300N Draft 802.11n Wireless Router

Model # AR680W

User's Manual

Ver. 1A

Table of Contents

1. Introduction 4
   1.1 Package Contents 4
   1.2 Features 4
2. Connecting the Router 5
3. Verifying Connection to the Router 6
4. Configuring the Router 9
   Cable Modem 10
   DSL 11
5. Connecting to the Router Wirelessly 12
6. Web Configuration Utility 13
   6.1 Setup 13
      6.1.1 Internet Setup 13
      6.1.2 Network Setup 14
      6.1.3 DDNS 15
      6.1.4 Time Settings 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 24
      6.4.2 MAC Filters 25
      6.4.3 URL Blocking 26
      6.4.4 Domain Blocking 27
      6.4.5 Schedule 27
   6.5 Applications & Gaming 28
      6.5.1 Port Range Forwarding 28
      6.5.2 Port Range Triggering 29
      6.5.3 DMZ 30
   6.6 Administration 31
      6.6.1 Management 31
      6.6.2 Log 32
      6.6.3 Diagnostics 33
      6.6.4 Factory Defaults 33
      6.6.5 Firmware Upgrade 34
      6.6.6 Restart 34
   6.7 Status 35

6.7.1 Router 35
6.7.2 Local Network 36
6.7.3 Wireless Network 36
7. Troubleshooting 37
Appendix A – Specifications 38
Appendix B – Information 39
Technical Support 41

1. Introduction

Congratulations on your purchase of the AR680W 300N Wireless Router. The 300N Wireless Router provides wireless data rate of up to 300 Mbps* when used with other AirLink101® 300N wireless products. The high bandwidth combined with extended wireless coverage delivers fast and reliable connections for all of your networking applications.

A full range of security features such as WEP, WPA-PSK, and WPA2-PSK provide the highest level of wireless network security. The built-in Web Configuration Utility allows you to set up the router with an easy-to-use user interface. Best of all, the 300N Wireless Router works with 802.11g and 802.11b network devices ensuring compatibility with your existing wireless products.

1.1 Package Contents

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

- 300N Wireless Router
- RJ-45 Cable
- Power Adapter
- Quick Installation Guide
- 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.

1.2 Features

- Industry's highest wireless data rate of up to 300 Mbps* with IEEE 802.11n draft specification version 1.1.
- 3 antennas for wider coverage and stronger signal strength to eliminate dead spots
- 64-bit/128-bit WEP encryption, Pre-shared Key (PSK), and Wi-Fi Protected Access (WPA2) and WPA support provide full protection for your wireless connection
- Higher data rate increases the reliability and stability of wireless connections
- Great for environments with higher wireless data traffic requirements
- Fully backward-compatible with 802.11b/g devices

- Works best with AirLink101® 300N Wireless Adapters, AWLH6080, AWLC6080 and AWLL6080

2. Connecting the Router

Note: Prior to connecting the router, be sure to power off your computer, DSL/Cable modem, and the router. You should setup the router with a wired connection first before attempting to setup any wireless connections.

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 (Ethernet)** 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** port that the computer is connected to are lit. If not, try the above steps again.

AR680W Icon Illustrations:

Power	Status	WAN	Wireless	LAN	WPS
				1 ~ 4	

Power
On: Power on

Status
Blinking: Function properly.

WAN
On: Link established

Blinking: Data transmission

Wireless
On: Wireless is ready
Blinking: Data transmission

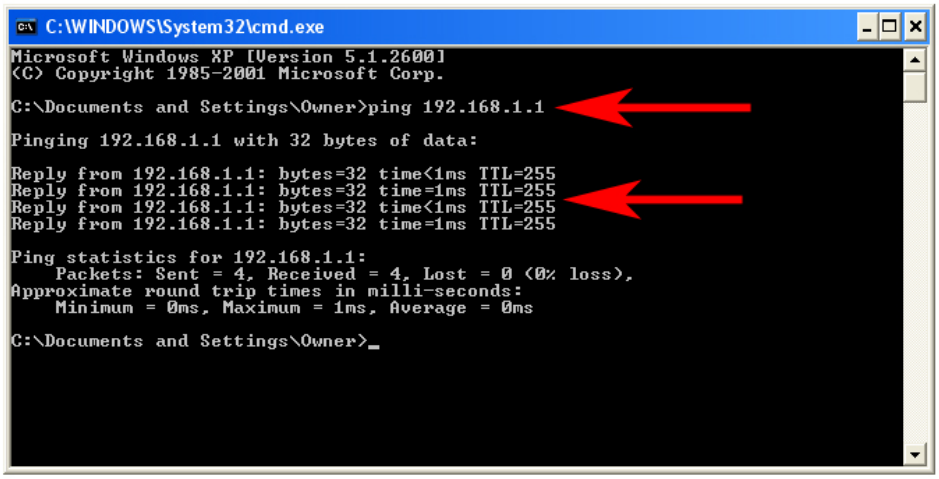
LAN
On: Link established
Blinking: Data transmission

WPS (WiFi Protected Setup)
Blinking Green: WPS setting in progression
Static Green: WPS successfully set up
Blinking Red: Error found

3. Verifying Connection to the Router

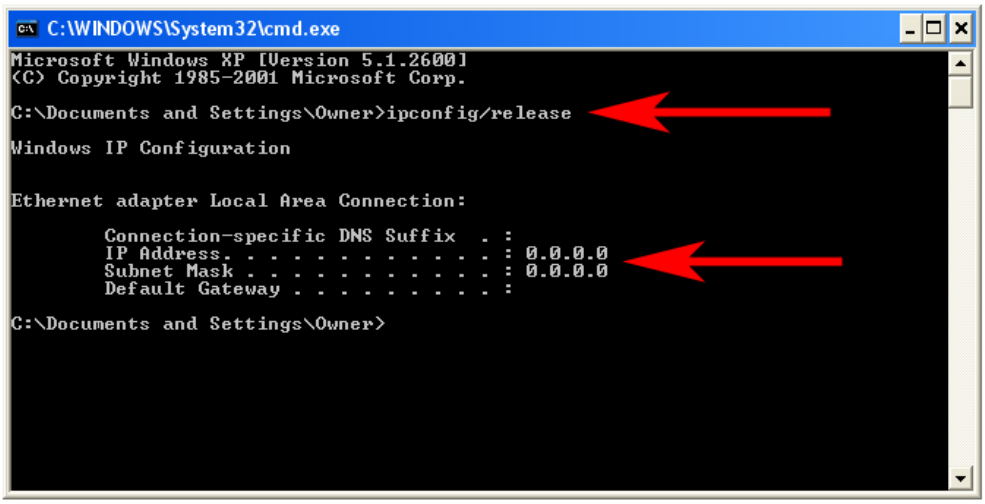
Step 1 Go to **Start**, **Run**, type **command** (for Windows 95/98/ME) or **cmd** (for Windows 2000/XP) and click **OK**. You will see the command prompt as below.

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

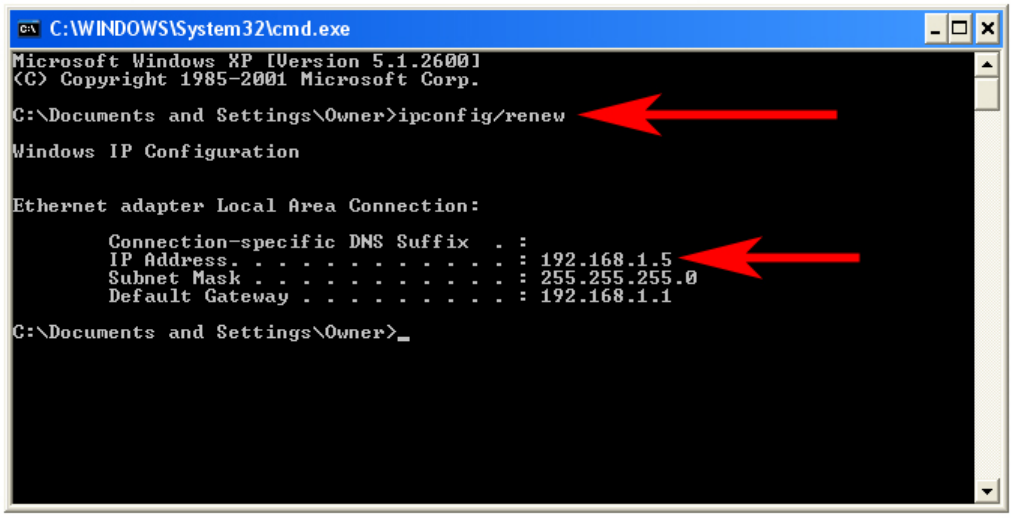


Step 3 If you get **Request timed out**, or **Destination host unreachable**, double-check the network cable connection between the computer and the router and try **Step 2** again. If you still encounter problem, go to the next step; otherwise proceed to **Section 3, Configuring the Router**.

Step 4 For Windows 2000/XP, type **ipconfig/release** and press **Enter**. (Windows 98se/ME users skip ahead to **Step 6**)

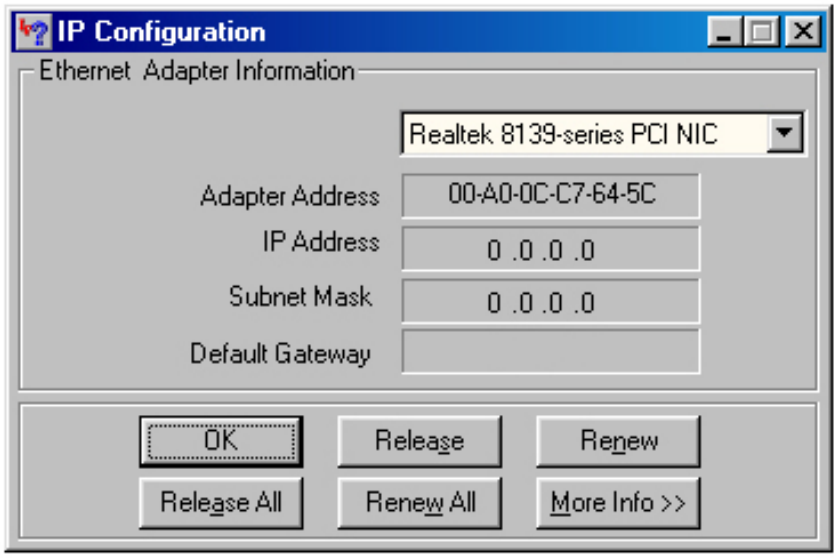


Step 5 Type **ipconfig/renew** and press **Enter**. You should get an IP address of **192.168.1.x** (where **x** is a number between 2 - 254). Proceed to **Section 3, Configuring the Router.** If you don't get an IP address, reset the router by holding in the reset button at the back of the router for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

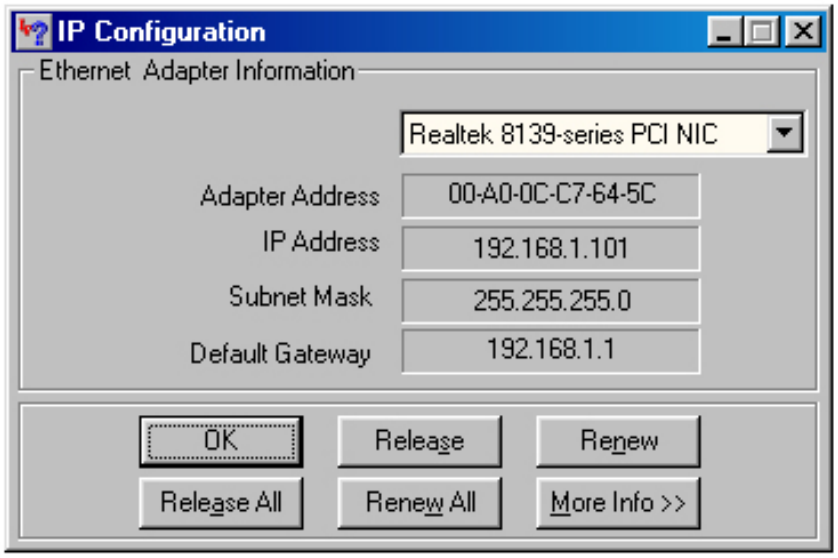


Step 6 For Windows 95/98/ME go to **Start**, **Run**, type **winipcfg** and click **OK**. (Step is not necessary for Windows 2000/XP)

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

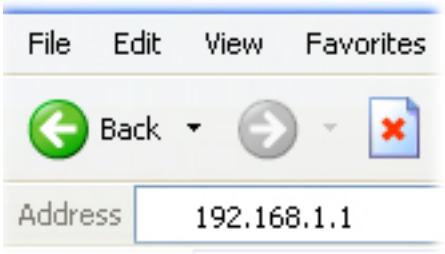


Step 8 After your IP address is released, click **Renew**. You should get an IP address of **192.168.1.x** (where **x** is a number between 2 - 254). If you don't get an IP address, reset the router by holding in the reset button at the back of the router for 10 seconds while it is ON and try **Renew**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



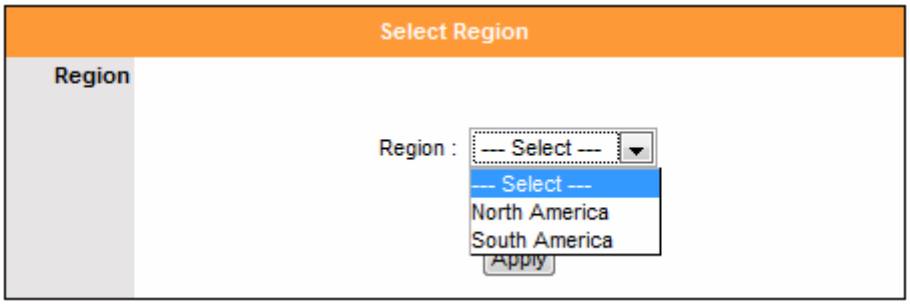
4. Configuring the Router

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 **Login**.

Step 3 Select the proper region, **North America** or **South America**, and click **Apply**.

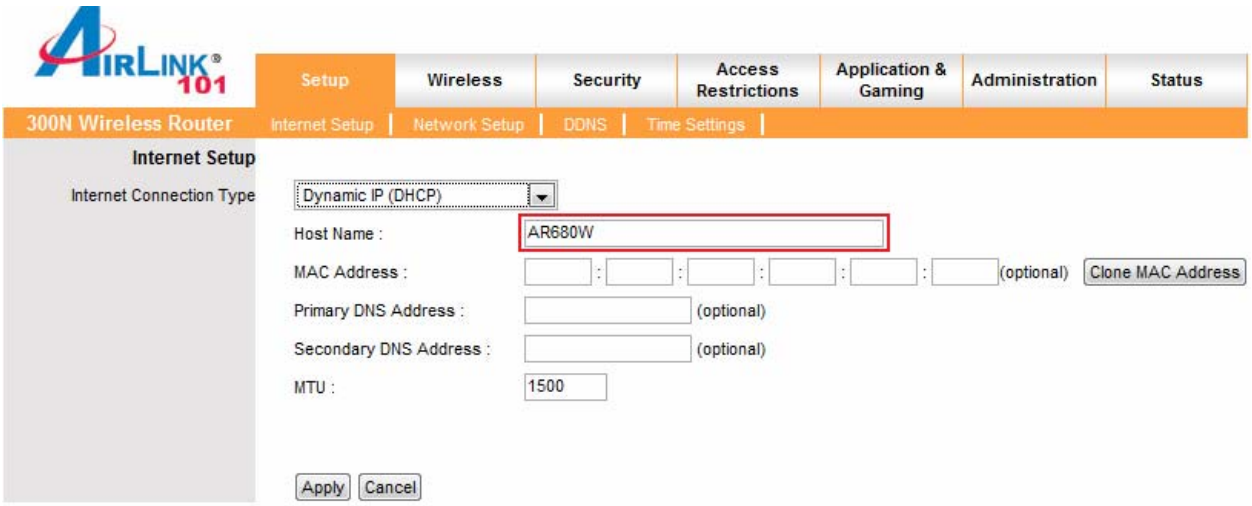


Warning: This device requires that the user or installer properly selects the current region of operation before using this device. This device will automatically limit the allowable channels determined by the current region of operation. **Incorrectly selecting the current region of operation may result in illegal operation and may cause harmful interference to other systems.** The user is obligated to ensure the

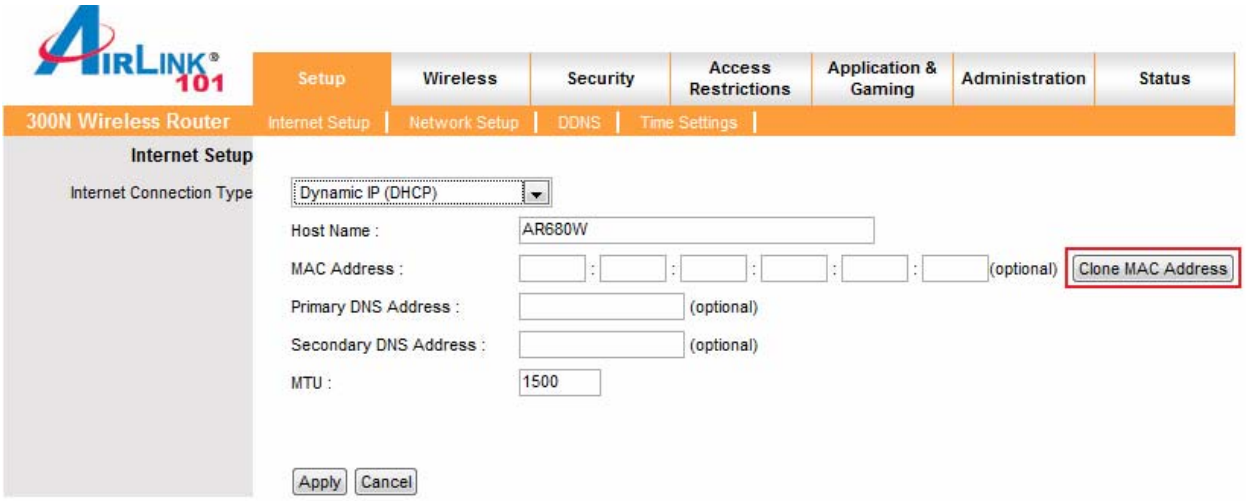
device is operating according to the channel limitations, indoor/outdoor restrictions and license requirements for the current country of operation.

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 on the **Clone MAC Address** button. Click **Apply** and **OK** to save the settings.

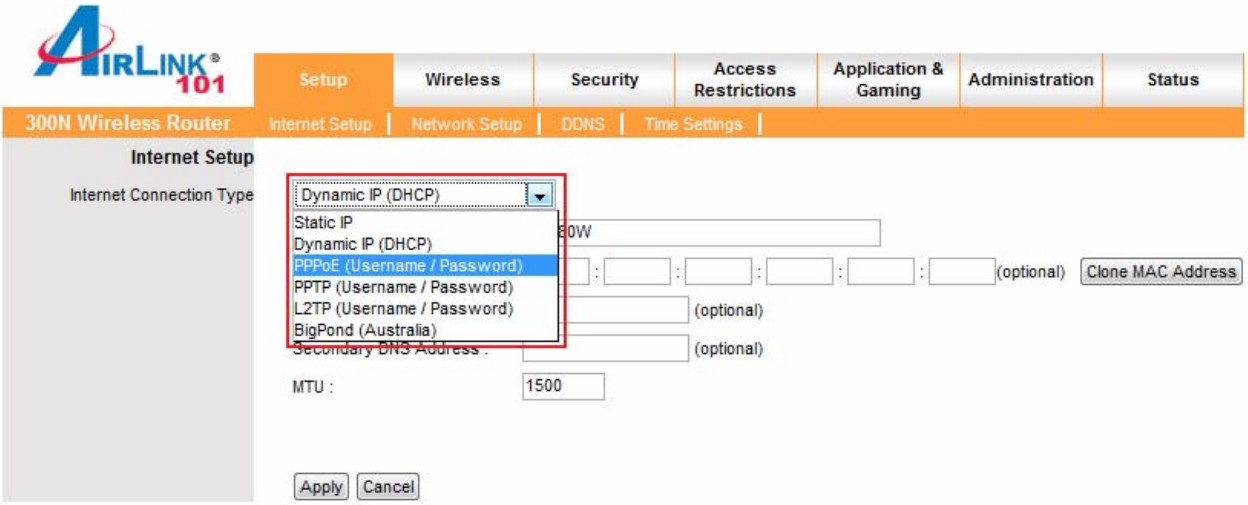


If you have trouble connecting to the Internet, please refer to the **Troubleshooting** section at the end of this guide.

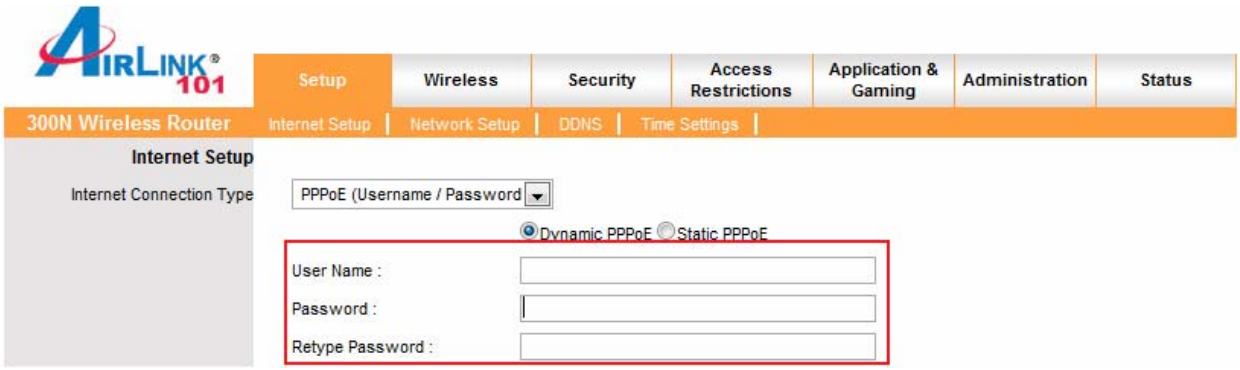
DSL

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** and **OK** to save the settings.

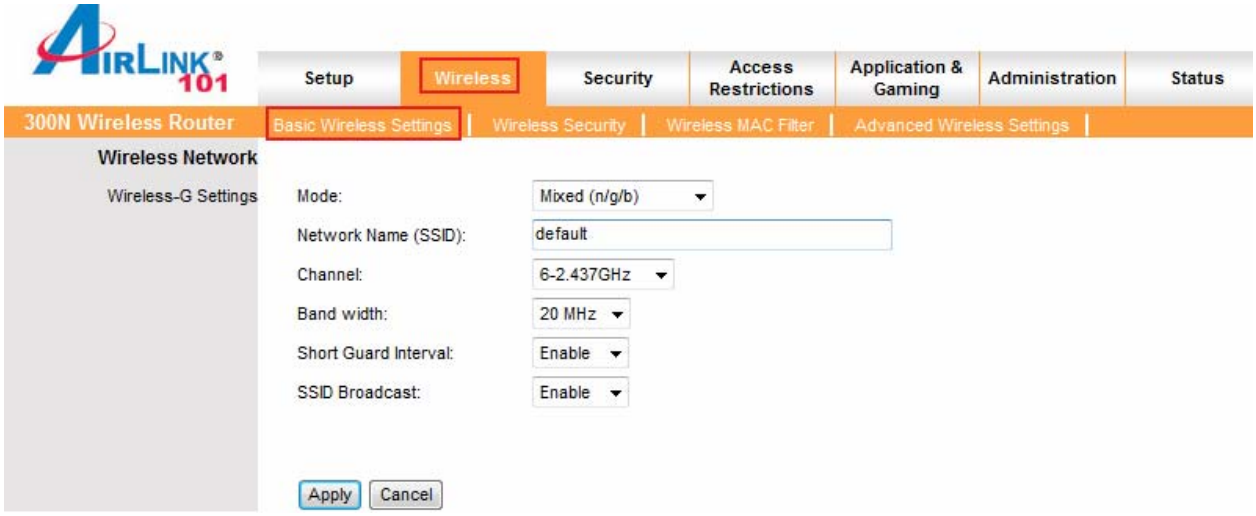
If you have trouble connecting to the Internet, please refer to the **Troubleshooting** section at the end of this manual.

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: **default**
Operating Mode: **Infrastructure**
Authentication: **Open System**
Channel #: **6**
WEP: **disabled**

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



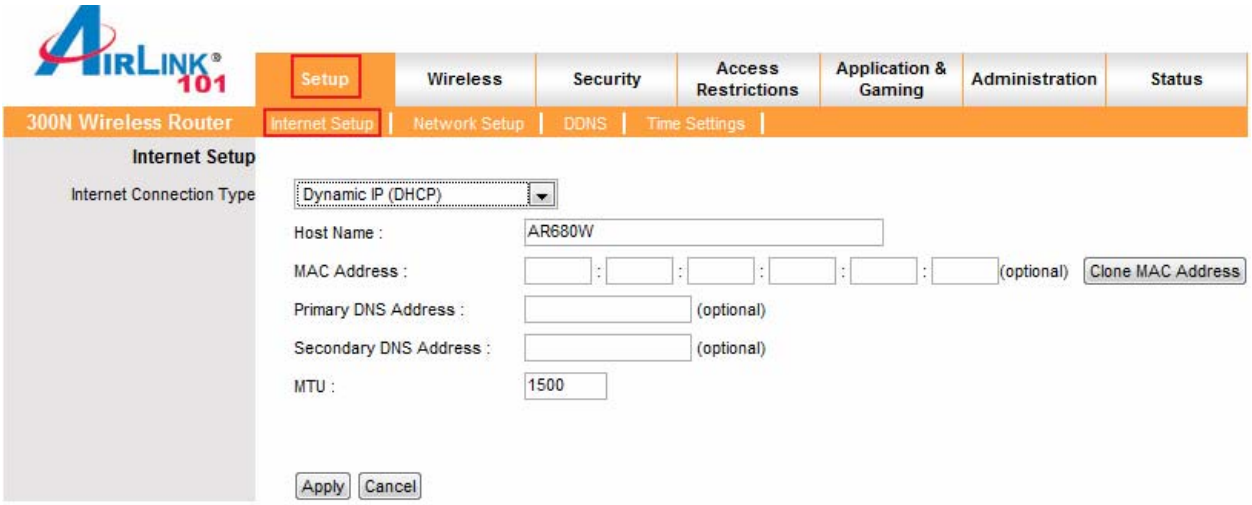
For more information about wireless settings, refer to section **6.2**.

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

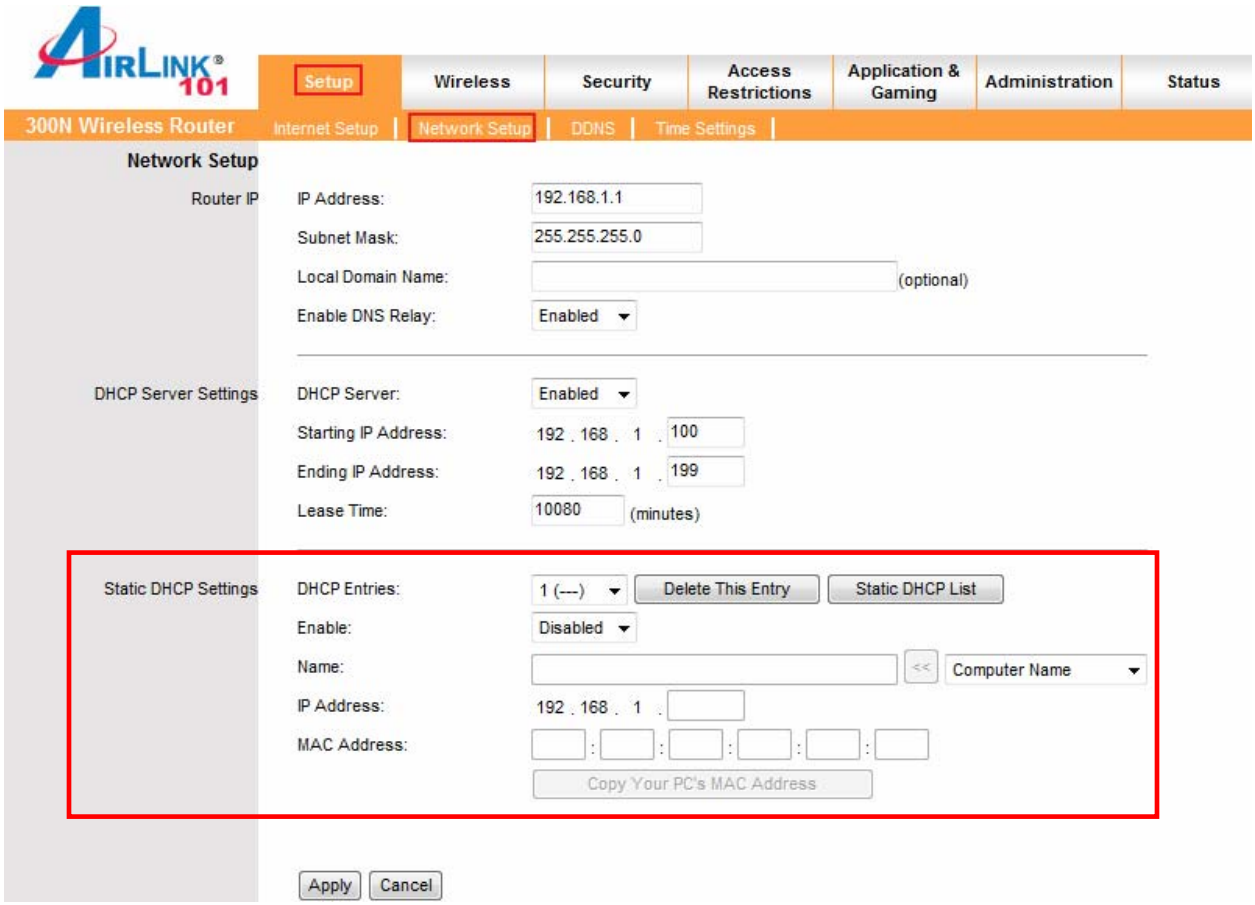
6.1.1 Internet Setup



This is the default screen when you log in to the router's web configuration utility. You can setup your Internet connection here.

6.1.2 Network Setup

Network Setup allows manually configuring TCP/IP and DHCP settings.



Assigning Static DHCP Settings

Step 1 Select **Enabled** in the under the Static DHCP Settings section

Step 2 Select a computer name from the drop-down menu or enter a name associated with this Static IP Address

.

Step 3 Enter the Static IP Address in the **IP Address** field

Step 4 Enter the MAC address of the corresponding computer in the **MAC Address** field

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

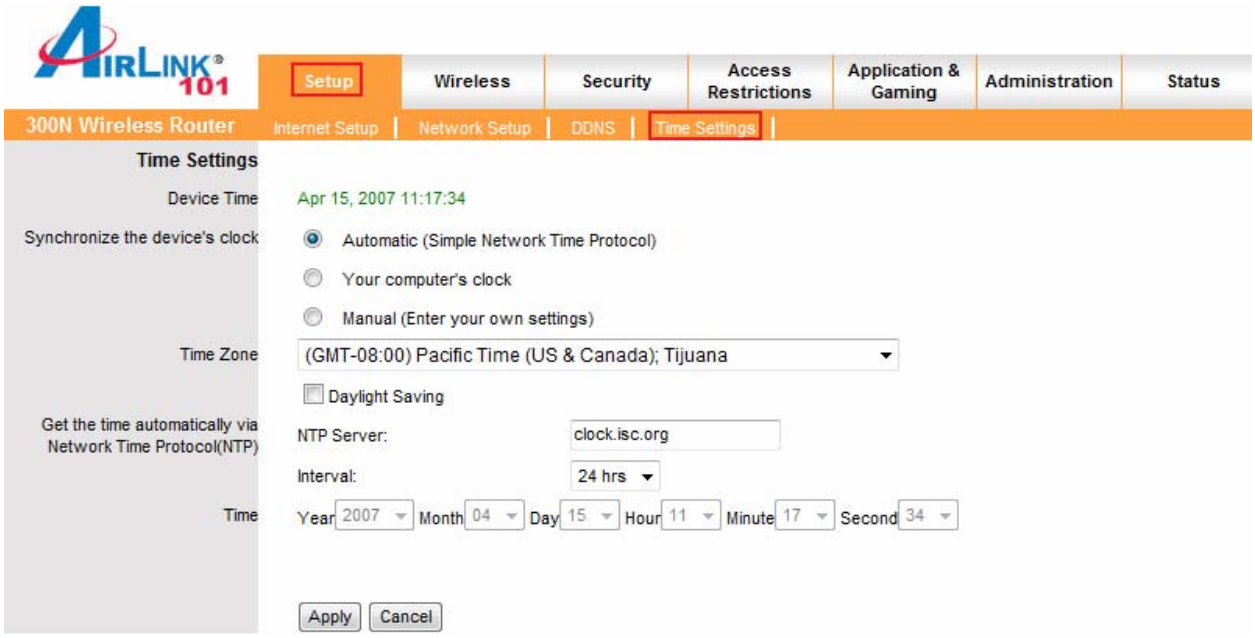
6.1.3 DDNS

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** and **OK** to save the settings.

6.1.4 Time Settings

Time Settings allow you to configure the router clock.



Automatic connects to the internet and synchronizes the router's clock with time provided by accurate timeservers on the internet. Using this feature requires that your router have a working internet connection.

Your computer's clock allows you to synchronize the router's clock with your computer's system clock

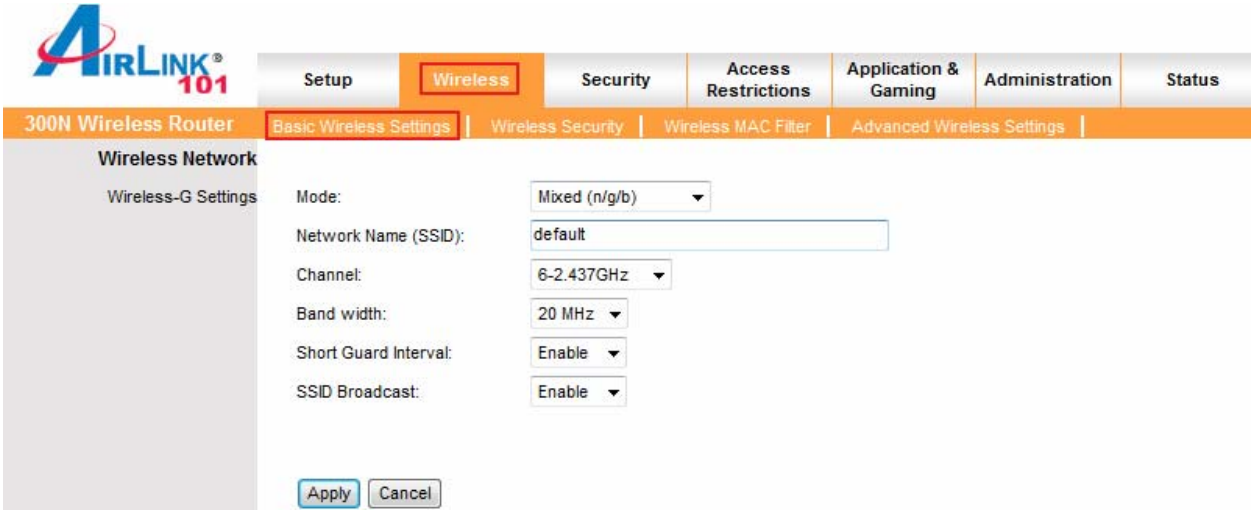
Manual provides you with the option of setting your own date and time.

Click **Apply** and **OK** to save the settings.

6.2. Wireless

6.2.1 Basic Wireless Settings

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



Mode: Choose from Mixed (n/g/b), Mixed (g/b), Wireless-11n Only, Wireless-11g Only, Wireless-11b Only, or Disabled to stop wireless function.

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

Channel: Select the desired channel.

Changing channels is useful when you are experiencing slow, unstable wireless connections, or if you are unable to establish a wireless connection at all.

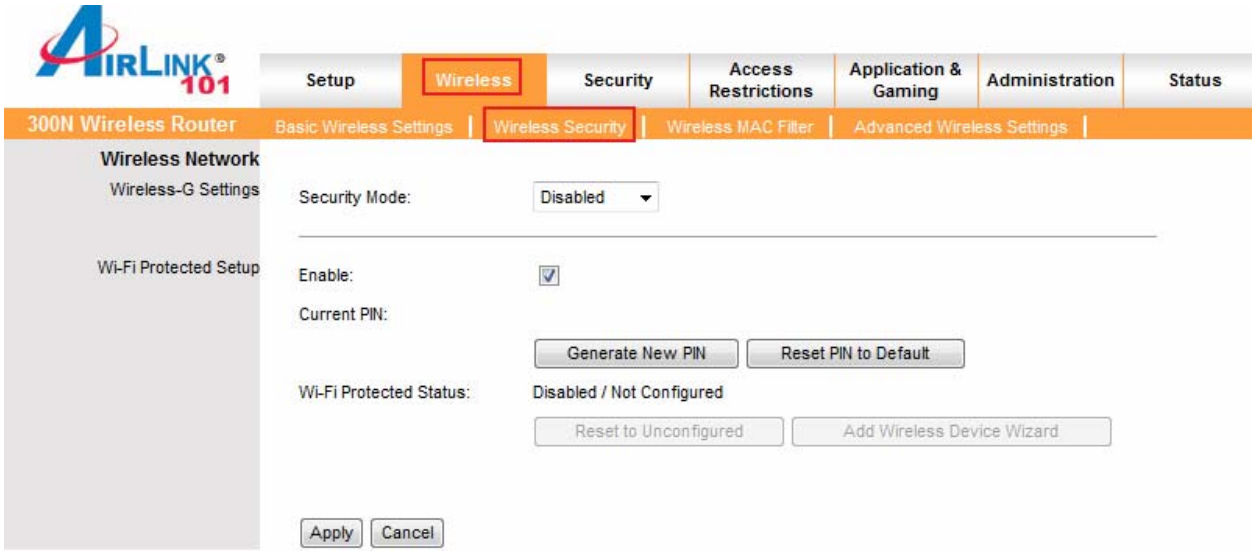
Your router has 11 channels available (1-11). Start with channel 1 and work your way up. Each time you change channels on the router, restart the wireless computers and then try to connect. If the computers are able to connect, test the channel out for a while and make sure that they hold the connection. Keep changing channels until you find one that gives you a stable connection.

All the network clients need to be using the same channel.

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

6.2.2 Wireless Security

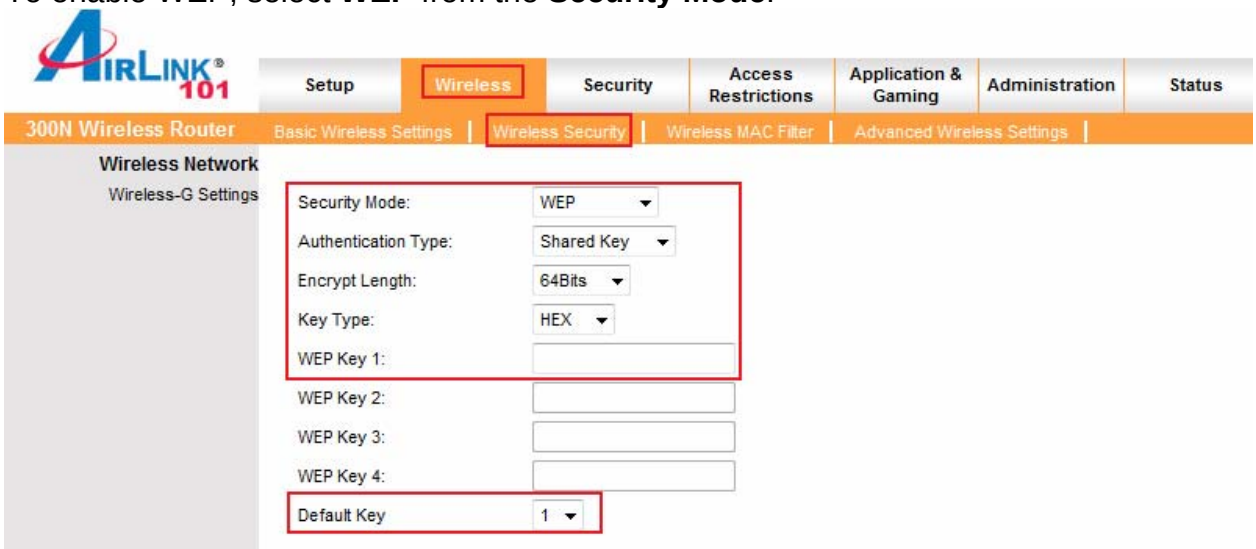
You can configure wireless security such as WEP or WPA encryption on this screen.



Note: It is recommended that you use WPA-PSK or WPA2-PSK encryption over WEP if your wireless clients support it. 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**.



Authentication Type: Select “Shared Key”

Encryption: Choose **64 bits**

Key Type: Choose **HEX**

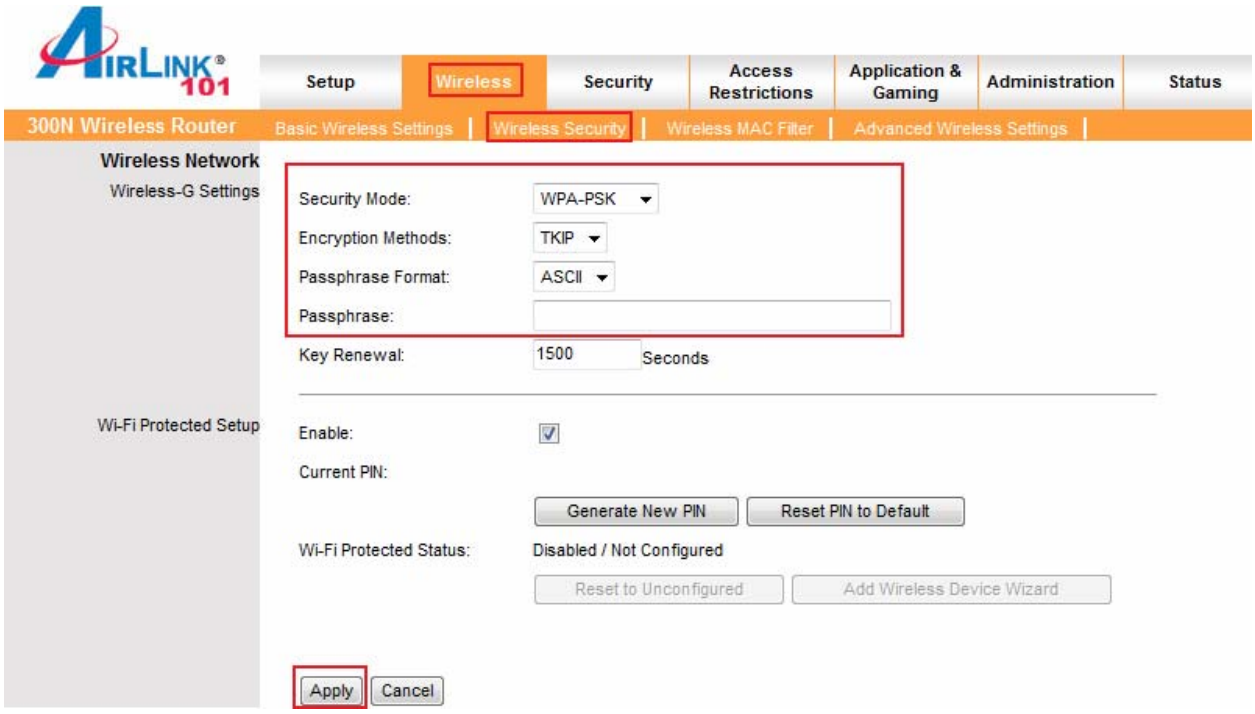
WEP Key 1: Enter a 10 digit number. This will be your wireless password. An easy one to remember is a phone number with area code (ex: 8887463238). You do not need to enter anything in WEP Key 2, 3 and 4.

Default Key: Select key 1

Click **Apply** and **OK** to save the settings.

WPA

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



Encryption Methods: Select either **TKIP** or **AES** as the encryption method. AES is only supported by some newer cards, so make sure that your card supports AES before selecting that option. TKIP will work with most cards. If you are unsure, choose TKIP.

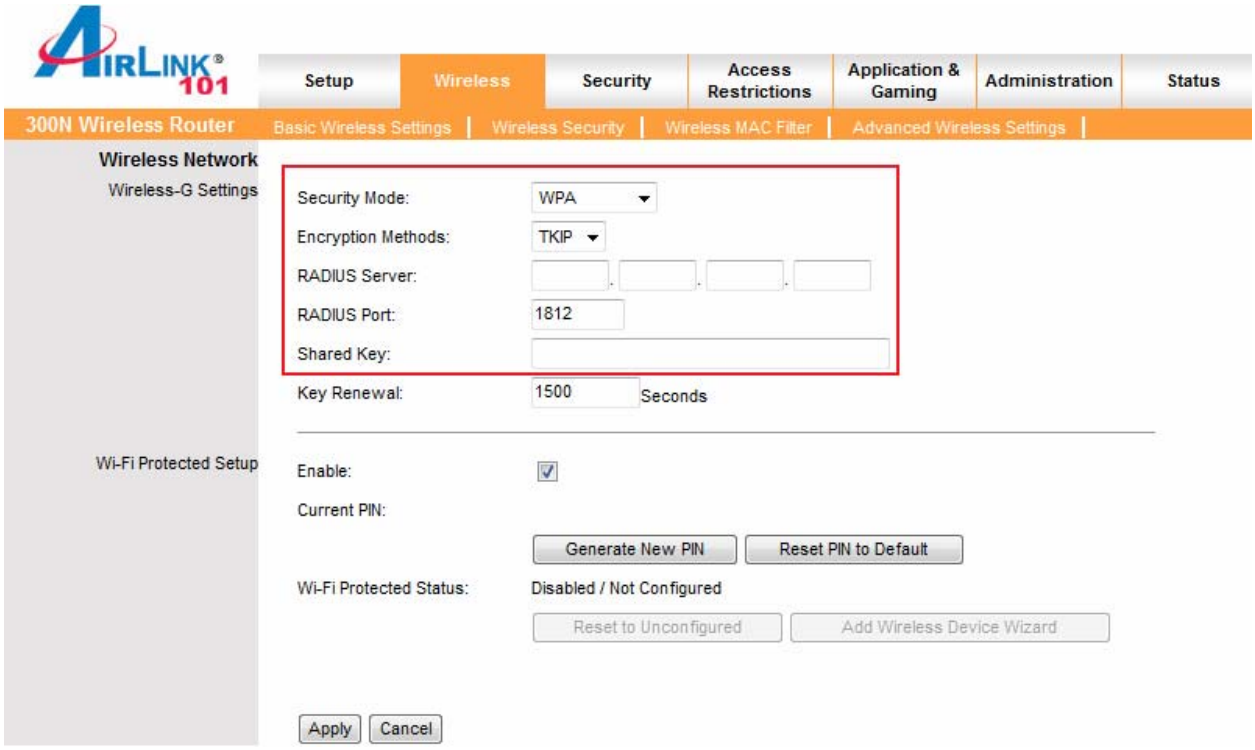
Passphrase: Enter a passphrase between 8 to 63 characters long. For best security, use a passphrase that is at least 30 characters long.

Key Renewal: Enter the desired key renewal time in seconds. It is best to leave this at the default setting of 1500.

Click **Apply** and **OK** to save the settings.

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**.



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

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

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

Shared Key: Enter the shared key.

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

Click **Apply** and **OK** to save the settings.

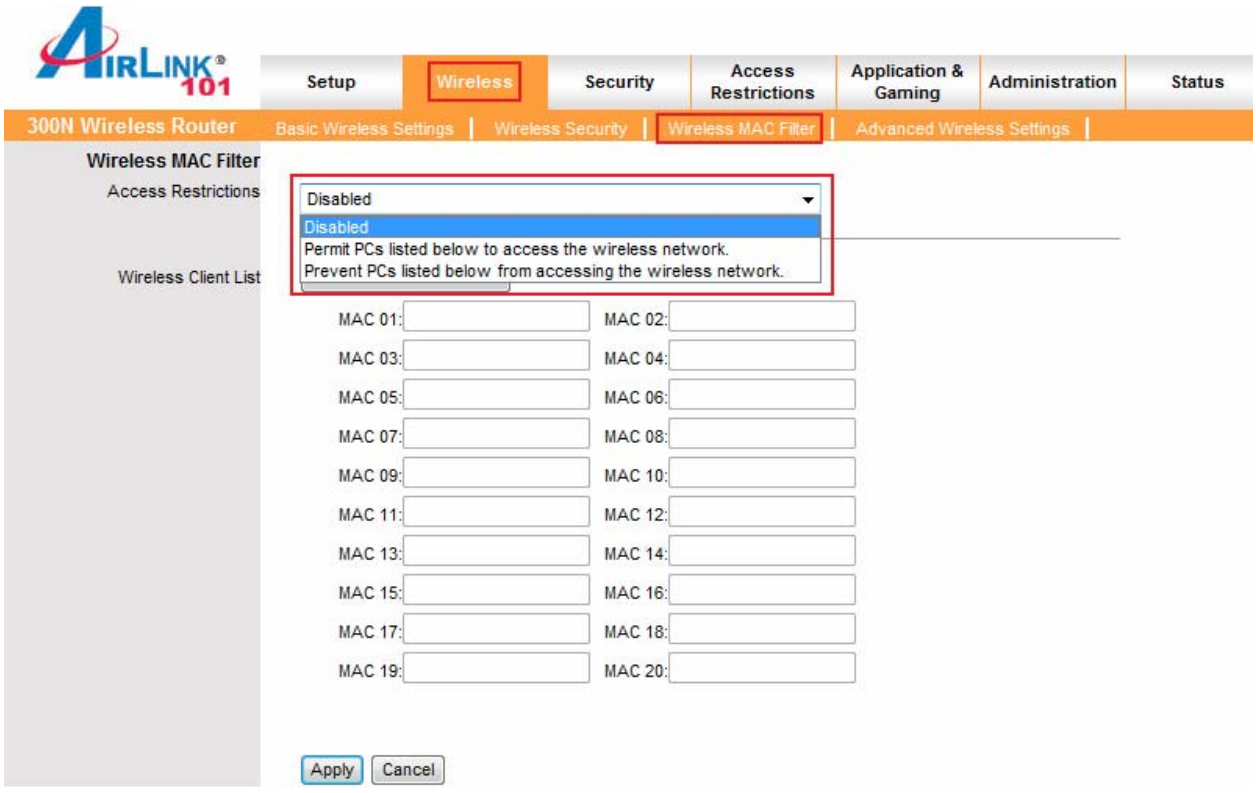
WiFi Protected Setup

This is an easier way to setup the wireless security for all your wireless clients. This security feature only works if your wireless adapters support **WPS PIN** feature. You will have to enter the **Current PIN** at your wireless client side to connect to this router.

Check/Uncheck the **Enable** box to enable or disable this function

6.2.3 Wireless MAC Filter

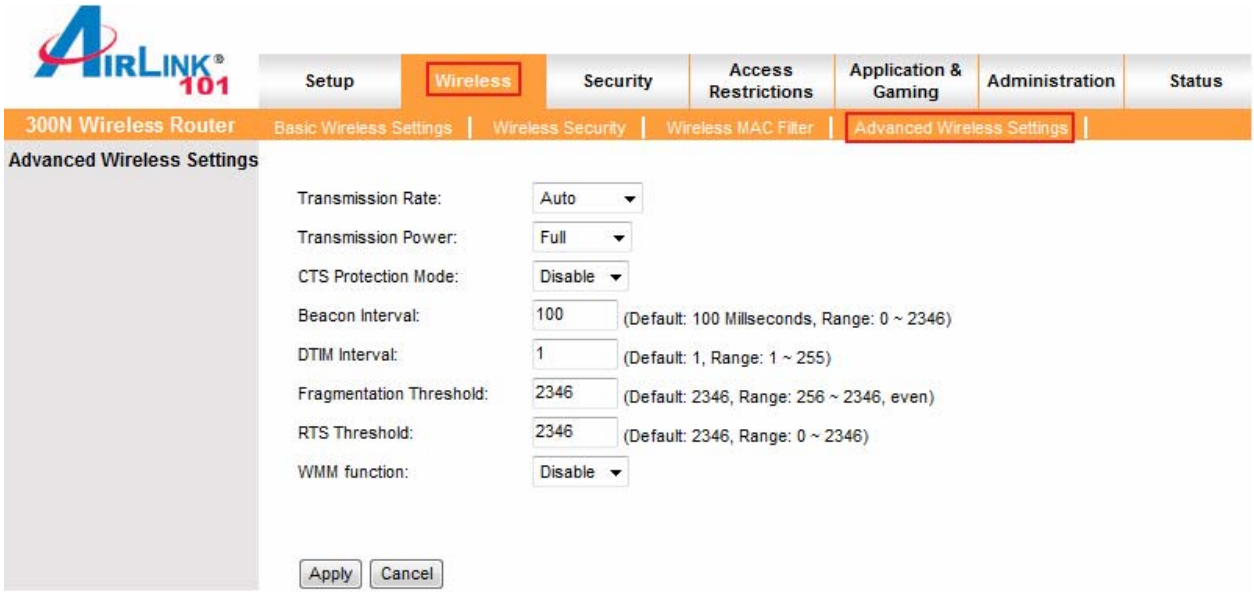
You can restrict certain wireless clients from accessing the router by specifying their MAC address and enabling access restriction. This should not be used as a security feature in place of encryption.



From the pull down menu, select 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** and **OK** to save the settings.

6.2.4 Advanced Wireless Settings

You can configure various advanced wireless settings on this screen. These settings are for advanced users ONLY. Most users will want to leave these settings alone.



Transmission Rate: Select from Auto, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 and 54 Mbps.

Transmission Power: Select from full, half, quarter, eighth, min.

CTS Protection Mode: Select from disable, enable, auto.

Beacon Interval: Enter a value from the valid range of 0 to 2346. The default value is 100 Milliseconds

DTIM Interval: Enter a value from the valid range of 0 to 255. The default value is 1.

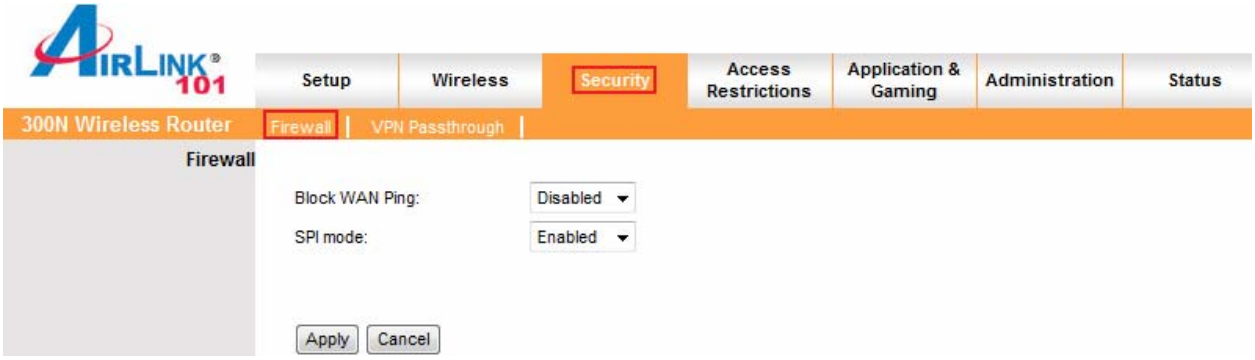
Fragmentation Threshold: Enter an even number from 256 to 2346. The default value is 2346.

RTS Threshold: Enter a value from the valid range of 0 to 2346. The default value is 2346.

Click **Apply** and **OK** to save the settings.

6.3 Security

6.3.1 Firewall



Block WAN Ping: This setting blocks remote users from being able to ping your internet IP address.

SPI Mode: Select to enable or disable Stateful Packet Inspection. This setting provides an additional level of security.

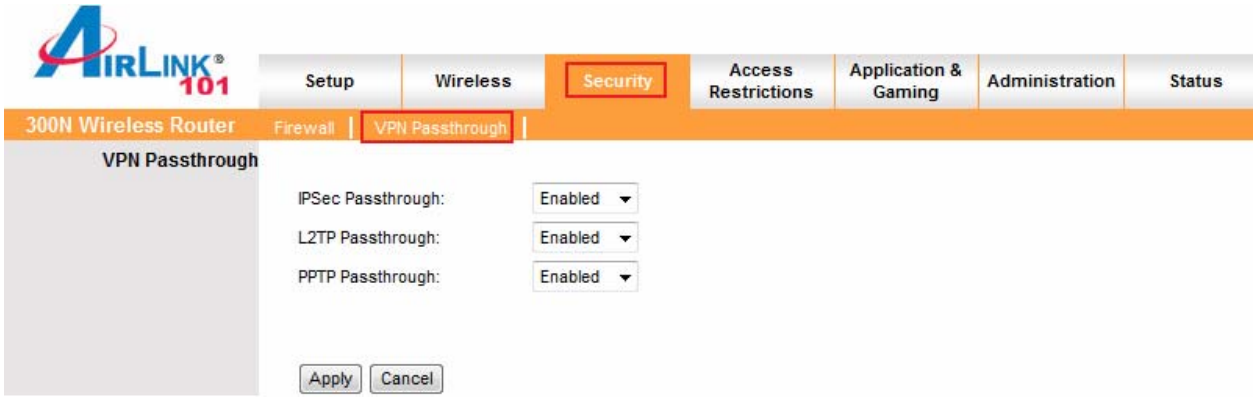
However, it may slow down some applications such as VOIP Phones and other services that require constant streams of data. You can disable this feature to eliminate lag problems with VOIP Phones.

It can also prevent VPN clients from working properly. If you are having trouble connecting to your VPN, you may want to disable this feature.

Click **Apply** and **OK** to save the settings.

6.3.2 VPN Passthrough

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



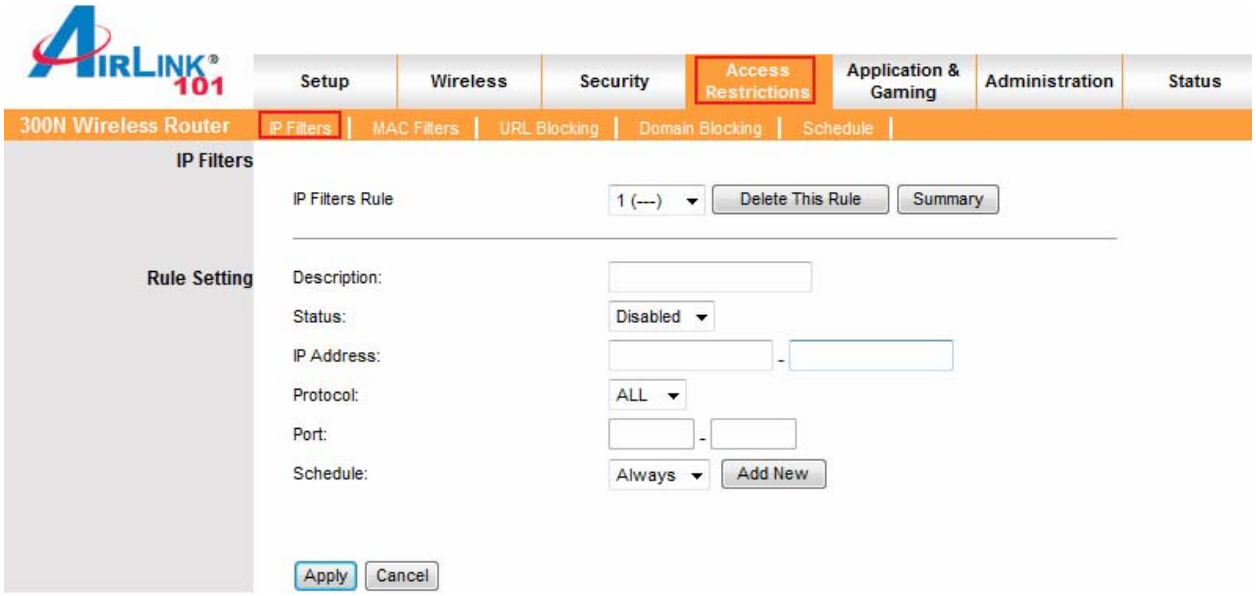
Click **Apply** and **OK** to save the settings.

6.4 Access Restrictions

You can setup policies that deny or allow specific clients to access the Internet based on IP address, MAC address, URL, Domain or a specified time.

6.4.1 IP Filters

Set up policies based on IP addresses.



Description: Enter a name for the policy.

Status: Choose to enable or disable the selected policy.

IP Addresses: Specify the range of IP addresses you wish to block from your router.

Protocol: Select protocol from All, TCP, UDP or ICMP

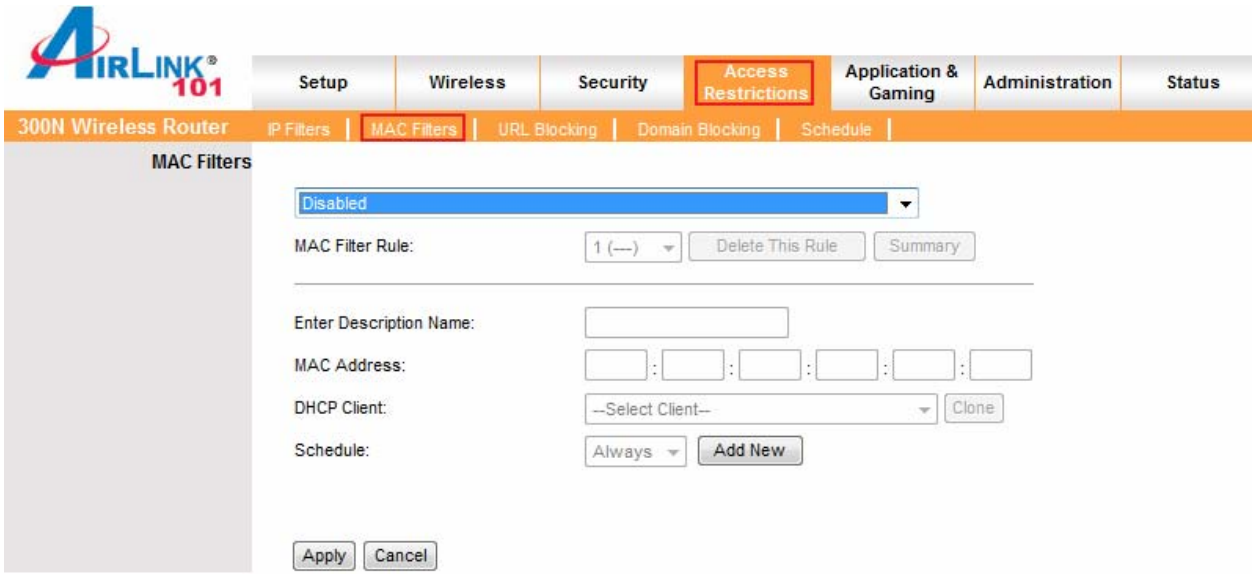
Port: Enter the range of ports you wish to block from the specified IP addresses

Schedule: Enter a schedule time

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

6.4.2 MAC Filters

Block or allow access to the network for devices with specific MAC addresses.



Enter Description Name: Enter a name for the policy.

MAC Address: Enter a MAC address

DHCP Client: Select DHCP client on your network.

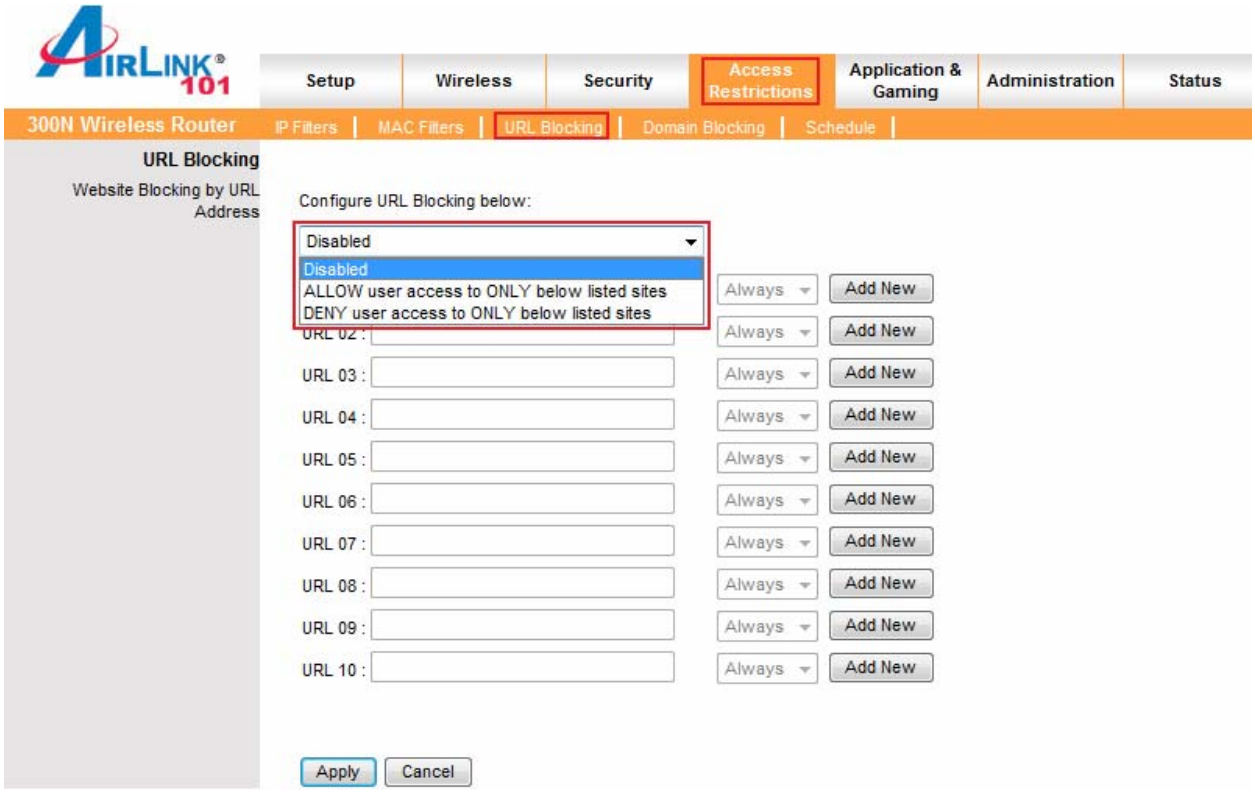
To view all the policies, click the **Summary** button.

6.4.3 URL Blocking

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

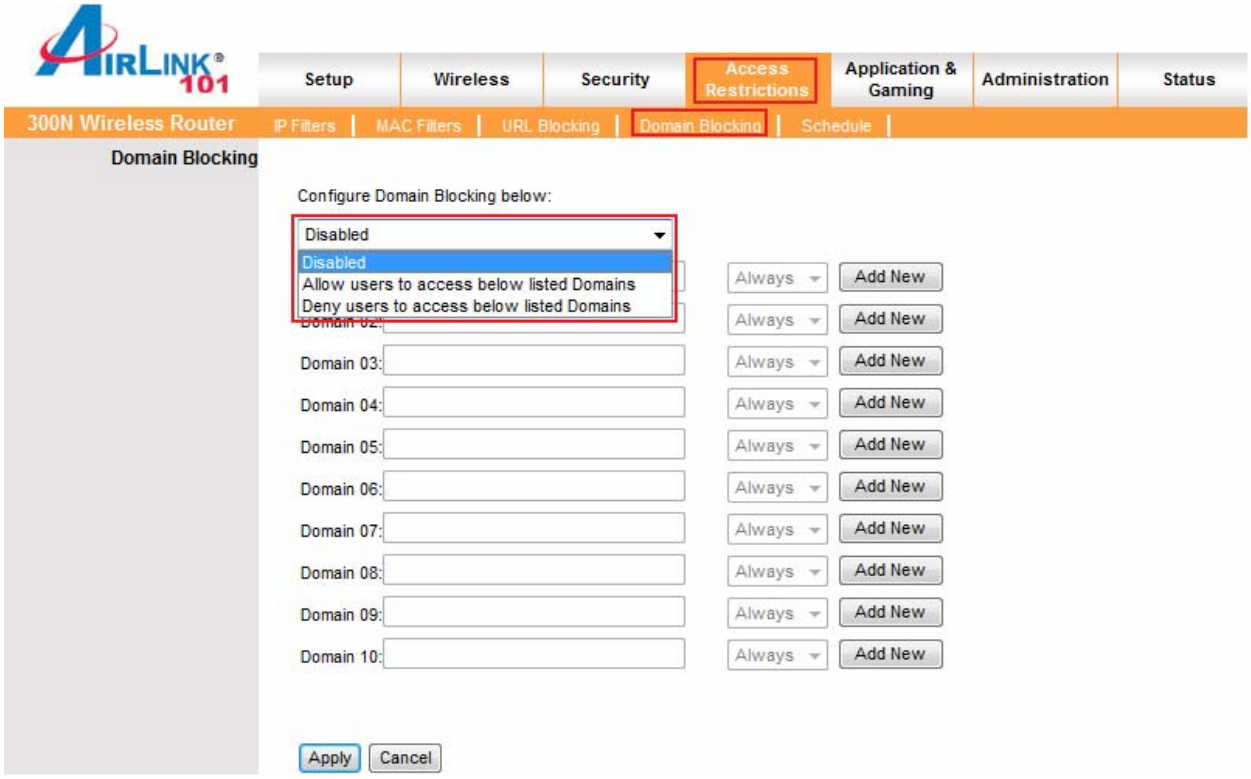
Enter the URL or the Keyword you wish to block.

Click **Apply** and **OK** to save the settings.



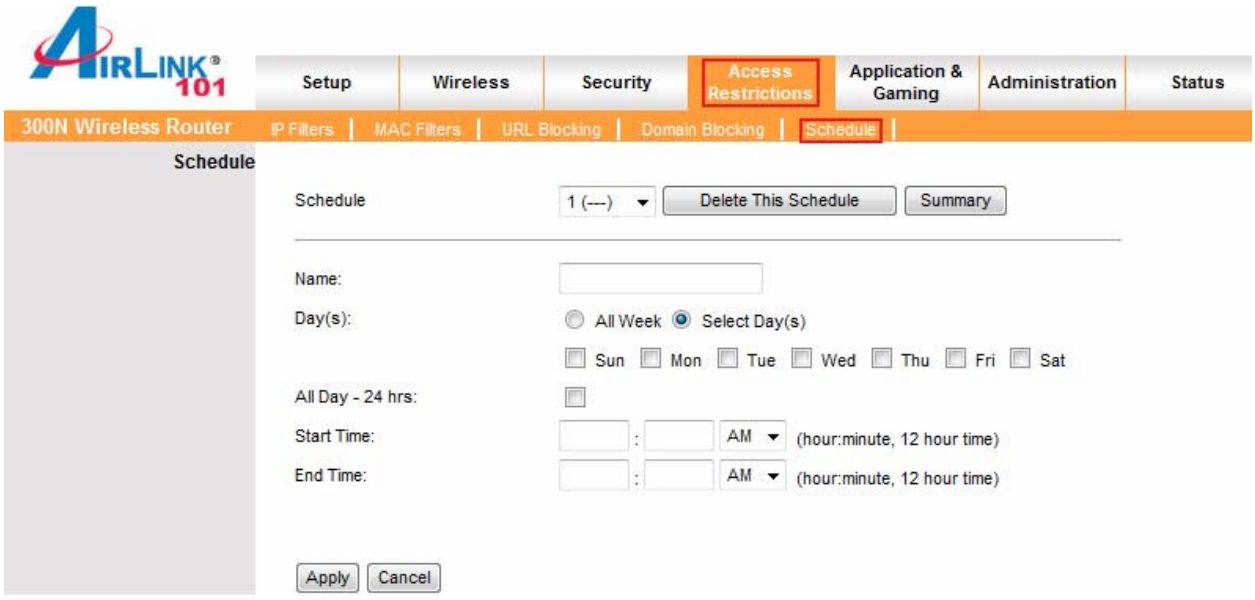
6.4.4 Domain Blocking

Block users from accessing specific domains on the internet.



6.4.5 Schedule

Select a time range in which the specified clients to access the Internet by **Day** and **Time**.

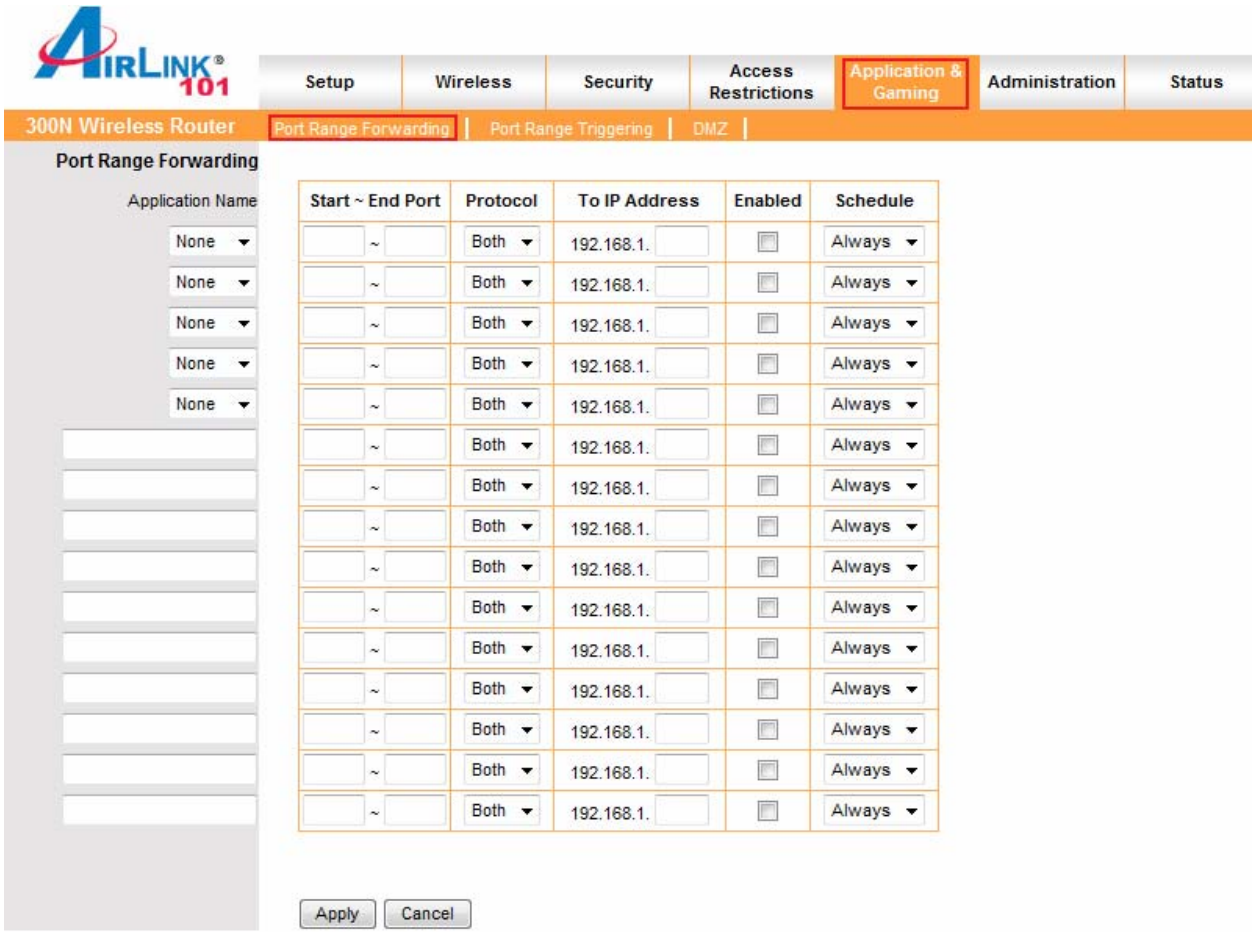


6.5 Applications & Gaming

6.5.1 Port Range Forwarding

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

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



If you are only forwarding one port, you can put it in both the **Start** and **End** Port boxes.

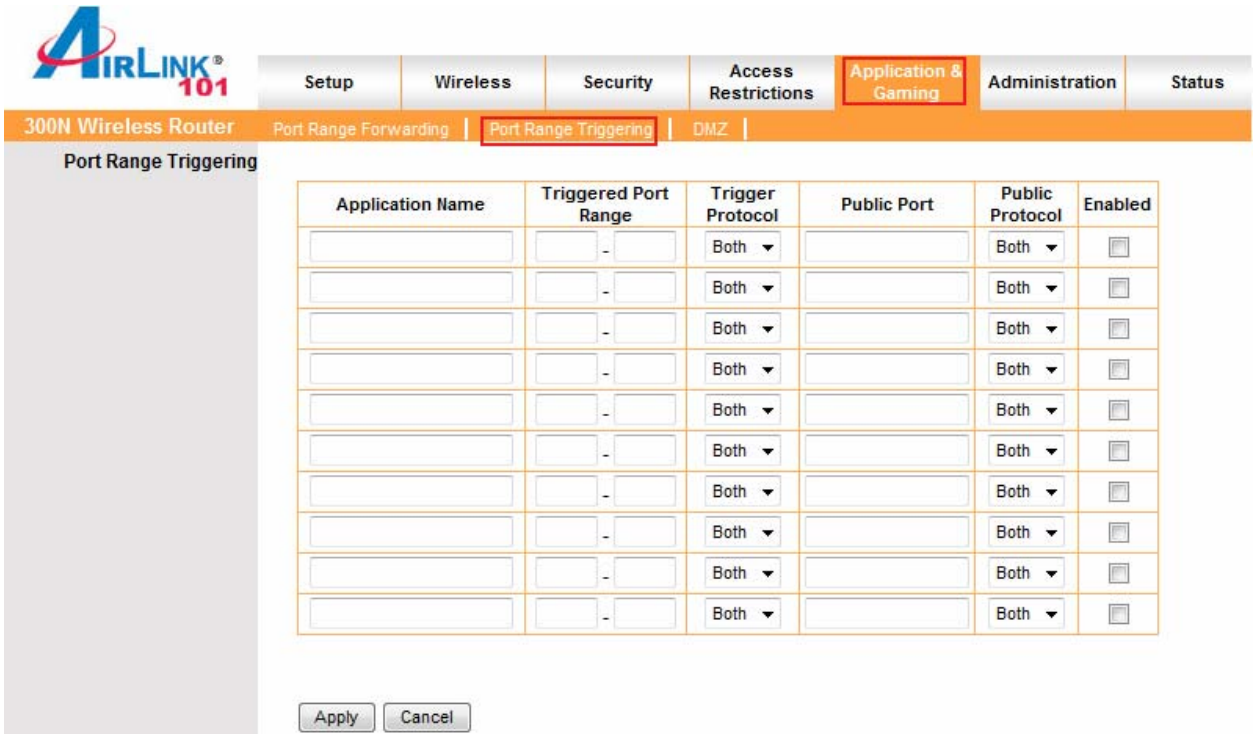
Protocol: If you don't know which one to choose, select both.

To IP Address: This should be the IP address of the computer you want to forward the ports to.

Make sure that you check the **Enabled** box to activate the setting, then click **Apply** and **OK** to save the settings.

6.5.2 Port Range Triggering

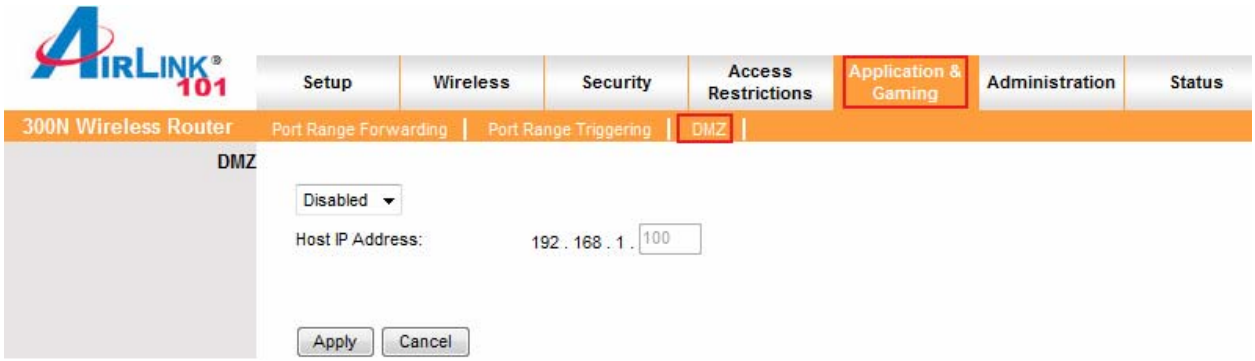
Port triggering allows the router to keep track of outgoing data for specific port numbers. The router remembers which computer sends out what data, so that when the requested data returns through the router, the data is sent back to the proper computer by way of IP address and port mapping rules.



Click **Apply** and **OK** to save the settings.

6.5.3 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.



DMZ: Select to enable or disable DMZ.

Host IP Address: Specify the IP address of the computer you wish to use with DMZ.

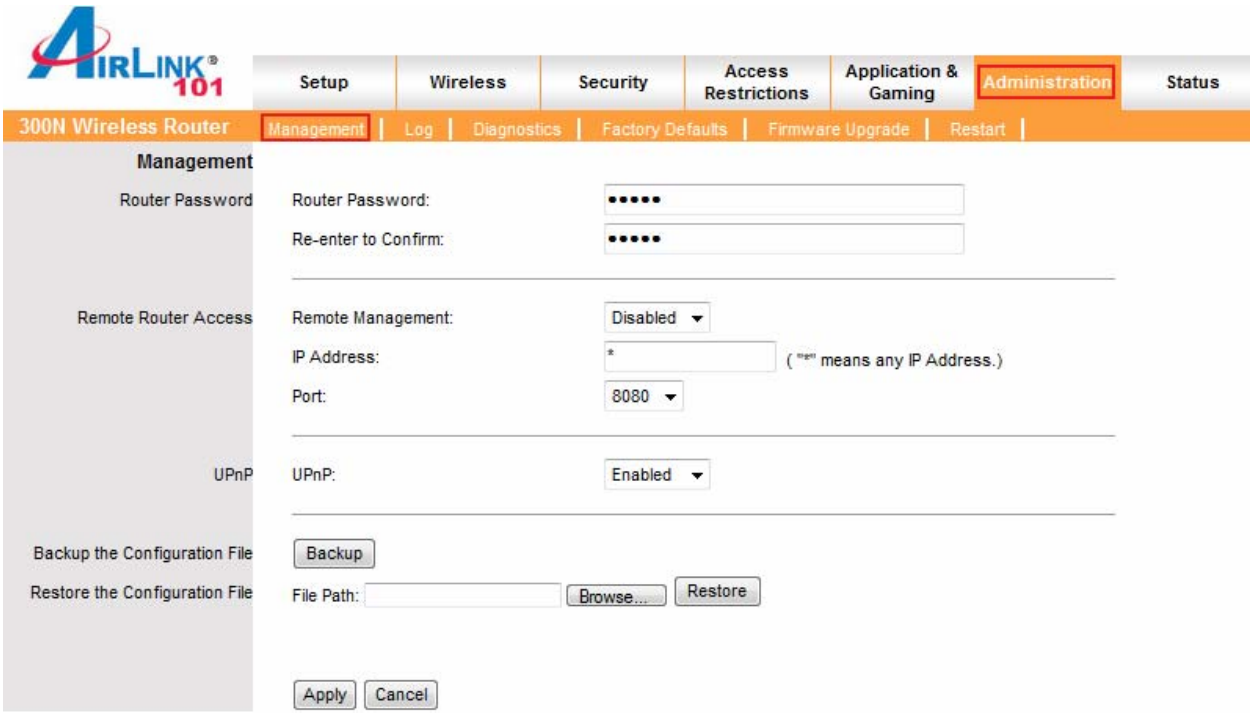
Note: Any DMZ host should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

Click **Apply** and **OK** to save the settings.

6.6 Administration

6.6.1 Management

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



Router Password: Set the router's login password.

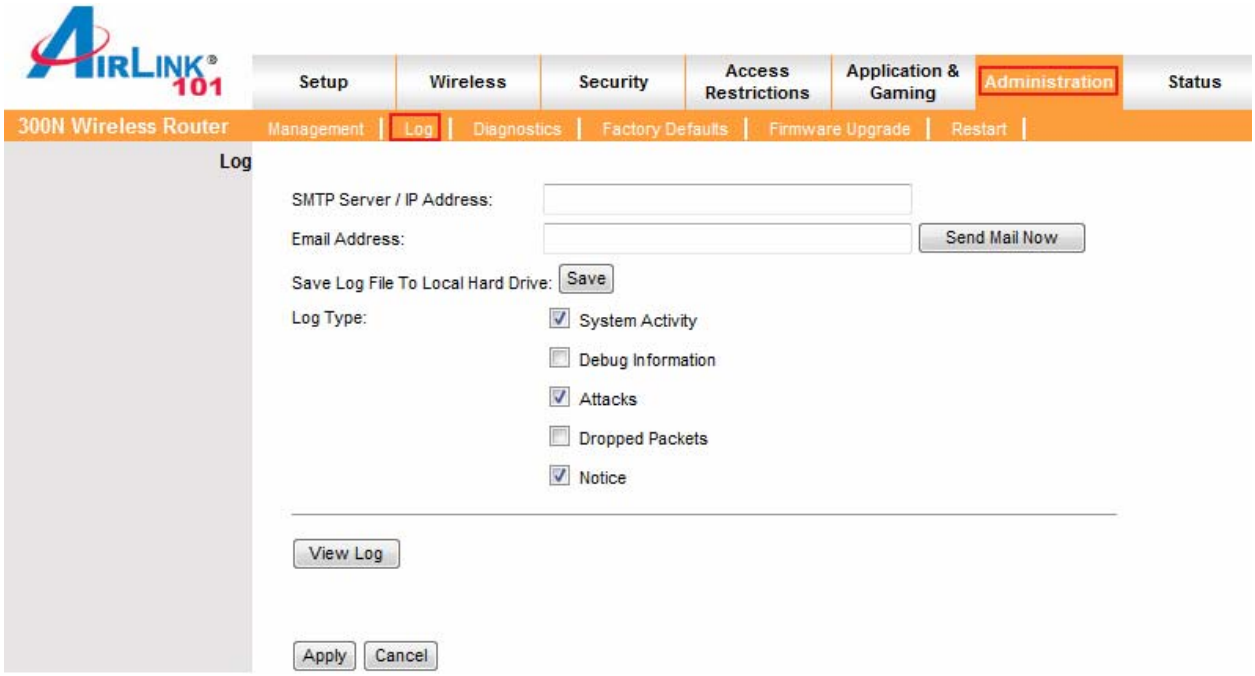
Remote Router Access: Select to enable or disable remote management/upgrade of the router. You can allow remote management from any IP Address or a specified IP Address as well as the port number.

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.

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.

6.6.2 Log

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



SMTP Server / IP Address: Enter your internet service provider's outgoing email server address.

Email Address: Enter an email address where you would like the log to be sent.

Send Mail Now: Send the log file to the specified the email address.

Save Log File to Local Hard Drive: Save the current log information to a file on your computer.

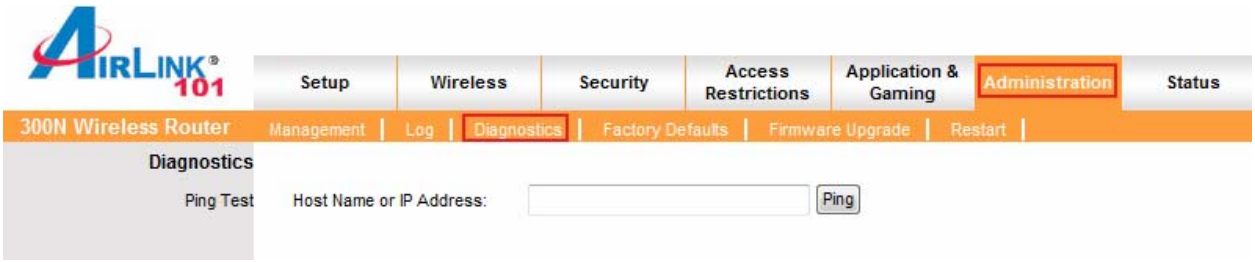
Log Type: Specify the information you want the system to log. Options include System Activity, Debug Information, Attacks, Dropped Packets, and Notice.

View Log: Allows you to see logged information related to System Activity, Debug Information, Attacks, Dropped Packets, and Notice.

Click **Apply** and **OK** to save the settings.

6.6.3 Diagnostics

The Diagnostics screen allows you to perform **Ping** tests.



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

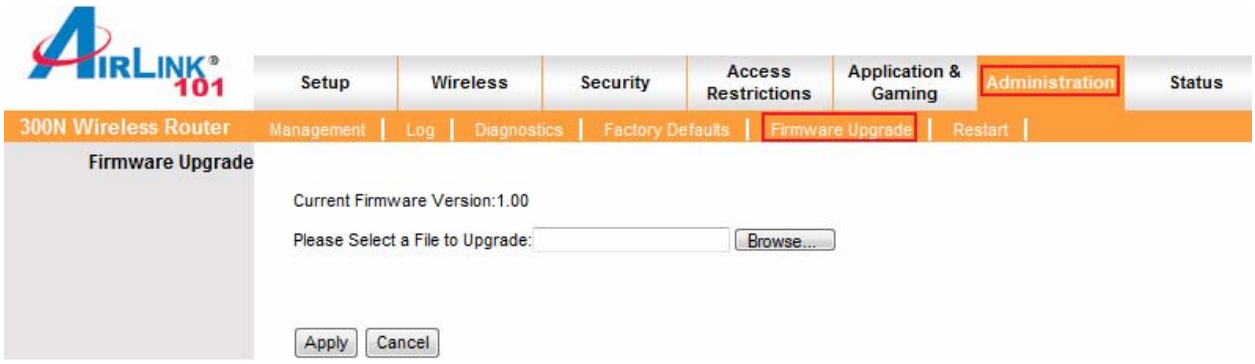
6.6.4 Factory Defaults

The Factory Defaults screen allows you to set all the router's settings to the factory default. You can use this anytime you think that you've changed settings that have stopped the router from working. Resetting to defaults will undo all of your changes.

Click on the **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.



You may download the new firmware from the Airlink101 website www.airlink101.com

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

Note: Do not power off the router during the firmware upgrading, otherwise your router may be damaged permanently.

6.6.6 Restart

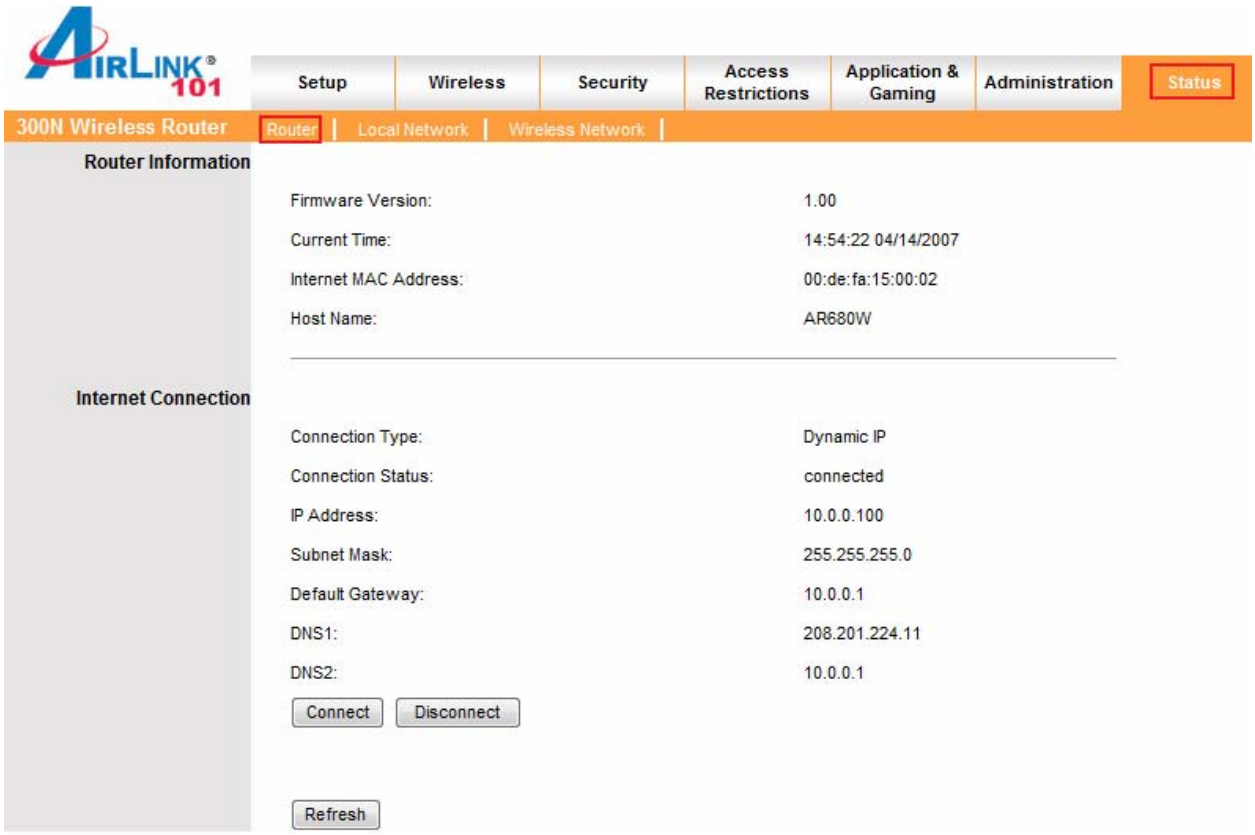
The Restart page allows you to restart the router without restoring the settings to factory default.

Click on the **Restart** button to restart the router.

6.7 Status

6.7.1 Router

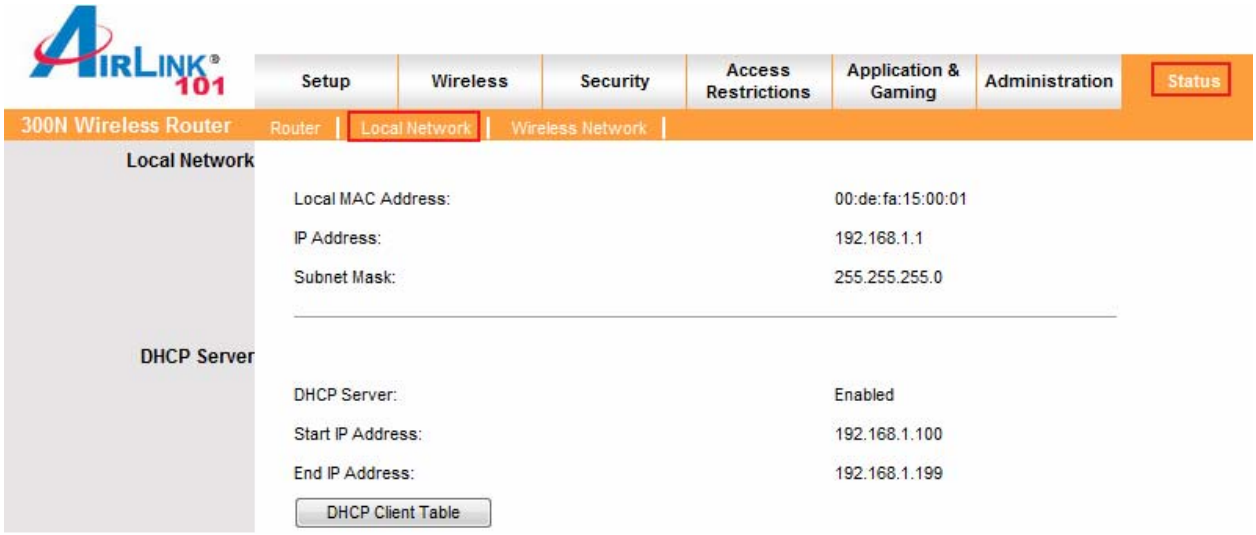
The Router screen displays a summary of all router status information, including the firmware version.



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

6.7.2 Local Network

The Local Network screen displays status information regarding your Local Area Network.



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

6.7.3 Wireless Network

The Wireless Network screen displays status information regarding your wireless network.

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.

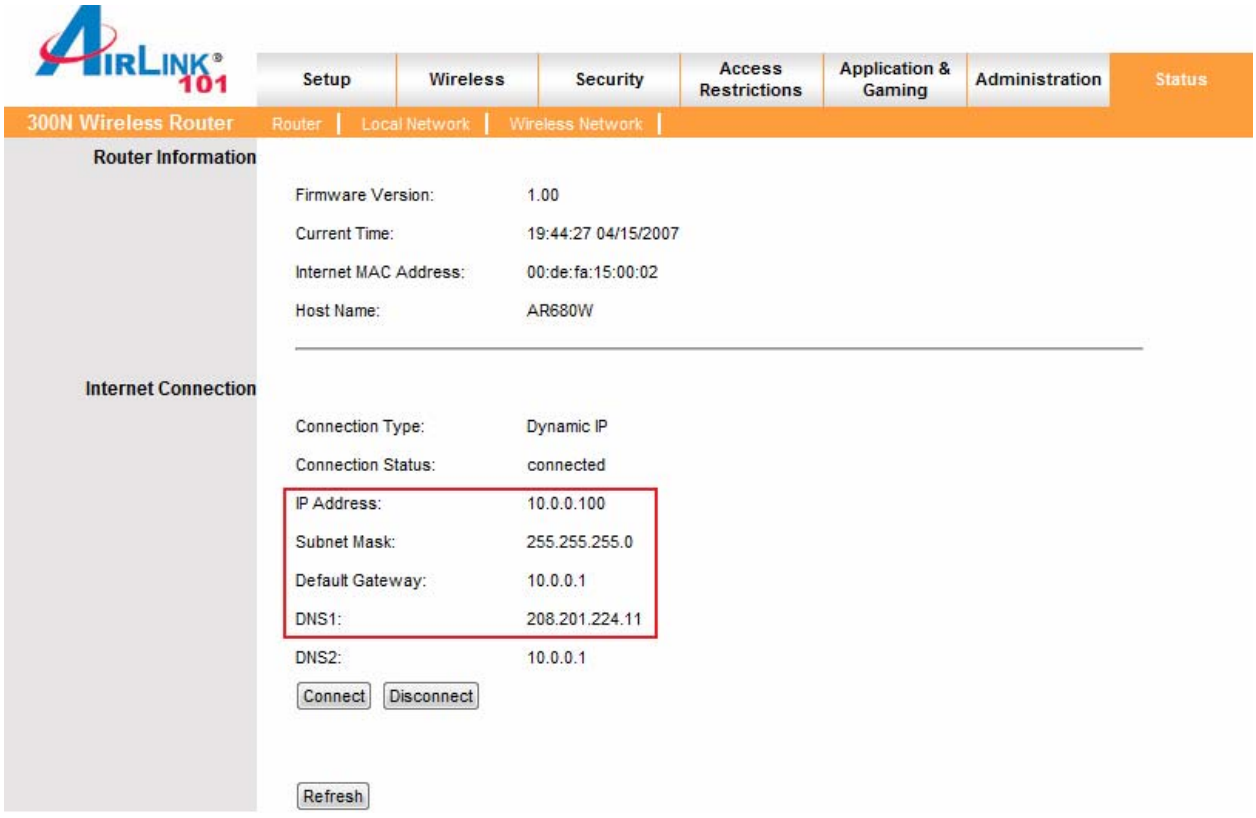
Step 3 Turn on the router and wait for the lights on the router to settle down.

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

Appendix A – Specifications

Standards
- IEEE 802.11b / 802.11g
- IEEE 802.11n draft

Chipset
- Ralink

Ports
- 1 x WAN port
- 4 x 10/100mbps LAN port

Antenna type
- 3 External 2dBi antennas

Security
- WEP 64/128-bit
- WPA2, WPA
- WMM

LEDs
- Power, Status, WAN, WLAN, LAN, WPS

Advanced Features
- Quality of Service (QoS)
- Stateful Packet Inspection (SPI) / DoS
- VPN Pass-through

WiFi Protected Setup
- PIN (Personal Identification Number)
- PBC (Push button configuration)

System Requirement
- Windows®, Mac®, or Linux® operating system
- Internet Explore 5.5 or above
- Installed Ethernet adapter
- Recommended use with 300N Wireless Adapters: AWLH6080, AWLC6080, and AWLL6080 for best performance

Power
- 5V / 2.5A

Dimensions
- 205 x 116 x 29 mm

Temperature
- Operating: 0ºC to 45ºC

Humidity
- 10% to 95% Non-Condensing

Warranty
- Limited 1-year warranty

Certification
- FCC, CE, C-Tick, UL, TUV

Appendix B – 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: 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.

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.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

European Union Notice:

Radio products with the CE marking comply with the R&TTE Directive (1999/5/EC), the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms:

- EN 60950 Product Safety
- EN 300 328 Technical requirement for radio equipment
- EN 301 489-1/-17 General EMC requirements for radio equipment

In addition to the requirements of Section 7.1.5 in RSS-Gen, the device's shall also contain the following or equivalent statement: “Privacy of communications may not be ensured when using this telephone”.

If privacy is provided as a standard feature, the privacy notice may be omitted provided that full justification accompanies the equipment certification application for evaluation by Industry Canada.

Technical Support

E-mail: support@airlink101.com

Toll Free: 1-888-746-3238

Web Site: www.airlink101.com

*Theoretical maximum wireless signal rate derived from IEEE 802.11g standard and IEEE 802.11n draft specification version 1.1. 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. Specifications are subject to change without notice. All products and trademarks are the property of their respective owners. Copyright ©2007 AirLink101®