Gemtek Wireless Broadband Anywhere

Gemtek Technology Co., Ltd.

High Speed Access Point Router

WX-5525G

User's Manual

Mar. 19, 2003 (Draft 1.0

CONTENTS

Introduction

Thank you for purchasing your WX-5525G Dual Band Wireless AP Router.

This user guide will assist you with the installation procedure.

The package you have received should contain the following items:

- WX-5525G Dual Band Wireless AP Router

- User Guide

- Power Supply / Cord

- Ethernet Cable

Note: if anything is missing, please contact your vendor

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.

Hardware Installation

Front Panel

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

LED	STATUS	Description
PWR/STAT	Off	No Power
	Red On	1. Power on 2. Reset to default 3. Firmware upgrade (first 1 minute)
	Red Blink	1. System up 2. Power on 3. Firmware upgrade
LAN	Off	no Ethernet link detected
	Green On	10/100Mbps Fast Ethernet link detected. No activity.
	Green Blink	Indicates data traffic on the 10/100 Mbps LAN
WAN	Orange On	10Mbps Ethernet link detected. No activity.
	Orange Blink	Indicates data traffic on the 10 Mbps WAN.
G	Yellow Blink	Indicates the device is linking or active data through wireless links

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.

|	
Power (DC 5v)	Used to connect to the power outlet. Only use the power adapter provided with the device. Use of an unauthorized power adapter may cause damage to your device and violate your warranty.
Reset	Press the Reset Button for approximately ten seconds, all configurations will set to factory default settings.
LAN	The RJ-45 Ethernet ports used to connect your PC, hub, switch or Ethernet network.
WAN	The RJ-45 Ethernet port labeled WAN is used to connect your AP Router to your **x**DSL or Cable modem.

WX-5525G AP Router Default Settings

The default settings are shown following.

User Name	**admin**	
Password	**admin**	
AP Router IP Address	**192.168.1.1**	
AP Router Subnet Mask	255.255.255.0	
RF ESSID	**Wireless Router**	
11b RF Channel	6	
RF Roaming	Enabled	
Encryption	Disabled	
DHCP client	Enabled	

Web Management Settings

START -UP & LOG IN

In order to configure the WX-5525G Wireless AP Router, please use your web browser (Microsoft Internet Explorer or Netscape) and manually input **192.168.1.1** into the address box (as shown below) and press Enter key.
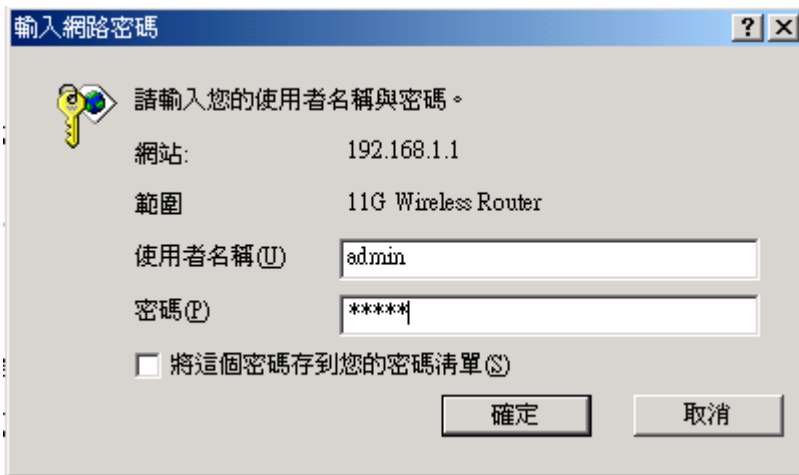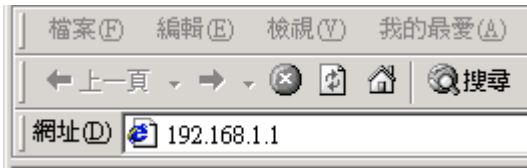
In order to configure the WX-5525G Wireless AP Router, please input the user-name into the **User Name** box. Enter the password into the **Password** box and press the **OK** button. The default username is **admin**, and the default password is **admin**

Once you have logged-in as administrator, it is a good idea to change the administrator password to ensure a secure connection to the Wireless AP.

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**

Setup

This screen contains all of the Router's basic setup functions. Most users will be able to use the Router's default settings without making any changes. Click the **Apply** button to save your 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

specific information, such as User Name, Password, IP Address, Default Gateway Address, or DNS IP Address. This information can be obtained from your ISP, if required.

Host Name: This entry is necessary for some ISPs and can be provided by them.
Domain Name: This entry is necessary for some ISPs and can be provided by them.
Configuration Type: The Router supports four connection types:

> **Automatic Configuration - DHCP**
> **Static IP**
> **PPPoE** (Point-to-Point Protocol over Ethernet)
> **PPTP** (Point-to-Point Tunneling Protocol)

These types can be selected from the drop-down menu next to Internet Connection. The information required and available features will differ depending on what kind of connection type you select.

Some descriptions of this information are included here:

- **Internet IP Address and Subnet Mask**

  This is the Router's IP Address and Subnet Mask as seen by external users on the Internet (including your ISP). If your Internet connection requires a static IP address, then your ISP will provide you with a Static IP Address and Subnet Mask.

- **Default Gateway**

  Your ISP will provide you with the Gateway IP Address.

- **DNS (Domain Name Server) IP Address**

  Your ISP will provide you with at least one DNS IP Address.

- **User Name and Password**

  Enter the **User Name** and **Password** you use when logging onto your ISP through a PPPoE or PPTP connection.

- **Connect on Demand**

  You can configure the Router to disconnect your Internet connection after a specified period of inactivity (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the

Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

- **Keep Alive Option**

  This option keeps you connected to the Internet indefinitely, even when your connection sits idle. To use this option, click the radio button next to *Keep Alive*. The default Redial Period is 30 seconds (in other words, the Router will check the Internet connection every 30 seconds).

IP Address and Subnet Mask: This is the Router's IP Address and Subnet Mask as seen on the internal LAN. The default value is 192.168.1.1 for IP Address and 255.255.255.0 for Subnet Mask.

Wireless:

2.4GHz Settings

Mode: The default setting is **Mixed**.

If you have Wireless-G and 802.11b devices in your network, then keep the default setting, **Mixed**. If you have only Wireless-G devices, select **G-Only**. If you want to disable wireless networking, select **Disable**.

Channel: The default setting is **6**.

Select the appropriate channel from the list provided to correspond with your network settings, between 1 and 11 (in North America). All devices in your wireless network must use the same channel in order to function correctly.

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: 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.

WEP: Make sure that all wireless devices on your network are using the same encryption level and key.   WEP keys must consist of the letters "A" through "F" and the numbers "0" through "9."

Click **Apply** to save your settings.

Security

Password:

Changing the password for the AP Router is as easy as typing the password into the **New Password** field. Then, type it again into the Re-enter to confirm.

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

Use the default password when you first open the configuration pages, after you have configured these settings, you should set a new password for the Router (using the Password screen). This will increase security, protecting the Router from unauthorized changes.

VPN Pass-Through: Virtual Private Networking (VPN) is typically used for work-related networking. For VPN tunnels, the Router supports IPSec Pass-Through, L2TP Pass-Through, and PPTP Pass-Through.

- **IPSec** - Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the Router, IPSec Pass-Through is enabled by default. To disable IPSec Pass-Through, uncheck the box next to *IPSec*.

- **L2TP** - Layer 2 Tunneling Protocol is a protocol used to tunnel Point-to-Point Protocol (PPP) over the Internet. To allow L2TP tunnels to pass through the Router, L2TP Pass-Through is enabled by default. To disable L2TP Pass-Through, uncheck the box next to *L2TP*.

- **PPTP** - Point-to-Point Tunneling Protocol is the method used to enable VPN sessions to a Windows NT 4.0 or 2000 server. To allow PPTP tunnels to pass through the Router, PPTP Pass-Through is enabled by default. To disable PPTP Pass-Through, uncheck the box next to *PPTP*.

Web Filters: Using the Web Filters feature, you may enable up to four different filters.

- **Proxy** - Use of WAN proxy servers may compromise network security. Denying Proxy will disable access to any WAN proxy servers. To enable proxy filtering, click the box next to *Proxy*.
- **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 box next to *Java*.
- **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 box next to *ActiveX*.
- **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 box next to *Cookies*.

DMZ: The default setting is **Disable**.

The DMZ hosting feature allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Forwarding feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer so the Internet can see it.

Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

1. To expose one PC, select **Enable**.
2. Enter the computer's IP address in the *DMZ Host IP Address* field.
3. Click the **Apply** button.

Block WAN Request: The default setting is **Enable**.

By enabling the Block WAN Request feature, you can prevent your network from being "pinged," or detected, by other Internet users. The Block WAN Request feature also reinforces your network security by hiding your network ports. Both functions of the Block WAN Request feature make it more difficult for outside users to work their way into your network. This feature is enabled by default. Select **Disable** to disable this feature.

System

Restore Factory Defaults: Click the **Yes** button to reset all configuration settings to factory default values. Note: Any settings you have saved will be lost when the default settings are restored. Click the **No** button to disable the Restore Factory Defaults feature. Click the **Apply** button to save the setting.

Firmware upgrade:
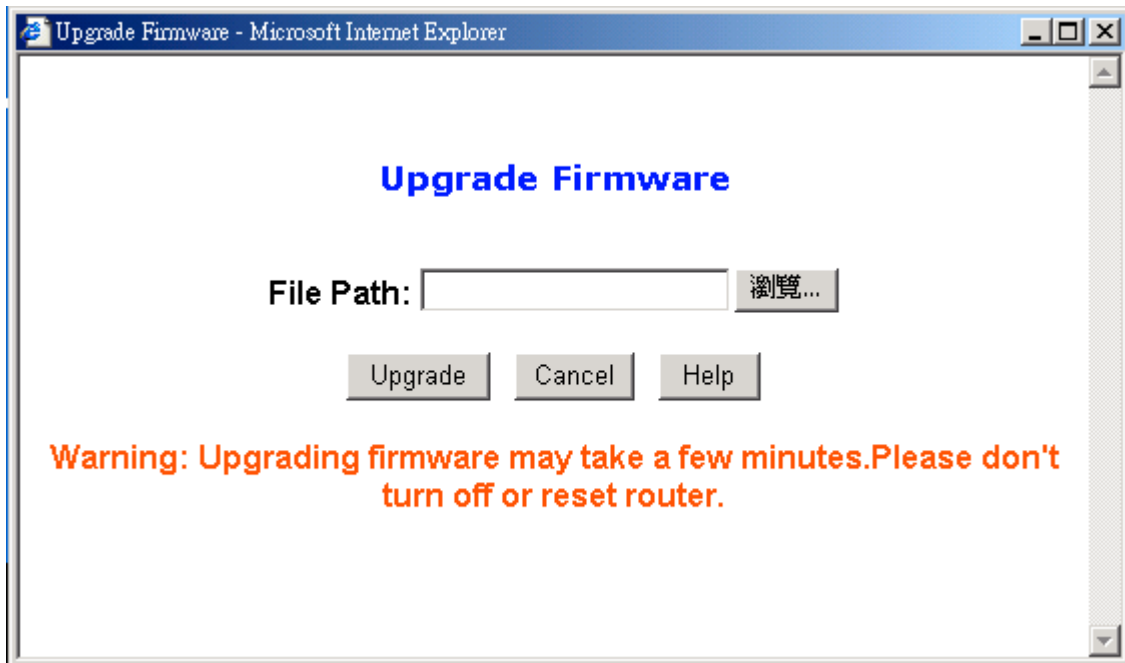
User may download the latest firmware from your vendor's website and store it in local drive.

Find the firmware from local drive and press the **Upgrade** button.

Multicast Pass-Through: The default setting is **Disable**.

IP Multicasting occurs when a single data transmission is sent to multiple recipients at the same time. Using the Multicast Pass-Through feature, the Router allows IP multicast packets to be forwarded to the appropriate computers. Keep the default setting, **Enable**, to support the feature, or select **Disable** to disable it.

MAC Cloning: The Router's MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs require that you register the MAC address of your network card/adapter, which was connected to your cable or DSL modem during installation. If your ISP requires MAC address registration, find your adapter's MAC address by following the instructions for your PC's operating system.

For Windows 98 and Millennium:

1.   Click the **Start** button, and select **Run**.

2.   Type **winipcfg** in the field provided, and press the **OK** key.

3.   Select the Ethernet adapter you are using.

4.   Click **More Info**.

5.   Write down your adapter's MAC address.

For Windows 2000 and XP:

1.   Click the **Start** button, and select **Run**.

2.   Type **cmd** in the field provided, and press the **OK** key.

3.   At the command prompt, run **ipconfig /all**, and look at your adapter's physical address.

4.   Write down your adapter's MAC address.

To clone your network adapter's MAC address onto the Router and avoid calling your ISP to change the registered MAC address, follow these instructions:

1.   Select **Enable**.

2.   Enter your adapter's MAC address in the *MAC Address* field.

3.   Click the **Apply** button.

To disable MAC address cloning, keep the default setting, **Disable**

Remote Management: The default setting is **Disable**.

This feature allows you to manage your Router from a remote location, via the Internet.   To disable this feature, keep the default setting, **Disable**. To enable this feature, select **Enable**, and use the specified port (default is **8080**) on your PC to remotely manage the Router. You must also change the Router's default password to one of your own, if you haven't already. A unique password will increase security.

To remotely manage the Router, enter **http://xxx.xxx.xxx.xxx:8080** (the x's represent the Router's Internet IP address, and 8080 represents the specified port) in your web browser's *Address* field. You will be asked for the Router's password. After successfully entering the password, you will be able to access the Router's web-based utility.

Note: If the Remote Management feature is enabled, anyone who knows the Router's Internet IP address and password will be able to alter the Router's settings.

MTU: The default setting is **Auto**.

MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Keep the default setting, **Auto**, to have the Router select the best MTU for your Internet connection. To specify a MTU size, select **Manual**, and enter the value desired (default is **1400**).   You should leave this value in the 1200 to 1500 range.

Log: The default setting is **Disable**.

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

To keep a permanent record of activity logs as a file on your PC's hard drive, Logviewer software must be used. This software is downloadable from the website*, www.nobrand.com*. In the *Send Log to* field, enter the fixed IP address of the PC running the Logviewer software. The Router will send updated logs to that PC.

To see a temporary log of the Router's most recent incoming traffic, click the **Incoming Access Log** button. To see a temporary log of the Router's most recent outgoing traffic, click the **Outgoing Access Log** button.

DHCP

The DHCP screen allows you to configure the settings for 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 configure your entire network PCs to connect to a DHCP server, the Router.

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: Click the **Enable** radio button to enable the Router's DHCP server option. If you already have a DHCP server on your network or you do not want a DHCP server, then click the **Disable** radio button.

Starting IP Address: Enter a numerical 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 192.168.1.253. The default Starting IP Address is **192.168.1.100**.

Maximum Number of DHCP 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 192.168.1.100 is your starting IP address. The default is **51**.

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. 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 three DNS Server IP Addresses here. The Router will utilize 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.

Currently Assigned: Click the **DHCP Clients Table** button to see a list of PCs assigned IP addresses by the Router. For each PC, the list shows the client hostname, MAC address, IP address, and the amount of DHCP client lease time left. Click the **Refresh** button to display the most current information.

Click **Apply** to save your settings.

SNMP

The *SNMP* screen allows you to customize the Simple Network Management Protocol   (SNMP)

settings for the Router and two SNMP Communities
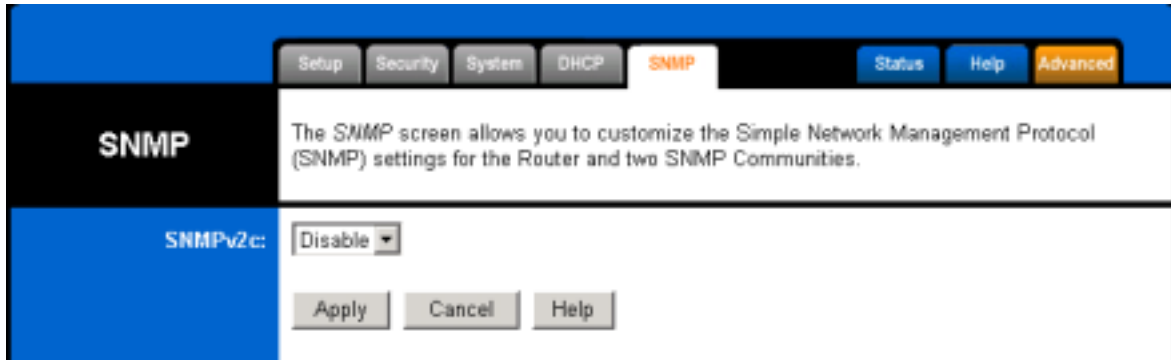
Status

This screen displays the Wireless Router's current status and settings. This information is read-only.

This page will auto re-flash every 10 seconds to keep most update information.
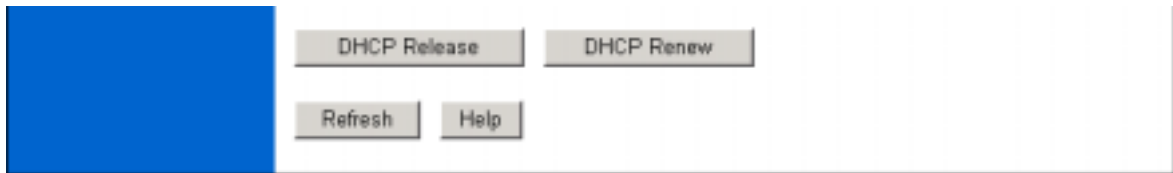
Host Name: The Host Name is the name of the Router. This entry is necessary for some ISPs.

Domain Name: The Domain Name is the name of the Router's domain. This entry is necessary for some ISPs.

DHCP Release: Click the **DHCP Release** button to delete the Router's current Internet IP address.

DHCP Renew: Click the **DHCP Renew** button to get a new Internet IP address for the Router.

Click the **Refresh** button to refresh the Router's status and settings.

Advanced Wireless

The Advanced Wireless screen allows you to customize data transmission settings and access the 802.1x Configuration screen. In most cases, the advanced settings on this screen should remain at their default values.

The advanced wireless settings should be left at their default values. Improper configuration may result in poor network performance.

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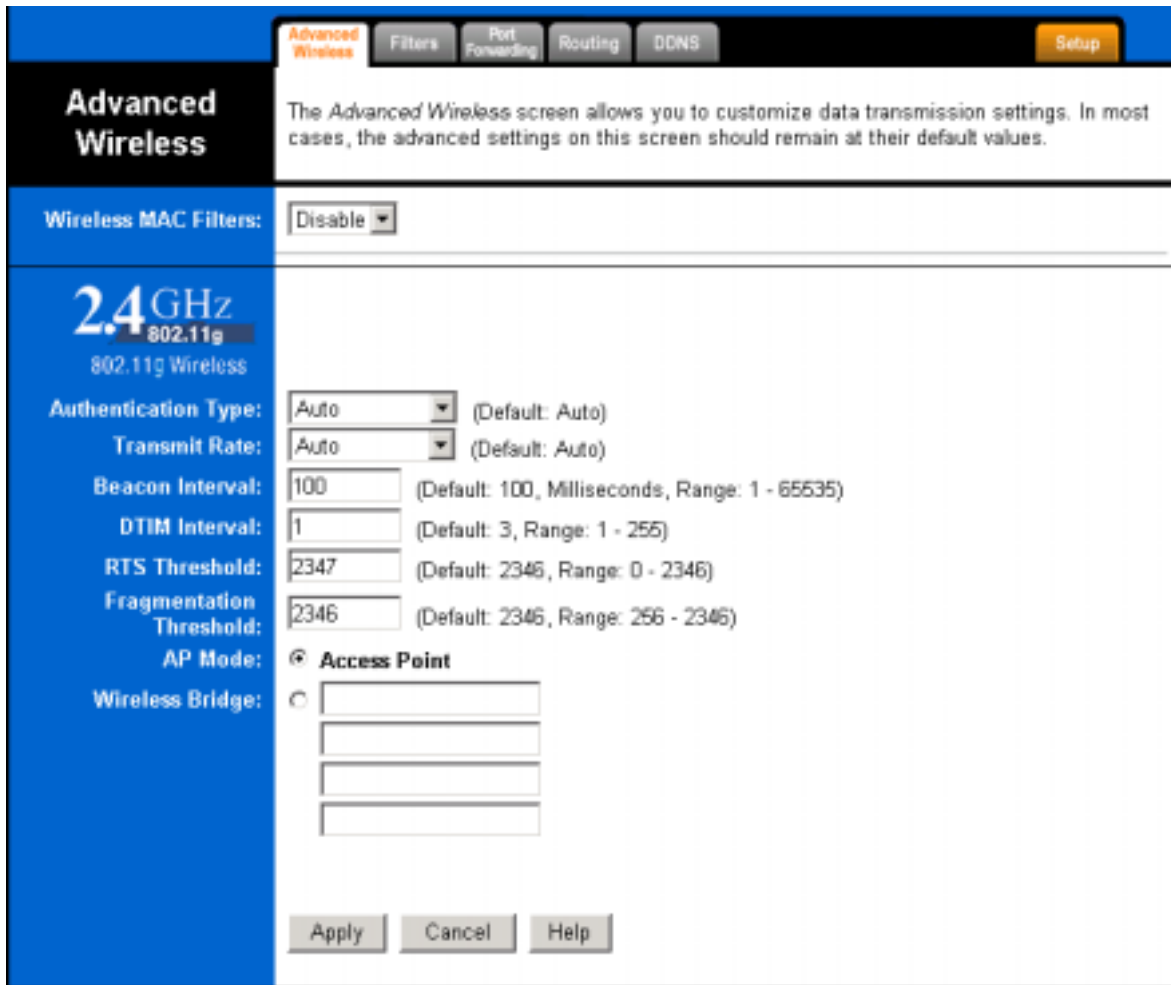
Beacon Interval: The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1000. A beacon is a packet broadcast by the Router to synchronize the wireless network. The default value is **100**.

DTIM Interval: This value, between 1 and 16384, 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**.

RTS Threshold: Should you encounter inconsistent data flow, only minor modifications of the default value, 2347, are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. 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 remain at its default value of **2347**.

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 modifications of this value are recommended. In most cases, it should remain at its default value of **2346**.

Transmission Rate: The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default setting is **Auto**.

Filters

The Filters screen allows you to block specific internal users from accessing the Internet. You can set up filters by using MAC addresses, IP addresses, or network port numbers (or a range of ports).

The *Internet Filter* screen allows you to block or allow specific kinds of Internet usage. You can set up Internet access policies for specific PCs and set up filters by using network port numbers.

Internet Access Policy: This feature allows you to customize up to 15 different Internet Access Policies for particular PCs, which are identified by their IP or MAC addresses. For each policy's designated PCs, the Router can do one or more of the following:

- block or allow Internet access or inbound traffic during the days and time periods specified
- block designated services
- block websites with specific URL addresses
- block websites that use specific keywords in their URL addresses.

To create or edit a policy, follow these instructions:

1. Select the policy's number (1-15) in the drop-down menu.

2. Enter a name in the *Enter Policy Name* field.

3. Select **Internet Access** or **Inbound Traffic** from the *Policy Type* drop-down

box, depending on the kind of access you want to control. Select **Internet**

Access to control your network PCs' access to the Internet. Select **Inbound**

Traffic to control Internet PCs' access to your local area network.

Note: The screen's settings will vary depending on which Policy Type you select.

4. Select **Deny** or **Allow**, depending on how you want to control access for specific PCs.
5. Click the **Edit List** button next to *PCs or Internet PCs.*
    a. On the *List of PCs* or *List of Internet PCs* screen, specify PCs by IP address or MAC address. Enter the appropriate IP addresses into the *IP* fields. If you have a range of IP addresses to filter, complete the appropriate *IP Range* fields. Enter the appropriate MAC addresses into the *MAC* fields.
    b. Click the **Apply** button to save your changes. Click the **Cancel** button to cancel your unsaved changes. Click the **Close** button to return to the *Internet Filter* screen.
6. Set the days when access will be filtered. Keep the default setting, **Everyday**, or select the appropriate days of the week.
7. Set the time when access will be filtered. Keep the default setting, **24 Hours**, or check the box next to *From* and use the drop-down boxes to designate a specific time period.

Note: Access for the listed PCs will be controlled during the selected days and times. Any blocked services or websites will be blocked at all times.

8. In the *Blocking Services* drop-down boxes, select the services you want to block (the default setting is **None**). In the *Blocking Services* fields, the range of ports for this service will appear. If you want to change the range of ports, enter the new numbers in the *Blocking Services* fields, or edit the service's settings (see below).
    To add a service or edit a service's settings, follow these instructions:
    a. Click the **Add Service** button.
    b. To create a new service, enter the name of the service in the *Service Name* field. To edit a service's settings, select the service from the box on the right of the screen.
    c. From the *Protocol* drop-down menu, select the protocol type for this service: **ICMP**, **UDP**, **TCP**, or **UDP & TCP**.
    d. In the *Port Range* fields, enter the range of ports for this service.
    e. To add a service, click the **Add** button. To edit the settings for a service, click the **Modify** button.
    f. To delete a service, select the service from the box on the right of the screen. Click

the **Delete** button.

g. Click the **Apply** button to save your changes. Click the **Cancel** button to undo your changes. Click the **Close** button to close the *Add Service* window.

9. 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. (This feature is not available if you chose **Inbound Traffic** for the *Policy Type.*)

10. 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. You can enter up to six keywords. (This feature is not available if you chose **Inbound Traffic** for the *Policy Type.*)

11. Click the **Apply** button to save your settings for an Internet Access Policy. Click the **Cancel** button to cancel your unsaved changes.

12. To create or edit additional policies, repeat steps 1-11.

Check all the settings and click **Apply** to save them.

Port Forwarding

The Port Range Forwarding screen sets up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)

When users send this type of request to your network via the Internet, the Router will forward those requests to the appropriate PC. Any PC whose port is being forwarded must have its DHCP client function disabled and must have a new static IP address assigned to it because its IP address may change when using the DHCP function.
Click **Apply** to save your settings.
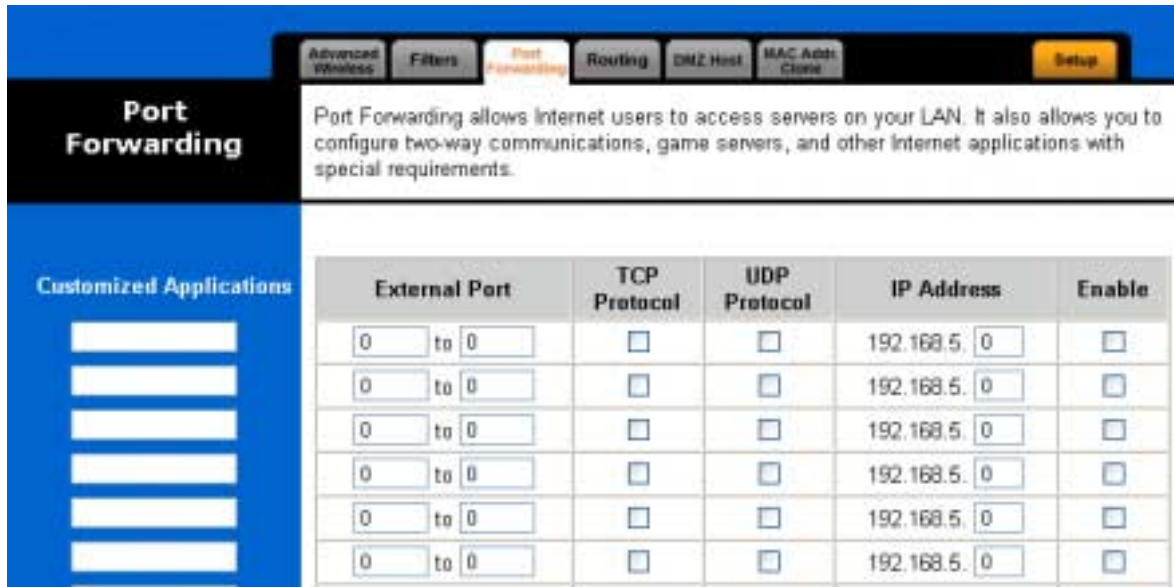
Customized Applications: Enter the name of the public service or other Internet application in the field provided.

External Port: Enter the numbers of the External Ports (the port numbers seen by users on the Internet).

TCP Protocol: Click this checkbox if the application requires TCP.

UDP Protocol: Click this checkbox if the application requires UDP.

IP Address: Enter the **IP Address** of the PC running the application.

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

The following table gives the typical port forwarding settings for common Internet applications.

Applications	External Port	TCP Protocol	UDP Protocol
FTP	21	☑	
Telnet	23	☑	
SMTP	25	☑	
DNS	53		☑
TFTP	69		☑
Finger	79	☑	
HTTP	80	☑	
POP3	110	☑	
NNTP	119	☑	
SNMP	161		☑

Routing

On the Routing screen, you can set the routing mode of the Router. Gateway mode is recommended for most users.

To set up routing:

1. Choose the correct working mode. Select **Gateway** if the Router is hosting your network's connection to the Internet (recommended for most users). Select **Router** if the Router exists on a network with other routers.
2. If you selected the Gateway mode, click the **Apply** button. If you selected the Router mode, proceed to step3.
3. For Dynamic Routing, select **Enable** from the drop-down box if you want the Router to automatically adjust to physical changes in the network's layout. The Router determines the network packets' route based on the fewest number of hops between the source and the destination. Select **Disable** to disable the Dynamic Routing feature for data transmissions.
4. 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.)
5. Enter the following data:

- **Destination IP Address** - The Destination IP Address 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 an 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.

Depending on where the Destination IP Address is located, select **LAN & Wireless** or **Internet (WAN)** from the *Interface* drop-down menu.

6. To cancel your changes, click the **Cancel** button. To save your changes, click the **Apply** button.

To delete a static route entry:

1. From the *Static Routing* drop-down list, select the entry number of the static route.
2. Click the **Delete This Entry** button.
3. To cancel a deletion, click the **Cancel** button. To save a deletion, click the **Apply** button.

Show Routing Table

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

- **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 an IP address is the network portion, and which portion is the host portion.
- **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 your network is on the internal LAN, the WAN (Internet), or Loopback (a dummy network in which one PC acts like a network - necessary for certain software programs).

DDNS

The Dynamic Domain Name System (DDNS) feature lets you assign a fixed 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. Select which DDNS Service provider you want to use, DynDNS.org or TZO.com
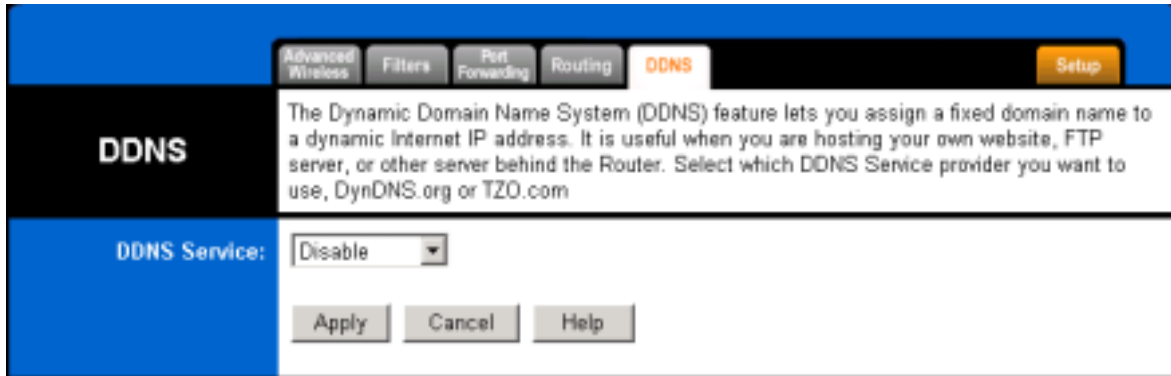
DynDNS.org:

DDNS Service: To disable DDNS Service, keep the default setting, **Disable**. 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* (you can click the link on the *DDNS* screen). 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.

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

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

TZO.com

DDNS Service: To disable DDNS Service, keep the default setting, **Disable**. To enable DDNS Service using TZO.com, 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 *.tzo.com*, or order TZO service at *www.tzo.com/order.html* (you can click the appropriate link on the *DDNS* screen). 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.

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

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

Troubleshooting

Basic Functions

Note: If you are using a cable or DSL modem and are experiencing problems connecting to the Internet, follow these steps:

1. Power off your cable or DSL modem, PC, and the Router.
2. Power on your modem and wait a few minutes until the modem has established a connection with your ISP.
3. Power on the Router.
4. Power on your PC and attempt to connect to the Internet.

For most users, the Router's default values should be satisfactory. Some users may need to enter additional information in order to connect to the Internet through their ISP or broadband (cable or DSL) carrier. For example, some cable providers require a specific MAC address for connection to the Internet. To learn more about this, click the **System** tab and then the **MAC Cloning** tab.

My Wireless AP Router will not turn on. No LED's light up.

Cause:
- The power is not connected.

Resolution:
- Connect the power adapter to your AP and plug it into the power outlet.

Note: Only use the power adapter provided with your AP. Using any other adapter may damage your SOHO AP Router.

LAN Connection Problems
I can't access my AP Router.

WX-5525R Dual Band AP Router

Cause:

- The unit is not powered on.
- There is not a network connection.
- The computer you are using does not have a compatible IP Address.

Resolution:

- Make sure your AP is powered on.
- Make sure that your computer has a compatible IP Address. Be sure that the IP Address used on your computer is set to the same subnet as the AP. For example, if the AP is set to 192.168.5.2, change the IP address of your computer to 192.168.5.15 or another unique IP Address that corresponds to the 192.168.5.X subnet.

  Use the Reset button located on the rear of the AP Router to revert to the default settings.

I can't connect to other computers on my LAN.

Cause:

- The IP Addresses of the computers are not set correctly.
- Network cables are not connected properly.
- Windows network settings are not set correctly.

Resolution:

- Make sure that each computer has a unique IP Address. If using DHCP through the AP Router, makes sure that each computer is enable DHCP function and restart the computer.
- Make sure that the Link LED is on. If it is not, try a different network cable.
- Check each computer for correct network settings.

Wireless Troubleshooting

I can't access the Wireless AP Router from a wireless network card

Cause:

- Out of range.
- IP Address is not set correctly.

WX-5525R Dual Band AP Router

<u>Resolution</u>:

- 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.
- Check your IP Address to make sure that it is compatible with the Wireless AP Router.

Technical Specifications

Standards:

    IEEE 802.3 10BASE-T Ethernet

    IEEE 802.3u 10/100BASE-TX Fast Ethernet

    IEEE 802.11a

    IEEE 802.11b

Protocols Supported:

    TCP/ IP

    IPX

    UDP

    DHCP Client

    DHCP Server

Management:

    Web-Based

Ports:

    LAN: 10BASE-T/100BASE-TX Fast Ethernet

    WAN: 10BASE-T Ethernet

Wireless AP Specifications

General Wireless Specifications:

    802.11g Wireless LAN

Access Point Frequency Band:

    5GHz (subject to local regulation)

Access Point Number of Channel:

11g:

    USA & Canada: 11 (1- 11)

  Most European: 13 (1-13)

  France : 4 (10-13)

  Japan   : 14 (1-14)

Access Point Data Rate:

11g:

  54 Mbps

  48 Mbps

  36 Mbps

  24 Mbps

  18 Mbps

  12 Mbps

  9 Mbps

  6 Mbps

Data encryption:

  64/128 bit WEP

Power Specifications :

DC power supply

 Input: DC 100-250 50-60 Hz 1A

 Output: 5V DC 2A

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules.   These limits are designed to provide reasonable protection against harmful interference in a residential installation.   This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.   However, there is no guarantee that interference will not occur in a particular installation.   If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance.   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 RF Radiation Exposure Statement:
This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled   environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

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

R&TTE Compliance Statement

This equipment complies with all the requirements of the DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000 .

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this manual and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries intended for use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Ireland, Italy, Luxembourg, The Netherlands, Portugal, Spain, Sweden and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

EU Countries Not intended for use

None.

Potential restrictive use

France: Only channels 10,11,12, and13