correct WAN type before you start.

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



- B. **WAN Type:** WAN connection type of your ISP. You can click **Change** button to choose a correct one from the following four options:

- **Static IP Address: ISP assigns you a static IP address.**



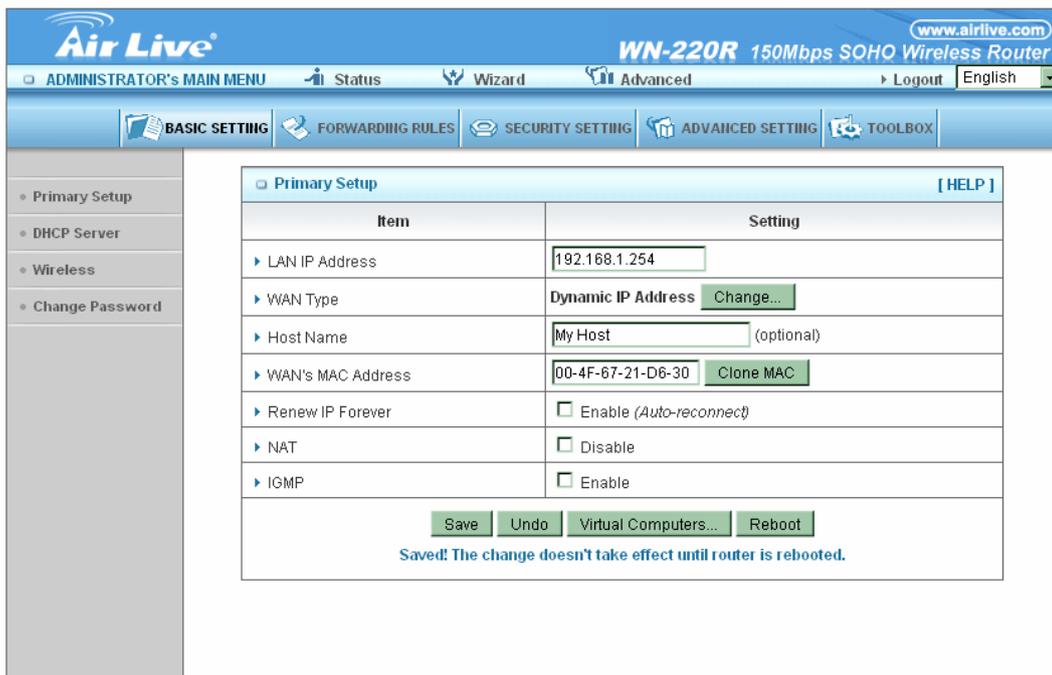
The screenshot shows the Air Live router configuration interface for a WN-220R 150Mbps SOHO Wireless Router. The 'Primary Setup' tab is selected, and the 'WAN Type' is set to 'Static IP Address'. The configuration table is as follows:

Item	Setting
LAN IP Address	192.168.1.254
WAN Type	Static IP Address Change...
WAN IP Address	0.0.0.0
WAN Subnet Mask	255.255.255.0
WAN Gateway	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
NAT	<input type="checkbox"/> Disable
IGMP	<input type="checkbox"/> Enable

Buttons at the bottom: Save, Undo, Virtual Computers..., Reboot. A message states: "Saved! The change doesn't take effect until router is rebooted."

WAN IP Address, Subnet Mask, Gateway, Primary and Secondary DNS: enter the proper setting provided by your ISP.

- **Dynamic IP Address: Obtain an IP address from ISP automatically.**



The screenshot shows the Air Live router configuration interface for a WN-220R 150Mbps SOHO Wireless Router. The 'Primary Setup' tab is selected, and the 'WAN Type' is set to 'Dynamic IP Address'. The configuration table is as follows:

Item	Setting
LAN IP Address	192.168.1.254
WAN Type	Dynamic IP Address Change...
Host Name	My Host (optional)
WAN's MAC Address	00-4F-67-21-D6-30 Clone MAC
Renew IP Forever	<input type="checkbox"/> Enable (Auto-reconnect)
NAT	<input type="checkbox"/> Disable
IGMP	<input type="checkbox"/> Enable

Buttons at the bottom: Save, Undo, Virtual Computers..., Reboot. A message states: "Saved! The change doesn't take effect until router is rebooted."

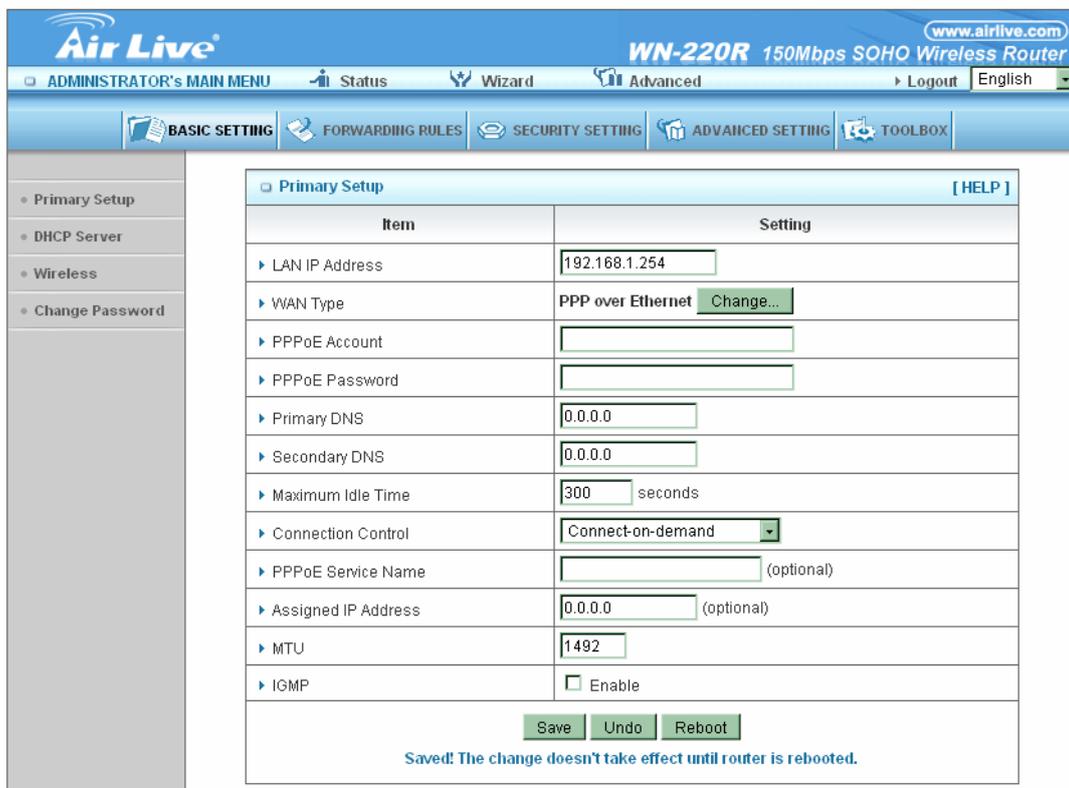
Host Name:

Optional. Required by some ISPs, for example, @Home.

Renew IP Forever:

This feature enables this product to renew your IP address automatically when the lease time is expiring-- even when the system is idle.

- **PPP over Ethernet: Some ISPs require the use of PPPoE to connect to their services.**



The screenshot shows the configuration interface for the Air Live WN-220R 150Mbps SOHO Wireless Router. The 'Primary Setup' section is active, displaying various configuration options for PPPoE. The 'WAN Type' is set to 'PPP over Ethernet'. Other settings include LAN IP Address (192.168.1.254), Primary DNS (0.0.0.0), Secondary DNS (0.0.0.0), Maximum Idle Time (300 seconds), and Connection Control (Connect-on-demand). There are 'Save', 'Undo', and 'Reboot' buttons at the bottom. A message states: 'Saved! The change doesn't take effect until router is rebooted.'

Item	Setting
LAN IP Address	192.168.1.254
WAN Type	PPP over Ethernet Change...
PPPoE Account	<input type="text"/>
PPPoE Password	<input type="text"/>
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Maximum Idle Time	300 seconds
Connection Control	Connect-on-demand
PPPoE Service Name	<input type="text"/> (optional)
Assigned IP Address	0.0.0.0 (optional)
MTU	1492
IGMP	<input type="checkbox"/> Enable

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 empty.

PPPoE Service Name:

Optional. Input the service name if your ISP requires it. Otherwise, leave it blank.

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.

Maximum Transmission Unit (MTU):

Most ISP offers MTU value to users. The most common MTU value is 1492.



Connection Control:

There are 3 modes to select:

Connect-on-demand:

The device will link up with ISP when the clients send outgoing packets.

Auto-Reconnect (Always-on):

The device will link with ISP until the connection is established.

Manually:

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

- **PPTP:** Some ISPs require the use of PPTP to connect to their services.

The screenshot shows the configuration page for the Air Live WN-220R 150Mbps SOHO Wireless Router. The page is titled "Primary Setup" and includes a sidebar with navigation options: Primary Setup, DHCP Server, Wireless, and Change Password. The main content area is a table with the following settings:

Item	Setting
LAN IP Address	192.168.1.254
WAN Type	PPTP Change...
IP Mode	Static IP Address
My IP Address	0.0.0.0
My Subnet Mask	255.255.255.0
Gateway IP	0.0.0.0
Server IP Address/Name	
PPTP Account	
PPTP Password	
Connection ID	(optional)
Maximum Idle Time	300 seconds
Connection Control	Connect-on-demand
MTU	1460
IGMP	<input type="checkbox"/> Enable

At the bottom of the form, there are buttons for "Save", "Undo", and "Reboot". A message below the buttons states: "Saved! The change doesn't take effect until router is rebooted."

First, please check your ISP assigned and Select Static IP Address or Dynamic IP Address.

My IP Address and My Subnet Mask:

The private IP address and subnet mask your ISP assigned to you.

Server IP Address:

The IP address of the PPTP server.

**PPTP Account and Password:**

The account and password your ISP assigned to you. If you don't want to change the password, keep it empty.

Connection ID:

Optional. Input the connection ID if your ISP requires it.

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 product will connect to ISP automatically, after system is restarted or connection is dropped.

Connection Control:

There are 3 modes to select:

➤ Connect-on-demand:

The device will link up with ISP when the clients send outgoing packets.

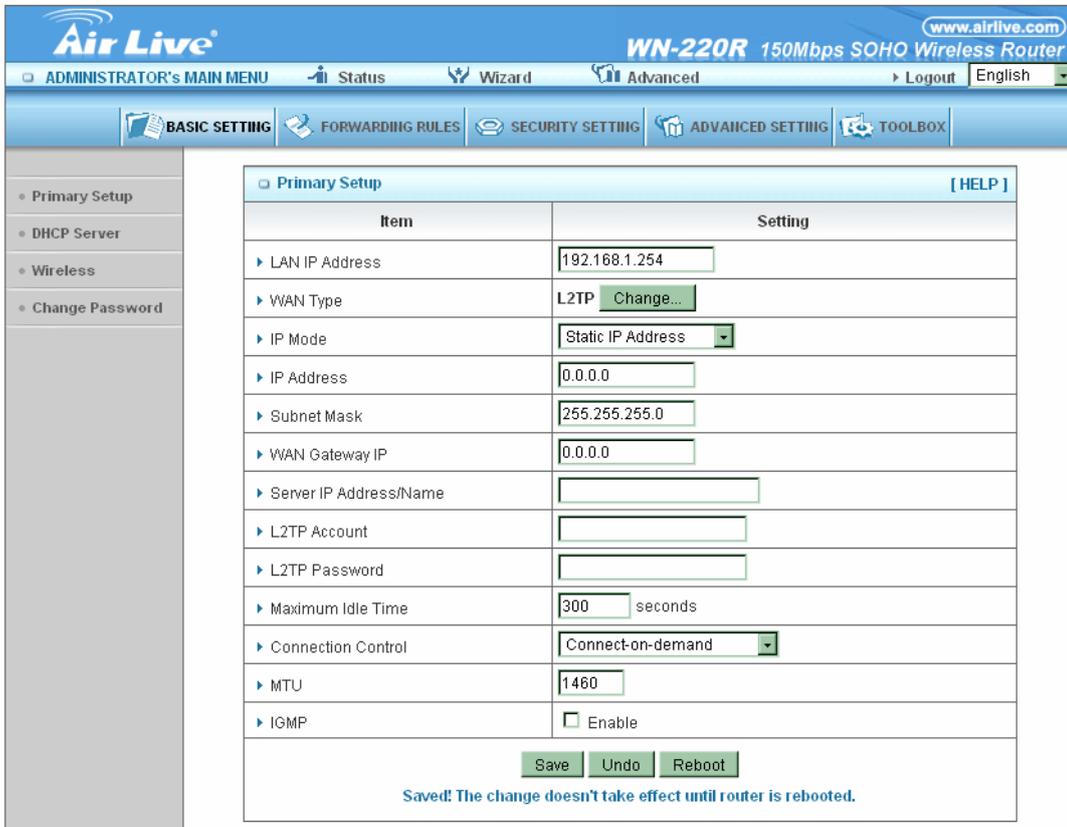
➤ Auto-Reconnect(Always-on):

The device will link with ISP until the connection is established.

➤ Manually:

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

- L2TP: Some ISPs require the use of L2TP to connect to their services



The screenshot shows the configuration interface for the Air Live WN-220R 150Mbps SOHO Wireless Router. The 'Primary Setup' section is active, displaying various network settings. The WAN Type is set to L2TP. The IP Mode is set to Static IP Address. The LAN IP Address is 192.168.1.254. The WAN Gateway IP is 0.0.0.0. The L2TP Account and Password fields are empty. The Maximum Idle Time is set to 300 seconds. The Connection Control is set to Connect-on-demand. The MTU is 1460. The IGMP checkbox is unchecked. At the bottom, there are buttons for Save, Undo, and Reboot, and a message: 'Saved! The change doesn't take effect until router is rebooted.'

Item	Setting
LAN IP Address	192.168.1.254
WAN Type	L2TP Change...
IP Mode	Static IP Address
IP Address	0.0.0.0
Subnet Mask	255.255.255.0
WAN Gateway IP	0.0.0.0
Server IP Address/Name	
L2TP Account	
L2TP Password	
Maximum Idle Time	300 seconds
Connection Control	Connect-on-demand
MTU	1460
IGMP	<input type="checkbox"/> Enable

First, please check your ISP assigned and Select Static IP Address or Dynamic IP Address.

For example: Use Static

My IP Address and My Subnet Mask:

The private IP address and subnet mask your ISP assigned to you.

Server IP Address:

The IP address of the PPTP server.

PPTP Account and Password:

The account and password your ISP assigned to you. If you don't want to change the password, keep it empty.

Connection ID:

Optional. Input the connection ID if your ISP requires it.

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 product will connect to ISP automatically, after system is restarted or connection is dropped.



Connection Control:

There are 3 modes to select:

➤ Connect-on-demand:

The device will link up with ISP when the clients send outgoing packets.

➤ Auto-Reconnect(Always-on):

The device will link with ISP until the connection is established.

➤ Manually :

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

● Virtual Computers(Only for Static and dynamic IP address Wan type)

The screenshot shows the 'Virtual Computers' configuration page in the Air Live WN-220R 150Mbps SOHO Wireless Router web interface. The page has a blue header with the Air Live logo and navigation tabs for 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', 'Logoff', and 'English'. Below the header are tabs for 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a tree view with 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'Virtual Computers' and includes a 'DHCP clients' dropdown menu set to '--- Select one ---', a 'Copy to ID' dropdown, and a table with 5 rows. Each row has columns for 'ID', 'Global IP', 'Local IP', and 'Enable'. The 'Local IP' column shows '192.168.1.' followed by an input field. Below the table are 'Save' and 'Undo' buttons. A '[HELP]' link is in the top right of the table area. A blue box on the left side of the table contains the text: 'Allow you to setup the one-to-one mapping of multiple global IP address and local IP address.'

ID	Global IP	Local IP	Enable
1	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>

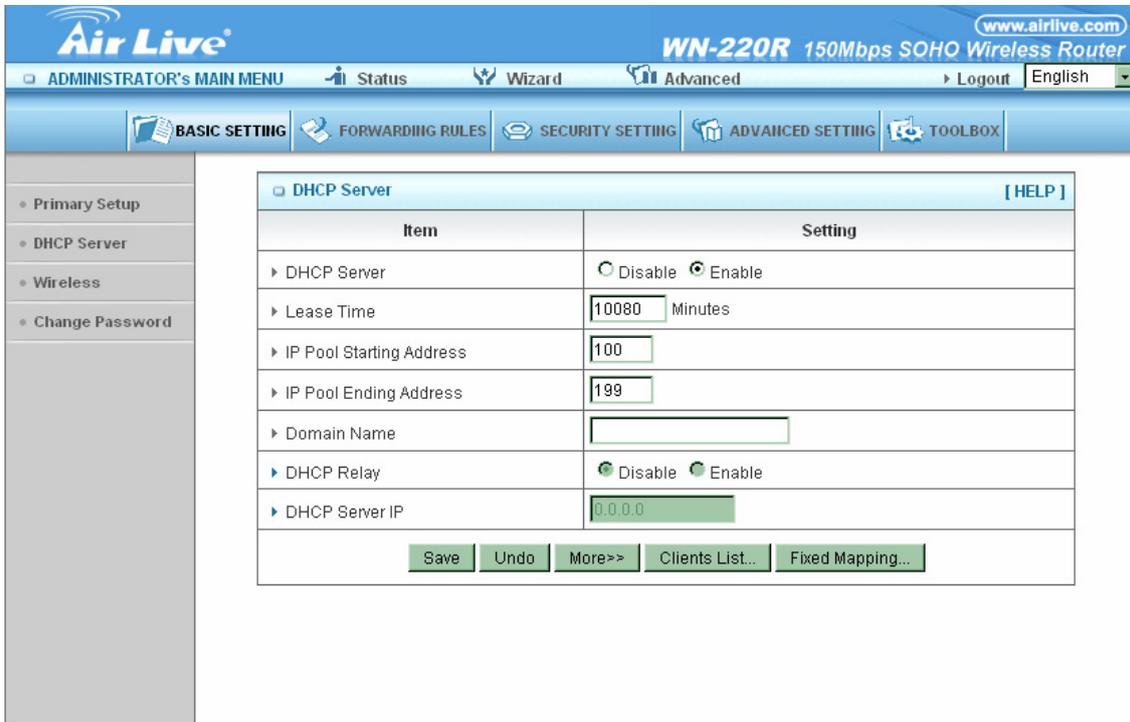
Virtual Computer enables you to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple global IP address and local IP address.

➤ Global IP: Enter the global IP address assigned by your ISP.

➤ Local IP: Enter the local IP address of your LAN PC corresponding to the global IP address.

➤ Enable: Check this item to enable the Virtual Computer feature.

3.3.1.2 DHCP Server



Press “More>>”

- **DHCP Server:**

Choose “Disable” or “Enable.”

- **Lease time:**

This is the length of time that the client may use the IP address it has been assigned by DHCP server.

- **IP pool starting Address/ IP pool starting 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 and ending address of the IP address pool.

- **Domain Name:**

Optional, this information will be passed to the client.

- **Primary DNS/Secondary DNS:**

This feature allows you to assign DNS Servers

- **Primary WINS/Secondary WINS:**

This feature allows you to assign WINS Servers

- **Gateway:**

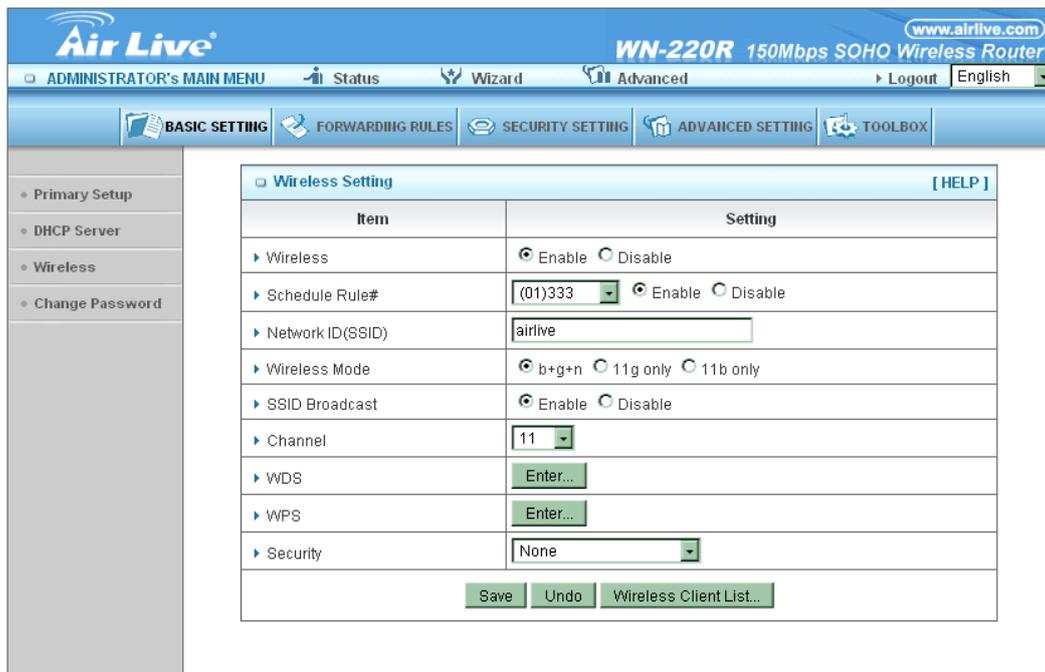
The Gateway Address would be the IP address of an alternate Gateway. This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.

3.3.1.3 DHCP Client List:



IP Address	Host Name	MAC Address	Select
192.168.1.191	ludy-x61	00-1D-72-96-57-E9	<input type="checkbox"/>

3.3.1.4 Wireless Setting



Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Schedule Rule#	(01)333 <input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network ID(SSID)	airlive
Wireless Mode	<input checked="" type="radio"/> b+g+n <input type="radio"/> 11g only <input type="radio"/> 11b only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	11
WDS	Enter...
WPS	Enter...
Security	None

Wireless settings allow you to set the wireless configuration items.

- **Wireless :**

The user can enable or disable wireless function.



- **Network ID (SSID):**

Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. (The factory setting is “airlive”).

- **SSID Broadcast:**

The router will Broadcast beacons that have some information, including SSID so that the wireless clients can know how many AP devices by scanning function in the network. Therefore, this function is disabled; the wireless clients can not find the device from beacons.

- **Channel:**

The radio channel number. The permissible channels depend on the Regulatory Domain.

- **WPS (WiFi Protection Setup)**

WPS is WiFi Protection Setup which is similar to WCN-NET and offers safe and easy way in Wireless Connection.

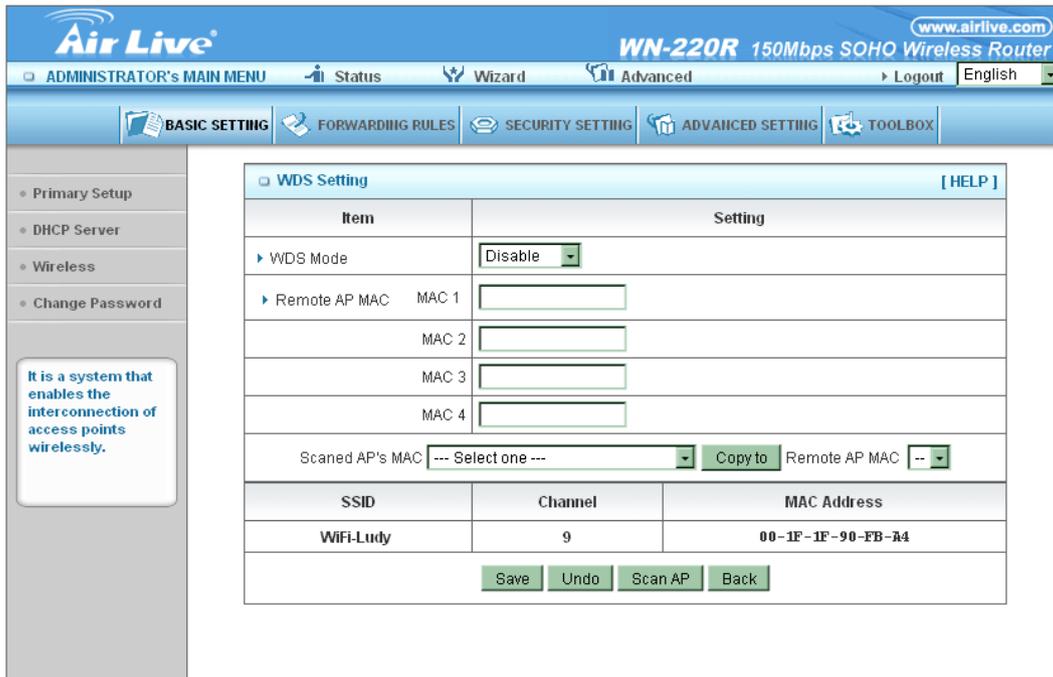
The screenshot shows the web interface for the Air Live WN-220R 150Mbps SOHO Wireless Router. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', 'Logout', and 'English'. The main menu includes 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar lists 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'Wi-Fi Protected Setup' and contains a table with the following settings:

Item	Setting
▶ WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ Setup	<input type="radio"/> Current AP PIN <input type="radio"/> Configure Wireless Station
▶ WPS state	Idle
▶ WPS status	Configured <input type="button" value="Release"/>

At the bottom of the table, there are three buttons: .

● **WDS(Wireless Distribution System)**

WDS operation as defined by the IEEE802.11 standard has been made available. Using WDS it is possible to wirelessly connect Access Points, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.



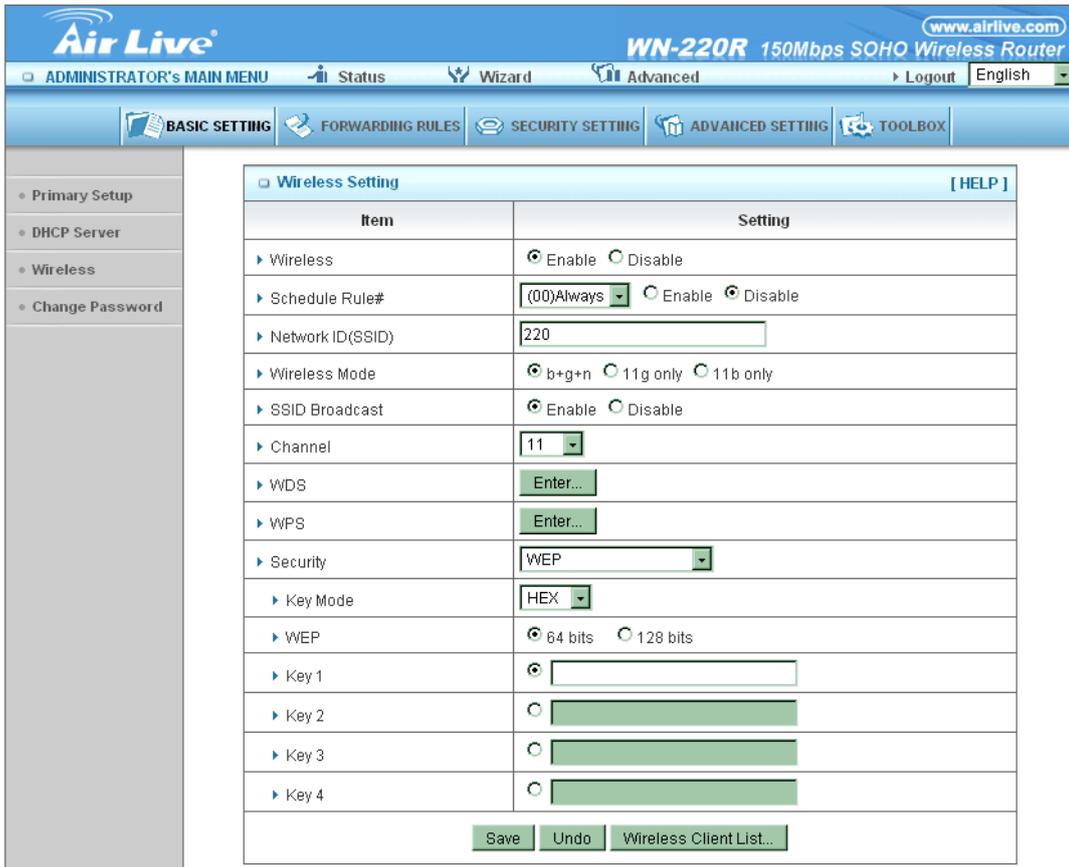
● **Security:**

Select the data privacy algorithm you want. Enabling the security can protect your data while it is transferred from one station to another.

There are several security types to use:

➤ WEP :

When you enable the 128 or 64 bit WEP key security, please select one WEP key to be used and input 26 or 10 hexadecimal (0, 1, 2...8, 9, A, B...F) digits.



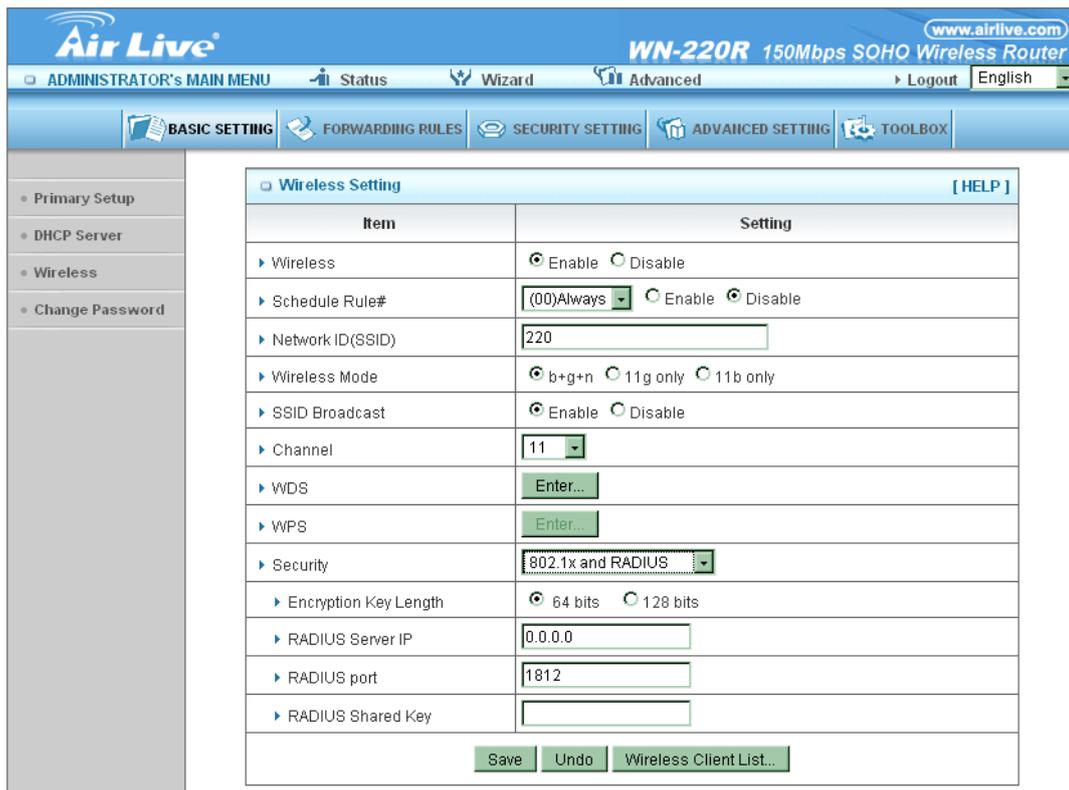
The screenshot shows the configuration page for the Air Live WN-220R 150Mbps SOHO Wireless Router. The page is titled "Wireless Setting" and includes a sidebar with navigation options: Primary Setup, DHCP Server, Wireless, and Change Password. The main content area is a table with the following items and settings:

Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Schedule Rule#	(00)Always <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network ID(SSID)	220
Wireless Mode	<input checked="" type="radio"/> b+g+n <input type="radio"/> 11g only <input type="radio"/> 11b only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	11
WDS	Enter...
WPS	Enter...
Security	WEP
Key Mode	HEX
WEP	<input checked="" type="radio"/> 64 bits <input type="radio"/> 128 bits
Key 1	<input checked="" type="radio"/> <input type="text"/>
Key 2	<input type="radio"/> <input type="text"/>
Key 3	<input type="radio"/> <input type="text"/>
Key 4	<input type="radio"/> <input type="text"/>

At the bottom of the table, there are buttons for "Save", "Undo", and "Wireless Client List..."

➤ 802.1X

Check Box was used to switch the function of the 802.1X. When the 802.1X function is enabled, the Wireless user must authenticate to this router first to use the Network service.



Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Schedule Rule#	(00)Always <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network ID(SSID)	220
Wireless Mode	<input checked="" type="radio"/> b+g+n <input type="radio"/> 11g only <input type="radio"/> 11b only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	11
WDS	Enter...
WPS	Enter...
Security	802.1x and RADIUS
Encryption Key Length	<input checked="" type="radio"/> 64 bits <input type="radio"/> 128 bits
RADIUS Server IP	0.0.0.0
RADIUS port	1812
RADIUS Shared Key	

Save Undo Wireless Client List...

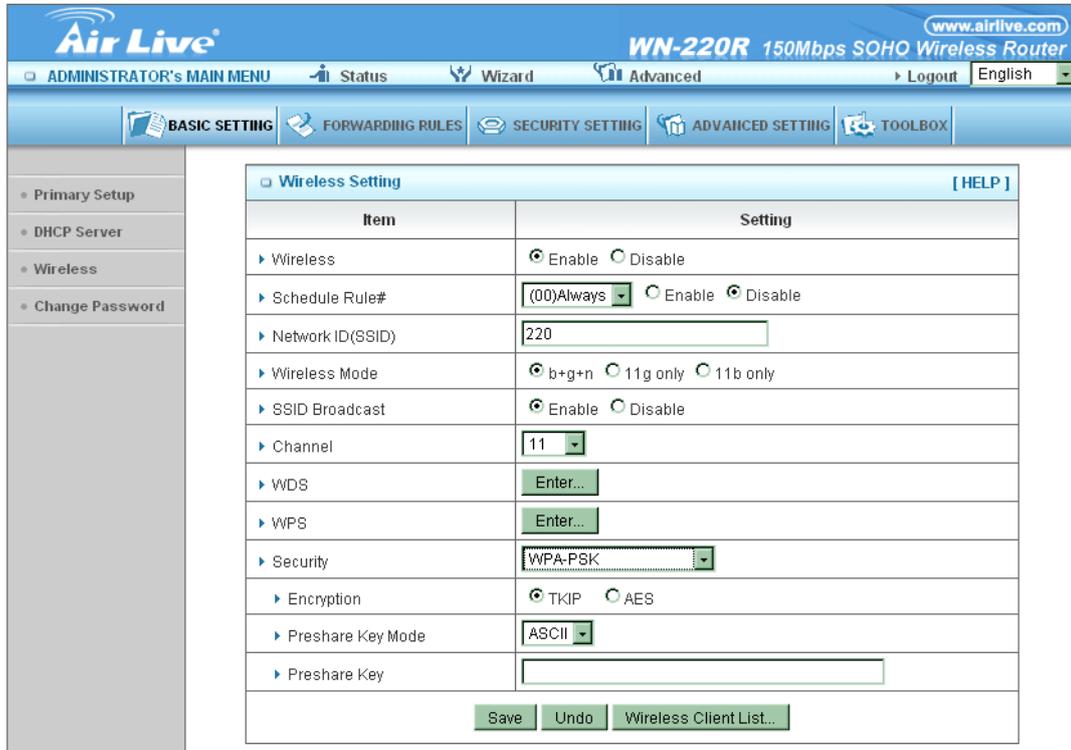
■ RADIUS Server

IP address or the 802.1X server's domain-name.

■ RADIUS Shared Key

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

➤ WPA-PSK



Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Schedule Rule#	(00)Always <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network ID(SSID)	220
Wireless Mode	<input checked="" type="radio"/> b+g+n <input type="radio"/> 11g only <input type="radio"/> 11b only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	11
WDS	Enter...
WPS	Enter...
Security	WPA-PSK
Encryption	<input checked="" type="radio"/> TKIP <input type="radio"/> AES
Preshare Key Mode	ASCII
Preshare Key	

Buttons: Save, Undo, Wireless Client List...

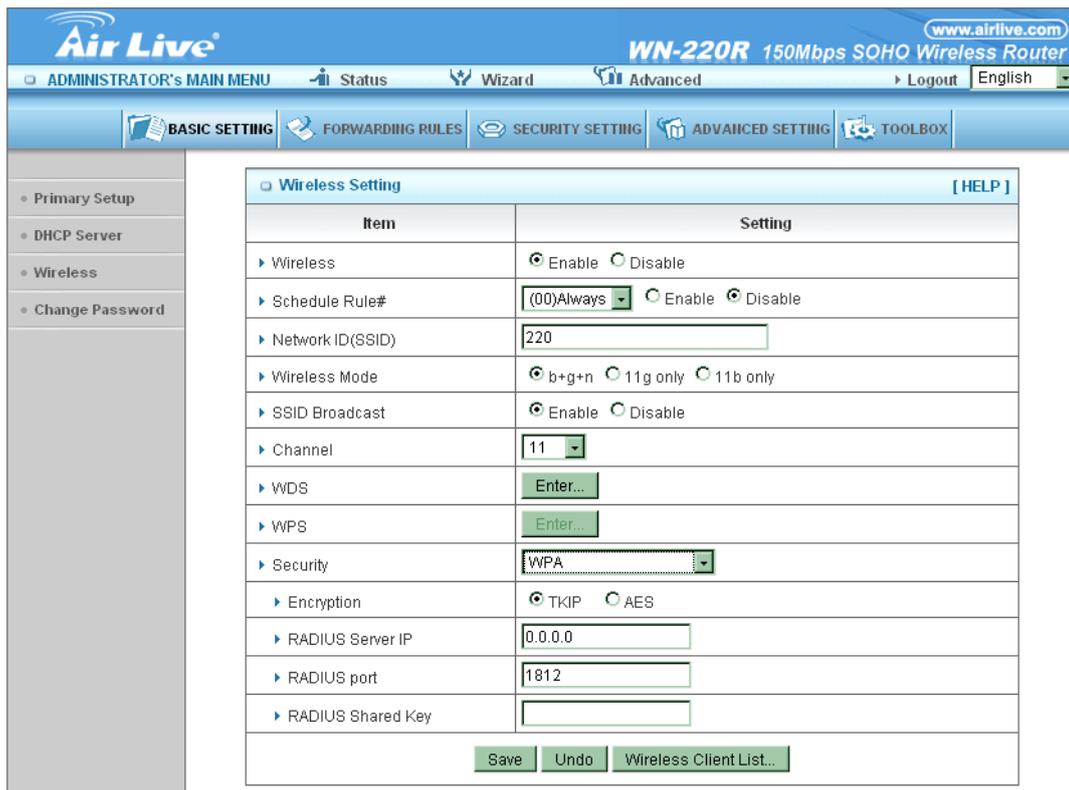
■ Select Encryption and Pre-share Key Mode

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



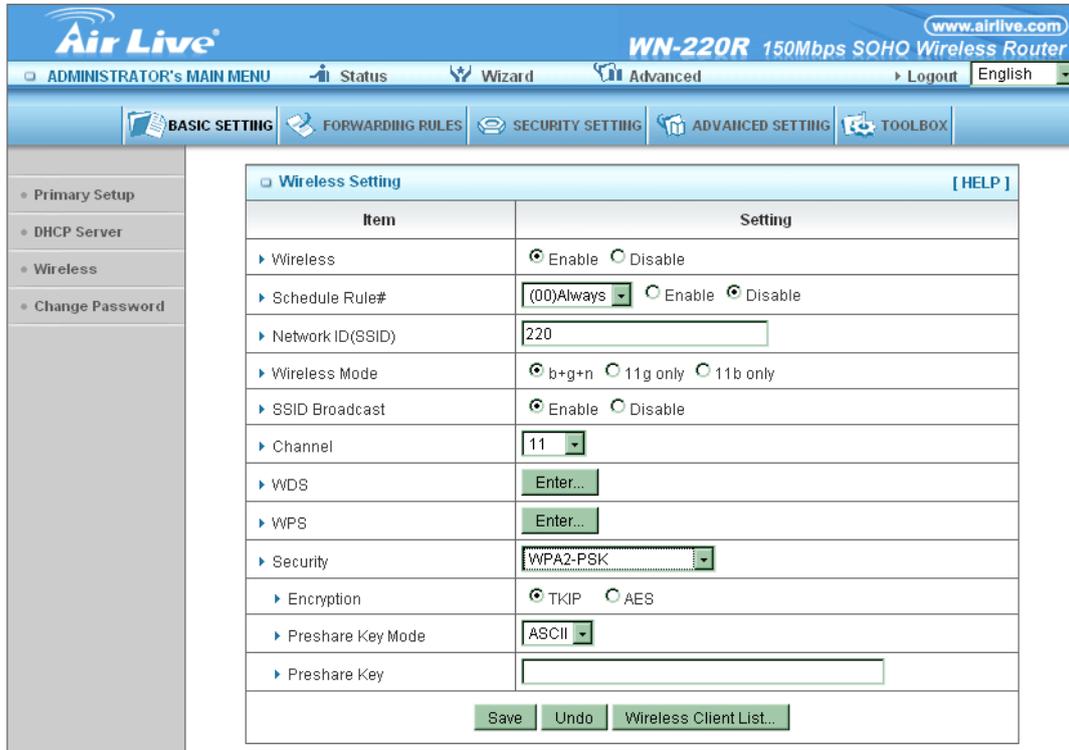
Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Schedule Rule#	(00)Always <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network ID(SSID)	220
Wireless Mode	<input checked="" type="radio"/> b+g+n <input type="radio"/> 11g only <input type="radio"/> 11b only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	11
WDS	Enter...
WPS	Enter...
Security	WPA
Encryption	<input checked="" type="radio"/> TKIP <input type="radio"/> AES
RADIUS Server IP	0.0.0.0
RADIUS port	1812
RADIUS Shared Key	

Save Undo Wireless Client List...

■ Select Encryption and RADIUS Shared Key

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(AES)



The screenshot shows the 'Wireless Setting' page in the AirLive WN-220R web interface. The page includes a navigation menu with options like 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', and 'Advanced'. The main content area is a table with 'Item' and 'Setting' columns. The 'Security' item is set to 'WPA2-PSK' and 'Encryption' is set to 'TKIP'. The 'Pre-share Key Mode' is set to 'ASCII'.

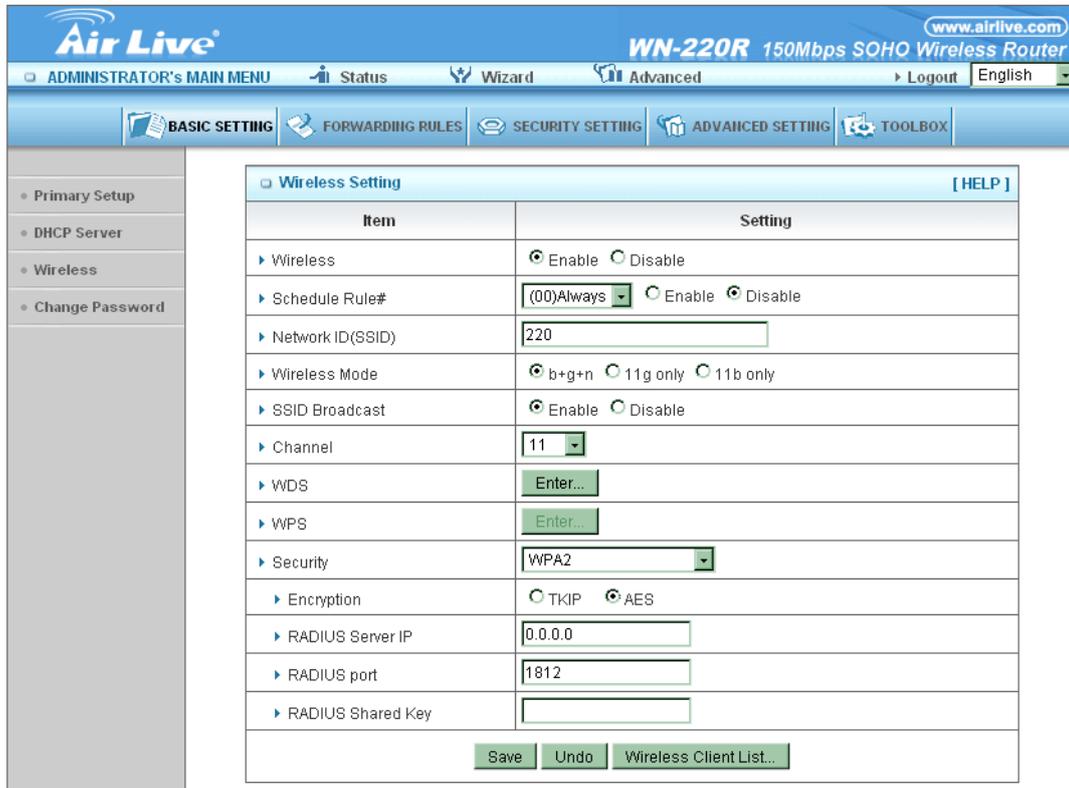
Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Schedule Rule#	(00)Always <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network ID(SSID)	220
Wireless Mode	<input checked="" type="radio"/> b+g+n <input type="radio"/> 11g only <input type="radio"/> 11b only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	11
WDS	Enter...
WPS	Enter...
Security	WPA2-PSK
Encryption	<input checked="" type="radio"/> TKIP <input type="radio"/> AES
Pre-share Key Mode	ASCII
Pre-share Key	

■ Select 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 ASCII, the length of Pre-share key is from 8 to 63.

■ Fill in the key, Ex 12345678

➤ WPA2(AES)



The screenshot shows the configuration page for the Air Live WN-220R 150Mbps SOHO Wireless Router. The 'Wireless Setting' section is active, and the 'Security' dropdown is set to 'WPA2'. The 'Encryption' radio buttons are set to 'AES'.

Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Schedule Rule#	(00)Always <input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network ID(SSID)	220
Wireless Mode	<input checked="" type="radio"/> b+g+n <input type="radio"/> 11g only <input type="radio"/> 11b only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	11
WDS	Enter...
WPS	Enter...
Security	WPA2
Encryption	<input type="radio"/> TKIP <input checked="" type="radio"/> AES
RADIUS Server IP	0.0.0.0
RADIUS port	1812
RADIUS Shared Key	

Buttons at the bottom: Save, Undo, Wireless Client List...

- 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.

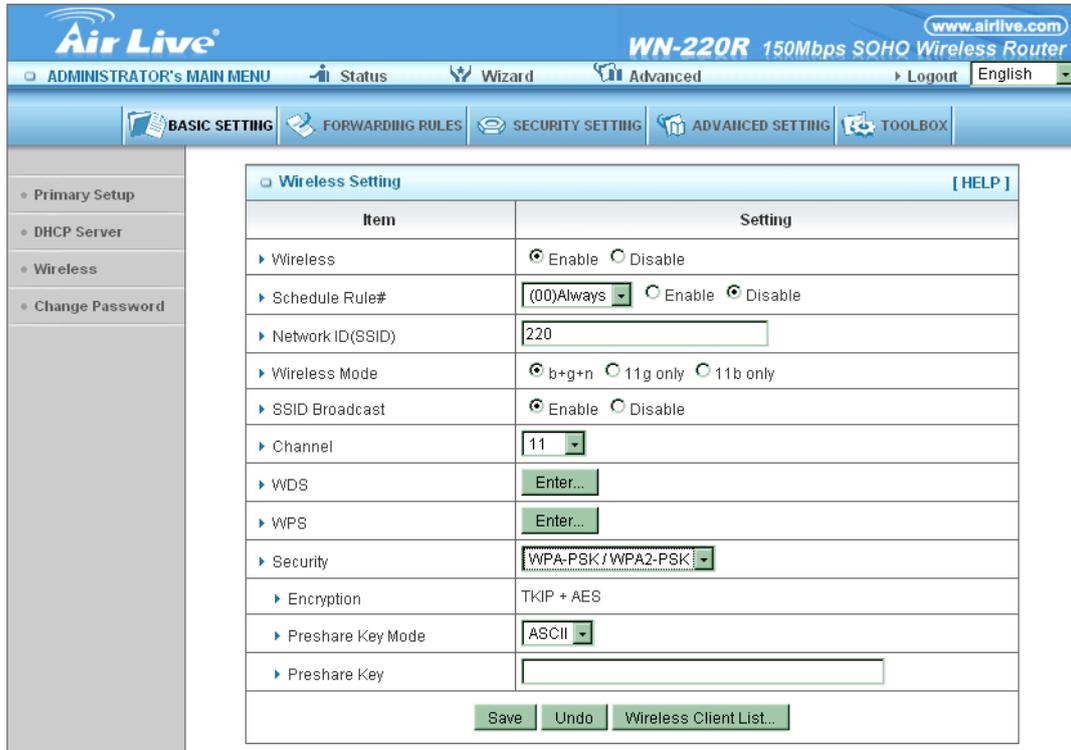
- Select RADIUS Shared Key

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

If ASCII, the length of Pre-share key is from 8 to 63.

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

➤ WPA-PSK /WPA2-PSK



The router will detect automatically which Security type the client uses to encrypt.

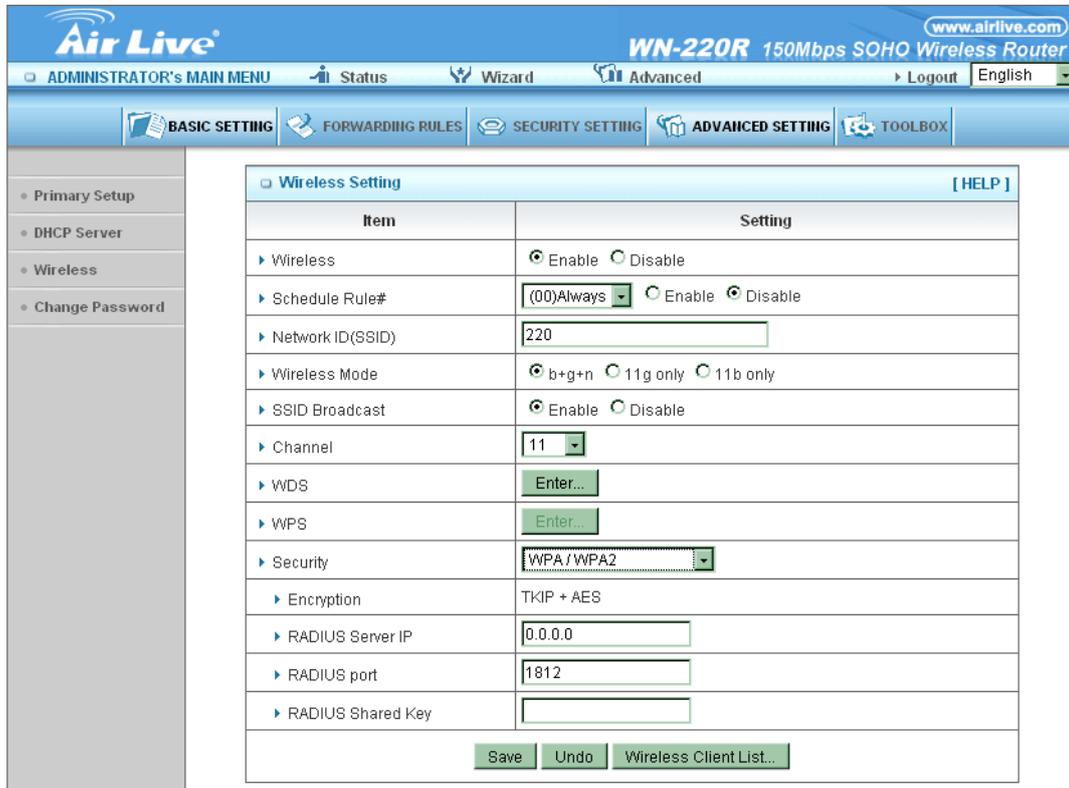
■ Select Pre-share Key Mode

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

If ASCII, the length of Pre-share key is from 8 to 63.

■ 2. Fill in the key, Ex 12345678

➤ WPA/WPA2



- 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

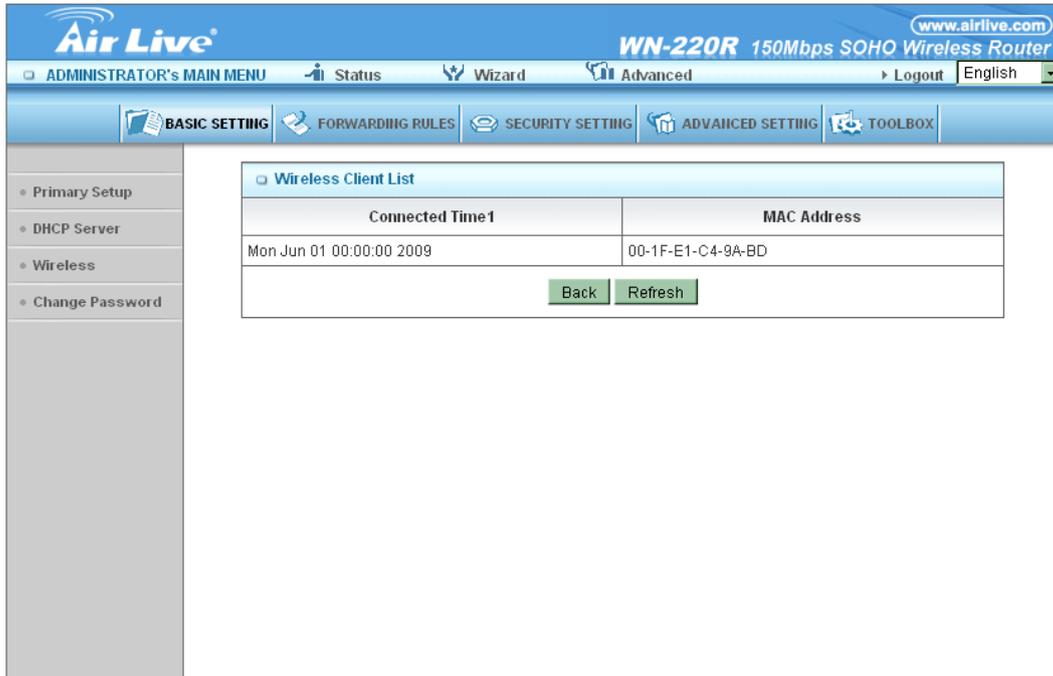
The router will detect automatically which Security type (Wpa-psk version 1 or 2) the client uses to encrypt.

- IP address or the 802.1X server's domain-name.
- Select RADIUS Shared Key

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

● **Wireless Client List**

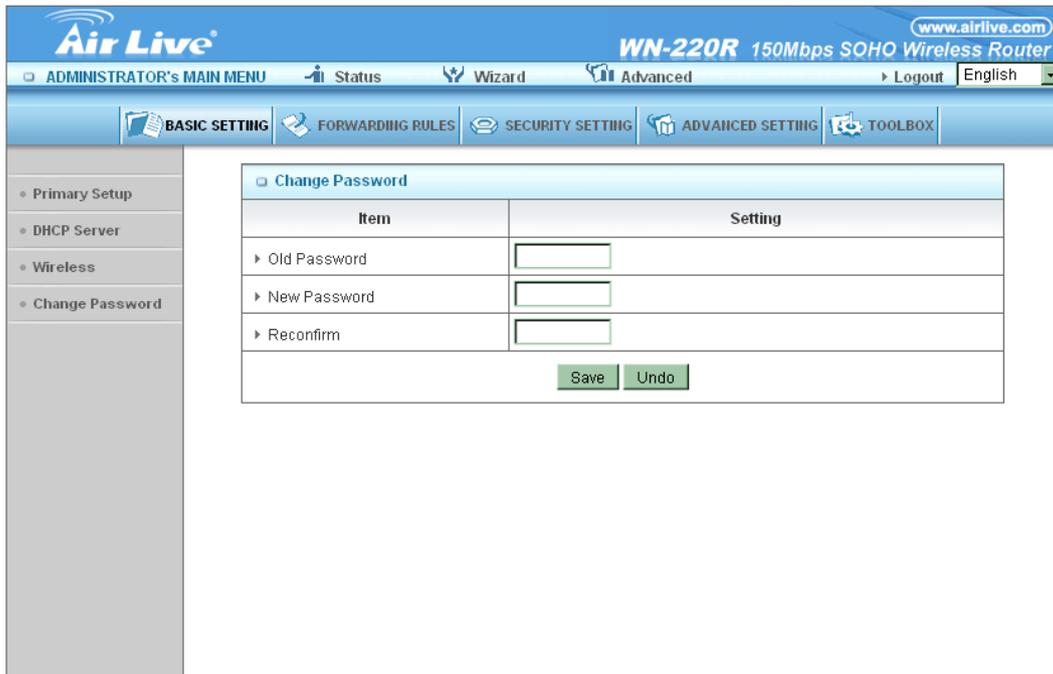


The screenshot shows the configuration interface for the Air Live WN-220R 150Mbps SOHO Wireless Router. The page title is "Wireless Client List". The interface includes a navigation menu on the left with options like "Primary Setup", "DHCP Server", "Wireless", and "Change Password". The main content area displays a table with the following data:

Connected Time1	MAC Address
Mon Jun 01 00:00:00 2009	00-1F-E1-C4-9A-BD

Below the table are "Back" and "Refresh" buttons.

3.3.1.5 Change Password



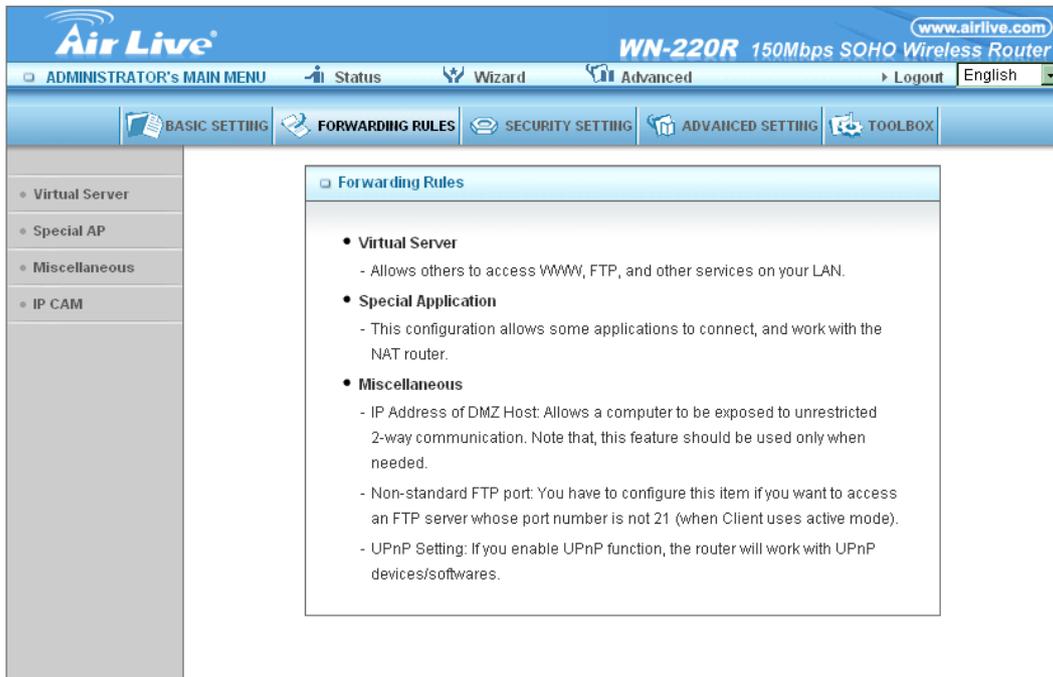
The screenshot shows the configuration interface for the Air Live WN-220R 150Mbps SOHO Wireless Router. The page title is "Change Password". The interface includes a navigation menu on the left with options like "Primary Setup", "DHCP Server", "Wireless", and "Change Password". The main content area displays a form with the following fields:

Item	Setting
▶ Old Password	<input type="text"/>
▶ New Password	<input type="text"/>
▶ Reconfirm	<input type="text"/>

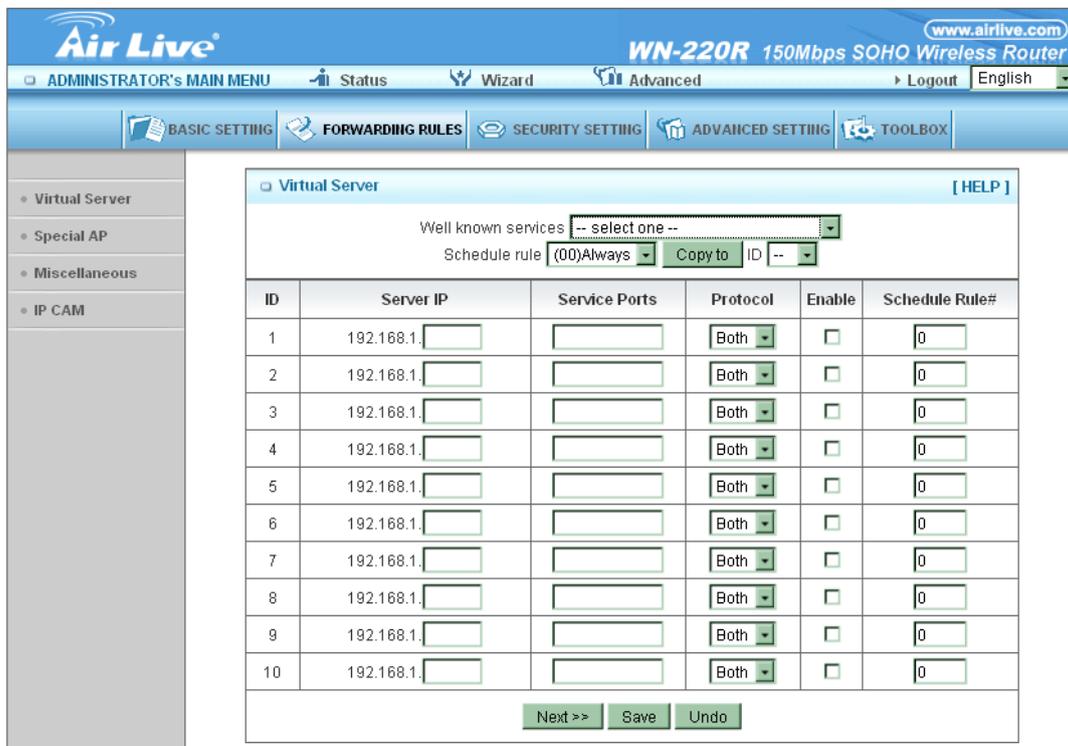
Below the form are "Save" and "Undo" buttons.

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

3.3.2 Forwarding Rules



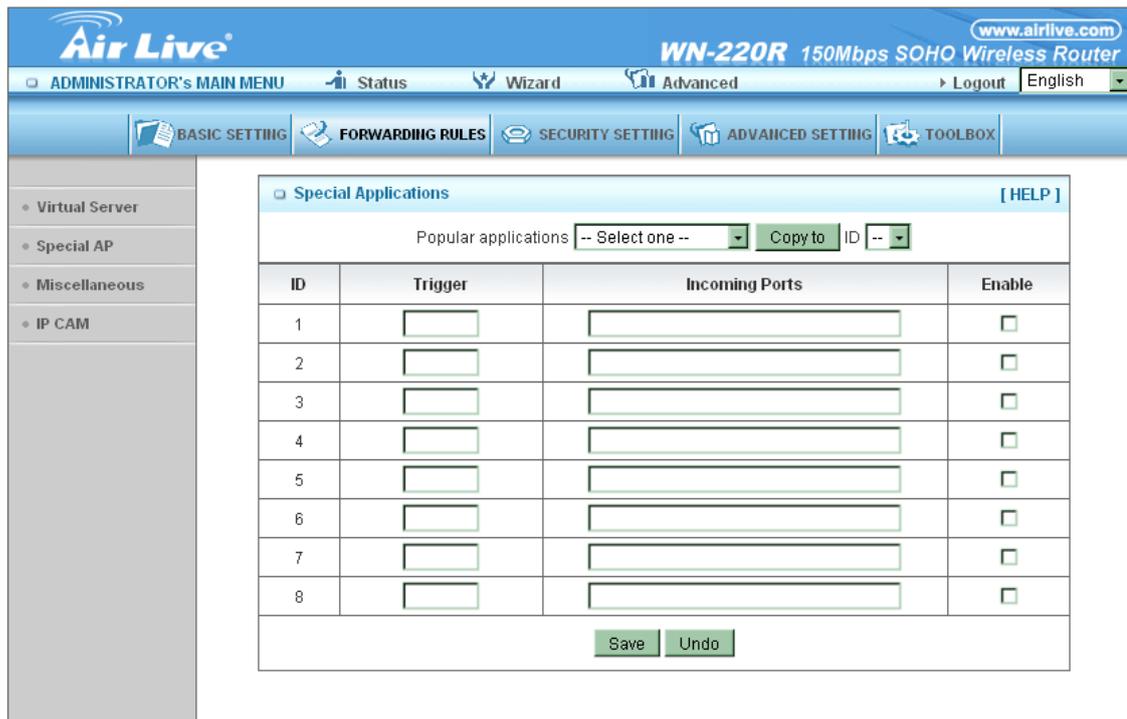
3.3.2.1 Virtual Server



This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

A virtual server is defined as a **Service Port**, and all requests to this port will be redirected to the computer specified by the **Server IP**. Virtual Server can work with **Scheduling Rules**, and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule**.

3.3.2.2 Special AP



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

- **Trigger:**

The outbound port number issued by the application..

- **Incoming Ports:**

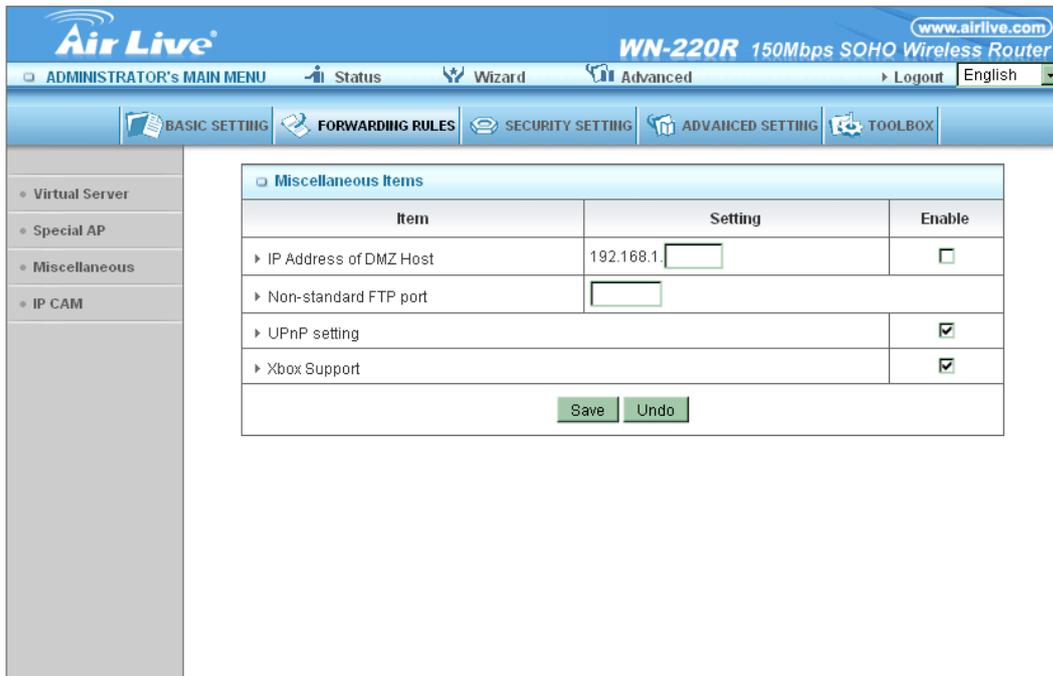
When the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

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

Note: At any given time, only one PC can use each Special Application tunnel.



3.3.2.3 Miscellaneous Items



- **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.

NOTE: This feature should be used only when needed.

- **Non-standard FTP port**

You have to configure this item if you want to access an FTP server whose port number is not 21. This setting will be lost after rebooting.

- **Xbox Support**

The Xbox is a video game console produced by Microsoft Corporation. Please enable this function when you play games.

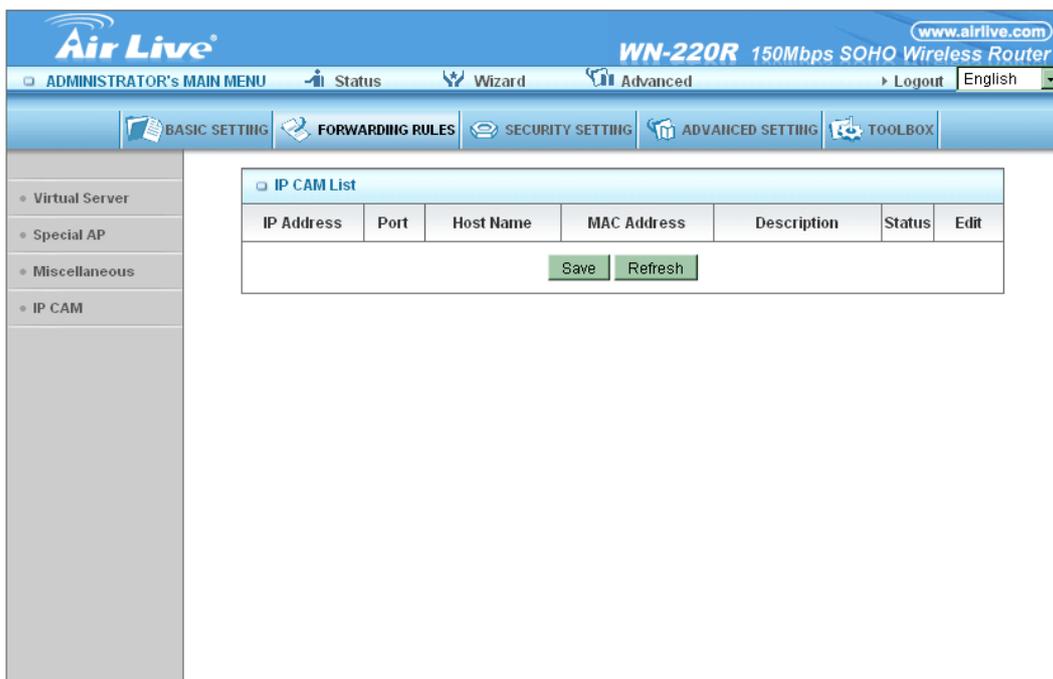
- **UpnP Setting**

The device also supports this function. If the OS supports this function enable it, like Windows Xp. When the user gets IP from Device and will see icon as below:



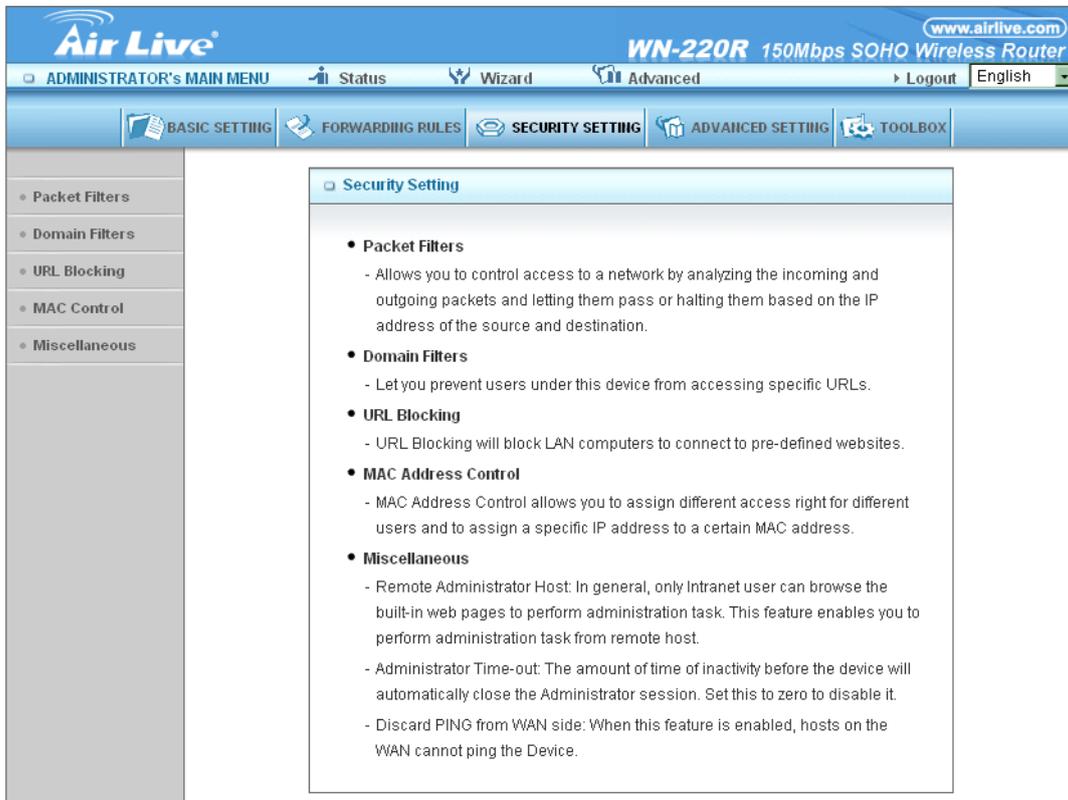


3.3.2.4 IPCamera PnP



This function will automatically search your AirLive IP Camera that connects to the same LAN with the router. With this function, you can get the information of your IP camera faster and easier.

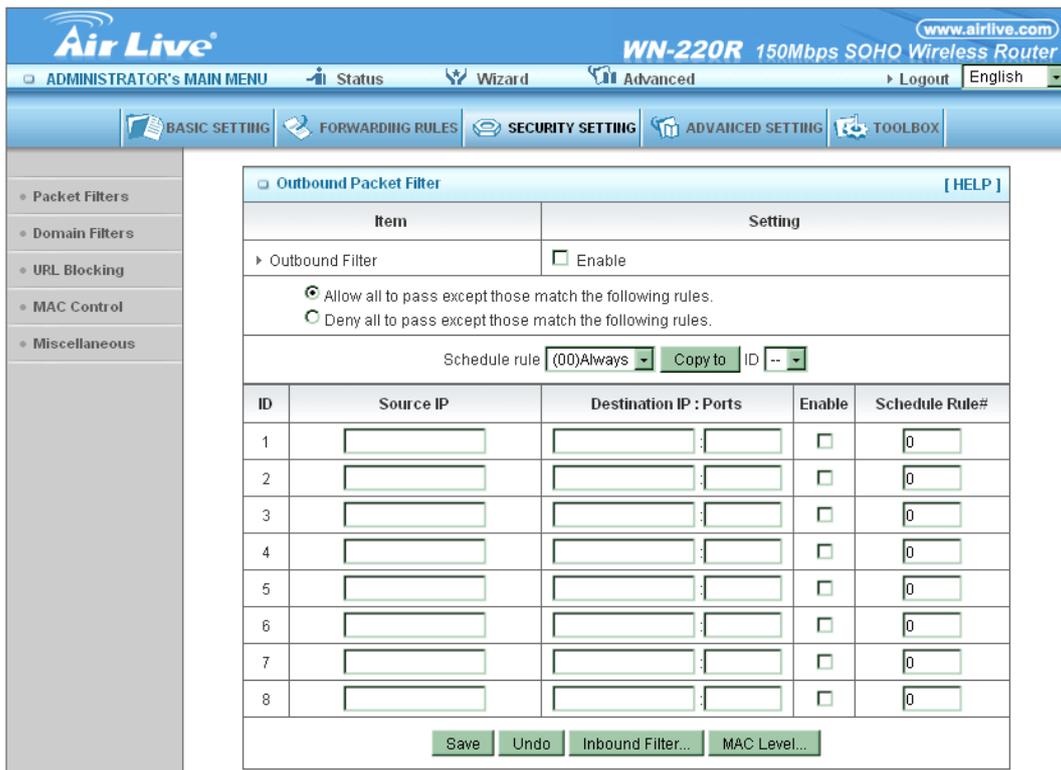
3.3.3 Security Settings



Security Setting

- Packet Filters**
 - Allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.
- Domain Filters**
 - Let you prevent users under this device from accessing specific URLs.
- URL Blocking**
 - URL Blocking will block LAN computers to connect to pre-defined websites.
- MAC Address Control**
 - MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.
- Miscellaneous**
 - Remote Administrator Host: 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.
 - Administrator Time-out: The amount of time of inactivity before the device will automatically close the Administrator session. Set this to zero to disable it.
 - Discard PING from WAN side: When this feature is enabled, hosts on the WAN cannot ping the Device.

3.3.3.1 Packet Filters



Outbound Packet Filter [HELP]

Enable

Allow all to pass except those match the following rules.
 Deny all to pass except those match the following rules.

Schedule rule: (00)Always Copy to ID --

ID	Source IP	Destination IP : Ports	Enable	Schedule Rule#
1	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/>



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:

- Allow all to pass except those match the specified rules
- 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 address
- Destination IP address
- Destination port address
- 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.

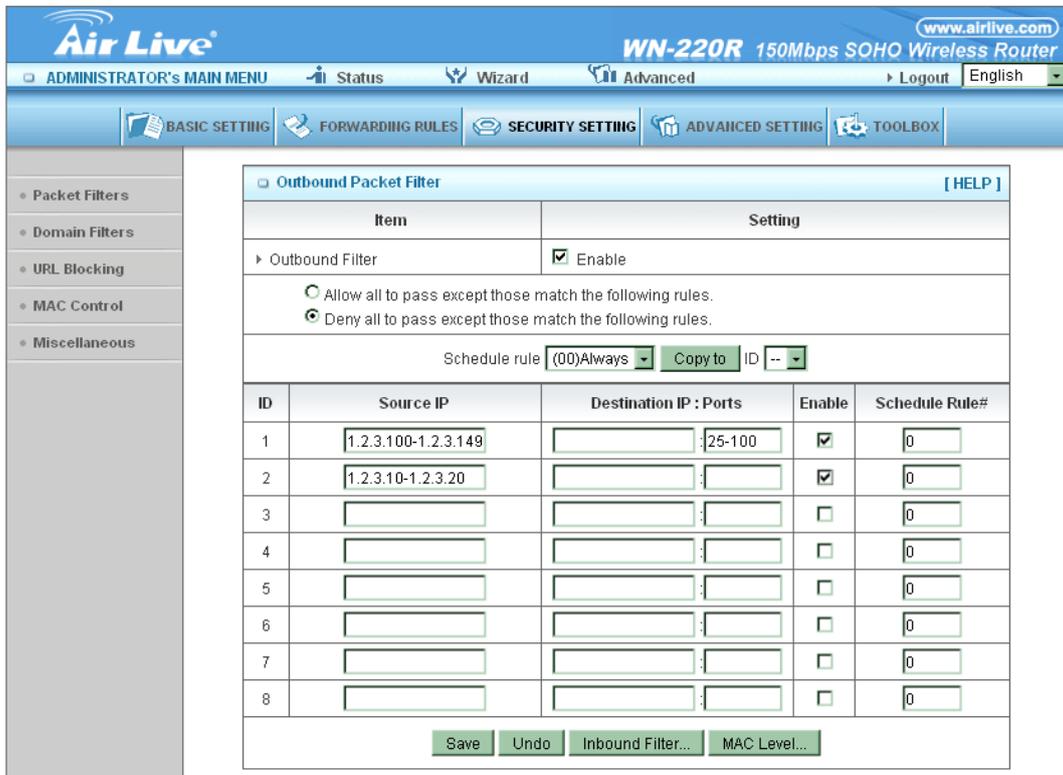
For source or destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example: T80, U53, U2000-2999. No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. Packet Filter can work with 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.

● Inbound Filter:

To enable **Inbound Packet Filter** click the check box next to **Enable** in the Inbound Packet Filter field.

Suppose you have SMTP Server (25), POP Server (110), Web Server (80), FTP Server (21), and News Server (119) defined in Virtual Server or DMZ Host.

➤ Example 1:



The screenshot shows the configuration page for the Air Live WN-220R 150Mbps SOHO Wireless Router. The page is titled "Outbound Packet Filter" and includes a sidebar with navigation options: Packet Filters, Domain Filters, URL Blocking, MAC Control, and Miscellaneous. The main content area shows the "Outbound Packet Filter" settings, which are currently enabled. The "Deny all to pass except those match the following rules" option is selected. A table below lists the filter rules:

ID	Source IP	Destination IP : Ports	Enable	Schedule Rule#
1	1.2.3.100-1.2.3.149	:25-100	<input checked="" type="checkbox"/>	0
2	1.2.3.10-1.2.3.20	:	<input checked="" type="checkbox"/>	0
3		:	<input type="checkbox"/>	0
4		:	<input type="checkbox"/>	0
5		:	<input type="checkbox"/>	0
6		:	<input type="checkbox"/>	0
7		:	<input type="checkbox"/>	0
8		:	<input type="checkbox"/>	0

At the bottom of the configuration area, there are buttons for "Save", "Undo", "Inbound Filter...", and "MAC Level...".

- (1.2.3.100-1.2.3.149) Remote hosts are allow to send mail (port 25), and browse the Internet (port 80)
- (1.2.3.10-1.2.3.20) Remote hosts can do everything (block nothing)
- Others are all blocked.

➤ Example 2:

The screenshot shows the 'Outbound Packet Filter' configuration page. The 'Outbound Filter' checkbox is checked. The 'Allow all to pass except those match the following rules' radio button is selected. The 'Schedule rule' is set to '(00)Always'. A table lists 8 rules. Rule 1 is active and configured with source IP '1.2.3.100-1.2.3.119' and destination ports '21' and '199'. Rules 2-8 are inactive.

ID	Source IP	Destination IP : Ports	Enable	Schedule Rule#
1	1.2.3.100-1.2.3.119	:21	<input checked="" type="checkbox"/>	0
2	1.2.3.10-1.2.3.199	:199	<input checked="" type="checkbox"/>	0
3			<input type="checkbox"/>	0
4			<input type="checkbox"/>	0
5			<input type="checkbox"/>	0
6			<input type="checkbox"/>	0
7			<input type="checkbox"/>	0
8			<input type="checkbox"/>	0

- (1.2.3.100-1.2.3.119) Remote hosts can do everything except read net news (port 119) and transfer files via FTP (port 21) behind Router Server.
- Others are all allowed.

After **Inbound Packet Filter** setting is configured, click the save button.

● **Outbound Filter:**

To enable **Outbound Packet Filter** click the check box next to Enable in the Outbound Packet Filter field.



➤ Example 1:

Router LAN IP is **192.168.12.254**

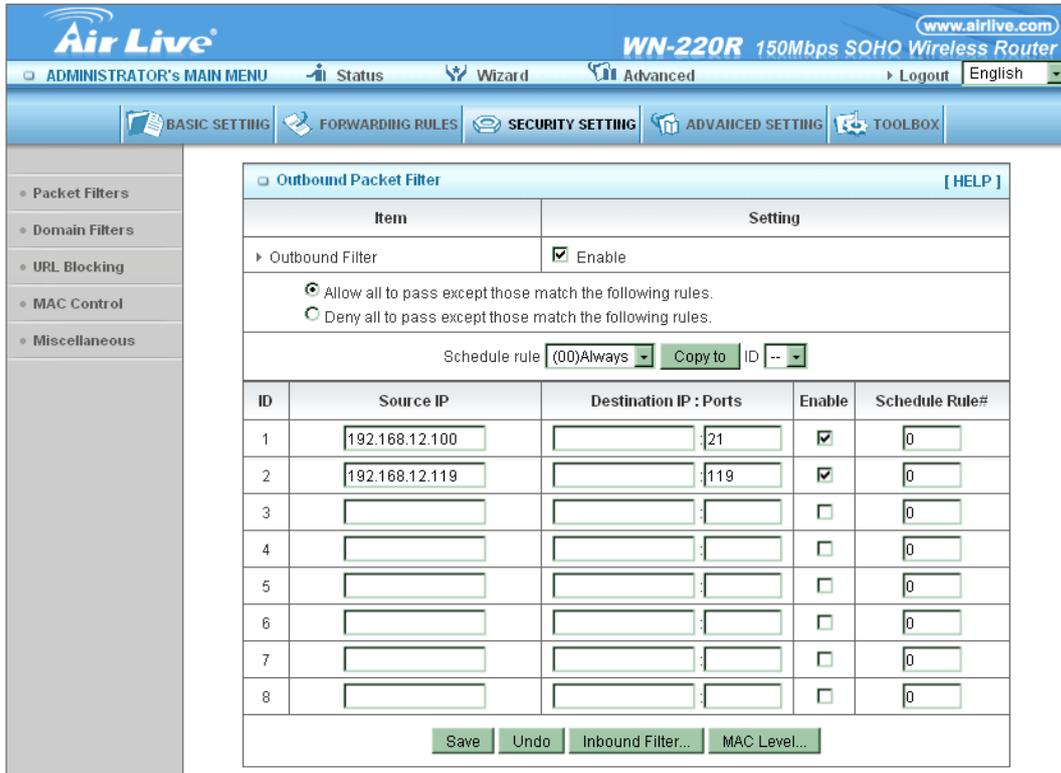
Outbound Packet Filter [HELP]

Item	Setting			
▶ Outbound Filter	<input checked="" type="checkbox"/> Enable			
<input checked="" type="radio"/> Allow all to pass except those match the following rules. <input type="radio"/> Deny all to pass except those match the following rules.				
Schedule rule: (00)Always <input type="button" value="Copy to"/> ID -- <input type="button" value="ID"/>				
ID	Source IP	Destination IP : Ports	Enable	Schedule Rule#
1	00-192.168.12.149	:21-100	<input checked="" type="checkbox"/>	0
2	2.10-192.168.12.20		<input checked="" type="checkbox"/>	0
3			<input type="checkbox"/>	0
4			<input type="checkbox"/>	0
5			<input type="checkbox"/>	0
6			<input type="checkbox"/>	0
7			<input type="checkbox"/>	0
8			<input type="checkbox"/>	0

- (192.168.12.100-192.168.12.149) Located hosts are only allowed to send mail (port 25), receive mail (port 110), and browse Internet (port 80); port 53 (DNS) is necessary to resolve the domain name.
- (192.168.12.10-192.168.12.20) Located hosts can do everything (block nothing)
- Others are all blocked.

➤ Example 2:

Router LAN IP is **192.168.12.254**



The screenshot shows the 'Outbound Packet Filter' configuration page. The 'Enable' checkbox is checked. The 'Allow all to pass except those match the following rules.' radio button is selected. The 'Schedule rule' is set to '(00)Always' and 'Copy to ID' is set to '--'. The table below lists the filter rules:

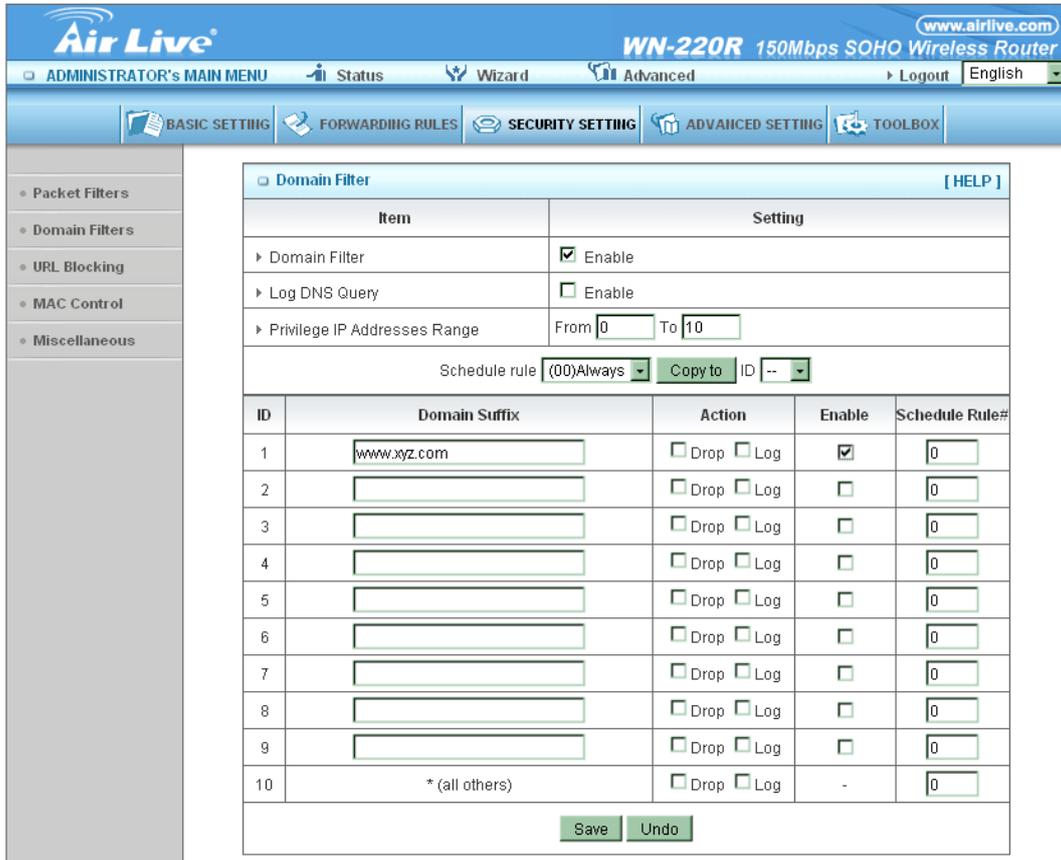
ID	Source IP	Destination IP : Ports	Enable	Schedule Rule#
1	192.168.12.100	:21	<input checked="" type="checkbox"/>	0
2	192.168.12.119	:119	<input checked="" type="checkbox"/>	0
3			<input type="checkbox"/>	0
4			<input type="checkbox"/>	0
5			<input type="checkbox"/>	0
6			<input type="checkbox"/>	0
7			<input type="checkbox"/>	0
8			<input type="checkbox"/>	0

Buttons at the bottom: Save, Undo, Inbound Filter..., MAC Level...

- (192.168.12.100 and 192.168.12.119) Located Hosts can do everything except read net news (port 119) and transfer files via FTP (port 21)
- Others are allowed

After **Outbound Packet Filter** setting is configured, click the save button.

3.3.3.2 Domain filters



Domain Filter [HELP]

Item	Setting
Domain Filter	<input checked="" type="checkbox"/> Enable
Log DNS Query	<input type="checkbox"/> Enable
Privilege IP Addresses Range	From <input type="text" value="0"/> To <input type="text" value="10"/>
Schedule rule: (00)Always <input type="button" value="Copy to"/> ID <input type="text" value="--"/>	

ID	Domain Suffix	Action	Enable	Schedule Rule#
1	<input type="text" value="www.xyz.com"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
2	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
9	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
10	*(all others)	<input type="checkbox"/> Drop <input type="checkbox"/> Log	-	<input type="text" value="0"/>

- **Domain Filter**

Let you prevent users under this device from accessing specific URLs.

- **Domain Filter Enable**

Check if you want to enable Domain Filter.

- **Log DNS Query**

Check if you want to log the action when someone accesses the specific URLs.

- **Privilege IP Addresses Range**

Setting a group of hosts and privilege these hosts to access network without restriction.

- **Domain Suffix**

A suffix of URL to be restricted. For example, ".com", "xxx.com".

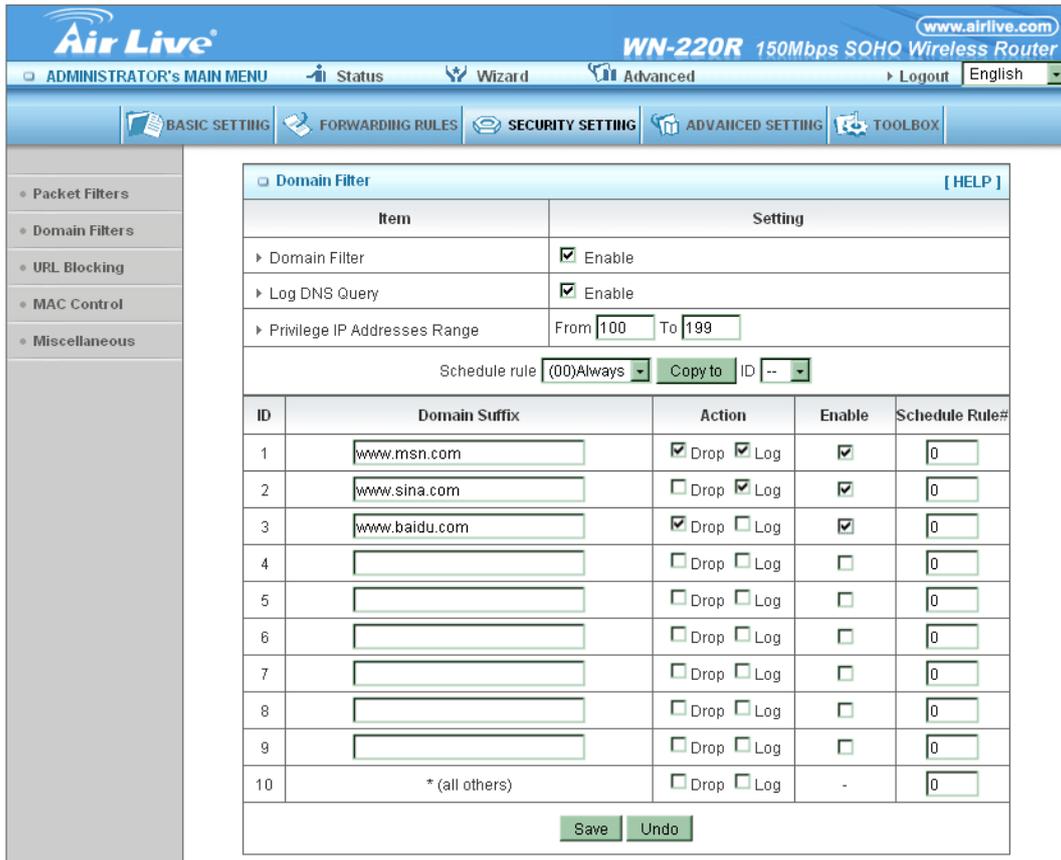
- **Action**

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.

● **Enable**

Check to enable each rule.

➤ Example:



Domain Filter [HELP]

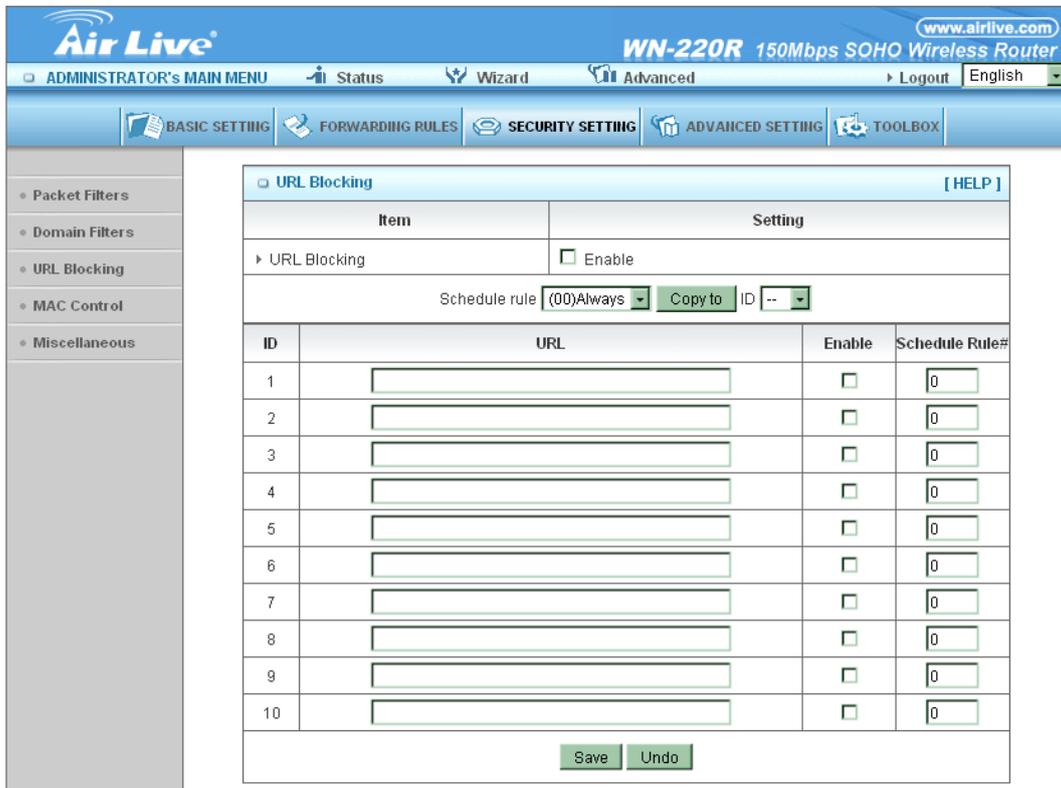
Item	Setting
▶ Domain Filter	<input checked="" type="checkbox"/> Enable
▶ Log DNS Query	<input checked="" type="checkbox"/> Enable
▶ Privilege IP Addresses Range	From <input type="text" value="100"/> To <input type="text" value="199"/>
Schedule rule: (00)Always <input type="button" value="Copy to"/> ID <input type="text" value="--"/>	

ID	Domain Suffix	Action	Enable	Schedule Rule#
1	<input type="text" value="www.msn.com"/>	<input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
2	<input type="text" value="www.sina.com"/>	<input type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text" value="www.baidu.com"/>	<input checked="" type="checkbox"/> Drop <input type="checkbox"/> Log	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
9	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>	<input type="text" value="0"/>
10	*(all others)	<input type="checkbox"/> Drop <input type="checkbox"/> Log	-	<input type="text" value="0"/>

In this example:

- URL include “www.msn.com” will be blocked, and the action will be record in log-file.
- URL include “www.sina.com” will not be blocked, but the action will be record in log-file.
- URL include “www.baidu.com” will be blocked, but the action will not be record in log-file.
- IP address x.x.x.1~x.x.x.99 can access Internet without restriction.

3.3.3.3 URL Blocking



ID	URL	Enable	Schedule Rule#
1	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
9	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
10	<input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>

URL Blocking will block LAN computers to connect to pre-defined Websites.

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

- **URL Blocking Enable**

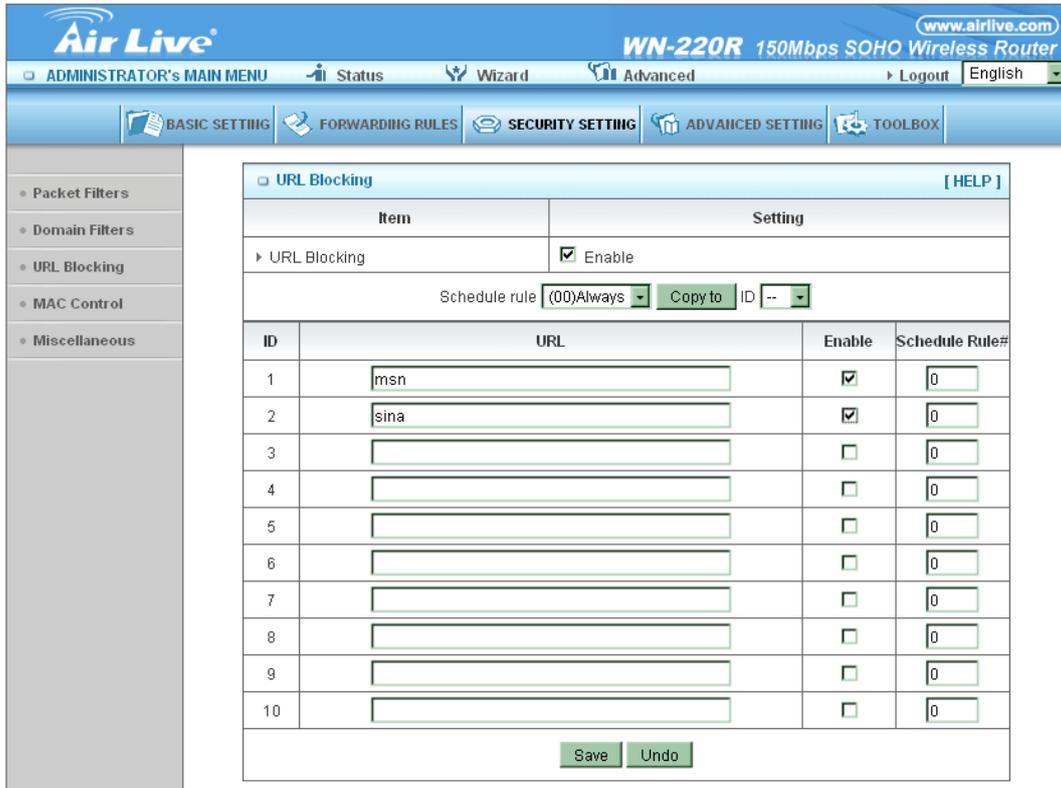
Checked if you want to enable URL Blocking.

- **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".

- **Enable**

Checked to enable each rule.



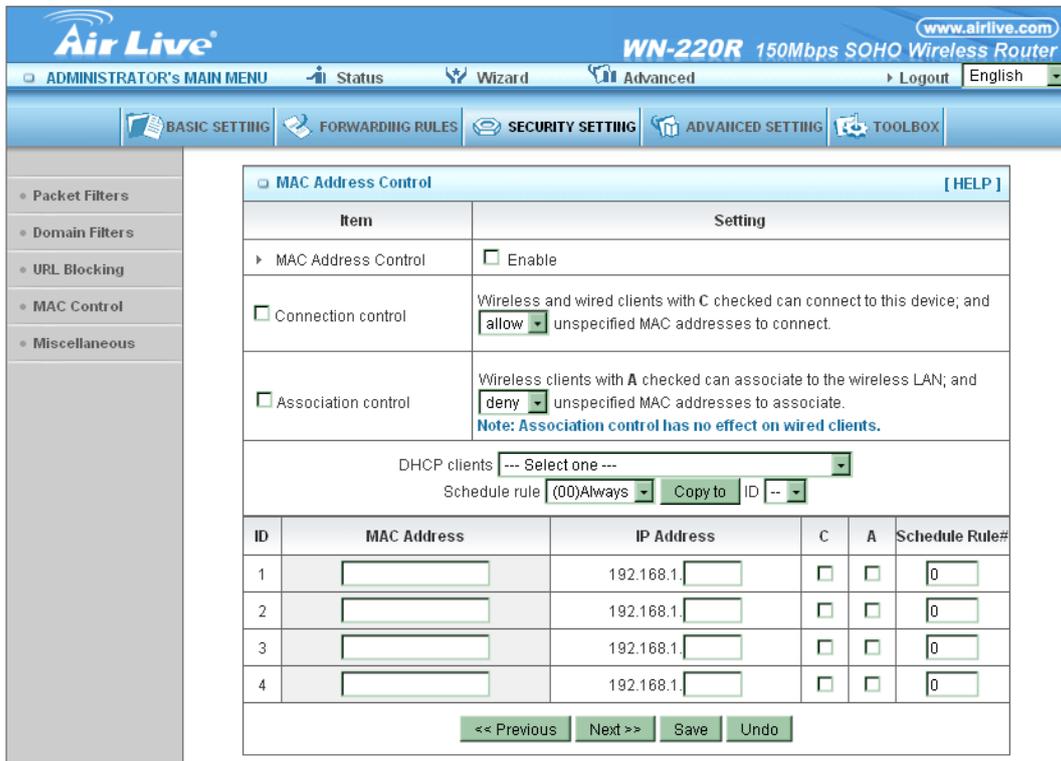
The screenshot shows the 'URL Blocking' configuration page in the Air Live WN-220R web interface. The page has a blue header with the Air Live logo and navigation tabs for 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', 'Logout', and 'English'. Below the header are tabs for 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The 'SECURITY SETTING' tab is active, showing a sidebar with options like 'Packet Filters', 'Domain Filters', 'URL Blocking', 'MAC Control', and 'Miscellaneous'. The main content area is titled 'URL Blocking' and includes a '[HELP]' link. It features a table with columns 'Item' and 'Setting'. Under 'Item', there is a 'URL Blocking' section with a 'Schedule rule' dropdown set to '(00)Always' and a 'Copy to ID' dropdown set to '--'. Below this is a table with columns 'ID', 'URL', 'Enable', and 'Schedule Rule#'. The table contains 10 rows. The first two rows have 'msn' and 'sina' in the 'URL' column, and their 'Enable' checkboxes are checked. The remaining eight rows have empty 'URL' fields and unchecked 'Enable' checkboxes. At the bottom of the table are 'Save' and 'Undo' buttons.

ID	URL	Enable	Schedule Rule#
1	msn	<input checked="" type="checkbox"/>	0
2	sina	<input checked="" type="checkbox"/>	0
3		<input type="checkbox"/>	0
4		<input type="checkbox"/>	0
5		<input type="checkbox"/>	0
6		<input type="checkbox"/>	0
7		<input type="checkbox"/>	0
8		<input type="checkbox"/>	0
9		<input type="checkbox"/>	0
10		<input type="checkbox"/>	0

In this example:

- URL include “msn” will be blocked, and the action will be record in log-file.
- URL include “sina” will be blocked, but the action will be record in log-file

3.3.3.4 MAC control



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

- **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.

- **Connection control**

Check "Connection control" to enable the controlling of which wired and wireless clients can connect to this device. If a client is denied to connect to 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 to this device.

- **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.



- **Control table**

ID	MAC Address	IP Address	C	A	Schedule Rule#
1	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/>	192.168.1. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>

"Control table" is the table at the bottom of the "MAC Address Control" page. Each row of this table indicates the MAC address and the expected IP address mapping of a client. There are four columns in this table:

MAC Address	MAC address indicates a specific client.
IP Address	Expected IP address of the corresponding client. Keep it empty if you don't care its IP address.
C	When "Connection control" is checked, check "C" will allow the corresponding client to connect to this device.
A	When "Association control" is checked, check "A" will allow the corresponding client to associate to the wireless LAN.

In this page, we provide the following Combobox and button to help you to input the MAC address.

DHCP clients ID

You can select a specific client in the "DHCP clients" Combobox, and then click on the "Copy to" button to copy the MAC address of the client you select to the ID selected in the "ID" Combobox.

- **Previous page and Next Page**

To make this setup page simple and clear, we have divided the "Control table" into several pages. You can use these buttons to navigate to different pages.



➤ Example:

The screenshot shows the configuration page for the Air Live WN-220R 150Mbps SOHO Wireless Router. The page is titled "MAC Address Control" and includes a sidebar with navigation options like "Packet Filters", "Domain Filters", "URL Blocking", "MAC Control", and "Miscellaneous". The main content area contains the following settings:

- MAC Address Control:** Enable
- Connection control:** Enabled. Setting: allow (dropdown). Description: Wireless and wired clients with C checked can connect to this device; and unspecified MAC addresses to connect.
- Association control:** Enabled. Setting: deny (dropdown). Description: Wireless clients with A checked can associate to the wireless LAN; and unspecified MAC addresses to associate. Note: Association control has no effect on wired clients.
- DHCP clients:** --- Select one --- (dropdown)
- Schedule rule:** (00)Always (dropdown) Copy to ID -- (dropdown)

ID	MAC Address	IP Address	C	A	Schedule Rule#
1	00-12-34-56-78-90	192.168.1.100	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
2	00-12-34-56-78-92	192.168.1.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
3	00-09-79-54-32-10	192.168.1.101	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0
4		192.168.1.	<input type="checkbox"/>	<input type="checkbox"/>	0

At the bottom of the table, there are navigation buttons: << Previous, Next >>, Save, and Undo.

In this scenario, there are three clients listed in the Control Table. Clients 1 and 2 are wireless, and client 3 is wired.

- The "MAC Address Control" function is enabled.
- "Connection control" is enabled, and all of the wired and wireless clients not listed in the "Control table" are "allowed" to connect to this device.
- "Association control" is enabled, and all of the wireless clients not listed in the "Control table" are "denied" to associate to the wireless LAN.
- Clients 1 and 3 have fixed IP addresses either from the DHCP server of this device or manually assigned:

ID 1 - "00-12-34-56-78-90" --> 192.168.12.100

ID 3 - "00-98-76-54-32-10" --> 192.168.12.101

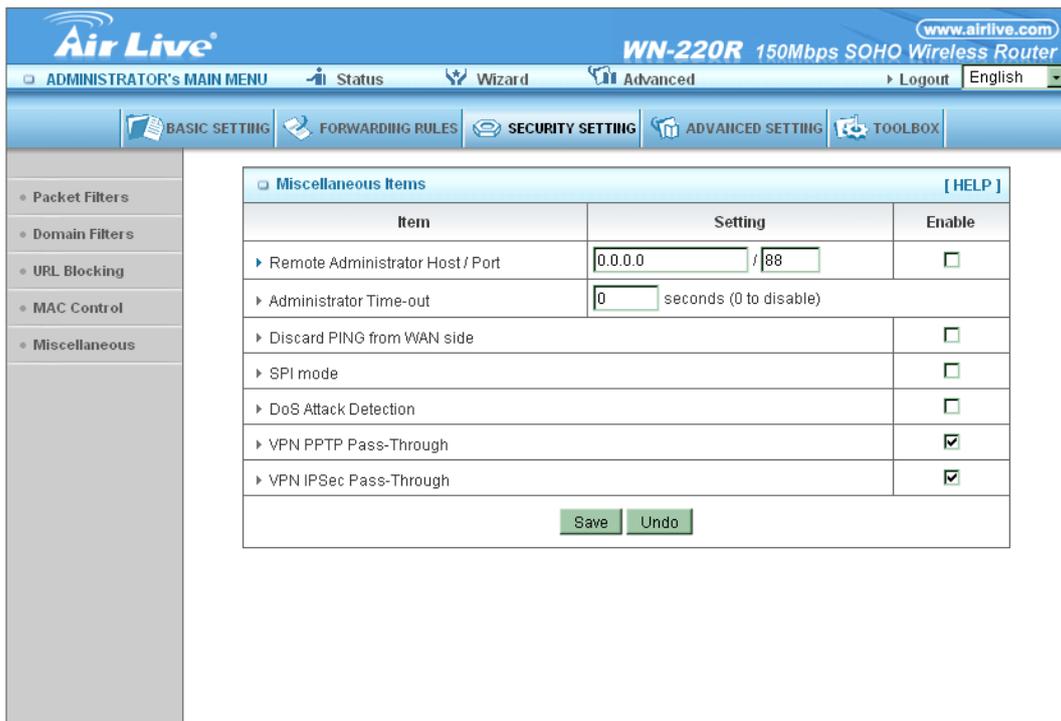
Client 2 will obtain its IP address from the IP Address pool specified in the "DHCP Server" page or can use a manually assigned static IP address.

If, for example, client 3 tries to use an IP address different from the address listed in the Control table (192.168.12.101), it will be denied to connect to this device.

- Clients 2 and 3 and other wired clients with a MAC address unspecified in the Control table are all allowed to connect to this device. But client 1 is denied to connect to this device.

- Clients 1 and 2 are allowed to associate to the wireless LAN, but a wireless client with a MAC address not specified in the Control table is denied to associate to the wireless LAN. Client 3 is a wired client and so is not affected by Association control.

3.3.3.5 Miscellaneous Items



● 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 to 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 88. You can change web server port to other port, too.

● Administrator Time-out

The time of no activity to logout automatically. Set it to zero to disable this feature.

● Discard PING from WAN side

When this feature is enabled, any host on the WAN cannot ping this product.

● SPI Mode

When this feature is enabled, the router will record the packet information pass through the router like IP address, port address, ACK, SEQ number and so on. And the router will check every incoming packet to detect if this packet is valid.



● 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.

● VPN PPTP and IPSec Pass-Through

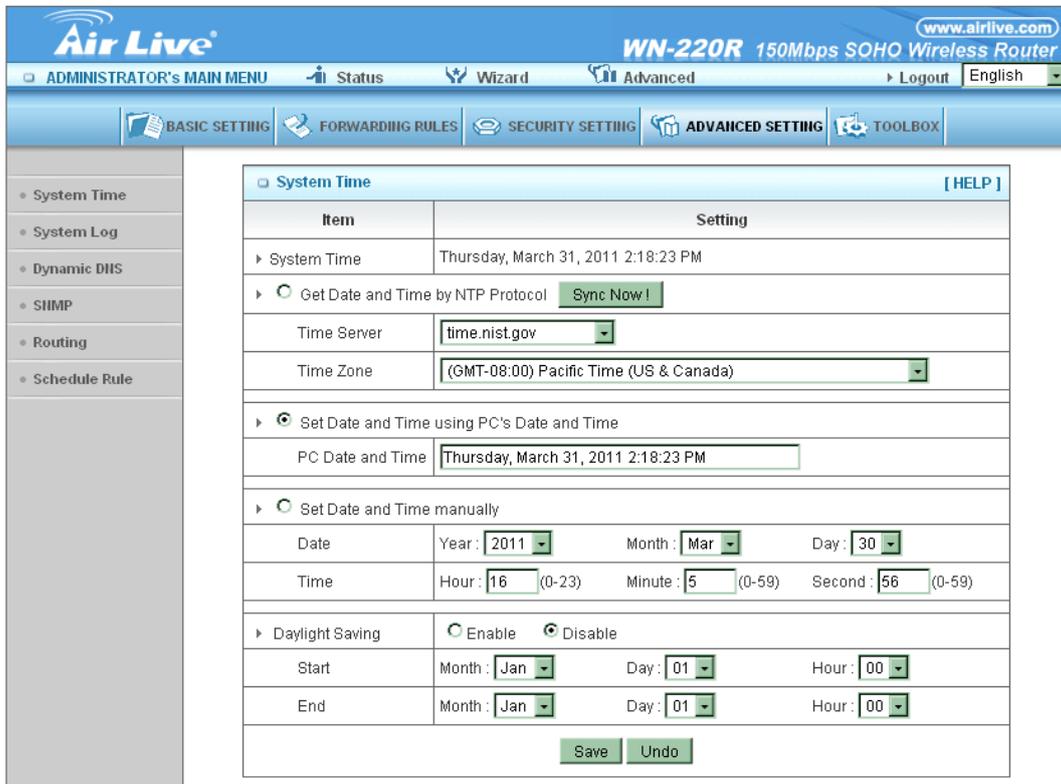
Virtual Private Networking (VPN) is typically used for work-related networking. For VPN tunnels, the router supports IPSec Passthrough and PPTP Passthrough.

3.3.4 Advanced Settings

The screenshot displays the web management interface for the Air Live WN-220R 150Mbps SOHO Wireless Router. The top navigation bar includes the Air Live logo, the model name 'WN-220R 150Mbps SOHO Wireless Router', and the website 'www.airlive.com'. Below this, there are links for 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', 'Logout', and a language dropdown set to 'English'. A secondary navigation bar contains icons for 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING' (which is active), and 'TOOLBOX'. On the left side, a vertical menu lists various settings: System Time, System Log, Dynamic DNS, SHMP, Routing, and Schedule Rule. The main content area is titled 'Advanced Setting' and contains a list of configuration options with brief descriptions:

- System Time**
 - Allow you to set device time manually or consult network time from NTP server.
- System Log**
 - Send system log to a dedicated host or email to specific receipts.
- Dynamic DNS**
 - To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).
- SNMP**
 - Gives a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.
- Routing**
 - If you have more than one routers and subnets, you may want to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.
- Schedule Rule**
 - Apply schedule rules to Packet Filters and Virtual Server.

3.3.4.1 System Time



System Time [HELP]	
Item	Setting
System Time	Thursday, March 31, 2011 2:18:23 PM
<input type="radio"/> Get Date and Time by NTP Protocol <input type="button" value="Sync Now!"/>	
Time Server	time.nist.gov
Time Zone	(GMT-08:00) Pacific Time (US & Canada)
<input checked="" type="radio"/> Set Date and Time using PC's Date and Time	
PC Date and Time	Thursday, March 31, 2011 2:18:23 PM
<input type="radio"/> Set Date and Time manually	
Date	Year: 2011 Month: Mar Day: 30
Time	Hour: 16 (0-23) Minute: 5 (0-59) Second: 56 (0-59)
<input type="checkbox"/> Daylight Saving <input checked="" type="checkbox"/> Disable	
Start	Month: Jan Day: 01 Hour: 00
End	Month: Jan Day: 01 Hour: 00
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

- **Get Date and Time by NTP Protocol**

Selected if you want to Get Date and Time by NTP Protocol.

- **Time Server**

Select a NTP time server to consult UTC time

- **Time Zone**

Select a time zone where this device locates.

- **Set Date and Time manually**

Selected if you want to Set Date and Time manually.

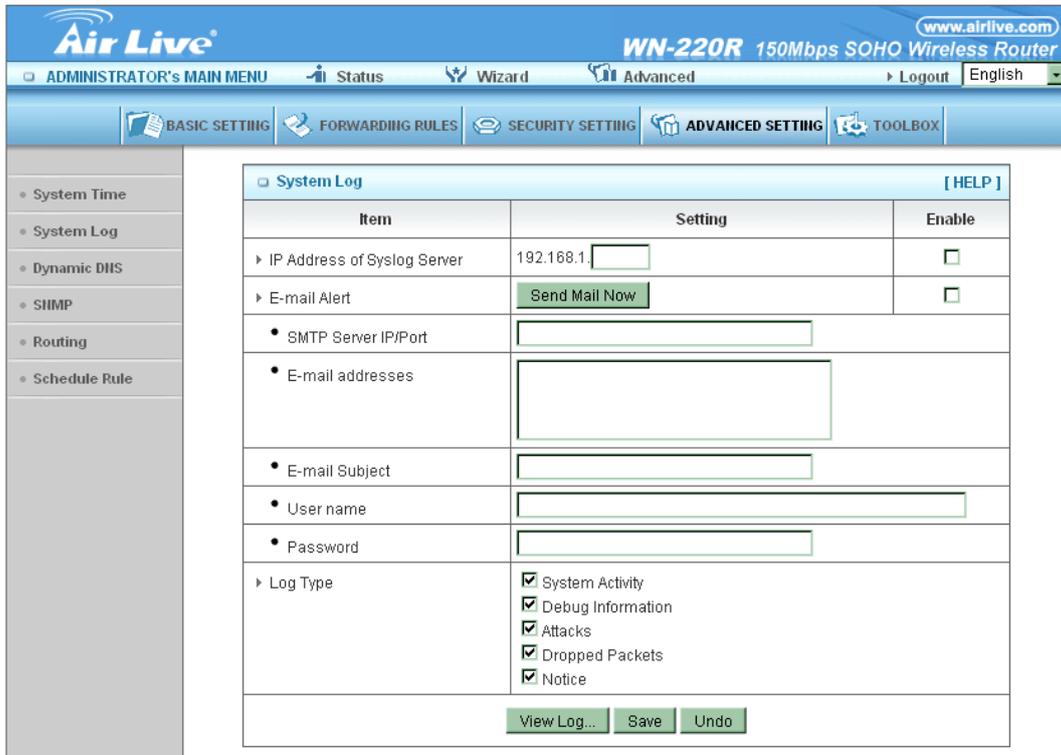
- **Set Date and Time manually**

Selected if you want to Set Date and Time manually.

- **Function of Buttons**

- Sync Now: Synchronize system time with network time server
- Daylight Saving: Set up where the location is.

3.3.4.2 System Log



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

- **IP Address for Syslog**

Host IP of destination where syslogs will be sent to.
Check Enable to enable this function.

- **E-mail Alert Enable**

Check if you want to enable Email alert (send syslog via email).

- **SMTP Server IP and Port**

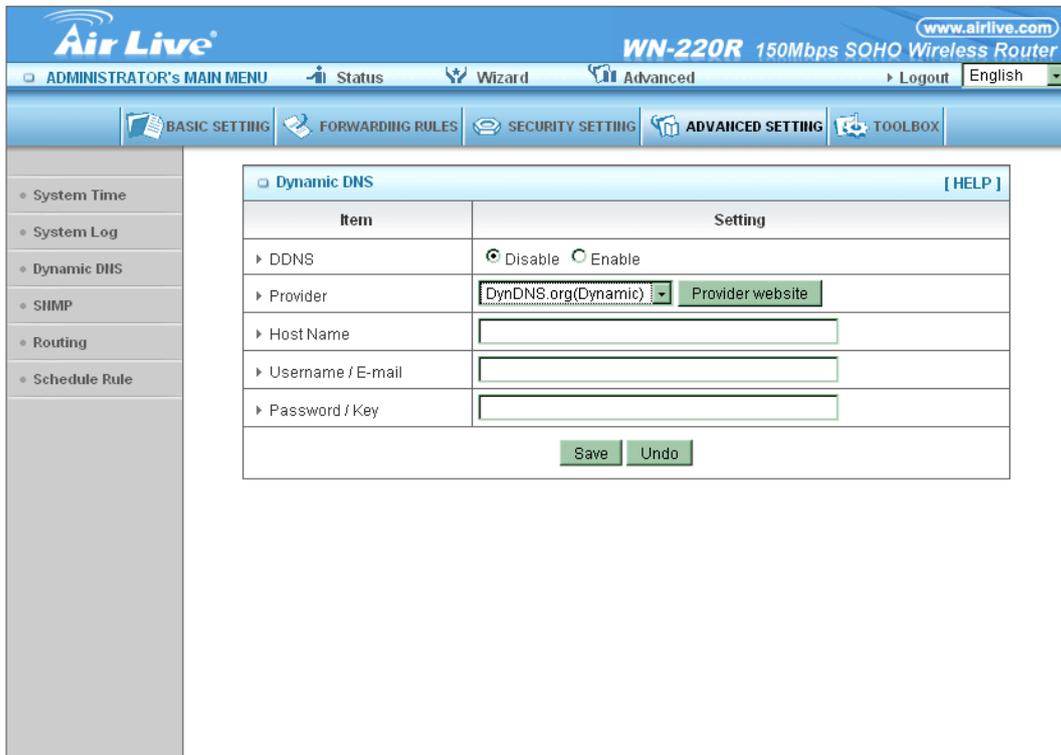
Input the SMTP server IP and port, which are concreted with ':'. If you do not specify port number, the default value is 25.

For example, "mail.your_url.com" or "192.168.1.100:26".

- **Send E-mail alert to**

The recipients are the ones who will receive these logs. You can assign more than 1 recipient by using ';' or ',' to separate these email addresses.

3.3.4.3 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.

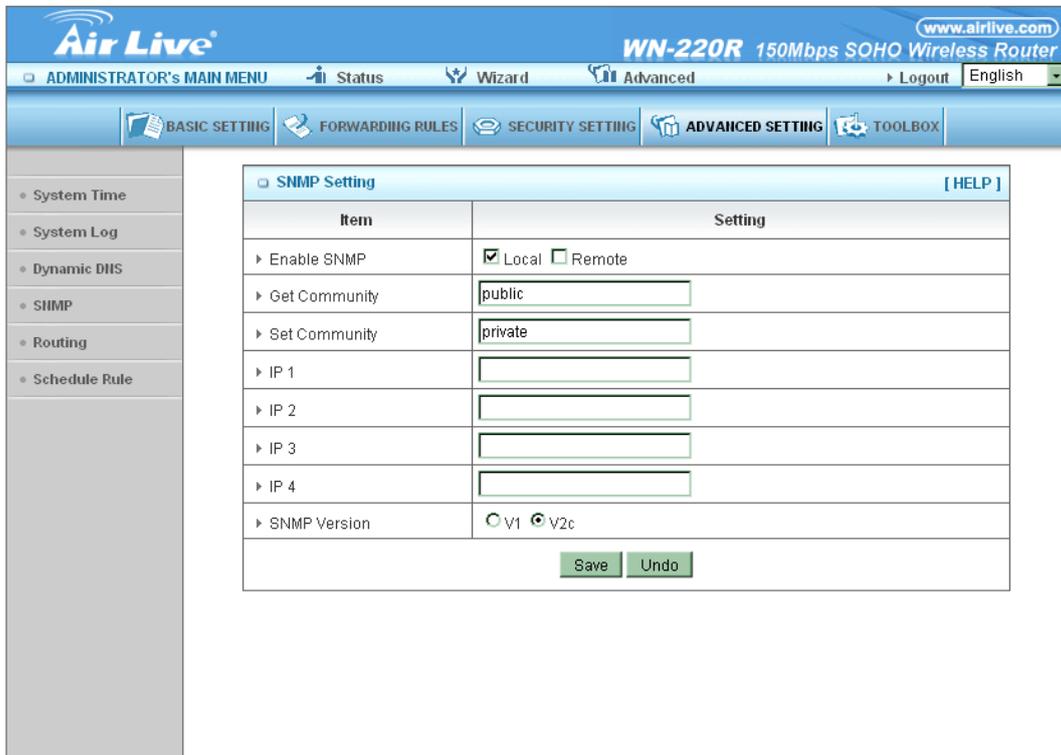
Next you can enter the appropriate information about your Dynamic DNS Server.

You have to define:

- **Provider**
- **Host Name**
- **Username/E-mail**
- **Password/Key**

You will get this information when you register an account on a Dynamic DNS server.

3.3.4.4 SNMP



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

- **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.

- **Get Community**

Setting the community of GetRequest your device will response.

- **Set Community**

Setting the community of SetRequest your device will accept.

IP 1, IP 2, IP 3, IP 4

Input your SNMP Management PC's IP here. User has to configure to where this device should send SNMP Trap message.

- **SNMP Version**

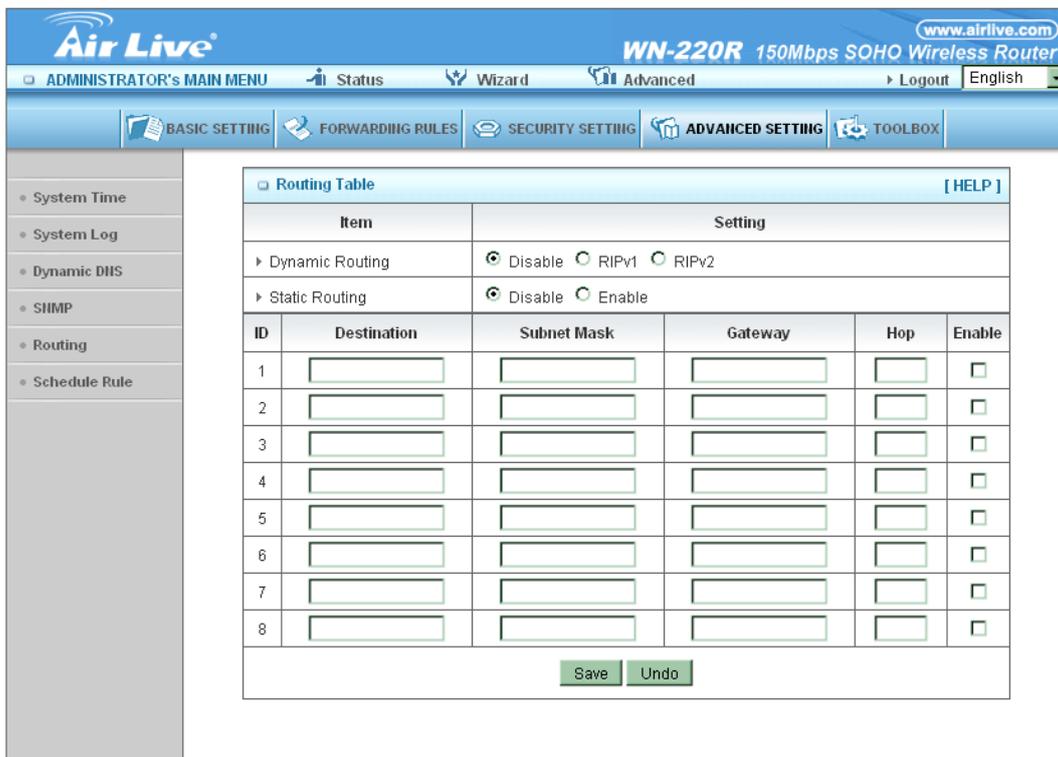
Please select proper SNMP Version that your SNMP Management software supports.

● **WAN Access IP Address**

If the user wants to limit to specific the IP address to access, please input in the item. The default 0.0.0.0 and means every IP of Internet can get some information of device with SNMP protocol.

Click on **“Save”** to store your setting or **“Undo”** to give up.

3.3.4.5 Routing



Routing Tables allow you to determine which physical interface address to use for outgoing IP data grams. 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.

Routing Table settings are settings used to setup the functions of static.

● **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.

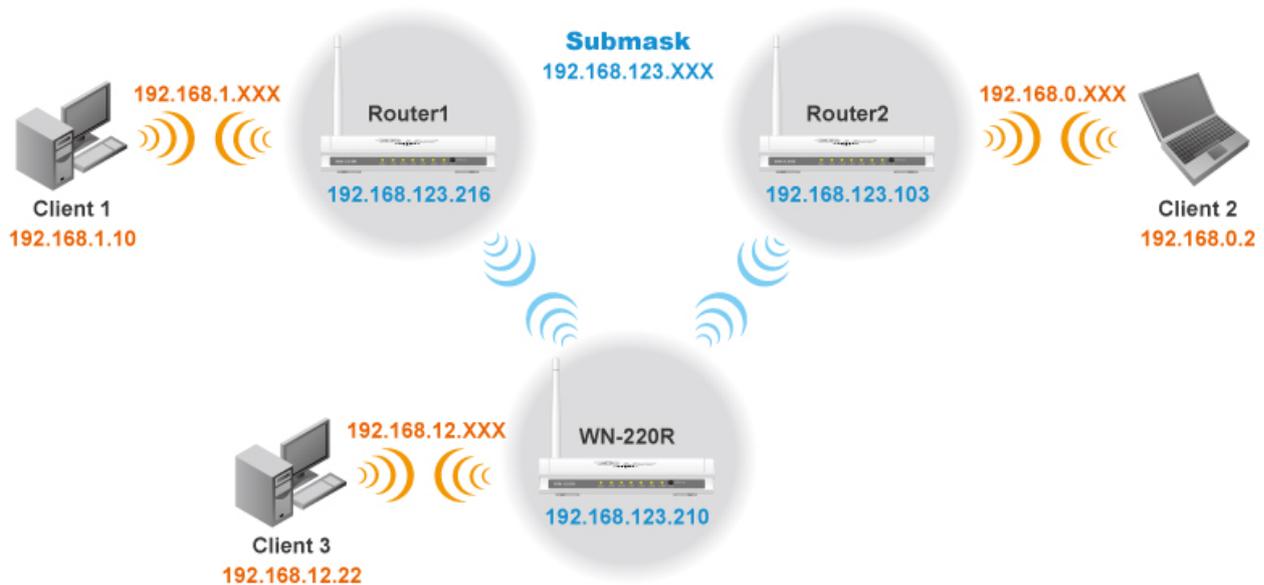
Otherwise, please select RIPv1 if you need this protocol.



- **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 unchecking the Enable checkbox.

➤ Example:



Configuration on NAT Router

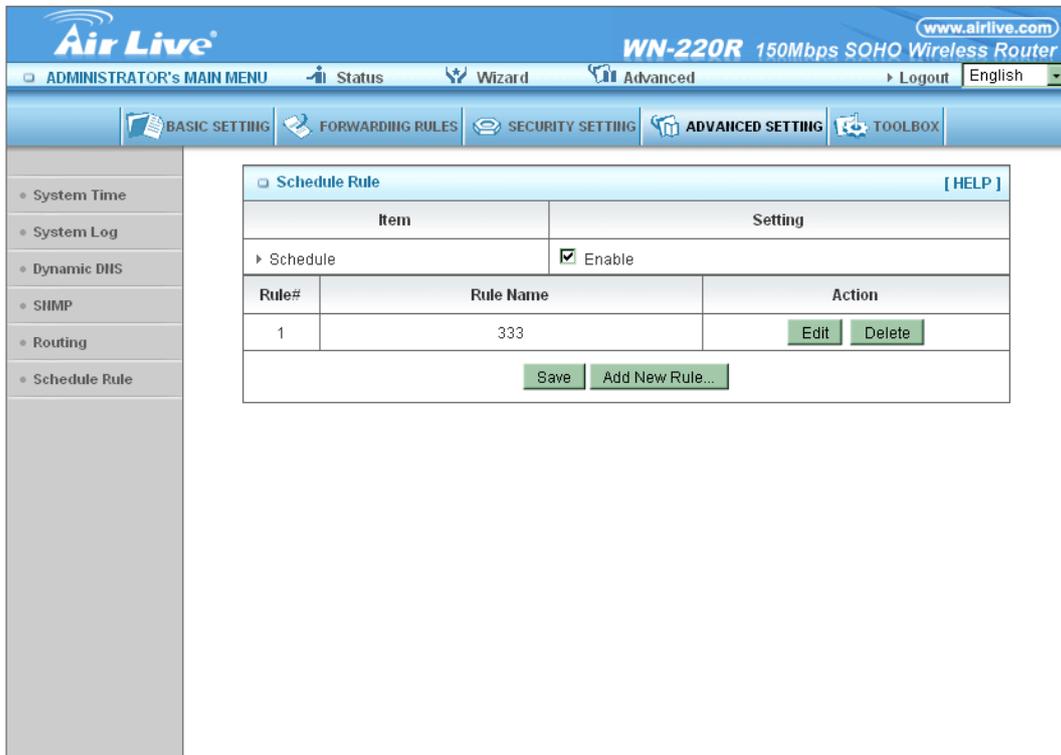
Destination	SubnetMask	Gateway	Hop	Enabled
192.168.1.0	255.255.255.0	192.168.123.216	1	✓
192.168.0.0	255.255.255.0	192.168.123.103	1	✓

So if, for example, the client3 wanted to send an IP data gram to 192.168.0.2, it would use the above table to determine that it had to go via 192.168.123.103 (a gateway), and if it sends Packets to 192.168.1.11 will go via 192.168.123.216

Each rule can be enabled or disabled individually.

After routing table setting is configured, click the **Save** button.

3.3.4.6 Schedule Rule



The screenshot shows the 'Schedule Rule' configuration page in the Air Live WN-220R web interface. The page has a blue header with the Air Live logo and the model name 'WN-220R 150Mbps SOHO Wireless Router'. The navigation menu includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', 'Logout', and 'English'. The main menu on the left lists 'System Time', 'System Log', 'Dynamic DNS', 'SHMP', 'Routing', and 'Schedule Rule'. The main content area is titled 'Schedule Rule' and contains a table with the following data:

Item	Setting
Schedule	<input checked="" type="checkbox"/> Enable

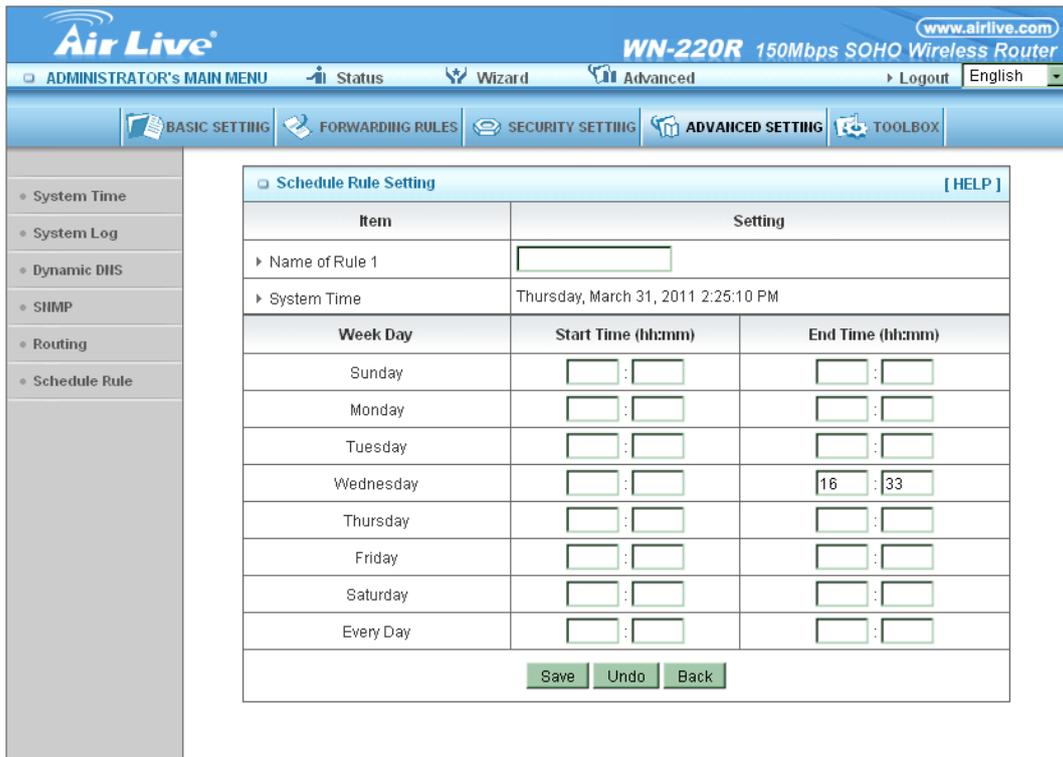
Rule#	Rule Name	Action
1	333	Edit Delete

At the bottom of the table, there are buttons for 'Save' and 'Add New Rule...'.

You can set the schedule time to decide which service will be turned on or off. Select the “enable” item.

Press “**Add New Rule**”

You can write a rule name and set which day and what time to schedule from “Start Time” to “End Time”. The following example configure “ftp time” as everyday 14:10 to 16:20



- **Schedule Enable**

Selected if you want to Enable the Scheduler.

- **Edit**

To edit the schedule rule.

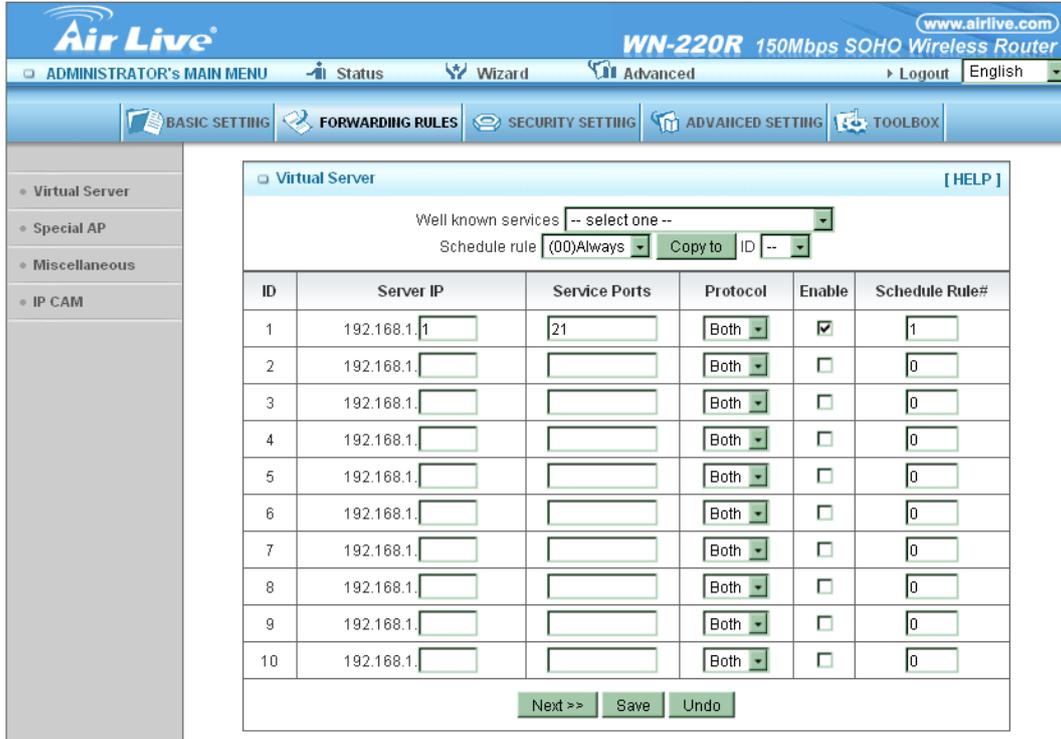
- **Delete**

To delete the schedule rule and the rule #of the rules behind the deleted one will decrease one automatically.

Schedule Rule can be applied to Virtual server and Packet Filter, for example:

➤ Example1:

Virtual Server – Apply Rule#1 (ftp time: everyday 14:20 to 16:30)



Virtual Server [HELP]

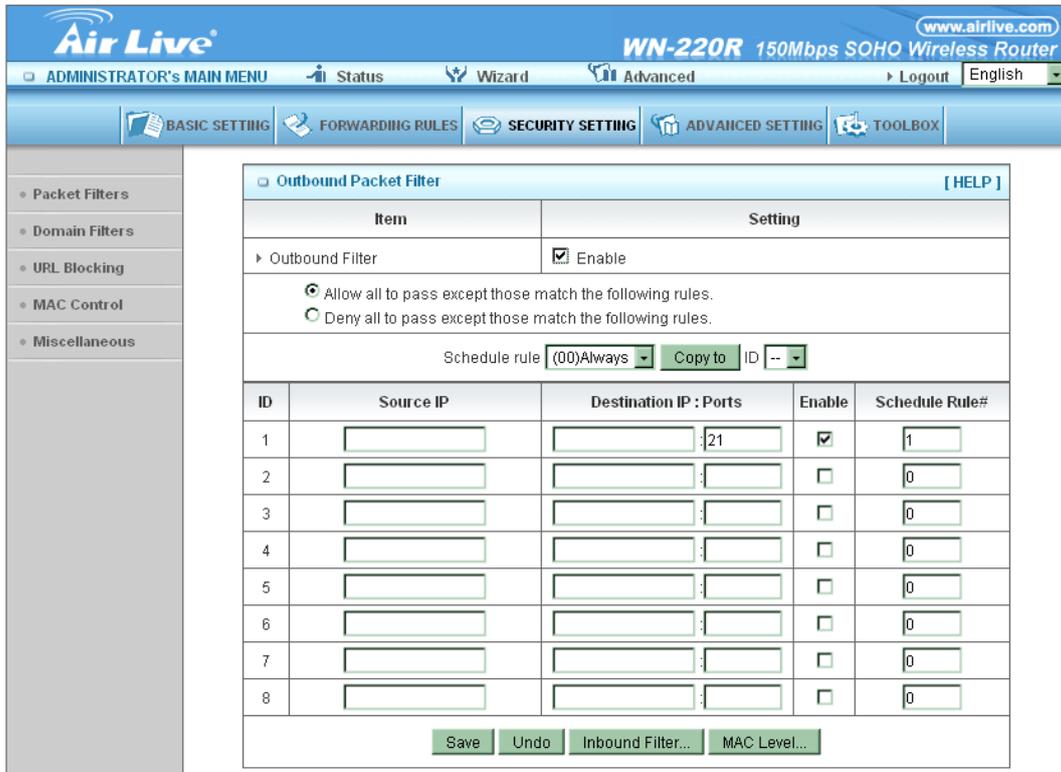
Well known services: -- select one --
 Schedule rule: (00)Always Copy to ID: --

ID	Server IP	Service Ports	Protocol	Enable	Schedule Rule#
1	192.168.1.1	21	Both	<input checked="" type="checkbox"/>	1
2	192.168.1.		Both	<input type="checkbox"/>	0
3	192.168.1.		Both	<input type="checkbox"/>	0
4	192.168.1.		Both	<input type="checkbox"/>	0
5	192.168.1.		Both	<input type="checkbox"/>	0
6	192.168.1.		Both	<input type="checkbox"/>	0
7	192.168.1.		Both	<input type="checkbox"/>	0
8	192.168.1.		Both	<input type="checkbox"/>	0
9	192.168.1.		Both	<input type="checkbox"/>	0
10	192.168.1.		Both	<input type="checkbox"/>	0

Next >> Save Undo

➤ Example2:

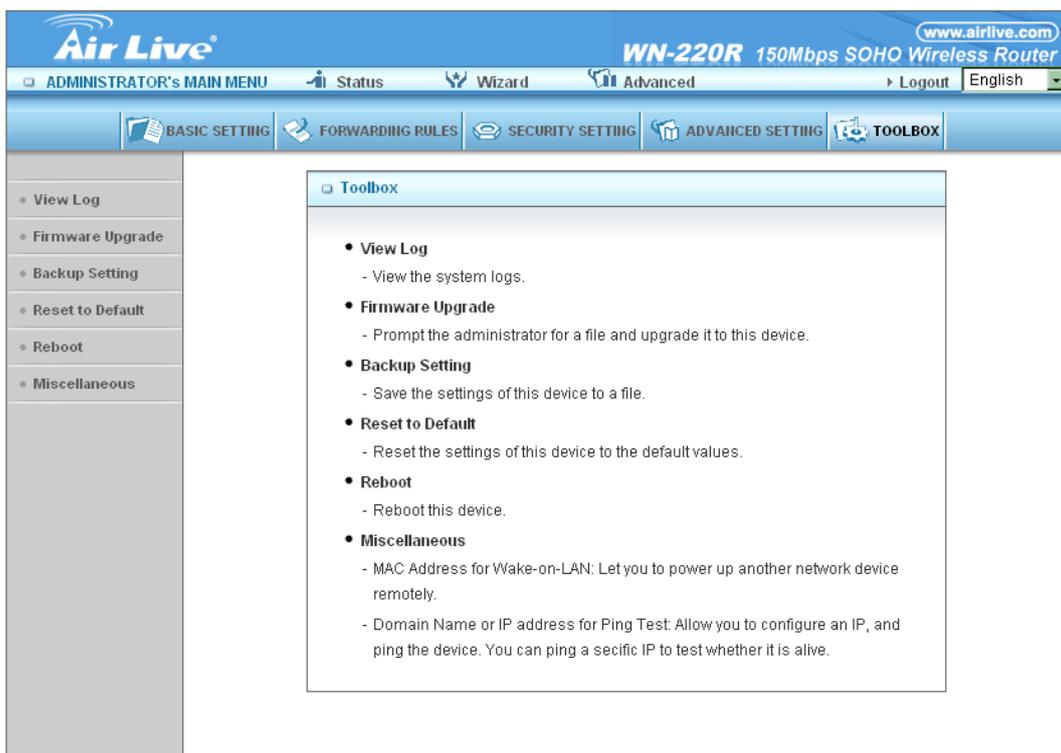
Packet Filter – Apply Rule#1 (ftp time: everyday 14:20 to 16:30).



The screenshot shows the 'Outbound Packet Filter' configuration page. The interface includes a top navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', 'Logout', and 'English'. Below this is a secondary navigation bar with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a tree view with 'Packet Filters', 'Domain Filters', 'URL Blocking', 'MAC Control', and 'Miscellaneous'. The main content area is titled 'Outbound Packet Filter' and includes a '[HELP]' link. It features a table with columns for 'Item' and 'Setting'. The 'Outbound Filter' is checked and enabled. Below this, there are radio buttons for 'Allow all to pass except those match the following rules.' (selected) and 'Deny all to pass except those match the following rules.'. A 'Schedule rule' dropdown is set to '(00)Always' and a 'Copy to ID' dropdown is set to '--'. A table below lists 8 filter rules. Rule 1 is enabled and has a schedule rule of 1. The other rules are disabled and have a schedule rule of 0. At the bottom, there are buttons for 'Save', 'Undo', 'Inbound Filter...', and 'MAC Level...'.

Item	Setting			
▶ Outbound Filter	<input checked="" type="checkbox"/> Enable			
<input checked="" type="radio"/> Allow all to pass except those match the following rules. <input type="radio"/> Deny all to pass except those match the following rules.				
Schedule rule: (00)Always Copy to ID: --				
ID	Source IP	Destination IP : Ports	Enable	Schedule Rule#
1	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input checked="" type="checkbox"/>	<input type="text" value="1"/>
2	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>

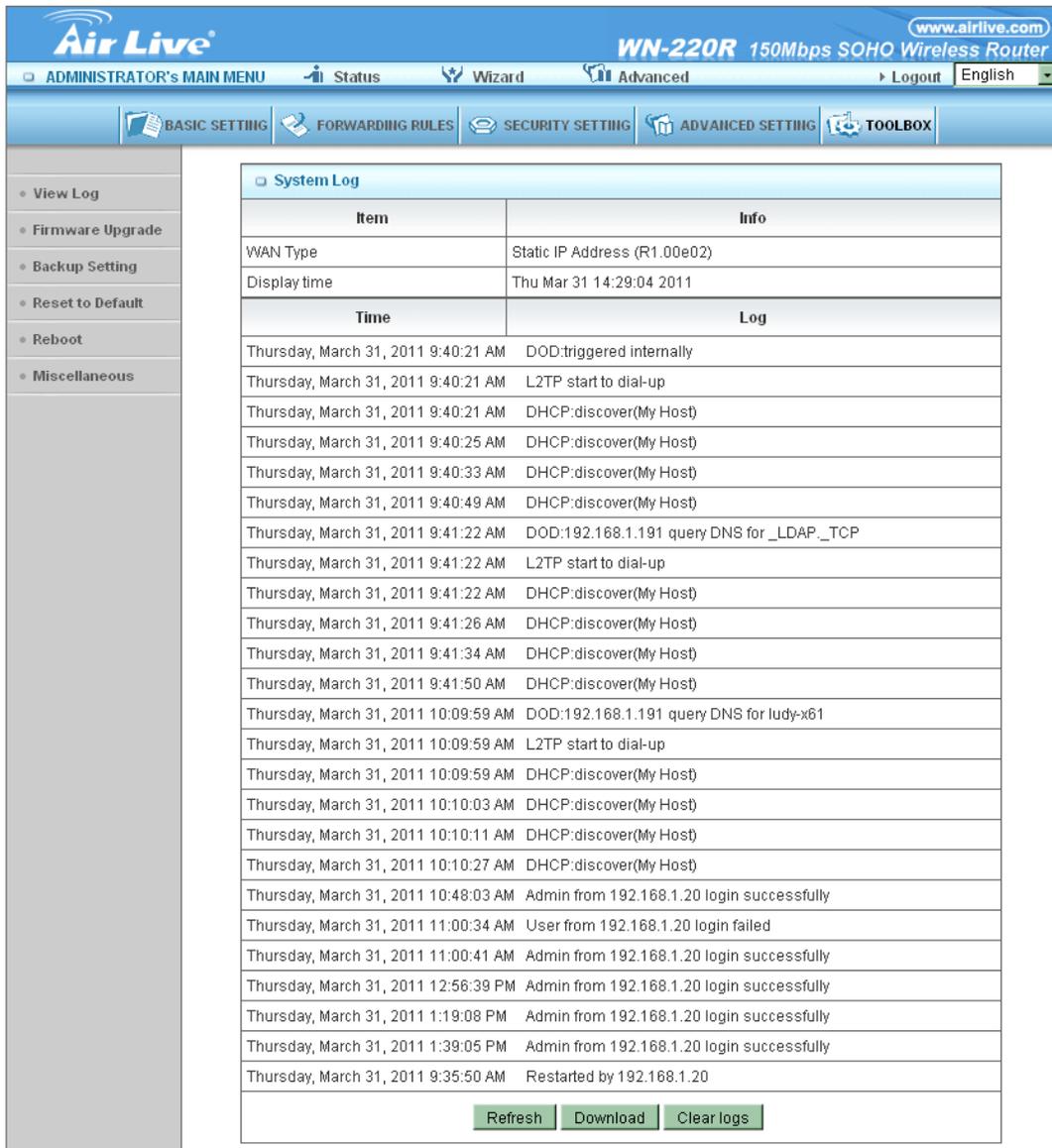
3.3.5 Toolbox



The screenshot shows the 'Toolbox' page in the Air Live WN-220R web interface. The top navigation bar and secondary navigation bar are identical to the previous screenshot. The left sidebar contains a tree view with 'View Log', 'Firmware Upgrade', 'Backup Setting', 'Reset to Default', 'Reboot', and 'Miscellaneous'. The main content area is titled 'Toolbox' and contains a list of tools with their descriptions:

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

3.3.5.1 View Log



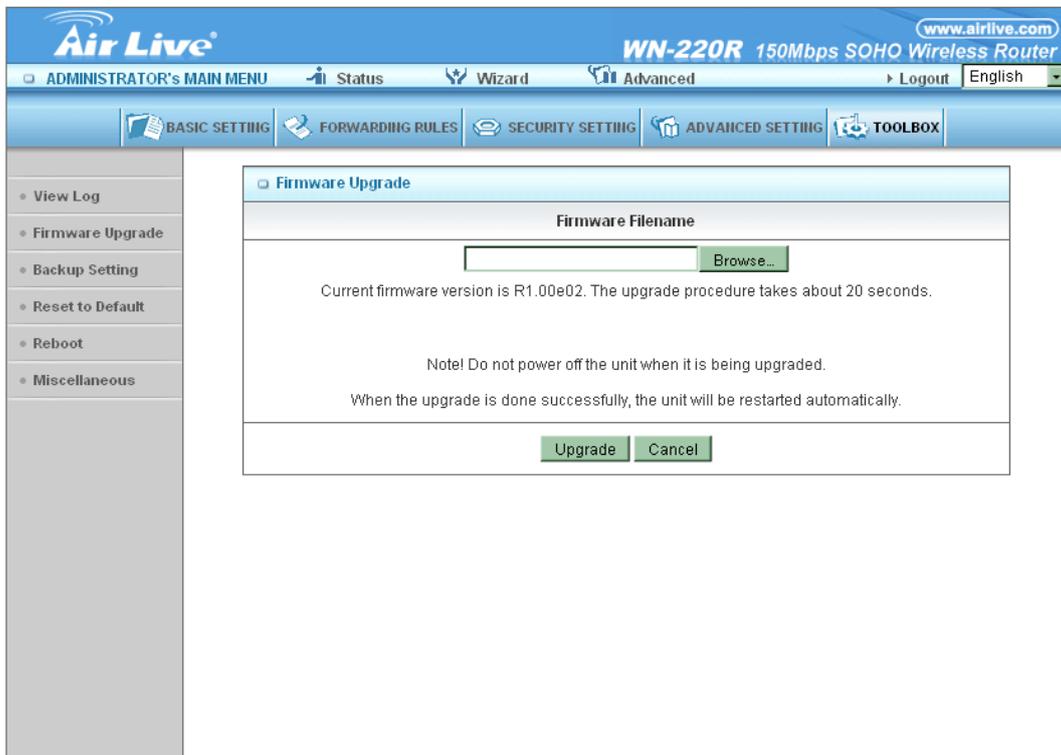
The screenshot shows the Air Live WN-220R web interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', 'Logout', and 'English'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a list of options: 'View Log', 'Firmware Upgrade', 'Backup Setting', 'Reset to Default', 'Reboot', and 'Miscellaneous'. The main content area displays the 'System Log' table.

System Log	
Item	Info
WAN Type	Static IP Address (R1.00e02)
Display time	Thu Mar 31 14:29:04 2011
Time	Log
Thursday, March 31, 2011 9:40:21 AM	DOD:triggered internally
Thursday, March 31, 2011 9:40:21 AM	L2TP start to dial-up
Thursday, March 31, 2011 9:40:21 AM	DHCP:discover(My Host)
Thursday, March 31, 2011 9:40:25 AM	DHCP:discover(My Host)
Thursday, March 31, 2011 9:40:33 AM	DHCP:discover(My Host)
Thursday, March 31, 2011 9:40:49 AM	DHCP:discover(My Host)
Thursday, March 31, 2011 9:41:22 AM	DOD:192.168.1.191 query DNS for _LDAP_TCP
Thursday, March 31, 2011 9:41:22 AM	L2TP start to dial-up
Thursday, March 31, 2011 9:41:22 AM	DHCP:discover(My Host)
Thursday, March 31, 2011 9:41:26 AM	DHCP:discover(My Host)
Thursday, March 31, 2011 9:41:34 AM	DHCP:discover(My Host)
Thursday, March 31, 2011 9:41:50 AM	DHCP:discover(My Host)
Thursday, March 31, 2011 10:09:59 AM	DOD:192.168.1.191 query DNS for ludy:x61
Thursday, March 31, 2011 10:09:59 AM	L2TP start to dial-up
Thursday, March 31, 2011 10:09:59 AM	DHCP:discover(My Host)
Thursday, March 31, 2011 10:10:03 AM	DHCP:discover(My Host)
Thursday, March 31, 2011 10:10:11 AM	DHCP:discover(My Host)
Thursday, March 31, 2011 10:10:27 AM	DHCP:discover(My Host)
Thursday, March 31, 2011 10:48:03 AM	Admin from 192.168.1.20 login successfully
Thursday, March 31, 2011 11:00:34 AM	User from 192.168.1.20 login failed
Thursday, March 31, 2011 11:00:41 AM	Admin from 192.168.1.20 login successfully
Thursday, March 31, 2011 12:56:39 PM	Admin from 192.168.1.20 login successfully
Thursday, March 31, 2011 1:19:08 PM	Admin from 192.168.1.20 login successfully
Thursday, March 31, 2011 1:39:05 PM	Admin from 192.168.1.20 login successfully
Thursday, March 31, 2011 9:35:50 AM	Restarted by 192.168.1.20

At the bottom of the log table, there are three buttons: 'Refresh', 'Download', and 'Clear logs'.

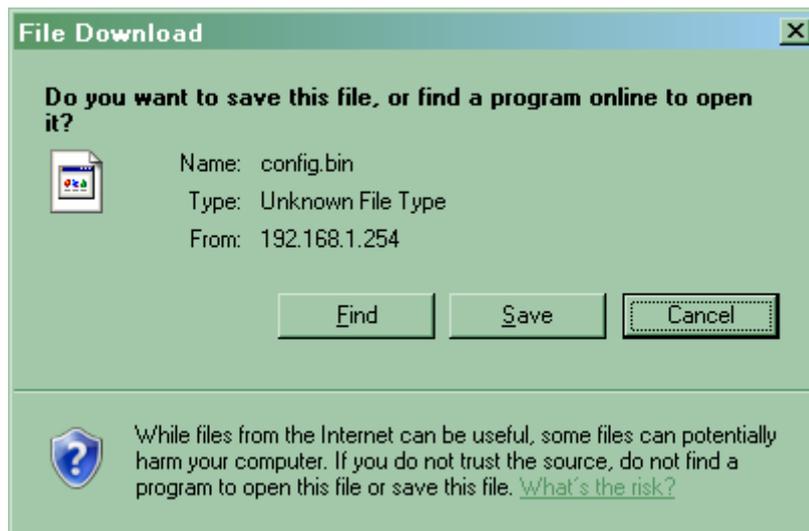
You can View system log by clicking the **View Log** button

3.3.5.2 Firmware Upgrade



You can upgrade firmware by clicking **Firmware Upgrade** button.

3.3.5.3 Backup Setting



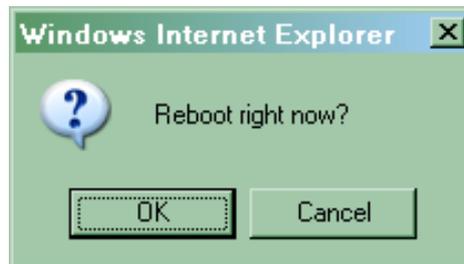
You can backup your settings by clicking the **Backup Setting** button and save it as a bin file. Once you want to restore these settings, please click **Firmware Upgrade** button and use the bin file you saved.

3.3.5.4 Reset to default



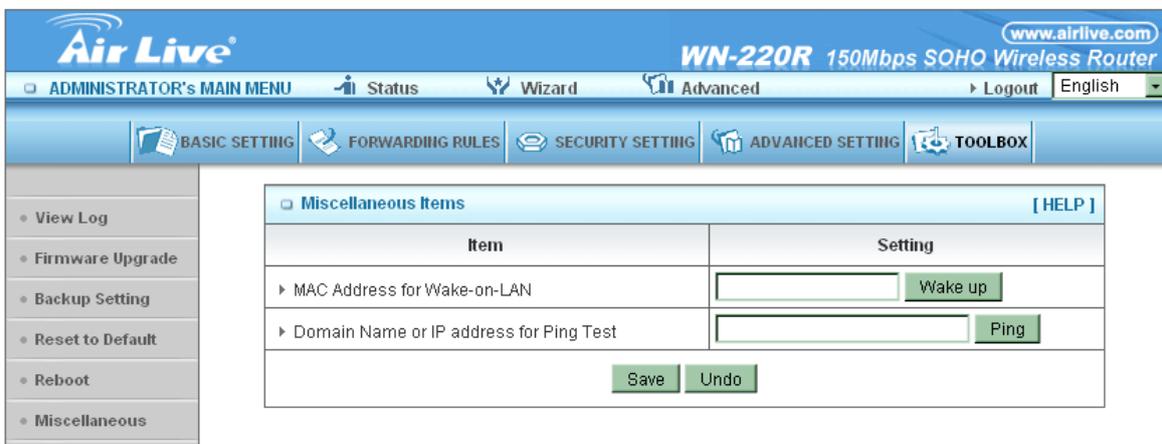
You can also reset this product to factory default by clicking the **Reset to default** button.

3.3.5.5 Reboot



You can also reboot this product by clicking the **Reboot** button.

3.3.5.6 Miscellaneous Items



- **MAC Address for Wake-on-LAN**

Wake-on-LAN is a technology that enables you to power up a networked device remotely. In order to enjoy this feature, the target device must be Wake-on-LAN enabled and you have to know the MAC address of this device, say 00-11-22-33-44-55. Clicking "Wake up" button will make the router to send the wake-up frame to the target device immediately.

- **Domain Name or IP Address for Test**

Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

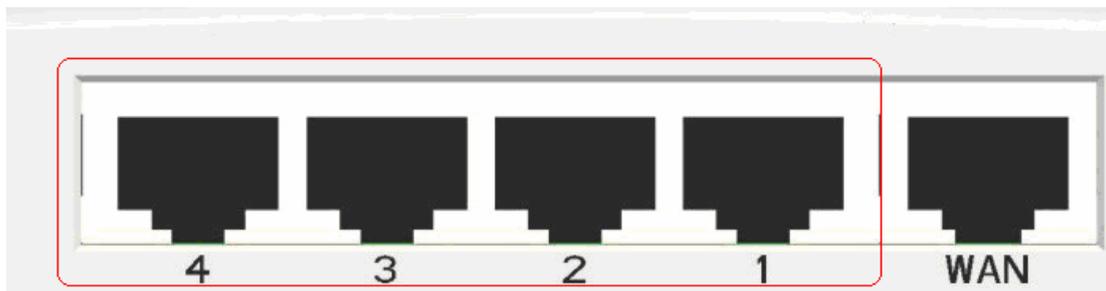


Appendix: FAQ and Troubleshooting

What can I do when I have some trouble at the first time?

1. Why can I not configure the router even if the cable is plugged in the ports of Router and the led is also light?

A: First, make sure that which port is plugged. If the cable is in the WAN port, please change to plug in LAN port 1 or LAN port 4:



Then, please check if the Pc gets ip address from Router. Use command mode as below:

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.123.115
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.123.254
```

If yes, please execute Browser, like Mozilla and key 192.168.123.254 in address.

If not, please ipconfig /release, then ipconfig /renew.

```
C:\>ipconfig /release

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 0.0.0.0
    Subnet Mask . . . . .             : 0.0.0.0
    Default Gateway . . . . .         : 

C:\>ipconfig /renew

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.123.115
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.123.254
```

Whatever I setup, the pc can not get IP. Please check Status Led and refer to the Q2.



2. Why can I not connect the router even if the cable is plugged in LAN port and the led is light?

A: First, please check Status Led. If the device is normal, the led will blink per second.

If not, please check how blinking Status led shows.

There are many abnormal symptoms as below:

Status Led is bright or dark in work: The system hanged up .Suggest powering off and on the router. But this symptom often occurs, please reset to default or upgrade latest FW to try again.

Status led flashes irregularly: Maybe the root cause is Flash and please press reset Button to reset to default or try to use Recovery mode.(Refer to Q3 and Q4)

Status flashes very fast while powering on: Maybe the router is the recovery mode and please refer to Q4.

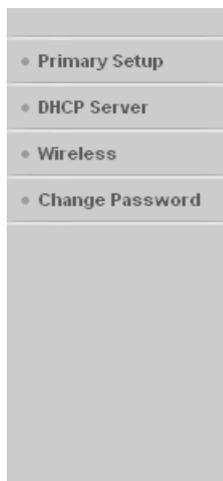
3. How to reset to factory default?

A: Press Wireless on /off and WPS button simultaneously about 5 sec

Status will start flashing about 5 times, remove the finger. The RESTORE process is completed.

4. Why can I not connect Internet even though the cables are plugged in WAN port and LAN port and the LEDs are blink? In addition, Status led is also normal and I can configure web management?

A: Make sure that the network cable from DSL or Cable modem is plugged in WAN port of Router and that the network cable from LAN port of router is plugged in Ethernet adapter. Then, please check which wan type you use. If you are not sure, please call the ISP. Then please go to this page to input the information ISP is assigned.



Choose WAN Type	
Type	Usage
<input type="radio"/> Static IP Address	ISP assigns you a static IP address.
<input checked="" type="radio"/> Dynamic IP Address	Obtain an IP address from ISP automatically.
<input type="radio"/> Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond)	
<input type="radio"/> PPP over Ethernet	Some ISPs require the use of PPPoE to connect to their services.
<input type="radio"/> PPTP	Some ISPs require the use of PPTP to connect to their services.
<input type="radio"/> L2TP	Some ISPs require the use of L2TP to connect to their services.
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	



5. When I use Static IP Address to roam Internet, I can access or ping global IP 202.93.91.218, but I can not access the site that inputs domain name, for example <http://espn.com> ?

A: Please check the dns configuration of Static IP Address. Please refer to the information of ISP and assign one or two in dns item.

How do I connect router by using wireless?

1. How to start to use wireless?

A: First, make sure that you already installed wireless client device in your computer. Then check the Configuration of wireless router. The default is as below:

Wireless Setting [HELP]	
Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Schedule Rule#	(01)333 <input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network ID(SSID)	airlive
Wireless Mode	<input checked="" type="radio"/> b+g+n <input type="radio"/> 11g only <input type="radio"/> 11b only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	11
WDS	Enter...
WPS	Enter...
Security	None

Save Undo Wireless Client List...

About wireless client, you will see wireless icon:



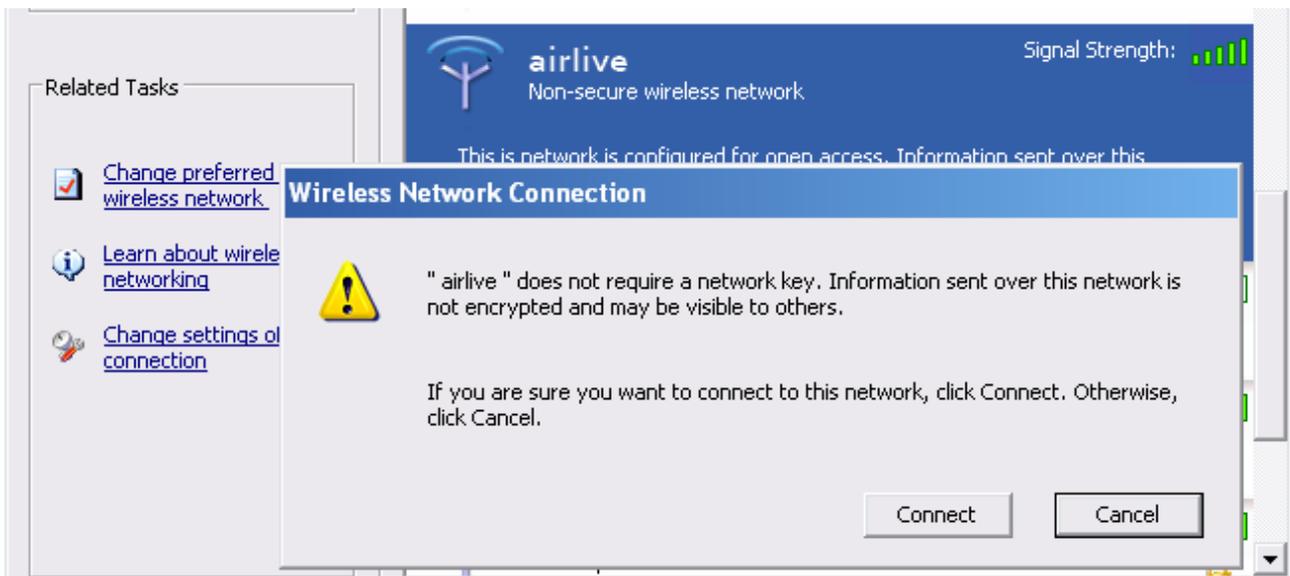
Then click and will see the AP list that wireless client can be accessed:



If the client can not access your wireless router, please refresh network list again. However, I still can not find the device which SSID is "airlive", please refer to Q3.



Choose the one that you will want to connect:



If successfully, the computer will show



And get IP from router:

```

Ethernet adapter Wireless Network Connection 5:

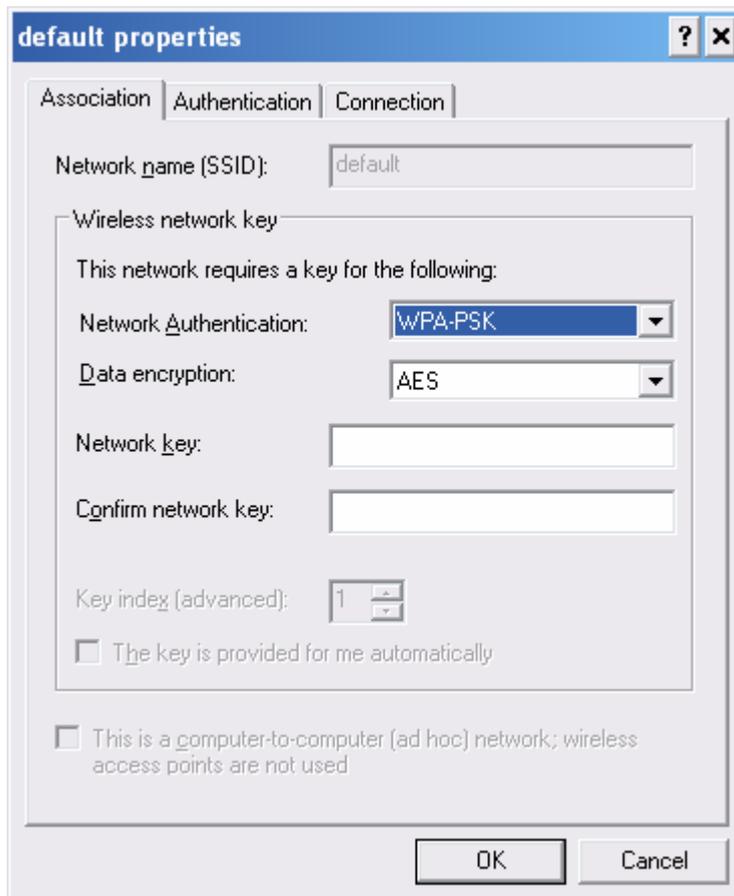
    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.123.165
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.123.254
    
```

2. When I use AES encryption of WPA-PSK to connect even if I input the correct pre-share key?

A: First, you must check if the driver of wireless client supports AES encryption. Please refer to the below:



If SSID is default and click “Properties” to check if the driver of wireless client supports AES encryption.



3. When I use wireless to connect the router, but I find the signal is very low even if I am close to the router?

A: Please check if the wireless client is normal, first. If yes, please send the unit to the seller and verify what the problem is.