



Traveler 3G II

11n 3G Mobile 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.

Regulatory Information

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: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices) 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.

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.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC NOTICE: To comply with FCC part 15 rules in the United States, the system must be professionally installed to ensure compliance with the Part 15 certification. It is the responsibility of the operator and professional installer to ensure that only certified systems are deployed in the United States. The use of the system in any other combination (such as co-located antennas transmitting the same information) is expressly forbidden.



© 2009 OvisLink Corporation, All Rights Reserved

Table of Contents

1. Introduction.....	2
1.1 Package Contents	2
1.2 System Requirements for Configuration	3
1.3 Interfaces.....	3
1.4 Features	6
2. Configuring Wireless WAN Mobile Broadband Router	9
2.1 Installation Considerations	9
2.2 Installation Instructions- Get Start Networking.....	9
2.3 Establish WiFi Connection	13
3. Using the Configuration Menu.....	14
3.1 Wizard setting.....	15
3.2 Administrator's Main Menu.....	25
3.2.1 Basic Setting	25
3.2.2 Forwarding Rules.....	50
3.2.3 Security Setting	56
3.2.4 Advanced Setting	68
3.2.5 Tool Box.....	84
4. Troubleshooting	87
5. Technical Specifications	93

1

Introduction

The Traveler 3G II is a high-performance tool that supports wireless networking at home, work, or in a public place. The Traveler 3G II supports USB 3G modem card, either WCDMA or EVDO and even HSDPA as well. It also supports 802.11n Wi-Fi standard and 802.3 Ethernet network.

The Traveler 3G II is compatible with industry security features.

1.1 Package Contents

Importance: Check your product package contents FIRST.

The Traveler 3G II package should contain the items listed below. If any of the items are missing, please contact your reseller.

items	Description	Quantity
1	Traveler 3G II	1
2	Power adapter 5V 2A	1
3	Li-ion Battery	1
4	CD	1
5	Leather case	1
6	RJ-45 Cable	1

Caution: Using a power supply with a different voltage rating than the one included with the Traveler 3G II will cause damage and void the warranty for this product.

1.2 System Requirements for Configuration

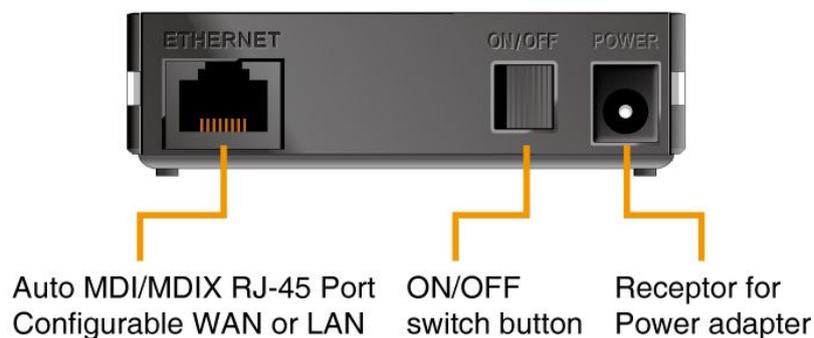
- A compatible USB 3G modem card with service

Note: Subject to services and service terms available from your carrier.

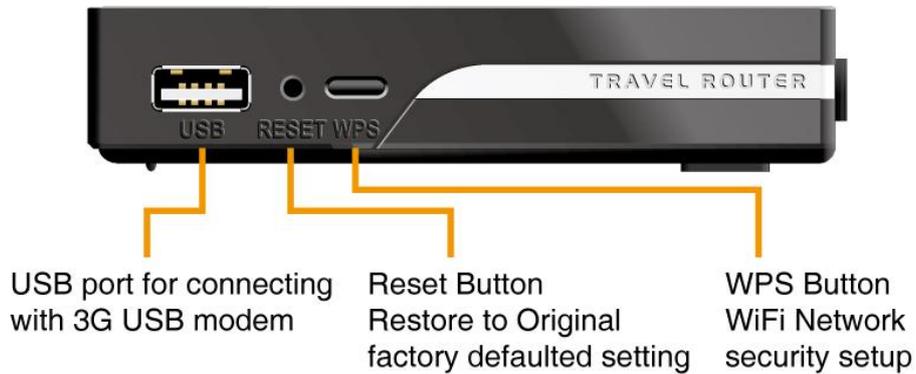
- Computers with Windows, Macintosh, or Linux-based operating systems with an installed Ethernet adapter
- Internet Explorer version 6.0 or Netscape Navigator version 7.0 and above.
- Wi-Fi System Requirements: An 802.11b, 802.11g, or 802.11n Adapter.

1.3 Interfaces

The Rear View



The Side View



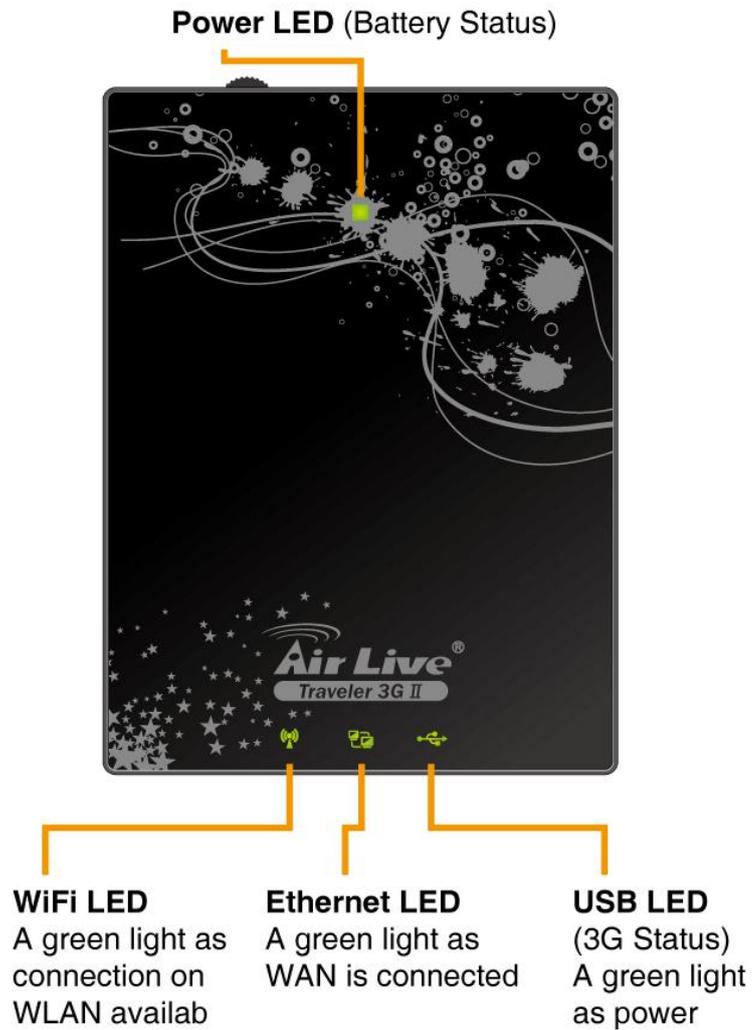
NOTE:

Press the reset button 3 seconds: the LEDs (WiFi and USB) will flash 2 times, and Ethernet port be resented to LAN.

Press the reset button 8 seconds: the LEDs (WiFi and USB) will flash 3 times, and restore the setting back to original factory defaulted setting as if your convenience of forgetting your applicable setting

Press the WPS button enables user to establish a wireless home network easily under secure environment between two clients.

LEDs– The Top View



■ Power LED: (and Battery Status)

When device is on and with battery inside

- Green: power adapter is plugged, and battery is fully charged
- Green in flash: power is provided by battery
- Amber: power adapter is plugged, and charging the battery
- Red: battery low

When device is on and without battery inside

- Amber: power adapter or CLA is plugged

When device is off and with battery inside

- Amber: power adapter is plugged, and charging the battery
- NA: power adapter is plugged, and battery charging finished
- NA: no power adapter is plugged

When device is off and without battery inside

- NA: no matter power adapter or CLA is plugged or not.

■ Ethernet LED:

- Green: Ethernet connection is established
- Green in flash: data packet transferred via Ethernet

■ USB LED: (WAN)

- Green: 3G/3.5G connection is established
- Green in flash: data packet transferred via 3G/3.5G connection

■ WiFi LED:

- Green: WLAN is active and available
- Green in flash: data packet transferred via WLAN

1.4 Features

■ IEEE 802.11b/g compliant

- Backward compatible to IEEE 802.11b standards
- Max physical rate up to 54Mbps in 802.11g mode
- Security Supports: WEP (64/128 bits), WPA, WPA2, WPA-PSK, WPA2-PSK, and 802.1x

- Provide 1 * 10/100 RJ-45 port
 - LAN or WAN (Configurable)
- WAN connection through external USB 3G/3.5G modem card
- WAN connection through 3G tethered-data-enabled cell phone
- WAN connection through Ethernet
 - Dynamic IP (DHCP Client)
 - Static IP
 - PPPoE
 - PPTP
 - L2TP
- PPTP over 3G WAN connection
- Built-in NAT function: one IP sharing with PCs
- Built-in firewall to protect your Intranet
- VPN pass through supported
 - PPTP
 - L2TP
 - IPSec
- Easy to upgrade firmware
 - Web UI
 - Windows utility
- Easy to manage:
 - Web UI
 - SNMP
 - UPnP
- L3/L4 QoS
- Network Protocols
 - UDP/TCP/IP/ARP/RARP/ICMP
 - DHCP/PPPoE
 - DNS/TFTP/HTTP



- Antenna
 - 1 x Internal Wi-Fi antenna
- Continue working 100 minutes with built-in Li-Ion battery (1700mAh)

Note: The Traveler 3G II is designed to work with either EVDO or WCDMA (UMTS) even up to 3.5G HSPA PC interface.

Please refer to your service provider for detailed feature information

2

Configuring Wireless WAN Mobile Broadband Router

2.1 Installation Considerations

The Traveler 3G II allows you access your network using a wireless connection, from virtually anywhere within its operating range. Keep in mind, however, the number, thickness, and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit this range.

Typical ranges are vary depending on the types of materials used, and background RF (radio frequency) noise in your home or business.

To maximize your wireless range, please follow these guidelines:

1. Keep the number of walls and ceilings between the Traveler 3G II and other network devices to a minimum. Each wall or ceiling can reduce the Traveler 3G II's range from 3-90 feet (1-30 meters).

Note: The same considerations apply to your broadband EVDO connection.

2. Keep your product away from electrical devices (such as microwaves, air conditioners, and televisions) that emit large quantities of RFI (Radio Frequency Interference).

2.2 Installation Instructions- Get Start Networking

Connect the Traveler 3G II to Your Network, please follow these guidelines:

Note: DO NOT switch on Traveler 3G II before performing the installation steps below.

1. Turn off the power switch.
2. Attach the Li-ion battery, and then insert the battery into battery holder. ---picture 2.1



Picture 2.1

3. Connect a USB modem with service to the in one of the following ways:
 - You can plug your USB 3G modem into the USB interface. ---see Picture 2.2



Picture 2.2

Note: The Traveler 3G II is designed to work with either UMTS or EV-DO and even HSDPA 3G card that can be used as a modem. Please refer to your service provider for detailed feature information.

4. Insert the Ethernet patch cable into Ethernet Port on the back panel of the Traveler 3G II, and an available Ethernet port on the network adapter in the computer you will use to configure the unit.-see Picture 2.3



Picture 2.3

Note: The Traveler 3G II Ethernet Port is “Auto-MDI/MDIX.” This provides patch Ethernet cable Ethernet Port access.

5. Connect the power adapter to the receptor on the back panel of your Traveler 3G II. Then plug the other end of the power adapter into a wall outlet or power strip. ---Picture 2.4



Picture 2.4

6. Turn on the power switch.
7. The LEDs (See Picture 2.5)
 - a. The Power LED will turn ON to indicate power has been applied.
 - b. Reference the Section 1.4, LEDs– the Top View.



Picture 2.5

2.3 Establish WiFi Connection

If you selected either WEP or WPA-PSK encryption, ensure these settings match your WiFi adapter settings.

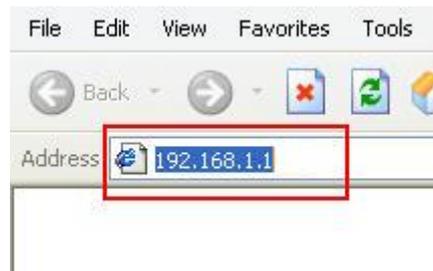
WiFi and encryption settings must match for access to the HSPA Wireless WAN Mobile Broadband Router Configuration Menu, and the Internet. Please refer to your WiFi adapter documentation for additional information.

3

Using the Configuration Menu

Once properly configured, the Traveler 3G II will obtain and assign IP address information automatically. Configuration settings can be established through the Traveler 3G II Configuration Menu. You can access this interface by performing the steps listed below:

1. Open a web-browser.
2. Type in the IP Address (http://192.168.1.1) of the Traveler 3G II .



Note: If you have changed the **default** IP Address assigned to the Traveler 3G II, ensure you enter the correct IP Address now.

3. Type "airlive" in the Password field.



www.airlive.com
11n 3G Mobile Router

USER's MAIN MENU Status

System Password: (default: airlive) Login

System Status [Help]

Item	WAN Status	Sidenote
Remaining Lease Time	-	
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0, 0.0.0.0	

Wireless Modem Information

Item	Status	Sidenote
Card Info	209	Supported Cards List
Link Status	Connected.	
Signal Strength	41%	
Network Name	Chunghwa Telecom	

Wireless Status

Item	WLAN Status	Sidenote
Wireless mode	Enable	(BIG/N Mixed)
SSID	LU3Gv2	
Channel	1	
Security	WPA2-PSK	(TKIP)

Statistics Information

Statistics of WAN	Inbound	Outbound
Octets	0	0
Unicast packets	0	0
Multicast packets	0	0

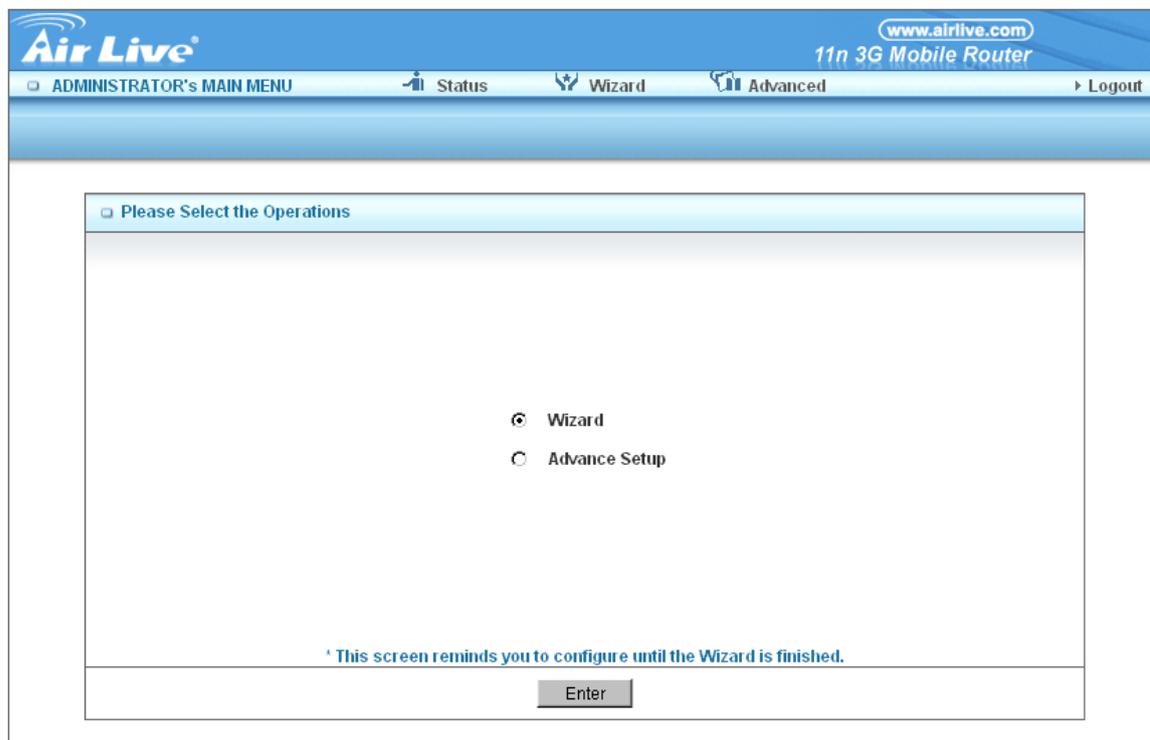
Refresh

Device Time: Fri, 01 Jan 2010 08:37:26 +0800

4. Click "login" button.

3.1 Wizard setting

- Press "Wizard" button → for basic settings with simpler way. (Please check section 3.1)
- Or you may click on "Advanced Setup" → for advanced settings. (Please check the section Administrator's Main Menu. Each item from section 3.2)

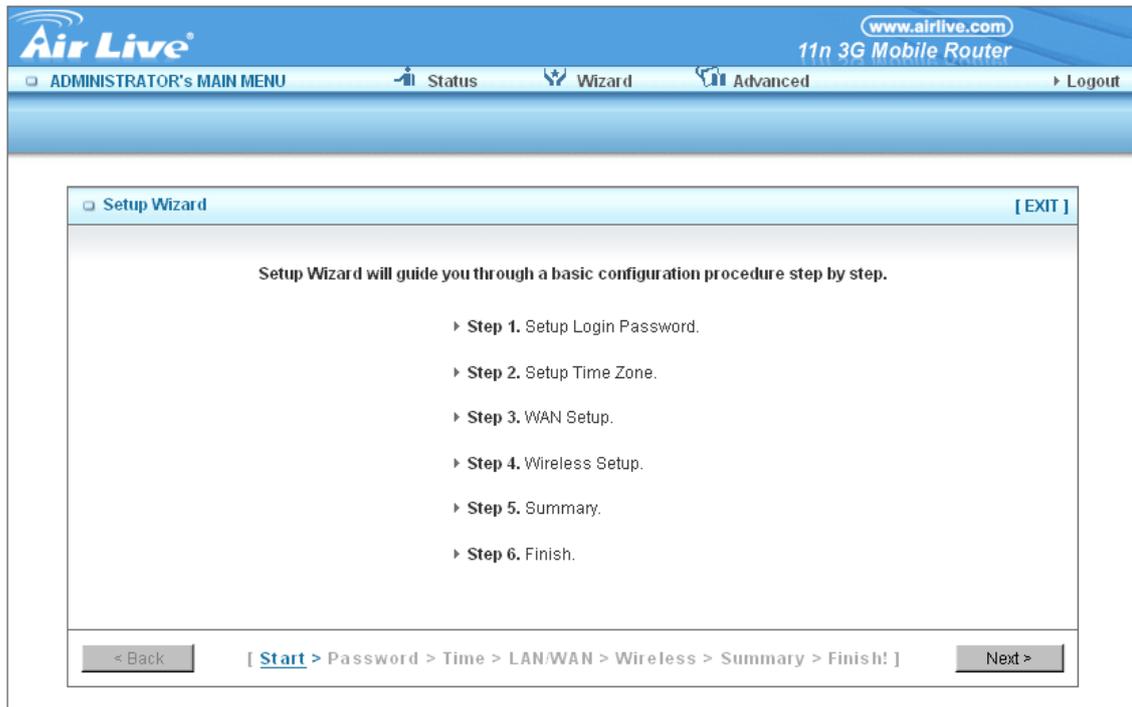


- Click on “Enter” button to get start.

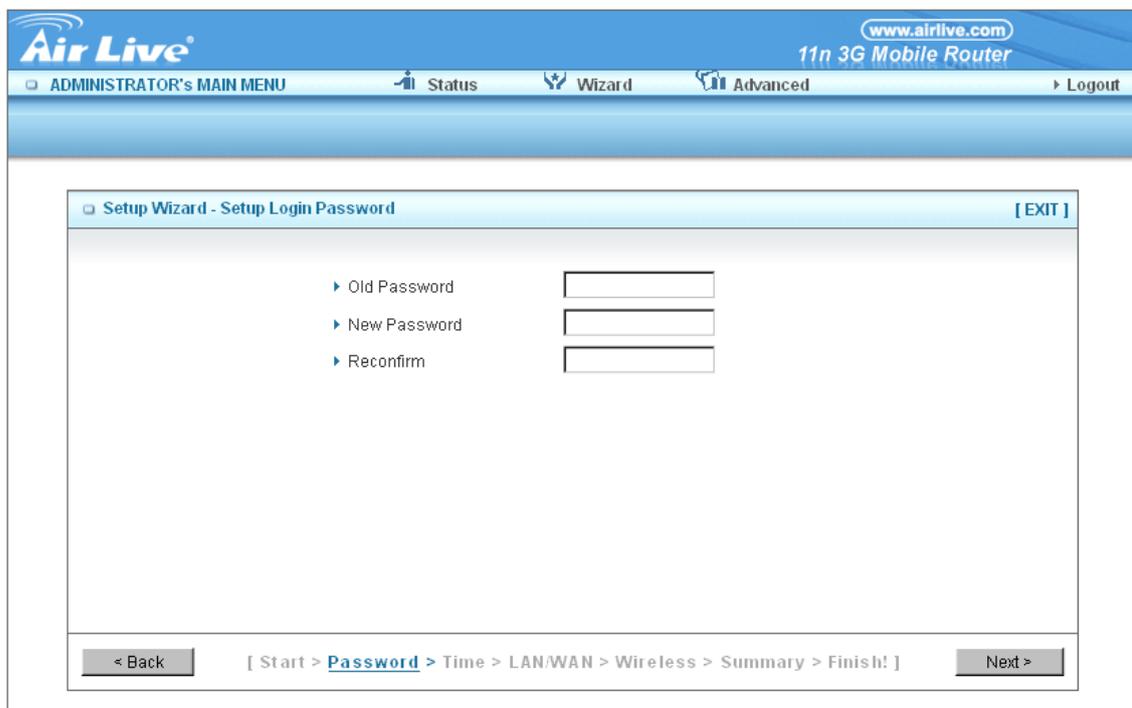
With wizard setting steps, you could configure the router in a very simple way. This configuration wizard includes settings of

- Login Password,
- Time Zone,
- WAN Setup
- Wireless Setup,

Press “**Next**” button to start configuration.



Step 1. Allow you to change the system password.

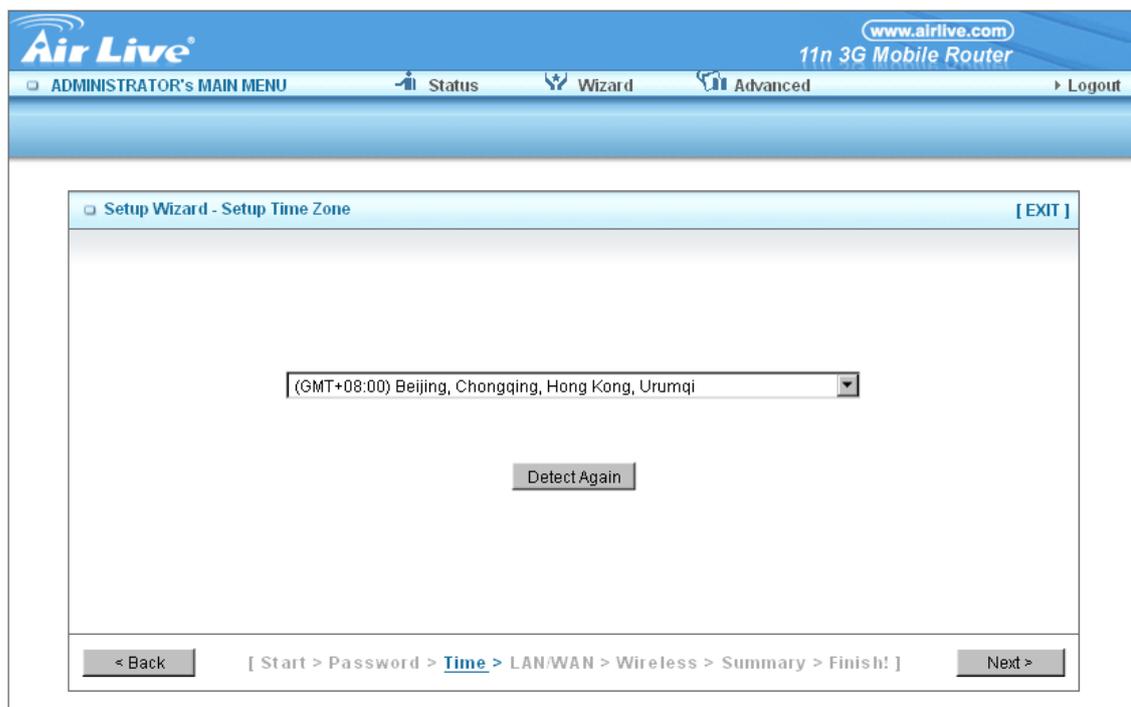


You can change Password here.

It is recommended that you change the system password into the one you prefer to on the basis of security.

1. Key in your Old Password (if it is the first initiation, the “airlive” will be the defaulted one.
2. Enter your New Password
3. Enter your Password again for confirmation; it must be the same as the New Password.
4. Then click on “Next” to get into next installation.

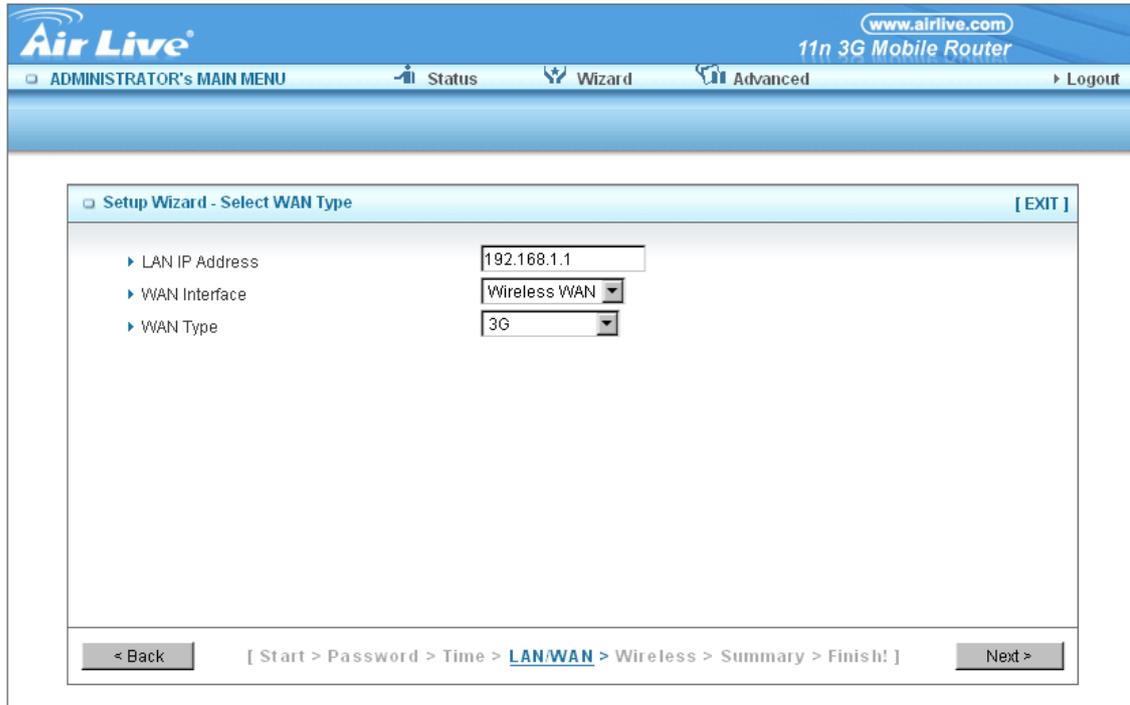
Step 2. Allow you to change the Time Zone.



You can change Time Zone here.

Or you can click the button “Detect Again”, the Time Zone will be changed to same with your PC.

Step 3. Select WAN Types will be used for Internet connection



The screenshot displays the 'Setup Wizard - Select WAN Type' configuration page. The page header includes the 'Air Live' logo and the model '11n 3G Mobile Router'. The navigation menu contains 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main configuration area lists three items: 'LAN IP Address' (192.168.1.1), 'WAN Interface' (Wireless WAN), and 'WAN Type' (3G). A progress bar at the bottom shows the current step as 'LAN/WAN' in a sequence: Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!.

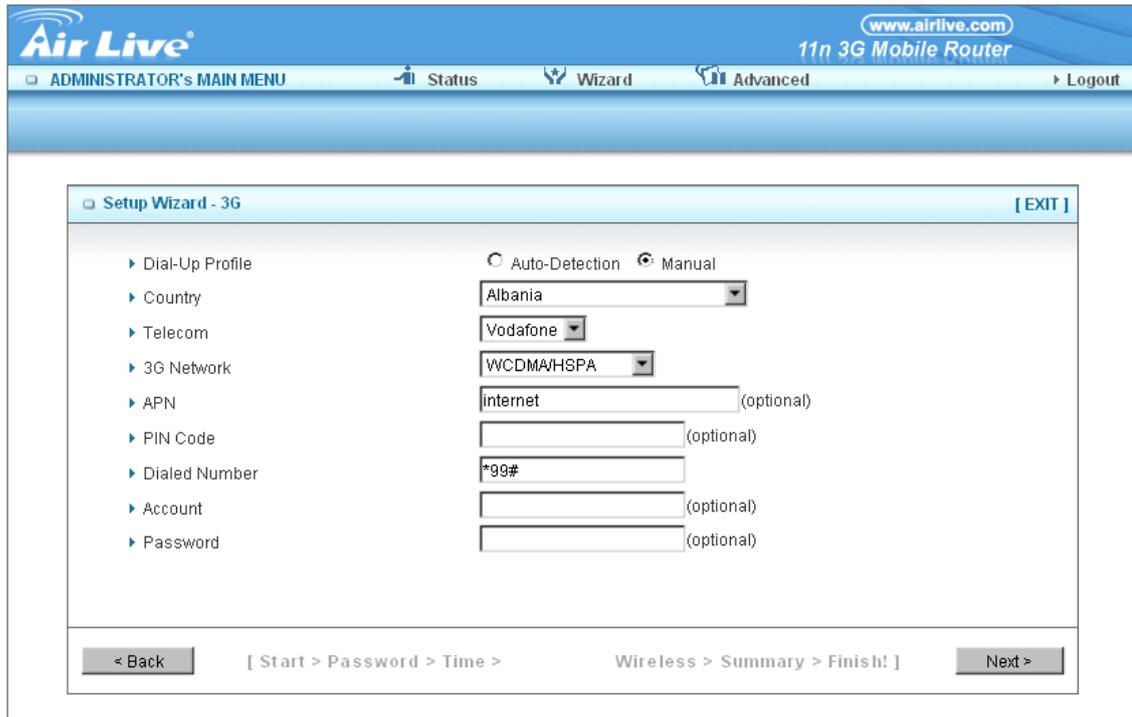
Please select the WAN Interface to Wireless WAN, and you might select the 3G, iBurst, or Wi-Fi HotSpot as your WAN Types. This guide will help you to connect your WAN to 3G mobile network.

The Ethernet Port will be set as LAN port, if you select the WAN Interface to Wireless WAN.

Pick up one of types you preferred to.

Click on “**Next**” button

Step 4. Configure the 3G Connection.



The screenshot shows the 'Setup Wizard - 3G' configuration page for the Air Live 11n 3G Mobile Router. The page has a blue header with the Air Live logo, the website URL 'www.airlive.com', and the device name '11n 3G Mobile Router'. Below the header is a navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout' options. The main content area is titled 'Setup Wizard - 3G' and includes an '[EXIT]' link. On the left, there is a list of configuration steps: Dial-Up Profile, Country, Telecom, 3G Network, APN, PIN Code, Dialed Number, Account, and Password. On the right, there are radio buttons for 'Auto-Detection' (unselected) and 'Manual' (selected). Below these are several dropdown menus and text input fields: 'Country' (Albania), 'Telecom' (Vodafone), '3G Network' (WCDMA/HSPA), 'APN' (internet), 'PIN Code' (empty), 'Dialed Number' (*99#), 'Account' (empty), and 'Password' (empty). At the bottom, there are navigation buttons: '< Back', '[Start > Password > Time > Wireless > Summary > Finish!]', and 'Next >'.

You might configure the 3G dial-up parameters manually. But if you are not sure, we highly recommend you to use Auto-Detection instead.

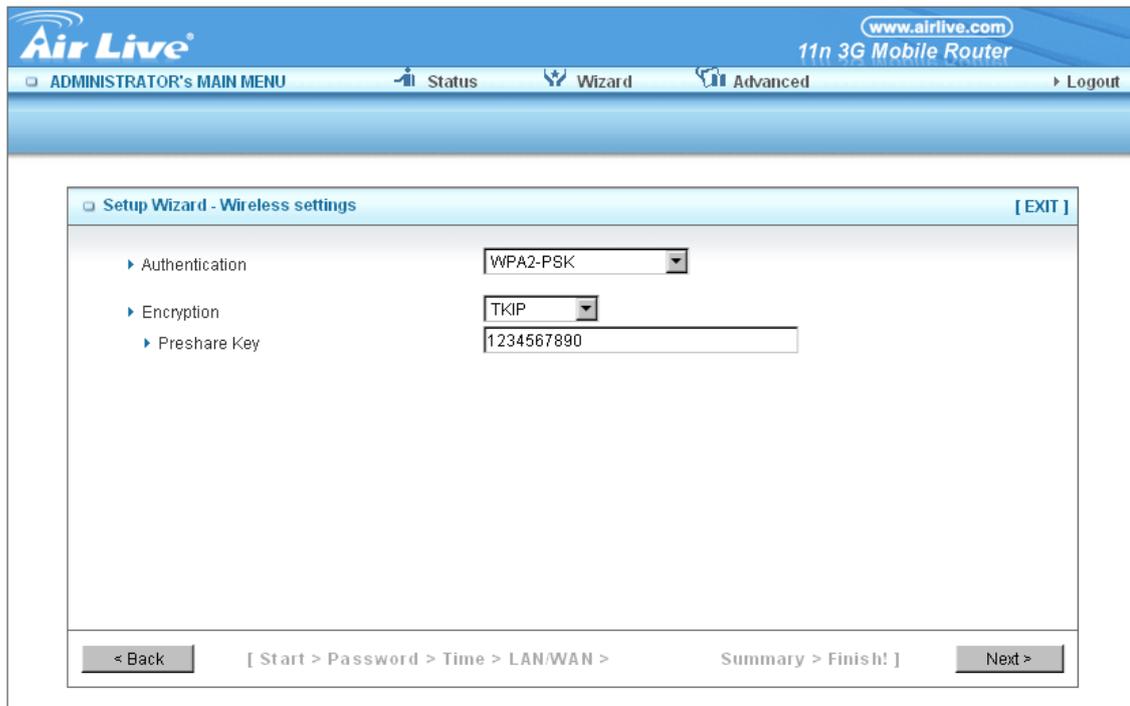
Step 5. Configure the wireless settings.



The screenshot shows the 'Setup Wizard - Wireless settings' page of the Air Live 11n 3G Mobile Router. The page has a blue header with the Air Live logo, the website URL 'www.airlive.com', and the device name '11n 3G Mobile Router'. Below the header is a navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area is titled 'Setup Wizard - Wireless settings' and contains three sections: 'Wireless Module' with radio buttons for 'Enable' (selected) and 'Disable'; 'Network ID(SSID)' with a text input field containing 'airlive'; and 'Channel' with a dropdown menu showing '11'. At the bottom of the page, there is a navigation bar with '< Back', '[Start > Password > Time > LAN/WAN > Summary > Finish!]', and 'Next >' buttons.

1. Select “**Enable**” or “**Disable**”. The default setting is “Enable”.
2. Network ID (airlive) will be defaulted.
3. **Channel**→ Select Wireless Channel matching to your local area for Wireless connection.
4. Click on “**Next**” to continue.

Step 6. Step 6: Select the Wireless security method of your wireless configuration.



The screenshot shows the 'Setup Wizard - Wireless settings' page. The page has a blue header with the 'Air Live' logo and 'www.airlive.com' on the right. Below the header is a navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area is titled 'Setup Wizard - Wireless settings' and contains three sections: 'Authentication' with a dropdown menu set to 'WPA2-PSK', 'Encryption' with a dropdown menu set to 'TKIP', and 'Preshare Key' with a text input field containing '1234567890'. At the bottom of the page, there is a navigation bar with '< Back', '[Start > Password > Time > LAN/WAN >', 'Summary > Finish!]', and 'Next >' buttons.

Click on “**Next**” to continue.

Step 7. Summary



www.airlive.com
11n 3G Mobile Router

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

Setup Wizard - Summary [EXIT]

Please confirm the information below

[WAN Setting]	
WAN Type	3G
APN	internet
PIN Code	-
Dialed Number	*99#
Username	-
Password	*****

[Wireless Setting]	
Wireless	Enable
SSID	LU3Gv2
Channel	1
Authentication	WPA2-PSK
Encryption	TKIP
Preshare Key	tkiptkip

Do you want to proceed the network testing?

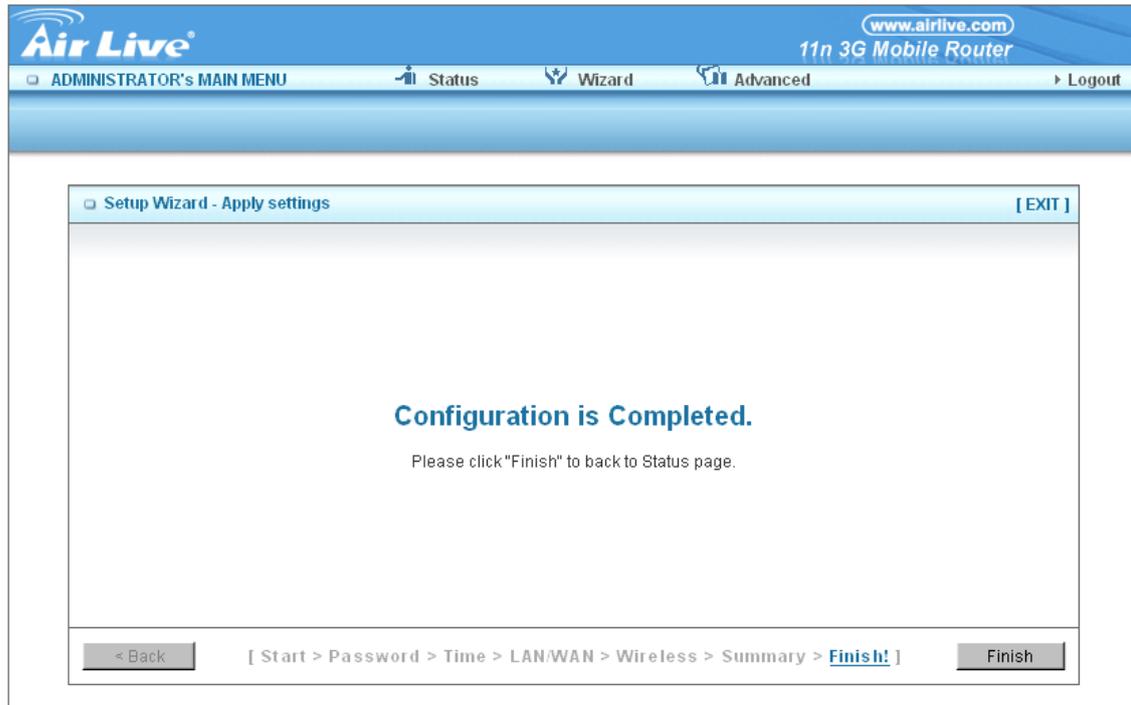
The Ethernet Port will be set as LAN Port after saving, confirm?

< Back [Start > Password > Time > LAN/WAN > Wireless > **Summary** > Finish!] Apply Settings

1. Select the option box “**The Ethernet Port will be set as LAN Port after saving, confirm?**” for continues.

Click on the “**Apply Settings**” button.

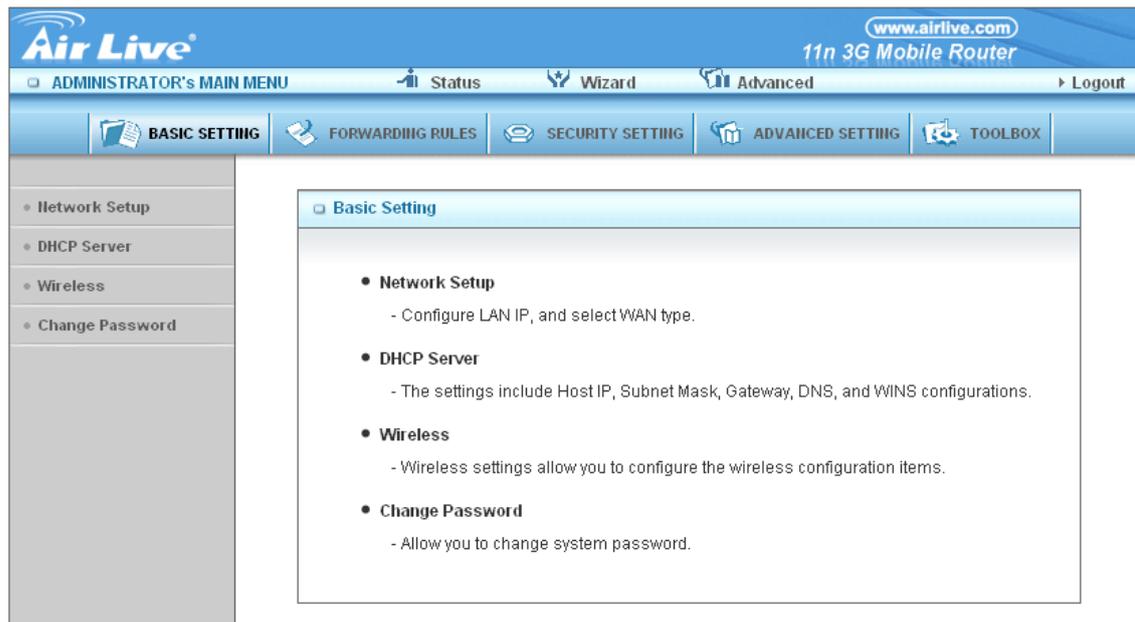
Step 8: System is applying.



Click **“Finish”** button to back the Status Page.

3.2 Administrator's Main Menu

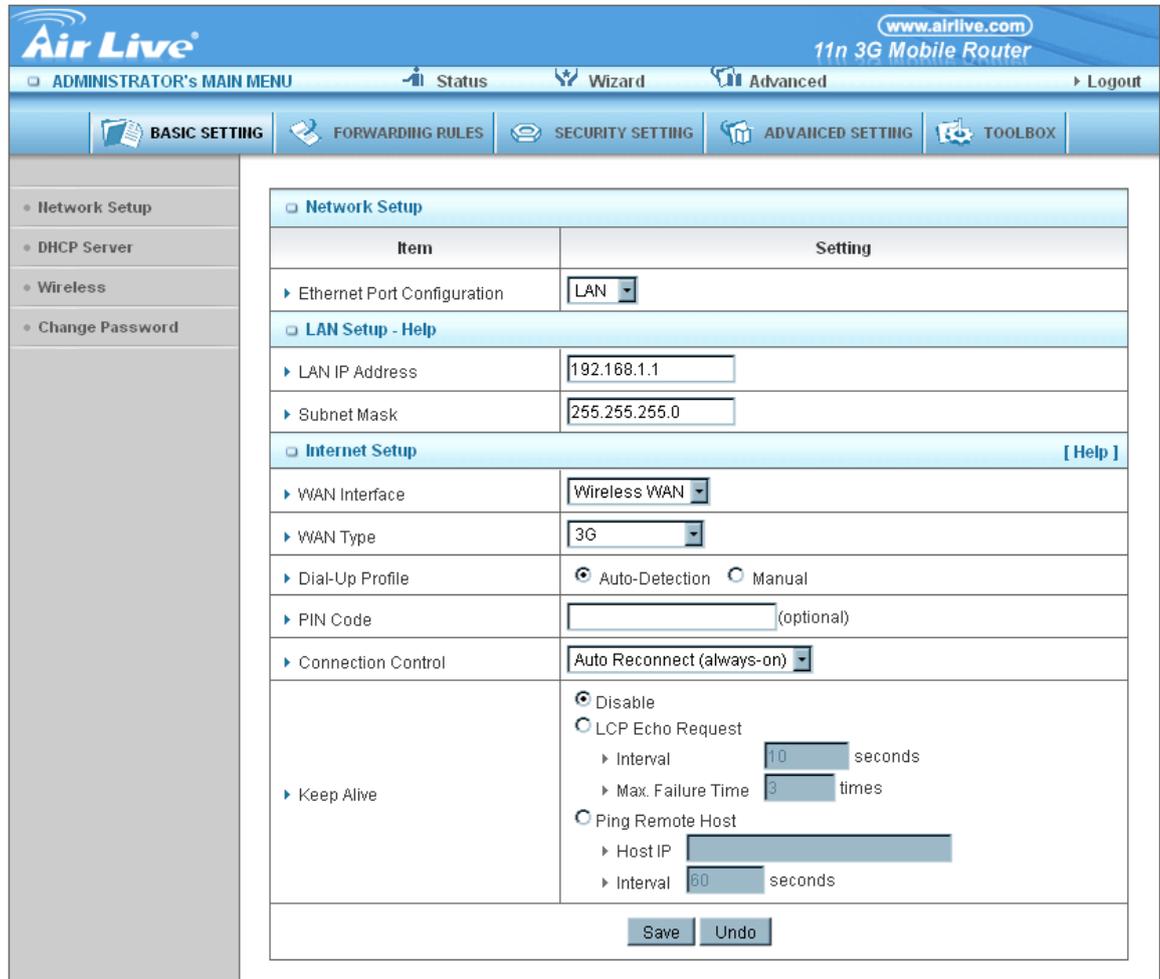
3.2.1 Basic Setting



The screenshot displays the web interface of the Air Live 11n 3G Mobile Router. The top navigation bar includes the Air Live logo, the website URL www.airlive.com, the device model "11n 3G Mobile Router", and a "Logout" button. Below this, a secondary menu contains "ADMINISTRATOR'S MAIN MENU", "Status", "Wizard", "Advanced", and "Logout". The main content area features a horizontal menu with "BASIC SETTING" (selected), "FORWARDING RULES", "SECURITY SETTING", "ADVANCED SETTING", and "TOOLBOX". On the left, a vertical sidebar lists "Network Setup", "DHCP Server", "Wireless", and "Change Password". The central pane, titled "Basic Setting", contains a bulleted list of options:

- **Network 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.

■ Network Setup



Item	Setting
▶ Ethernet Port Configuration	LAN
LAN Setup - Help	
▶ LAN IP Address	192.168.1.1
▶ Subnet Mask	255.255.255.0
Internet Setup [Help]	
▶ WAN Interface	Wireless WAN
▶ WAN Type	3G
▶ Dial-Up Profile	<input checked="" type="radio"/> Auto-Detection <input type="radio"/> Manual
▶ PIN Code	<input type="text"/> (optional)
▶ Connection Control	Auto Reconnect (always-on)
▶ Keep Alive	<input checked="" type="radio"/> Disable
	<input type="radio"/> LCP Echo Request
	▶ Interval <input type="text" value="10"/> seconds
	▶ Max. Failure Time <input type="text" value="3"/> times
	<input type="radio"/> Ping Remote Host
	▶ Interval <input type="text" value="60"/> seconds

Save Undo

1. Ethernet port Configuration:

Off: Disable the Ethernet port.

LAN: The Ethernet port is as LAN port.

WAN: The Ethernet port is as LAN port.

Auto: It will be WAN Port if detect a DHCP server on the Ethernet port.

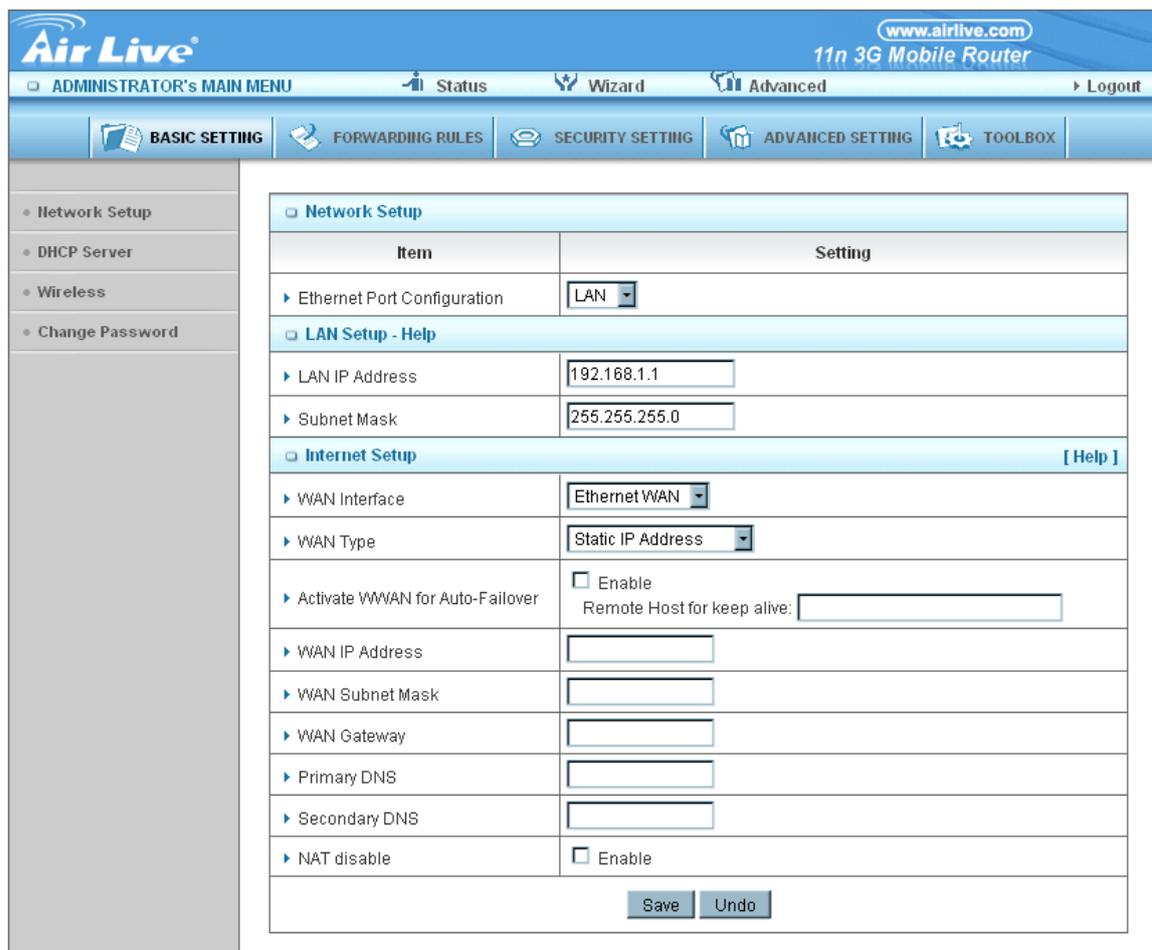
Otherwise will be LAN port.

- LAP 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.

3. **WAN Interface:** Select the WAN interface, whether use the wireless or wired (Ethernet WAN) as your WAN interface.
4. **WAN Type:** When wired WAN interface is selected, you might choose Static IP address, Dynamic IP address, PPPoE, PPTP or L2TP as your WAN connection. When wireless WAN interface is selected, you might choose 3G, iBurst or Wi-Fi HotSpot as your WAN connection.

- **Static IP Address:**

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

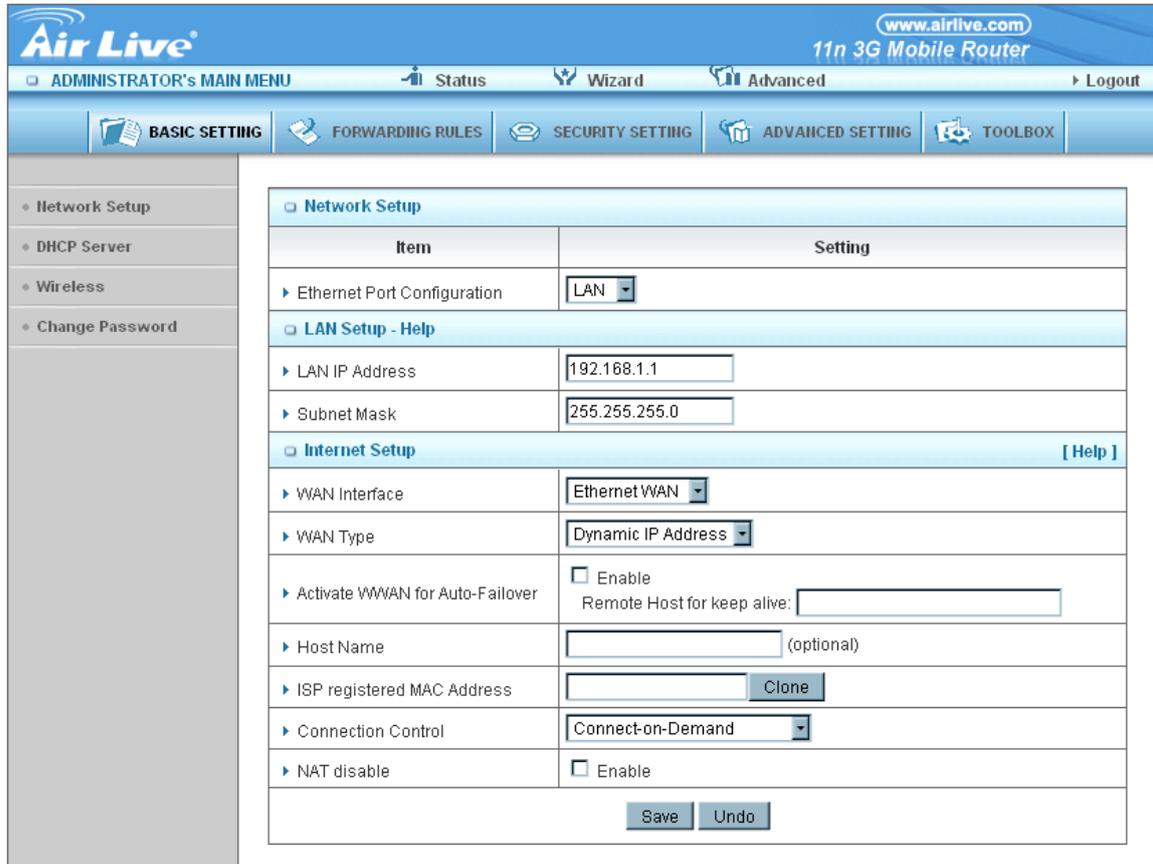


The screenshot shows the 'Network Setup' configuration page in the Air Live 11n 3G Mobile Router administrator interface. The page is divided into several sections: Network Setup, LAN Setup - Help, and Internet Setup. The 'Internet Setup' section is currently active and shows the following configuration options:

Item	Setting
▶ Ethernet Port Configuration	LAN
LAN Setup - Help	
▶ LAN IP Address	192.168.1.1
▶ Subnet Mask	255.255.255.0
Internet Setup [Help]	
▶ WAN Interface	Ethernet WAN
▶ WAN Type	Static IP Address
▶ Activate WWAN for Auto-Failover	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
▶ WAN IP Address	<input type="text"/>
▶ WAN Subnet Mask	<input type="text"/>
▶ WAN Gateway	<input type="text"/>
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ NAT disable	<input type="checkbox"/> Enable

At the bottom of the configuration area, there are 'Save' and 'Undo' buttons.

- **Dynamic IP Address:**



Item	Setting
▶ Ethernet Port Configuration	LAN
LAN Setup - Help	
▶ LAN IP Address	192.168.1.1
▶ Subnet Mask	255.255.255.0
Internet Setup [Help]	
▶ WAN Interface	Ethernet WAN
▶ WAN Type	Dynamic IP Address
▶ Activate WWAN for Auto-Failover	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
▶ Host Name	<input type="text"/> (optional)
▶ ISP registered MAC Address	<input type="text"/> Clone
▶ Connection Control	Connect-on-Demand
▶ NAT disable	<input type="checkbox"/> Enable

Save Undo

1. Host Name: optional, required by some ISPs, for example, @Home.

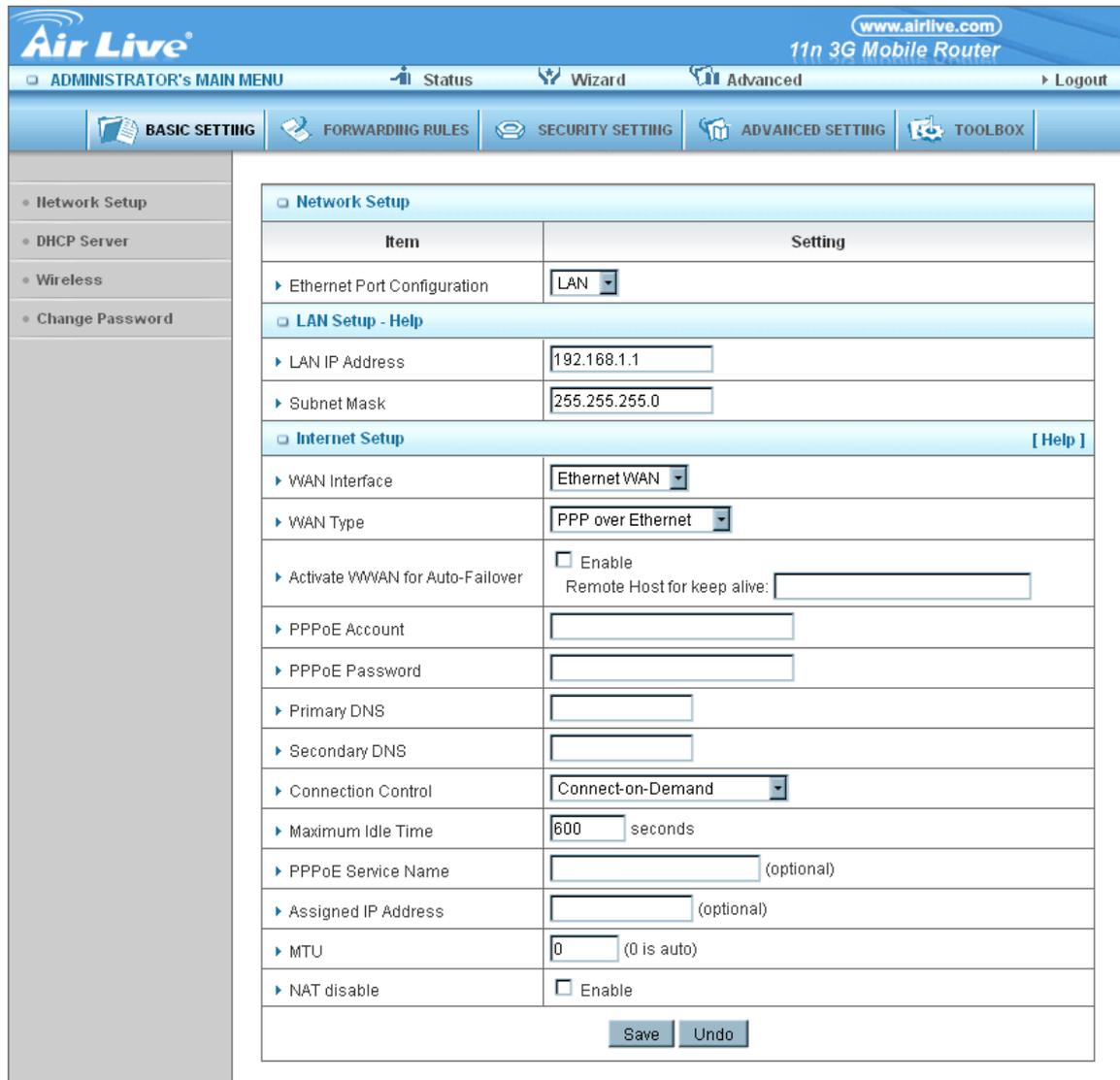
2. Connection Control: There are 3 modes to select:

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.

- **PPP over Ethernet**



The screenshot shows the configuration page for the Air Live 11n 3G Mobile Router. The interface includes a navigation menu with options like 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area is titled 'Network Setup' and contains a table of configuration items.

Item	Setting
▶ Ethernet Port Configuration	LAN
LAN Setup - Help	
▶ LAN IP Address	192.168.1.1
▶ Subnet Mask	255.255.255.0
Internet Setup [Help]	
▶ WAN Interface	Ethernet WAN
▶ WAN Type	PPP over Ethernet
▶ Activate WWAN for Auto-Failover	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
▶ PPPoE Account	<input type="text"/>
▶ PPPoE Password	<input type="text"/>
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ Connection Control	Connect-on-Demand
▶ Maximum Idle Time	600 seconds
▶ PPPoE Service Name	<input type="text"/> (optional)
▶ Assigned IP Address	<input type="text"/> (optional)
▶ MTU	0 (0 is auto)
▶ NAT disable	<input type="checkbox"/> Enable

At the bottom of the configuration table, there are 'Save' and 'Undo' buttons.

1. 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.

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

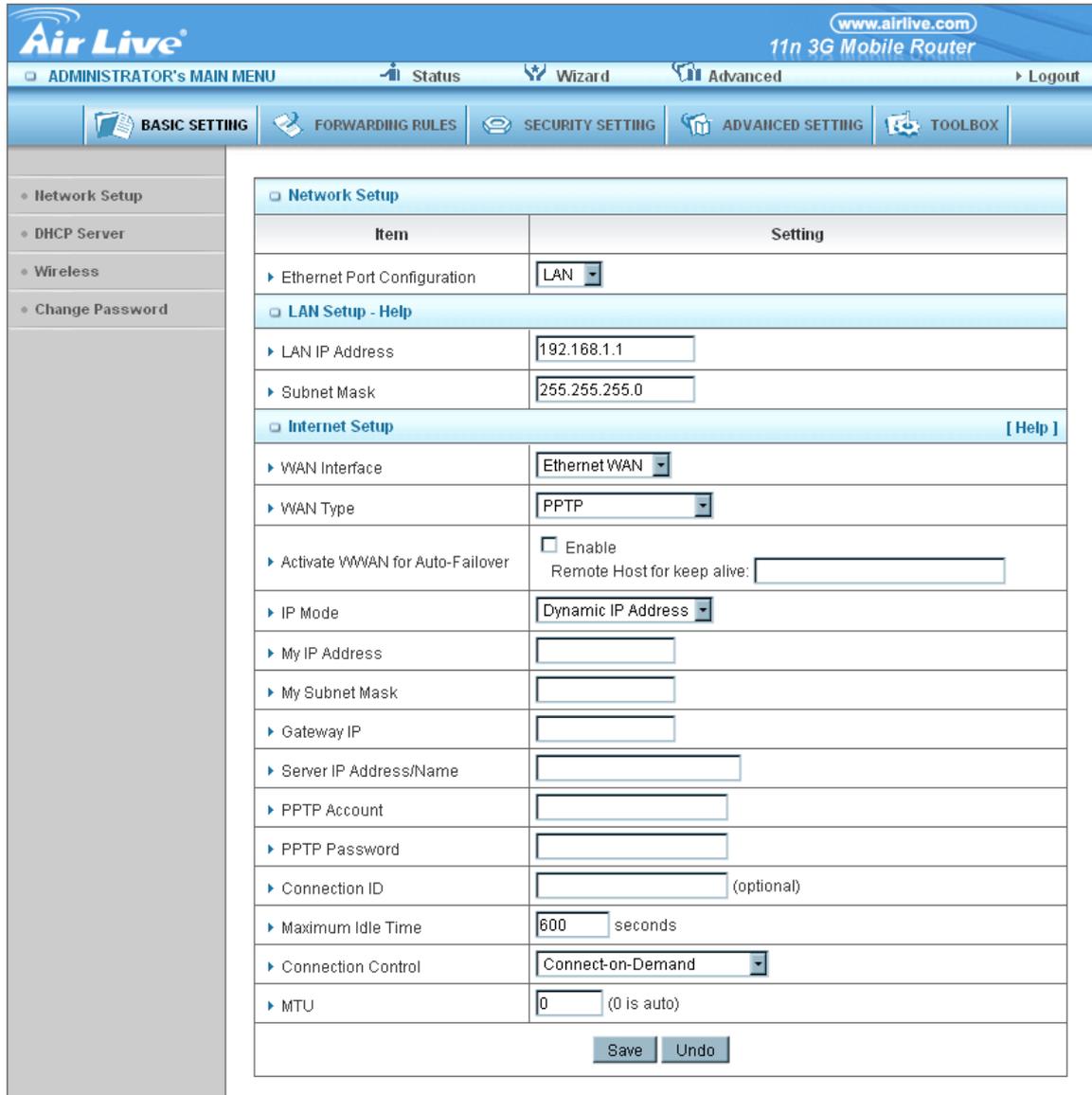
Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

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.

3. 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.
4. PPPoE Service Name: optional. Input the service name if your ISP requires it. Otherwise, leave it blank.
5. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The default MTU value is 0(auto).

- PPTP



The screenshot shows the 'Internet Setup' configuration page for a PPTP connection. The interface includes a navigation menu on the left and a main configuration area with various settings.

Item	Setting
▶ Ethernet Port Configuration	LAN
LAN Setup - Help	
▶ LAN IP Address	192.168.1.1
▶ Subnet Mask	255.255.255.0
Internet Setup [Help]	
▶ WAN Interface	Ethernet WAN
▶ WAN Type	PPTP
▶ Activate WWAN for Auto-Failover	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
▶ IP Mode	Dynamic IP Address
▶ My IP Address	<input type="text"/>
▶ My Subnet Mask	<input type="text"/>
▶ Gateway IP	<input type="text"/>
▶ Server IP Address/Name	<input type="text"/>
▶ PPTP Account	<input type="text"/>
▶ PPTP Password	<input type="text"/>
▶ Connection ID	<input type="text"/> (optional)
▶ Maximum Idle Time	600 seconds
▶ Connection Control	Connect-on-Demand
▶ MTU	0 (0 is auto)

Buttons: Save, Undo

First, please check your ISP assigned and Select Static IP Address or Dynamic IP Address. For example: Use Static, the private IP address, subnet mask and Gateway are your ISP assigned to you.

1. My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned to you.
2. Server IP Address: the IP address of the PPTP server.
3. 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.

4. Connection ID: optional. Input the connection ID if your ISP requires it.
5. 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.

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

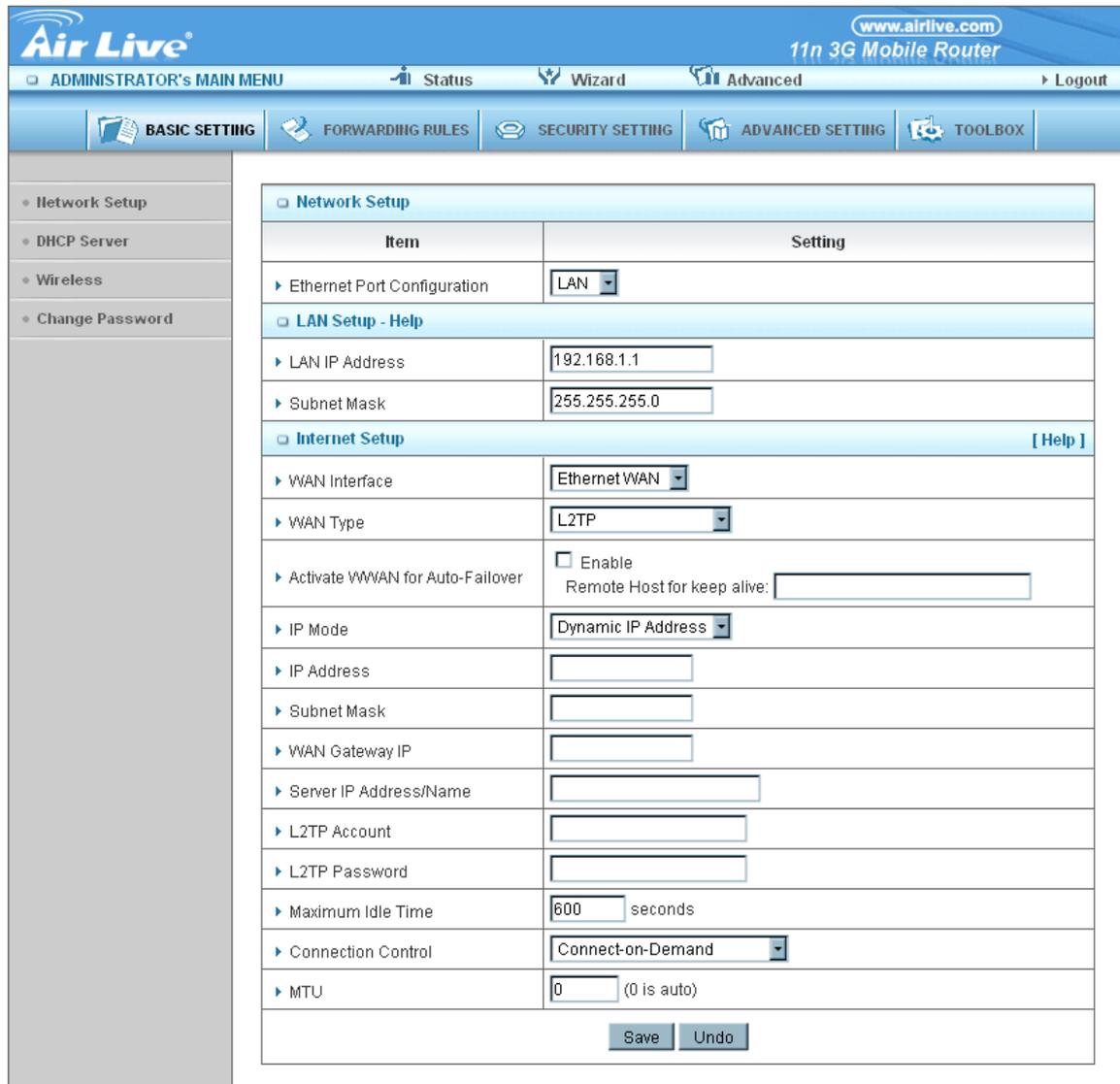
Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

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.

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

- **L2TP**



The screenshot shows the configuration interface for the Air Live 11n 3G Mobile Router. The 'Internet Setup' section is expanded, showing the following settings:

Item	Setting
Ethernet Port Configuration	LAN
LAN Setup - Help	
LAN IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Internet Setup [Help]	
WAN Interface	Ethernet WAN
WAN Type	L2TP
Activate WWAN for Auto-Failover	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
IP Mode	Dynamic IP Address
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
WAN Gateway IP	<input type="text"/>
Server IP Address/Name	<input type="text"/>
L2TP Account	<input type="text"/>
L2TP Password	<input type="text"/>
Maximum Idle Time	600 seconds
Connection Control	Connect-on-Demand
MTU	0 (0 is auto)

Buttons: Save, Undo

First, please check your ISP assigned and Select Static IP Address or Dynamic IP Address. For example: Use Static, the private IP address, subnet mask and Gateway are your ISP assigned to you.

1. My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned to you.
2. Server IP Address: the IP address of the L2TP server.
3. L2TP Account and Password: the account and password your ISP assigned to you. If you don't want to change the password, keep it

empty.

4. Connection ID: optional. Input the connection ID if your ISP requires it.
5. Maximum Idle Time: the time of no activity to disconnect your L2TP session. Set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will connect to ISP automatically, after system is restarted or connection is dropped.

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

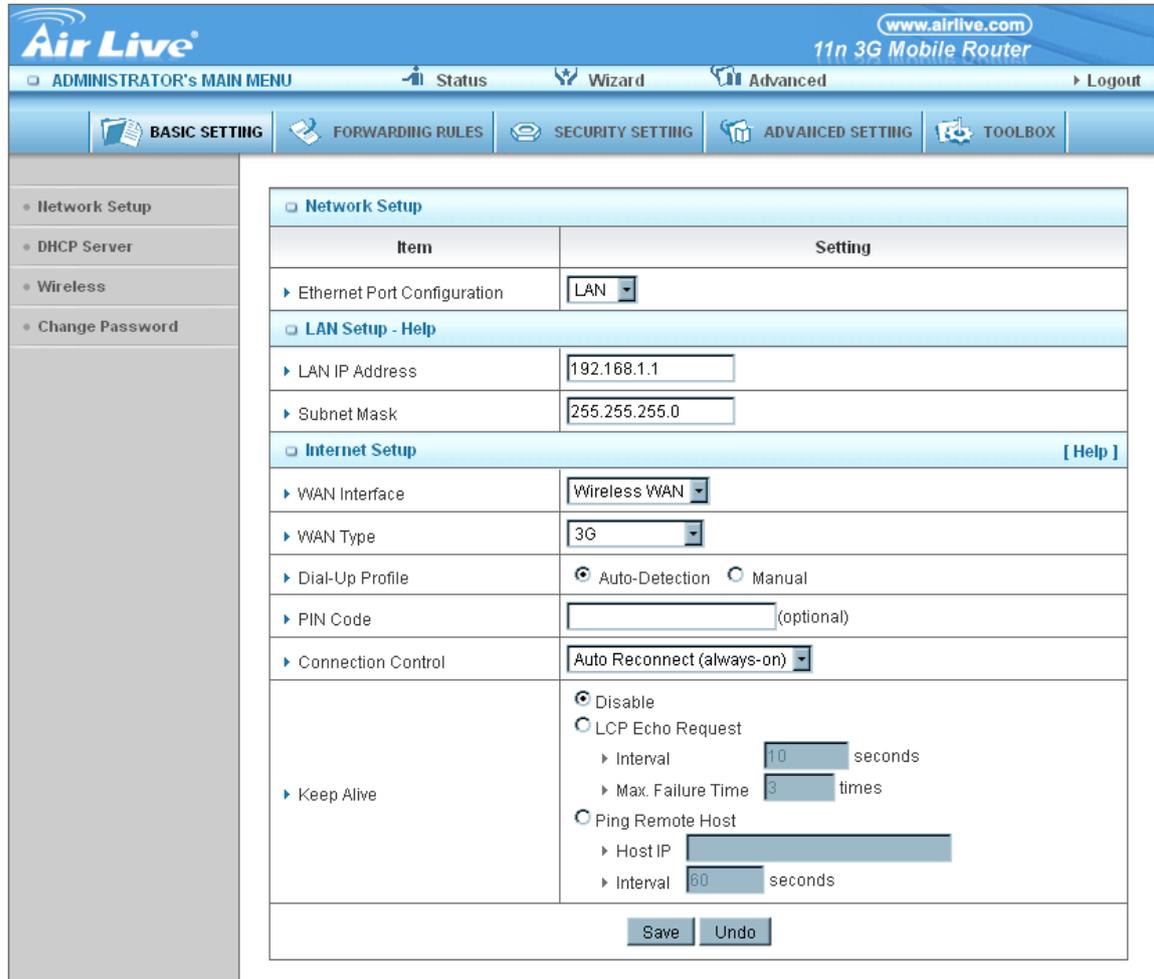
Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

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.

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

- 3G



The screenshot shows the 'Network Setup' configuration page in the Air Live web interface. The page is titled 'Air Live 11n 3G Mobile Router' and includes a navigation menu with options like 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main configuration area is divided into sections: 'Network Setup', 'LAN Setup - Help', and 'Internet Setup'. The 'Internet Setup' section is currently expanded, showing fields for 'WAN Interface' (Wireless WAN), 'WAN Type' (3G), 'Dial-Up Profile' (Auto-Detection), 'PIN Code' (optional), 'Connection Control' (Auto Reconnect (always-on)), and 'Keep Alive' options (Disable, LCP Echo Request, and Ping Remote Host).

Item	Setting
▶ Ethernet Port Configuration	LAN
LAN Setup - Help	
▶ LAN IP Address	192.168.1.1
▶ Subnet Mask	255.255.255.0
Internet Setup [Help]	
▶ WAN Interface	Wireless WAN
▶ WAN Type	3G
▶ Dial-Up Profile	<input checked="" type="radio"/> Auto-Detection <input type="radio"/> Manual
▶ PIN Code	<input type="text"/> (optional)
▶ Connection Control	Auto Reconnect (always-on)
▶ Keep Alive	<input checked="" type="radio"/> Disable
	<input type="radio"/> LCP Echo Request
	▶ Interval <input type="text" value="10"/> seconds
	▶ Max. Failure Time <input type="text" value="3"/> times
<input type="radio"/> Ping Remote Host	▶ Host IP <input type="text"/>
	▶ Interval <input type="text" value="60"/> seconds

Buttons: Save Undo

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

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

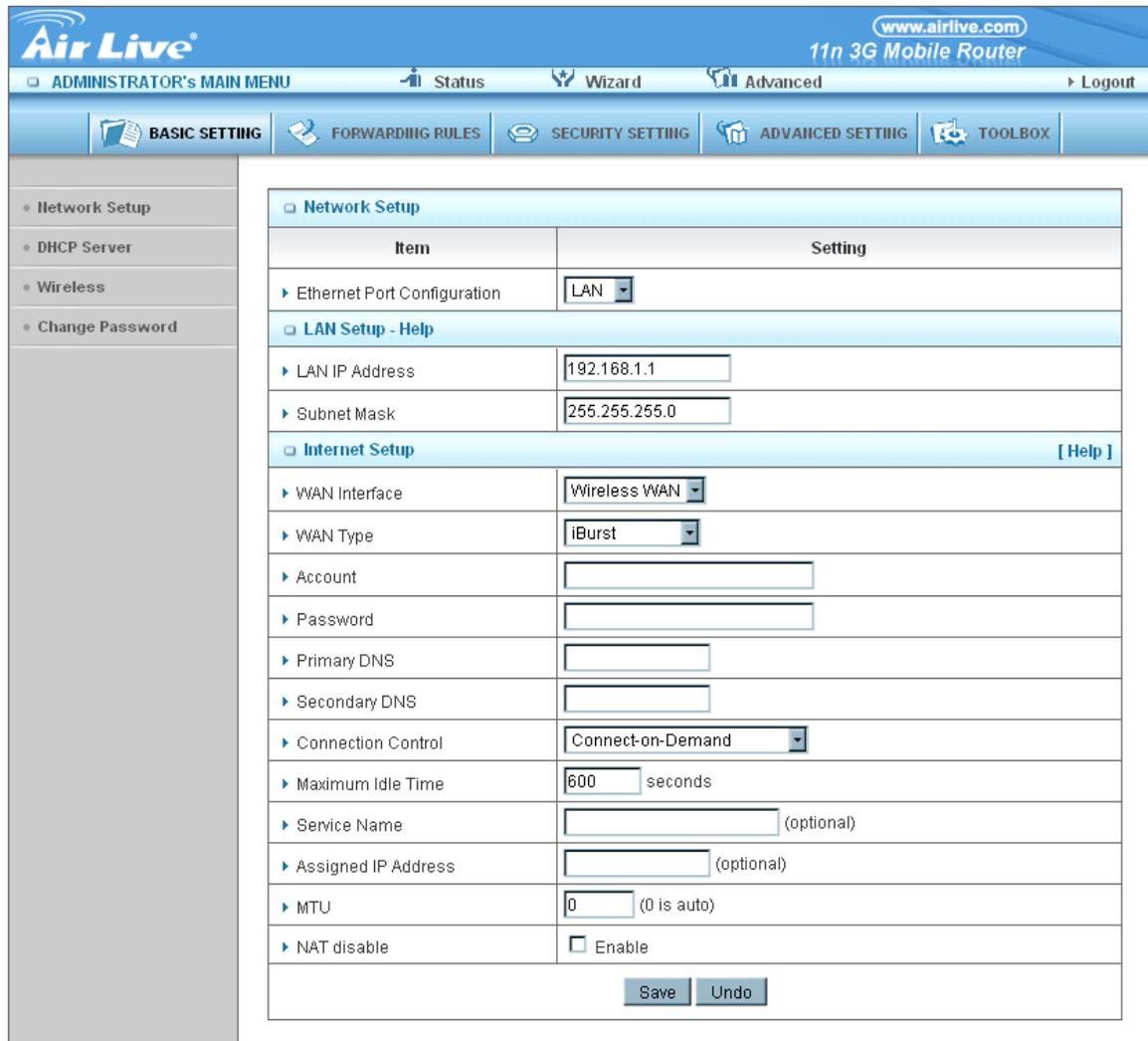
1. APN: Enter the APN for your 3G network here.
2. Pin Code: Enter the Pin Code for your SIM card
3. Dial-Number: This field should not be altered except when required by your service provider.

4. User Name: Enter the new *User Name* for your 3G network here.
5. Password: Enter the new *Password* for your 3G network here.
6. Primary DNS: This feature allows you to assign a Primary DNS Server (Optional)
7. Secondary DNS: This feature allows you to assign a Secondary DNS Server (Optional)
8. Connection Control: There are 3 modes to select:

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

Auto Reconnect (Always-on): The device will link with ISP until the connection is established.
9. Manually: The device will not make the link until someone clicks the connect-button in the Status-page.
10. Maximum Idle Time: The Connection will be broken when the idle time arrives.
11. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The default MTU value is 0(auto).

- **iBurst**



The screenshot shows the configuration page for the Air Live 11n 3G Mobile Router. The interface includes a top navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a tree view with 'Network Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'Network Setup' and contains a table with the following items and settings:

Item	Setting
▶ Ethernet Port Configuration	LAN
LAN Setup - Help	
▶ LAN IP Address	192.168.1.1
▶ Subnet Mask	255.255.255.0
Internet Setup [Help]	
▶ WAN Interface	Wireless WAN
▶ WAN Type	iBurst
▶ Account	<input type="text"/>
▶ Password	<input type="password"/>
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ Connection Control	Connect-on-Demand
▶ Maximum Idle Time	600 seconds
▶ Service Name	<input type="text"/> (optional)
▶ Assigned IP Address	<input type="text"/> (optional)
▶ MTU	0 (0 is auto)
▶ NAT disable	<input type="checkbox"/> Enable

At the bottom of the form are 'Save' and 'Undo' buttons.

1. Account/Password: the account information assigned by your ISP
2. DNS Setting: the address of your DNS server
3. Connection Control: There are 3 modes to select:

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

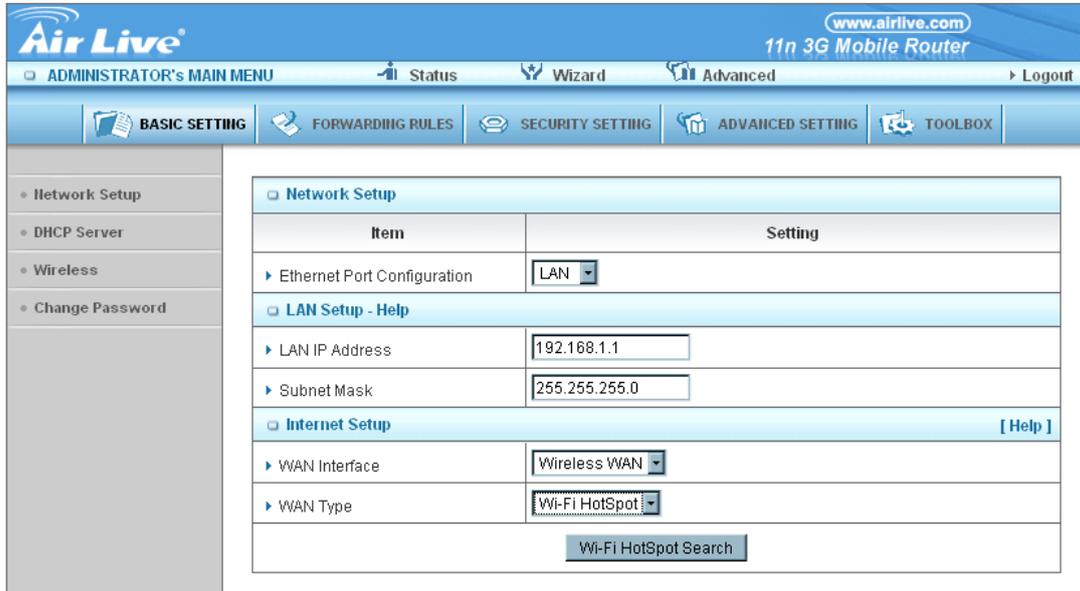
Auto Reconnect (Always-on): The device will link with ISP until the connection is established.

Manually: The device will not make the link until someone clicks

the connect-button in the Status-page.

4. Server Name/Assigned IP Address: fill in if any.
5. Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The default MTU value is 0(auto).

- **Wi-Fi HotSpot**

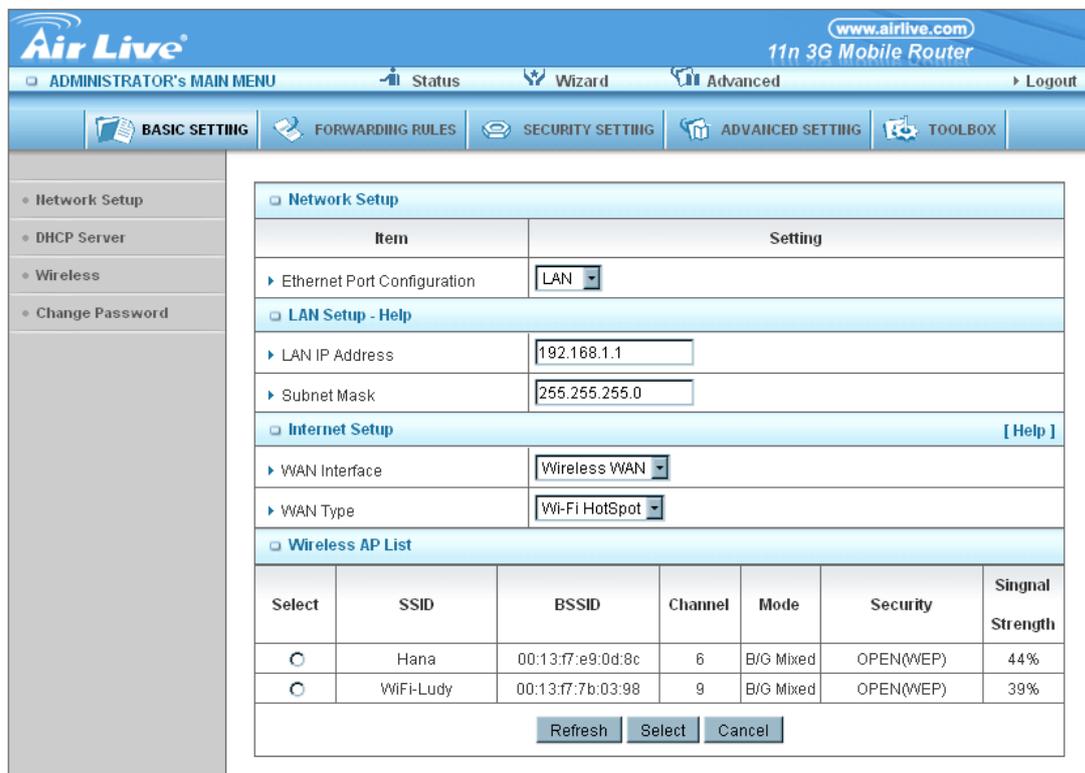


The screenshot shows the 'Network Setup' page in the Air Live web interface. The 'WAN Type' is set to 'Wi-Fi HotSpot'. The 'Wi-Fi HotSpot Search' button is highlighted.

Item	Setting
Ethernet Port Configuration	LAN
LAN Setup - Help	
LAN IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Internet Setup [Help]	
WAN Interface	Wireless WAN
WAN Type	Wi-Fi HotSpot

Wi-Fi HotSpot Search

1. Click on Wi-Fi HotSpot search for searching the SSID of your WISP.

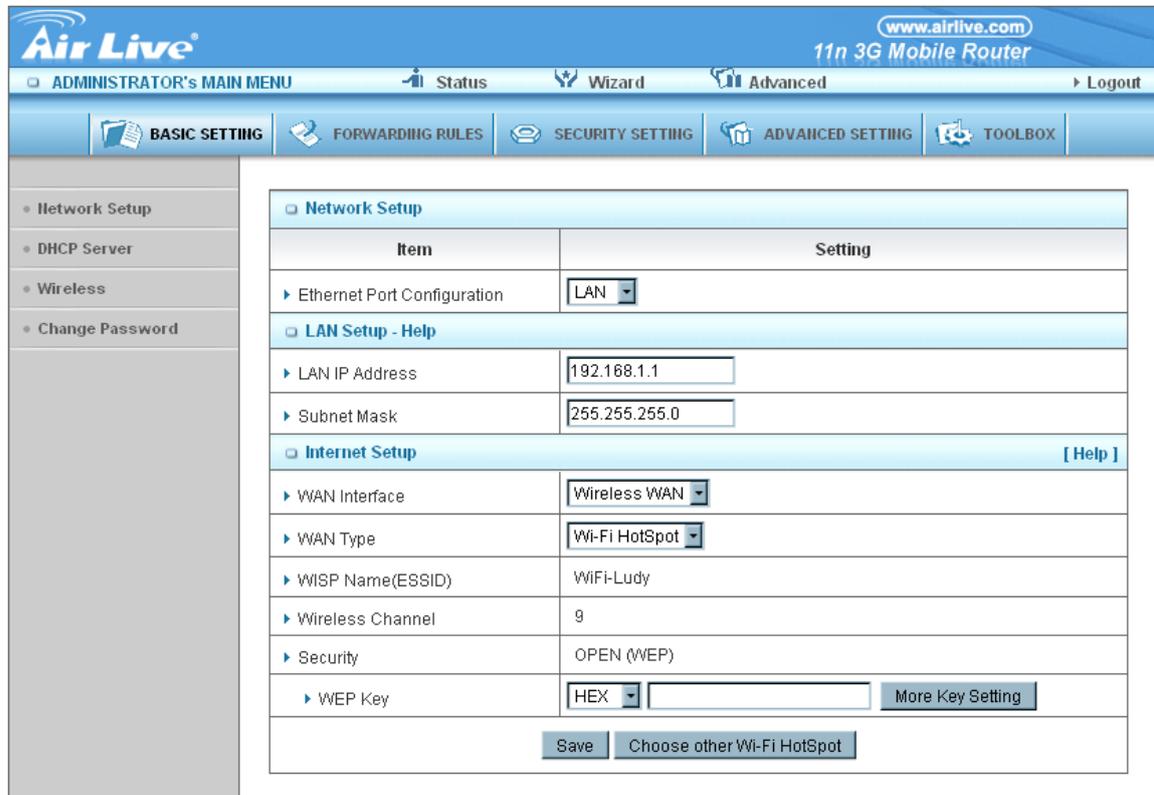


The screenshot shows the 'Wireless AP List' table in the Air Live web interface. The table contains two rows of data. The 'Wi-Fi HotSpot Search' button is highlighted.

Select	SSID	BSSID	Channel	Mode	Security	Signal Strength
<input type="radio"/>	Hana	00:13:f7:e9:0d:8c	6	B/G Mixed	OPEN(WEP)	44%
<input type="radio"/>	WiFi-Ludy	00:13:f7:7b:03:98	9	B/G Mixed	OPEN(WEP)	39%

Refresh Select Cancel

2. Select the SSID of your WISP and then click on select.



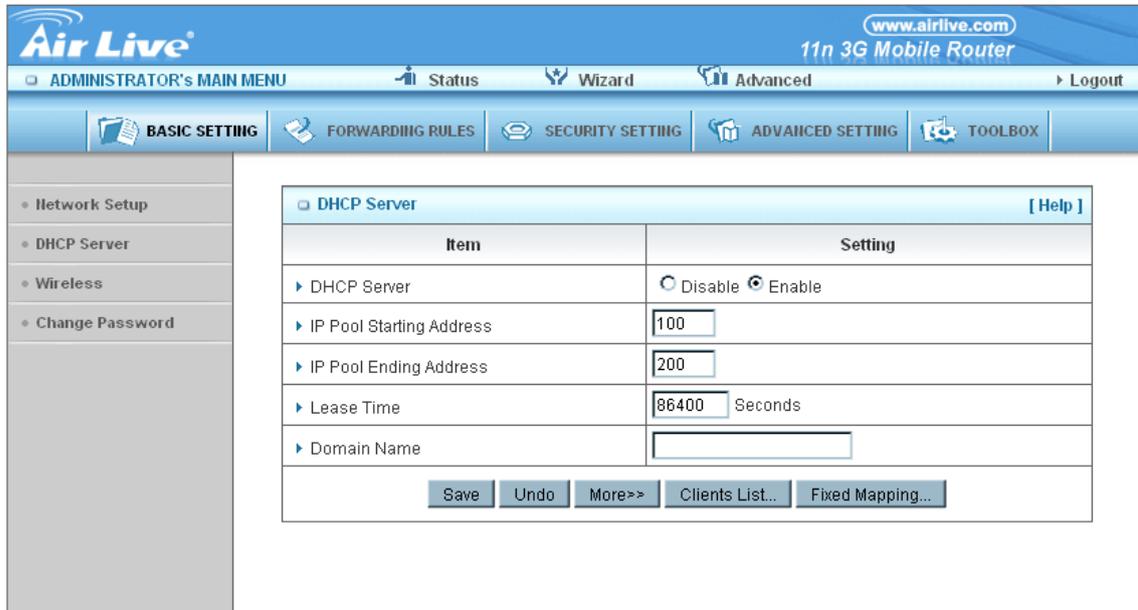
The screenshot shows the web interface for the Air Live 11n 3G Mobile Router. The page is titled "Network Setup" and contains a table with the following configuration items:

Item	Setting
▶ Ethernet Port Configuration	LAN
LAN Setup - Help	
▶ LAN IP Address	192.168.1.1
▶ Subnet Mask	255.255.255.0
Internet Setup [Help]	
▶ WAN Interface	Wireless WAN
▶ WAN Type	Wi-Fi HotSpot
▶ WISP Name(ESSID)	WiFi-Ludy
▶ Wireless Channel	9
▶ Security	OPEN (WEP)
▶ WEP Key	HEX <input type="text"/> More Key Setting

At the bottom of the form, there are two buttons: "Save" and "Choose other Wi-Fi HotSpot".

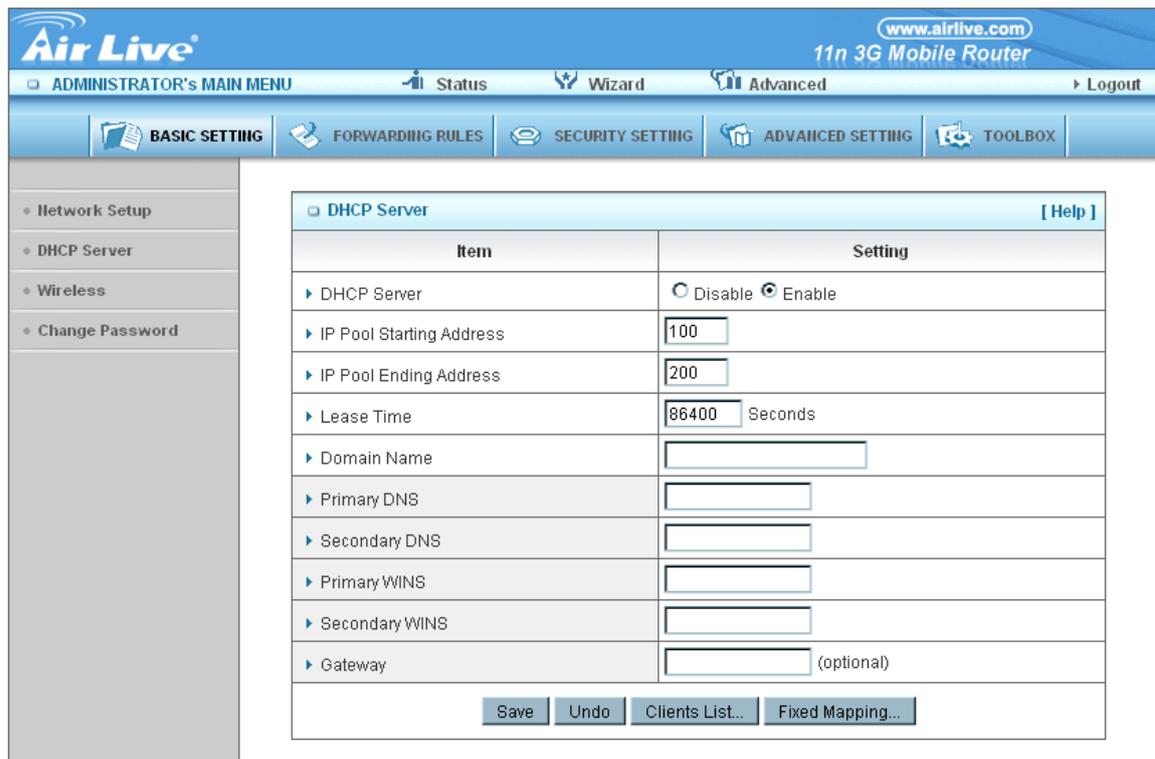
3. Fill in the security parameter if any.

■ DHCP Server



Item	Setting
DHCP Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IP Pool Starting Address	100
IP Pool Ending Address	200
Lease Time	86400 Seconds
Domain Name	

Press “More>>”



Item	Setting
DHCP Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IP Pool Starting Address	100
IP Pool Ending Address	200
Lease Time	86400 Seconds
Domain Name	
Primary DNS	
Secondary DNS	
Primary WINS	
Secondary WINS	
Gateway	(optional)

1. **DHCP Server:** Choose either **Disable** or **Enable**

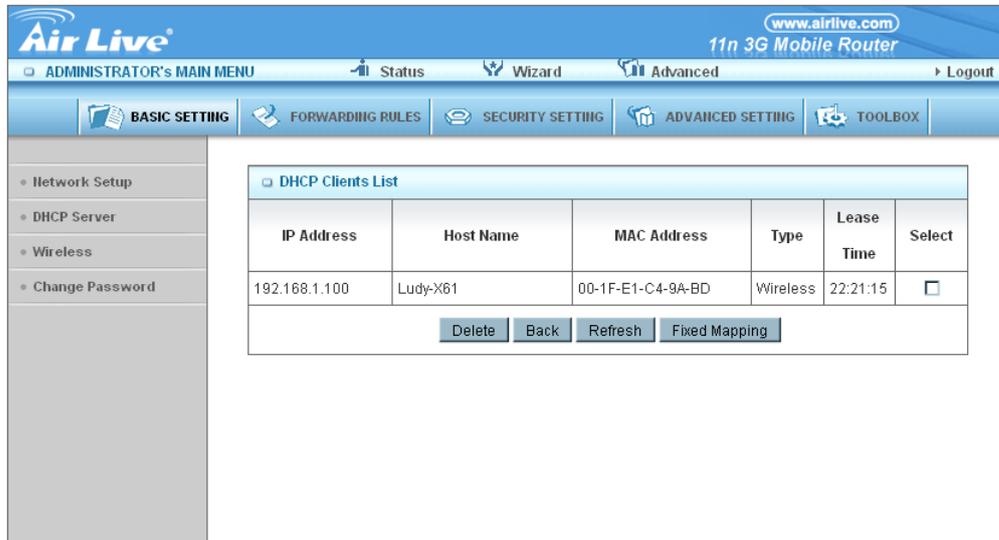
2. **Lease Time:** DHCP leases time to the DHCP client
3. **IP Pool Starting/Ending Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool
4. **Domain Name:** Optional, this information will be passed to the client
5. **Primary DNS/Secondary DNS:** Optional, This feature allows you to assign a DNS Servers
6. **Primary WINS/Secondary WINS:** Optional, this feature allows you to assign a WINS Servers
7. **Gateway:** Optional, Gateway Address would be the IP address of an alternate Gateway.

This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.

After you finish your selection then either Click on “**Save**” to store what you just pick or click “**Undo**” to give up

- **DHCP Clients List**

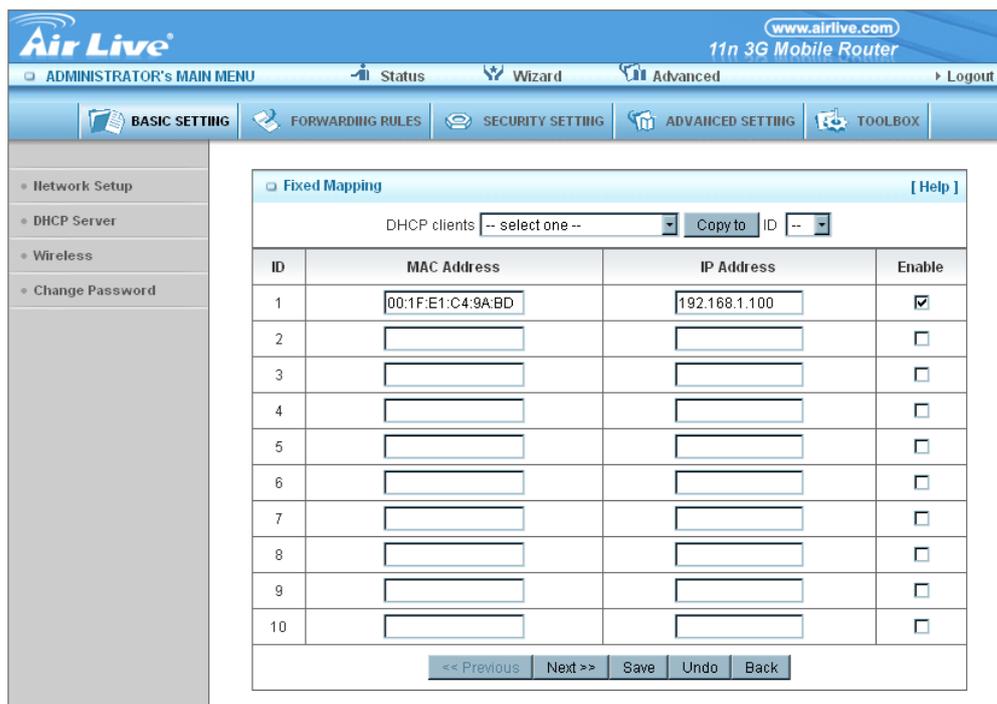
The list of DHCP clients shows here.



IP Address	Host Name	MAC Address	Type	Lease Time	Select
192.168.1.100	Ludy-X61	00-1F-E1-C4-9A-BD	Wireless	22:21:15	<input type="checkbox"/>

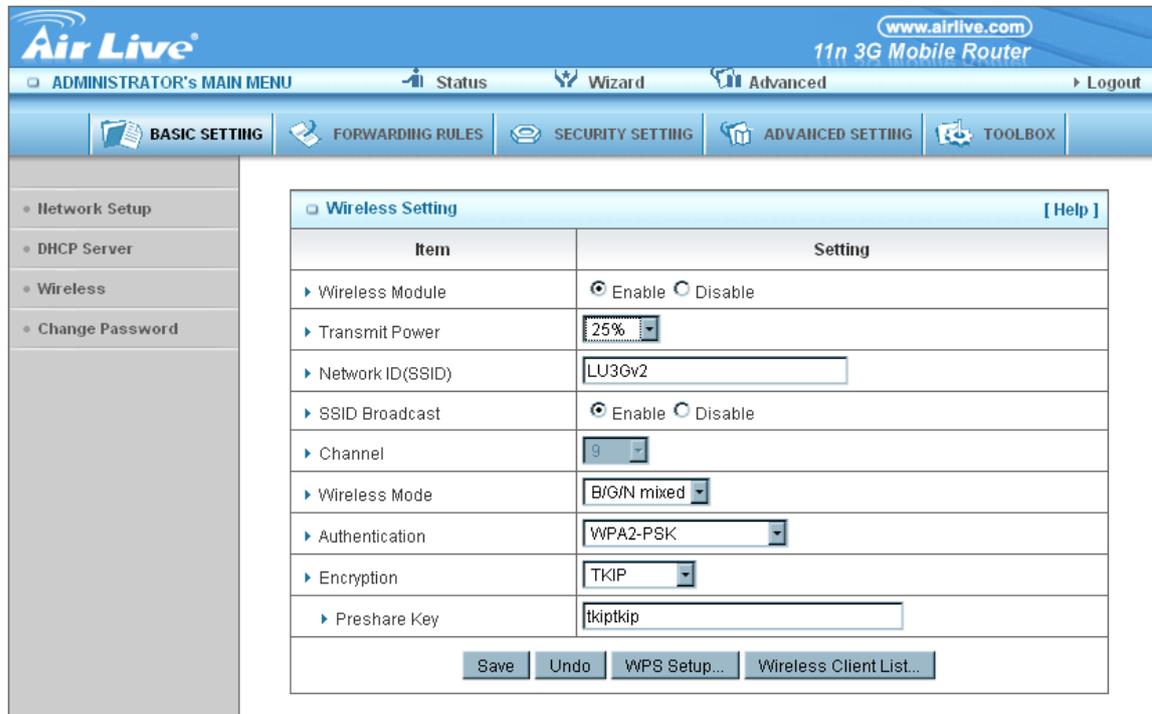
- **DHCP Fixed Mapping**

The DHCP Server will reserve the special IP for special MAC address, shows below.



ID	MAC Address	IP Address	Enable
1	00:1F:E1:C4:9A:BD	192.168.1.100	<input checked="" type="checkbox"/>
2			<input type="checkbox"/>
3			<input type="checkbox"/>
4			<input type="checkbox"/>
5			<input type="checkbox"/>
6			<input type="checkbox"/>
7			<input type="checkbox"/>
8			<input type="checkbox"/>
9			<input type="checkbox"/>
10			<input type="checkbox"/>

■ Wireless Settings



The screenshot shows the 'Wireless Setting' page in the Air Live administrator interface. The page has a blue header with the Air Live logo and '11n 3G Mobile Router'. Below the header is a navigation bar with tabs for 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. A secondary navigation bar contains 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. On the left is a sidebar menu with options like 'Network Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'Wireless Setting' and contains a table of configuration items.

Item	Setting
Wireless Module	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Transmit Power	25%
Network ID(SSID)	LU3Gv2
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	9
Wireless Mode	B/G/N mixed
Authentication	WPA2-PSK
Encryption	TKIP
Preshare Key	tkiptkip

At the bottom of the table are buttons for 'Save', 'Undo', 'WPS Setup...', and 'Wireless Client List...'.

Wireless settings allow you to set the wireless configuration items.

1. **Wireless:** *Enabled* is the default. Selecting this option will allow you to set your Wireless Access Point (WAP) settings.
2. **Transmit Power:** Configure the wireless output power here.
3. **Network ID (SSID):** Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is *default*. The SSID can be easily changed to establish a new wireless network. (Note: SSID names may contain up to 32 ASCII characters).
4. **SSID Broadcast:** The router will broadcast beacons that have some information, including ssid so that wireless clients can know how many AP devices by scanning function in the network. Therefore, this function is disabled; the wireless clients can not find the device from beacons.
5. **Channel:** *Auto* is the default. Devices on the network must share the same channel. (Note: Wireless adapters automatically scan and match

the wireless settings. You may also select the channel you wish to use).

6. **Wireless Mode:** Choose *B/G Mixed, B only, G only, N only, G/N Mixed* or *B/G/N mixed*. The factory default setting is *B/G/N mixed*.
7. **Authentication mode:** You may select from nine kinds of authentication to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, WPA/WPA2.

- **Open**

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

- **Shared**

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

- **Auto**

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

- **WPA-PSK**

Select Encryption and Pre-share Key Mode

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

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

Fill in the key, Ex 12345678

- **WPA**

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

Select Encryption and RADIUS Shared Key

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

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

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

- **WPA-PSK2**

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

- **WPA2**

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

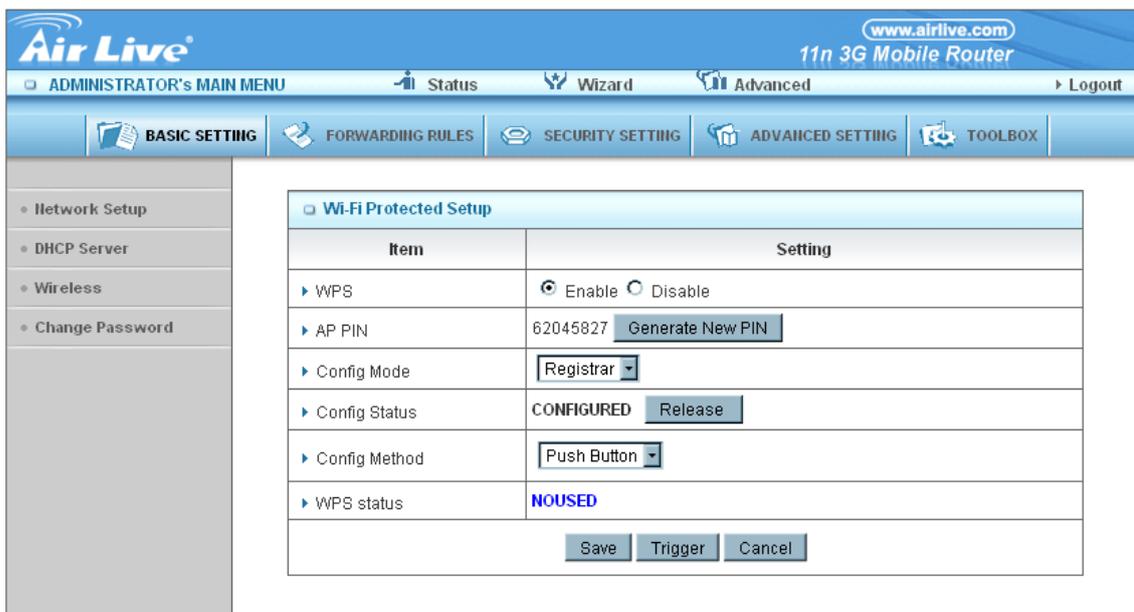
- **WPA-PSK/WPA-PSK2**

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

- **WPA/WPA2**

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

8. **WPS (Wi-Fi Protection Setup):** WPS is Wi-Fi Protection Setup which is similar to WCN-NET and offers safe and easy way in Wireless Connection.

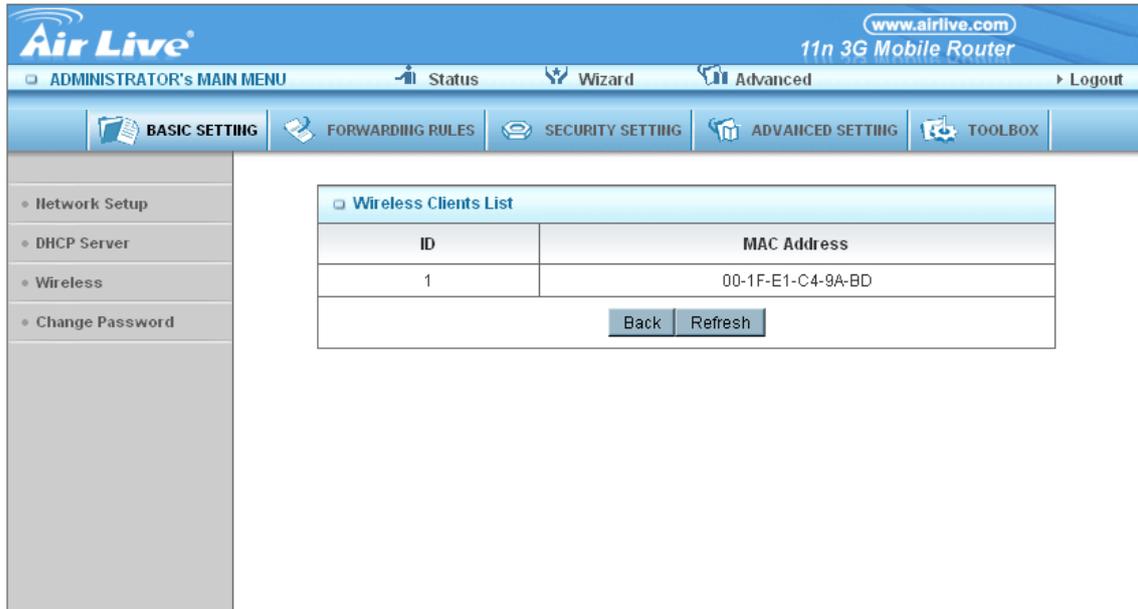


The screenshot shows the web interface for the Air Live 11n 3G Mobile Router. The top navigation bar includes 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar lists 'Network Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'Wi-Fi Protected Setup' and contains a table with the following items and settings:

Item	Setting
▶ WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ AP PIN	62045827 <input type="button" value="Generate New PIN"/>
▶ Config Mode	Registrar
▶ Config Status	CONFIGURED <input type="button" value="Release"/>
▶ Config Method	Push Button
▶ WPS status	NOUSED

At the bottom of the configuration area are three buttons: 'Save', 'Trigger', and 'Cancel'.

9. **Wireless Client List:** The list of wireless client is shows here.



The screenshot shows the web interface of an Air Live 11n 3G Mobile Router. The top navigation bar includes the Air Live logo, the website URL www.airlive.com, and the device model "11n 3G Mobile Router". Below this, there are tabs for "ADMINISTRATOR's MAIN MENU", "Status", "Wizard", "Advanced", and "Logout". A secondary navigation bar contains "BASIC SETTING", "FORWARDING RULES", "SECURITY SETTING", "ADVANCED SETTING", and "TOOLBOX".

The left sidebar menu includes the following options:

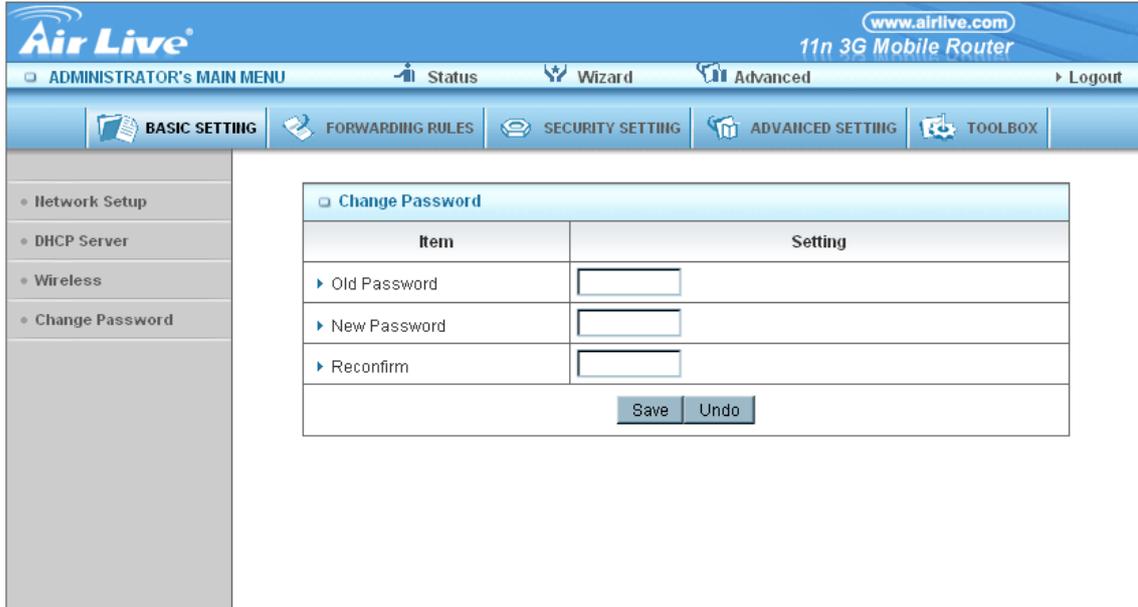
- Network Setup
- DHCP Server
- Wireless
- Change Password

The main content area displays the "Wireless Clients List" section, which contains a table with the following data:

ID	MAC Address
1	00-1F-E1-C4-9A-BD

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

■ Change Password



The screenshot shows the Air Live web interface for the 11n 3G Mobile Router. The top navigation bar includes the Air Live logo, the website URL www.airlive.com, and the device model '11n 3G Mobile Router'. Below this is a menu with 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. A secondary menu contains 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. On the left, a sidebar lists 'Network Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'Change Password' and contains a table with the following structure:

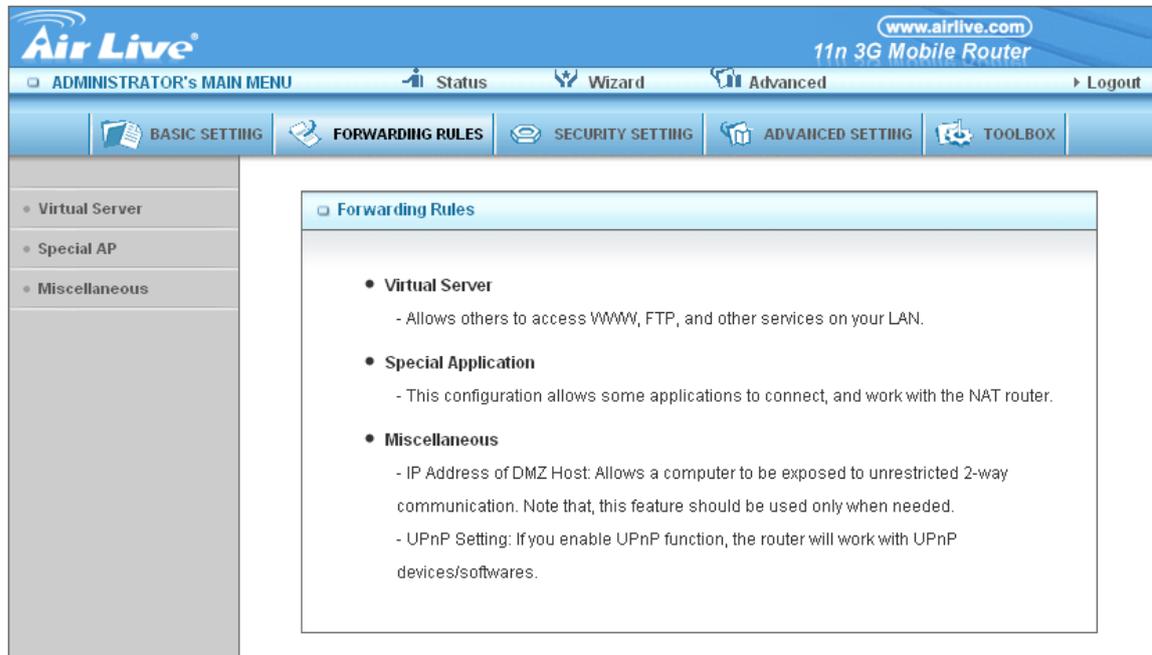
Item	Setting
▶ Old Password	<input type="text"/>
▶ New Password	<input type="text"/>
▶ Reconfirm	<input type="text"/>

Below the table are two buttons: 'Save' and 'Undo'.

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

Click on “Save” to store what you just select or “Undo” to give up

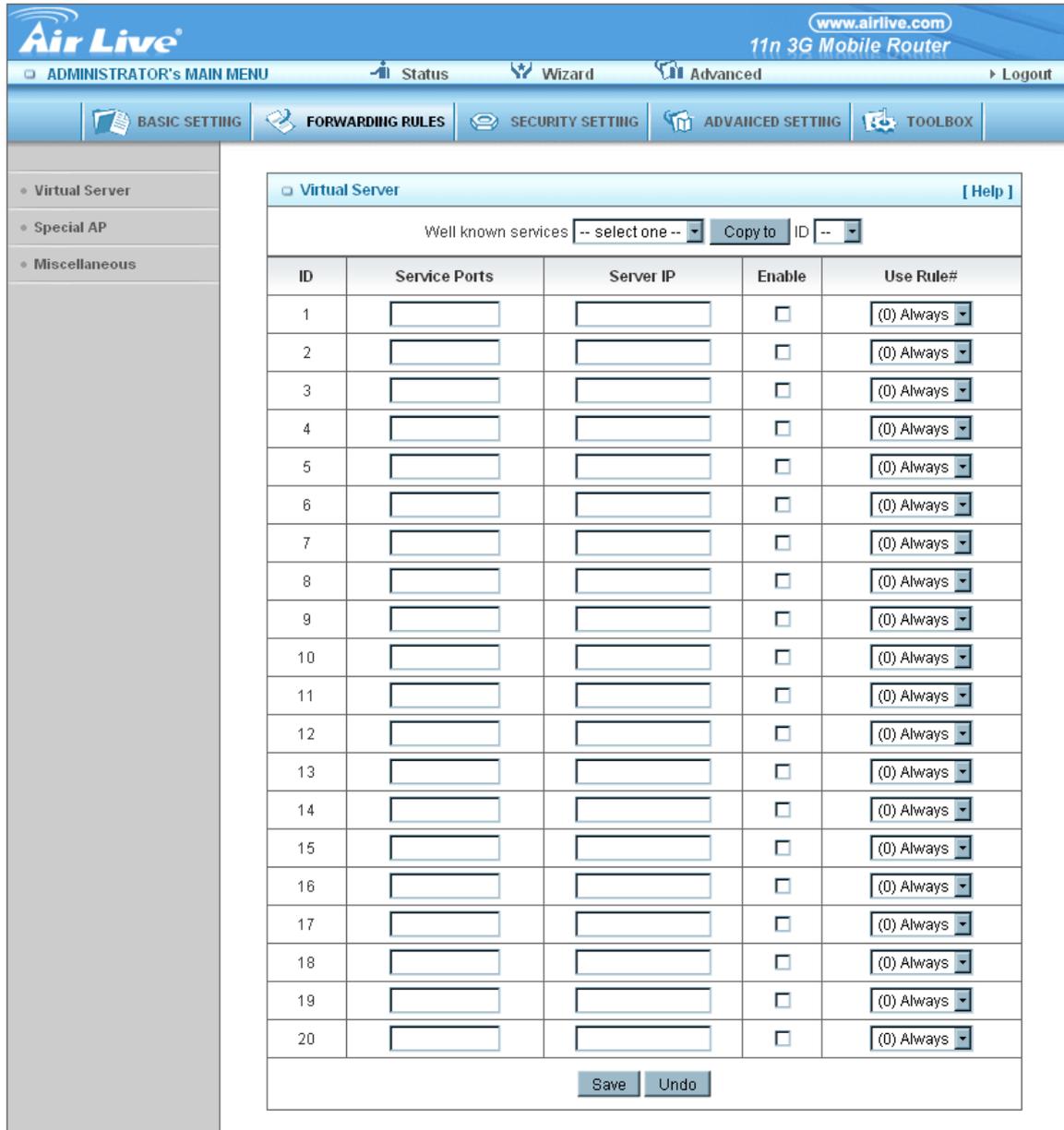
3.2.2 Forwarding Rules



The screenshot displays the web management interface for an Air Live 11n 3G Mobile Router. The top navigation bar includes the Air Live logo, the website URL www.airlive.com, the device model "11n 3G Mobile Router", and a "Logout" button. Below this, a secondary menu contains "ADMINISTRATOR'S MAIN MENU", "Status", "Wizard", "Advanced", and "Logout". A main menu bar features "BASIC SETTING", "FORWARDING RULES" (which is selected), "SECURITY SETTING", "ADVANCED SETTING", and "TOOLBOX". On the left side, a sidebar menu lists "Virtual Server", "Special AP", and "Miscellaneous". The main content area, titled "Forwarding Rules", contains the following information:

- **Virtual Server**
 - Allows others to access WWW, FTP, and other services on your LAN.
- **Special Application**
 - This configuration allows some applications to connect, and work with the NAT router.
- **Miscellaneous**
 - IP Address of DMZ Host: Allows a computer to be exposed to unrestricted 2-way communication. Note that, this feature should be used only when needed.
 - UPnP Setting: If you enable UPnP function, the router will work with UPnP devices/software.

■ Virtual Server



Well known services: -- select one -- Copy to ID: --

ID	Service Ports	Server IP	Enable	Use Rule#
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
11	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
12	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
13	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
14	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
15	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
16	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
17	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
18	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
19	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always
20	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always

Save Undo

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

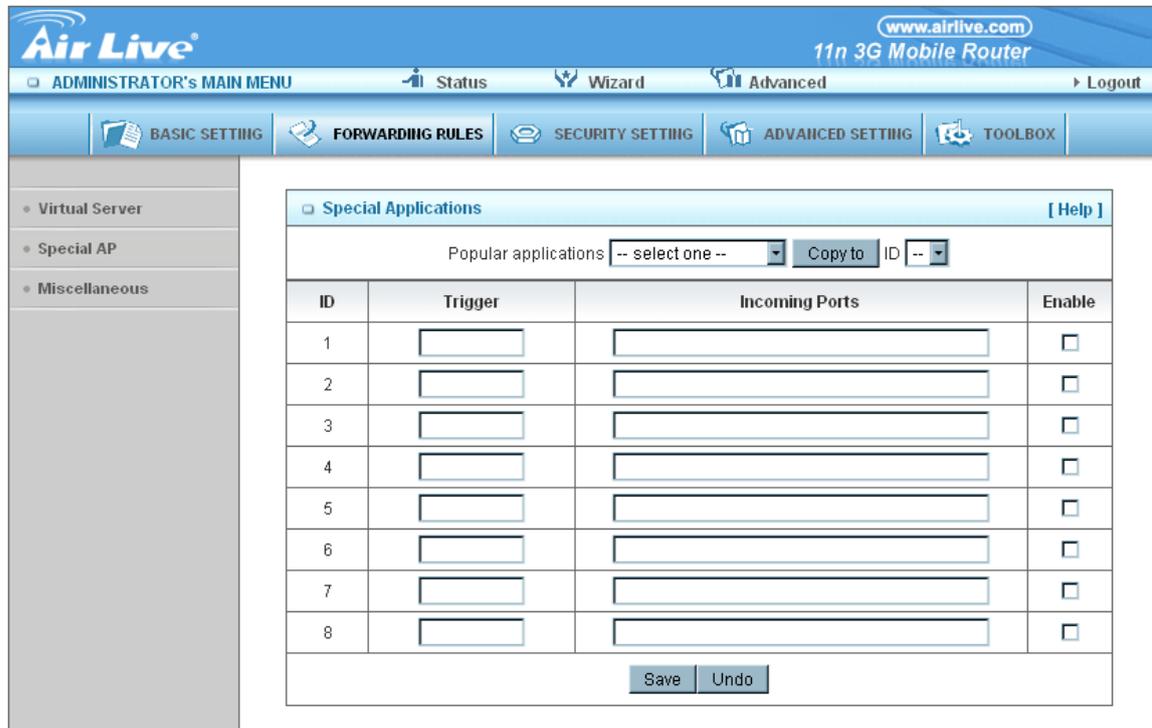
redirected to the computer specified by the Server IP. Virtual Server can work with Scheduling Rules, and give user more flexibility on Access control. For Detail, please refer to Scheduling Rule.

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

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

Click on “Save” to store what you just select or “Undo” to give up

■ Special AP



The screenshot shows the Air Live 11n 3G Mobile Router administrator interface. The top navigation bar includes 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this, there are tabs for 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The 'Special Applications' page is active, showing a table with 8 rows for configuring special applications. Each row has columns for ID, Trigger, Incoming Ports, and Enable. A 'Popular applications' dropdown menu is at the top, with a 'Copy to' button and an 'ID' dropdown. 'Save' and 'Undo' buttons are at the bottom of the table.

ID	Trigger	Incoming Ports	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

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

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

This product provides some predefined settings.

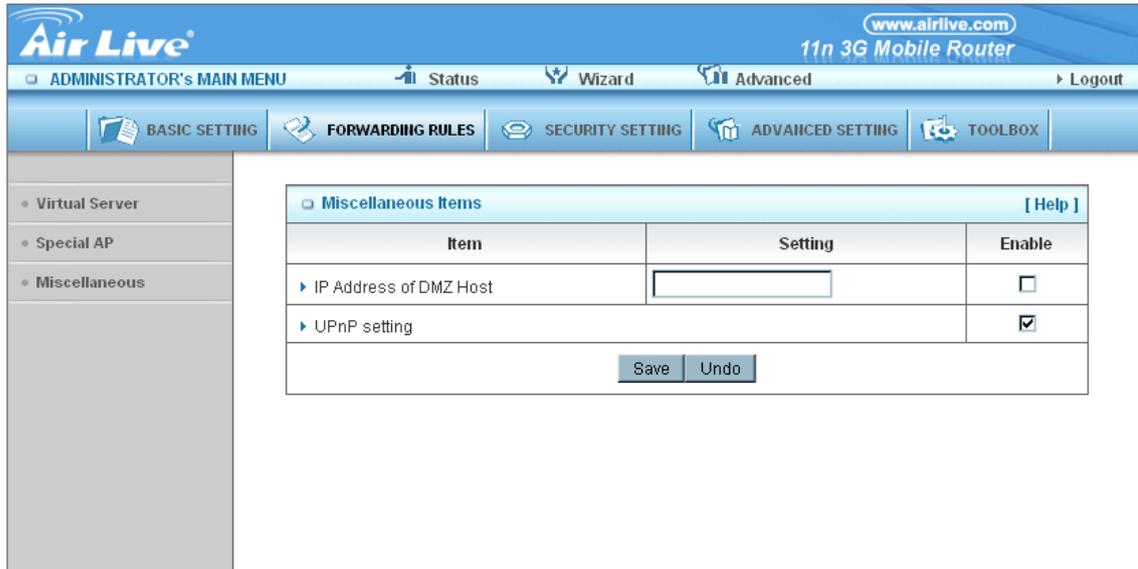
- Select your application and
- Click “**Copy to**” to add the predefined setting to your list.

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



Click on “Save” to store what you just select or” Undo” to give up

■ Miscellaneous



1. IP Address of DMZ Host

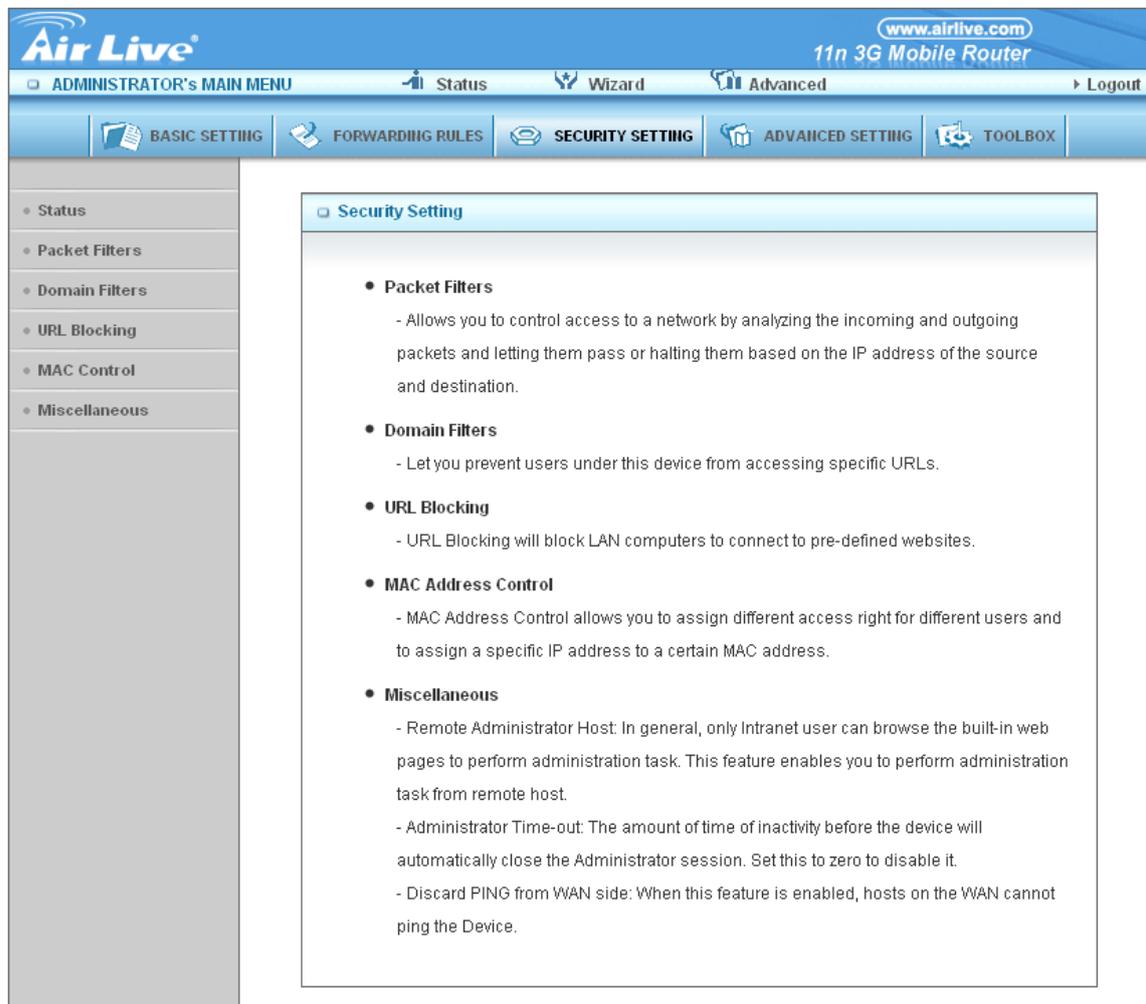
DMZ (Demilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

2. UPnP Setting

The device 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:

Click on “Save” to store what you just select or “Undo” to give up

3.2.3 Security Setting



The screenshot displays the web-based administrator interface for the Air Live 11n 3G Mobile Router. The top navigation bar includes the Air Live logo, the website URL www.airlive.com, the device model "11n 3G Mobile Router", and a "Logout" button. Below this, a secondary menu contains "ADMINISTRATOR'S MAIN MENU", "Status", "Wizard", "Advanced", and "Logout". A third menu highlights the current page, "SECURITY SETTING", among other options: "BASIC SETTING", "FORWARDING RULES", "ADVANCED SETTING", and "TOOLBOX".

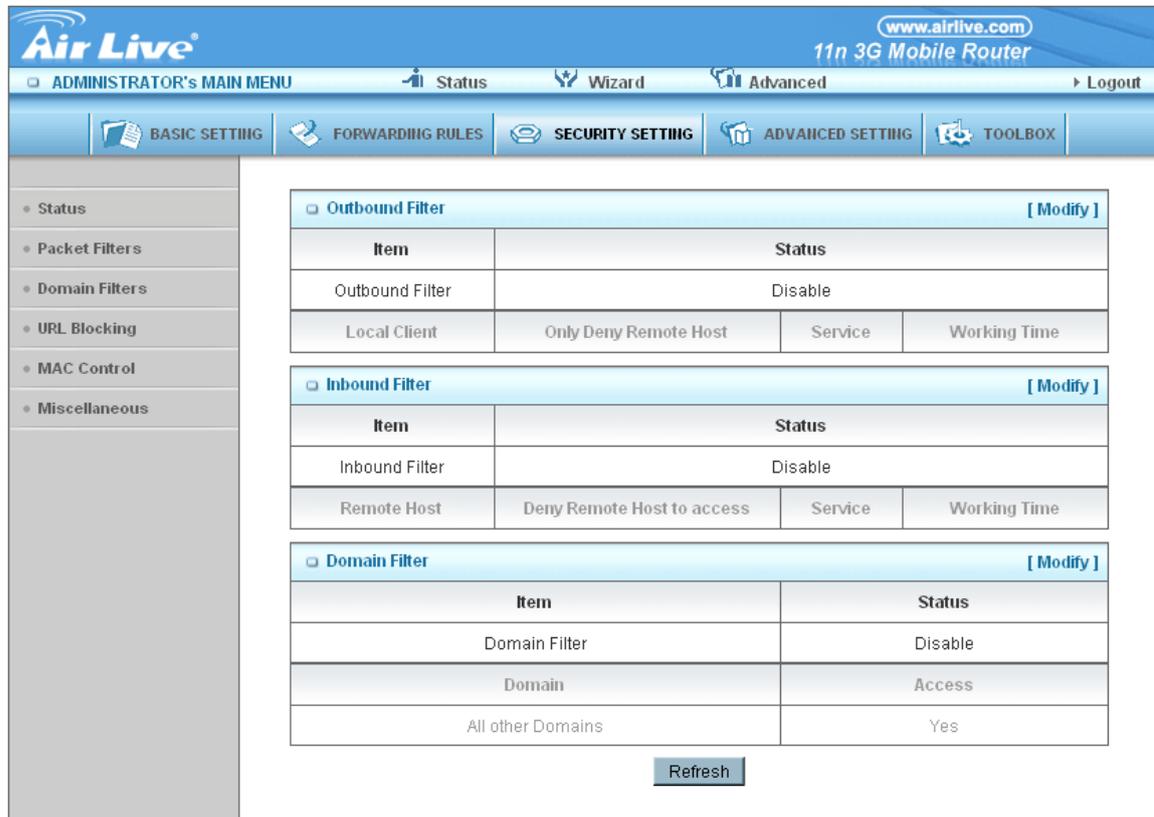
The left sidebar lists the following menu items:

- Status
- Packet Filters
- Domain Filters
- URL Blocking
- MAC Control
- Miscellaneous

The main content area is titled "Security Setting" and contains the following information:

- **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.

■ Status



The screenshot shows the 'Status' page for the 'SECURITY SETTING' section. The interface includes a top navigation bar with 'ADMINISTRATOR'S MAIN MENU' and 'Logout', and a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The main content area displays three filter status tables:

Outbound Filter [Modify]			
Item	Status		
Outbound Filter	Disable		
Local Client	Only Deny Remote Host	Service	Working Time

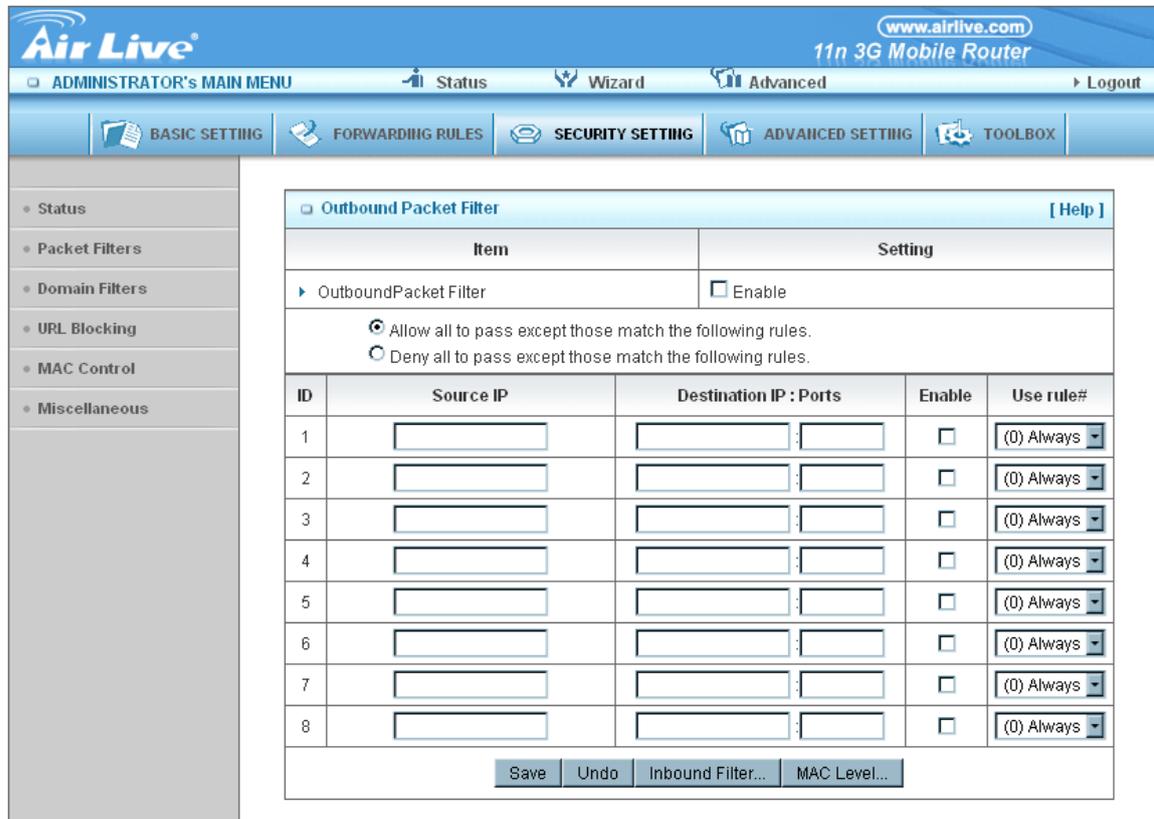
Inbound Filter [Modify]			
Item	Status		
Inbound Filter	Disable		
Remote Host	Deny Remote Host to access	Service	Working Time

Domain Filter [Modify]	
Item	Status
Domain Filter	Disable
Domain	Access
All other Domains	Yes

Refresh

The Status of the security setting will show here.

■ Packet Filters



Outbound Packet Filter [Help]

Item	Setting			
OutboundPacket Filter	<input 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.				
ID	Source IP	Destination IP : Ports	Enable	Use rule#
1	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
2	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
3	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
4	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
5	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
6	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
7	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
8	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾

Save Undo Inbound Filter... MAC Level...

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

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

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

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

- Source IP address
- Source port
- Destination IP address
- Destination port

- Protocol: TCP or UDP or both.
- Use Rule#

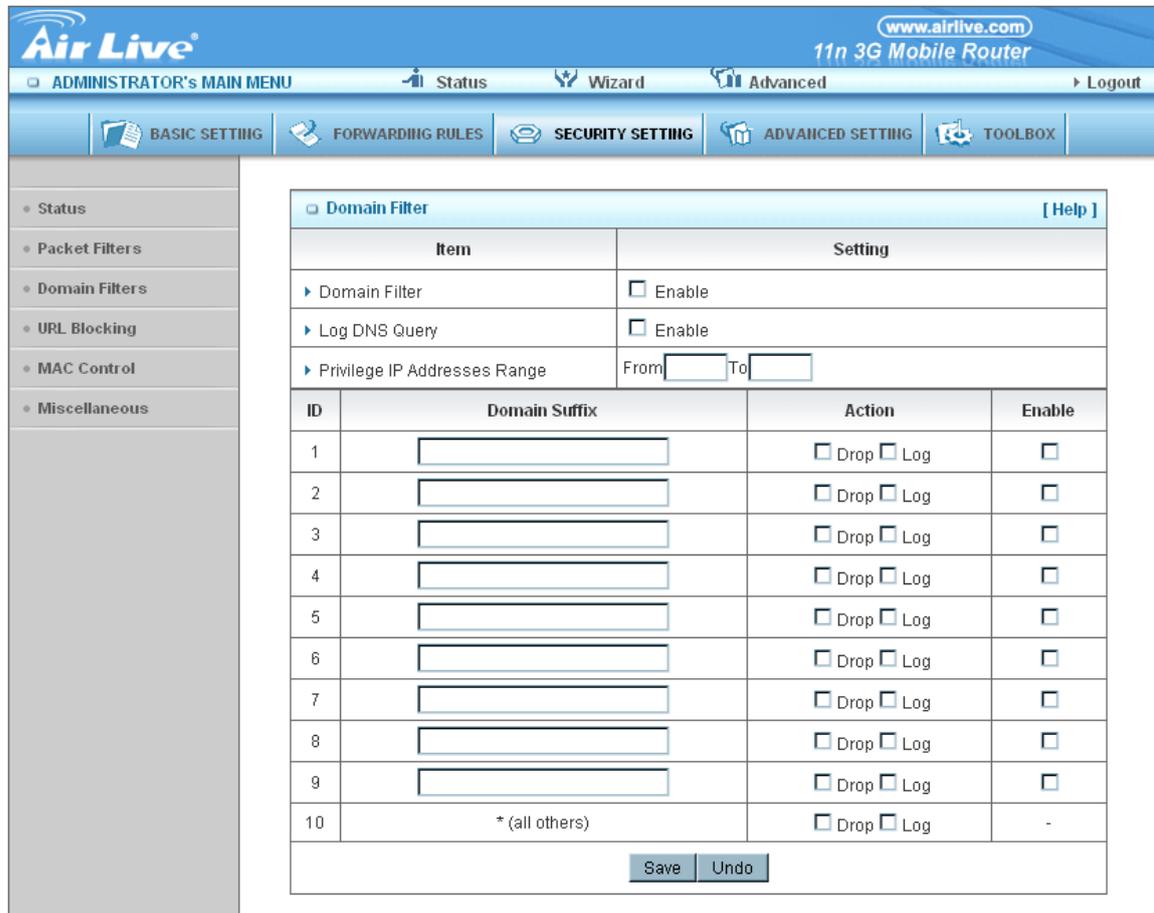
For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.

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

Each rule can be enabled or disabled individually.

Click on “Save” to store what you just select or “Undo” to give up

■ Domain Filters



Domain Filter [Help]

Item	Setting
▶ Domain Filter	<input type="checkbox"/> Enable
▶ Log DNS Query	<input type="checkbox"/> Enable
▶ Privilege IP Addresses Range	From <input type="text"/> To <input type="text"/>

ID	Domain Suffix	Action	Enable
1	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
10	*(all others)	<input type="checkbox"/> Drop <input type="checkbox"/> Log	-

Save Undo

1. Domain Filter

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

2. Domain Filter Enable

Check if you want to enable Domain Filter.

3. Log DNS Query

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

4. Privilege IP Address Range

Setting a group of hosts and privilege these hosts to access network



without restriction.

5. **Domain Suffix**

A suffix of URL can be restricted, for example, ".com", "xxx.com".

6. **Action**

When someone is accessing the URL met the domain-suffix, what kind of action you want.

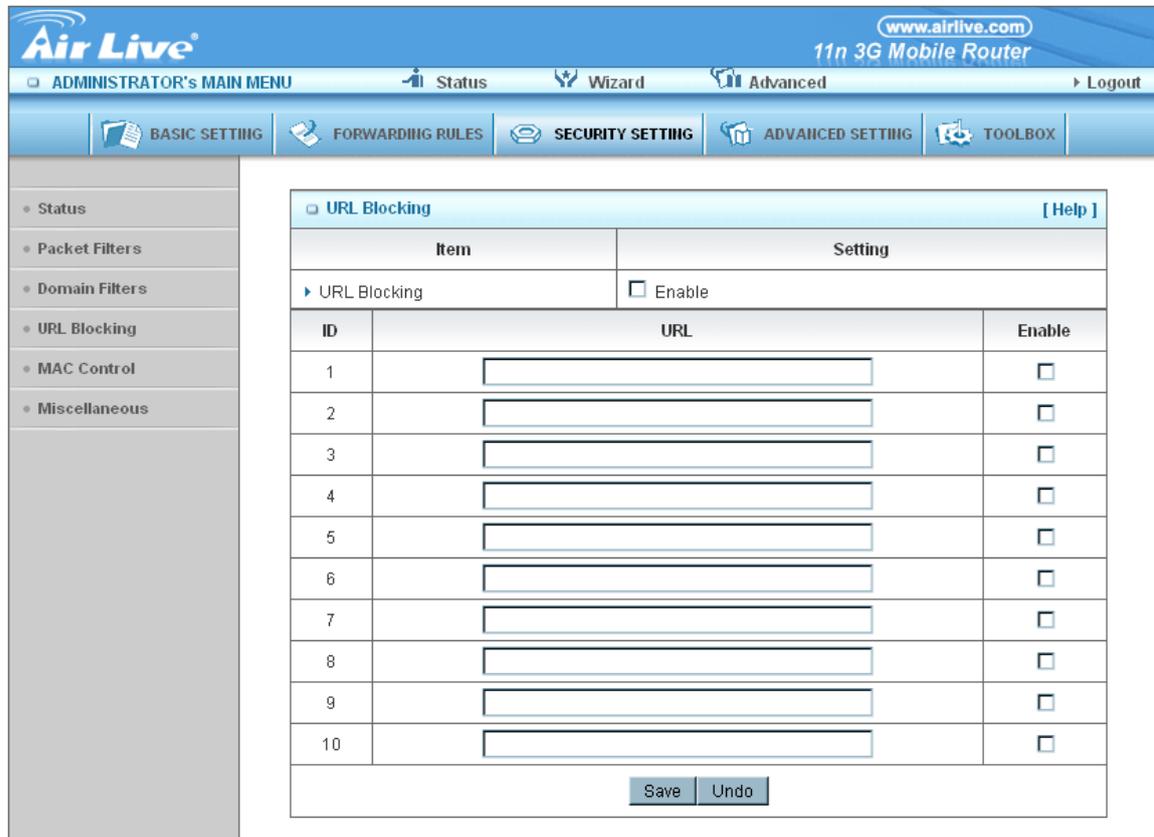
Check drop to block the access. Check "log" to log these access.

7. **Enable**

Check to enable each rule.

Click on "Save" to store what you just select or "Undo" to give up

■ URL Blocking



The screenshot shows the Air Live administrator interface. The top navigation bar includes the Air Live logo, the website URL www.airlive.com, the device model "11n 3G Mobile Router", and a "Logout" link. Below this is a menu with "ADMINISTRATOR'S MAIN MENU" and sub-menus for "Status", "Wizard", and "Advanced". A secondary navigation bar contains "BASIC SETTING", "FORWARDING RULES", "SECURITY SETTING", "ADVANCED SETTING", and "TOOLBOX". The left sidebar lists various configuration categories, with "URL Blocking" selected. The main content area displays the "URL Blocking" configuration page, which includes a "URL Blocking" section with an "Enable" checkbox. Below this is a table with 10 rows, each containing an "ID", a "URL" input field, and an "Enable" checkbox. At the bottom of the table are "Save" and "Undo" buttons.

URL Blocking [Help]		
Item	Setting	
URL Blocking	<input type="checkbox"/> Enable	
ID	URL	Enable
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="checkbox"/>

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

1. URL Blocking Enable

Check if you want to enable URL Blocking.

2. URL

If any part of the Website's URL matches the pre-defined word, the connection will be blocked.



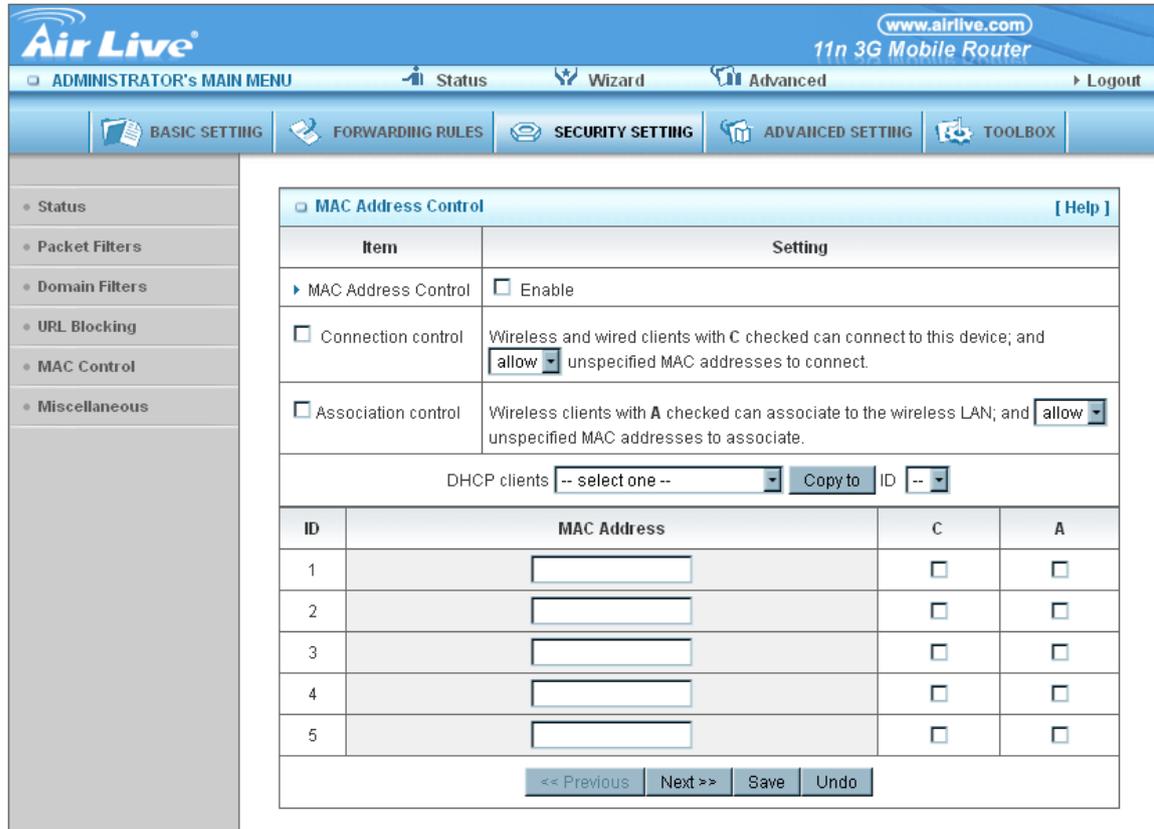
For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".

3. **Enable**

Check to enable each rule.

Click on "Save" to store what you just select or "Undo" to give up

■ MAC Control



The screenshot shows the 'MAC Address Control' configuration page in the Air Live web interface. The page includes a navigation menu with options like 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area is titled 'MAC Address Control' and contains several settings:

- MAC Address Control:** A checkbox for 'Enable'.
- Connection control:** A checkbox for 'Connection control'. Below it, a description states: 'Wireless and wired clients with C checked can connect to this device; and [allow] unspecified MAC addresses to connect.' The 'allow' is shown in a dropdown menu.
- Association control:** A checkbox for 'Association control'. Below it, a description states: 'Wireless clients with A checked can associate to the wireless LAN; and [allow] unspecified MAC addresses to associate.' The 'allow' is shown in a dropdown menu.
- DHCP clients:** A dropdown menu for 'DHCP clients' (currently set to '-- select one --') and a 'Copy to' button followed by an 'ID' dropdown menu.
- Control Table:** A table with 5 rows and 4 columns: ID, MAC Address, C, and A. Each row has input fields for the MAC address and checkboxes for C and A.
- Navigation:** Buttons for '<< Previous', 'Next >>', 'Save', and 'Undo'.

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

1. MAC Address Control

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

2. Connection control

Check "Connection control" to enable the controlling of which wired and wireless clients can connect 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.

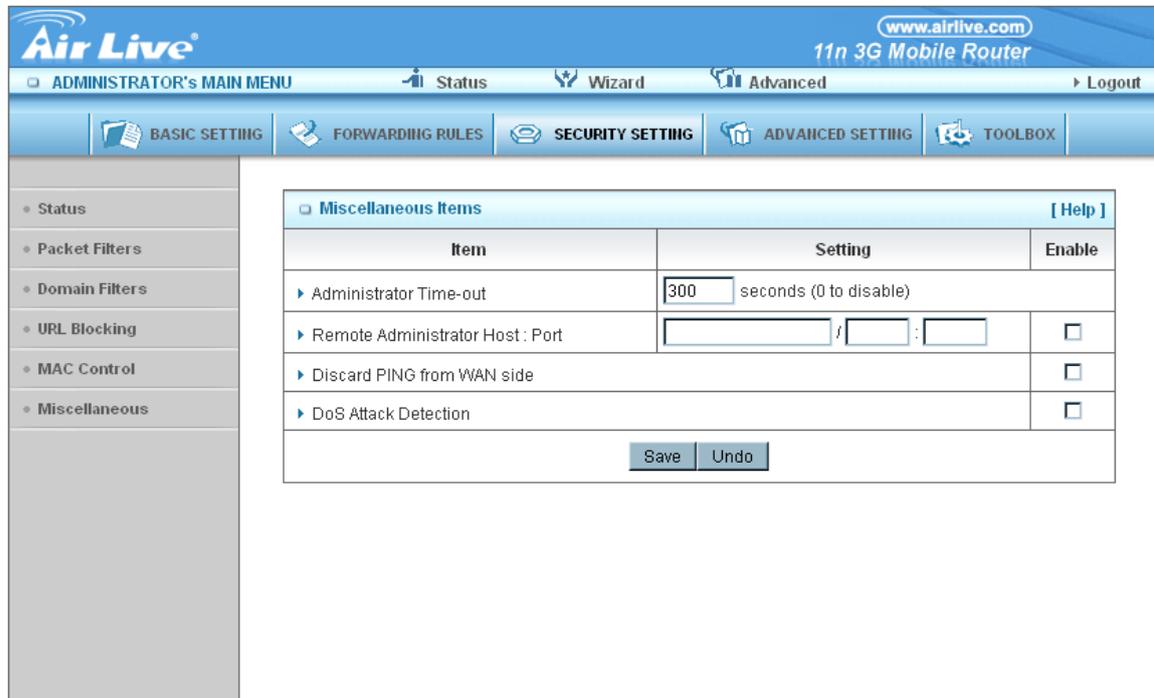
3. Association control

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

Click on "Save" to store what you just select or "Undo" to give up

Click on "Next Page" to go down or "Previous page" back to last page

■ Miscellaneous



The screenshot shows the Air Live administrator interface. The top navigation bar includes the Air Live logo, the website URL www.airlive.com, the device model 11n 3G Mobile Router, and a Logout button. Below this is a menu with options: ADMINISTRATOR's MAIN MENU, Status, Wizard, and Advanced. A secondary menu contains BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING, and TOOLBOX. On the left side, a sidebar lists various configuration categories: Status, Packet Filters, Domain Filters, URL Blocking, MAC Control, and Miscellaneous. The main content area is titled 'Miscellaneous Items' and contains a table with the following data:

Item	Setting	Enable
▶ Administrator Time-out	<input type="text" value="300"/> seconds (0 to disable)	
▶ Remote Administrator Host : Port	<input type="text"/> / <input type="text"/> : <input type="text"/>	<input type="checkbox"/>
▶ Discard PING from WAN side		<input type="checkbox"/>
▶ DoS Attack Detection		<input type="checkbox"/>

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

1. Administrator Time-out

The time of no activity to logout automatically, you may set it to zero to disable this feature.

2. Remote Administrator Host/Port

In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect 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 80. You can change web server port to other port, too.

3. Discard PING from WAN side



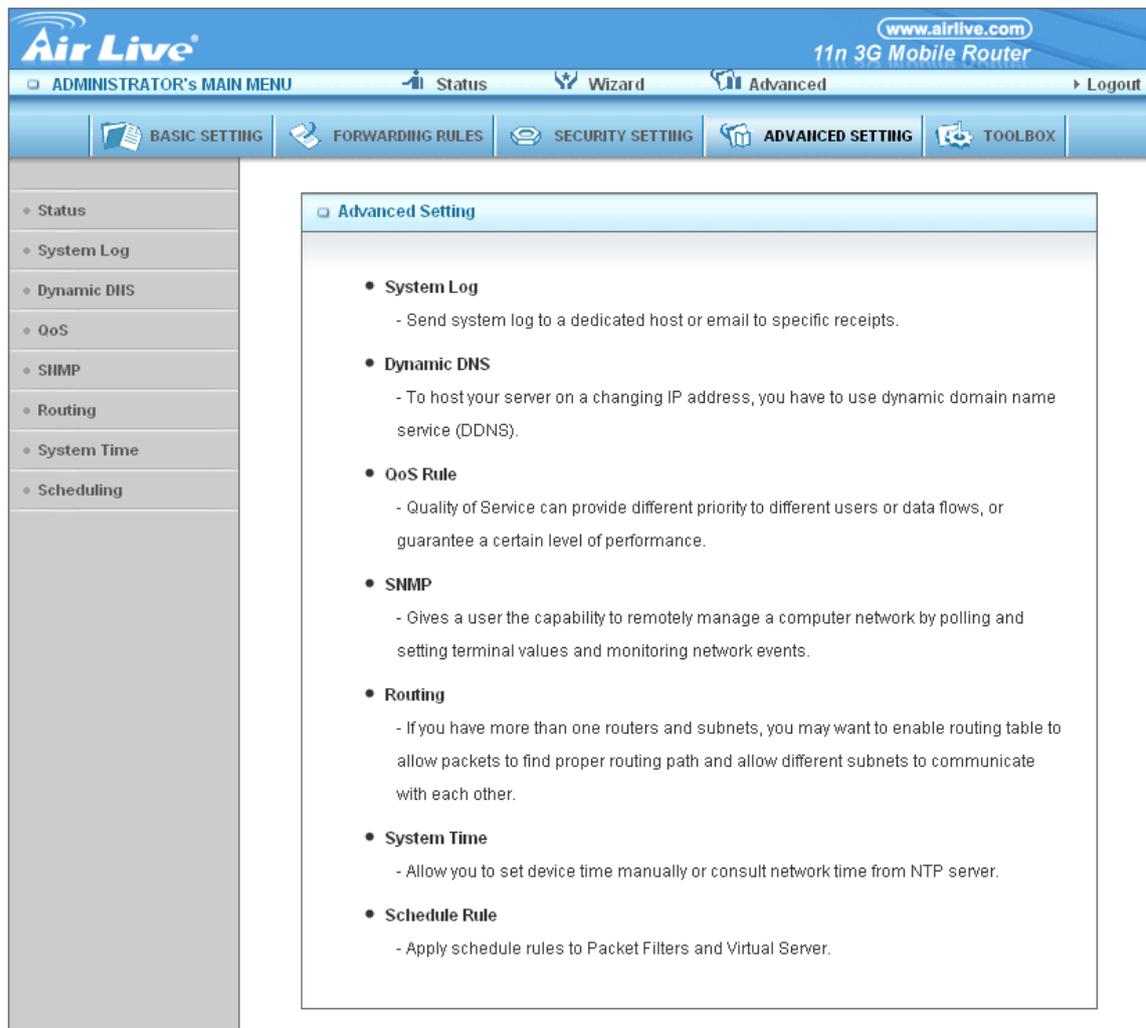
When this feature is enabled, any host on the WAN cannot ping this product.

4. DoS Attack Detection

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

Click on “Save” to store what you just select or” Undo” to give up

3.2.4 Advanced Setting

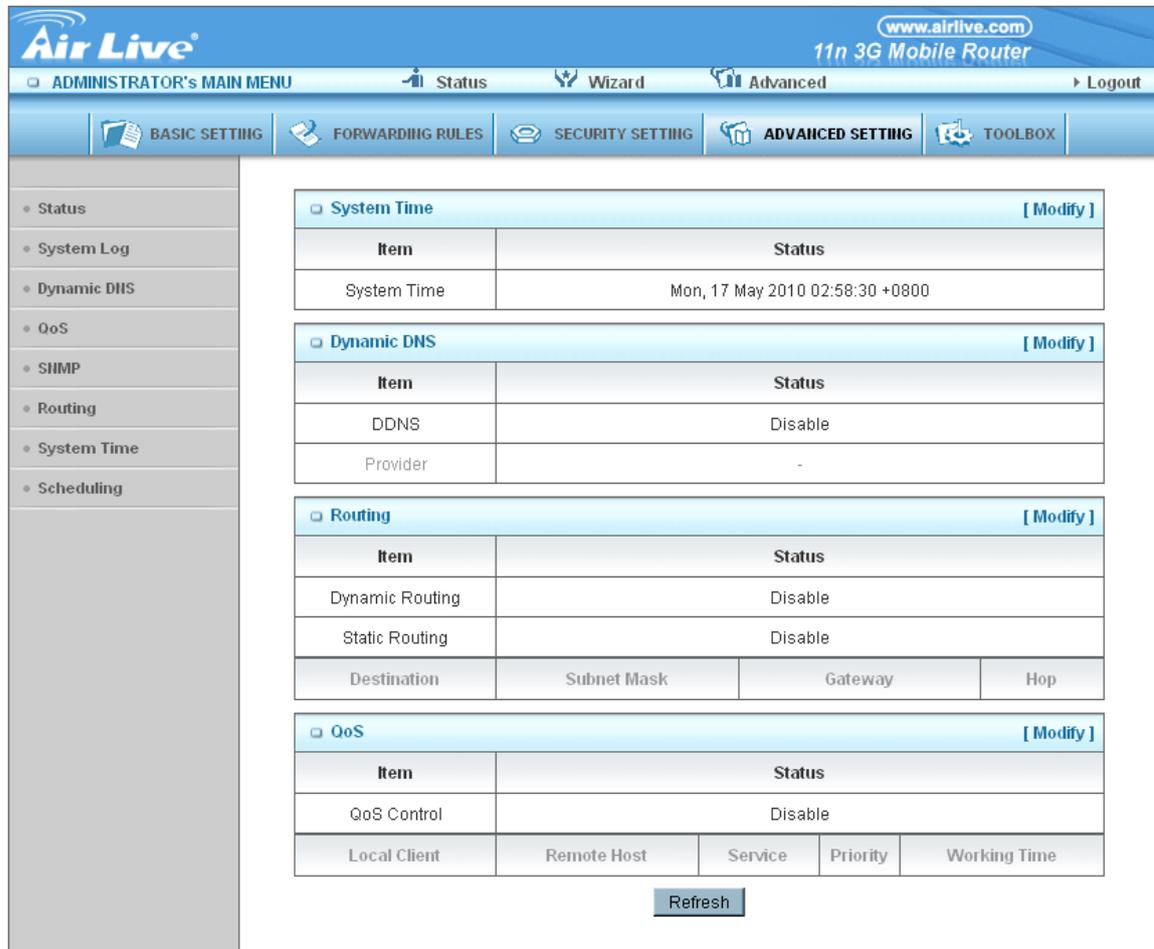


The screenshot displays the web interface of the Air Live 11n 3G Mobile Router. The top navigation bar includes the Air Live logo, the website URL www.airlive.com, and the device name "11n 3G Mobile Router". Below this, there are tabs for "ADMINISTRATOR'S MAIN MENU", "Status", "Wizard", "Advanced", and "Logout". A secondary menu bar contains "BASIC SETTING", "FORWARDING RULES", "SECURITY SETTING", "ADVANCED SETTING" (which is highlighted), and "TOOLBOX".

The left sidebar lists various system settings: Status, System Log, Dynamic DNS, QoS, SIIMP, Routing, System Time, and Scheduling. The main content area is titled "Advanced Setting" and contains a list of configuration options:

- **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).
- **QoS Rule**
 - Quality of Service can provide different priority to different users or data flows, or guarantee a certain level of performance.
- **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.
- **System Time**
 - Allow you to set device time manually or consult network time from NTP server.
- **Schedule Rule**
 - Apply schedule rules to Packet Filters and Virtual Server.

■ Status



The screenshot shows the 'Status' page of the Air Live 11n 3G Mobile Router. The interface includes a top navigation bar with 'ADMINISTRATOR's MAIN MENU' and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The main content area is divided into a left sidebar and a main panel. The sidebar lists menu items: Status, System Log, Dynamic DNS, QoS, SHMP, Routing, System Time, and Scheduling. The main panel displays four expandable sections, each with a table of settings and status:

- System Time**: [Modify]

Item	Status
System Time	Mon, 17 May 2010 02:58:30 +0800
- Dynamic DNS**: [Modify]

Item	Status
DDNS	Disable
Provider	-
- Routing**: [Modify]

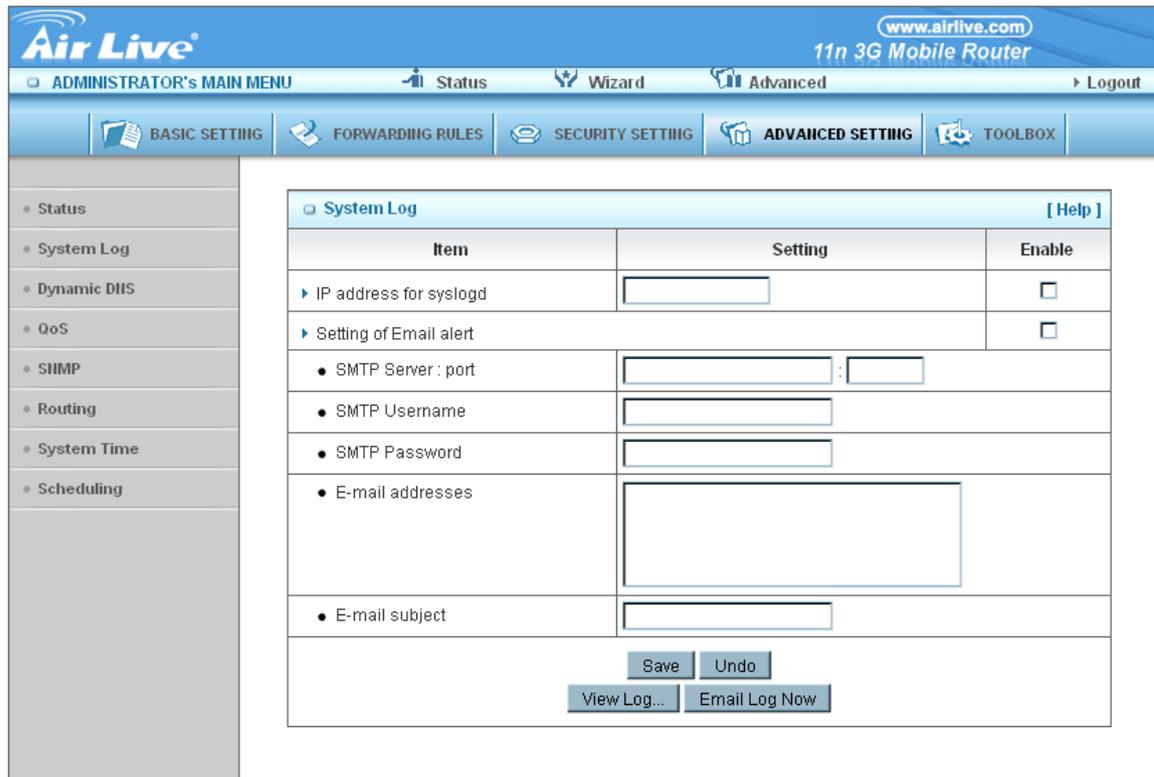
Item	Status		
Dynamic Routing	Disable		
Static Routing	Disable		
Destination	Subnet Mask	Gateway	Hop
- QoS**: [Modify]

Item	Status			
QoS Control	Disable			
Local Client	Remote Host	Service	Priority	Working Time

A 'Refresh' button is located at the bottom of the main panel.

The system status will show here

■ System Log



Item	Setting	Enable
▶ IP address for syslogd	<input type="text"/>	<input type="checkbox"/>
▶ Setting of Email alert		<input type="checkbox"/>
• SMTP Server : port	<input type="text"/> : <input type="text"/>	
• SMTP Username	<input type="text"/>	
• SMTP Password	<input type="text"/>	
• E-mail addresses	<input type="text"/>	
• E-mail subject	<input type="text"/>	

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:

1. IP Address for Sys log

Host IP of destination where sys log will be sent to.

Check **Enable** to enable this function.

2. E-mail Alert Enable

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

3. SMTP Server IP and Port

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

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



4. **Send E-mail alert to**

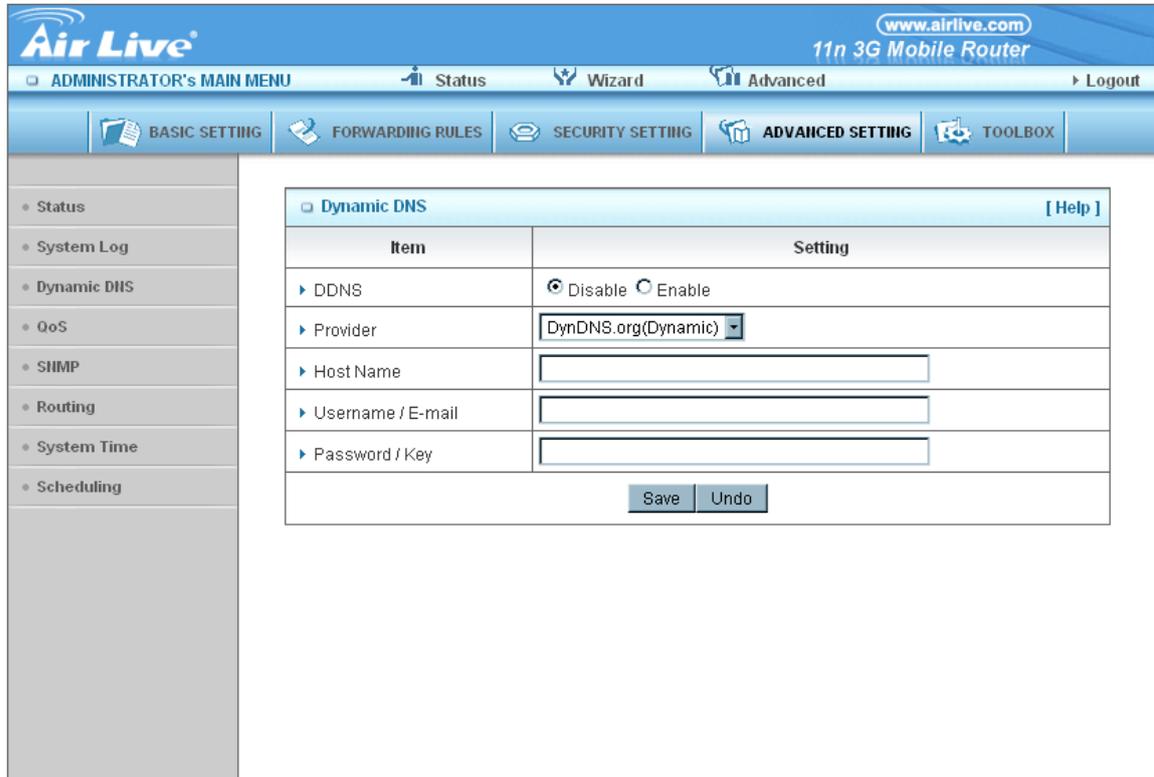
The recipients who will receive these logs, you can assign more than 1 recipient, using ';' or ',' to separate these email addresses.

5. **E-mail Subject**

The subject of email alert, this setting is optional.

Click on “Save” to store what you just select or “Undo” to give up

■ Dynamic DNS



The screenshot shows the 'Dynamic DNS' configuration page in the Air Live administrator interface. The page has a blue header with the Air Live logo, the website URL 'www.airlive.com', and the device model '11n 3G Mobile Router'. Below the header is a navigation bar with tabs for 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. A secondary navigation bar contains 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. On the left is a sidebar menu with options like 'Status', 'System Log', 'Dynamic DNS', 'QoS', 'SHMP', 'Routing', 'System Time', and 'Scheduling'. The main content area is titled 'Dynamic DNS' and contains a table with the following items and settings:

Item	Setting
▶ DDNS	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
▶ Provider	DynDNS.org(Dynamic) ▼
▶ Host Name	<input type="text"/>
▶ Username / E-mail	<input type="text"/>
▶ Password / Key	<input type="text"/>

At the bottom of the table are 'Save' and 'Undo' buttons. A '[Help]' link is located in the top right corner of the table area.

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

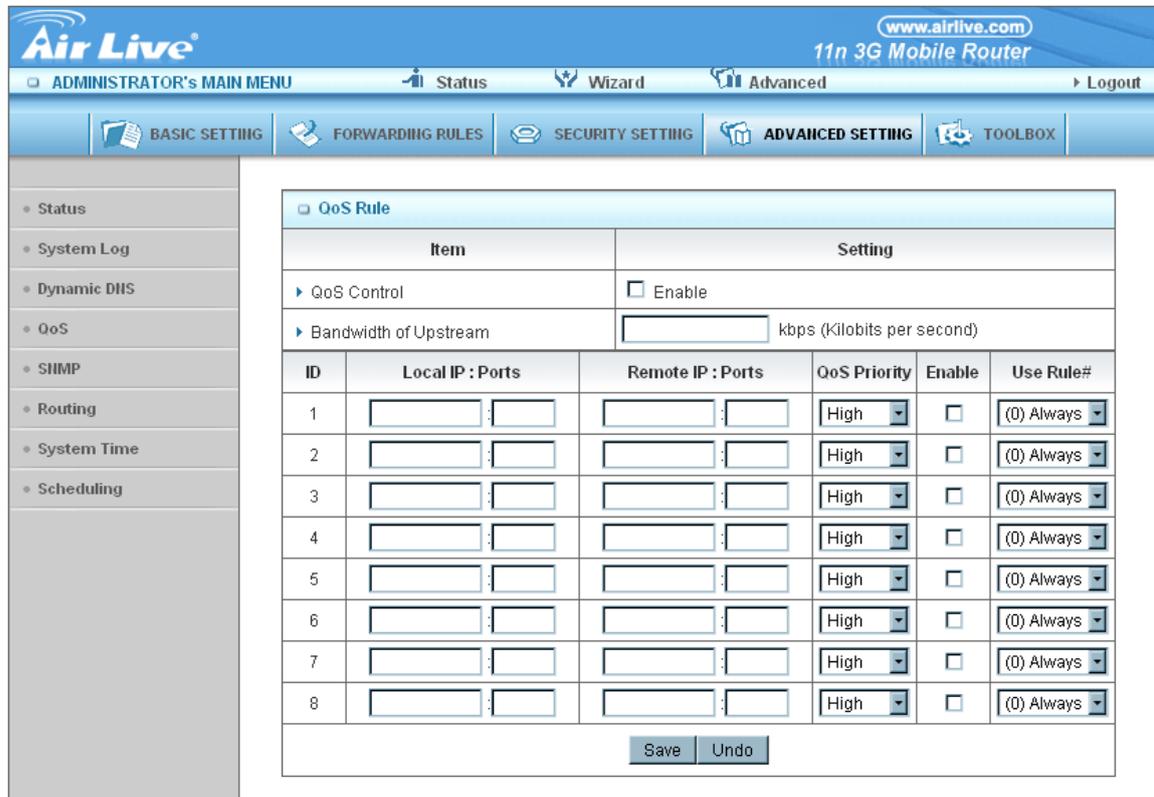
Username/E-mail

Password/Key

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

Click on “Save” to store what you just select or “Undo” to give up

■ QoS



The screenshot shows the 'QoS Rule' configuration page in the Air Live 11n 3G Mobile Router administrator interface. The page has a blue header with the Air Live logo and 'www.airlive.com' on the right. Below the header is a navigation bar with 'ADMINISTRATOR'S MAIN MENU' and icons for 'Status', 'Wizard', and 'Advanced', along with a 'Logout' link. A secondary navigation bar contains 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar shows a tree view with 'QoS' selected. The main content area is titled 'QoS Rule' and contains the following configuration options:

- QoS Control:** Enable
- Bandwidth of Upstream:** kbps (Kilobits per second)

ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use Rule#
1	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	(0) Always
2	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	(0) Always
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	(0) Always
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	(0) Always
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	(0) Always
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	(0) Always
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	(0) Always
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	(0) Always

At the bottom of the table are 'Save' and 'Undo' buttons.

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

1. **Enable**

This Item enables QoS function or not.

2. **Bandwidth of Upstream**

Set the limitation of upstream speed.

3. **Local: IP**

Define the Local IP address of packets here.

4. **Local: Ports**

Define the Local port of the packets in this field.

5. Remote: IP

Define the Remote IP address of packets here.

6. Remote: Ports

Define the Remote port of the packets in this field.

7. QoS Priority

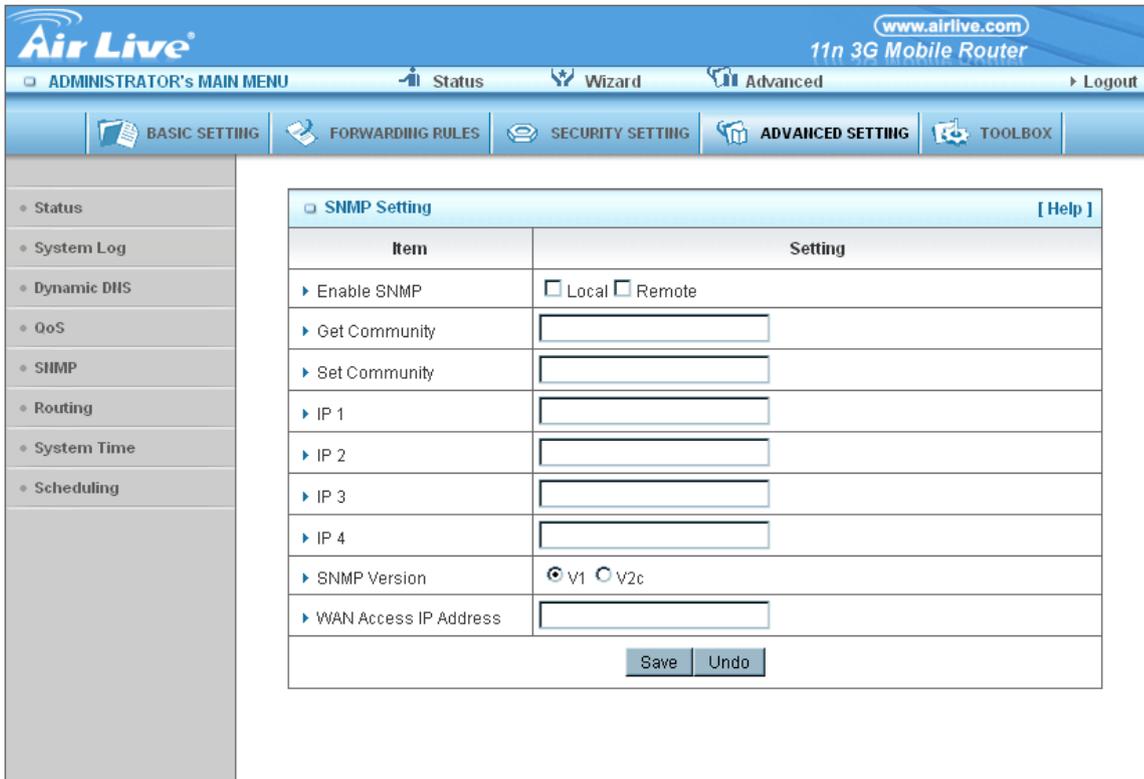
This defines the priority level of the current Policy Configuration. Packets associated with this policy will be serviced based upon the priority level set. For critical applications High or Normal levels are recommended. For non-critical applications select a Low level.

8. User Rule#

The QoS item can work with Scheduling Rule number#. Please reference the section 4.7.7 schedule.

Click on “Save” to store what you just select or “Undo” to give up

■ SNMP



Item	Setting
▶ Enable SNMP	<input type="checkbox"/> Local <input type="checkbox"/> Remote
▶ Get Community	<input type="text"/>
▶ Set Community	<input type="text"/>
▶ IP 1	<input type="text"/>
▶ IP 2	<input type="text"/>
▶ IP 3	<input type="text"/>
▶ IP 4	<input type="text"/>
▶ SNMP Version	<input checked="" type="radio"/> V1 <input type="radio"/> V2c
▶ WAN Access IP Address	<input type="text"/>

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

1. Enable SNMP

You must check Local, Remote or both to enable SNMP function. If Local is checked, this device will response request from LAN. If Remote is checked, this device will response request from WAN.

2. Get Community

Setting the community of GetRequest your device will response.

3. 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.

4. **SNMP Version**

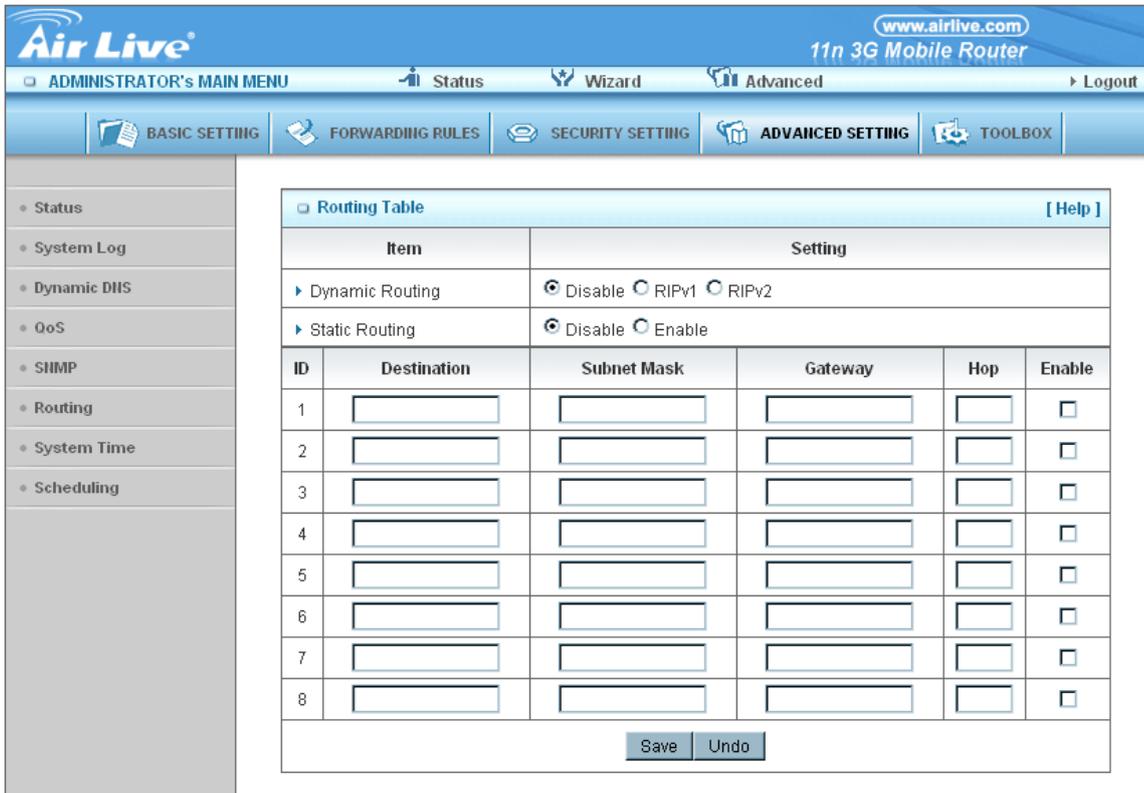
Please select proper SNMP Version that your SNMP Management software supports.

5. **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 what you just select or “Undo” to give up.

■ Routing



The screenshot shows the 'Routing Table' configuration page in the Air Live web interface. The page has a blue header with the Air Live logo and '11n 3G Mobile Router'. Below the header is a navigation bar with tabs for 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. A secondary navigation bar contains 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. On the left is a sidebar menu with options like 'Status', 'System Log', 'Dynamic DNS', 'QoS', 'SHMP', 'Routing', 'System Time', and 'Scheduling'. The main content area is titled 'Routing Table' and includes a '[Help]' link. It contains two sections: 'Dynamic Routing' with radio buttons for 'Disable', 'RIPv1', and 'RIPv2'; and 'Static Routing' with radio buttons for 'Disable' and 'Enable'. Below these is a table with 8 rows and 6 columns: ID, Destination, Subnet Mask, Gateway, Hop, and Enable. Each cell in the table contains an input field. At the bottom of the table are 'Save' and 'Undo' buttons.

Routing Table		[Help]			
Item	Setting				
Dynamic Routing	<input checked="" type="radio"/> Disable <input type="radio"/> RIPv1 <input type="radio"/> RIPv2				
Static Routing	<input checked="" type="radio"/> Disable <input type="radio"/> Enable				
ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

1. 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 and dynamic routing.

2. 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.

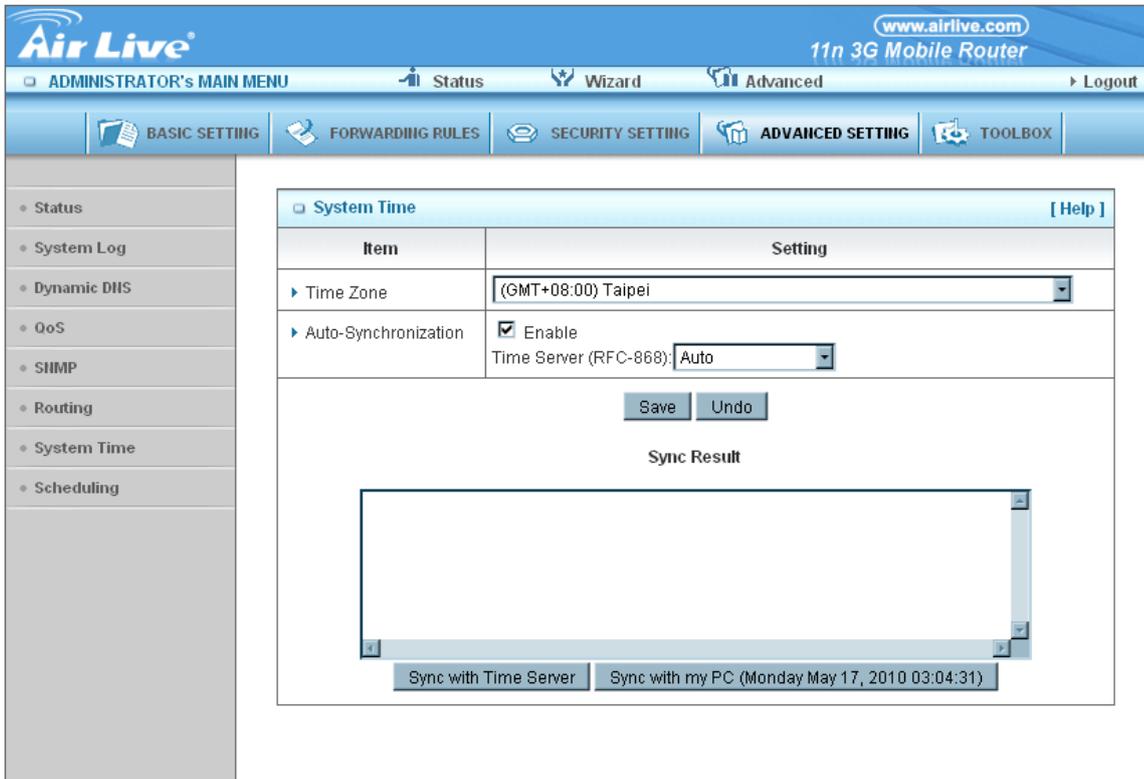
3. Static Routing



For static routing, you can specify up to 8 routing rules. You can enter the destination IP address, subnet mask, gateway, hop for each routing rule, and then enable or disable the rule by checking or un-checking the Enable checkbox.

Click on “Save” to store what you just select or “Undo” to give up.

■ System Time



The screenshot shows the 'System Time' configuration page in the Air Live web interface. The page has a blue header with the Air Live logo and '11n 3G Mobile Router'. Below the header is a navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. A secondary navigation bar contains 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. On the left is a sidebar menu with items like 'Status', 'System Log', 'Dynamic DNS', 'QoS', 'SIIMP', 'Routing', 'System Time', and 'Scheduling'. The main content area is titled 'System Time' and contains a table with the following settings:

Item	Setting
Time Zone	(GMT+08:00) Taipei
Auto-Synchronization	<input checked="" type="checkbox"/> Enable
Time Server (RFC-868):	Auto

Below the table are 'Save' and 'Undo' buttons. A 'Sync Result' section contains a large empty text box. At the bottom of the page are two buttons: 'Sync with Time Server' and 'Sync with my PC (Monday May 17, 2010 03:04:31)'.

1. Time Zone

Select a time zone where this device locates.

2. Auto-Synchronization

Select the "Enable" item to enable this function.

3. Time Server

Select a NTP time server to consult UTC time

4. Sync with Time Server

Select if you want to set Date and Time by NTP Protocol.

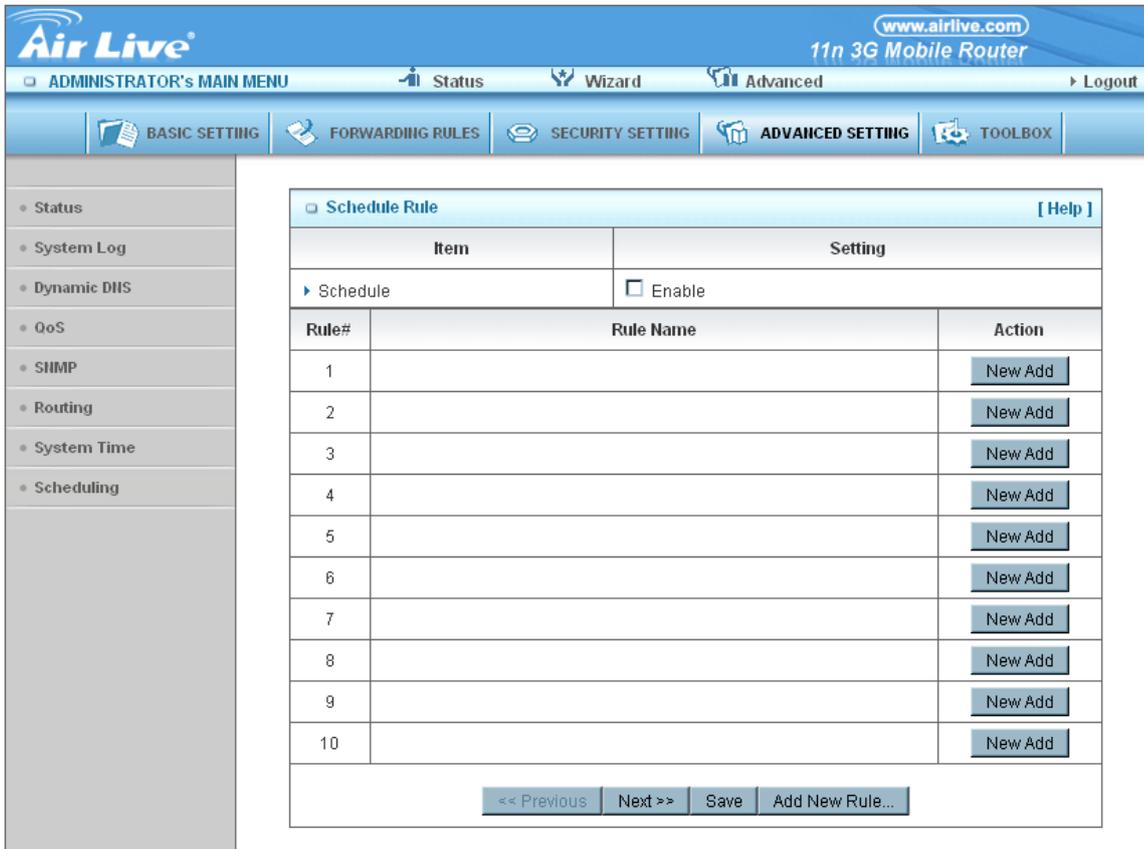
5. Sync with my PC

Select if you want to set Date and Time using PC's Date and Time



Click on “Save” to store what you just select or “Undo” to give up.

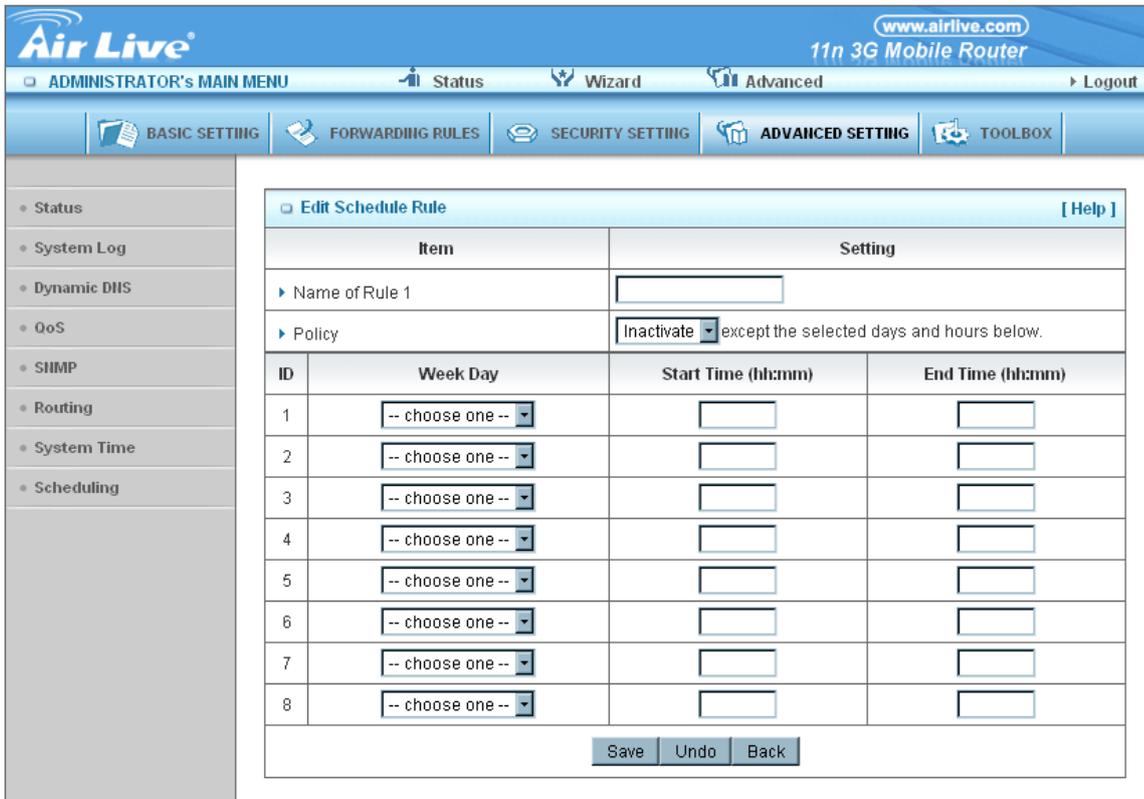
■ Scheduling



The screenshot shows the web interface for the Air Live 11n 3G Mobile Router. The top navigation bar includes the Air Live logo, the website URL (www.airlive.com), the device name (11n 3G Mobile Router), and menu items for ADMINISTRATOR's MAIN MENU, Status, Wizard, Advanced, and Logout. Below this is a secondary navigation bar with tabs for BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING, and TOOLBOX. A left sidebar contains a list of configuration categories: Status, System Log, Dynamic DNS, QoS, SHMP, Routing, System Time, and Scheduling. The main content area is titled "Schedule Rule" and includes a "[Help]" link. It features a table with two columns: "Item" and "Setting". Under the "Item" column, there is a "Schedule" section with a "Schedule" sub-section containing a "Schedule" table. The "Schedule" table has three columns: "Rule#", "Rule Name", and "Action". The "Action" column contains "New Add" buttons for each rule number from 1 to 10. Below the table, there are navigation buttons: "<< Previous", "Next >>", "Save", and "Add New Rule...".

Schedule Rule		[Help]
Item	Setting	
▶ Schedule	<input type="checkbox"/> Enable	
Rule#	Rule Name	Action
1		New Add
2		New Add
3		New Add
4		New Add
5		New Add
6		New Add
7		New Add
8		New Add
9		New Add
10		New Add

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



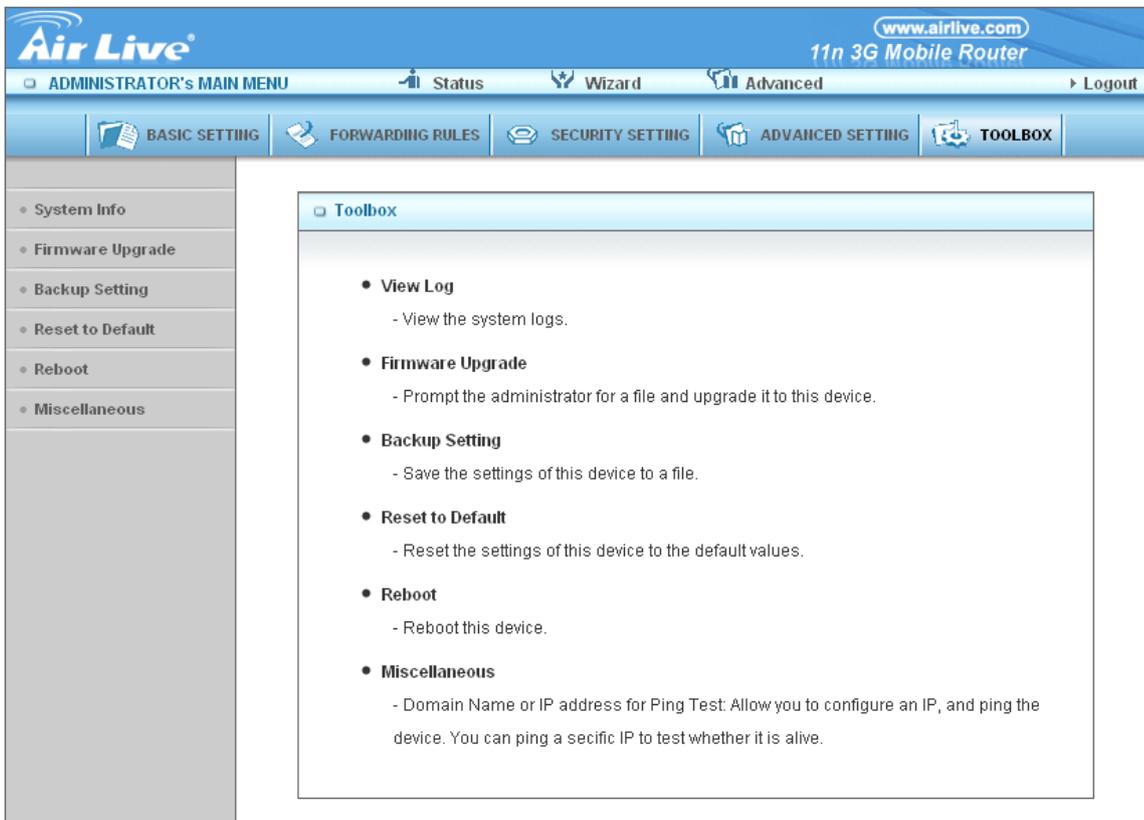
The screenshot shows the 'Edit Schedule Rule' configuration page in the Air Live web interface. The page includes a navigation menu with options like 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. The main content area is titled 'Edit Schedule Rule' and contains the following fields and table:

- Name of Rule 1:** A text input field.
- Policy:** A dropdown menu set to 'Inactivate' with the text 'except the selected days and hours below.'
- Schedule Table:** A table with 8 rows, each representing a day of the week. Each row has columns for 'ID', 'Week Day' (a dropdown menu), 'Start Time (hh:mm)', and 'End Time (hh:mm)'. All 'Week Day' dropdowns are currently set to '-- choose one --'.
- Buttons:** 'Save', 'Undo', and 'Back' buttons are located at the bottom of the table.

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

Click on “Save” to store what you just select.

3.2.5 Tool Box

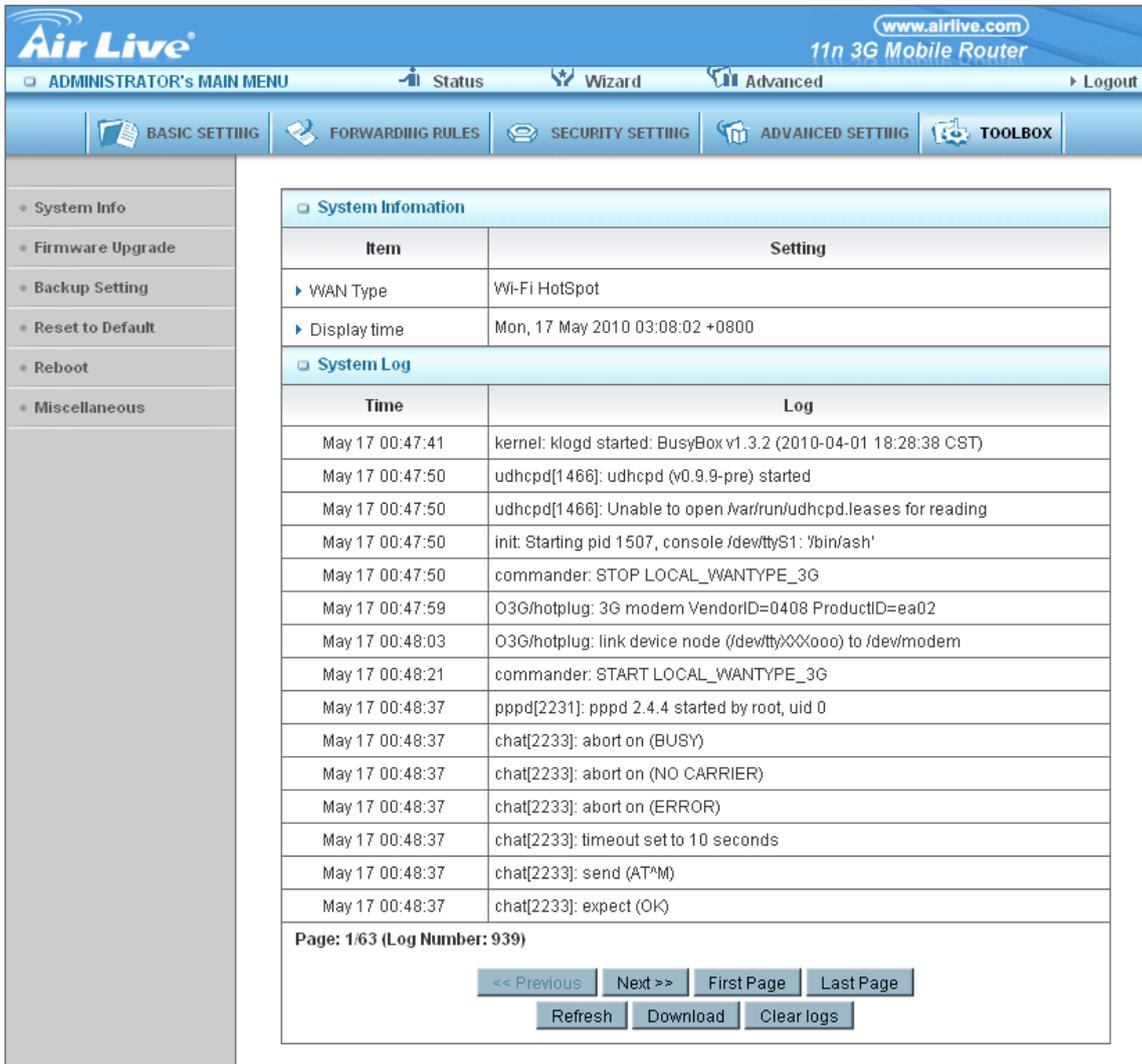


The screenshot displays the web-based configuration interface for an Air Live 11n 3G Mobile Router. The top navigation bar includes the Air Live logo, the website URL www.airlive.com, the device model "11n 3G Mobile Router", and a "Logout" button. Below this, a secondary menu contains "ADMINISTRATOR'S MAIN MENU", "Status", "Wizard", "Advanced", and "Logout". A third menu bar features "BASIC SETTING", "FORWARDING RULES", "SECURITY SETTING", "ADVANCED SETTING", and "TOOLBOX".

The "TOOLBOX" section is expanded, showing a list of utility functions:

- **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**
 - 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.

■ System Info



The screenshot shows the web interface of the Air Live 11n 3G Mobile Router. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this are tabs for 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. On the left, a sidebar menu lists 'System Info', 'Firmware Upgrade', 'Backup Setting', 'Reset to Default', 'Reboot', and 'Miscellaneous'. The main content area is divided into two sections: 'System Information' and 'System Log'.

System Information

Item	Setting
▶ WAN Type	Wi-Fi HotSpot
▶ Display time	Mon, 17 May 2010 03:08:02 +0800

System Log

Time	Log
May 17 00:47:41	kernel: klogd started: BusyBox v1.3.2 (2010-04-01 18:28:38 CST)
May 17 00:47:50	udhcpd[1466]: udhcpd (v0.9.9-pre) started
May 17 00:47:50	udhcpd[1466]: Unable to open /var/run/udhcpd.leases for reading
May 17 00:47:50	init: Starting pid 1507, console /dev/ttyS1: /bin/ash'
May 17 00:47:50	commander: STOP LOCAL_WANTYPE_3G
May 17 00:47:59	O3G/hotplug: 3G modem VendorID=0408 ProductID=ea02
May 17 00:48:03	O3G/hotplug: link device node (/dev/ttyXXX000) to /dev/modem
May 17 00:48:21	commander: START LOCAL_WANTYPE_3G
May 17 00:48:37	pppd[2231]: pppd 2.4.4 started by root, uid 0
May 17 00:48:37	chat[2233]: abort on (BUSY)
May 17 00:48:37	chat[2233]: abort on (NO CARRIER)
May 17 00:48:37	chat[2233]: abort on (ERROR)
May 17 00:48:37	chat[2233]: timeout set to 10 seconds
May 17 00:48:37	chat[2233]: send (AT^M)
May 17 00:48:37	chat[2233]: expect (OK)

Page: 1/63 (Log Number: 939)

Navigation buttons: << Previous, Next >>, First Page, Last Page, Refresh, Download, Clear logs

You can view the System Information and System log.

And download/clear the System log, in this page.

■ Firmware Upgrade

You can upgrade firmware by clicking “Upgrade” button.

■ 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 reference the Section 3.2.5.2 **Firmware Upgrade**.

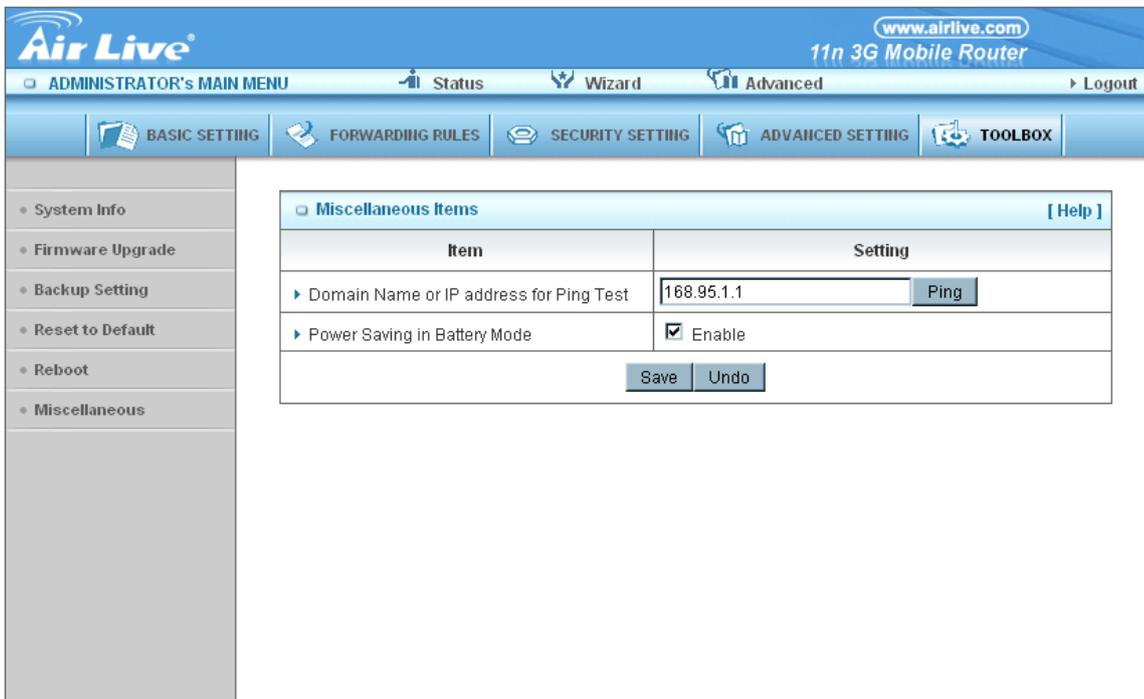
■ Reset to Default

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

■ Reboot

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

■ Miscellaneous



The screenshot shows the web interface of the Air Live 11n 3G Mobile Router. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a list of menu items: 'System Info', 'Firmware Upgrade', 'Backup Setting', 'Reset to Default', 'Reboot', and 'Miscellaneous'. The main content area is titled 'Miscellaneous Items' and contains a table with two columns: 'Item' and 'Setting'.

Item	Setting
▶ Domain Name or IP address for Ping Test	168.95.1.1 <input type="button" value="Ping"/>
▶ Power Saving in Battery Mode	<input checked="" type="checkbox"/> Enable

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

1. 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.

2. Domain Name or IP address for Ping Test

You can key in URL or IP address, and then click the "Ping" button for test.

4

Troubleshooting

This section provides an overview of common issues, and possible solutions for the installation and operation of the Traveler 3G II .

1. Unable to access the Configuration Menu when I use my computer to configure the router. Why?

Note: It is recommended that you use an Ethernet connection to configure the

Ensure that the **Ethernet LED** on the Traveler 3G II is **ON**.

If the **LED** is **NOT ON**, check to see if the cable for the Ethernet connection is securely inserted.

Note: Ensure that the **IP Address** is in the same range and subnet as the Traveler 3G II . The IP Address of the Traveler 3G II is 192.168.1.1. All the computers on the network must have a unique IP Address within the same range (e.g., 192.168.123.x). Any computers that have identical IP Addresses will not be visible on the network. All computers must also have the same subnet mask (e.g., 255.255.255.0).

Do a **Ping test** to make sure that the Traveler 3G II is responding.

Go to **Start > Run**.

1: Type **cmd**.

2: Press **Enter**.

3: Type "**ping 192.168.1.1**". A successful ping shows four replies.

Note: If you have changed the **default** IP Address, ensure you ping the correct IP Address assigned to the Traveler 3G II .

Ensure that your Ethernet Adapter is working properly, and that all network drivers are installed properly.

Note: Network adapter names will vary depending on your specific adapter. The installation steps listed below are applicable for all network adapters.

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

2: Why my wireless client can NOT access the Internet?

Note: Establish WiFi Connection. As long as you select either **WEP** or **WPA-PSK** encryption, ensure encryption settings match your WiFi settings. Please refer to your WiFi adapter documentation for additional information.

Ensure that the wireless client is associated and joined with the correct Access Point.

To check this connection, follow the steps below:

1. **Right-click** on the **Local Area Connection icon** in the taskbar.
2. Select **View Available Wireless Networks in Wireless Configure**. The **Connect to Wireless Network** screen appears. Ensure you have selected the correct available network.

Ensure the IP Address assigned to the wireless adapter is within the same subnet as the Access Point and gateway. The Traveler 3G II has an IP Address of **192.168.1.1**. Wireless adapters must have an IP Address in the same range (e.g., 192.168.123.x). Although the subnet mask must be the same for all the computers on the network, no two devices may have the same IP Address. Therefore, each device must have a unique IP

Address.

To check the **IP Address** assigned to the wireless adapter, follow the steps below:

1. Enter ipconfig /all in command mode
2. Enter ping 192.168.1.1. to check if you can access the Traveler 3G II

3. Why does my wireless connection keep dropping?

You may try following steps to solve.

- Antenna Orientation.
 - 1: Try different antenna orientations for the Traveler 3G II .
 - 2: Try to keep the antenna at least 6 inches away from the wall or other objects.
- Try changing the channel on the Traveler 3G II , and your Access Point and Wireless adapter to a different channel to avoid interference.
- Keep your product away (at least 3-6 feet) from electrical devices that generate RF noise, like microwaves, monitors, electric motors, etc.

4. Why I am unable to achieve a wireless connection?

Note: An Ethernet connection is required to troubleshoot the Traveler 3G II .

If you have enabled Encryption on the Traveler 3G II , you must also enable encryption on all wireless clients in order to establish a wireless connection.

- For 802.11g, the encryption settings are: 64 or 128 bit. Ensure that the encryption bit level is the same for both the Traveler 3G II , and your Wireless Client.
- Ensure that the SSID (Service Set Identifier) on the Traveler 3G II and the Wireless Client are exactly the same.

If they are not, your wireless connection will not be established.

- Move the Traveler 3G II and the wireless client into the same room, and then test the wireless connection.
- Disable all security settings such as **WEP**, and **MAC Address Control**.
- Turn off the Traveler 3G II and the client.

Turn the Traveler 3G II back on again, and then turn on the client.

- Ensure that all devices are set to **Infrastructure** mode.
- Ensure that the LED indicators are indicating normal activity. If not, ensure that the AC power and Ethernet cables are firmly connected.
- Ensure that the IP Address, subnet mask, gateway and DNS settings are correctly entered for the network.
- If you are using 2.4GHz cordless phones, X-10 equipment, or other home security systems, ceiling fans, or lights, your wireless connection may degrade dramatically, or drop altogether.

To avoid interference, change the Channel on the Traveler 3G II , and all devices in your network.

- Keep your product at least 3-6 feet away from electrical devices that generate RF noise. Examples include: microwaves, monitors, electric motors, and so forth.

5. I just do not remember my encryption key. What should I do?

- If you forgot your encryption key, the WiFi card will be unable to establish a proper connection.

If an encryption key setting has been set for the Traveler 3G II , it must also be set for the WiFi card that will connect to the Traveler 3G II .

To reset the encryption key(s), login to the Traveler 3G II using a wired connection. (Please refer to “Basic > Wireless (Security–No Encryption)” on page 10, for additional information).

6. How do I reset my Traveler 3G II to its factory default settings?

If other troubleshooting methods have failed, you may choose to **Reset** the Traveler 3G II to its factory default settings.

To hard-reset the Traveler 3G II its factory **default** settings, follow the steps listed below:

1. Ensure the Traveler 3G II is powered on
2. Locate the **Reset** button on the back of the Traveler 3G II .
3. Use a paper clip to press the **Reset** button.
4. Hold for 8 seconds and then release.
5. After the Traveler 3G II reboots, it is reset to the factory **default** settings.

Note: Please note that this process will take a few minutes.

7. What is VPN?

- VPN stands for “Virtual Private Networking.” VPNs create a "tunnel" through an existing Internet connection using PPTP (Point-to-Point Tunneling Protocol) or IPSec (IP Security) protocols with various encryption schemes including Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) .
- This feature allows you to use your existing Internet connection to connect to a remote site with added security. If your VPN connection is not functional, verify that your VPN dial-up configuration is correct.

Note: This information should be provided to you from your VPN provider.

Pressing the Reset Button restores to its original factory **default** settings.

8. What can I do if my Ethernet cable does not work properly?

- First, ensure that there is a solid cable connection between the Ethernet port on the Router, and your NIC (Network Interface Card).

- Second, ensure that the settings on your NIC adapter are “Enabled,” and set to accept an IP address from the DHCP.
- If settings appear to be correct, ensure that you are *not* using a crossover Ethernet cable. Although the Traveler 3G II is MDI/MDIX compatible, not all NICs are. Therefore, it is recommended that you use a patch cable when possible.

Technical Support 45

5

Technical Specifications

3G Access	USB port
Standards	IEEE 802.11 b/g IEEE 802.3 IEEE 802.3u
Wireless	
Standard	IEEE 802.11 B/G/N
Data Rate	54, 48, 36, 24, 18, 12, 9, and 6 Mbps per channel, Auto Fall-Back
Frequency	2.4 – 2.462 GHz, CCK / OFDM modulation
Range Coverage	Tx/Rx power 18dbm/Per Cell indoors approx. 35-100 meters; outdoors up to 100-300 meters
# of Channels	1-11 for N. America (FCC);1-11 for Canada (DOC) 1-13 Europe (Except Spain and France) (ETSI) 1-14 Japan (TELEC);
Security	64-bit and 128-bit WEP Encryption; WPA encryption
Antenna	Internal Pi-Pa Antenna
Firewall	IP Filtering NAT (Network Address Translation) with VPN Pass through MAC Filtering
Supported WAN type	3G,Static IP, Dynamic IP, PPPoE, PPTP, L2TP
Connection Scheme	Connect-on-demand, Auto-Disconnect
NAT function	Class C ;One-to-Many; Max 253 Users; Virtual Server; DMZ Host
VPN	PPTP, L2TP and IPSec Pass Through
Config.& Management	Web-Based IE, Navigator browser and SNMP
	DHCP Server and Client
Working Environment	Temperature: 0~40°C, Humidity 10%~90% non-condensing
OS supported	Windows 95/98/ME/NT/2000/XP; Linux
Power	Switching 5V 2.5A
Battery	Li-ion battery, 1700mAH.