

# **Wireless LAN 802.11g Series**

## **WLF-2454AP-S**

### **User's Guide**

**Version 1.0**

## Contents

<b>1. Introduction</b> .....	<b>2</b>
<b>2. Safety Notification</b> .....	<b>3</b>
<b>3. Hardware Installation</b> .....	<b>4</b>
<b>4 Web Management Settings</b> .....	<b>5</b>
4.1. Setup.....	6
4.2. Security.....	9
4.3. System.....	11
4.4. DHCP.....	14
4.5. SNMP.....	16
4.6. Status.....	17
4.7. Advanced Wireless.....	18
4.8. Filters.....	21
4.9. Port Forwarding.....	23
4.10. Routing.....	25
4.11. DDNS.....	27
<b>5. Troubleshooting</b> .....	<b>28</b>

## 1. Introduction

Thank you for purchasing the WLF2454AP-S Wireless 802.11g AP Router.

This user guide will assist you with the installation procedure.

The package you have received should contain the following items:

- AP Router Wireless 802.11g AP Router
- Power Supply / Cord
- Ethernet Cable
- Installation CD

Note: if anything is missing, please contact your dealer.

## 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.
- 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 the following status LED's.

LED	STATUS	Description
PWR/STAT	Off	No power
	Red On	1. Power on
	Red Blink	1. System startup
LAN	Off	no Ethernet link detected
	Green On	10/100Mbps Fast Ethernet link detected. No activity.
	Green Blink	Indicates traffic on the 10/100 Mbps LAN interface
WAN	Orange Blink	Indicates traffic on the 10 Mbps WAN interface
G	Yellow Blink	Indicates the device is linking to another wireless device, or active data is being transmitted via the wireless link.

#### Rear Panel

The rear panel features 4 LAN ports, 1 WAN port and a 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 agreement.
Reset	Press the Reset Button for approximately ten seconds, to reset all settings to factory default values.
LAN	The RJ-45 Ethernet port is 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 xDSL or Cable modem.

#### AP Router Default Settings

The default settings are shown in the following table.

User	
Password	Admin
AP Router IP Address	192.168.1.1
AP Router Subnet Mask	255.255.255.0
RF ESSID	wlan-g
11g RF Channel	6
Mode	Mixed (11b and 11g)
Encryption	Disabled
DHCP client	Enabled

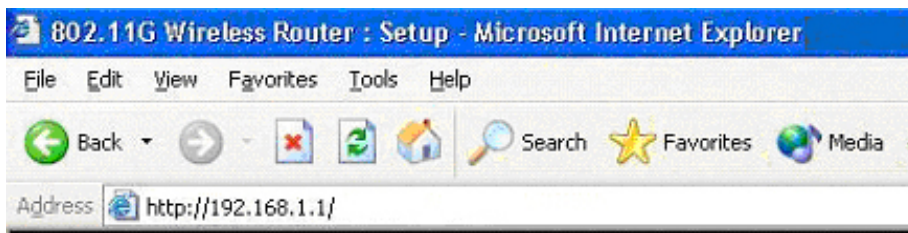
## 4 Web Management Settings

### TURN ON POWER SUPPLY

A 'Quick' power cycle can cause the AP's firmware to become corrupt. When powered on, be careful not to power the unit off again for at least 5 seconds, while data is being written to the flash.

### START UP & LOGIN

In order to configure the Wireless 11g AP Router, you must use your web browser and manually enter <http://192.168.1.1> into the Address box and press Enter. The Main Page will appear.



In order to configure the Wireless 11g AP Router, you must enter the password into the **Password** box and leave the **User Name** blank. The default password is "**admin**".

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

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

## 4.1. Setup

### **ENSURE YOU HAVE THE CORRECT NETWORK SETTINGS IN YOUR COMPUTER**

To change the configuration, use Internet Explorer (IE) or Netscape Communicator to connect to the WEB management **192.168.1.1**.

### Setup

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

**Setup**

The Setup screen lets you configure the basic Internet, LAN, and wireless settings. For further information, please see the User Guide or click the Help button.

**Firmware Version:** 1.4.3.9, Mar.10, 2003

**Time Zone:** (GMT-08:00) Pacific Time (USA & Canada)  Automatically adjust clock for daylight saving changes.

**Internet**

**MAC Address:** 00:11:22:33:44:56

**Host Name:**  Host and Domain settings may be required by your ISP.

**Domain Name:**

**Connection Type:** Automatic Configuration - DHCP  Select the type of connection you have to the Internet.

**LAN**

**MAC Address:** 00:11:22:33:44:55

**IP Address:** 192 . 168 . 1 . 1 This is the IP address and Subnet Mask of

**Subnet Mask:** 255.255.255.0 the Router as it is seen by your local network.

**Wireless:**

**MAC Address:** 00:90:4B:22:05:F0

**Mode:** Mixed

**Domain:** FCC

**Channel:** 6

**SSID:** sparklan-g **SSID Broadcast:** Enable

**WEP:**  Enable  Disable

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.

### Internet:

**Host Name:** This entry may be necessary with some ISP's. Please consult your ISP.

**Domain Name:** This entry may be necessary with some ISP's. Please consult your ISP.

**Connection 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 options 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.

Descriptions of these options:

### **Internet IP Address and Subnet Mask (Static IP or PPTP)**

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 (Static IP or PPTP)**

Your ISP will provide you with the Gateway IP Address.

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

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

- **User Name and Password (PPPoE or PPTP)**

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 AP Router 802.11g AP Router max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

- **Keep Alive Option**

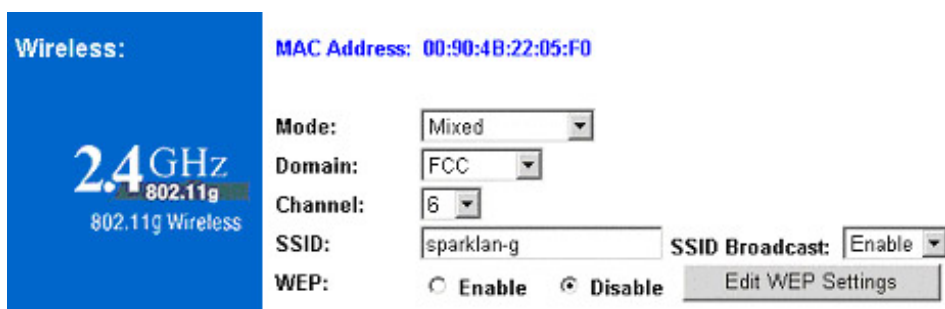
This option keeps you connected to the Internet indefinitely, even when your connection sits idle. To use this option, click the radio button next to *Keep Alive*. The default Redial Period is 30 seconds (in other words, the Router will check the Internet connection every 30 seconds).



**LAN 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:** This section provide the Wireless Network settings for your WLAN

## 2.4GHz Settings



Wireless: **2.4GHz** 802.11g 802.11g Wireless

MAC Address: 00:90:4B:22:05:F0

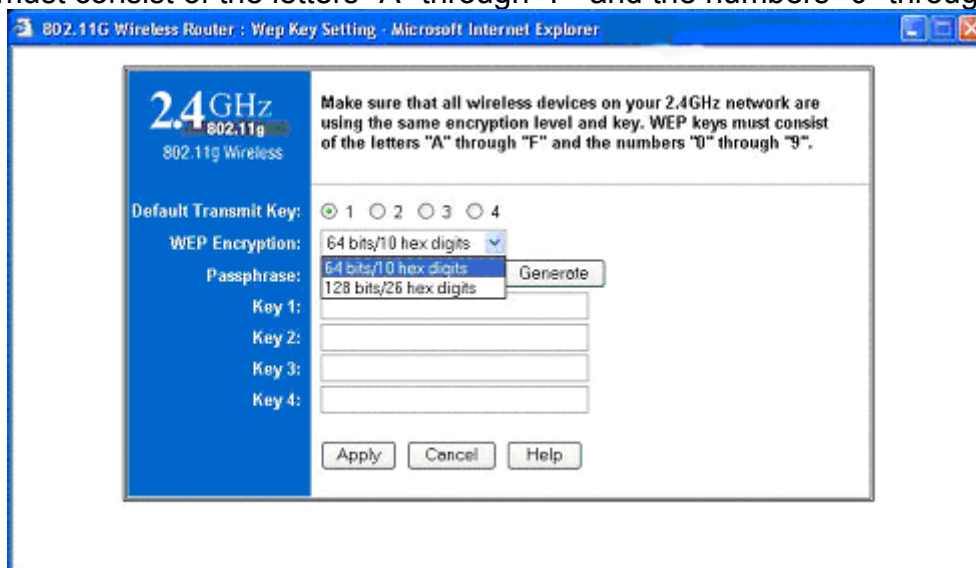
Mode: Mixed  
Domain: FCC  
Channel: 6  
SSID: sparklan-g SSID Broadcast: Enable  
WEP:  Enable  Disable

**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 must select the same SSID for all the APs that will be communicating with mobile wireless stations.

**Domain:** Please select the correct Domain for your physical location. ETSI is recommended.

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

**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."



802.11G Wireless Router : Wep Key Setting - Microsoft Internet Explorer

**2.4GHz** 802.11g 802.11g Wireless

Make sure that all wireless devices on your 2.4GHz 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".

Default Transmit Key:  1  2  3  4

WEP Encryption: 64 bits/10 hex digits  
Passphrase: 64 bits/10 hex digits   
128 bits/26 hex digits

Key 1:   
Key 2:   
Key 3:   
Key 4:

\* Click **Apply** to save your settings.

## 4.2. Security

The screenshot shows the 'Security' configuration page. At the top, there are navigation tabs: Setup, Security (highlighted), System, DHCP, and SNMP. On the right, there are buttons for Status, Help, and Advanced. The main heading is 'Security'. Below it, a text box explains that the Security screen allows changing the Router's security settings and strongly recommends changing the factory default password 'admin'. The 'Router Password' section has two input fields: '(Enter New Password)' and '(Re-enter to Confirm)'. The 'VPN Pass-Through' section has three checked checkboxes: IPsec, L2TP, and PPTP. The 'Web Filters' section has four unchecked checkboxes: Proxy, Java, ActiveX, and Cookies. The 'DMZ' section has a dropdown menu set to 'Disable' and a 'DMZ Host IP Address' field with the value '192 . 168 . 1 . 0'. The 'Block WAN Request' section has a dropdown menu set to 'Enable'. At the bottom, there are three buttons: Apply, Cancel, and Help.

**Router Password:** Changing the password for the AP Router is as easy as typing the password into the **Enter 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 Security screen). This will increase security, protecting the Router from unauthorised changes.

**VPN Pass-Through:** Virtual Private Networking (VPN) is typically used for business-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 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 unknown ports to one PC on the LAN. Note: DMZ hosting is not secure, as it opens all ports to the internet.

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, otherwise 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:** 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.

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

## 4.3. System

The screenshot shows the 'System' configuration page. At the top, there are tabs for 'Setup', 'Security', 'System' (selected), 'DHCP', and 'SNMP'. On the right, there are buttons for 'Status', 'Help', and 'Advanced'. The main heading is 'System'. Below it, a description states: 'The System screen lets you enable a variety of the Router's general features, from restoring factory defaults to enabling its logging capability.'

**Restore Defaults:**  Yes  No  
**CAUTION:** Any settings you have saved will be lost when the default settings are restored.

**Firmware Upgrade:**  Firmware: 1.4.4.5, June.10, 2003

**Multicast Pass-Through:** Enable ▾

**MAC Cloning:** Disable ▾ MAC Address: 00 . 00 . 00 . 00 . 00 . 00

**Remote Management:** Disable ▾ Port Number: 8080

**MTU:** Auto ▾ Size: 1400

**UPnP:** Disable ▾

**Log:** Disable ▾

At the bottom, there are buttons for 'Apply', 'Cancel', and 'Help'.

**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:** Click the **Upgrade** button to load new firmware onto the Router. If the Router is not experiencing difficulties, then there is no need to download a more recent firmware version, unless that version has a new feature that you want to use.

**Note: When you upgrade the Router's firmware, you may lose its configuration settings, so make sure you write down the Router's settings before you upgrade its firmware.**

*To upgrade the Router's firmware:*

1. Download the firmware upgrade file from [www.alloy.com.au](http://www.alloy.com.au)
2. Extract the firmware upgrade file (if compressed)
3. Click the Upgrade button.

4. On the Firmware Upgrade screen, click the **Browse** button to find the firmware upgrade file.



5. Double-click the firmware upgrade file.

6. Click the Upgrade button, and follow the on-screen instructions.

**Note: Do not power off the Router or press the Reset button while the firmware is being upgraded.**

**Multicast Pass-Through:** IP Multicasting occurs when a single data packet 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. This feature is enabled by default, or select **Disable** to disable the feature.

**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/adaptor, 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:** 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 should also change the Router's default password, if you haven't already done so. 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:** 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 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, Log viewer software must be used. In the Send Log to field, enter the fixed IP address of the PC running the Log viewer 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.

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

## 4.4. DHCP

The DHCP screen allows you to configure the settings for the Router's Dynamic Host Configuration Protocol (DHCP) server function. A DHCP server automatically assigns an IP address to each computer on your network. The Router can be used as a DHCP server for your network. If you already have a DHCP server for your network, then disable the DHCP Server feature.

**DHCP Server:**

**Starting IP Address:** 192 . 168 . 1 . 100

**Maximum Number of DHCP Users:**

**Client Lease Time:**  Minutes (0 means one day)

**Static DNS 1:**  .  .  .

**2:**  .  .  .

**3:**  .  .  .

**WINS:**  .  .  .

**Currently Assigned:**

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 of 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 networked computer (note that each IP Address must be unique).

**DHCP Server:** Select the **Enable** option 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 select **Disable** from the options.

**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 192.168.5.253. The default Starting IP Address is **192.168.1.100**.

**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 192.168.1.1 is your starting IP address. The default is **50**.

**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 "leasing" 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 IP addresses. 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.

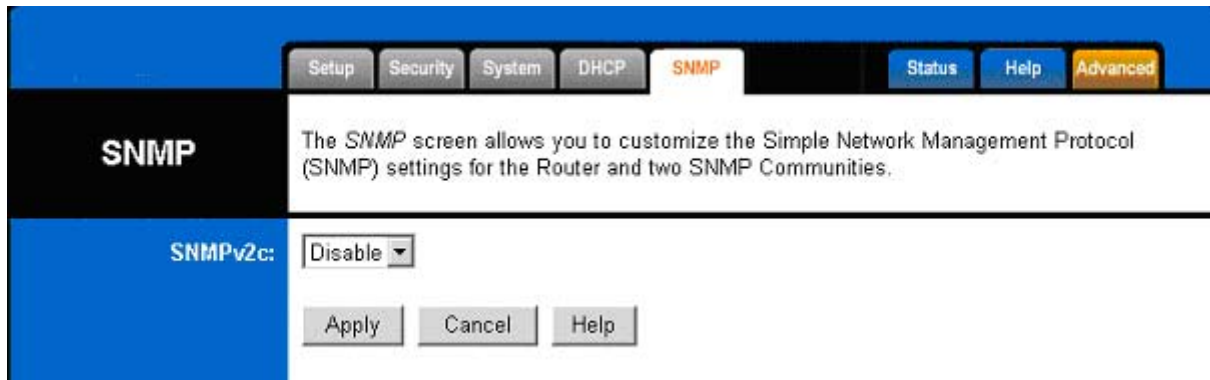
**WINS:** The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter that server's IP Address here. Otherwise, leave this blank.

**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.



## 4.5. SNMP



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

<b>SNMPv2c</b>		To enable the SNMP support feature, select <b>Enable</b> . Otherwise, select <b>Disable</b> .
<b>Identification</b>	<b>Contact</b>	In the contact field, enter contact information for the Router.
	<b>Device Name</b>	In the Device Name field, enter the name of the Router.
	<b>Location</b>	In the Location field, specify the area or location where the Router resides.
<b>SNMP Community</b>	<b>public</b>	You may change the SNMP Community's name from its default, <b>public</b> . Then configure the community's access as either <b>Read-Only</b> or <b>Read-Write</b> .
	<b>private</b>	You may change the SNMP Community's name from its default, <b>private</b> . Then configure the community's access as either <b>Read-Only</b> or <b>Read-Write</b> .

Click **Apply** to save your settings.

## 4.6. Status

Status	
The Status screen displays the Router's current status and configuration. This information is read-only.	
<b>Firmware Version:</b>	1.4.4.5, June.10, 2003
<b>Current Time:</b>	Sun Jan 4 00:49:55 1970
<b>Host Name:</b>	
<b>Domain Name:</b>	
<b>LAN</b>	<b>MAC Address: 00:90:4B:A0:4A:74</b>
	IP Address: 192.168.0.155
	Subnet Mask: 255.255.255.0
	DHCP server: Disable
	<b>MAC Address: 00:90:4B:25:FC:B4</b>
	Mode: G-Only
	Channel: 1
	SSID: ALLOY
	Encryption Function: Enable
<b>Internet</b>	<b>MAC Address: 00:90:4B:A0:4A:75</b>
<b>Configuration Type:</b>	Automatic Configuration - DHCP
	IP Address: 0.0.0.0
	Subnet Mask: 0.0.0.0
	Default Gateway: 0.0.0.0
	0.0.0.0
	DNS: 0.0.0.0
	0.0.0.0

This screen displays the Wireless Router's current status and settings. This information is read-only. This page will auto re-refresh every 5 seconds to keep the most up to date 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.

## 4.7. Advanced Wireless

The screenshot shows the 'Advanced Wireless' configuration page. At the top, there are tabs for 'Advanced Wireless', 'Filters', 'Port Forwarding', 'Routing', and 'DDNS', along with a 'Setup' button. Below the tabs, a text box explains that the screen allows for customizing data transmission settings. The 'Wireless MAC Filters' dropdown is set to 'Disable'. On the left, a sidebar indicates '2.4GHz 802.11g 802.11g Wireless' and lists various settings: Authentication Type (Auto), Transmit Rate (Auto), Beacon Interval (100), DTIM Interval (3), RTS Threshold (2347), Fragmentation Threshold (2346), AP Mode (Access Point), and Wireless Bridge (disabled). At the bottom, there are 'Apply', 'Cancel', and 'Help' buttons, as well as 'DHCP Release', 'DHCP Renew', 'Refresh', and 'Help' buttons.

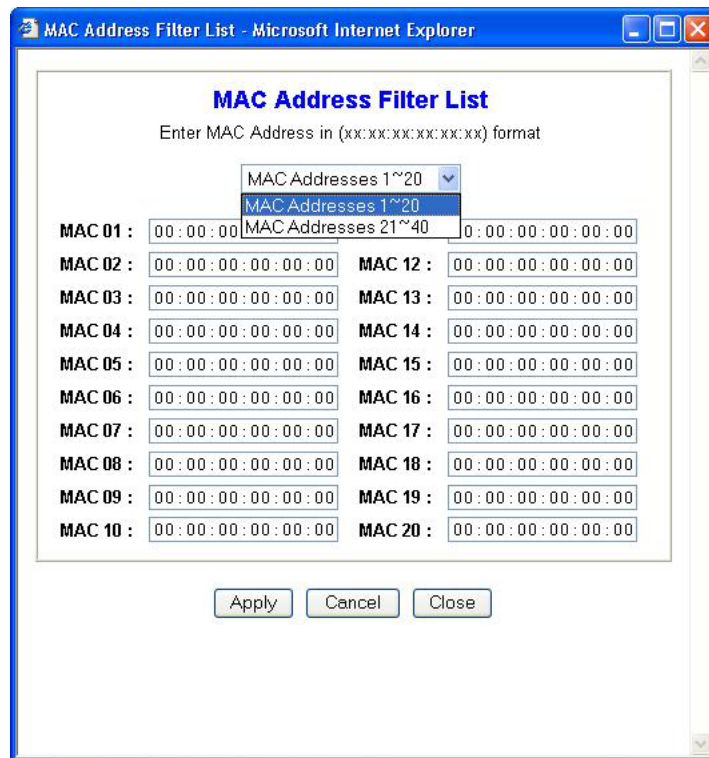
**Wireless MAC Filters:** This function allows the administrator to have access control by entering MAC addresses of client stations. When this function has been **Enabled**, two new options will appear.

This screenshot shows the 'Advanced Wireless' configuration page with 'Wireless MAC Filters' set to 'Enable'. Below the dropdown, there are two radio button options: 'Prevent PCs listed from accessing the wireless network.' (which is selected) and 'Permit PCs listed to access the wireless network.'. An 'Edit MAC Filter List' button is located below these options.

Depending on the filtering purpose, it can be selected to **Prevent** or **Permit** access.

Click on **Edit MAC Filter List** to add the client stations to the MAC list.

The table can store up to **40** different MAC addresses. Please follow the format that is required when an address is to be entered.



#### Authentication Type:

**Auto:** Auto is the default authentication algorithm. The AP will change its authentication type automatically to fulfill client's requirement.

**Open System:** Open System authentication is not required to be successful while a client may decline to authenticate with any particular other client.

**Shared Key:** Shared Key is only available if the WEP option is implemented. Shared Key authentication supports authentication of clients as either a member of those who know a shared secret key or a member of those who do not. IEEE 802.11 Shared Key authentication accomplishes this without the need to transmit the secret key in clear text. Requiring the use of the WEP privacy mechanism.

**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**.

**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 Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Access Point Clients hear the beacons and awaken to receive the broadcast and multicast messages.

**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**.

**RTS Threshold:** This value should remain at its default setting of 2346. Should you encounter inconsistent data flow, only minor modifications 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.

**Fragmentation Threshold:** This value specifies the maximum size for a packet before data is fragmented into multiple packets. It should remain at its default setting of 2346. 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.

**AP Mode or Wireless Bridge Mode:** The WLF2454AP-S can operate in two modes. When **AP Mode** is selected, the device operates as a normal Access Point.

**Wireless Bridge Mode** enables communication with another AP Router to bridge 2 or more LANS over a wireless connection.

\* Click **Apply** to save your settings.

## 4.8. Filters

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.

<p><b>Internet Access Policy</b></p>	<p>This feature allows you to customize up to 10 different Internet Access Policies for particular PCs, which are identified by their IP or MAC addresses. For each designated policy, the Router can do one or more of the following:</p> <ul style="list-style-type: none"> <li>• block or allow Internet access or inbound traffic during the days and time periods specified</li> <li>• block designated services</li> <li>• block websites with specific URL addresses</li> <li>• block websites that use specific keywords in their URL addresses.</li> </ul> <p><i>To create or edit a policy, follow these instructions:</i></p> <ol style="list-style-type: none"> <li>1. Select the policy's number (1-10) in the drop-down menu.</li> <li>2. Enter a name in the <i>Enter Policy Name</i> field.</li> <li>3. Select <b>Internet Access</b> or <b>Inbound Traffic</b> from the <i>Policy Type</i> drop-down box, depending on the kind of access you want to control. Select <b>Internet Access</b> to control your network PCs' access to the Internet. Select <b>Inbound Traffic</b> to control Internet PCs' access to your local area network.</li> </ol>
--------------------------------------	---

Note: This 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.

<b>Delete</b>	To delete an Internet Access Policy, select the policy's number, and click the <b>Delete</b> button.
<b>Summary</b>	To see a summary of all the policies, click the <b>Summary</b> button. The <i>Internet Policy Summary</i> screen will show each policy's number, Name, Type, Days, and Time of Day. To delete a policy, click its box, and then click the <b>Delete</b> button. Click the <b>Close</b> button to return to the <i>Internet Filter</i> screen.

## 4.9. 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.

External Port	Protocol TCP	Protocol UDP	IP Address	Enable
0 to 0	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1.0	<input type="checkbox"/>
0 to 0	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1.0	<input type="checkbox"/>
0 to 0	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1.0	<input type="checkbox"/>
0 to 0	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1.0	<input type="checkbox"/>
0 to 0	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1.0	<input type="checkbox"/>
0 to 0	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1.0	<input type="checkbox"/>
0 to 0	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1.0	<input type="checkbox"/>
0 to 0	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1.0	<input type="checkbox"/>
0 to 0	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1.0	<input type="checkbox"/>
0 to 0	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1.0	<input type="checkbox"/>
0 to 0	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1.0	<input type="checkbox"/>

Port Triggering

Apply Cancel Help

The *Port 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 static IP address assigned to it, otherwise its IP address may change when using the DHCP function.



<b>Customized Applications</b>	Enter the name of the public service or other Internet application in the field provided.
<b>External Port</b>	Enter the numbers of the External Ports (the port numbers seen by users on the Internet).
<b>TCP Protocol</b>	Click this checkbox if the application requires TCP.
<b>UDP Protocol</b>	Click this checkbox if the application requires UDP.
<b>IP Address</b>	Enter the IP Address of the PC running the application.
<b>Enable</b>	Click the <b>Enable</b> checkbox to enable port forwarding for the application.
<b>Port Triggering</b>	<p>Port 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. Click the <b>Port Triggering</b> button to set up triggered ports, and follow these instructions:</p> <ol style="list-style-type: none"> <li>1. Enter the Application Name of the trigger.</li> <li>2. Enter the Outgoing Port Range used by the application. Check with the Internet application for the port number(s) needed.</li> <li>3. Enter the Incoming Port Range used by the application. Check with the Internet application for the port number(s) needed.</li> <li>4. Click the <b>Apply</b> button to save your changes. Click the <b>Cancel</b> button to cancel your unsaved changes. Click the <b>Close</b> button to return to the <i>Port Forwarding</i> screen.</li> </ol>

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

## 4.10. Routing

Advanced Wireless Filters Port Forwarding **Routing** DDNS Setup

**Routing**

On this screen, configure the routing mode and settings for the Router. Gateway mode is recommended for most users.

**Operating Mode:** Gateway

**Static Routing:** 1 --- (Select Route Entry) Delete This Entry

**Enter Route Name:**

**Destination IP Address:** 0 . 0 . 0 . 0

**Subnet Mask:** 0 . 0 . 0 . 0

**Gateway:** 0 . 0 . 0 . 0

**Interface:** LAN & Wireless

Show Routing Table

Apply Cancel Help

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

<p><b>Operating Mode</b></p>	<p>The default setting is <b>Gateway</b>.</p> <p>Choose the correct working mode. Keep the default setting, <b>Gateway</b>, if the Router is hosting your network's connection to the Internet (Gateway mode is recommended for most users). Select <b>Router</b> if the Router exists on a network with other routers.</p>
<p><b>Dynamic Routing (RIP)</b></p>	<p><b>Note: This feature is not available in Gateway mode.</b></p> <p>The default setting is <b>Disable</b>.</p> <p>Dynamic Routing enables the Router to automatically adjust to physical changes in the network's layout and exchange routing tables with other routers. The Router determines the network packets' route based on the fewest number of hops between the source and destination.</p> <p>To enable the Dynamic Routing feature, select <b>Enable</b>. To disable the Dynamic Routing feature for all data transmissions, keep the default setting, <b>Disable</b>.</p>
<p><b>Static Routing, Destination IP Address, Subnet Mask, Gateway, and Interface</b></p>	<ol style="list-style-type: none"> <li>To set up a static route between the Router and another network, select a number from the <i>Static Routing</i> drop-down list. (A static route is a pre-determined pathway that network information must travel to reach a specific host or network.)</li> <li>Enter the following data: <ul style="list-style-type: none"> <li>• <b>Destination IP Address</b> - The Destination IP Address is the address of the network or host to which you want to assign a static route.</li> <li>• <b>Subnet Mask</b> - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.</li> <li>• <b>Gateway</b> - This is the IP address of the gateway device that allows for contact between</li> </ul> </li> </ol>

	<p>the Router and the network or host.</p> <p>3. Depending on where the Destination IP Address is located, select <b>LAN &amp; Wireless</b> or <b>Internet (WAN)</b> from the <i>Interface</i> drop-down menu.</p> <p>4. To save your changes, click the <b>Apply</b> button. To cancel your unsaved changes, click the <b>Cancel</b> button.</p> <p>For additional static routes, repeat steps 1-4.</p>
<b>Delete This Entry</b>	<p>To delete a static route entry:</p> <ol style="list-style-type: none"> <li>1. From the <i>Static Routing</i> drop-down list, select the entry number of the static route.</li> <li>2. Click the <b>Delete This Entry</b> button.</li> <li>3. To save a deletion, click the <b>Apply</b> button. To cancel a deletion, click the <b>Cancel</b> button.</li> </ol>
<b>Show Routing Table</b>	<p>Click the <b>Show Routing Table</b> 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 <b>Refresh</b> button to refresh the data displayed.</p> <ul style="list-style-type: none"> <li>• <b>Destination LAN IP</b> - The Destination IP Address is the address of the network or host to which the static route is assigned.</li> <li>• <b>Subnet Mask</b> - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.</li> <li>• <b>Gateway</b> - This is the IP address of the gateway device that allows for contact between the Router and the network or host.</li> <li>• <b>Interface</b> - This interface tells you whether the Destination IP Address is on the <b>LAN &amp; Wireless</b> (internal wired and wireless networks), the <b>WAN</b> (Internet), or <b>Loopback</b> (a dummy network in which one PC acts like a network—necessary for certain software programs).</li> </ul>

\* Click **Apply** to save your settings.

## 4.11. 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.org

<b>DDNS Service</b>	To disable DDNS Service, keep the default setting, <b>Disable</b> . To enable DDNS Service using DynDNS.org, follow these instructions: <ol style="list-style-type: none"> <li>1. On the <i>DDNS</i> screen, select <b>DynDNS.org</b> from the <i>DDNS Service Provider</i> drop-down menu.</li> <li>2. Sign up for DynDNS service at <a href="http://www.dyndns.org">www.dyndns.org</a> (you can click the link on the <i>DDNS</i> screen). Write down your account information.</li> <li>3. Complete the <i>User Name</i>, <i>Password</i>, and <i>Host Name</i> fields.</li> <li>4. Click the <b>Apply</b> button to save your changes. Click the <b>Cancel</b> button to cancel unsaved changes.</li> </ol>
<b>Internet IP Address</b>	The Router's current Internet IP Address is displayed here.
<b>Status</b>	The status of the DDNS service connection is displayed here.

### TZO.com

<b>DDNS Service</b>	To disable DDNS Service, keep the default setting, <b>Disable</b> . To enable DDNS Service using TZO.com, follow these instructions: <ol style="list-style-type: none"> <li>1. On the <i>DDNS</i> screen, select <b>TZO.com</b> from the <i>DDNS Service Provider</i> drop-down menu.</li> <li>2. Sign up for a free, 30-day trial of TZO service at <a href="http://www.tzo.com/order.html">www.tzo.com/order.html</a> (you can click the appropriate link on the <i>DDNS</i> screen). Write down your account information.</li> <li>3. Complete the <i>Email Address</i>, <i>TZO Password Key</i>, and <i>Domain Name</i> fields.</li> <li>4. Click the <b>Apply</b> button to save your changes. Click the <b>Cancel</b> button to cancel unsaved changes.</li> </ol>
<b>Internet IP Address</b>	The Router's current Internet IP Address is displayed here.
<b>Status</b>	The status of the DDNS service connection is displayed here.

\* Click **Apply** to save your settings.

## 5. 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 **Advanced** tab and then the **MAC Address Clone** 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 AP Router.

### **LAN Connection Problems I can't access my 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 192.168.1.1, change the IP address of your computer to 192.168.1.15 or another unique IP Address that corresponds to the 192.168.1.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, make sure that each computer is enabled to use the 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.

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