



MIMO XR™ Wireless Broadband Router

Model # AR525W

User's Manual

Ver. 1B

Table of Contents

1. Introduction.....	3
2. Connecting the Router	4
3. Verifying Connection to the Router.....	5
4. Configuring the Router	8
Cable Modem.....	9
DSL.....	10
5. Connecting to the Router Wirelessly	11
6. Web Configuration Utility	12
6.1 Setup	12
6.1.1 Basic Setup.....	12
6.1.2 DDNS.....	14
6.1.3 MAC Address Clone.....	15
6.1.4 Advanced Routing	16
6.2. Wireless.....	17
6.2.1 Basic Wireless Settings.....	17
6.2.2 Wireless Security	18
WEP	18
WPA.....	19
WPA with RADIUS.....	20
6.2.3 Wireless MAC Filter.....	21
6.2.4 Advanced Wireless Settings	22
6.3 Security	23
6.3.1 Firewall	23
6.3.2 VPN Passthrough.....	24
6.4 Access Restrictions	25
6.4.1 Internet Access Policy.....	25
6.5 Applications & Gaming	28
6.5.1 Single Port Forwarding	28
6.5.2 Port Range Forwarding	29
6.5.3 Port Range Triggering.....	30
6.5.4 DMZ.....	31
6.5.5 QoS	32
6.6 Administration	33
6.6.1 Management.....	33
6.6.2 Log	34
6.6.3 Diagnostics.....	35
6.6.4 Factory Defaults.....	36
6.6.5 Firmware Upgrade	37
6.7 Status.....	38
6.7.1 Router.....	38
6.7.2 Local Network	39
6.7.3 Wireless Network.....	40
7. Troubleshooting	41
Technical Support	42

1. Introduction

Congratulations on your purchase of this MIMO XR™ Wireless Broadband Router. The MIMO XR™ Wireless Broadband Router allows Internet sharing and creates a dynamic wireless network for you to access your network with greater mobility. When used with other Airlink101™ MIMO XR™ wireless products, the wireless signal range extends farther than standard 802.11g products. Best of all the MIMO XR™ Wireless Broadband Router is backwards-compatible with existing 802.11g and 802.11b network devices.

This product is specifically designed for Small Office and Home Office needs. It provides a complete SOHO solution for Internet surfing and is easy to configure and operate even for non-technical users. Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read this manual carefully for proper operation of this product.

Package Contents

Before you begin the installation, please check the items of your package:

- One MIMO XR™ Wireless Broadband Router
- One RJ-45 cable
- Three Detachable Antennas
- One Power Adapter
- One Quick Installation Guide
- One Manual CD

If any item contained is damaged or missing, please contact your local dealer immediately. Also, keep the box and packaging materials in case you need to ship the unit in the future.

2. Connecting the Router

Note: Prior to connecting the router, be sure to power off your computer, DSL/Cable modem, and the router. To achieve maximum wireless coverage, tilt the router's antennas outward at 45° angle.

Step 1 Connect one end of a network cable to the **WAN** port of the router and connect the other end of the cable to the DSL/Cable modem.

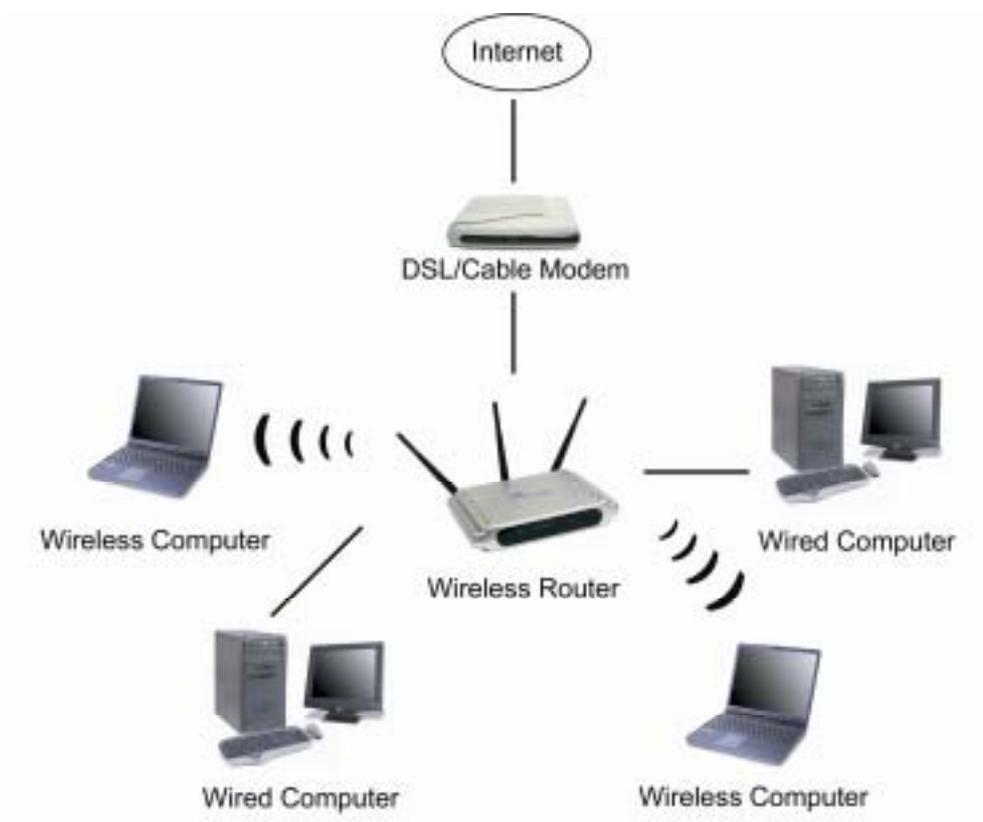
Step 2 With another network cable, connect one end of the cable to your computer's network card and connect the other end to one of the **LAN** ports of the router.

Step 3 Power on the DSL/Cable modem and wait for the lights on the modem to settle down.

Step 4 Power on the router by connecting one end of the supplied power adapter to the power jack of the router and connecting the other end to an electrical outlet.

Step 5 Power on your computer.

Step 6 Make sure the **WAN**, **WLAN**, and the **LAN** ports that the computer is connected to are lit. If not, try the above steps again.



3. Verifying Connection to the Router

Step 1 Go to **Start, Run**, type **command** (for Windows 95/98/ME) or **cmd** (for Windows 2000/XP) and click **OK**. You will see the command prompt as below.

Step 2 Type **ping 192.168.1.1** and press **Enter**. You should get four reply responses back.

```
C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Owner>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Documents and Settings\Owner>
```

Step 3 If you get **Request timed out**, or **Destination host unreachable**, double-check the network cable connection between the computer and the router and try **Step 2** again. If you still encounter problem, go to the next step; otherwise proceed to **Section 3, Configure the Router**.

Step 4 For Windows 2000/XP, type **ipconfig/release** and press **Enter**.

```
C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

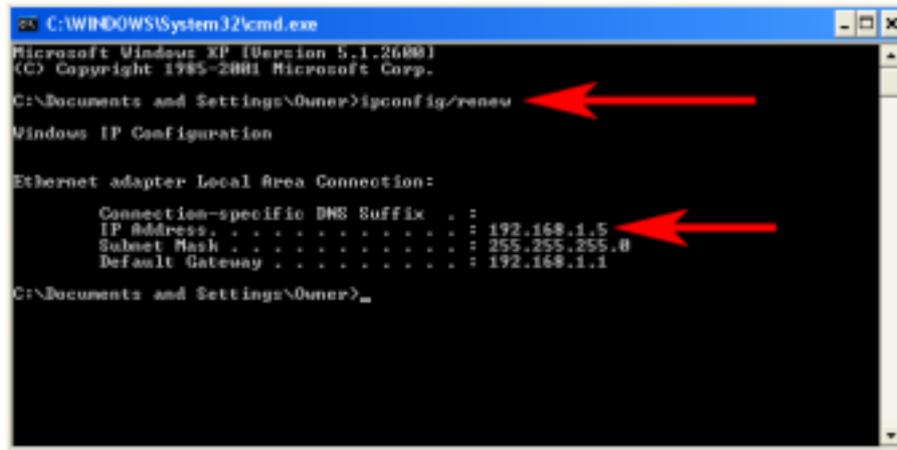
C:\Documents and Settings\Owner>ipconfig/release
Windows IP Configuration

Ethernet adapter Local Area Connection:

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

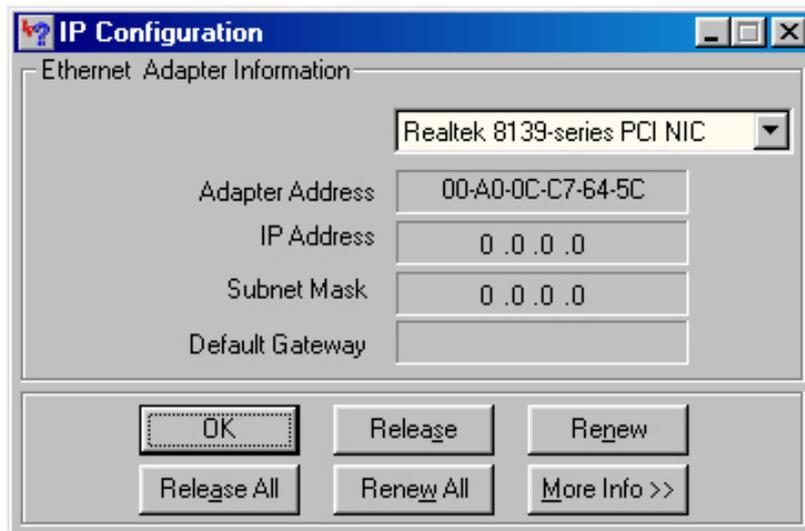
C:\Documents and Settings\Owner>
```

Step 5 Type **ipconfig/renew** and press **Enter**. You should get an IP address of **192.168.1.x** (where **x** is a number between 2 - 254). Proceed to **Section 3, Configure the Router**. If you don't get an IP address, reset the router by holding in the reset button at the back of the router for 10 seconds while it is ON and try **ipconfig/renew** again.

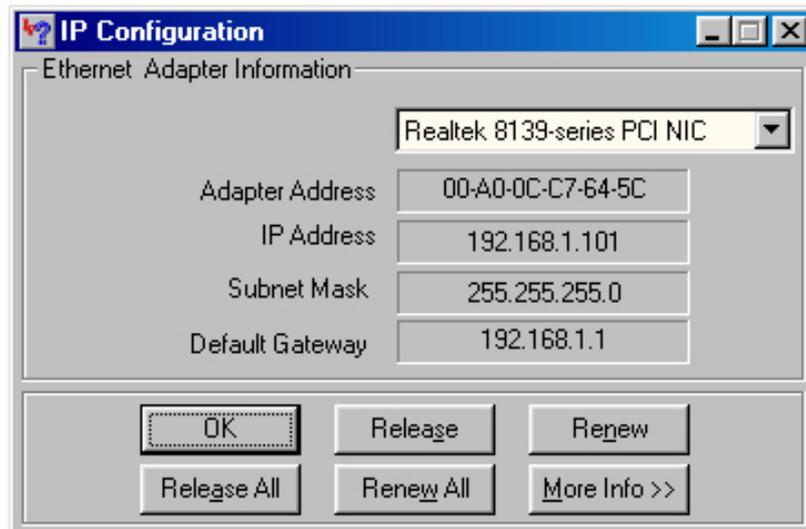


Step 6 For Windows 95/98/ME go to **Start, Run**, type **winipcfg** and click **OK**.

Step 7 Select your network card from the drop-down menu and click **Release**.

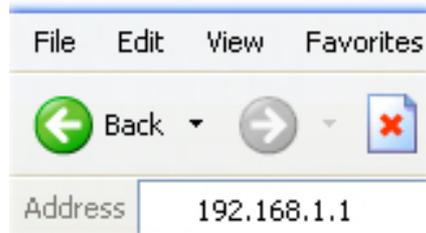


Step 8 After your IP address is released, click **Renew**. You should get an IP address of **192.168.1.x** (where **x** is a number between 2 - 254). If you don't get an IP address, reset the router by holding in the reset button at the back of the router for 10 seconds while it is ON and try **Renew** again.



4. Configuring the Router

Step 1 Open the web browser and type **192.168.1.1** in the URL Address field and press **Enter**.



Step 2 Enter **admin** for both the username and password fields and click **OK**.



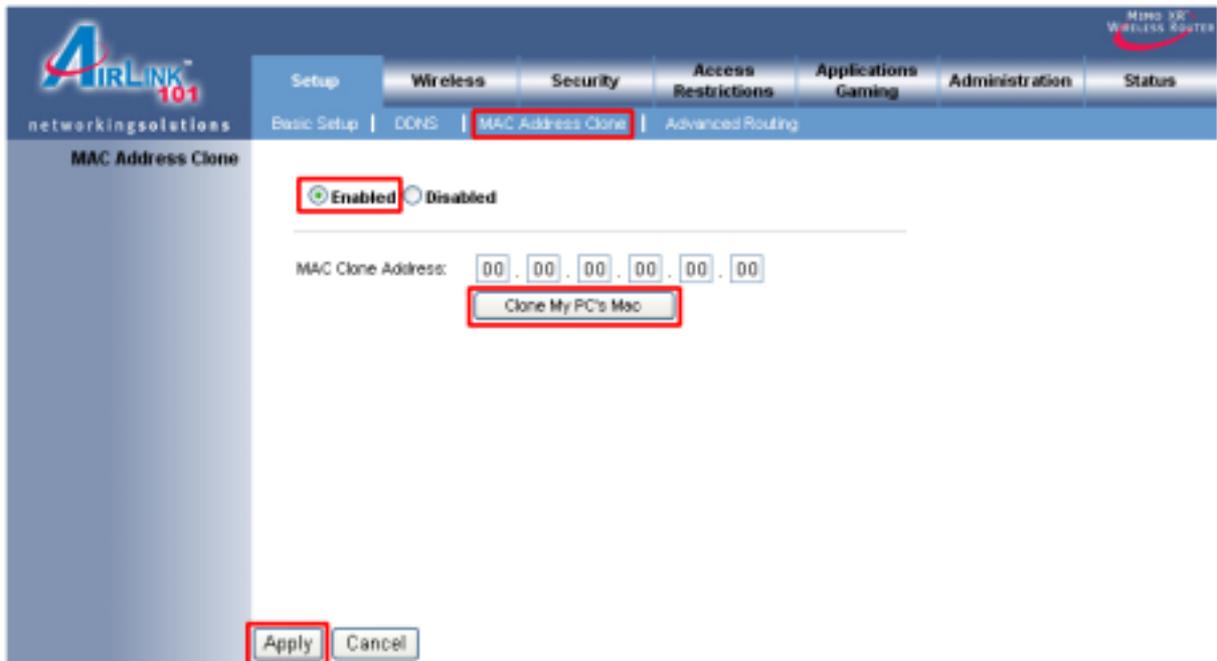
Cable Modem

For most cable modem users, you should be able to connect to the Internet without any configuration. If your ISP has provided you with a host name, enter it in the optional **Host Name** field. Click **Apply** to save the setting.



The screenshot shows the AIRLINK 101 web interface. The top navigation bar includes tabs for Setup, Wireless, Security, Access Restrictions, Applications Gaming, Administration, and Status. The 'Setup' tab is active, and the 'Basic Setup' sub-tab is selected. The 'Internet Setup' section is visible, showing the 'Internet Connection Type' set to 'Automatic Configuration - DHCP'. Below this, the 'Optional Settings (required by some Internet Service Providers)' section is expanded, showing the 'Host Name' field highlighted with a red box, the 'Domain Name' set to 'airlink101', and the 'MTU' set to 'Auto' with a 'Size' of '1500'.

If your ISP requires a registered MAC Address, click on the **MAC Address Clone** tab, select **Enabled**, and click on the **Clone My PC's MAC** button. Click **Apply** to save the setting.



The screenshot shows the AIRLINK 101 web interface with the 'MAC Address Clone' tab selected. The 'Enabled' radio button is selected and highlighted with a red box. Below it, the 'MAC Clone Address' field is shown with six '00' segments. The 'Clone My PC's Mac' button is highlighted with a red box. At the bottom of the page, the 'Apply' button is highlighted with a red box, and the 'Cancel' button is visible next to it.

If you have trouble connecting to the Internet, please refer to the **Troubleshooting** section at the end of this guide.

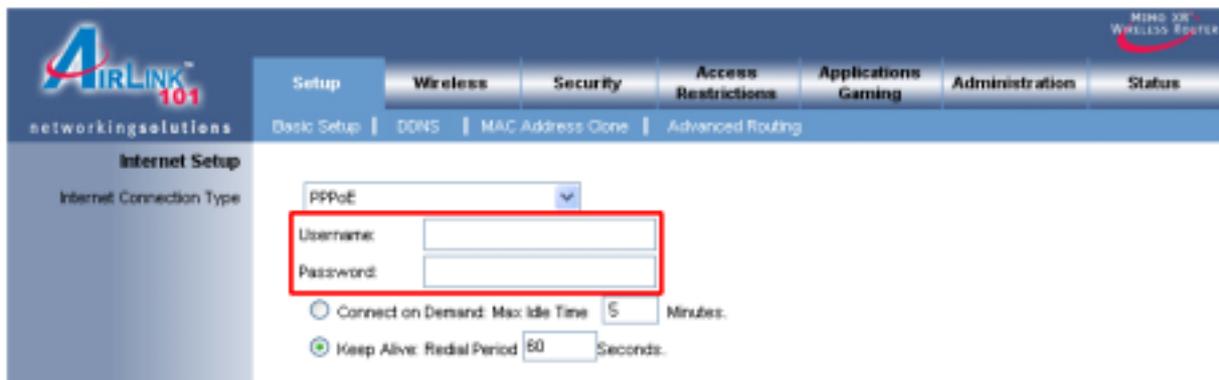
DSL

For DSL users, follow the steps below to configure the router.

Step 1 Select **PPPoE** from the drop-down menu.



Step 2 Enter your username and password provided by your ISP.



Note: Depending on the ISP, you may need to include the domain name with your username.

Example: **username@sbcglobal.net**

Step 3 Click **Apply** to save the setting.

If you have trouble connecting to the Internet, please refer to the **Troubleshooting** section at the end of this manual.

5. Connecting to the Router Wirelessly

Below are the default wireless settings of the router. You must configure your wireless network card to the same settings in order to establish a wireless connection to the router. Please refer to your wireless network card's manual on how to configure these settings.

SSID (Network Name): **default**

Operating Mode: **Infrastructure**

Authentication: **Auto**

Channel #: **6**

Encryption: **Disabled**

If you want to change the router's wireless settings, log in to the router and select the **Wireless** tab. Be sure to click **Apply** to save the setting.



6. Web Configuration Utility

This router has a built-in web configuration utility that you can use to configure the router's settings. Simply log in to the router using your computer's web browser.

6.1 Setup

6.1.1 Basic Setup

This is the default screen when you log in to the router's web configuration utility. You can setup your Internet connection here as well as configuring the DHCP settings and selecting your Time Zone.

The screenshot displays the 'Basic Setup' page of the router's web configuration utility. The page is titled 'AIRLINK 101 network solutions' and features a navigation menu with tabs for 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications (Gaming)', 'Administration', and 'Status'. The 'Setup' tab is active, and the 'Basic Setup' sub-tab is selected. The page is divided into three main sections: 'Internet Setup', 'Network Setup', and 'Time Settings'.
Internet Setup: The 'Internet Connection Type' is set to 'Automatic Configuration - DHCP'. Below this, there are fields for 'Host Name', 'Domain Name' (set to 'Airlink101'), and 'MTU' (set to 'Auto' with a 'Size' of '1500').
Network Setup: The 'Router IP' is set to 'Local IP Address: 192.168.1.1' and 'Subnet Mask: 255.255.255.0'.
DHCP Server Setting: The 'DHCP Server' is 'Enabled'. There are radio buttons for 'Enabled', 'Disabled', and 'Static DHCP'. Below this, there are fields for 'Start IP Address: 192.168.1.100', 'Maximum Number of Users: 50', and 'IP Address Range: 192.168.1.100-140'. There is also a 'Client Lease Time' field set to '0 minutes (0 means one day)'. Below these are three rows for 'Static DNS' (Static DNS 1, 2, and 3) and a row for 'WINS', each with four input fields.
Time Settings: The 'Time Zone' is set to '(GMT-08:00) Pacific Time (USA & Canada)'. There is a checkbox for 'Automatically adjust clock for daylight saving changes' which is currently unchecked.
At the bottom of the page, there are 'Apply' and 'Cancel' buttons.

Remember to click **Apply** to save your changes.

Assigning Static IP Address

If you want to assign a static IP Address to one of the computers in your network, click on the **Static DHCP** button.



Static DHCP Client List

DHCP Client Table

Assign this IP	To this MAC	Enabled
192.168.1. <input type="text"/>	<input type="text" value="00:00:00:00:00:00"/>	<input type="checkbox"/>
192.168.1. <input type="text"/>	<input type="text" value="00:00:00:00:00:00"/>	<input type="checkbox"/>
192.168.1. <input type="text"/>	<input type="text" value="00:00:00:00:00:00"/>	<input type="checkbox"/>
192.168.1. <input type="text"/>	<input type="text" value="00:00:00:00:00:00"/>	<input type="checkbox"/>
192.168.1. <input type="text"/>	<input type="text" value="00:00:00:00:00:00"/>	<input type="checkbox"/>
192.168.1. <input type="text"/>	<input type="text" value="00:00:00:00:00:00"/>	<input type="checkbox"/>
192.168.1. <input type="text"/>	<input type="text" value="00:00:00:00:00:00"/>	<input type="checkbox"/>
192.168.1. <input type="text"/>	<input type="text" value="00:00:00:00:00:00"/>	<input type="checkbox"/>
192.168.1. <input type="text"/>	<input type="text" value="00:00:00:00:00:00"/>	<input type="checkbox"/>
192.168.1. <input type="text"/>	<input type="text" value="00:00:00:00:00:00"/>	<input type="checkbox"/>

Step 1 Enter the Static IP Address in the **Assign this IP** field.

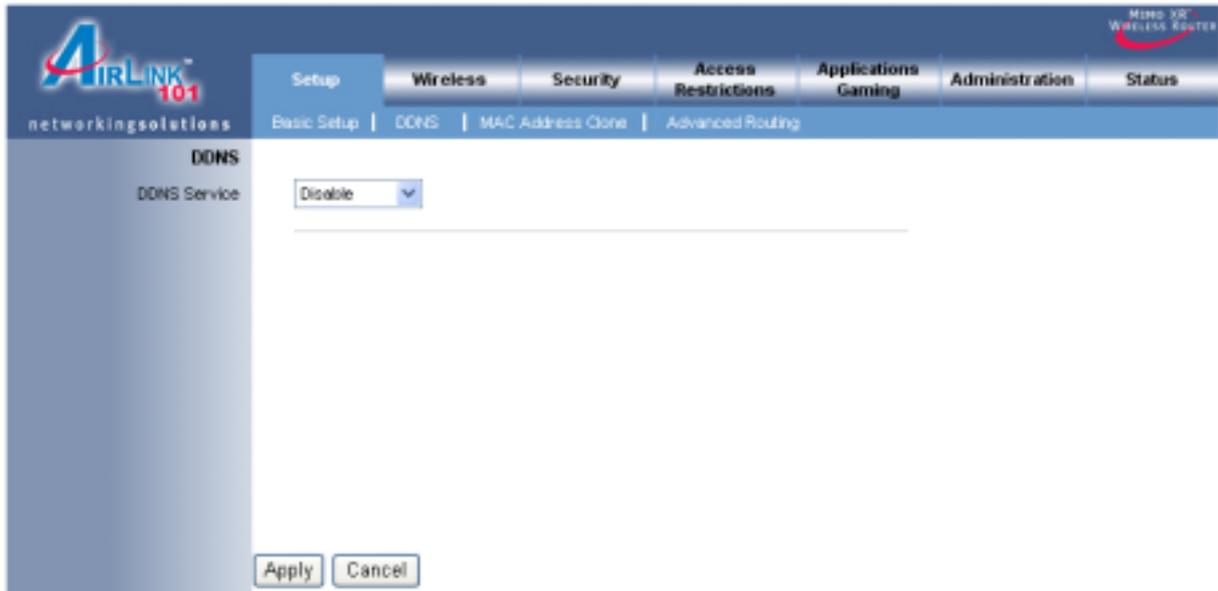
Step 2 Enter the MAC address of the corresponding computer in the **To this MAC** field.

Step 3 Check the **Enabled** box.

Step 4 Click **Save Settings**.

6.1.2 DDNS

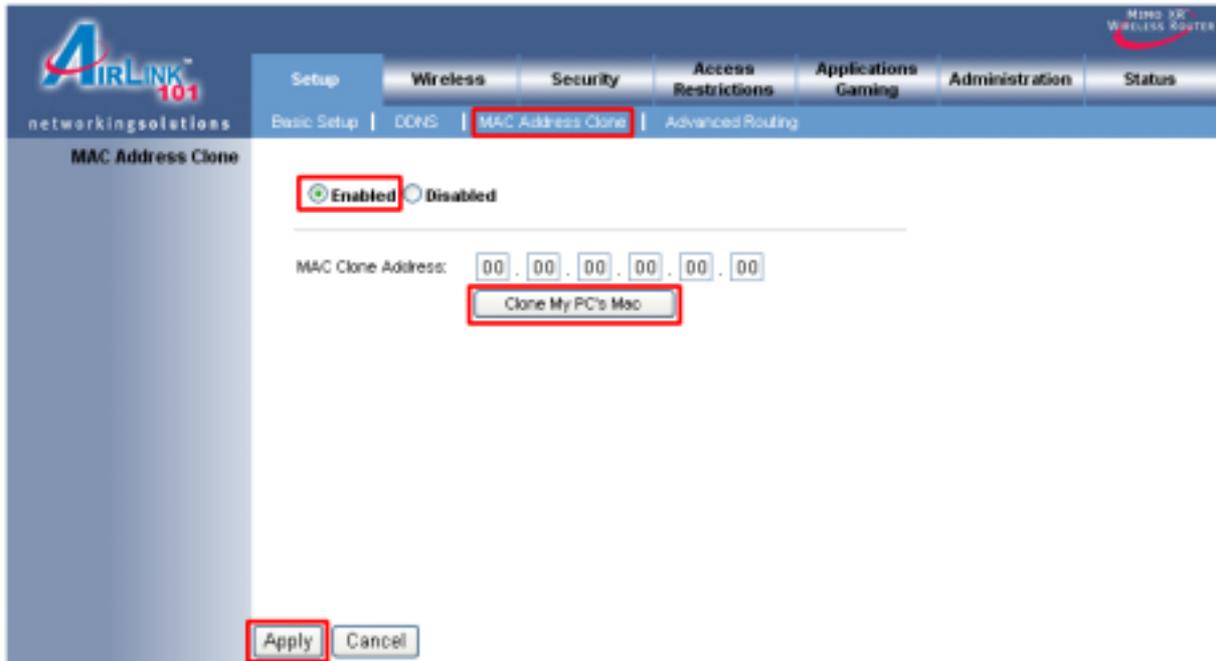
Dynamic DNS (DDNS) allows any user who wishes to access your server to reach it by a registered DNS name instead of an IP address. Before you enable **DDNS**, you need to register an account with one of the DDNS providers listed in the drop-down menu.



To Enable DDNS, select the DDNS provider you have registered with and enter the required fields. Click **Apply** to save the setting.

6.1.3 MAC Address Clone

Some ISPs require a registered MAC address to access the Internet. You can use the following steps to clone your PC's registered MAC address to access the Internet.



Step 1 Select **Enabled** from the drop-down menu.

Step 2 Click the **Clone My PC's MAC** button.

Step 3 Click **Apply** to save the setting.

6.1.4 Advanced Routing

You can configure your own static routing table using the Advanced Routing function.



The screenshot shows the configuration interface for the AIRLINK 101 wireless router. The top navigation bar includes 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications Gaming', 'Administration', and 'Status'. The 'Advanced Routing' section is active, showing options for NAT (Enabled), Dynamic Routing (RP) (Disabled), and Static Routing. The Static Routing section contains a 'Route Entries' table with one entry selected. Below the table are input fields for 'Enter Route Name', 'Destination LAN IP', 'Subnet Mask', 'Gateway', and 'Interface'. A 'Show Routing Table' button is located below the interface dropdown. At the bottom of the page are 'Apply' and 'Cancel' buttons.

Route Entries:	1 ...	Delete This Entry
Enter Route Name:		
Destination LAN IP:	0 . 0 . 0 . 0	
Subnet Mask :	0 . 0 . 0 . 0	
Gateway :	0 . 0 . 0 . 0	
Interface :	LAN & Wireless	

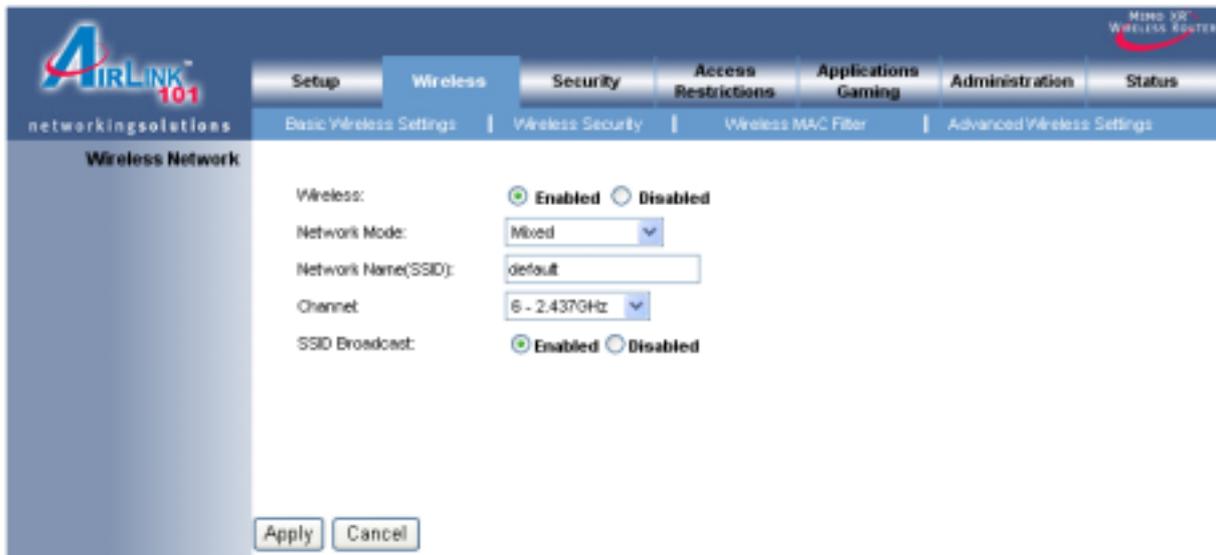
To see the current routing table, click on **Show Routing Table** button.

Be sure to click **Apply** to save each entry.

6.2. Wireless

6.2.1 Basic Wireless Settings

You can configure the router's basic wireless settings on this screen.



The screenshot shows the 'Basic Wireless Settings' page of an AIRLINK 101 router. The page has a blue header with the AIRLINK 101 logo and navigation tabs for Setup, Wireless, Security, Access Restrictions, Applications Gaming, Administration, and Status. Below the header, there are sub-tabs for Basic Wireless Settings, Wireless Security, Wireless MAC Filter, and Advanced Wireless Settings. The main content area is titled 'Wireless Network' and contains the following settings:

- Wireless: Enabled Disabled
- Network Mode:
- Network Name(SSID):
- Channel:
- SSID Broadcast: Enabled Disabled

At the bottom of the settings area, there are 'Apply' and 'Cancel' buttons.

Wireless: Select to Enable or Disable the wireless feature of the router.

Network Mode: Choose from Mixed (B & G), Wireless-B only, and Wireless-G only.

Network Name (SSID): You can change the router's SSID in this field. Once you have changed the SSID, your network clients need to re-connect themselves using the new SSID.

Channel: Select the desired channel. All the network clients need to use the same channel.

SSID Broadcast: Choose to enable or disable the broadcast of your SSID.

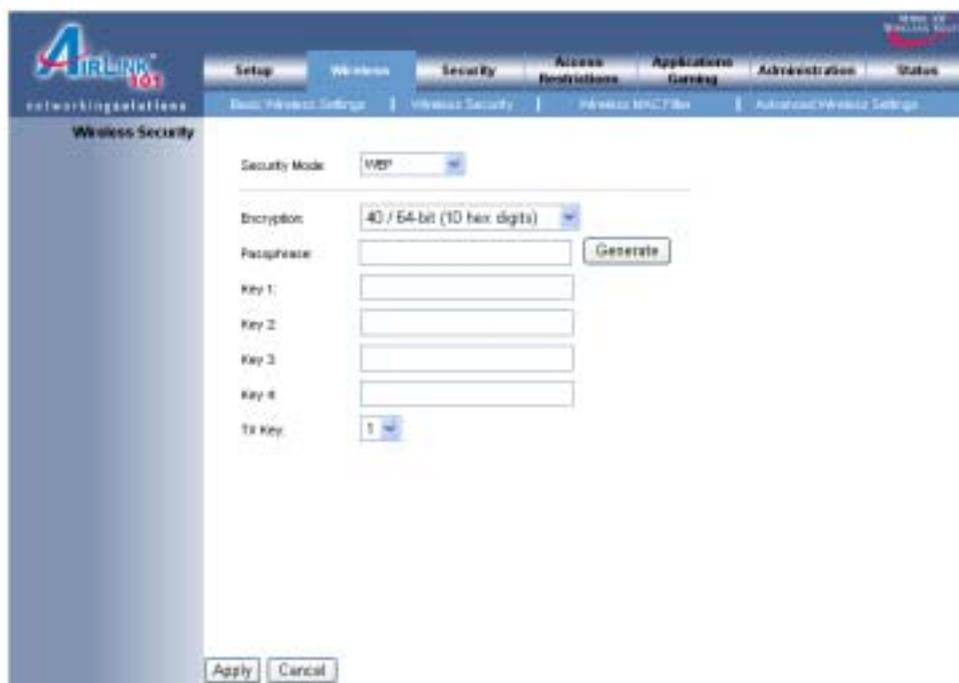
6.2.2 Wireless Security

You can configure wireless security such as WEP or WPA encryption on this screen.

Note: It is recommended that you use WPA encryption over WEP if your wireless clients support WPA. All of the wireless clients must use the same security settings in order to connect to the router.

WEP

To enable WEP, select **WEP** from the **Security Mode**.



The screenshot shows the 'Wireless Security' configuration page for an AIRLINK 101 router. The 'Security Mode' is set to 'WEP'. The 'Encryption' is set to '40 / 64-bit (10 hex digits)'. There is a 'Passphrase' field with a 'Generate' button next to it. Below the passphrase field are four input fields for 'Key 1', 'Key 2', 'Key 3', and 'Key 4'. The 'TX Key' is set to '1'. At the bottom of the page, there are 'Apply' and 'Cancel' buttons.

Encryption: Choose from **64 bits** or **128 bits**

Passphrase: You can enter a passphrase and click on the **Generate** button and the router will automatically generate four WEP keys for you.

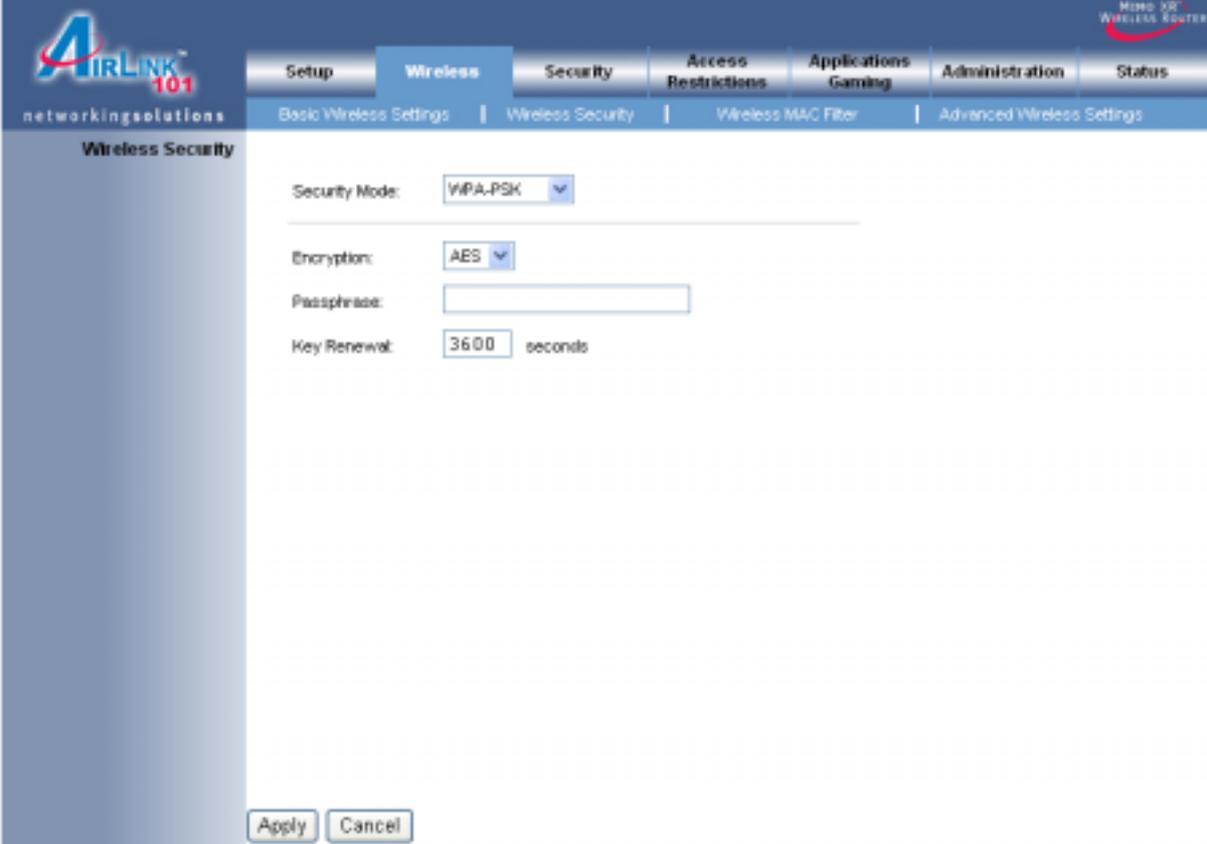
WEP Key 1 – 4: Manually assign a passphrase for each key. If you selected **64 bits** encryption, enter **10** HEX characters (0-F) for each key. If you selected **128 bits** encryption, enter **26** HEX characters (0-F) for each key.

TX Key: Select a key to be the active key.

Click **Apply** to save the setting.

WPA

To enable WPA, select **WPA-PSK** or **WPA2-PSK** from the **Security Mode**.



The screenshot shows the configuration interface for the AIRLINK 101 wireless router. The page is titled "Wireless Security" and is part of the "Wireless" settings section. The "Security Mode" is set to "WPA-PSK", the "Encryption" is set to "AES", the "Passphrase" field is empty, and the "Key Renewal" is set to "3600 seconds". The "Apply" and "Cancel" buttons are visible at the bottom of the form.

Setup	Wireless	Security	Access Restrictions	Applications Gaming	Administration	Status
Basic Wireless Settings	Wireless Security	Wireless MAC Filter	Advanced Wireless Settings			

Wireless Security

Security Mode:

Encryption:

Passphrase:

Key Renewal: seconds

Encryption: Select either **TKIP** or **AES** as the encryption method.

Passphrase: Enter a passphrase between 8 to 63 characters long.

Key Renewal: Enter the desired key renewal time in seconds.

Click **Apply** to save the setting.

WPA with RADIUS

If you are using a RADIUS server in your network for authentication, you may choose **WPA** or **WPA2** from the **Security Mode**.

The screenshot shows the configuration interface for the AIRLINK 101 wireless router. The 'Wireless Security' tab is selected, and the 'Security Mode' is set to 'WPA2'. The 'Encryption' is set to 'AES'. The 'RADIUS Server' is set to '0.0.0.0', the 'RADIUS Port' is '1812', and the 'Key Renewal' is '3600 seconds'. The 'Shared Secret' field is empty. The 'Apply' and 'Cancel' buttons are at the bottom.

Encryption Methods: Select either **TKIP** or **AES** as the encryption method. (WPA2 uses AES only).

RADIUS Server: Enter the IP Address of your RADIUS server.

RADIUS Port: Enter the port number of your RADIUS server.

Shared Secret: Enter the shared key.

Key Renewal: Enter the desired key renewal time in seconds.

Click **Apply** to save the setting.

6.2.3 Wireless MAC Filter

You can restrict certain wireless clients from accessing the router by specifying their MAC address and enabling access restriction.

The screenshot shows the configuration interface for the Wireless MAC Filter. At the top, there is a navigation bar with tabs for Setup, Wireless, Security, Access Restrictions, Applications Gaming, Administration, and Status. Below this, there are sub-tabs for Basic Wireless Settings, Wireless Security, Wireless MAC Filter, and Advanced Wireless Settings. The main content area is titled 'Wireless MAC Filter' and includes a sidebar with 'Access Restriction' and 'MAC Address Filter List' sections. The 'Enabled' radio button is selected. Below this, there are two options: 'Prevent PCs listed below from accessing the wireless network.' (selected) and 'Permit PCs listed below to access the wireless network.' A 'Wireless Client Table' contains 16 rows, each with a label (MAC 1 through MAC 16) and a text input field containing '00:00:00:00:00:00'. At the bottom, there are 'Apply' and 'Cancel' buttons.

Select **Enabled** and choose whether the specified wireless clients will be prevented or permitted to access the wireless network. Enter their MAC address in the fields below and click **Apply** to save the setting.

6.2.4 Advanced Wireless Settings

You can configure various advanced wireless settings on this screen.

The screenshot displays the 'Advanced Wireless' configuration page for an AIRLINK 101 wireless router. The page is part of a web interface with a navigation menu at the top. The 'Wireless' tab is selected, and the 'Advanced Wireless Settings' sub-tab is active. The settings are organized into several sections:

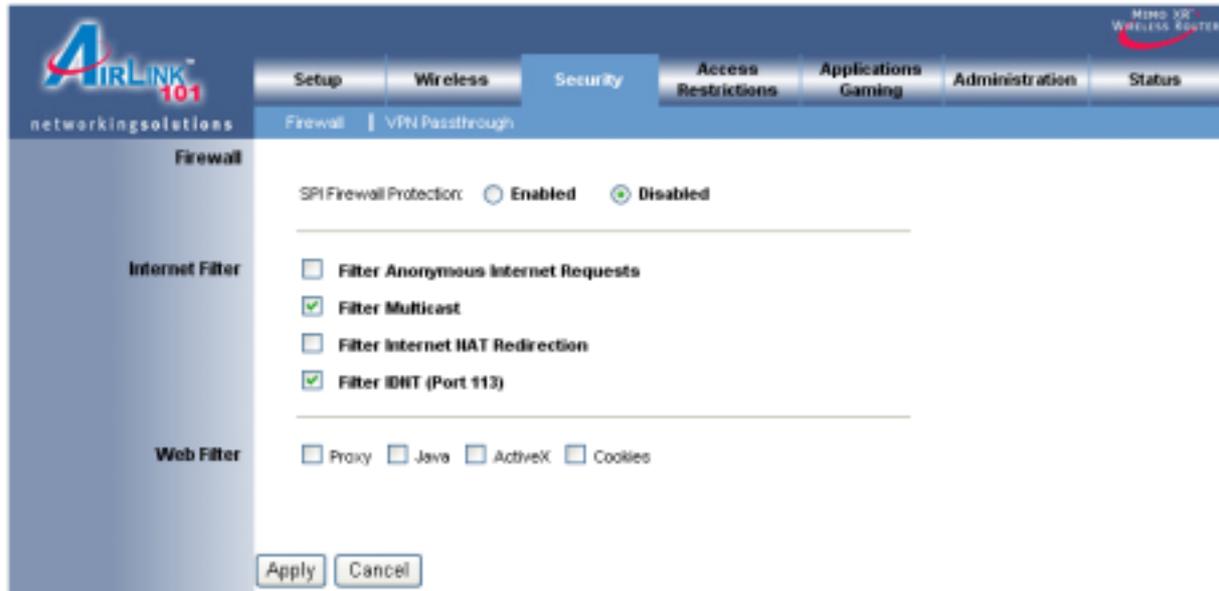
- Frame Burst Mode:** Enabled Disabled (Default: Enabled)
- AP Isolation:** Enabled Disabled (Default: Disabled)
- Authentication Type:** Auto (Default: Auto)
- Basic Rate:** Default (Default: Default)
- Transmission Rate:** Auto (Default: Auto)
- Transmission Power:** Full (Default: Full)
- CTS Protection Mode:** Auto (Default: Auto)
- Beacon Interval:** 100 (Default: 100, Milliseconds, Range: 20-1000)
- DTIM Interval:** 1 (Default: 1, Range: 1 - 255)
- Fragmentation Threshold:** 2346 (Default: 2346, Range: 256 - 2346)
- RTS Threshold:** 2346 (Default: 2346, Range: 256 - 2346)

At the bottom of the settings area, there are two buttons: 'Apply' and 'Cancel'. The 'Apply' button is highlighted with a blue border, indicating it is the recommended action to save the changes.

Click **Apply** to save the setting.

6.3 Security

6.3.1 Firewall



SPI Firewall Protection: Select to enable or disable Stateful Packet Inspection.

Internet Filter: Place a check to enable various Internet filter including Anonymous Internet Requests, Multicast packets, NAT Redirection, and IDNT port.

Web Filters: You can select to filter Proxy, Java, ActiveX, and/or Cookies.

Click **Apply** to save the setting.

6.3.2 VPN Passthrough

You can select to enable or disable the passthrough of **IPSec**, **PPTP**, and/or **L2TP**.



Click **Apply** to save the setting.

6.4 Access Restrictions

6.4.1 Internet Access Policy

You can setup policies that deny or allow specific clients to access the Internet.

The screenshot shows the 'Internet Access Policy' configuration page in the ARLINK 103 interface. The page is divided into several sections:

- Access Policy:** Includes a dropdown for 'Access Policy' (currently '1'), a 'Delete This Policy' button, and a 'Default' button.
- Enter Policy Name:** A text input field.
- Status:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- Applied PCs:** A 'URL List' button with a note: '(This Policy applies only to PCs on the List.)'
- Access restriction:** Radio buttons for 'Deny' (selected) and 'Allow'. A note says: 'Internet access during selected days and hours.'
- Schedule:** 'Days' section with checkboxes for 'Everyday', 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', 'Sat'. 'Times' section with a '24 Hours' radio button and two time range selectors (HH:MM - HH:MM).
- Inside Blocking by URL Address:** Four text input fields labeled 'URL 1' through 'URL 4'.
- Inside Blocking by Keyword:** Four text input fields labeled 'Keyword 1' through 'Keyword 4'.
- Blocked Applications:** A table with two columns: 'Applications' and 'Blocked List'. The 'Applications' column lists protocols and port ranges: DNS [53-53], HTTP [80-80], HTTPS [443-443], FTP [21-21], POP3 [110-110], SMTP [143-143], SMTP [25-25], NNTP [119-119], and SNMP [161-161]. The 'Blocked List' column has a single checkbox for each application.
- Application Name, Port Range, Protocol:** Three input fields at the bottom for adding a new application.

Buttons at the bottom include 'Apply' and 'Cancel'.

Enter Policy Name: Enter a name for the policy.

Status: Choose to enable or disable the selected policy.

PCs: Click on the **Edit List** button to specify the network clients. Policy only applies to the PCs that are in the list.

AIRLINK 101
networkingsolutions

List of PCs

MAC Address

01	00:00:00:00:00:00	06	00:00:00:00:00:00
02	00:00:00:00:00:00	07	00:00:00:00:00:00
03	00:00:00:00:00:00	08	00:00:00:00:00:00
04	00:00:00:00:00:00	09	00:00:00:00:00:00
05	00:00:00:00:00:00	10	00:00:00:00:00:00

IP Address

01	192.168.1.0	04	192.168.1.0
02	192.168.1.0	05	192.168.1.0
03	192.168.1.0	06	192.168.1.0

IP Address Range

01	192.168.1.0	-	0	03	192.168.1.0	-	0
02	192.168.1.0	-	0	04	192.168.1.0	-	0

Save Settings Cancel Changes Close

You can specify each client by its MAC Address or IP Address. You can also specify a group of clients by entering their IP Address Range. Once you have specified all the clients, click **Save Settings**.

Access Restrictions: Select to **Deny** or **Allow** the specified clients to access the Internet by **Day** and **Time**.

Access restriction

Deny Internet access during selected days and hours.

Allow

Schedule

Days: Everyday Sun Mon Tue Wed Thu Fri Sat

Times: 24 Hours 00 : 00 ~ 00 : 00

Blocked Application Port

Select which application port to block, if any, when the specified PCs have Internet access.

For your convenience, 10 preset applications and their ports are listed. If you have a custom application, manually enter its name, port range, protocol and click **Add**.

Blocked Applications

Note: only three applications can be blocked per policy.

Applications		Blocked List
DNS [53~53]		
HTTP [80~80]		
HTTPS [443~443]		
FTP [21~21]		
POP3 [110~110]	>>	
IMAP [143~143]	<<	
SMTP [25~25]		
NNTP [119~119]		
SNMP [161~161]		

Application Name	<input type="text"/>
Port Range	<input type="text"/> ~ <input type="text"/>
Protocol	TCP <input type="button" value="v"/>

Website Blocking

You can block the specified clients from accessing certain websites by URL or Keyword.

Website Blocking by URL Address	URL 1:	<input type="text"/>	URL 2:	<input type="text"/>
	URL 3:	<input type="text"/>	URL 4:	<input type="text"/>
Website Blocking by Keyword	Keyword 1:	<input type="text"/>	Keyword 2:	<input type="text"/>
	Keyword 3:	<input type="text"/>	Keyword 4:	<input type="text"/>

Enter the URL or the Keyword you wish to block.

Click **Apply** to save the setting.

To view all the policies, click the **Summary** button.

6.5 Applications & Gaming

6.5.1 Single Port Forwarding

If you want to host ftp server or online gaming, you must open up ports on the router. This page allows you to setup single port forwarding for the specified applications.

Before using forwarding, you should assign static IP addresses to the designated PCs.

The screenshot shows the 'Single Port Forwarding' configuration page in the AIRLINK 101 router's web interface. The page is titled 'Single Port Forwarding' and features a navigation menu at the top with options: Setup, Wireless, Security, Access Restrictions, Applications Gaming (selected), Administration, and Status. Below the navigation menu, there are sub-menus: Single Port Forwarding, Port Range Forwarding, Port Range Triggering, DMZ, and Qos. The main content area is divided into two sections. On the left, there is a section for 'Application Name' with five dropdown menus, each currently set to 'None'. Below these are several empty text input fields. On the right, there is a table with the following columns: External Port, Internal Port, Protocol, To IP address, and Enable. The table contains 15 rows. The first five rows have '---' in the External Port, Internal Port, and Protocol columns, and '192.168.1.0' in the To IP address column. The last ten rows have empty input fields for External Port and Internal Port, 'TCP' in the Protocol column, and '192.168.1.0' in the To IP address column. Each row has a checkbox in the Enable column. At the bottom of the page, there are 'Apply' and 'Cancel' buttons.

External Port	Internal Port	Protocol	To IP address	Enable
---	---	---	192 . 168 . 1 . 0	<input type="checkbox"/>
---	---	---	192 . 168 . 1 . 0	<input type="checkbox"/>
---	---	---	192 . 168 . 1 . 0	<input type="checkbox"/>
---	---	---	192 . 168 . 1 . 0	<input type="checkbox"/>
---	---	---	192 . 168 . 1 . 0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	TCP	192 . 168 . 1 . 0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	TCP	192 . 168 . 1 . 0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	TCP	192 . 168 . 1 . 0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	TCP	192 . 168 . 1 . 0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	TCP	192 . 168 . 1 . 0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	TCP	192 . 168 . 1 . 0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	TCP	192 . 168 . 1 . 0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	TCP	192 . 168 . 1 . 0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	TCP	192 . 168 . 1 . 0	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	TCP	192 . 168 . 1 . 0	<input type="checkbox"/>

Click **Apply** to save the setting.

6.5.2 Port Range Forwarding

If you want to host ftp server or online gaming, you must open up ports on the router. This page allows you to setup port range forwarding for the specified applications.

Before using forwarding, you should assign static IP addresses to the designated PCs.

The screenshot shows the 'Port Range Forwarding' configuration page in the Airlink 101 router's web interface. The page has a navigation bar with tabs for Setup, Wireless, Security, Access Restrictions, Applications (selected), Administration, and Status. Below the navigation bar, there are sub-tabs for Single Port Forwarding, Port Range Forwarding (selected), Port Range Triggering, DMZ, and QoS. The main content area is titled 'Port Range Forwarding' and includes a section for 'Application Name' with a list of input fields. Below this is a table with the following columns: 'Start - End Port', 'Protocol', 'To IP address', and 'Enable'. The table contains 15 rows, each with a 'Start - End Port' field, a 'Protocol' dropdown menu set to 'TCP', a 'To IP address' field, and an 'Enable' checkbox. At the bottom of the page, there are 'Apply' and 'Cancel' buttons.

Start - End Port	Protocol	To IP address	Enable
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1. <input type="text"/>	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1. <input type="text"/>	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1. <input type="text"/>	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1. <input type="text"/>	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1. <input type="text"/>	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1. <input type="text"/>	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1. <input type="text"/>	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1. <input type="text"/>	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1. <input type="text"/>	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1. <input type="text"/>	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1. <input type="text"/>	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1. <input type="text"/>	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1. <input type="text"/>	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1. <input type="text"/>	<input type="checkbox"/>
<input type="text"/> ~ <input type="text"/>	TCP	192.168.1. <input type="text"/>	<input type="checkbox"/>

Click **Apply** to save the setting.

6.5.3 Port Range Triggering

Port triggering allows the router to keep track of outgoing data for specific port numbers. The router remembers which computer sends out what data, so when the requested data returns through the router, the data is sent back to the proper computer by way of IP address and port mapping rules.

The screenshot shows the configuration interface for Port Triggering on an AIRLINK 101 router. The interface includes a navigation menu at the top with options like Setup, Wireless, Security, Access Restrictions, Applications Gaming, Administration, and Status. The 'Applications Gaming' menu is expanded to show 'Single Port Forwarding', 'Port Range Forwarding', 'Port Range Triggering', 'DMZ', and 'Gos'. The 'Port Triggering' sub-menu is selected, displaying a table with the following structure:

Application Name	Triggered Range	Forwarded Range	Enabled
	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>
	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>
	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>
	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>
	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>
	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>
	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>
	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>
	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>
	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>

At the bottom of the configuration area, there are 'Apply' and 'Cancel' buttons.

Click **Apply** to save the setting.

6.5.4 DMZ

DMZ (De-Militarized Zone) Host is a host without the protection of the router's firewall. It allows a computer to be exposed to unrestricted two-way communication with the Internet. You should only use this feature when the Port Forwarding function fails to make an application work.

Warning: Setting your computer as a DMZ host exposes it to various security vulnerabilities. This feature should be used only when needed.

The screenshot shows the Airlink 101 router's web interface. The top navigation bar includes 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications Gaming' (selected), 'Administration', and 'Status'. Below this, there are sub-menus: 'Single Port Forwarding', 'Port Range Forwarding', 'Port Range Triggering', 'DMZ', and 'Gos'. The main content area is titled 'DMZ' and contains the following settings:

- Enabled Disabled
- Source IP Address: Any IP Address, [0][0][0][0]~[0]
- Destination: IP Address: 192.168.1.[0], MAC Address: [00:00:00:00:00:00]

At the bottom of the form are 'Apply' and 'Cancel' buttons.

DMZ: Select to enable or disable DMZ.

Source IP Address: Select any source IP address or specify a source IP address.

Destination: Specify the Destination by its IP Address or MAC Address.

Note: Any DMZ host should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

Click **Apply** to save the setting.

6.5.5 QoS

QoS (Quality of Service) manages information as it is transmitted and received. It ensures better service to those applications with a higher priority.

The screenshot shows the QoS configuration interface for AIRLINK 101. The navigation tabs include Setup, Wireless, Security, Access Restrictions, Applications Gaming, Administration, and Status. The 'Applications Gaming' tab is active, showing sub-options for Single Port Forwarding, Port Range Forwarding, Port Range Triggering, DMZ, and QoS.

QoS (Quality of Service)

Wireless

WMM Support: Enabled Disabled (Default: Enabled)

No Acknowledgement: Enabled Disabled (Default: Enabled)

Internet Access Priority

Enabled Disabled

Category

Applications

Applications:	MSN Messenger
Priority:	Medium (Recommend)
<input type="button" value="Add"/>	

Summary

Priority	Name	Information		

Click **Apply** to save the setting.

6.6 Administration

6.6.1 Management

The Management screen allows you to change the router's log in password as well as other administrative settings.

The screenshot shows the 'Management' page of an Airtelink 101 router. The page is organized into several sections:

- Router Password:** Contains two password input fields for 'Router Password' and 'Re-enter to confirm', both currently showing asterisks.
- Web Access:** Includes two radio button options: 'Use HTTP' (Disabled) and 'Web Utility Access via Wireless' (Enabled).
- Remote Access:** Includes three radio button options: 'Remote Management' (Disabled), 'Use HTTP' (Disabled), and 'Remote Upgrade' (Disabled). Below these is an 'Allow Remote IP Address' section with a radio button for 'Any IP Address' and an IP address input field (0.0.0.0). A 'Remote Management Port' input field is set to 8000.
- Backup and Restore:** Features two buttons: 'Backup Configurations' and 'Restore Configurations'.
- iPoP:** Includes a radio button for 'Enabled' (selected) and 'Disabled'. Below are two sections: 'Allow Users to Configure' (Disabled) and 'Allow Users to Disable Internet Access' (Disabled).

At the bottom of the page are 'Apply' and 'Cancel' buttons.

Router Password: Set the router's log in password.

Web Access: Select to enable or disable HTTPs and Wireless access for the Web Configuration Utility.

Remote Router Access: Select to enable or disable remote management/upgrade of the router. You can allow remote management from any IP Address or a specified IP Address as well as the port number.

Backup and Restore: You can choose to backup the router's settings so that you don't have to manually configure the settings again if you reset the router to factory default.

UPnP: Universal Plug and Play (UPnP) allows Windows Me and XP to automatically configure the router for various Internet applications, such as gaming and videoconferencing.

6.6.2 Log

You can choose to enable or disable logging of your network activity on this screen.



Click **Apply** and to save the setting.

6.6.3 Diagnostics

The Diagnostics screen allows you to perform Ping and Traceroute tests.

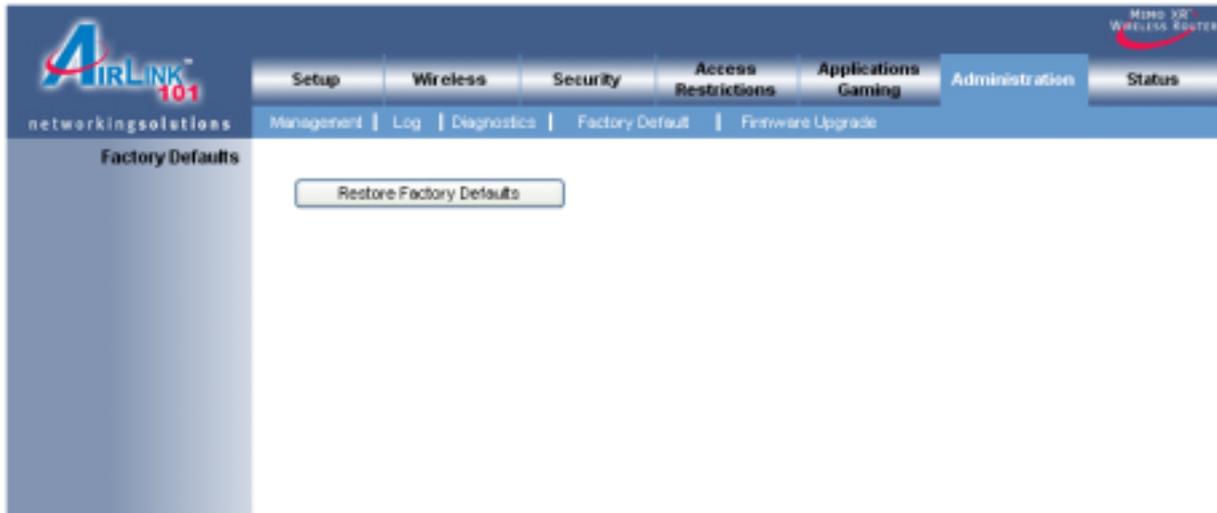
The screenshot displays the Airlink 101 web interface. At the top, there is a navigation bar with tabs for Setup, Wireless, Security, Access Restrictions, Applications Gaming, Administration, and Status. Below this, a secondary navigation bar includes links for Management, Log, Diagnostics, Factory Default, and Firmware Upgrade. The main content area is titled 'Diagnostics' and is split into two sections: 'Ping Test' and 'Traceroute Test'. The 'Ping Test' section contains a text input field for 'IP or URL Address', a 'Packet Size' dropdown menu set to '64 bytes (32-65500)', and a 'Times to Ping' dropdown menu set to '5'. A 'Start to Ping' button is located below these fields. The 'Traceroute Test' section contains a text input field for 'IP or URL Address' and a 'Start to Traceroute' button below it.

Ping Test: Enter the IP or URL Address you wish to ping and click **Start to Ping**.

Traceroute: Enter the IP or URL Address you wish to trace and click **Start to Traceroute**.

6.6.4 Factory Defaults

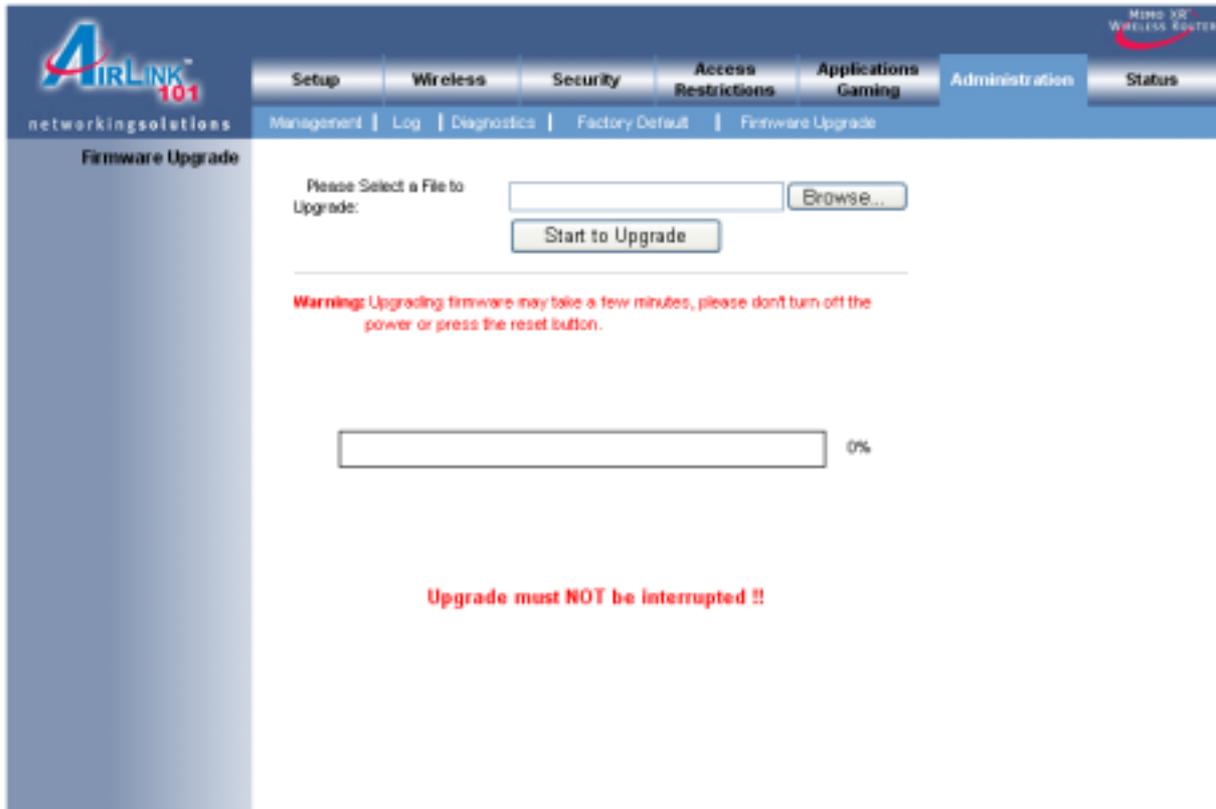
The Factory Defaults screen allows you to set all the router's settings to the factory default.



Click on the **Restore Factory Defaults** button to restore all the settings to default.

6.6.5 Firmware Upgrade

The Firmware Upgrade screen allows you to upgrade the router's firmware.



The screenshot shows the web interface for the Airlink 101 router's firmware upgrade. The page has a blue header with the Airlink 101 logo and navigation tabs for Setup, Wireless, Security, Access Restrictions, Applications Gaming, Administration, and Status. Below the header, there are sub-navigation links for Management, Log, Diagnostics, Factory Default, and Firmware Upgrade. The main content area is titled "Firmware Upgrade" and contains a file selection field with a "Browse..." button and a "Start to Upgrade" button. A warning message in red text states: "Warning: Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button." Below the warning is a progress bar showing 0% completion. At the bottom, a red warning message reads: "Upgrade must NOT be interrupted !!".

You must download and unzip the new firmware first from www.airlink101.com

Click on **Browse** to browse to the new firmware, and click **Start to Upgrade**.

6.7 Status

6.7.1 Router

The Router screen displays various status of the router including the firmware version.



The screenshot displays the web interface of an Airlink 101 router. The top navigation bar includes tabs for Setup, Wireless, Security, Access Restrictions, Applications Gaming, Administration, and Status. The Status tab is active, showing Router Information and Internet Connections.

Router Information

Firmware Version:	v1.0.18
Current Time:	Thu Jul 21 22:01:53 2006 (GMT -08:00)
Internet MAC Address:	00:14:A5:01:4F:41
Host Name:	
Domain Name:	Airlink101

Internet Connections

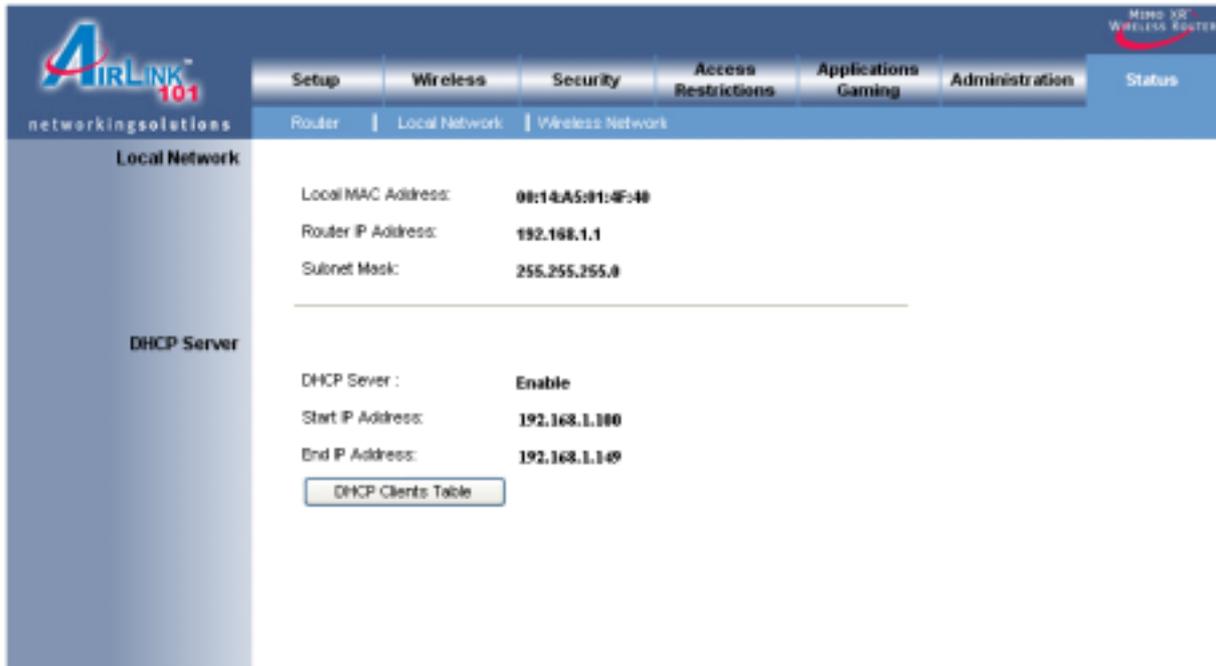
Connection Type:	Automatic Configuration - DHCP
Internet IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1
DNS 1:	192.168.1.1
DNS 2:	0.0.0.0
DNS 3:	0.0.0.0
MTU:	Auto

Buttons: IP Address Release, IP Address Renew, Refresh

Click on the **Refresh** button to reload the screen.

6.7.2 Local Network

The Local Network screen displays various status about your Local Area Network.



The screenshot shows the AIRLINK 101 web interface. The top navigation bar includes tabs for Setup, Wireless, Security, Access Restrictions, Applications Gaming, Administration, and Status. The 'Local Network' tab is selected. The page displays the following information:

Local MAC Address:	08:14:A5:01:4F:40
Router IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0

DHCP Server

DHCP Server :	Enable
Start IP Address:	192.168.1.100
End IP Address:	192.168.1.149

[DHCP Clients Table](#)

Click on the **DHCP Client Table** to display a list of all the DHCP clients in your network.

6.7.3 Wireless Network

The Wireless Network screen displays various status about your wireless network.



The screenshot shows the Airlink 101 web interface. The top navigation bar includes tabs for Setup, Wireless, Security, Access Restrictions, Applications Gaming, Administration, and Status. The 'Wireless' tab is selected. Below the navigation bar, there are links for Router, Local Network, and Wireless Network. The main content area is titled 'Wireless Network' and displays the following configuration details:

MAC Address:	00:14:AS:01:4F:40
Mode:	Mixed
Network Name (SSID):	default
Channel:	6
Security:	Disable
SSID Broadcast:	Enable

7. Troubleshooting

If you have trouble connecting to the Internet, try the following steps.

Step 1 Power off the Cable/DSL modem, router, and computer and wait for **5 minutes**.

Step 2 Turn on the Cable/DSL modem and wait for the lights on the modem to settle down.

Step 3 Turn on the router and wait for the lights on the router to settle down.

Step 4 Turn on the computer.

Step 5 Reconfigure the router as described in **Section 3**.

Step 6 Log in to the router and select the **Status** tab.

Step 7 Verify that the **IP Address**, **Default Gateway**, and at least one of the **DNS** fields have valid numbers assigned to them (instead of all 0's).



If you see all 0's, click on the **IP Renew** button (for Cable Modem users) or the **Connect** button (for DSL users).

If each field has a valid number assigned, the router is connected to the Internet.

Technical Support

E-mail: support@airlink101.com

Toll Free: 1-888-746-3238

Web Site: www.airlink101.com

*Theoretical maximum wireless signal rate based on IEEE standard 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, mix of wireless products used, radio frequency interference (e.g., cordless telephones and microwaves) as well as network overhead lower actual data throughput rate.

Copyright © 2005 AirLink101. All rights reserved. AirLink101, the stylized AirLink101 logo, specific product designations, and all other words and logos that are identified as trademarks and/or service marks are, unless noted otherwise, the trademarks and service marks of AirLink101. All other product or service names are the property of their respective holders. AirLink101 products are protected under numerous U.S. and foreign patents and pending applications, mask work rights, and copyrights.

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.

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.

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

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.

Gemtek declares that WRTR-142G (FCC ID: MXF-R940711G) is limited in CH1~CH11 for 2.4GHz by specified firmware controlled in U.S.A.