Wireless 802.11ag AP Router

User’s Manual

Version 1.4

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.
If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted in indoor environment only.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The WX-7615A (FCC ID: RYK-7615A) is limited in CH1~CH11 for 2.4 GHz by specified firmware controlled in U.S.A.

Copyright Statement

March. 2005

Contents

1. Introduction

Thank you for purchasing your Wireless 802.11ag AP Router.

This user guide will assist you with the installation procedure.

The package you have received should contain the following items:

- Wireless 802.11ag AP Router
- Quick Installation Guide
- User Manual CD-ROM
- Detachable Antenna
- Universal AC/DC Power Adapter
- RJ-45 Network Cable

Note: if anything is missing, please contact your vendor

2. Safety Notification

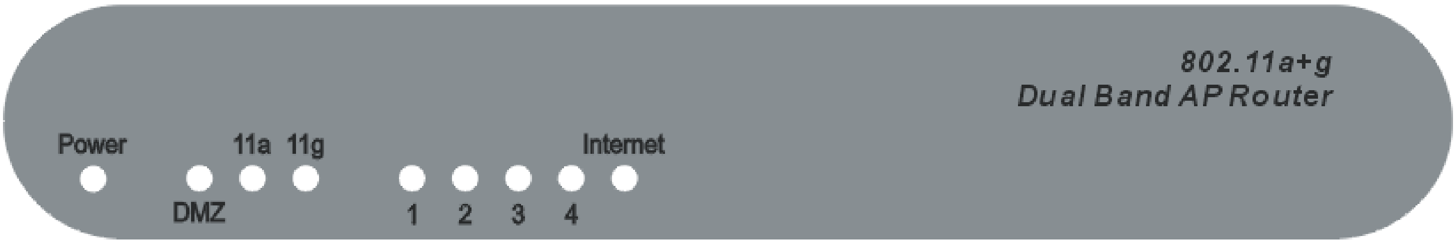
Your Wireless AP Router should be placed in a safe and secure location. To ensure proper operation, please keep the unit away from water and other damaging elements. Please read the user manual thoroughly before you install the device.
The device should only be repaired by authorized and qualified personnel.

- Please do not try to open or repair the device yourself.
- Do not place the device in a damp or humid location, i.e. a bathroom.
- The device should be placed in a sheltered and non-slip location within a temperature range of +5 to +40 Celsius degree.
- Please do not expose the device to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.

3. Hardware Installation

Front Panel

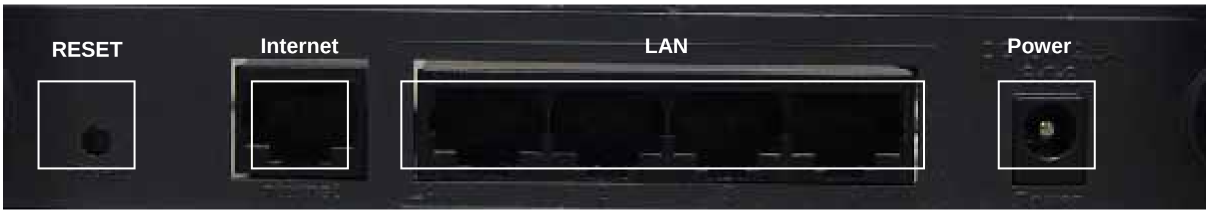
The front panel provides LED's for device status. Refer to the following table for the meaning of each feature.



Power	The **Power** LED lights up and will keep while the Router is powered on. When the Router goes through its self-diagnostic mode during every boot-up, this LED will flash. When the diagnostic is complete, the LED will be lit continuously.
DMZ	The **DMZ** LED indicates when the DMZ function is being used. This LED will remain lit as long as DMZ is enabled.
11a	The **11a** LED flashes when there is a successful Wireless-A connection.
11g	The **11g** LED flashes when there is a successful Wireless-G connection.
Ethernet	**LED 1, 2, 3, 4**. These numbered LEDs, corresponding with the numbered ports on the Router's rear panel. If the LED is continuously lit, the Router is successfully connected to a device through that port. A flashing LED indicates network activity over that port.
Internet	The **Internet** LED lights up when there is a connection built through the Internet port.

Rear Panel

The rear panel features 4 LAN ports, 1 WAN port and Reset button. Refer to the following table for the meaning of each feature.



RESET Button	The **RESET button** can restore device to factory default settings by press this button for approx. 10 seconds during device power on status.
Internet	The **Internet** port is where you will connect your broadband Internet connection.
LAN 1,2,3,4	These ports (1, 2, 3, 4) connect the Router to your networked PCs and other Ethernet network devices.
Power	The **POWER** port is where you will connect the power adapter.

AP Router Default Settings

User	
Password	admin
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
RF ESSID	A band: wlan-a G band: wlan-g
Channel	A band: Auto G band: 6
Mode	G band: Mixed
Encryption	Disabled
DHCP Server	Enabled

Hardware Installation for Connection to Your Broadband Modem

1. Power off your network devices.

2. Locate an optimum location for the Router. The best place for the Router is usually at the center of your wireless network, with line of sight to all of your wireless devices.

3. Adjust the antennas. Normally, the higher location of your Router will get better the performance.

4. Using a standard Ethernet network cable, connect the Router’s Internet port to your broadband modem.

5. Connect your network PCs or Ethernet devices to the Router’s LAN ports using standard Ethernet network cabling.

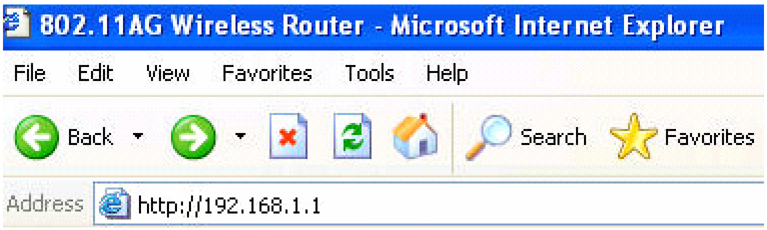
6. Connect the AC power adapter to the Router's Power port. Then connect the other end to an electrical outlet. Only use the power adapter supplied with the Router. Use of a different adapter may cause product damage.

7. The Hardware installation is complete, please refer to the following content for Router configuration.

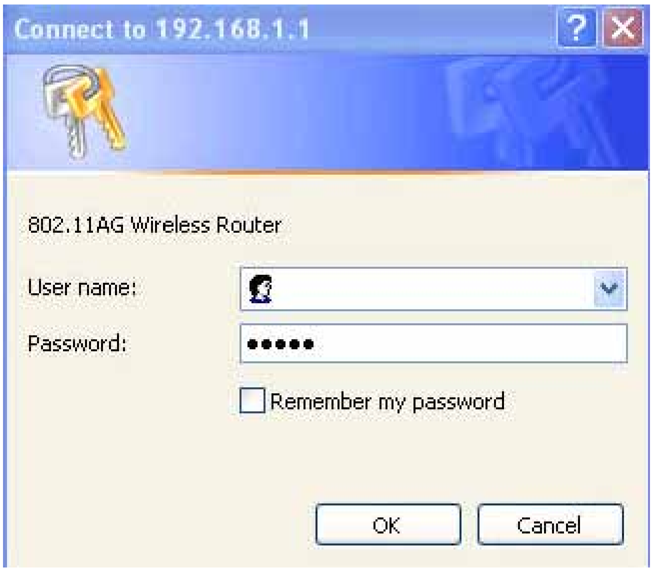
4. How to Configuring the Dual Band Router

TURN ON POWER SUPPLY
Quick power cycle would caused system corruption. When power on, be careful not to shut down in about 5 seconds, because data is writing to the flash.

START UP & LOGIN
In order to configure the Wireless 11ag Router, you must use web browser and manually input http://**192.168.1.1** into the Address box and press Enter. The Main Page will appear.


802.11AG Wireless Router - Microsoft Internet Explorer

http://192.168.1.1


Connect to 192.168.1.1

802.11AG Wireless Router

User name:

Password: ●●●●●

□ Remember my password

In order to configure the Wireless 11ag Router, you must input the password into the **Password** box and leave blank on the **User Name** box. The default password is “**admin**”.

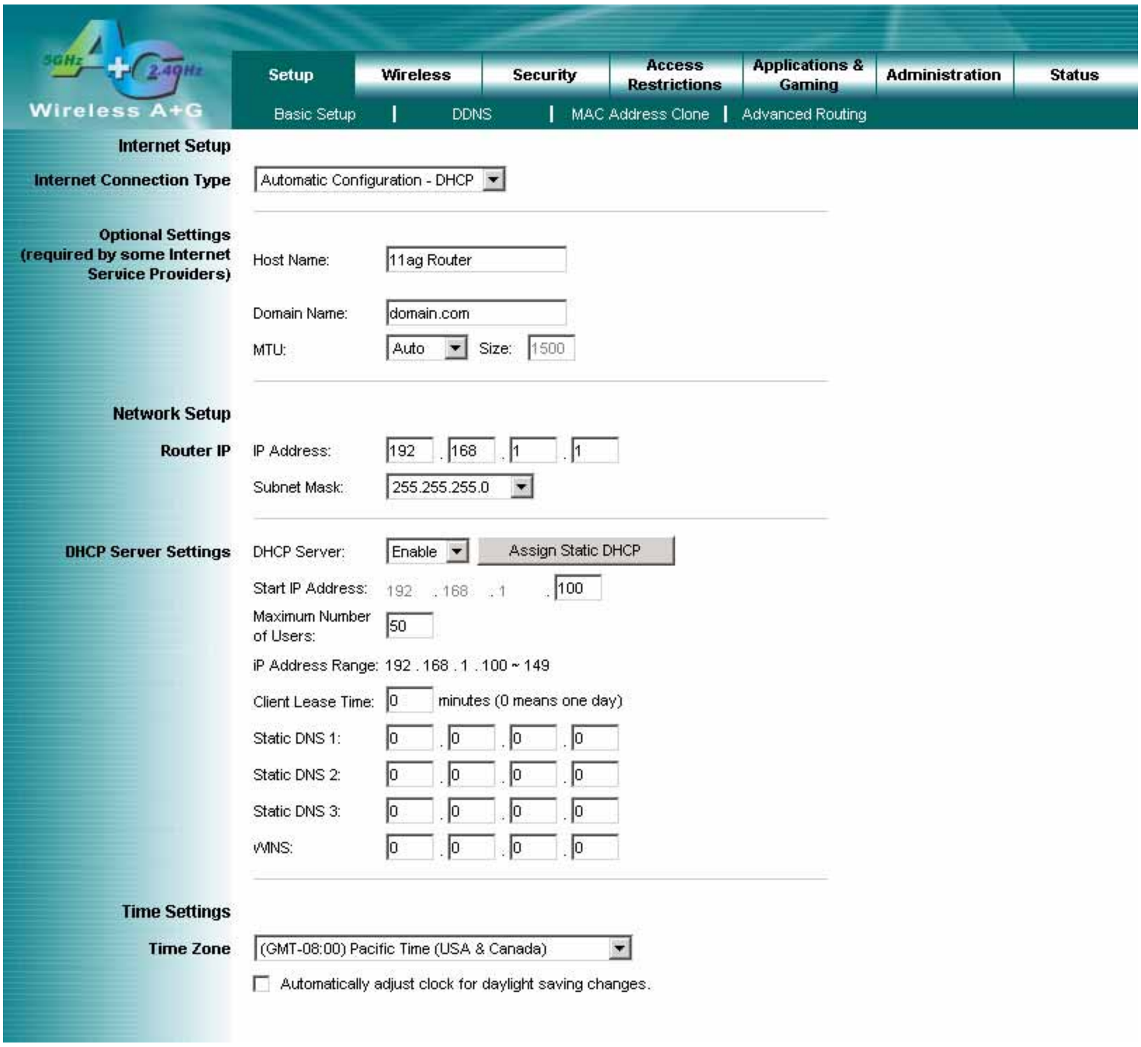
Once you have logged-in as administrator, it is a good idea to change the administrator password to ensure a secure protection to the Wireless 11ag Router. The Security Settings section described later in this manual describes how to change the password.

Once you have input the correct password and logged-in, the screen will change to the Setup page screen.

4.1 Setup – Basic Setup

MAKE CORRECT NETWORK SETTINGS OF YOUR COMPUTER
To change the configuration, use Internet Explorer (IE) or Netscape Communicator to connect the WEB management **192.168.1.1**.

This following screen contains all of the Router's basic setup functions.



Internet Setup

Internet Connection Type: Automatic Configuration - DHCP

Optional Settings (required by some Internet Service Providers)

Host Name: 11ag Router

Domain Name: domain.com

MTU: Auto Size: 1500

Network Setup

Router IP

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0

DHCP Server Settings

DHCP Server: Enable

Start IP Address: 192 . 168 . 1 . 100

Maximum Number of Users: 50

IP Address Range: 192 . 168 . 1 . 100 ~ 149

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 0 . 0 . 0 . 0

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

Time Settings

Time Zone: (GMT-08:00) Pacific Time (USA & Canada)

☐ Automatically adjust clock for daylight saving changes.

Most users will be able to configure the AP Router and get it working properly using the settings on this screen. Some Internet Service Providers (ISPs) will require that you enter broadband specific information into this device, such as User Name, Password, IP Address, Default Gateway Address, or DNS IP Address for Internet access. This information can be obtained from your ISP, if required.

Internet Setup

Internet Connection Type:

- **Automatic Configuration – DHCP**

  This' s default connection type. If your ISP supports DHCP assigning dynamic IP address then please select this type.

- **Static IP**

  If you are required to use a fixed IP address to connect to the Internet, then select **Static IP**.
  Internet IP Address: This' s the Router's WAN IP address. Usually it will provide by your ISP, and need to input here.
  Subnet Mask: This' s the Router's Subnet Mask, Usually it will provide by your ISP, and need to input here.
  Default Gateway: This' s the Router's Gateway Address, Usually it will provide by your ISP, and need to input here.
  DNS (1-3): Your ISP will provide you at least one DNS Server IP Address and need to input here.

- **PPPoE**

  PPPoE (Point-to-Point Protocol over Ethernet) is one of Internet connections type. If you are connected to the

Internet through a DSL line, check with your ISP to see if they use PPPoE type. If yes, you will have to enable **PPPoE**.

User Name and Password: Enter the User Name and Password provided by your ISP.

Connect on Demand: The Max Idle Time means the Router will disconnect the Internet connection if there is no any traffic through this Router during a specified period time. If your Internet connection has been terminated due to over this idle time, the Connect on Demand option will trigger the Router to automatically re-establish your connection as soon as you try to access the Internet again.

Keep Alive: The Redial Period means the Router will periodically check your Internet connection by Redial Period time. If the connection is disconnected, then the Router will redial automatically for your connection.

♦ **PPTP**

Point to Point Tunneling Protocol (PPTP), is one of VPN tunnel that can use to encrypt data and prevent the unauthorized viewing of confidential data that is transmitted across publish networks.

Internet IP Address and Subnet Mask: This' s the Routers IP Address and Subnet Mask. If your Internet connection requires a static IP address, then your ISP will provide you a Static IP Address and Subnet Mask for input here.

Default Gateway: Your ISP will provide you with the Gateway IP Address.

User Name and Password: This' s PPTP login User Name and Password. Your ISP will provide you such information for input here.

Keep Alive: The Redial Period means the Router will periodically check your Internet connection by Redial Period time. If the connection is disconnected, then the Router will redial automatically for your connection.

These types can be selected from the Internet Connection Type drop-down menu. The information required and available features with minor different that depend on what kinds of connection type you are selected.

Optional Settings

These settings may be required by your ISP. If your ISP would provide such information, please note to specify them into your device.

Host Name and Domain Name: These fields allow you to input a host and domain name for the Router. Some ISPs require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.

MTU: MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Select **Manual** if you want to manually enter the largest packet size that will be transmitted. The recommended size, entered in the *Size* field, is 1500. You should leave this value in the 1200 to 1500 range. To have the Router select the best MTU for your Internet connection, please select the default setting--**Auto**.

Network Setup

The Network Setup section changes the Router's local network settings.

Router IP

IP Address and Subnet Mask. This' s Router's LAN IP Address and Subnet Mask. The default IP Address is **192.168.1.1** and the default Subnet Mask is **255.255.255.0**.

DHCP Server Settings

The settings allow you to configure the Router's Dynamic Host Configuration Protocol (DHCP) server function. The Router can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer on your network. If you choose to enable the Router's DHCP server option, you must make sure there is no other DHCP server on your network. If you disable the Router's DHCP server function, you must configure the IP Address, Subnet Mask, and DNS for each network computer (note that each IP Address must be unique).

DHCP Server: DHCP is enabled by factory default. If you already have a DHCP server on your network or you do not want a DHCP server, then select **Disable** from the options.

Assign Static DHCP: The function can enable DHCP server to assign a same IP address for appointed PC. If you want a PC to be assigned the same IP address every time when it reboots, then click the **Assign Static IP** button.

How to set a PC as Static DHCP client
On the *Static DHCP Client List* screen, enter the static local IP address in the *Assign this IP* field, and enter the MAC address of the PC in the *To this MAC* field. Then click the **Enabled** checkbox. When you have finished your entries, click the **Save Settings** button to save your changes.
Click the **Cancel Changes** button to cancel your changes. To exit this screen, click the **Close** button.

How to set a DHCP client as Static DHCP client
Click the **DHCP Client Table** button can see a list of DHCP client. On the *DHCP Client Table*, you will see a list of DHCP clients with the following information: Client Names, Interfaces, IP Addresses, and MAC Addresses. From the *To Sort by* drop-down menu, you can sort the table by Client Name, Interface, IP Address, or MAC Address. If you want to add any of the DHCP clients to the Static DHCP Client List, then click the **Save to Static DHCP Client List** checkbox and then click the **Save Settings** button. Click the **Cancel Changes** button to cancel your changes. To view the most up-to-date information, click the **Refresh** button. To exit this screen, click the **Close** button.

Start IP Address: Enter a value for the DHCP server to start with when issuing IP addresses. Because the Router’s default IP address is 192.168.1.1, the Starting IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.254. The default Starting IP Address is **192.168.1.100**.

Maximum Number of Users: Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The absolute maximum is 253 - possible if 192.168.1.1 is your starting IP address. The default is **50.**

IP Address Range: The range of DHCP addresses. This range is according to the setting of Maximum Number of Users.

Client Lease Time: The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be “leased” this dynamic IP address. Once the leased time is up, the user will get a new dynamic IP address automatically. The default is 0 minutes, which means one day.

Static DNS 1-3: The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. If you wish to utilize another, enter that IP Address in one of these fields. You can enter up to 3 DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.

WINS: The Windows Internet Naming Service (WINS) manages each PC’s interaction with the Internet. If you use a WINS server, enter that server’s IP Address here. Otherwise, leave this blank.

Time Settings
Change the time zone in which your network functions from this pull-down menu. Click the checkbox if you want the Router to automatically adjust for daylight savings time.

Change these settings as described here and click the **Apply** button to apply your changes or click **Cancel** to cancel your changes. For additional information, click **Help**.

4.2 Setup – DDNS

The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router. Before using this feature, you need to sign up for DDNS service with one of two DDNS service providers, DynDNS.org or TZO.

DynDNS service

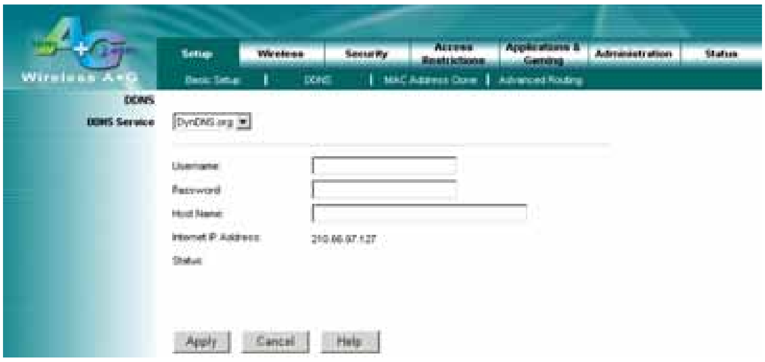
To enable DDNS Service using DynDNS.org, follow these instructions:

1. On the *DDNS* screen, select **DynDNS.org** from the *DDNS Service Provider* drop-down menu.

2. Sign up for DynDNS service at *www.dyndns.org* for applying one DDNS account. Write down your account information.

3. Complete the *User Name*, *Password*, and *Host Name* fields.

4. Click the **Apply** button to save your changes. Click the **Cancel** button to cancel unsaved changes.



DDNS
DDNS Service: DynDNS.org
Username:
Password:
Host Name:
Internet IP Address: 210.66.97.127
Status:

TZO service

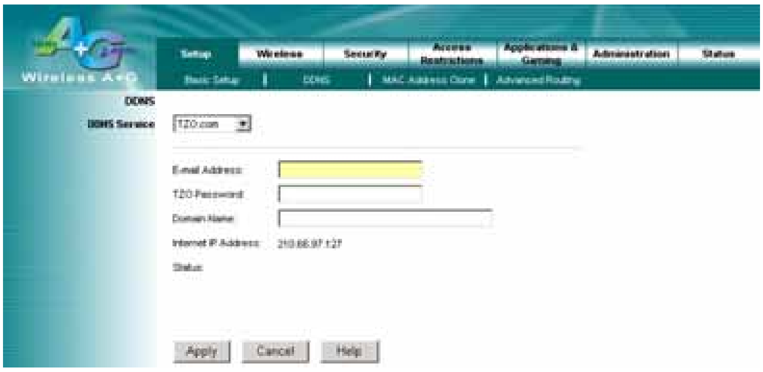
To enable DDNS Service using TZO, follow these instructions:

1. On the *DDNS* screen, select **TZO.com** from the *DDNS Service Provider* drop-down menu.

2. Sign up for a free, 30-day trial of TZO service at *www.tzo.com/order.html* . Write down your account information.

3. Complete the *Email Address*, *TZO Password Key*, and *Domain Name* fields.

4. Click the **Apply** button to save your changes. Click the **Cancel** button to cancel unsaved changes.



DDNS
DDNS Service: TZO.com
E-mail Address:
TZO Password:
Domain Name:
Internet IP Address: 210.66.97.127
Status:

Internet IP Address: The Router's current Internet IP Address is displayed here.

Status: The status of the DDNS service connection is displayed here.

Change these settings as described here and click the **Apply** button to apply your changes or click **Cancel** button to cancel your changes. For additional information, click **Help**.

4.3 Setup – MAC Address Clone

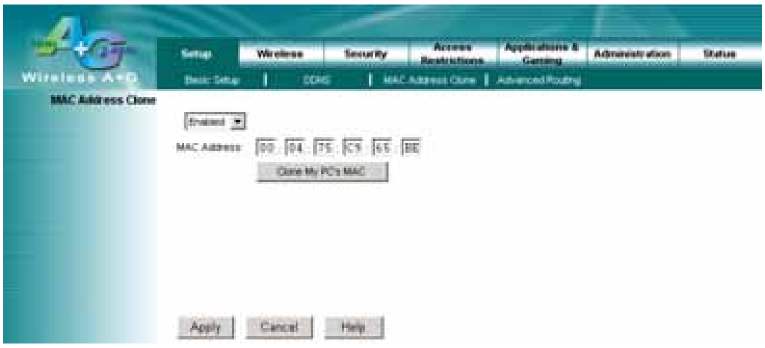
A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs will require you to register a MAC address in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you may assign the MAC address you have currently registered with your ISP to the Router with the MAC Address Clone feature.

MAC Address Clone

Enabled/Disabled: To have the MAC Address cloned, select **Enabled** from the drop-down menu.

MAC Address: Enter the MAC Address registered with your ISP here.

Clone My PC's MAC: Clicking this button will clone the MAC address of the PC you are currently using.



MAC Address Clone

Enabled

MAC Address: 00 : 04 : 75 : C9 : 65 : BE

Change these settings as described here and click the **Apply** button to apply your changes or click **Cancel** button to cancel your changes. For additional information, click **Help**.

4.4 Setup – Advanced Routing

The Advanced Routing is used to set up the Routers advanced functions. Operating Mode allows you to select the type of routing functions. Dynamic Routing will automatically adjust how packets travel on your network. Static Routing sets up a fixed route to another network destination.

Operating mode:

If this Router is hosting your networks connection to the Internet, select **Gateway**. If another Router exists on your network, select **Router**. When Router is chosen, Dynamic Routing will be **enabled**.

Dynamic Routing

This feature enables the Router to automatically adjust to physical changes in the networks layout and exchange routing tables with the other router(s). The Router determines the network packets route based on the fewest number of hops between the source and the destination. This feature is **Disabled** by default.

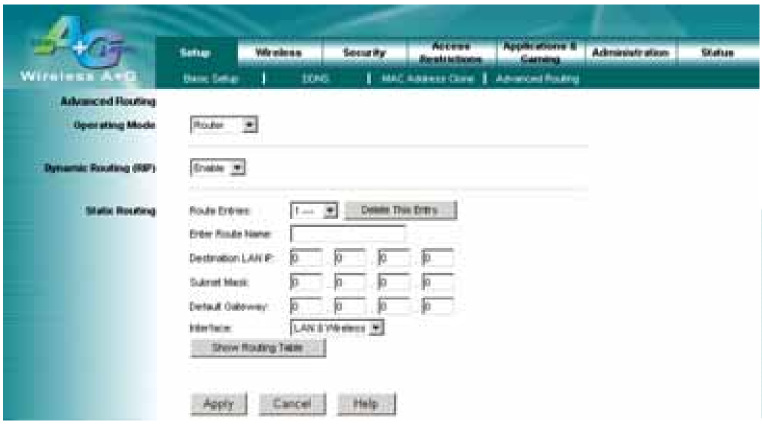
Static Routing

To set up a static route between the Router and another network, select a number from the *Static Routing* drop-down list. (A static route is a pre-determined pathway that network information must travel to reach a specific host or network.) Enter the information described below to set up a new static route. (Click the Delete This Entry button to delete a static route.)

- ♦ **Destination LAN IP:** The Destination LAN IP is the address of the remote network or host to which you want to assign a static route.
- ♦ **Subnet Mask:** The Subnet Mask determines which portion of a Destination LAN IP address is the network portion, and which portion is the host portion.
- ♦ **Default Gateway:** This is the IP address of the gateway device that allows for contact between the Router and the remote network or host.
- ♦ **Interface** - This interface tells you whether the Destination IP Address is on the **LAN & Wireless** (internal wired and wireless networks) , **WAN** (Internet) or **Loopback** (a dummy network in which one PC acts like a network—necessary for certain software programs)..

Show Routing Table

Click the **Show Routing Table** button to view all of the valid route entries in use. The Destination IP address, Subnet Mask, Gateway, and Interface will be displayed for each entry. Click the **Refresh** button to refresh the data displayed or click the **Close** button to close the window.



Advanced Routing

Operating Mode: Router

Dynamic Routing (RIP): Enable

Static Routing

Route Entries: 1 ---

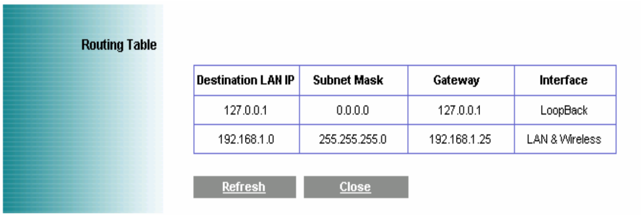
Enter Route Name:

Destination LAN IP: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Default Gateway: 0 . 0 . 0 . 0

Interface: LAN & Wireless



Routing Table

Destination LAN IP	Subnet Mask	Gateway	Interface
127.0.0.1	0.0.0.0	127.0.0.1	LoopBack
192.168.1.0	255.255.255.0	192.168.1.25	LAN & Wireless

Change these settings as described here and click the **Apply** button to apply your changes or click **Cancel** button to cancel your changes. For additional information, click **Help**.

4.5 Wireless – Basic Wireless Settings

Wireless Network

Wireless-A Settings

If you are using a Wireless-A network, then the following settings that you may need to configure.
Mode: This mode is controlling the Wireless-A (802.11a) networking, **Enabled** or **Disabled**.

Turbo Mode: Using this mode enables high-speed connections but severely limits range. To perform this Turbo Mode, both the Router and wireless PCs must support this function. Turbo Mode is Atheros proprietary technology, so it does not compatible with non-Atheros chipset Wireless LAN device, only with Atheros Wireless-A turbo adapters. To increase the speed of your wireless transmissions up to 108 Mbps, select **Enabled.** (Note: the Router's range will decrease in Turbo Mode.) If you do not want to use Turbo Mode, select **Disabled**.

Network Name (SSID): The service set identifier (SSID) or network name. It is case sensitive and must not exceed 32 characters, which may be any keyboard character. You shall have selected the same SSID for all the APs that will be communicating with mobile wireless stations.

Channel: Select the appropriate channel from the list provided to correspond with your network settings. You shall assign a different channel for each AP to avoid signal interference. If you want the Router to automatically scan for a clear channel, then select **Auto (DFS)**.

SSID Broadcast: When wireless clients survey the local area for wireless networks associated, they will detect the SSID broadcast by the Router. To broadcast the Router's SSID, keep the default setting, **Enabled**. If you do not want to broadcast the Router's SSID, then select **Disabled**.

Wireless-G Settings

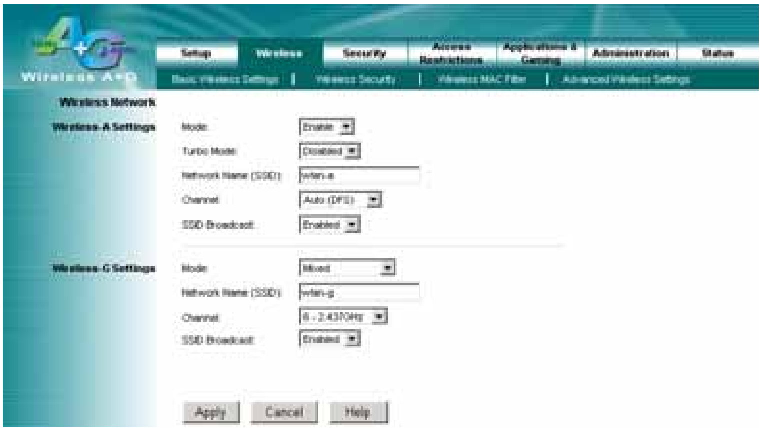
If you are using a Wireless-B, Wireless-G, or Wireless B+G network, then the following settings that you may need to configure.

Mode: From this drop-down menu, you can select the wireless standards running on your network. If you have both 802.11g and 802.11b devices in your network, keep the default setting ---**Mixed**. If you have only 802.11g devices, select **Wireless-G Only**. If you have only 802.11b devices, select **Wireless-B Only**. If you do not have any 802.11g and 802.11b devices in your network, select **Disabled**.

Network Name (SSID): The service set identifier (SSID) or network name. It is case sensitive and must not exceed 32 characters, which may be any keyboard character. You shall have selected the same SSID for all the APs that will be communicating with mobile wireless stations.

Channel: Select the appropriate channel from the list provided to correspond with your network settings. You shall assign a different channel for each AP to avoid signal interference.

SSID Broadcast: When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router's SSID, keep the default setting, **Enabled**. If you do not want to broadcast the Router's SSID, then select **Disabled**.



Wireless Network

Wireless-A Settings

Mode:	Enable
Turbo Mode:	Disabled
Network Name (SSID):	wlan-a
Channel:	Auto (DFS)
SSID Broadcast:	Enabled

Wireless-G Settings

Mode:	Mixed
Network Name (SSID):	wlan-g
Channel:	6 - 2.437GHz
SSID Broadcast:	Enabled

Change these settings as described here and click the **Apply** button to apply your changes or click **Cancel** button to cancel your changes. For additional information, click **Help**.

4.6 Wireless – Wireless Security

The Wireless Security settings configure the security of your wireless network. There are three wireless security mode options supported by the Router: WEP (Wired Equivalent Privacy), WPA Pre-Shared Key, WPA RADIUS.

Wireless Security

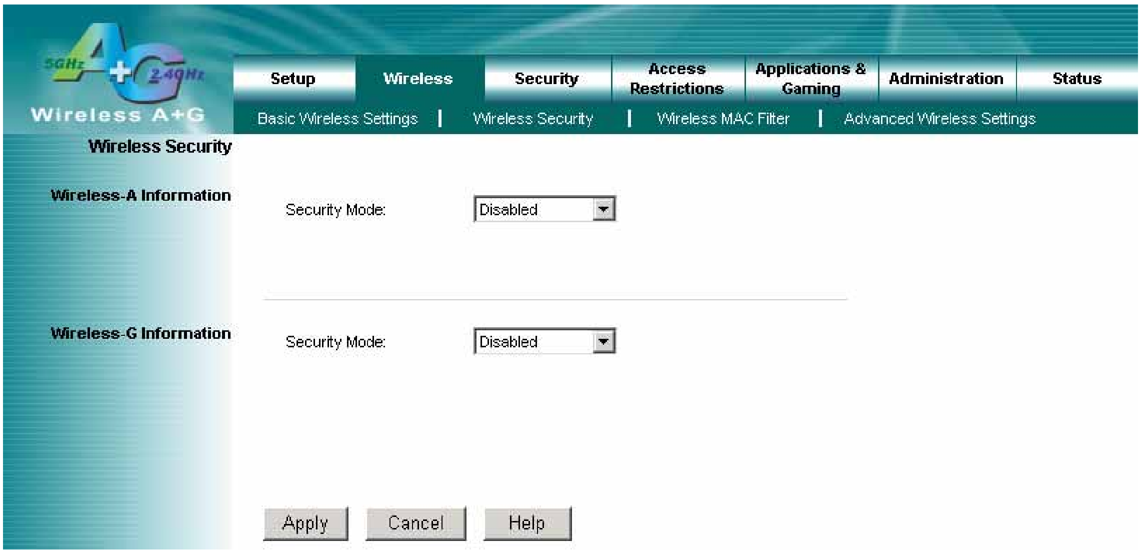
The security options are the same and independent for your Wireless-A and Wireless-G networks. You can use different wireless security methods for your networks; however, within each network (Wireless-A or Wireless-G), all devices must use the same security method and settings.

Security Mode:

WEP: WEP is a basic encryption method, select a level of WEP encryption, **40/64-bit** or **128-bit**. If you want to use a Passphrase, then enter it in the *Passphrase* field and click the **Generate** button. If you want to enter the WEP key manually, then enter it in the *WEP Key 1-4* field(s). To indicate which WEP key to use, select the appropriate *TX Key* number.

WPA Pre-Shared Key: This security mode offers two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of encryption method you want to use, **TKIP** or **AES**. Enter the Passphrase, which can have 8 to 63 characters. Then enter the Key Renewal period, which instructs the Router how often it should change the encryption keys.

WPA RADIUS: This security mode must work with a RADIUS server using EAP –TLS or PEAP for user authentication. To use WPA RADIUS, select the type of encryption method you want to use, **TKIP** or **AES**.
Enter the RADIUS server's IP address and port number (default is 1812), along with the authentication shared key by the Router and the server.
Enter the Key Renewal period, which instructs the Router how often it should change the encryption keys.



Wireless Security

Wireless-A Information

Security Mode: Disabled

Wireless-G Information

Security Mode: Disabled

4.7 Wireless – Wireless MAC Filter

This function allows administrator to have access control by enter MAC address of wireless devices which transmitting within your wireless network.

Wireless MAC Filter

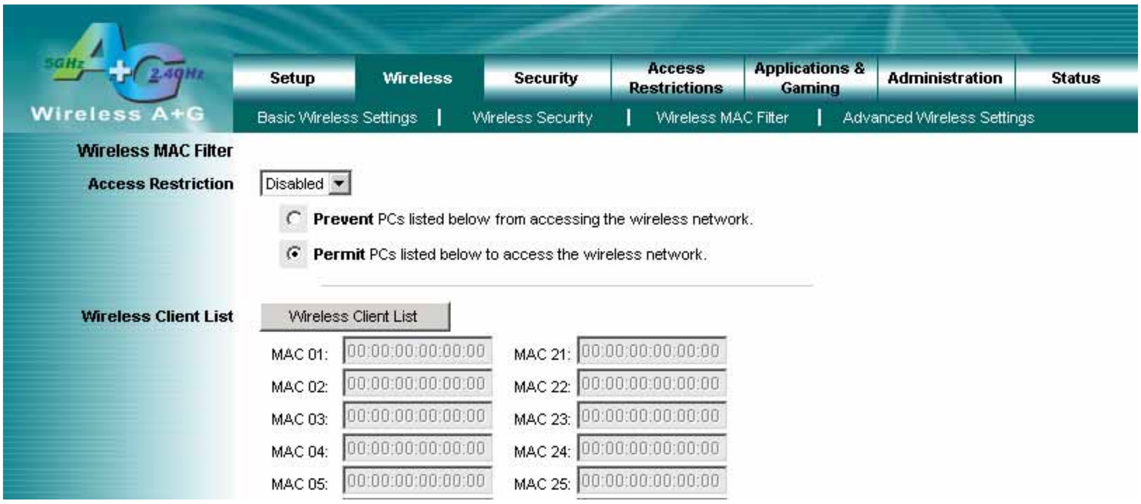
Access Restrictions
This policy can effectively control each wireless device using the wireless network. Enable this function to filter wireless devices by MAC Address, either permitting or blocking access. If you do not want to filter users by MAC Address, select **Disabled**.

Prevent PCs listed below from accessing the wireless network: Select this option will block selected wireless client by MAC address.

Permit PCs listed below to access the wireless network: Select this option will permit selected wireless client by MAC Address.

Wireless Client List

Wireless Client List: Click the **Wireless Client MAC List** button to display a list of wireless clients by MAC Address. From the *To Sort by* drop-down menu, you can sort the table by Client Name, Interface, IP Address, MAC Address. If you want to add any of the wireless clients to the Wireless MAC Filter List, then click the **On the List** checkbox and then click the **Save Settings** button. Click the **Cancel Changes** button to cancel your changes. To view the most updated information, click the **Refresh** button. To exit this screen, click the **Close** button.



Wireless MAC Filter

Access Restriction: Disabled

○ **Prevent** PCs listed below from accessing the wireless network.

● **Permit** PCs listed below to access the wireless network.

Wireless Client List

MAC 01:	00:00:00:00:00:00	MAC 21:	00:00:00:00:00:00
MAC 02:	00:00:00:00:00:00	MAC 22:	00:00:00:00:00:00
MAC 03:	00:00:00:00:00:00	MAC 23:	00:00:00:00:00:00
MAC 04:	00:00:00:00:00:00	MAC 24:	00:00:00:00:00:00
MAC 05:	00:00:00:00:00:00	MAC 25:	00:00:00:00:00:00

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. For additional information, click **Help**.

4.8 Wireless – Advanced Wireless Settings

This section provides Router's advanced wireless settings. These settings should be adjusted carefully. Any improper settings will affect the Router's wireless performance.

Advanced Wireless

Wireless-A Settings

Authentication Type:

Open System: This is default setting, those wireless clients that NOT use a WEP key for authentication.
Shared Key: This option means the wireless clients use a WEP key for authentication. Shared Key is only available if the WEP option is implemented.

Transmission Rate: The data transmission rate should be set depending on the speed of your wireless network. You can select a proper transmission speeds to fit your wireless clients requirement, or you can select **Auto (Default)** to have the Router automatically adjust one the fastest and suitable data rate to fit network status at the time. Usually this function can be named Auto-Fallback feature. Auto-Fallback will treat one best connection rate between the Router and a wireless client. The default value is **Auto (Default)**.

Transmission Power: This option provides the Router's RFoutput power adjustment. To minimize the possibility of eavesdropping by unauthorized wireless users, suggest to decrease the transmission power with a needed by your wireless environment. By drop down menu, you can select the appropriate level, **Full (Default)**, **Half**, **Quarter**, **Eighth**, or **Min**. The default is **Full (Default)**.

Frame Burst Mode: This option can trigger your wireless network with higher performance. However, it should depend on the manufacturer of your wireless products, the default is **Enabled**.

Beacon Interval: The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1000. A beacon is a packet broadcast by the Router to synchronize the wireless network. The default value is **100**.

DTIM Interval: This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.
The default value is **1**.

Fragmentation Threshold: This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of **2346**.

Beacon interval*: The data transmitted on your wireless network that keeps the network synchronized.*

DTIM*: A message included in data packets that can increase wireless efficiency.*

Fragmentation*: Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.*

RTS Threshold: Using this setting can regulate your wireless network if you experience any inconsistent data flow situation, only by minor adjustment of the default value, the default value **2346** is recommended. The RTS/CTS mechanism will not be enabled if your wireless network packet less than RTS threshold value. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should keep at its default value of **2346**.

Wireless-G Settings

Authentication Type:

Open System: This is default setting, those wireless clients that NOT use a WEP key for authentication.
Shared Key: This option means the wireless clients use a WEP key for authentication. Shared Key is only available if the WEP option is implemented.

Basic Rate: The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Router can transmit. The Router will announce its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Router will also announce that it will automatically select the best rate for transmission. The default setting is **Default**, when the Router can transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps). Other options are **1-2Mbps**, for older wireless technology, and **All**, when the Router can transmit at all wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the Router's rate of data transmission, configure the Transmission Rate setting.

Transmission Rate: The data transmission rate should be set depending on the speed of your wireless network. You can select a proper transmission speeds to fit your wireless clients requirement, or you can select **Auto (Default)** to have the Router automatically adjust one the fastest and suitable data rate to fit network status at the time. Usually this function can be named Auto-Fallback feature. Auto-Fallback will treat one best connection rate between the Router and a wireless client. The default value is **Auto (Default)**.

Transmission Power: This option provides the Router's RFoutput power adjustment. To minimize the possibility of eavesdropping by unauthorized wireless users, suggest to decrease the transmission power with a needed by your wireless environment. By drop down menu, you can select the appropriate level, **Full (Default)**, **Half**, **Quarter**, **Eighth**, or **Min**. The default is **Full (Default)**.

CTS Protection Mode: CTS (Clear-To-Send) Protection Mode should be set to **Auto (Default)**. The Router will automatically use CTS Protection Mode when your Wireless-G products are experiencing severe problems and are not able to transmit to the Router in an environment with heavy 802.11b traffic. This function boosts the Router's ability to catch all Wireless-G transmissions but will severely decrease performance. If you do not want to use CTS Protection Mode at all, select **Disabled**.

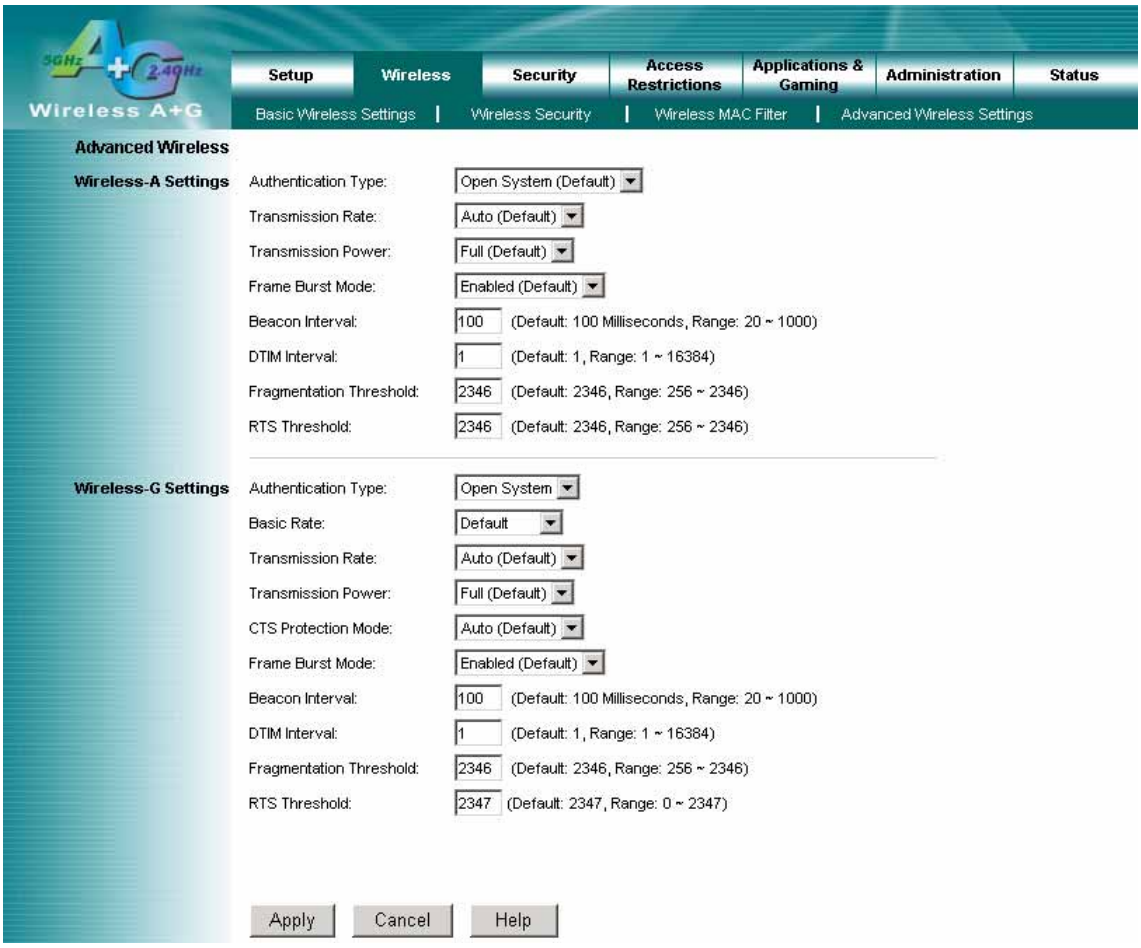
Frame Burst Mode: This option can trigger your wireless network with higher performance. However, it should depend on the manufacturer of your wireless products, the default is **Enabled**.

Beacon Interval: The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1000. A beacon is a packet broadcast by the Router to synchronize the wireless network. The default value is **100**.

DTIM Interval: This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is **1**.

Fragmentation Threshold: This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of **2346**.

RTS Threshold: Using this setting can regulate your wireless network if you experience any inconsistent data flow situation, only by minor adjustment of the default value, the default value **2346** is recommended. The RTS/CTS mechanism will not be enabled if your wireless network packet less than RTS threshold value. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should keep at its default value of **2346**.



Advanced Wireless

Wireless-A Settings

Authentication Type: Open System (Default)

Transmission Rate: Auto (Default)

Transmission Power: Full (Default)

Frame Burst Mode: Enabled (Default)

Beacon Interval: 100 (Default: 100 Milliseconds, Range: 20 ~ 1000)

DTIM Interval: 1 (Default: 1, Range: 1 ~ 16384)

Fragmentation Threshold: 2346 (Default: 2346, Range: 256 ~ 2346)

RTS Threshold: 2346 (Default: 2346, Range: 256 ~ 2346)

Wireless-G Settings

Authentication Type: Open System

Basic Rate: Default

Transmission Rate: Auto (Default)

Transmission Power: Full (Default)

CTS Protection Mode: Auto (Default)

Frame Burst Mode: Enabled (Default)

Beacon Interval: 100 (Default: 100 Milliseconds, Range: 20 ~ 1000)

DTIM Interval: 1 (Default: 1, Range: 1 ~ 16384)

Fragmentation Threshold: 2346 (Default: 2346, Range: 256 ~ 2346)

RTS Threshold: 2347 (Default: 2347, Range: 0 ~ 2347)

Change these settings as described here and click the **Apply** button to apply your changes or click **Cancel** to cancel your changes. For additional information, click **Help**.

4.9 Security

The section offers the Block Anonymous Internet Requests feature. You can enable this feature to secure your network.

Firewall

SPI Firewall Protection: Enable this feature to use Stateful Packet Inspection (SPI) for more detailed review of data packets entering your network environment.

Block Anonymous Requests: Enable this feature can restrict ICMP request such as “ping” command to probe your network from Internet users. It can hide your local network to enhance the security. This feature is enabled by default. Select **Disabled** to allow anonymous Internet requests.

Web Filters: Using the Web Filters feature, you may enable up to four specific filtering methods.

- **Proxy:** Use of WAN proxy servers may compromise the Router's security. Denying Proxy will disable access to any WAN proxy servers. To enable proxy filtering, click the Proxy box.
- **Java:** Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language. To enable Java filtering, click the Java box.
- **ActiveX:** ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. To enable ActiveX filtering, click the ActiveX box.
- **Cookies:** A cookie is data stored on your PC and used by Internet sites when you interact with them. To enable cookie filtering, click the Cookies box.

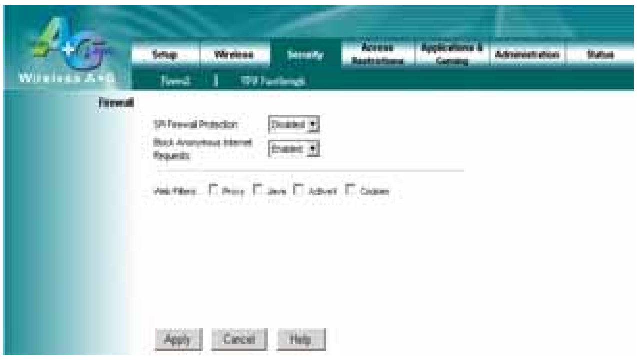
VPN Pass through

This Router provides VPN Pass through function for LAN client behind the Router to build VPN tunnels for secure the network. Use the settings on this tab to allow VPN tunnels using IPSec, L2TP, or PPTP protocols to pass through the Router’s firewall.

IPSec Passthrough: Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. IPSec Pass-Through is enabled by default. To disable IPSec Passthrough, select **Disabled**.

L2TP Passthrough: Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. L2TP Pass-Through is enabled by default. To disable L2TP Passthrough, select **Disabled**.

PPTP Passthrough: Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. PPTP Pass-Through is enabled by default. To disable PPTP Passthrough, select **Disabled**.

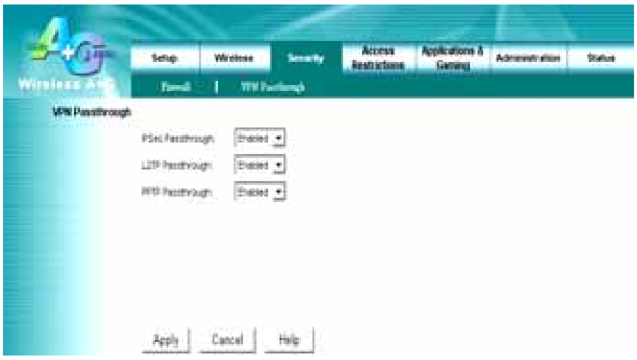


Firewall

SPI Firewall Protection: Disabled

Block Anonymous Internet Requests: Enabled

Web Filters: □ Proxy □ Java □ ActiveX □ Cookies



VPN Passthrough

IPSec Passthrough: Enabled

L2TP Passthrough: Enabled

PPTP Passthrough: Enabled

Change these settings as described here and click the **Apply** button to apply your changes or click **Cancel** to cancel your changes. For additional information, click **Help**.

4.10 Access Restrictions – Internet Access Policy

The Internet Access Policy screen allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, specified applications, websites, and incoming traffic during specific days and times.

Internet Access Policy

Access Policy: Use the settings on this screen to establish an access policy. Selecting a policy from the drop-down menu will display that policy's settings. To delete a policy, select that policy's number and click the **Delete This Policy** button. To view all the policies, click the **Summary** button.

On the Summary screen, the policies are listed with the following information: No., Policy Name, Access, Days, Time, and status (Enabled). You can change the type of access, days, and times of a policy. To activate a policy, click the **Enabled** checkbox. To delete a policy, click its **Delete** button. Click the **Save Settings** button to save your changes, or click the **Cancel Changes** button to cancel your changes. To return to the Internet Access Policy tab, click the **Close** button. To view the list of PCs for a specific policy, click the **Edit List** button.

On the Internet Access PCs list screen, you can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs. After making your changes, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Click the **Close** button to exit this screen.

Internet Access policy creation procedure

1. Select a number from the *Access Policy* drop-down menu.

2. Enter a Policy Name in the field provided.

3. Select **Enabled** from the Status drop-down menu.

4. Click the **Edit List** button to select which PCs will be applyed by the policy. The PCs List screen will appear. You can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs. After making your changes, click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Then click the **Close** button.

5. Select **Deny** or **Allow** option from Access restriction which depending on whether you want to block or allow Internet access for the PCs you listed on the PCs List table screen.

6. Define the schedule of days and times what you want this policy to be enforced. Select the days during which the policy will be taken effect, or select **Everyday**. Enter a range of hours and minutes during which the policy will be taken effect, or select **24 Hours**.

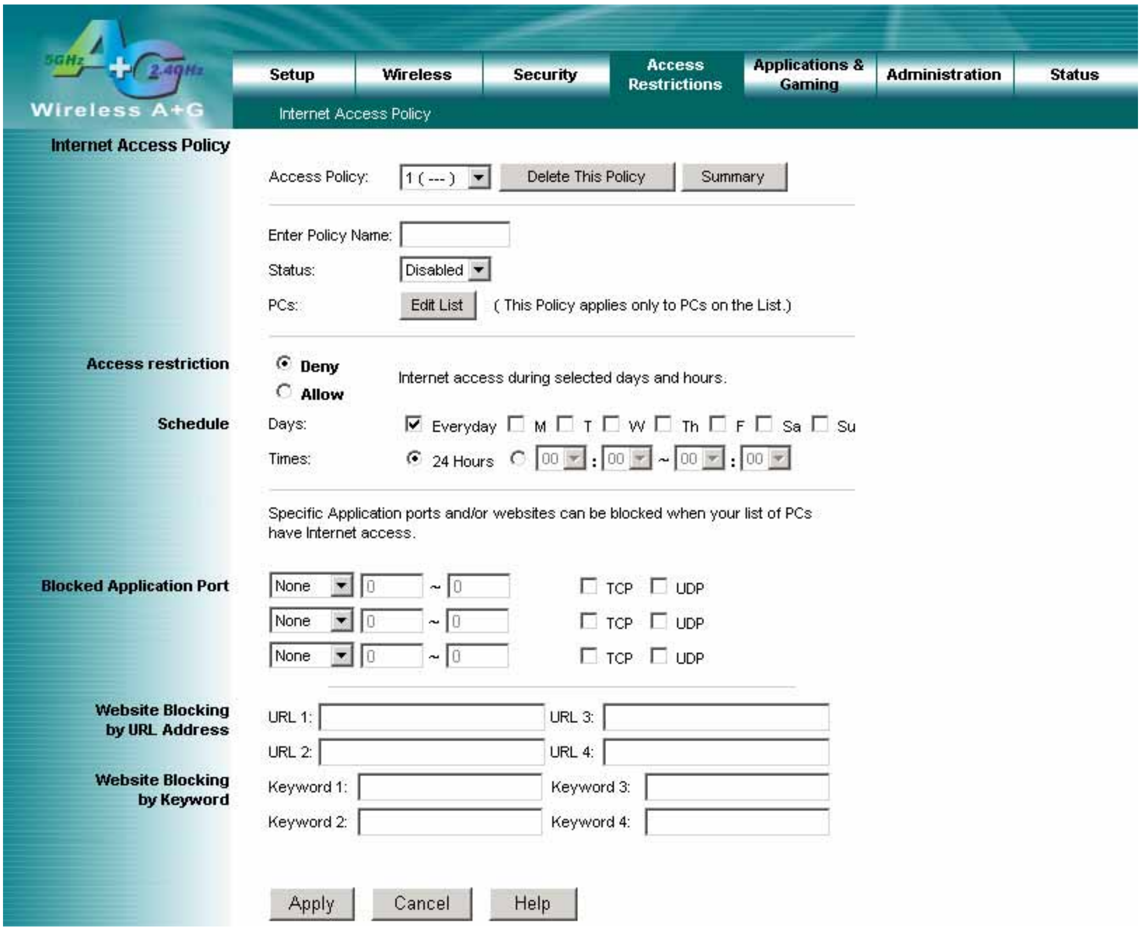
7. Select what kind of service that will be filtered by drop-down menus next to Blocked Application Port. Each drop-down menu offers a choice of application service. Each preset applications that you selected will show the appropriate port range automatically. If the application you want to filter is not listed or you want to customize the settings, then select **Custom** from the drop-down menu. Enter the port range you want to filter. Then select its protocol(s), **TCP** and/or **UDP**.

8. If you want to block websites with specific URL addresses, enter each URL address in a Website Blocking by URL Address field. You can enter up to four URL addresses.

9. If you want to block websites that use specific keywords as part of their URL addresses, enter each keyword in a Website Blocking by Keyword field.

Note1: The policy of above step 1 ~ step 6 are only limited when the certain Days/Times is within the Schedule. If the certain Days/Times is not within the schedule, then passing all hosts to Internet. That means beyond the policy control, the router will not restrict the access.

Note2: The policy of above step 7 ~ step 9 will BLOCK all hosts, not only PCs in the list.



Internet Access Policy

Access Policy: 1 (---)

Enter Policy Name:

Status: Disabled

PCs: (This Policy applies only to PCs on the List.)

Access restriction: ● Deny ○ Allow Internet access during selected days and hours.

Schedule

Days: ☑ Everyday □ M □ T □ W □ Th □ F □ Sa □ Su

Times: ● 24 Hours ○ 00 : 00 ~ 00 : 00

Specific Application ports and/or websites can be blocked when your list of PCs have Internet access.

Blocked Application Port

None 0 ~ 0 □ TCP □ UDP

None 0 ~ 0 □ TCP □ UDP

None 0 ~ 0 □ TCP □ UDP

Website Blocking by URL Address

URL 1: URL 3:

URL 2: URL 4:

Website Blocking by Keyword

Keyword 1: Keyword 3:

Keyword 2: Keyword 4:

Click the **Apply** button to save the policy’s settings. To cancel the policy’s settings, click the **Cancel** button. For additional information, click **Help**.

4.11 Application & Gaming – Port Range Forwarding

The Port Range Forwarding screen allows you to offer public services from your local network, such as web servers, ftp servers, e-mail servers. Before using forwarding feature, the servers that will provide Internet services should assign one static IP address.

Port Range Forwarding
To forward a service from local network, please fill in the relevant information on each field.

Application Name: Each drop-down menu offers a choice of preset applications (select **None** if you do not want to use any of the preset applications). Select up to five preset applications. For custom applications, enter the name of your application in one of the available fields.
The preset applications are among the most generally used Internet applications. They include the following:

FTP (File Transfer Protocol): A protocol used to transfer files over a TCP/IP network.

Telnet: Telnet offers a way to remotely log on to a network device and work on it. By logging on to this device remotely, users can access services or resources that they may not have on their own workstation.

SMTP (Simple Mail Transfer Protocol): The standard e-mail protocol on the Internet. It is a TCP/IP protocol that defines the message format and the Message Transfer Agent (MTA), which stores and forwards the mail.

DNS (Domain Name System): DNS is a method for naming computers and network services. TCP/IP networks use the DNS naming convention to locate computers and services through user-friendly domain names. When a user enters a domain name in an application, the DNS service maps the name to an IP address.

TFTP (Trivial File Transfer Protocol): It's one protocol to use UDP for small files transmission between 2 network devices.

Finger: A UNIX command widely used on the Internet to find out information about a particular user, such as a telephone number, whether the user is currently logged on, and the last time the user was logged on. The person being "fingered" must have placed his or her profile on the system in order for the information to be available. Fingering requires entering the full user@domain address.

HTTP (HyperText Transport Protocol): HTTP is a convention for sending messages from a server to a client by using TCP/IP.

POP3 (Post Office Protocol 3): A standard mail server commonly used on the Internet. It provides a message store that holds incoming e-mail until users log on and download it.

NNTP (Network News Transfer Protocol): NNTP is a protocol that enables you to post, distribute, and retrieve messages on Internet and intranet newsgroups.

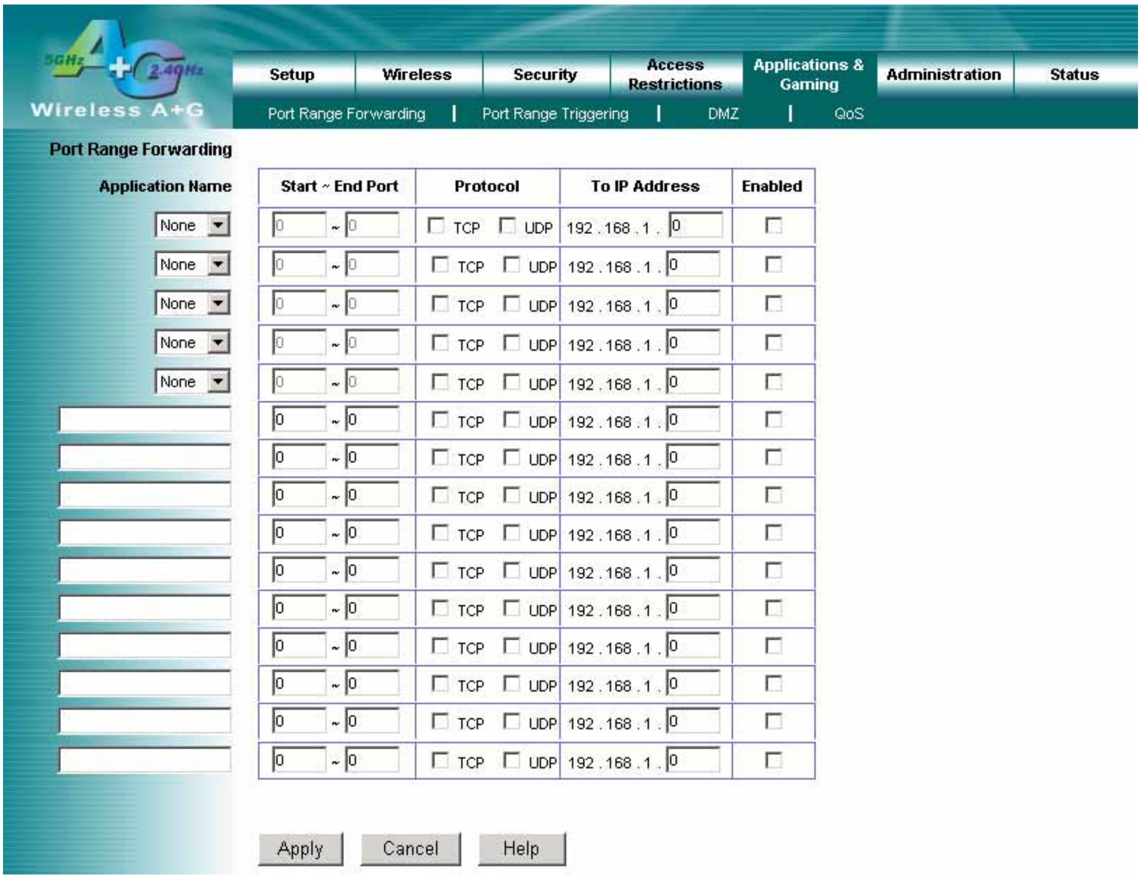
SNMP (Simple Network Management Protocol): SNMP is one protocol that allows you to customize the SNMP settings. SNMP is a popular network monitoring and management protocol.

Start/End: This is the port range. Enter the range of port number that used by the designated compter or Internet application.

Protocol: Select the protocol that used for this application, **TCP** and/or **UDP**.

To IP Address: For each application, enter the IP address of the computer running the specific application.

Enabled: Click the **Enabled** checkbox to enable port forwarding for the relevant application.



Port Range Forwarding

Application Name	Start ~ End Port	Protocol	To IP Address	Enabled
None	0 ~ 0	□ TCP □ UDP	192 . 168 . 1 . 0	□
None	0 ~ 0	□ TCP □ UDP	192 . 168 . 1 . 0	□
None	0 ~ 0	□ TCP □ UDP	192 . 168 . 1 . 0	□
None	0 ~ 0	□ TCP □ UDP	192 . 168 . 1 . 0	□
None	0 ~ 0	□ TCP □ UDP	192 . 168 . 1 . 0	□
	0 ~ 0	□ TCP □ UDP	192 . 168 . 1 . 0	□
	0 ~ 0	□ TCP □ UDP	192 . 168 . 1 . 0	□
	0 ~ 0	□ TCP □ UDP	192 . 168 . 1 . 0	□
	0 ~ 0	□ TCP □ UDP	192 . 168 . 1 . 0	□
	0 ~ 0	□ TCP □ UDP	192 . 168 . 1 . 0	□
	0 ~ 0	□ TCP □ UDP	192 . 168 . 1 . 0	□
	0 ~ 0	□ TCP □ UDP	192 . 168 . 1 . 0	□
	0 ~ 0	□ TCP □ UDP	192 . 168 . 1 . 0	□
	0 ~ 0	□ TCP □ UDP	192 . 168 . 1 . 0	□
	0 ~ 0	□ TCP □ UDP	192 . 168 . 1 . 0	□

Change these settings as described here and click the **Apply** button to apply your changes or click **Cancel** to cancel your changes. For additional information, click **Help**.

4.12 Application & Gaming – Port Range Triggering

The Port Range Triggering is used for special Internet applications whose outgoing ports differ from the incoming ports. For this feature, the Router will watch outgoing data for specific port numbers. The Router will remember the IP address of the computer that sends a transmission requesting data, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.

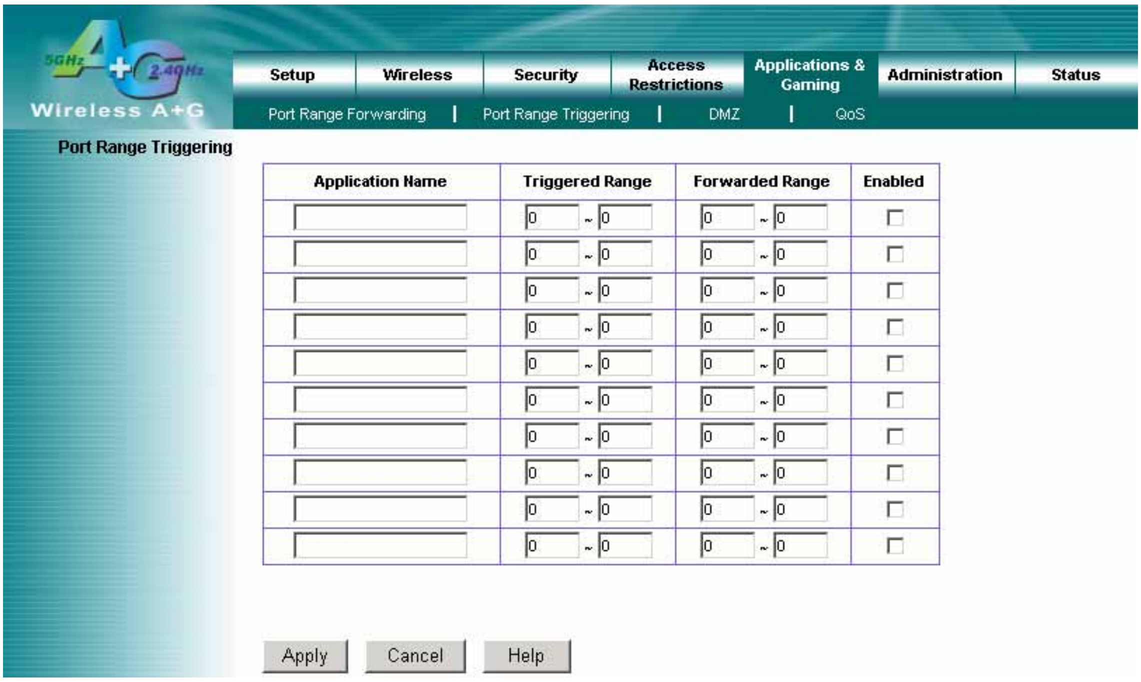
Port Range Triggering

Application Name: Enter the application name of the trigger.

Triggered Range: For each application, list the triggered port number range. Check with the Internet application documentation for the port number(s) needed. In the first field, enter the starting port number of the Triggered Range. In the second field, enter the ending port number of the Triggered Range.

Forwarded Range: For each application, list the forwarded port number range. Check with the Internet application documentation for the port number(s) needed. In the first field, enter the starting port number of the Forwarded Range. In the second field, enter the ending port number of the Forwarded Range.

Enabled: Click the **Enabled** checkbox to enable port range triggering for the relevant application.



Application Name	Triggered Range	Forwarded Range	Enabled
	0 ~ 0	0 ~ 0	☐
	0 ~ 0	0 ~ 0	☐
	0 ~ 0	0 ~ 0	☐
	0 ~ 0	0 ~ 0	☐
	0 ~ 0	0 ~ 0	☐
	0 ~ 0	0 ~ 0	☐
	0 ~ 0	0 ~ 0	☐
	0 ~ 0	0 ~ 0	☐
	0 ~ 0	0 ~ 0	☐
	0 ~ 0	0 ~ 0	☐

Change these settings as described here and click the **Apply** button to apply your changes or click **Cancel** to cancel your changes. For additional information, click **Help**.

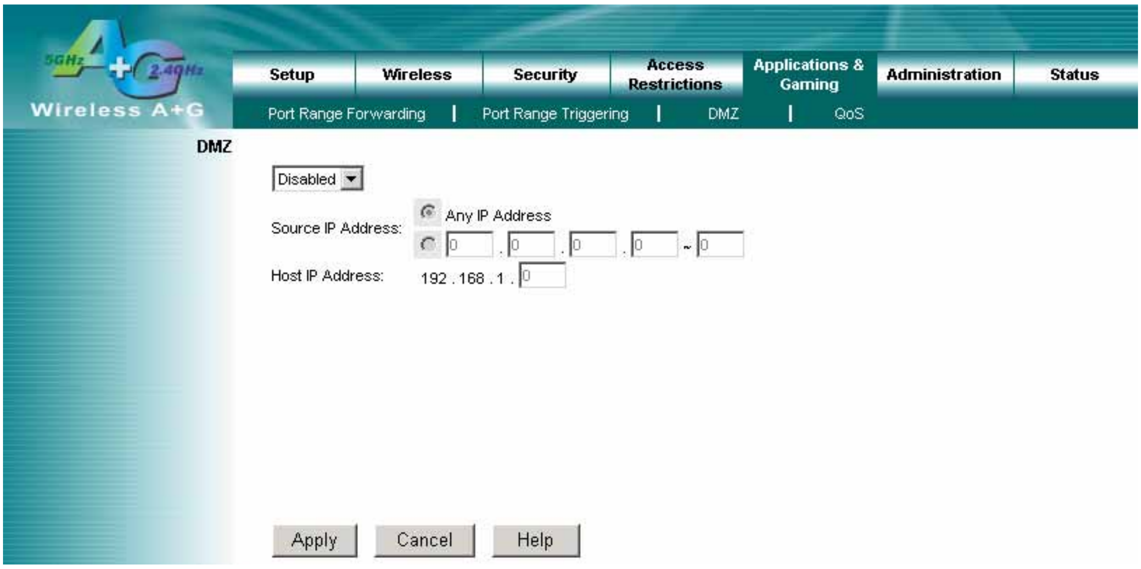
4.13 Application & Gaming – DMZ

The DMZ (De-Militarized Zone) feature allows a computer or small sub-network that locates between a trusted internal network and an un-trusted external network, such as the Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.
Any computer whose port is being forwarded from DMZ must have its DHCP client function disabled and should have a static IP address assigned to it because its IP address may change when using the DHCP function.

DMZ

To expose one PC, select **Enabled**.
Internet Source IP Address: If you want to allow any Internet IP address to access the exposed computer, select **Any IP Address**. If you want to allow a specific IP address or range of IP addresses to access the exposed computer, select the second option and enter the IP address or range of IP addresses in the fields provided.

Destination Host IP Address: Enter the IP address of the computer you want to expose.



DMZ

Disabled ▾

Source IP Address: ● Any IP Address
○ 0 . 0 . 0 . 0 ~ 0

Host IP Address: 192 . 168 . 1 . 0

Change these settings as described here and click the **Apply** button to apply your changes or click **Cancel** to cancel your changes. For additional information, click **Help**.

4.14 Application & Gaming –QoS

QoS (Quality of Service) is a set of service requirements that the network must meet to ensure an adequate service level for data transmission. Using QoS, you can control how network bandwidth is allocated to applications. QoS provides a guaranteed, end-to-end, express delivery system for information across the network.

Qos (Quality of Service)

There are three types of QoS available, Application Port Priority, MAC Address Priority, and LAN Port Priority.

Application Port Priority

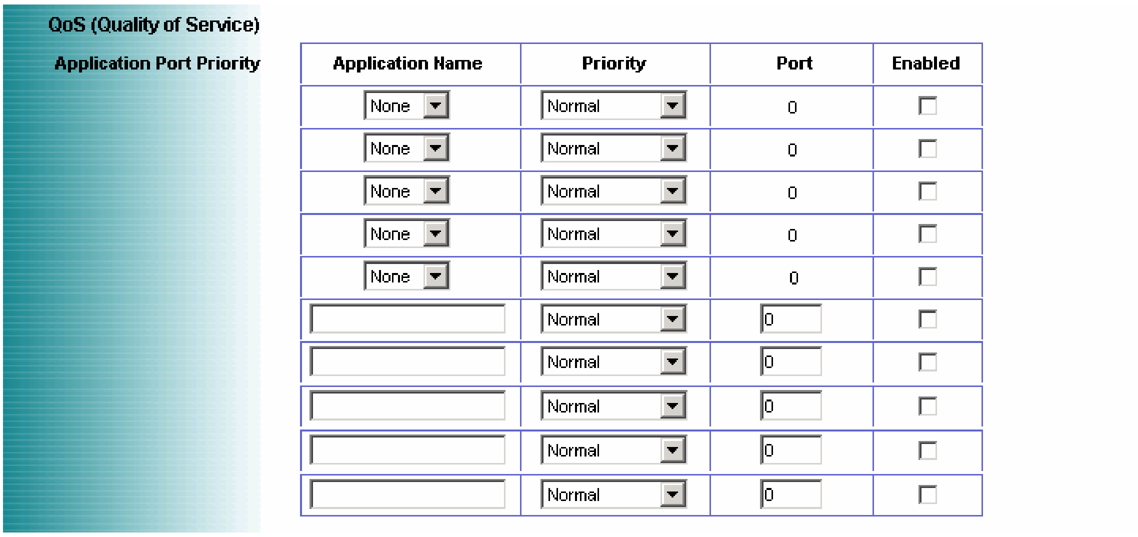
Depending on the settings of the *QoS* screen, this feature will assign information a specific priority for up to five preset applications and up to five additional applications that you specify.

Application Name: Each drop-down menu offers a choice of preset applications (select **None** if you do not want to use any of the preset applications). Select up to five preset applications. For custom applications, enter the name of your application in one of the available fields.

Priority: Select one of these priority levels: **Normal**, **Above Normal, High, Highest**.

Port: For preset applications, the port number is automatically displayed. For custom applications, enter the appropriate port number in the Port field.

Enabled: Click the **Enabled** checkbox to enable QoS for the relevant application.



QoS (Quality of Service)

Application Port Priority

Application Name	Priority	Port	Enabled
None	Normal	0	□
None	Normal	0	□
None	Normal	0	□
None	Normal	0	□
None	Normal	0	□
	Normal	0	□
	Normal	0	□
	Normal	0	□
	Normal	0	□
	Normal	0	□

MAC Address Priority

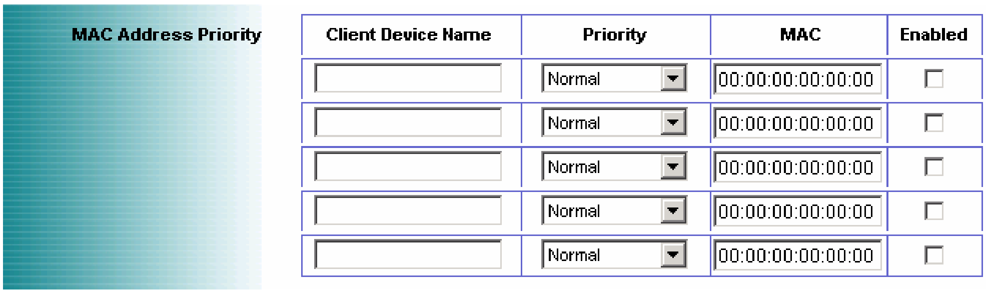
Depending on the settings of the QoS screen, this feature will assign a specific priority for up to five network devices.

Client Device Name: Enter the name of your network device.

Priority: Select one of these priority levels: **Normal, Above Normal, High, Highest**.

MAC: Enter the MAC address of the device.

Enabled: Click the **Enabled** checkbox to enable QoS for the appropriate MAC address.



MAC Address Priority

Client Device Name	Priority	MAC	Enabled
	Normal	00:00:00:00:00:00	□
	Normal	00:00:00:00:00:00	□
	Normal	00:00:00:00:00:00	□
	Normal	00:00:00:00:00:00	□
	Normal	00:00:00:00:00:00	□

LAN Port Priority

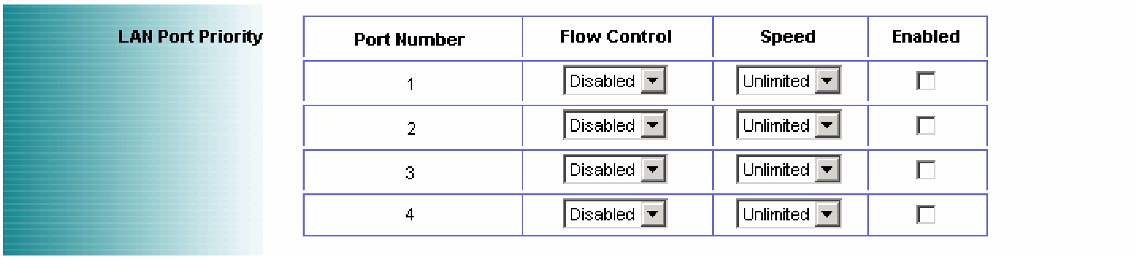
QoS allows you to prioritize performance for the Router’s LAN Ports (1-4). It does not require support from your ISP because the prioritized ports are LAN ports going out to your network.

Port Number: The Router’s LAN port numbers are automatically displayed here.

Flow Control: For each port, if you want the Router to control the transmission of data between network devices, select **Enabled**. To disable this feature, select **Disabled**.

Speed: This setting limits the speed possible for each port. To use this feature, select **50M**, **20M**, **10M**, **5M**, **2M**, **1M**, **512k**, or **256k** (M stands for Mbps, while k stands for kbps). If you do not want to use this feature, keep the default, **Unlimited**.

Enabled: Click the **Enabled** checkbox to enable QoS for the appropriate LAN port.



LAN Port Priority

Port Number	Flow Control	Speed	Enabled
1	Disabled	Unlimited	□
2	Disabled	Unlimited	□
3	Disabled	Unlimited	□
4	Disabled	Unlimited	□

Change these settings as described here and click the **Apply** button to apply your changes or click **Cancel** to cancel your changes. For additional information, click **Help**.

4.15 Administration – Management

This section allows the network's administrator to manage specific Router functions for access and security.

Management

Router Password

Router Password and Re-enter to Confirm: You can change the Router's password from here. Enter a new Router password and then type it again in the Re-enter to Confirm field to confirm.

Remote Router Access

Remote Management: To access the Router remotely, from outside of local network, select **Enabled**. Otherwise, keep the default setting, **Disabled**.

Remote Upgrade: If you want to be able to upgrade the Router remotely, from outside of local network, select **Enabled**. (You must have the Remote Management feature enabled as well.) Otherwise, keep the default setting, **Disabled**.

Allow Remote IP Address: If you want to be able to access the Router from outside with any external IP address, select **Any IP Address**. If you want to specify an external IP address or range of IP addresses, then select the second option and complete the fields provided.

Remote Management Port: Enter the port number that will be open to outside access.

UPnP

Universal Plug and Play (UPnP) is a distributed, open networking architecture that leverages TCP/IP and the Web technologies to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and public spaces.

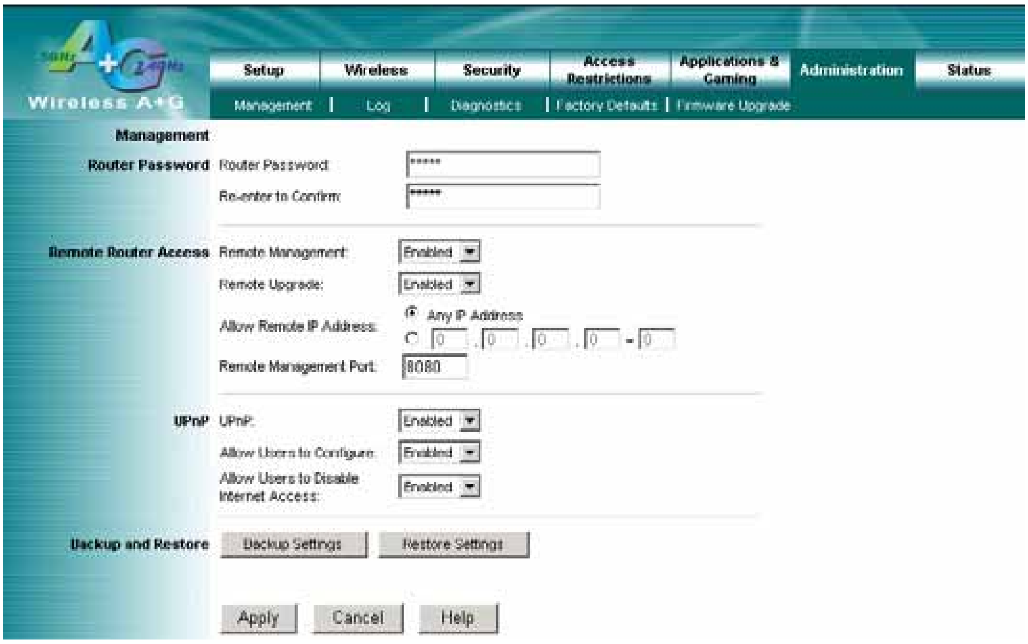
UPnP: If you want to use UPnP, keep the default setting, **Enabled**. Otherwise, select **Disabled**.

Allow Users to Configure: Keep the default setting, **Enabled**, if you want to be able to make manual changes to the Router while using the UPnP feature. Otherwise, select **Disabled**.

Allow Users to Disable Internet Access: Keep the default setting, **Enabled**, if you want to be able to forbit any and all Internet connections. Otherwise, select **Disabled**.

Backup and Restore

Backup Settings: To back up the Router's configuration, click this button and follow the on-screen instructions.
Restore Settings: To restore the Router's configuration, click this button and follow the on-screen instructions.
(You must have previously backed up the Router's configuration.)



Management

Router Password
Router Password: *****
Re-enter to Confirm: *****

Remote Router Access
Remote Management: Enabled
Remote Upgrade: Enabled
Allow Remote IP Address: ● Any IP Address
○ 0 . 0 . 0 . 0 - 0
Remote Management Port: 8080

UPnP
UPnP: Enabled
Allow Users to Configure: Enabled
Allow Users to Disable Internet Access: Enabled

Backup and Restore

Change these settings as described here and click the **Apply** button to apply your changes or click **Cancel** to cancel your changes. For additional information, click **Help**.

4.16 Administration – Log

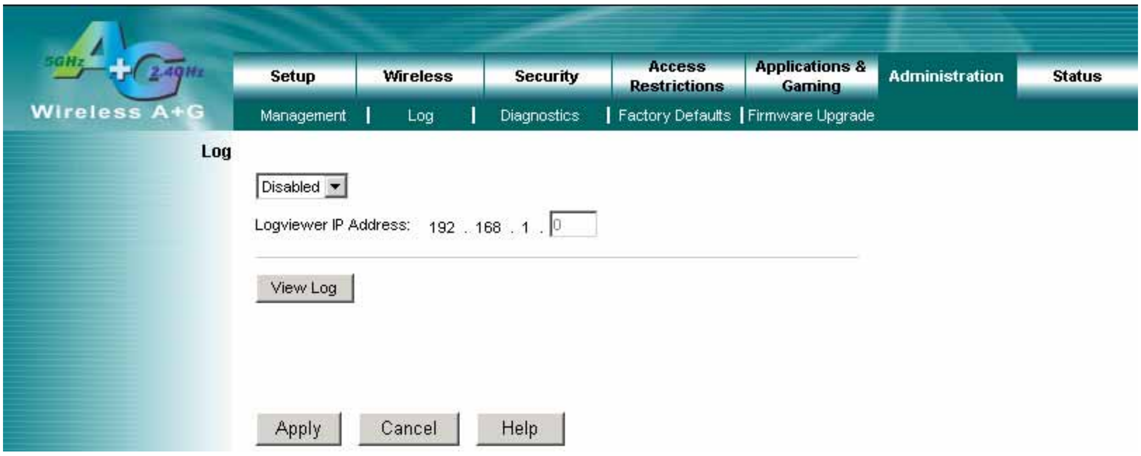
The Router can keep logs of all traffic for your Internet connection. This feature is disabled by default. To keep activity logs, select **Enable**.

Log

To disable the Log function, keep the default setting, **Disabled**. To monitor traffic between the network and the Internet, select **Enabled**.

Logviewer IP Address: For a permanent record of the Router's activity logs, Logviewer software must be used. This software can be gotten from CD. The Log viewer saves all incoming and outgoing activity in a permanent file on your PC's hard drive. In the Logviewer IP Address field, enter the fixed IP address of the PC running the Log viewer software. The Router will now send updated logs to that PC.

View Log: When you wish to view the logs, click **View Log**. A new screen will appear. Select **Incoming Log** or **Outgoing Log** from the Type drop-down menu. The Incoming Log will display a temporary log of the Source IP Addresses and Destination Port Numbers for the incoming Internet traffic. Click the **Save the Log** button to save this information to a file on your PC's hard drive. Click the **Refresh** button to update the log. Click the **Clear** button to clear all the information that is displayed.
The Outgoing Log will display a temporary log of the LAN IP Addresses, Destination URLs or IP Addresses, and Service or Port Numbers for the outgoing Internet traffic. Click the **Save the Log** button to save this information to a file on your PC's hard drive. Click the **Refresh** button to update the log. Click the **Clear** button to clear all the information that is displayed.



Log

Disabled

Logviewer IP Address: 192 . 168 . 1 . 0

Change these settings as described here and click the **Apply** button to apply your changes or click **Cancel** to cancel your changes. For additional information, click **Help**.

4.17 Administration – Diagnostics

The diagnostics function provides two ways for Router's status of Internet connection.

Diagnostics

Ping Test

This utility verifies configurations and tests IP connectivity between two computers. Ping sends an ICMP request from the source computer, and the destination computer responds with an ICMP reply.

To IP or URL Address: Enter the IP address or URL that you want to ping.

Packet Size: Enter the size of the packet you want to use.

Times to Ping: Select the number of times you wish to ping: **5**, **10**, **15**, or **Unlimited**.

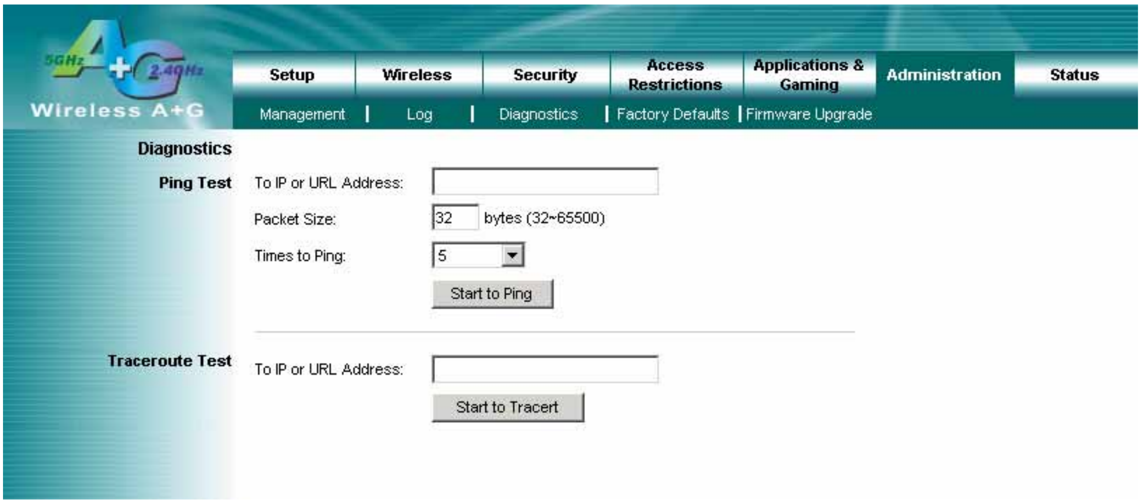
Start to Ping: Click this button to begin the test. A new screen will appear and display the test results. Click the **Close** button to return to the *Diagnostics* screen.

Traceroute Test

Traceroute function provides a trace for the route that a packet takes to destination.

To IP or URL Address: Enter the destination IP address or URL that you want to trace the routes.

Start to Tracert: Click this button to begin the Tracert. A new screen will appear and display the trace results. Click the
Close button to return to the *Diagnostics* screen.



Diagnostics

Ping Test

To IP or URL Address:

Packet Size: 32 bytes (32~65500)

Times to Ping: 5

Traceroute Test

To IP or URL Address:

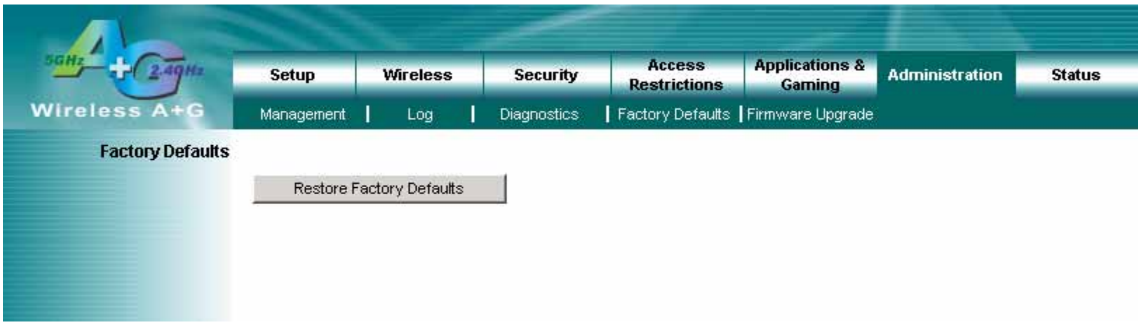
Change these settings as described here and click the **Apply** button to apply your changes or click **Cancel** to cancel your changes. For additional information, click **Help**.

4.18 Administration – Factory Defaults

This Factory Defaults allows you to restore the Router's configuration to its factory default settings.

Factory Defaults

Restore Factory Defaults: Click this button to reset all configuration settings to their default values. Any settings you have saved will be lost when the default settings are restored.



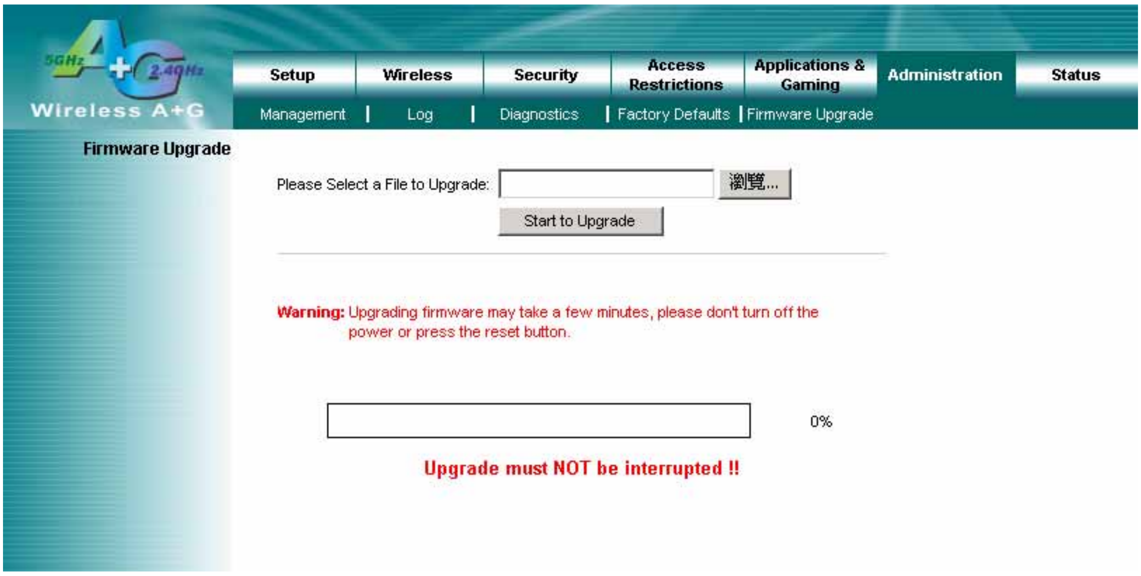
4.19 Administration – Firmware Upgrade

This Firmware Upgrade screen allows you to upgrade the Router’s firmware. Do not upgrade the firmware unless you are experiencing problems with the Router or the new firmware has a feature you want to use.

Firmware Upgrade

Please select a file to upgrade: In the field provided, enter the name of the extracted firmware upgrade file, or click the **Browse** button to find this file.

Start to Upgrade: After you have selected the appropriate file, click this button for upgrade.



Please Select a File to Upgrade:

Warning: Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button.

0%

Upgrade must NOT be interrupted !!

4.20 Status – Router

The Router screen on the Status Tab displays information about the Router and its current settings. The Internet Connection information will vary depending on the Internet Connection Type you use.

Router Information

Firmware Version: This is the Router’s current firmware.

Current Time: This shows the time by the time zone you selected on the Setup Tab.

Internet MAC Address: This is the Router’s MAC Address.

Host Name: If required by your ISP, it would be entered on the Setup Tab.

Domain Name: If required by your ISP, it would be entered on the Setup Tab.

Internet Connection

Connection Type: This indicates the current Internet connection type you are using.

Connection Status: The status of the connection is displayed only for a PPPoE connection type. For this dial-up style connection, click the **Connect** button, if there is no connection to establish. When your PPPoE connection is active, you can click the **Disconnect** button to end the connection.

IP Address: The Router’s Internet IP Address.

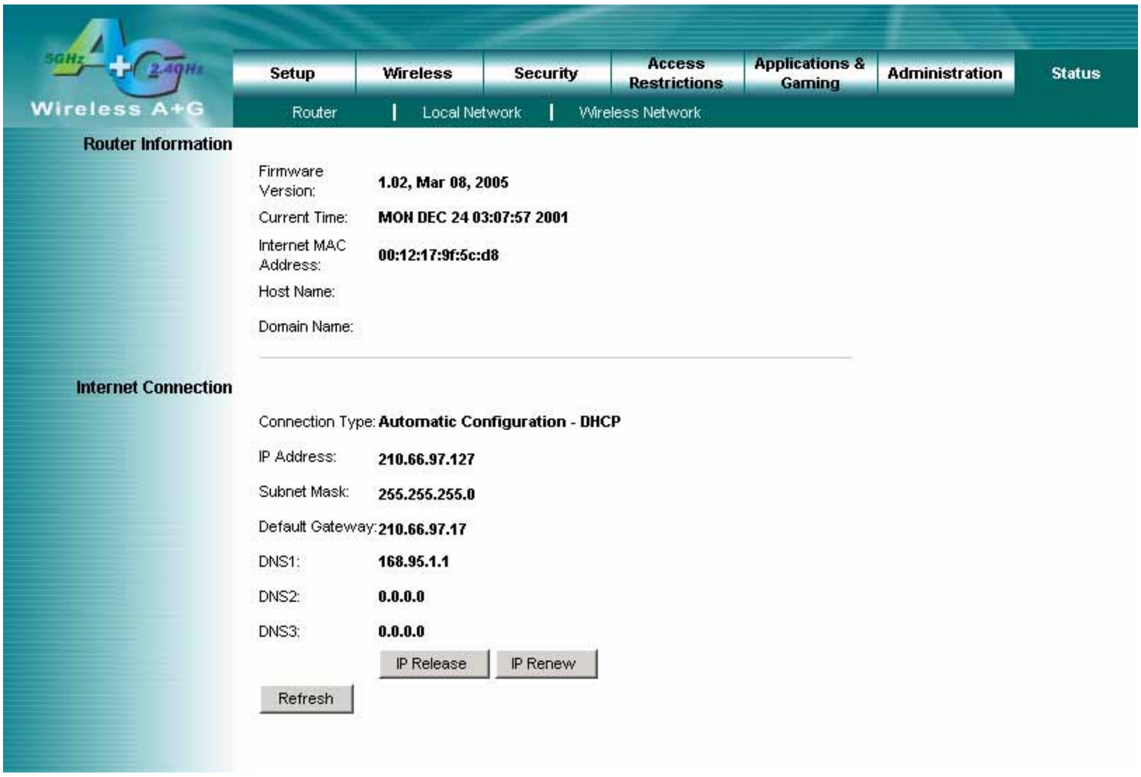
Subnet Mask and Default Gateway: The Router’s Subnet Mask and Default Gateway address are displayed here.

DNS1-3: The DNS (Domain Name System) IP addresses currently is used by the Router. The Router at least one DNS IP should be used for domain name resolution.

IP Release: This button is for DHCP connection type, click this button to release the current Internet IP address.

IP Renew: This button is for DHCP connection type, click this button to renew the current Internet IP address.

Click the **Refresh** button to update the on-screen information.



Router Information

Firmware Version: 1.02, Mar 08, 2005

Current Time: MON DEC 24 03:07:57 2001

Internet MAC Address: 00:12:17:9f:5c:d8

Host Name:

Domain Name:

Internet Connection

Connection Type: Automatic Configuration - DHCP

IP Address: 210.66.97.127

Subnet Mask: 255.255.255.0

Default Gateway: 210.66.97.17

DNS1: 168.95.1.1

DNS2: 0.0.0.0

DNS3: 0.0.0.0

4.21 Status – Local Network

The Local Network screen on the Status Tab displays the status of your network.

Local Network

Local MAC Address: This is the Router's local MAC Address.

Router IP Address: This is the Router's local IP Address.

Subnet Mask: This is the Router's local subnet mask.

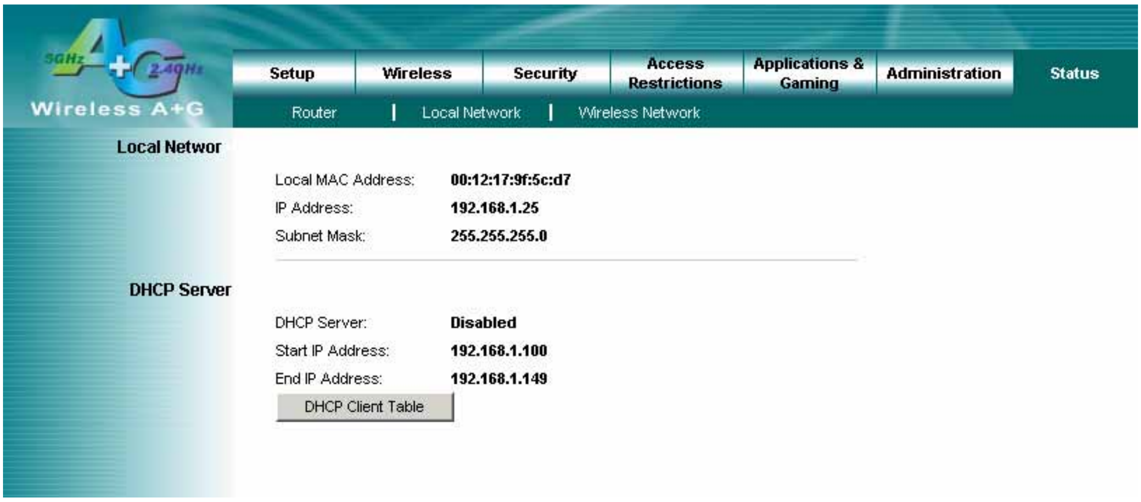
DHCP Server

DHCP Server: The Router's embedded DHCP server status.

Start IP Address: This is beginning range of assigned IP by Router's DHCP server.

End IP Address: This is end range of assigned IP by Router's DHCP server.

DHCP Client Table: Clicking this button will open a screen to show which hosts are using the Router as a DHCP server. On the DHCP Client Table screen, you will see a list of DHCP clients with the following information: Client Names, Interfaces, IP Addresses, MAC Addresses, and the assigned IP addresses expired time. From the To Sort by drop-down menu, you can sort the table by Client Name, Interface, IP Address, or MAC Address. To remove a DHCP client from this list, click its **Delete** button. To view the most up-to-date information, click the **Refresh** button. To exit this screen, click the **Close** button.



Local Networ

Local MAC Address: 00:12:17:9f:5c:d7
IP Address: 192.168.1.25
Subnet Mask: 255.255.255.0

DHCP Server

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

4.22 Status – Wireless Network

The Wireless Network screen on the Status Tab displays the information of your Wireless networks.

Wireless Network

Wireless-A

MAC Address: This is the Router’s Wireless-A band MAC Address.

Mode: This mode is displaying the current status of Wireless-A band network. **Enabled** means the A band network is **ON**.

Turbo Mode: This mode is displaying the turbo mode status. (**Enabled/Disabled**)

Network Name (SSID): The Wireless-A band network name.

Channel: The current A band channel you are using.

Security: This displays what type of encryption you are using.

SSID Broadcast: This displays the Router’s SSID Broadcast status.

Wireless-G

MAC Address: This is the Router’s Wireless-G band MAC Address.

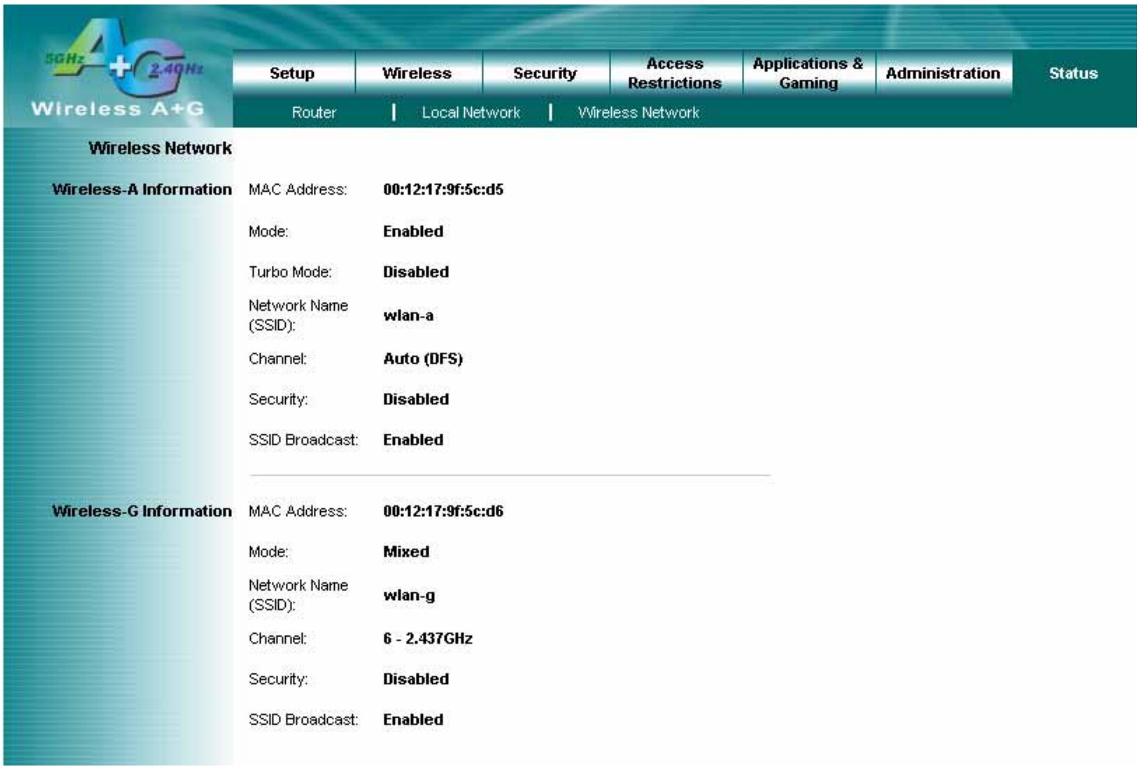
Mode: This displays the Wireless-G band network mode.

Network Name (SSID): The Wireless-G band network name.

Channel: The current G band channel you are using.

Security: This displays what type of encryption you are using.

SSID Broadcast: This displays the Router’s SSID Broadcast status.



Wireless Network

Wireless-A Information	MAC Address:	00:12:17:9f:5c:d5
	Mode:	Enabled
	Turbo Mode:	Disabled
	Network Name (SSID):	wlan-a
	Channel:	Auto (DFS)
	Security:	Disabled
	SSID Broadcast:	Enabled
Wireless-G Information	MAC Address:	00:12:17:9f:5c:d6
	Mode:	Mixed
	Network Name (SSID):	wlan-g
	Channel:	6 - 2.437GHz
	Security:	Disabled
	SSID Broadcast:	Enabled

5. Troubleshooting – Q & A

1. I'm trying to log on the Router's Web configuration page, but I do not see the login screen.

Answer:

1. Please make sure the IP address that you input on address field of IE browser is correct.
2. Make sure the physical layer connection is established. If you are using wired to connect this Router, check the relevant LAN LED whether is lit or not.
3. On Dos Prompt screen, using " ping " command to probe this Router, check if you got reply from it.
   Command: ping < Destination IP address >
4. If you have any TCP/IP setting problem, please refer to the Quick Installation Guide.

2. I need to set up a server behind my Router and make it available to the public.

Answer:

This is Router's forwarding function. Please refer to the section 4.12. Generally, using a server like a web, ftp, or mail server, you need to know what kinds of the respective port numbers they are using.
For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming).
Below is an example for how to set up a FTP server behind Router for public network access.
1. Log on the Router's web configuration page, http://192.168.1.1 or the IP address that you have changed.
2. Select the Applications & Gaming => Port Range Forwarding tab.
3. Enter any name you want to use like "FTP service".
4. Enter the External Port range of the FTP service you are using. For example, your FTP service port range should be port 20 ~ 21.
5. Select the protocol, TCP and UDP.
6. Enter the IP address of the FTP server that locate on your local network. For example, if your FTP server's IP address is 192.168.1.10, then you should enter 10 in the address field.
7. Click the **Enabled** option for enable this service.

3. I forgot my password, how to log on this Router for configuration?

Answer:

1. Reset the Router to factory default by pressing the Reset button for 10 seconds then releasing it.
2. Log on the Router's web management by http://192.168.1.1
   Leave username blank and enter the default password **admin**.

4. How to set the Router to factory default setting.

Answer:

1. Reset the Router to factory default by pressing the Reset button for 10 seconds then releasing it.
2. After release the Reset button, the Router will get back all setting to factory default and reboot system.
3. While the reboot is complete, log on the Router's web management by default IP http://192.168.1.1
   Leave username blank and enter the default password **admin**.

5. My SOHO AP will not turn on. No LED's light up.

Answer:

Usually it is caused by the power is not connected.
Please double check the power adapter if it connected to your Router and the other side is plugged into the power outlet. If it still has no power, please contact your reseller.

6. I can't access the AP from a wireless client.

Answer:

Generally to make the wireless client unable to access AP with following possible issues:
1. Settings are not the same among each wireless adapter.
2. Out of range.
3. IP Address is not set correctly.

Resolution:

Make sure that the mode, SSID, Channel and encryption settings are set the same on each wireless adapter. Make sure that your computer is within range and free from any strong electrical devices that may cause interference.

7. What devices cause interference?

Answer:

The Router is operating in the unlicensed 2.4 GHz band. Other devices operates in this frequency range that may cause interference include microwave ovens and 2.4 GHz portable phones. PCs or analog cellular phones do not operate at 2.4 GHz and do not cause interference. Proper placement of access points usually eliminates interference problems created by other 2.4 GHz devices.