FORMOSA
Wireless Systems Corp.

XG-520
Wireless 802.11b/g
Portable Router

User's Manual

FCC Certifications

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 or more 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.

CAUTION:
Any changes or modifications not expressly approved by the grantee of this device could void the user’s authority to operate the 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.

For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

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 20cm between the radiator and your body.

CE Mark Warning
This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.
All trademarks and brand names are the property of their respective proprietors.
Specifications are subject to change without prior notification.

CE Statement：
Hereby, we declares that this device is in compliance with the essential requirement and other relevant provisions of the R&TTE Directive 1999/5/EC.

Table of Content

CHAPTER 1: INTRODUCTION

The wireless 802.11b/g portable router is a compact/ travel size IEEE802.11b/g Access Point with 1 Fast Ethernet port, which provides a powerful high-speed wireless connection for compatible wireless-enabled devices into the network with the freedom to roam. With web-based UI, this portable router is easy to be setup and maintained. All functions can be configured within the easy and friendly user interface via web browser.

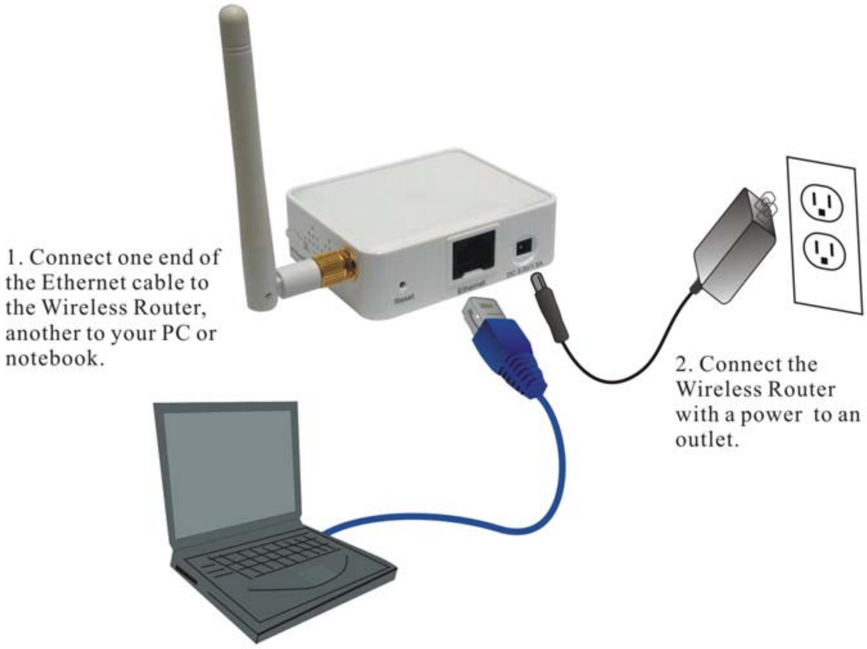
Via the fast wireless network speed of 54 Mbps, you can be very comfortable to have experience of high speed web surfing, files downloading, online game playing, and video conference session and streaming high quality multimedia materials. The wireless 802.11b/g portable router provides WPA/WPA2, 64/128 bit WEP encryption and IEEE802.1x which ensures a high level of security to protect users' data and privacy when traveling.

Features

1. Create temporary, personal, wireless access in your hotel room or a coffee shop hotspot.
2. Travel size design with 2dBi high gain antenna.
3. High security with built-in security: WEP 64/128, WPA, WPA2, 802.1x and 802.11i.
4. Support Router/AP, WDS (Bridge + Repeater), or Client Mode.
5. Advanced Quality of Service (QoS) - 802.11e, WMM.

Hardware Connection

1. Connect one end of the Ethernet cable to the Wireless Router, another end to your PC or notebook.
2. Connect the Wireless Router with a power to an outlet.

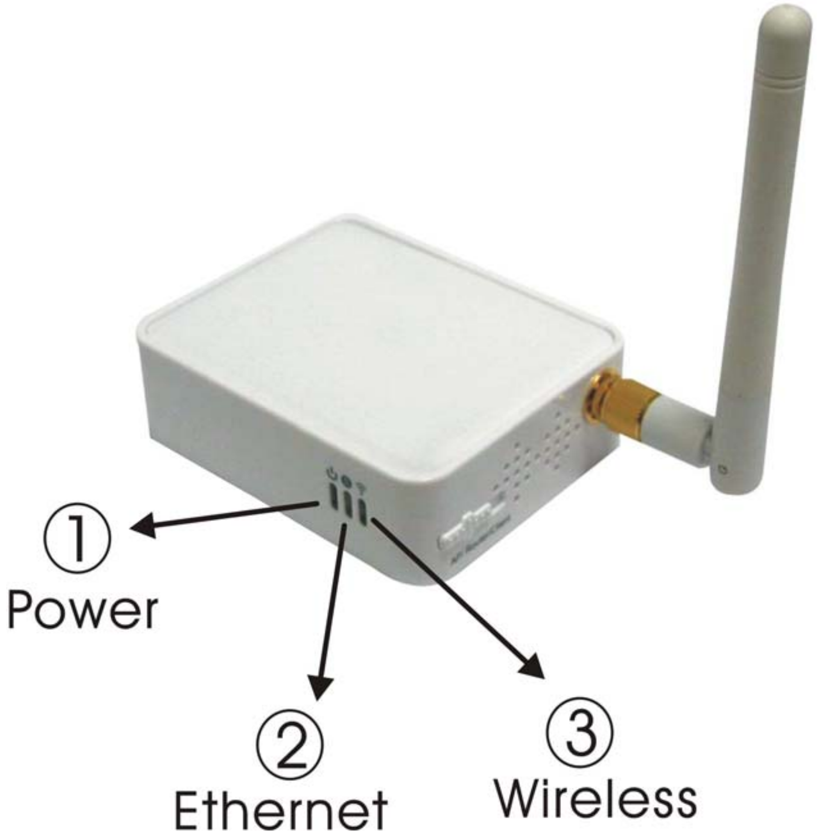


1. Connect one end of the Ethernet cable to the Wireless Router, another to your PC or notebook.

2. Connect the Wireless Router with a power to an outlet.

LED Indicators

Front Panel: (LED Indicators)



	LED Indicator	Color	Status	
			Solid	**Flashing**
1	Power	Blue	Turns solid Blue when the power is applied to this device.	NA
2	Ethernet	Blue	Turns solid Blue when an Ethernet cable is connected.	Receiving/ Sending data
3	Wireless	Blue	Turns solid Blue when the wireless is applied to this device.	Receiving/ Sending data

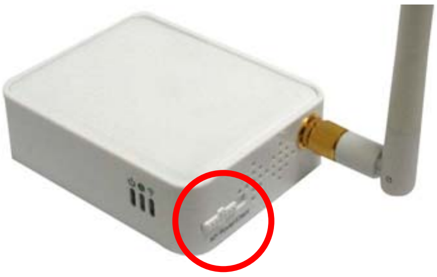
CHAPTER 2: ABOUT THE OPERATION MODES

This device provides three operational applications with Access Point, Gateway, and Client (Infrastructure) modes, which are mutually exclusive.

This device is shipped with configuration that is functional right out of the box. If you want to change the settings in order to perform more advanced configuration or even change the mode of operation, you can manually switch to the mode you desire by the manufacturer as described in the following sections.

Operation Modes

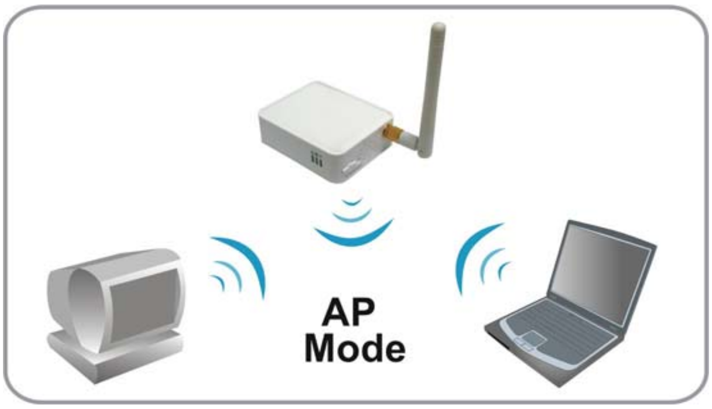
You have to MANUALLY switch the bar into the mode you preferred, AP, Router or Client mode, then the device will reboot automatically into the mode you have selected.



After the device rebooting, you can go to check the operation mode on your PC or notebook and click **Setup** button to enter the mode configuration page.

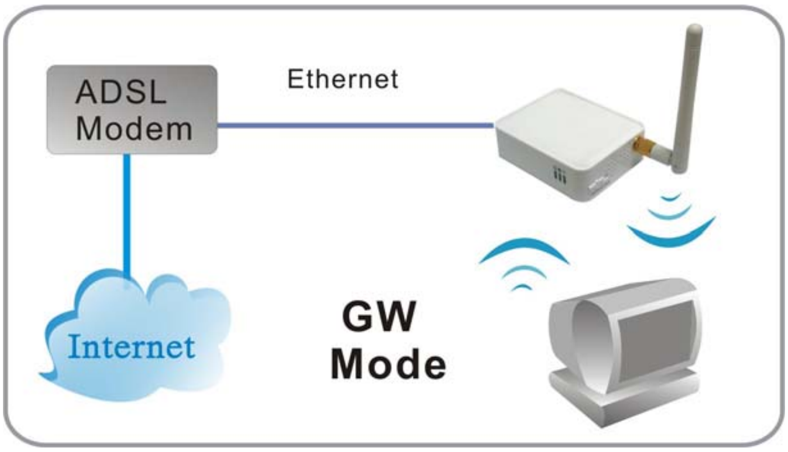
Access Point Mode

When acting as an access point, this device connects all the stations (PC/notebook with wireless network adapter) to a wireless network. All stations can have the Internet access if only the Access Point has the Internet connection.



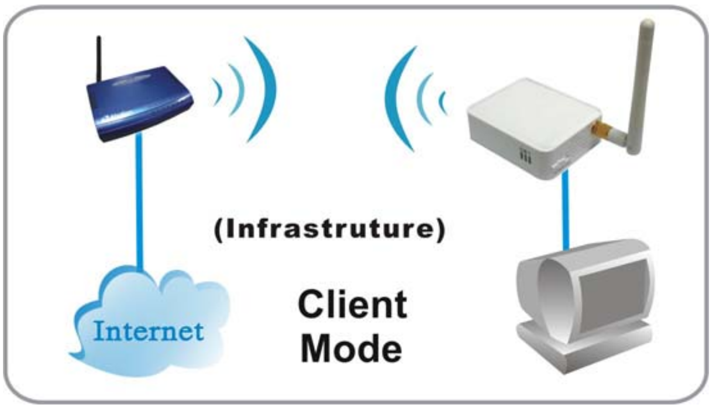
Gateway Mode

When Gateway mode is selected, the AP will enter the gateway mode. And the wireless connection will be set up from a point-to-point local LAN into a point-to-multipoint WAN.



Client Mode (Infrastructure)

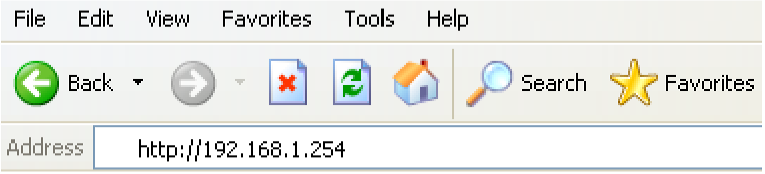
If set to Client (Infrastructure) mode, this device can work like a wireless station when it’s connected to a computer so that the computer can send packets from wired end to wireless interface.


(Infrastruture)
Internet
Client
Mode

CHAPTER 3: CONFIGURATION

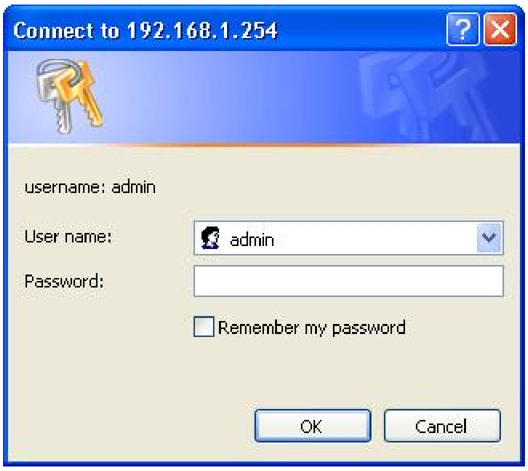
Login

1. Start your computer, then connect an Ethernet cable between your computer and the Wireless Portable Router.
2. Make sure your wired station is set to the same subnet as the Wireless Portable Router, i.e. 192.168.1.123.
3. Start your WEB browser. In the *Address* box, enter the following: http://192.168.1.254



Address: http://192.168.1.254

4. After connected successfully, the following screen will show up. No password is required by default, simply enter the username "**admin**", which is fixed and cannot be changed.



username: admin

User name: admin

Password:

□ Remember my password

The configuration menu is divided into four categories: **Mode, Status, TCP/IP,** and **Other** settings. Click on the desired setup item to expand the page in the main navigation page. The setup pages covered in this utility are described below.

Common Connection Types

Cable Modems

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	Usually, none. However, some ISP's may require you to use a particular Hostname, Domain name, or MAC (physical) address.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you. Some ISP's may also require you to use a particular Hostname, Domain name, or MAC (physical) address.

DSL Modems

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	None.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you.
PPPoE	You connect to the ISP only when required. The IP address is usually allocated automatically.	User name and password.

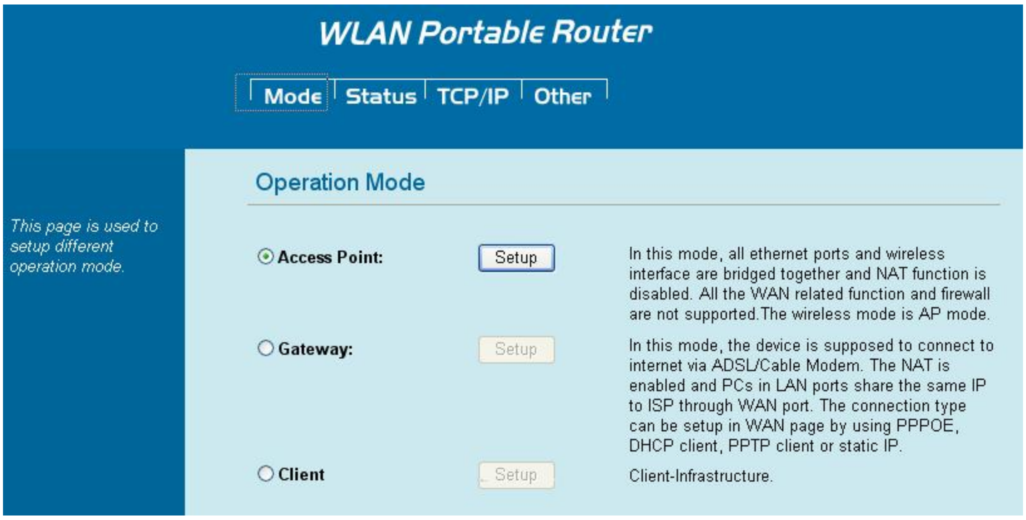
PPTP	Mainly used in Europe. You connect to the ISP only when required. The IP address is usually allocated automatically, but may be Static (Fixed).	- PPTP Server IP Address. - User name and password. - IP Address allocated to you, if Static (Fixed).

Other Modems (e.g. Broadband Wireless)

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	None.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you.

Configuration via Web

You have to MANUALLY switch the bar into the mode you preferred, AP, Router or Client mode, then the device will reboot automatically into the mode you have selected.
After the device rebooting, you can go to check the operation mode on your PC or notebook and click **Setup** button to enter the mode configuration page.



This page is used to setup different operation mode.

Operation Mode

● **Access Point:** Setup
In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.The wireless mode is AP mode.

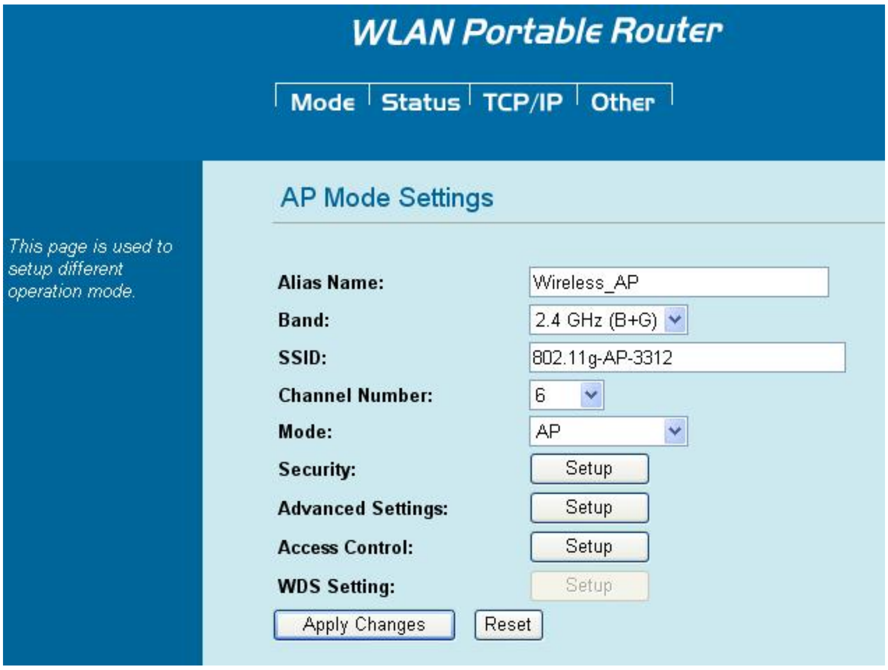
○ **Gateway:** Setup
In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

○ **Client** Setup
Client-Infrastructure.

Operation Modes

Access Point	In this mode, all Ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported. The wireless mode is AP mode.
Gateway	In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPoE, DHCP client, PPTP client or static IP.
Client	If set to Client (Infrastructure) mode, this device can work like a wireless station when it’s connected to a computer so that the computer can send packets from wired end to wireless interface.

Access Point Mode

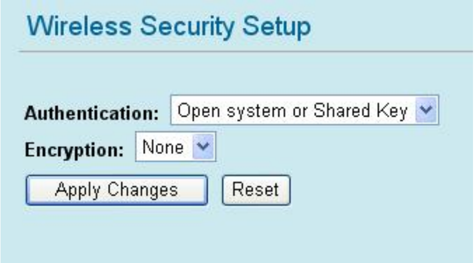


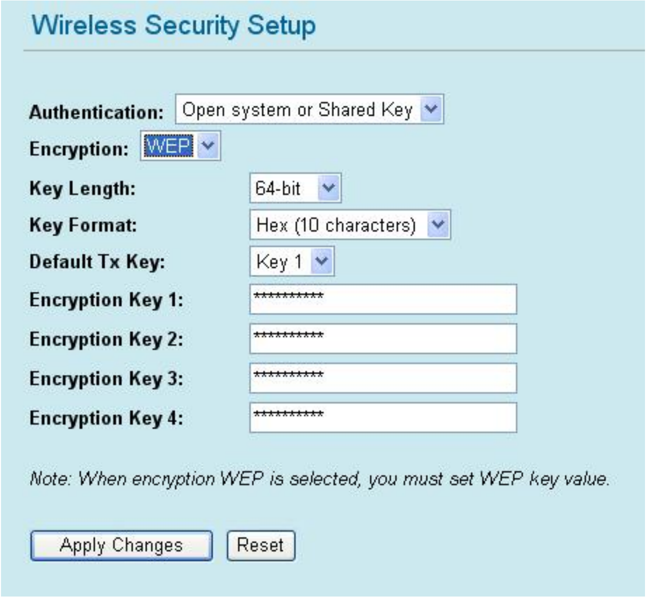
This page is used to setup different operation mode.

AP Mode Settings

Alias Name: Wireless_AP
Band: 2.4 GHz (B+G)
SSID: 802.11g-AP-3312
Channel Number: 6
Mode: AP
Security:
Advanced Settings:
Access Control:
WDS Setting:

AP Mode Settings	
Alias Name	The name of this device. You can assign a name for this router to distinguish form other APs.
Band	You can choose one mode of the following you need. ⦿ 2.4GHz (B): 802.11b supported rate only. ⦿ 2.4GHz (G): 802.11g supported rate only. ⦿ 2.4GHz (B+G): 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz (B+G) mode.
SSID	The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific

	WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. A SSID is also referred to as a network name because essentially it is a name that identifies a wireless network.
Channel Number	Allow user to set the channel manually or automatically. If set channel manually, just select the channel 1~11 you want to specify. If "Auto" is selected, user can set the channel range to have the Wireless Portable Router automatically survey and choose the channel with best situation for communication. The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel. Default setting is **Auto**.
Mode	Select the mode form the pull-down list including **AP** and **WDS Repeater**.
Security	Click the **Setup** button the **Wireless Security Setup** page will pop up.  Wireless Security Setup Authentication: Open system or Shared Key Encryption: None **Authentication**: Select an authentication from the pull-down list including **Open system or Shared Key, Open System, Open System with 802.1x, Shared Key, WPA-RADIUS, WPA-PSK, WPA2-RADIUS** and **WPA2-PSK**. **Encryption**: For **Open system or Shared Key** and **Open System** authentication modes, the selection of encryption type are **None** and **WEP**. For **Open System with 802.1x** and **Shared Key** authentication modes, the selection of encryption type is **WEP**. For **WPA-RADIUS, WPA-PSK**, **WPA2-RADIUS** and **WPA2-PSK** authentication mode, the encryption type supports both **TKIP** and **AES**.



Wireless Security Setup

Authentication: Open system or Shared Key

Encryption: WEP

Key Length: 64-bit

Key Format: Hex (10 characters)

Default Tx Key: Key 1

Encryption Key 1: **********

Encryption Key 2: **********

Encryption Key 3: **********

Encryption Key 4: **********

Note: When encryption WEP is selected, you must set WEP key value.

Open system: When this authentication is enabled, there is no need to enter password when making a connection.

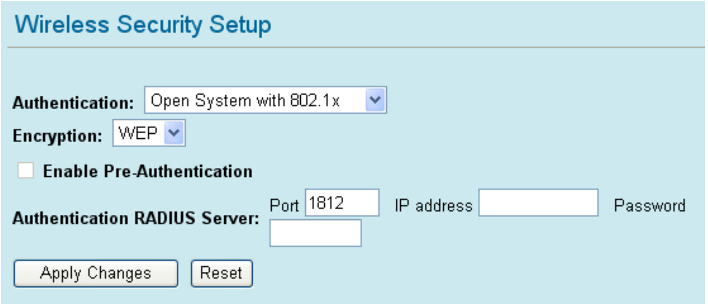
Shared Key: The client or station must use the same encryption and enter the same password when make a connection with the wireless router.

Key Length/ Key Format: Only valid when using **WEP** encryption algorithm. There are several formats to enter the keys.

- **Hexadecimal (64 bits)**: 10 Hex characters.
- **Hexadecimal (128 bits)**: 26 Hex characters.
- **ASCII (64 bits)**: 5 ASCII characters.
- **ASCII (128 bits)**: 13 ASCII characters.

Default Tx Key: There are four keys 1~4 that you can select at will. All computers, access points, and wireless adapters must use the same key when making a connection.

Encryption Key 1~4: Enter the password in the encryption key field that the encryption key number must match the selected Tx key.



Wireless Security Setup

Authentication: Open System with 802.1x

Encryption: WEP

□ Enable Pre-Authentication

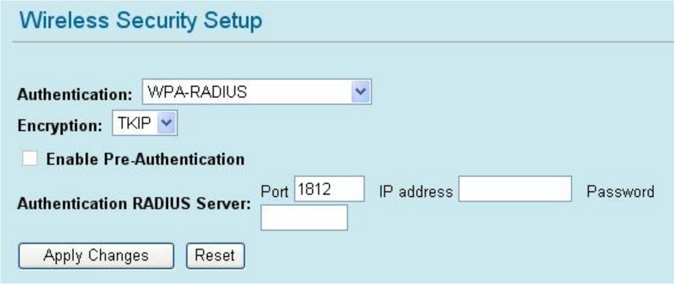
Authentication RADIUS Server: Port 1812 IP address Password

Enable Pre-Authentication: This function only valid under

WPA2-RADIUS authentication. The two most important features beyond WPA to become standardized through 802.11i/ WPA2 are: pre-authentication, which enables secure fast roaming without noticeable signal latency. Pre-authentication provides a way to establish a PMK security association before a client associates. The advantage is that the client reduces the time that it's disconnected to the network.

Authentication RADIUS Server: RADIUS (Remote Authentication Dial-In User Service) is an authentication, authorization and accounting client-server protocol. The client is a Network Access Server that desires to authenticate its links. The server is a server that has access to a user database with authentication information.
Port: Enter the RADIUS Server's port number provided by your ISP. The default is 1812.
IP address: Enter the RADIUS Server's IP Address provided by your ISP.

Password: Enter the password that the AP shares with the RADIUS Server.



Wireless Security Setup

Authentication: WPA-RADIUS

Encryption: TKIP

□ Enable Pre-Authentication

Authentication RADIUS Server: Port 1812 IP address Password

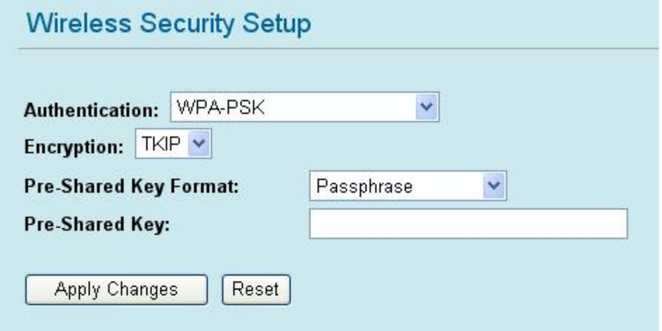
WPA (Wi-Fi Protected Access): It is designed to improve WEP security and provides stronger data protection and network access control than WEP. Most wireless networks should use either WEP or WPA security.

WPA-RADIUS/ WPA2-RADIUS: WPA- RADIUS mode (802.1x or WPA-Enterprise). This mode is more difficult to configure, the 802.1x RADIUS servers and an Extensible Authentication Protocol (EAP) are used for authentication. The enhanced WPA2 uses Advanced Encryption Standard (AES) instead of Temporal Key Integrity Protocol (TKIP) to provide stronger encryption mechanism.

Enable Pre-Authentication: This function only valid under WPA2-RADIUS authentication. The two most important features beyond WPA to become standardized through 802.11i/ WPA2 are: pre-authentication, which enables secure fast roaming without noticeable signal latency. Pre-authentication provides a way to establish a PMK security association before a client associates. The advantage is that the client reduces the time that it's disconnected to the network.

Authentication RADIUS Server: RADIUS (Remote Authentication Dial-In User Service) is an authentication, authorization and accounting client-server protocol. The client is a Network Access Server that desires to authenticate its links. The server is a server that has access to a user database with authentication information.
Port: Enter the RADIUS Server's port number provided by your ISP. The default is 1812.
IP address: Enter the RADIUS Server's IP Address provided by your ISP.

Password: Enter the password that the AP shares with the RADIUS Server.



Wireless Security Setup

Authentication: WPA-PSK

Encryption: TKIP

Pre-Shared Key Format: Passphrase

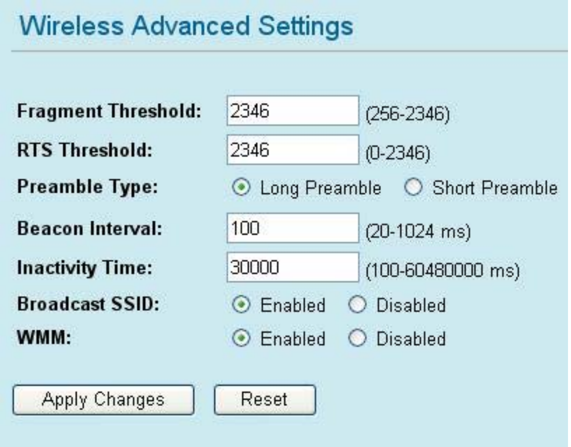
Pre-Shared Key:

WPA-PSK/ WPA2-PSK: WPA-PSK is easier to configure than WEP. All computers, access points, and wireless adapters must use the same type of security when making a connection. WPA-PSK mode (Pre-Shared Key or WPA-Personal). In this mode, a pre-shared key or passphrase is used for authentication. The enhanced WPA2 uses Advanced Encryption Standard (AES) instead of Temporal Key Integrity Protocol (TKIP) to provide stronger encryption mechanism.

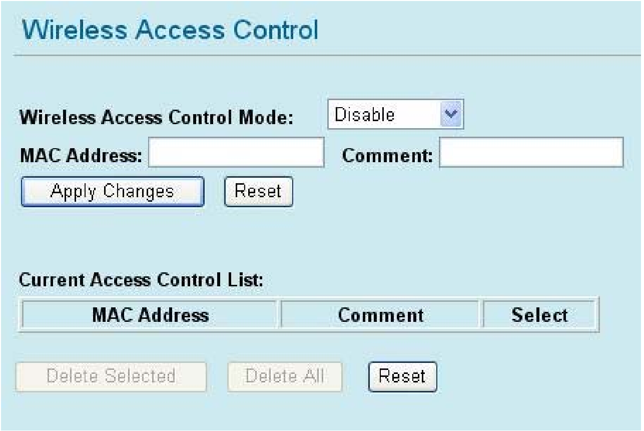
Pre-Shared Key Format: There are two formats for choice to set the Pre-shared key select the format form the pull-down list, **Passphrase** and **Hex (64 characters)**. If Hex is selected, users will have to enter a 64 characters string. For easier configuration, the Passphrase (at least 8 than 63 characters) format is recommended.

Pre-Shared Key: This is the shared secret password between computers, access points, and wireless adapters. Only for **WPA-PSK** and **WPA2-PSK** authentication modes, this field must be filled with character longer than 8 and less than 63 characters, in which the 802.1x Authentication will be activated. Make sure the same password is used on all computers, access points, and wireless adapters.

Apply Changes: Click this button to save and apply the current

	settings. **Reset**: Click to clear and reset the current settings.
Advanced Settings	Click the **Setup** button to enter the **Wireless Advanced Settings** page.  Wireless Advanced Settings Fragment Threshold: 2346 (256-2346) RTS Threshold: 2346 (0-2346) Preamble Type: ● Long Preamble ○ Short Preamble Beacon Interval: 100 (20-1024 ms) Inactivity Time: 30000 (100-60480000 ms) Broadcast SSID: ● Enabled ○ Disabled WMM: ● Enabled ○ Disabled **Fragment Threshold**: Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. If your wireless card often transmits large files in wireless network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346. The default value is 2346. **RTS Threshold**: RTS Threshold is a mechanism implemented to prevent the “Hidden Node” problem. “Hidden Node” is a situation in which two stations are within range of the same Access Point, but are not within range of each other. Therefore, they are hidden nodes for each other. When a station starts data transmission with the Access Point, it might not notice that the other station is already using the wireless medium. When these two stations send data at the same time, they might collide when arriving simultaneously at the Access Point. The collision will most certainly result in a loss of messages for both stations. Thus, the RTS Threshold mechanism provides a solution to prevent data collisions. When you enable RTS Threshold on a suspect “hidden station”, this station and its Access Point will use a Request to Send (RTS). The station will send an RTS to the Access Point, informing that it is going to transmit the data. Upon receipt, the Access Point will respond with a CTS message to all station within its range to notify all other stations to defer transmission. It will also confirm the requestor station that the Access Point has reserved it for the time frame of the requested transmission. If the “Hidden Node” problem is an issue, please specify the packet size. The RTS mechanism will be activated if the data size exceeds the value you set. The value can be set from 0 to 2346. This value should remain at its default setting of 2346. Should

	you encounter inconsistent data flow, only minor modifications of this value are recommended. ***Warning: Enabling RTS Threshold will cause redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.*** **Preamble Type**: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. If you want to change the Preamble type into Long or Short, please select the mode you need. **Beacon Interval**: Beacon Interval is the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point). The default setting is 100 minutes. **Inactivity Time:** By default, the unit adaptively selects the highest possible rate for transmission. For most networks the default setting is 30000 that is the best choice. If obstacles or interference are present, the system will automatically fall back to a lower rate. **Broadcast SSID**: • **Enabled**: This wireless AP will broadcast its SSID to stations. • **Disabled**: This wireless AP will NOT broadcast its SSID to stations. If stations want to connect to this wireless AP, this AP's SSID should be known in advance to make a connection. **WMM**: Wi-Fi Multi-Media function that is meant to improve audio, video and voice applications transmitted over Wi-Fi. Select **Enabled** or **Disabled** to execute WMM function. **Apply Changes**: Click to save and apply the current setting. **Reset**: Click to clear and reset the current settings.
Access Control	Click the **Setup** button to enter the **Wireless Access Control** page.

<table>
<tr>
<td></td>
<td>


Wireless Access Control

Wireless Access Control Mode: Disable

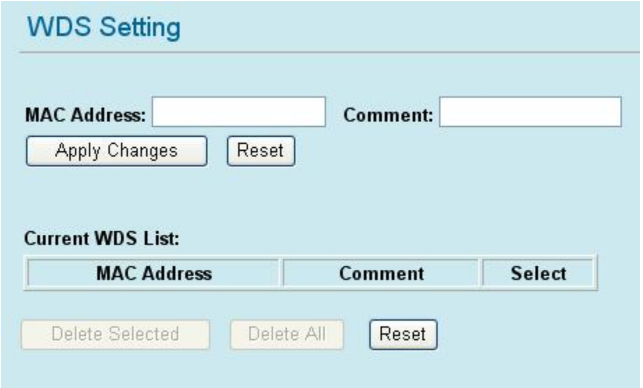
MAC Address:

Comment:

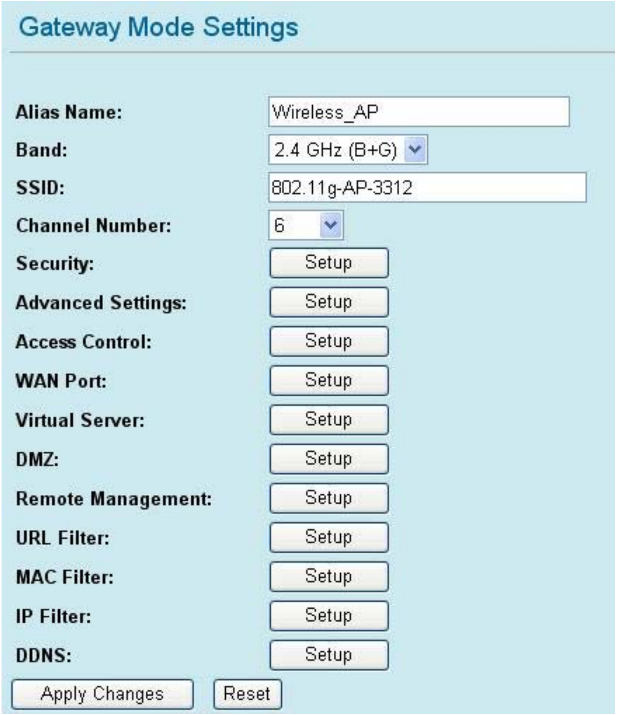
<b>Wireless Access Control Mode</b>: Select the Access Control Mode from the pull-down menu.

- <b>Disable</b>: Select to disable Wireless Access Control Mode.
- <b>Allow Listed</b>: Only the stations shown in the table can associate with the AP.
- <b>Deny Listed</b>: Stations shown in the table won’t be able to associate with the AP.

<b>MAC Address</b>: Enter the MAC address of a station that is allowed to access this Access Point.
<b>Comment</b>: You may enter up to 20 characters as a remark to the previous MAC address.
<b>Apply Changes</b>: Press to save the new settings on the screen.
<b>Reset</b>: Press to discard the data you have entered since last time you press Apply Changes.
<b>Current Access Control List</b>: This table displays you the AP MAC information.
<b>Delete Selected</b>: To delete clients from access to this Access Point, you may firstly check the select checkbox next to the MAC address and Comment, and press <b>Delete Selected</b> button.
<b>Delete All</b>: To delete all the clients from access to this Access Point just press <b>Delete All</b> button without selecting the checkbox.
<b>Reset</b>: If you have made any selection, press Reset will clear all the select mark.
</td>
</tr>
<tr>
<td><b>WDS Setting</b></td>
<td>If you select the mode into <b>WDS Repeater</b> mode, then you can access the <b>WDS Setting</b> setup.</td>
</tr>
</table>

	 WDS Setting MAC Address: Comment: Apply Changes Reset Current WDS List: MAC Address Comment Select Delete Selected Delete All Reset **MAC Address**: Enter the AP MAC address in this column; the maximum input is 12 digits. **Comment**: Enter a comment or description for the AP MAC address. **Apply Changes**: Click to add a new MAC address in the below Current WDS List. **Reset**: Click to clear previous settings. **Current WDS List:** This table displays you the AP MAC information. **Delete Selected**: To delete clients from access to this Access Point, you may firstly check the Select checkbox next to the MAC address and Comments, and press Delete Selected. **Delete All**: To delete all the clients from access to this Access Point just press Delete All. **Reset**: If you have made any selection, press **Reset** button will clear all the select mark.
Apply Changes	Click the **Apply Changes** button to save the current settings.
Reset	Click the **Reset** button to reset this page.

Gateway Mode



Gateway Mode Settings

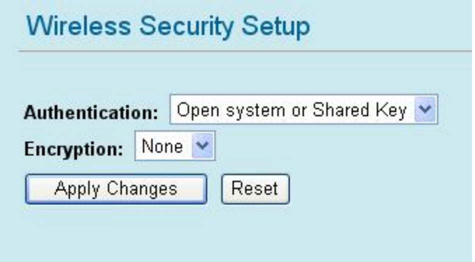
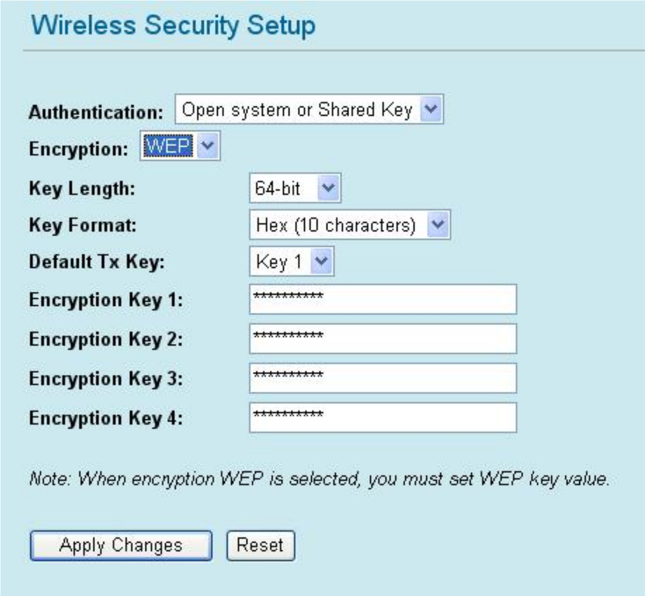
Alias Name: Wireless_AP

Band: 2.4 GHz (B+G)

SSID: 802.11g-AP-3312

Channel Number: 6

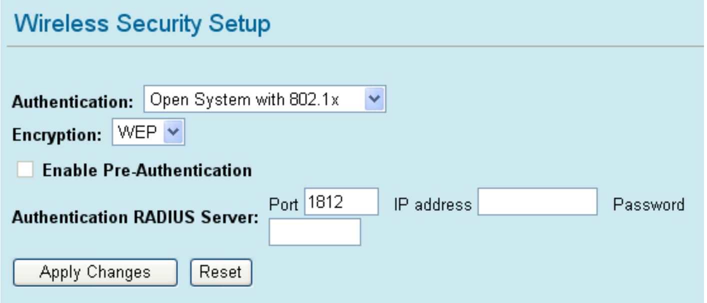
Gateway Mode Settings	
Alias Name	Display the name of this device.
Band	You can choose one mode of the following you need. ⦿ 2.4GHz (B): 802.11b supported rate only. ⦿ 2.4GHz (G): 802.11g supported rate only. ⦿ 2.4GHz (B+G): 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz (B+G) mode.
SSID	The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. A SSID is also referred to as a network name because essentially it is a name that identifies a wireless network.
Channel Number	Allow user to set the channel manually or automatically. If set channel manually, just select the channel you want to specify. If "Auto" is selected, user can set the channel range to have the Wireless Portable Router automatically survey and choose the channel with best situation for communication. The number of channels supported depends on the region of this Portable Router. All stations communicating with the Portable Router must use the same channel.

Security	Click **Setup** button to enter the **Wireless Security Setup** page.  Wireless Security Setup Authentication: Open system or Shared Key Encryption: None **Authentication**: Select an authentication from the pull-down list including **Open system or Shared Key, Open System, Open System with 802.1x, Shared Key, WPA-RADIUS, WPA-PSK, WPA2-RADIUS** and **WPA2-PSK**. **Encryption**: For **Open system or Shared Key** and **Open System** authentication modes, the selection of encryption type are **None** and **WEP**. For **Open System with 802.1x** and **Shared Key** authentication modes, the selection of encryption type is **WEP**. For **WPA-RADIUS, WPA-PSK**, **WPA2-RADIUS** and **WPA2-PSK** authentication mode, the encryption type supports both **TKIP** and **AES**.  Wireless Security Setup Authentication: Open system or Shared Key Encryption: WEP Key Length: 64-bit Key Format: Hex (10 characters) Default Tx Key: Key 1 Encryption Key 1: ********** Encryption Key 2: ********** Encryption Key 3: ********** Encryption Key 4: ********** Note: When encryption WEP is selected, you must set WEP key value. **Open system:** When this authentication is enabled, there is no need to enter password when making a connection. **Shared Key**: The client or station must use the same encryption and enter the same password when make a connection with the wireless router. **Key Length/ Key Format**: Only valid when using WEP encryption algorithm. There are several formats to enter the keys. • **Hexadecimal (64 bits):** 10 Hex characters. • **Hexadecimal (128 bits)**: 26 Hex characters.

- **ASCII (64 bits):** 5 ASCII characters.
- **ASCII (128 bits):** 13 ASCII characters.

Default Tx Key: There are four keys 1~4 that you can select at will. All computers, access points, and wireless adapters must use the same key when making a connection.

Encryption Key 1~4: Enter the password in the encryption key field that the encryption key number must match the selected Tx key.



Wireless Security Setup

Authentication: Open System with 802.1x

Encryption: WEP

□ Enable Pre-Authentication

Authentication RADIUS Server: Port 1812 IP address Password

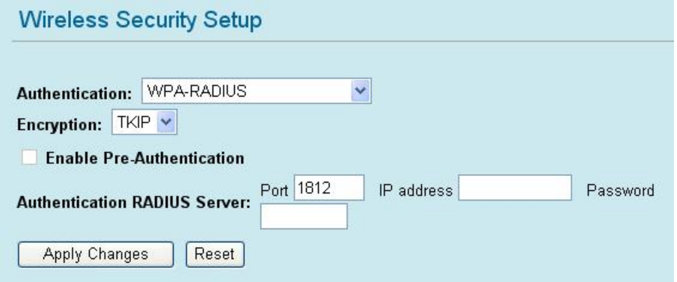
Enable Pre-Authentication: This function only valid under WPA2-RADIUS authentication. The two most important features beyond WPA to become standardized through 802.11i/ WPA2 are: pre-authentication, which enables secure fast roaming without noticeable signal latency. Pre-authentication provides a way to establish a PMK security association before a client associates. The advantage is that the client reduces the time that it's disconnected to the network.

Authentication RADIUS Server: RADIUS (Remote Authentication Dial-In User Service) is an authentication, authorization and accounting client-server protocol. The client is a Network Access Server that desires to authenticate its links. The server is a server that has access to a user database with authentication information.

Port: Enter the RADIUS Server's port number provided by your ISP. The default is 1812.

IP address: Enter the RADIUS Server's IP Address provided by your ISP.

Password: Enter the password that the AP shares with the RADIUS Server.



Wireless Security Setup

Authentication: WPA-RADIUS

Encryption: TKIP

□ Enable Pre-Authentication

Authentication RADIUS Server: Port 1812 IP address Password

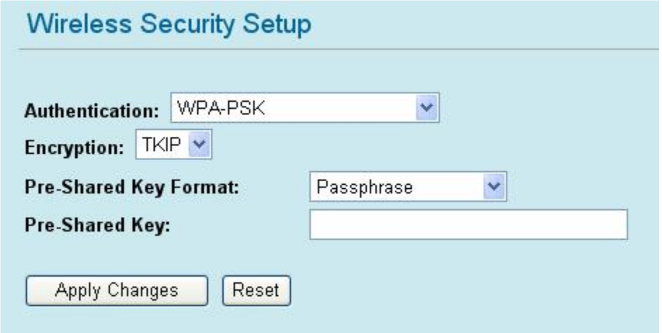
WPA (Wi-Fi Protected Access): It is designed to improve WEP security and provides stronger data protection and network access control than WEP. Most wireless networks should use either WEP or WPA security.

WPA-RADIUS/ WPA2-RADIUS: WPA- RADIUS mode (802.1x or WPA-Enterprise). This mode is more difficult to configure, the 802.1x RADIUS servers and an Extensible Authentication Protocol (EAP) are used for authentication. The enhanced WPA2 uses Advanced Encryption Standard (AES) instead of Temporal Key Integrity Protocol (TKIP) to provide stronger encryption mechanism.

Enable Pre-Authentication: This function only valid under WPA2-RADIUS authentication. The two most important features beyond WPA to become standardized through 802.11i/ WPA2 are: pre-authentication, which enables secure fast roaming without noticeable signal latency. Pre-authentication provides a way to establish a PMK security association before a client associates. The advantage is that the client reduces the time that it's disconnected to the network.

Authentication RADIUS Server: RADIUS (Remote Authentication Dial-In User Service) is an authentication, authorization and accounting client-server protocol. The client is a Network Access Server that desires to authenticate its links. The server is a server that has access to a user database with authentication information.
Port: Enter the RADIUS Server's port number provided by your ISP. The default is 1812.
IP address: Enter the RADIUS Server's IP Address provided by your ISP.

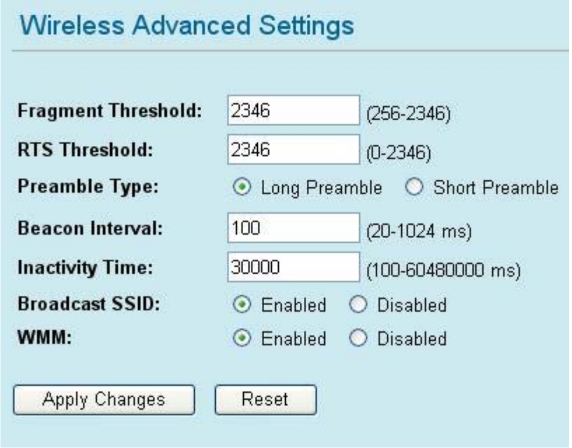
Password: Enter the password that the AP shares with the RADIUS Server.



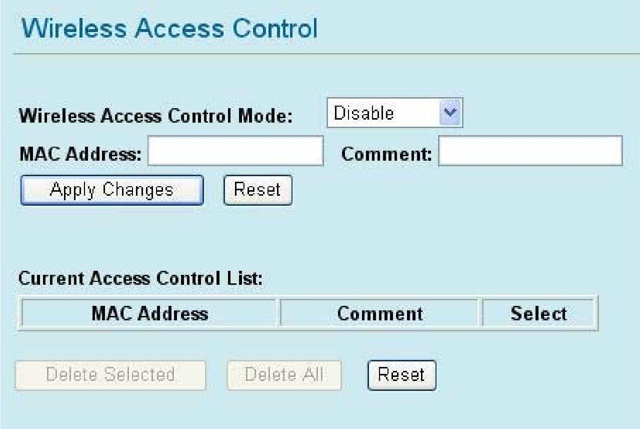
Wireless Security Setup

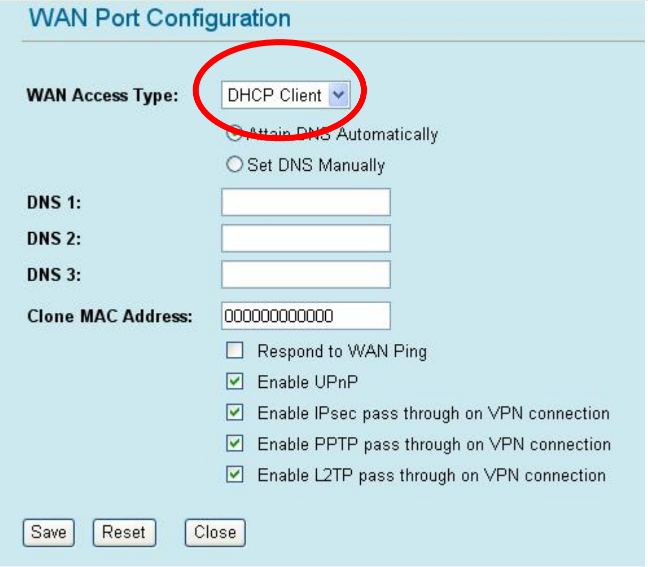
Authentication: WPA-PSK
Encryption: TKIP
Pre-Shared Key Format: Passphrase
Pre-Shared Key:

WPA-PSK/ WPA2-PSK: WPA-PSK is easier to configure than WEP. All computers, access points, and wireless adapters must use the same type of security when making a connection. **WPA-PSK** mode (Pre-Shared Key or WPA-Personal). In this mode, a pre-shared key or passphrase is used for authentication. The enhanced WPA2 uses **AES** (Advanced Encryption Standard) instead of **TKIP** (Temporal Key Integrity Protocol) to provide stronger encryption

	mechanism. **Pre-Shared Key Format**: There are two formats for choice to set the Pre-shared key select the format form the pull-down list, **Passphrase** and **Hex (64 characters)**. If Hex is selected, users will have to enter a 64 characters string. For easier configuration, the Passphrase (at least 8 than 63 characters) format is recommended. **Pre-Shared Key**: This is the shared secret password between computers, access points, and wireless adapters. Only for **WPA-PSK** and **WPA2-PSK** authentication modes, this field must be filled with character longer than 8 and less than 63 characters, in which the 802.1x Authentication will be activated. Make sure the same password is used on all computers, access points, and wireless adapters. **Apply Changes**: Click this button to save and apply the current settings. **Reset**: Click to clear and reset the current settings.
Advanced Settings	Click the **Setup** button to enter the **Wireless Advanced Settings** page.  Wireless Advanced Settings Fragment Threshold: 2346 (256-2346) RTS Threshold: 2346 (0-2346) Preamble Type: ● Long Preamble ○ Short Preamble Beacon Interval: 100 (20-1024 ms) Inactivity Time: 30000 (100-60480000 ms) Broadcast SSID: ● Enabled ○ Disabled WMM: ● Enabled ○ Disabled **Fragment Threshold**: Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. If your wireless card often transmits large files in wireless network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346. The default value is 2346. **RTS Threshold**: RTS Threshold is a mechanism implemented to prevent the “Hidden Node” problem. “Hidden Node” is a situation in which two stations are within range of the same Access Point, but are not within range of each other. Therefore, they are hidden nodes for each other. When a station starts data transmission with the Access Point, it might not notice that the other station is already using the wireless medium. When these two stations send data at the same time, they might collide when arriving simultaneously at the Access Point. The collision will most certainly result in a loss of messages for both

	stations. Thus, the RTS Threshold mechanism provides a solution to prevent data collisions. When you enable RTS Threshold on a suspect “hidden station”, this station and its Access Point will use a Request to Send (RTS). The station will send an RTS to the Access Point, informing that it is going to transmit the data. Upon receipt, the Access Point will respond with a CTS message to all station within its range to notify all other stations to defer transmission. It will also confirm the requestor station that the Access Point has reserved it for the time frame of the requested transmission. If the “Hidden Node” problem is an issue, please specify the packet size. The RTS mechanism will be activated if the data size exceeds the value you set. The value can be set from 0 to 2346. This value should remain at its default setting of 2346. Should you encounter inconsistent data flow, only minor modifications of this value are recommended. ***Warning: Enabling RTS Threshold will cause redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.*** **Preamble Type**: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. If you want to change the Preamble type into **Long** or **Short**, please select the mode you need. **Beacon Interval**: Beacon Interval is the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point). The default setting is 100 minutes. **Inactivity Time:** By default, the unit adaptively selects the highest possible rate for transmission. For most networks the default setting is 30000 that is the best choice. If obstacles or interference are present, the system will automatically fall back to a lower rate. **Broadcast SSID**: • **Enabled**: This wireless AP will broadcast its SSID to stations. • **Disabled**: This wireless AP will NOT broadcast its SSID to stations. If stations want to connect to this wireless AP, this AP’s SSID should be known in advance to make a connection. **WMM**: Wi-Fi Multi-Media function that is meant to improve audio, video and voice applications transmitted over Wi-Fi. Select **Enabled** or **Disabled** to execute WMM function. **Apply Changes**: Click to save and apply the current setting. **Reset**: Click to clear and reset the current settings.
Access Control	Click the **Setup** button to enter the **Wireless Access Control** page.

	 Wireless Access Control Wireless Access Control Mode: Disable MAC Address: Comment: Apply Changes Reset Current Access Control List: MAC Address | Comment | Select Delete Selected Delete All Reset **Wireless Access Control Mode**: Select the Access Control Mode from the pull-down menu. • **Disable**: Select to disable Wireless Access Control Mode. • **Allow Listed**: Only the stations shown in the table can associate with the AP. • **Deny Listed**: Stations shown in the table won’t be able to associate with the AP. **MAC Address**: Enter the MAC address of a station that is allowed to access this Access Point. **Comment**: You may enter up to 20 characters as a remark to the previous MAC address. **Apply Changes**: Press to save the new settings on the screen. **Reset**: Press to discard the data you have entered since last time you press Apply Changes. **Current Access Control List**: This table displays you the AP MAC information. **Delete Selected**: To delete clients from access to this Access Point, you may firstly check the select checkbox next to the MAC address and Comment, and press **Delete Selected** button. **Delete All**: To delete all the clients from access to this Access Point just press **Delete All** button without selecting the checkbox. **Reset**: If you have made any selection, press Reset will clear all the select mark.
WAN Port	Click **Setup** to enter the **WAN Port Configuration** screen.



WAN Port Configuration

WAN Access Type: DHCP Client

○ Attain DNS Automatically

○ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Respond to WAN Ping

☑ Enable UPnP

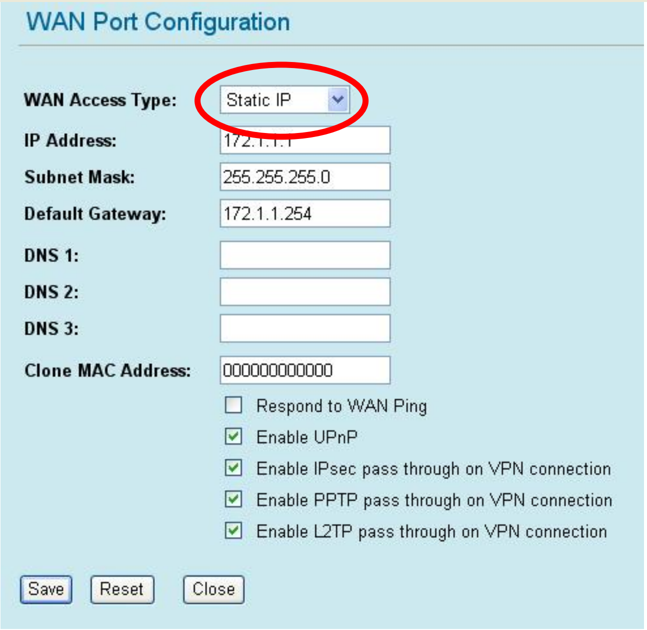
☑ Enable IPsec pass through on VPN connection

☑ Enable PPTP pass through on VPN connection

☑ Enable L2TP pass through on VPN connection

DHCP Client

WAN Access Type: Select the WAN access type (Static IP, DHCP, PPPoE and PPTP) from the pull-down menu.
Attain DNS Automatically: Select to attain DNS automatically.
Set DNS Manually: Select to set DNS manually.
DNS 1~3: Enter the DNS server IP address(es) provided by your ISP, or you can specify your own preferred DNS server IP address(es). DNS 1 and DNS 2 servers are optional. You can enter another DNS server's IP address as a backup. DNS 1 and DNS 2 servers will be used when the DNS 1 server failed.
Clone MAC Address: Enter the MAC address that you wish to clone.
Respond to WAN Ping: Click to allow pinging from WAN side.
Save: Click to save and apply the current settings.
Reset: Click to clear and reset the current settings.
Close: click to exit the current settings.



WAN Port Configuration

WAN Access Type: Static IP

IP Address: 172.1.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 172.1.1.254

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Respond to WAN Ping
☑ Enable UPnP
☑ Enable IPsec pass through on VPN connection
☑ Enable PPTP pass through on VPN connection
☑ Enable L2TP pass through on VPN connection

Static IP

IP Address: Enter the WAN IP address provided by your ISP in this column.

Subnet Mask: Enter the Subnet Mask in this column.

Default Gateway: Enter the default gateway IP provided by your ISP in this column.

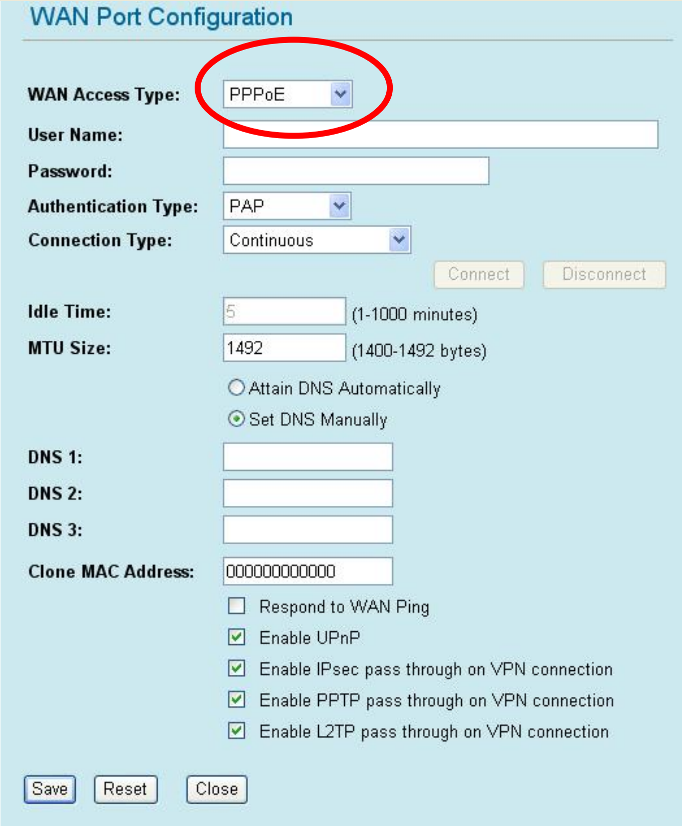
DNS 1~3: The DNS should be set to the address provided by your ISP.

Clone MAC Address: Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this Clone MAC address in this section to replace the WAN MAC address with the MAC address of that PC.

Save: Click to save and apply the current settings.

Reset: Click to clear and reset the current settings.

Close: click to exit the current settings.



WAN Port Configuration

WAN Access Type: PPPoE

User Name:

Password:

Authentication Type: PAP

Connection Type: Continuous

Idle Time: 5 (1-1000 minutes)

MTU Size: 1492 (1400-1492 bytes)

○ Attain DNS Automatically

● Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Respond to WAN Ping

☑ Enable UPnP

☑ Enable IPsec pass through on VPN connection

☑ Enable PPTP pass through on VPN connection

☑ Enable L2TP pass through on VPN connection

PPPoE

User Name: Input the **User Name** that provided by your ISP (case sensitive).

Password: Input the **Password** that provided by your ISP (case sensitive).

Authentication Type: Select **PAP, CHAP, MSCHAP-v1** or **MSCHAP-v2** form the pull-down menu.

Connection Type: Select the connection type **Continuous**, **Connect on Demand** or **Manual** from the pull-down menu. If you select **Manual** you can click **Connect** button to make a connection.

Idle Time: It represents that the device will idle after the minutes you set. The time must be set between 1~1000 minutes. Default value of idle time is 5 minutes. This function will be available when the **Connection Type** is selected to **Connect on Demand**.

MTU Size (Maximum Transmission Unit): MTU (Maximum Transmission Unit, namely the maximum packet size, the default value is 1492 for your application. Reducing the packet size can help connecting to certain web sites or speeding up packet transfer rate. If the incorrect selection is entered, you may not be able to open certain web sites.

Attain DNS Automatically: Select to attain DNS automatically.

Set DNS Manually: Select to enter DNS manually.

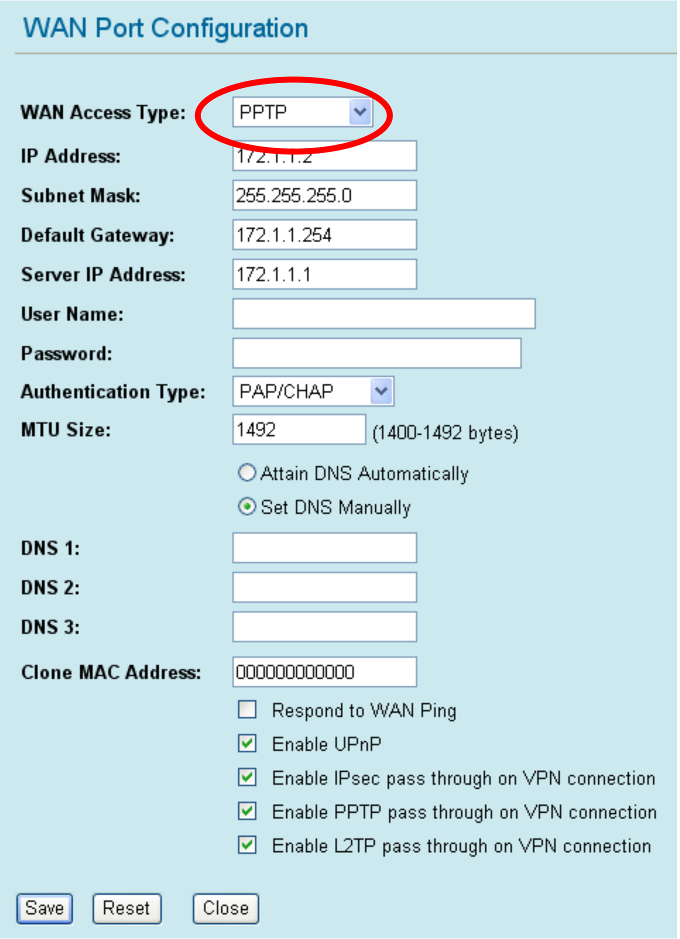
DNS 1~3: The DNS should be set to the address provided by your ISP.

Clone MAC Address: Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this Clone MAC address in this section to replace the WAN MAC address with the MAC address of that PC.

Save: Click to save and apply the current settings.

Reset: Click to clear and reset the current settings.

Close: click to exit the current settings.



WAN Port Configuration

WAN Access Type: PPTP

IP Address: 172.1.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 172.1.1.254

Server IP Address: 172.1.1.1

User Name:

Password:

Authentication Type: PAP/CHAP

MTU Size: 1492 (1400-1492 bytes)

○ Attain DNS Automatically

● Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Respond to WAN Ping

☑ Enable UPnP

☑ Enable IPsec pass through on VPN connection

☑ Enable PPTP pass through on VPN connection

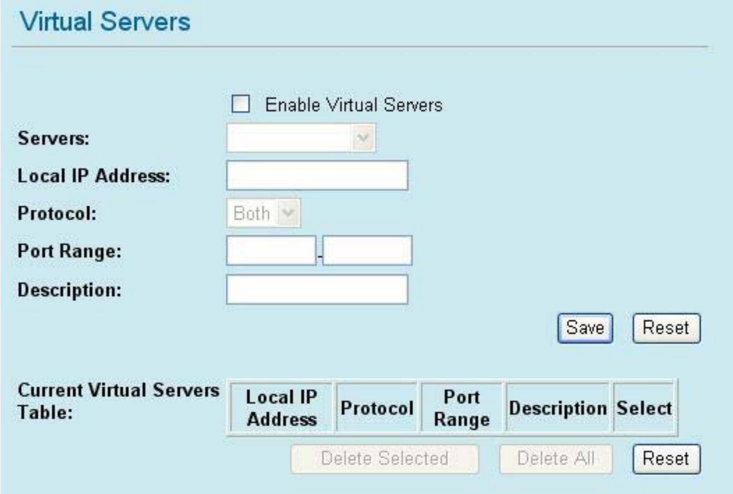
☑ Enable L2TP pass through on VPN connection

PPTP

IP Address: Enter the WAN IP address provided by your ISP in this column.

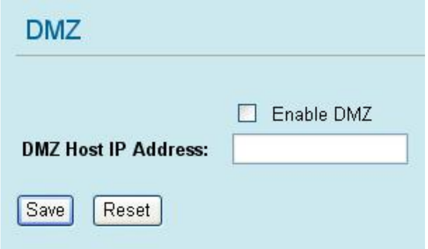
Subnet Mask: Enter the Subnet Mask in this column.

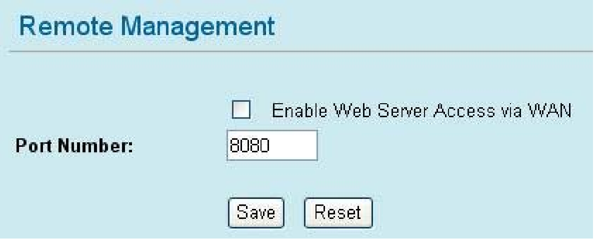
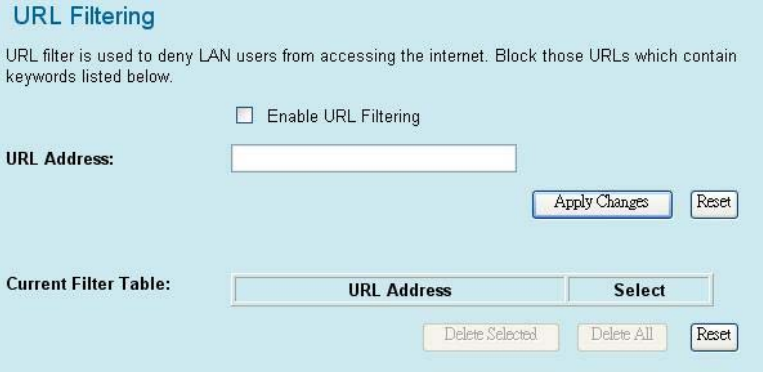
Default Gateway: Enter the default gateway IP provided by your ISP

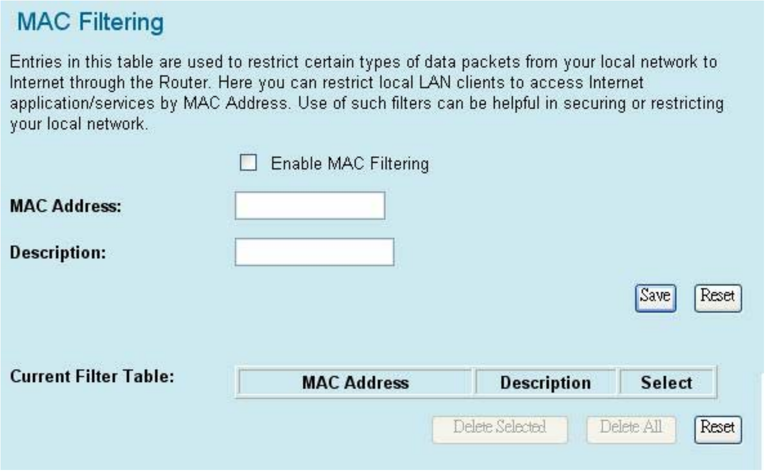
<table>
<tr><td></td><td>
in this column.
<b>Server IP address</b>: Enter the server IP address that provided by your ISP.
<b>User Name:</b> Input the <b>User Name</b> that provided by your ISP (case sensitive).
<b>Password:</b> Input the <b>Password</b> that provided by your ISP (case sensitive).
<b>Authentication Type:</b> Select <b>PAP/CHAP or MSCHAP-v1 /MSCHAP-v2</b> form the pull-down menu.
<b>MTU Size (Maximum Transmission Unit)</b>: MTU (Maximum Transmission Unit, namely the maximum packet size, the default value is 1492 for your application. Reducing the packet size can help connecting to certain web sites or speeding up packet transfer rate. If the incorrect selection is entered, you may not be able to open certain web sites.
<b>Attain DNS Automatically</b>: Select to attain DNS automatically.
<b>Set DNS Manually</b>: Select to enter DNS manually.
<b>DNS 1~3:</b> The DNS should be set to the address provided by your ISP.
<b>Clone MAC Address:</b> Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC’s MAC address that your ISP had originally connected your Internet connection to. Type in this Clone MAC address in this section to replace the WAN MAC address with the MAC address of that PC.
<b>Save</b>: Click to save and apply the current settings.
<b>Reset</b>: Click to clear and reset the current settings.
<b>Close</b>: click to exit the current settings.
</td></tr>
<tr><td><b>Virtual Server</b></td><td>
Click <b>Setup</b> to enter the <b>Virtual Servers</b> screen.

Virtual Servers
☐ Enable Virtual Servers
Servers:
Local IP Address:
Protocol: Both
Port Range: -
Description:

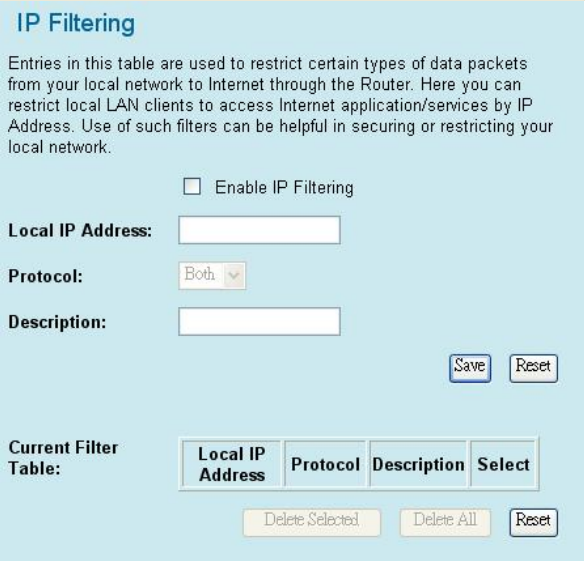
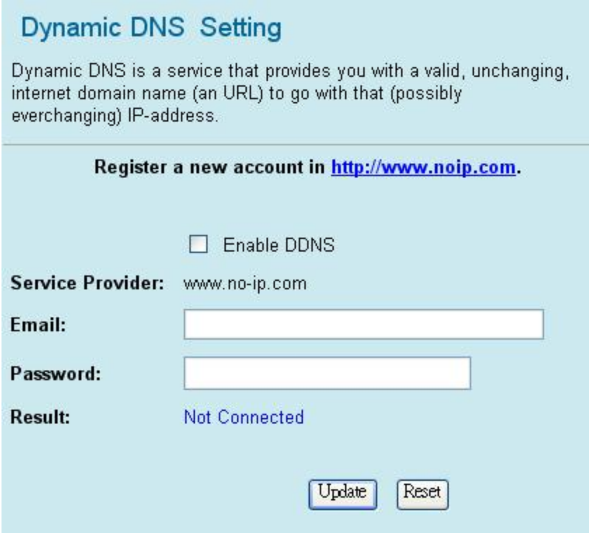
Current Virtual Servers Table:
<table>
<tr><th>Local IP Address</th><th>Protocol</th><th>Port Range</th><th>Description</th><th>Select</th></tr>
</table>

</td></tr>
</table>

	Enable Virtual Servers: Check to enable the virtual servers function. **Servers**: Select the server type (Web, FTP, E-Mail (POP3), E-Mail (SMTP), DNS and Telnet) from the pull-down menu. **Local IP Address**: Enter the local server's IP address. **Protocol:** Select the protocol (TCP, UDP or Both) used to the remote system or service. **Port Range:** For TCP and UDP Services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields. **Description:** You may key in a description for the local IP address. **Save:** Click to save and apply the current settings. **Reset:** Click to clear and reset the current settings. **Current Virtual Servers Table:** Shows the current virtual servers information. **Delete Selected:** To delete clients from access to this Router, you may firstly check the box next to Description column, and press **Delete Selected** button to erase. **Delete All:** To delete all the clients from access to this Router just press **Delete All** button without selecting. **Reset:** If you have made any selection, press **Reset** button will clear all the select mark.
DMZ	Click **Setup** to enter the **DMZ** screen.  DMZ □ Enable DMZ DMZ Host IP Address: **Enable DMZ**: If the DMZ Host Function is enabled, it means that you set up DMZ host at a particular computer to be exposed to the Internet so that some applications/software, especially Internet/online game can have two-way connections. **DMZ Host IP Address**: Enter the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/ Public IP address above. **Save:** Click to save the current settings. **Reset:** Click to resetore to the default values. ***Note: You need to give your LAN PC clients a fixed/ static IP***

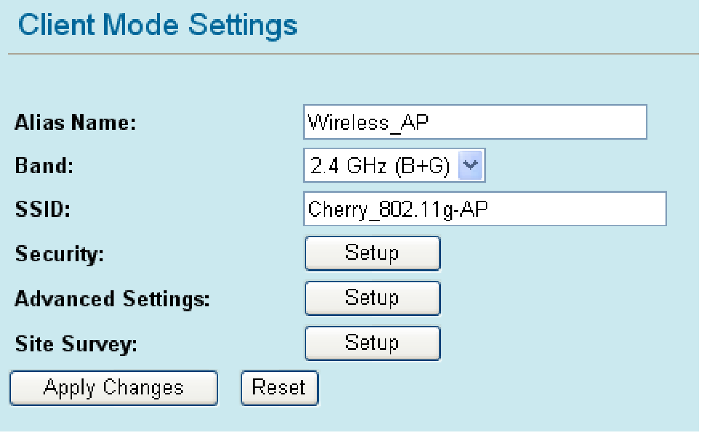
	address for DMZ to work properly.
Remote Management	Click **Setup** to enter the **Remote Management** screen.  Remote Management ☐ Enable Web Server Access via WAN Port Number: 8080 **Enable Web Server Access via WAN:** To permit remote access of the Router, from outside the local network, select to enable this function. Otherwise, keeps the default setting, Disabled. **Port Number:** Enter the port number that will be open to outside access. The default port number is 8080. **Save:** Click to save the current settings. **Reset:** Click to restore to the default values.
URL Filter	Click **Setup** to enter the **URL Filtering** screen.  URL Filtering URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below. ☐ Enable URL Filtering URL Address: Current Filter Table: URL Address | Select **Enable URL Filtering**: Check to enable the URL filtering function. **URL Address:** You can block websites with specific URL addresses. **Apply Changes:** Click to save the current settings. **Reset**: Click to clear the current settings. **Current Filter Table:** Shows the current URL address status. **Delete Selected**: Select the unwanted URL addresses and then click the **Delete Selected** button to eliminate them. **Delete All:** Click to delete all the URL addresses in the table. **Reset:** Click the **Reset** button to clear the current settings.

MAC Filter	Click **Setup** to enter the **MAC Filtering** screen.  MAC Filtering Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Router. Here you can restrict local LAN clients to access Internet application/services by MAC Address. Use of such filters can be helpful in securing or restricting your local network. ☐ Enable MAC Filtering MAC Address: Description: Save Reset Current Filter Table: MAC Address | Description | Select Delete Selected Delete All Reset **Enable MAC Filtering:** Click to enable the MAC filtering function. **MAC Address:** For MAC filtering enters the 12-digit MAC address in the appropriate MAC address field. **Description:** You may key in a description for the MAC address. **Save**: Click to save the current settings. **Reset:** Click to restore to the default values. **Current Filter Table:** Shows the current MAC address status. **Delete Selected:** Select the unwanted MAC addresses and then click the **Delete Selected** button to eliminate them. **Delete All:** Click to **Delete All** button to delete all the MAC addresses in the table. **Reset:** Click to clear the current settings.
IP Filter	Click **Setup** to enter the **IP Filtering** screen.

	 IP Filtering Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Router. Here you can restrict local LAN clients to access Internet application/services by IP Address. Use of such filters can be helpful in securing or restricting your local network. □ Enable IP Filtering Local IP Address: Protocol: Both Description: Save Reset Current Filter Table: Local IP Address | Protocol | Description | Select Delete Selected Delete All Reset **Enable IP Filtering:** Click to enable the IP filtering function. **Local IP Address:** For IP filtering enters the 15-digit IP address in the appropriate IP field. **Protocol**: Select the protocol (TCP, UDP or Both) used to the remote system or service. **Description:** You may key in a description for the IP address. **Save**: Click to save the current settings. **Reset:** Click to restore to the default values. **Current Filter Table:** Shows the current IP address status. **Delete Selected:** Select the unwanted IP addresses and then click the Delete Selected button to eliminate them. **Delete All:** Click to delete all the IP addresses in the table. **Reset:** Click to clear the current settings.
DDNS	Click **Setup** to enter the **Dynamic DNS Setting** screen.  Dynamic DNS Setting Dynamic DNS is a service that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address. Register a new account in http://www.noip.com. □ Enable DDNS Service Provider: www.no-ip.com Email: Password: Result: Not Connected Update Reset Dynamic DNS lets you update your current dynamic IP address with one or many dynamic DNS server so that anyone can contact you. If

	you do not have an account, please register a new account at http://www.noip.com. **Enable DDNS**: Check to enable the DDNS function. **Service Provider:** A company that provides access to the internet. www.no-ip.com **Email:** Enter your email that you registered in http://www.noip.com website. **Password:** Enter your passwords that you registered in http://www.noip.com website. Maximum input is 32 alphanumeric characters (case sensitive). **Result:** Shows the current result. **Update:** Click this button to update the information. **Reset:** Click to clear the current settings.
Apply Changes	Click to save the current settings.
Reset	Click to discard this page.

Client Mode



Client Mode Settings

Alias Name: Wireless_AP

Band: 2.4 GHz (B+G)

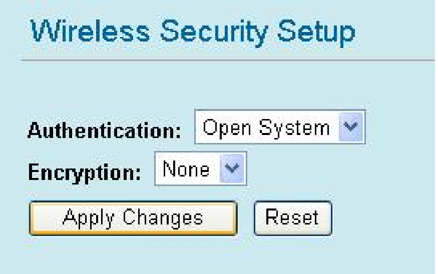
SSID: Cherry_802.11g-AP

Security: Setup

Advanced Settings: Setup

Site Survey: Setup

Client Mode Settings	
Alias Name	Display the name of this device.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz (B): 802.11b supported rate only. ⊙ 2.4GHz (G): 802.11g supported rate only. ⊙ 2.4GHz (B+G): 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz (B+G) mode.
SSID	The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. A SSID is also referred to as a network name because essentially it is a name that identifies a wireless network.
Security	Click **Setup** button to enter the **Wireless Security Setup** page.

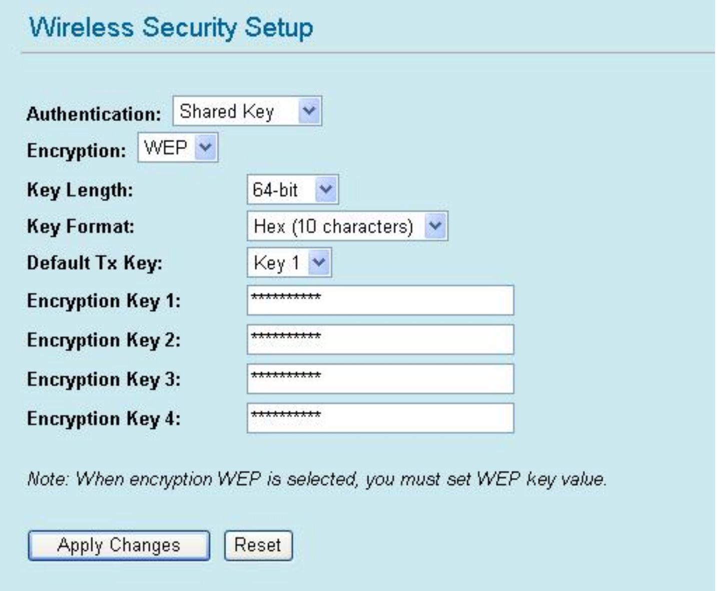

Wireless Security Setup

Authentication: Open System

Encryption: None

Authentication: Select an authentication from the pull-down list including **Open System, Shared Key, WPA-PSK** and **WPA2-PSK**.

Encryption: For **Open System** authentication mode, the selections of encryption type are **None** and **WEP**. For **Shared Key** authentication mode, the selection of encryption type is **WEP**. For **WPA-PSK**, and **WPA2-PSK** authentication modes, the encryption type supports **TKIP_AES**.


Wireless Security Setup

Authentication: Shared Key

Encryption: WEP

Key Length: 64-bit

Key Format: Hex (10 characters)

Default Tx Key: Key 1

Encryption Key 1: **********

Encryption Key 2: **********

Encryption Key 3: **********

Encryption Key 4: **********

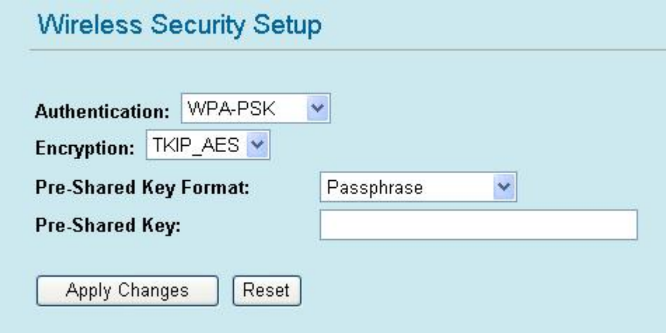
Note: When encryption WEP is selected, you must set WEP key value.

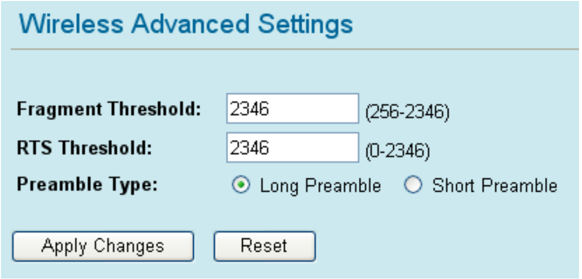
Open System: When this authentication is enabled, and the encryption default setting is **None**. There is no need to enter password when making a connection.

Shared Key: When this authentication is selected, the encryption is **WEP**. The client or station must use the same encryption and enter the same password when make a connection with the wireless router.

Key Length/ Key Format: Only valid when using **WEP** encryption algorithm. There are four formats to enter the keys.

- **Hexadecimal (64 bits)**: 10 Hex characters.
- **Hexadecimal (128 bits)**: 26 Hex characters.
- **ASCII (64 bits)**: 5 ASCII characters.
- **ASCII (128 bits)**: 13 ASCII characters.

	Default Tx Key: There are four keys 1~4 that you can select at will. All computers, access points, and wireless adapters must use the same key when making a connection. **Encryption Key 1~4**: Enter the password in the encryption key field that the encryption key number must match the selected Tx key.  Wireless Security Setup Authentication: WPA-PSK Encryption: TKIP_AES Pre-Shared Key Format: Passphrase Pre-Shared Key: **WPA (Wi-Fi Protected Access)**: It is designed to improve WEP security and provides stronger data protection and network access control than WEP. Most wireless networks should use either WEP or WPA security. **WPA-PSK/ WPA2-PSK:** WPA-PSK is easier to configure than WEP. All computers, access points, and wireless adapters must use the same type of security when making a connection. WPA-PSK mode (Pre-Shared Key or WPA-Personal). In this mode, a pre-shared key or passphrase is used for authentication. The enhanced WPA2 uses Advanced Encryption Standard (AES) instead of Temporal Key Integrity Protocol (TKIP) to provide stronger encryption mechanism. **Pre-Shared Key Format**: There are two formats for choice to set the Pre-shared key select the format form the pull-down list, **Passphrase** and **Hex (64 characters)**. If Hex is selected, users will have to enter a 64 characters string. For easier configuration, the Passphrase (at least 8 than 63 characters) format is recommended. **Pre-Shared Key**: This is the shared secret password between computers, access points, and wireless adapters. Only for **WPA-PSK** and **WPA2-PSK** authentication modes, this field must be filled with character longer than 8 and less than 63 characters, in which the 802.1x Authentication will be activated. Make sure the same password is used on all computers, access points, and wireless adapters. **Apply Changes**: Click this button to save and apply the current settings. **Reset**: Click to clear and reset the current settings.
Advanced Settings	Click **Setup** button to enter the **Wireless Advanced Settings** page.



Wireless Advanced Settings

Fragment Threshold: 2346 (256-2346)

RTS Threshold: 2346 (0-2346)

Preamble Type: ● Long Preamble ○ Short Preamble

Fragment Threshold: Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. If your 802.11g Wireless LAN PC Card often transmit large files in wireless network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346. The default value is 2346.

RTS Threshold: RTS Threshold is a mechanism implemented to prevent the “Hidden Node” problem. “Hidden Node” is a situation in which two stations are within range of the same Access Point, but are not within range of each other. Therefore, they are hidden nodes for each other. When a station starts data transmission with the Access Point, it might not notice that the other station is already using the wireless medium. When these two stations send data at the same time, they might collide when arriving simultaneously at the Access Point. The collision will most certainly result in a loss of messages for both stations.

Thus, the RTS Threshold mechanism provides a solution to prevent data collisions. When you enable RTS Threshold on a suspect “hidden station”, this station and its Access Point will use a Request to Send (RTS). The station will send an RTS to the Access Point, informing that it is going to transmit the data. Upon receipt, the Access Point will respond with a CTS message to all station within its range to notify all other stations to defer transmission. It will also confirm the requestor station that the Access Point has reserved it for the time-frame of the requested transmission.

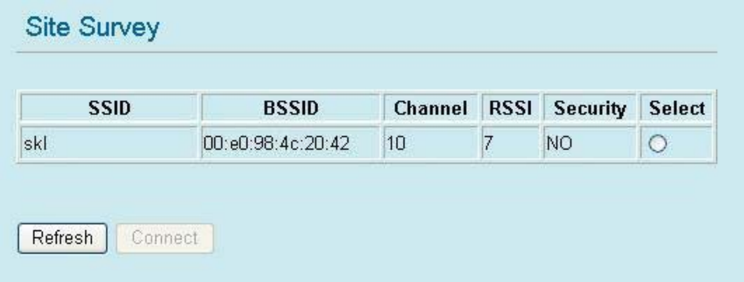
If the “Hidden Node” problem is an issue, please specify the packet size. *The RTS mechanism will be activated if the data size exceeds the value you set.* The default value is 2346.

Warning: *Enabling RTS Threshold will cause redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.*

This value should remain at its default setting of 2346. Should you encounter inconsistent data flow, only minor modifications of this value are recommended.

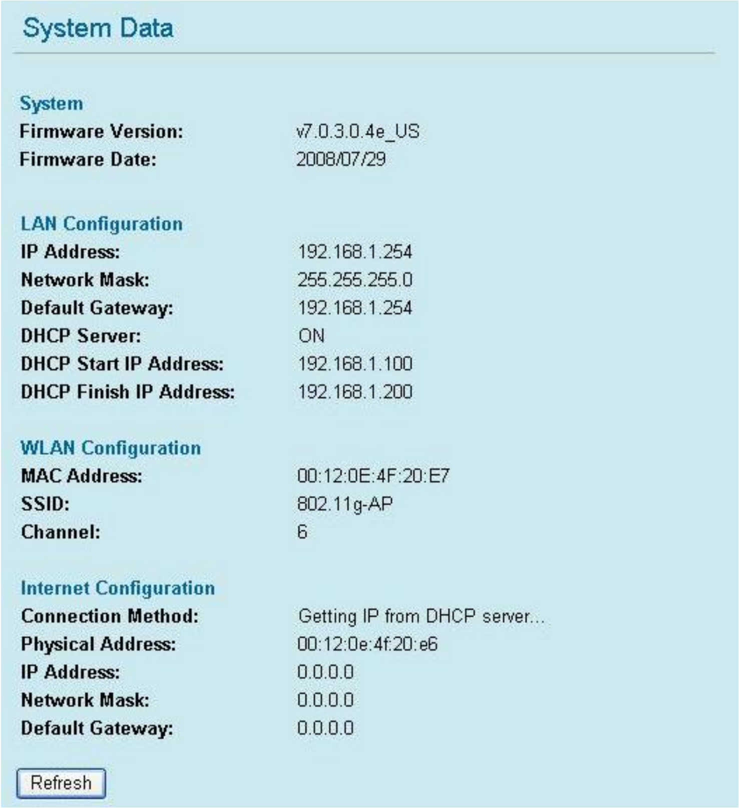
Preamble Type: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. If you want to change the Preamble type into **Long** or **Short**, please select the mode you need.

Apply Changes: Click to save and apply the current setting.

<table>
<tr><td></td><td><b>Reset</b>: Click to clear and reset the current settings.</td></tr>
<tr><td><b>Site Survey</b></td><td>Site survey displays all the active Access Points, SSID, BSSID, Channel, RSSI and Security in the neighborhood.

Site Survey
<table><tr><th>SSID</th><th>BSSID</th><th>Channel</th><th>RSSI</th><th>Security</th><th>Select</th></tr><tr><td>skl</td><td>00:e0:98:4c:20:42</td><td>10</td><td>7</td><td>NO</td><td>○</td></tr></table>
<b>Refresh</b>: Check this button to refresh all the Site Survey statistics.
<b>Connect</b>: Select a site that you would like to communicate, and then click the <b>Connect</b> button.</td></tr>
<tr><td><b>Apply Changes</b></td><td>Click to save the current settings.</td></tr>
<tr><td><b>Reset</b></td><td>Click to reset this page.</td></tr>
</table>

Status

System



System Data

System

Firmware Version: v7.0.3.0.4e_US

Firmware Date: 2008/07/29

LAN Configuration

IP Address: 192.168.1.254

Network Mask: 255.255.255.0

Default Gateway: 192.168.1.254

DHCP Server: ON

DHCP Start IP Address: 192.168.1.100

DHCP Finish IP Address: 192.168.1.200

WLAN Configuration

MAC Address: 00:12:0E:4F:20:E7

SSID: 802.11g-AP

Channel: 6

Internet Configuration

Connection Method: Getting IP from DHCP server...

Physical Address: 00:12:0e:4f:20:e6

IP Address: 0.0.0.0

Network Mask: 0.0.0.0

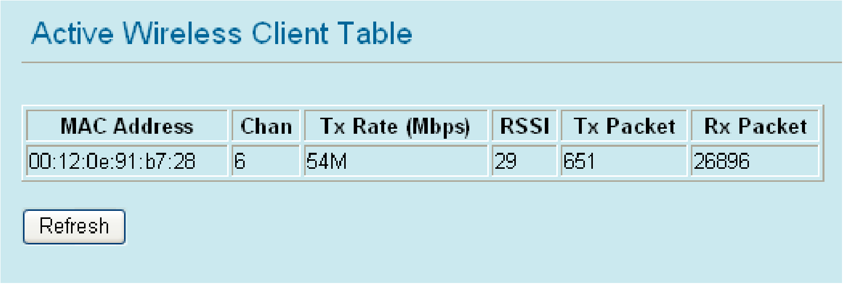
Default Gateway: 0.0.0.0

System	
Firmware Version	The current version of the firmware installed in this device.
Firmware Date	The firmware released date.
LAN Configuration	
MAC Address	Shows the MAC address of this device.
IP Address	Shows the LAN IP address.
Network Mask	Shows the LAN subnet mask.
Default Gateway	Shows the LAN default gateway.
DHCP Server	Shows the current DHCP Server status.
DHCP Start IP Address	Shows the DHCP Start IP address.
DHCP Finish IP Address	Shows the DHCP Finish IP address.
WLAN Configuration	
MAC Address	Shows the MAC address of this device.

SSID	A network name because essentially it is a name that identifies a wireless network.
Channel	The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel.
Internet Configuration	
Connection Method	Shows connection information.
Physical Address	Click to refresh the current system data.
IP Address	Shows the LAN IP address.
Network Mask	Shows the LAN subnet mask.
Default Gateway	Shows the LAN default gateway.
Refresh	Click to refresh the current system data.

Active Clients

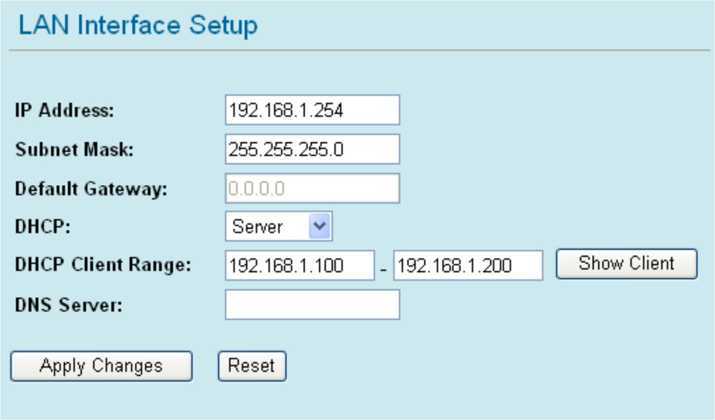
This page displays the Active Wireless Clients Table that is currently connecting with this Wireless Portable Router. Click **Refresh** button to refresh the current client table.



Active Wireless Client Table

MAC Address	Chan	Tx Rate (Mbps)	RSSI	Tx Packet	Rx Packet
00:12:0e:91:b7:28	6	54M	29	651	26896

TCP/IP



LAN Interface Setup

IP Address: 192.168.1.254

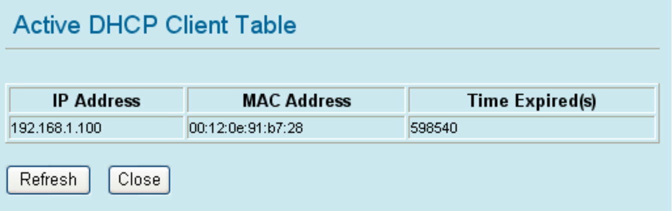
Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DHCP: Server

DHCP Client Range: 192.168.1.100 - 192.168.1.200

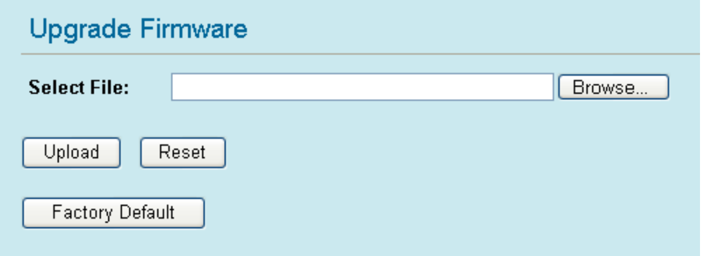
DNS Server:

LAN Interface Setup	
IP Address	Here shows the IP address of the router. Default setting is 192.168.1.254 (this is the local address of this Router).
Subnet Mask	Here shows the subnet mask of the router. Default setting is 255.255.255.0.
Default Gateway	Shows the default gateway IP address.
DHCP	**Disabled**: Select to disable this Router to distribute IP Addresses. **Server**: Select to enable this Router to distribute IP Addresses (DHCP Server). And the following field will be activated for you to enter the starting IP Address.
DHCP Client Range	The starting address of this local IP network address pool. The pool is a piece of continuous IP address segment. Keep the default value 192.168.1.1 should work for most cases. • Maximum: 253. Default value 253 should work for most cases. *Note: If "Continuous IP address poll starts" is set at 192.168.1.1 and the "Number of IP address in pool" is 253, the device will distribute IP addresses from 192.168.1.1 to 192.168.1.253 to all the computers in the network that request IP addresses from DHCP server (Router).*
Show Client	Click to show Active DHCP Client Table.  Active DHCP Client Table IP Address / MAC Address / Time Expired(s) 192.168.1.100 / 00:12:0e:91:b7:28 / 598540

	Refresh: Click this button to refresh the table. **Close**: Click this button to close the window.
DNS Server	Enter the Domain Name Service IP address.
Apply Changes	After completing the settings on this page, click to save the settings.
Reset	Click to restore to default values.

Other

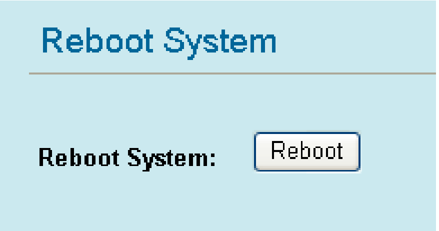
Upgrade Firmware



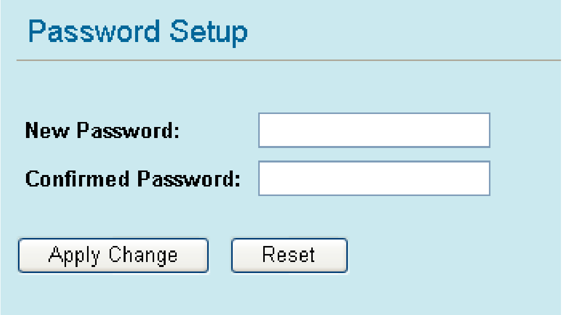
Upgrade Firmware	
Select File	Click the **Browse** button, find and open the firmware file (the browser will display to correct file path).
Upload	Click the Upload button to perform.
Reset	Click the Reset button to restore default values.
Factory Default	Click this button to come back to default factory settings.

Reboot

Click the Reboot button to restart the hardware system.



Password



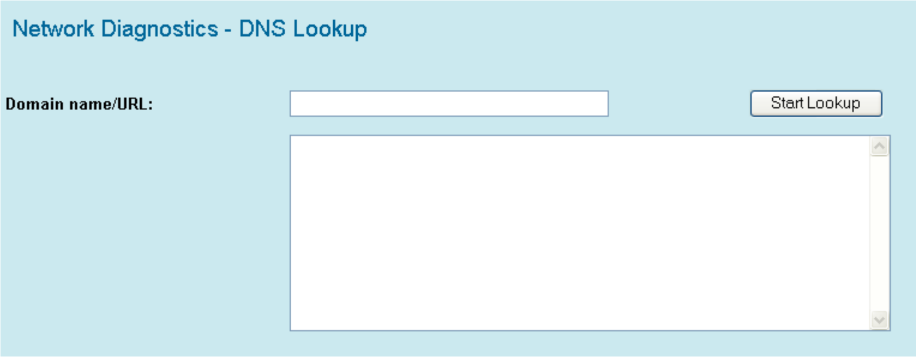
Password Setup

New Password:

Confirmed Password:

Password Setup	
New Password	Maximum input is 36 alphanumeric characters (case sensitive).
Confirmed Password	Key in the password again to confirm.
Apply Change	After completing the settings on this page, click the **Apply Change** button to save the settings.
Reset	Click the **Reset** button to clear settings.

Diagnostics



Network Diagnostics - DNS Lookup

Domain name/URL:

Network Diagnostics - DNS Lookup	
Domain name /URL	Enter Domain name /URL you would like to lookup, then click **Start Lookup** button.

CHAPTER 4:
PC CONFIGURATION

Overview

For each PC, the following may need to be configured:

- TCP/IP network settings
- Internet Access configuration
- Wireless configuration

Windows Clients

- This section describes how to configure Windows clients for Internet access via the Wireless Router.
- The first step is to check the PC's TCP/IP settings.
- The Wireless Router uses the TCP/IP network protocol for all functions, so it is essential that the TCP/IP protocol be installed and configured on each PC.

TCP/IP Settings - Overview

If using default Wireless Router settings, and default Windows TCP/IP settings, no changes need to be made.

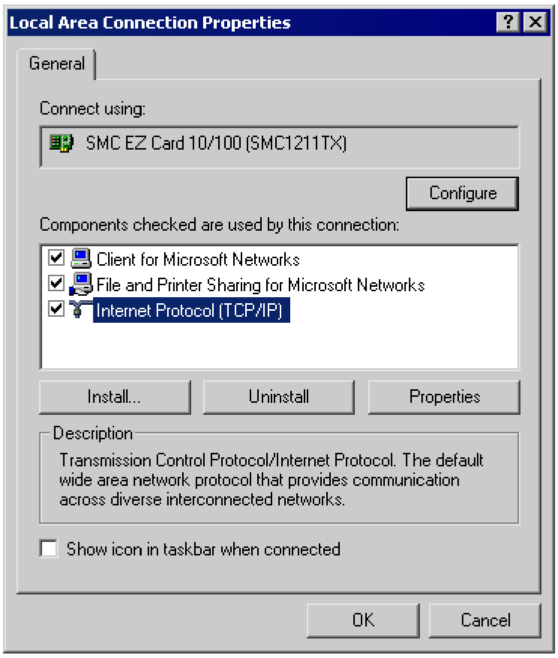
- By default, the Wireless Router will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

If using a Fixed (specified) IP address, the following changes are required:

- The *Gateway* must be set to the IP address of the Wireless Router.
- The *DNS* should be set to the address provided by your ISP.

Checking TCP/IP Settings - Windows 2000

1. Select Control Panel - Network and Dial-up Connection.
2. Right - click the *Local Area Connection* icon and select *Properties*. You should see a screen like the following:



Local Area Connection Properties

General

Connect using:

SMC EZ Card 10/100 (SMC1211TX)

Components checked are used by this connection:

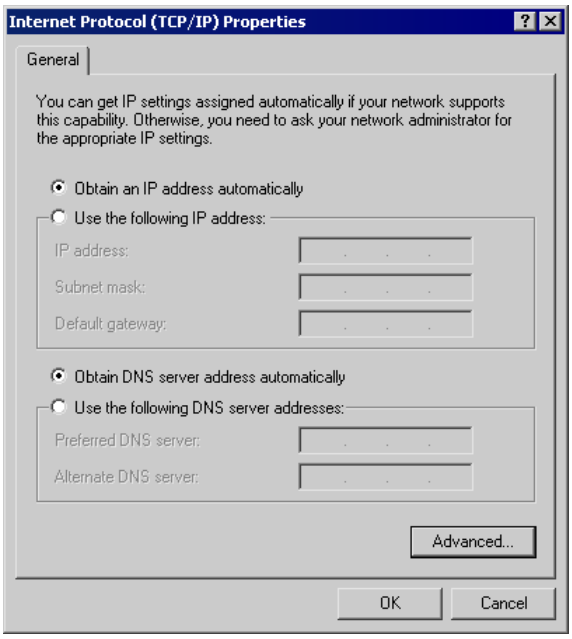
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in taskbar when connected

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

5. Ensure your TCP/IP settings are correct, as described below.

Using DHCP

- To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. Using this is recommended. By default, the Wireless Router will act as a DHCP Server.
- Restart your PC to ensure it obtains an IP Address from the Wireless Router.

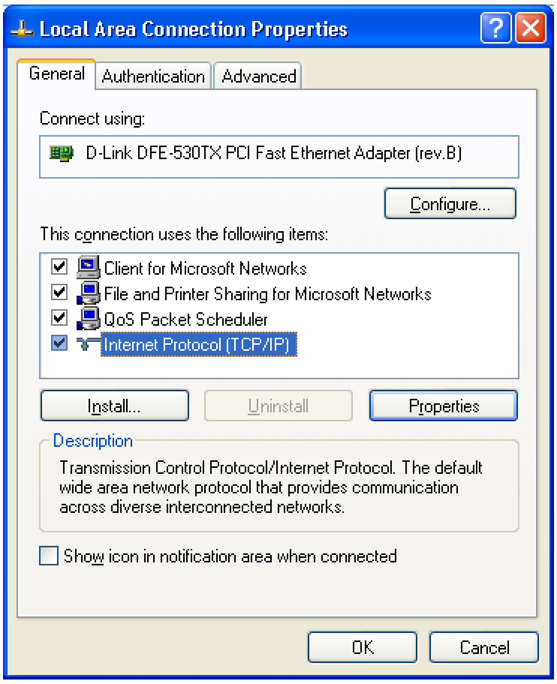
Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- Enter the Wireless Router's IP address in the *Default gateway* field and click *OK*. (Your LAN administrator can advise you of the IP Address they assigned to the Wireless Router.)
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enters the DNS address or addresses provided by your ISP, then click *OK*.

Checking TCP/IP Settings - Windows XP

1. Select Control Panel - Network Connection.
2. Right click the *Local Area Connection* and choose *Properties*. You should see a screen like the following:



Local Area Connection Properties

General | Authentication | Advanced

Connect using:

D-Link DFE-530TX PCI Fast Ethernet Adapter (rev.B)

Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

Description

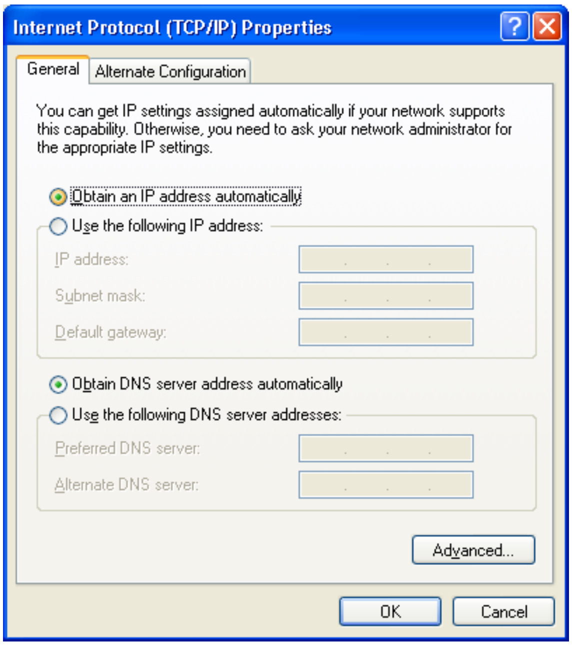
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected

OK | Cancel

3. Select the *TCP/IP* protocol for your network card.

4. Click on the *Properties* button. You should then see a screen like the following.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

5. Ensure your TCP/IP settings are correct.

Using DHCP

- To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. Using this is recommended. By default, the Wireless Router will act as a DHCP Server.
- Restart your PC to ensure it obtains an IP Address from the Wireless Router.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- In the *Default gateway* field, enter the Wireless Router's IP address and click *OK*. Your LAN administrator can advise you of the IP Address they assigned to the Wireless Router.
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enters the DNS address or addresses provided by your ISP, then click *OK*.

Internet Access

To configure your PCs to use the Wireless Router for Internet access:

- Ensure that the ADSL modem, DSL modem, Cable modem, or other permanent connection is functional.
- Use the following procedure to configure your Browser to access the Internet via the LAN, rather than by a Dial-up connection.

For Windows 2000

1. Select Start Menu - Settings - Control Panel - Internet Options.
2. Select the Connection tab, and click the *Setup* button.
3. Select "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" and click *Next*.
4. Select "I connect through a local area network (LAN)" and click *Next*.
5. Ensure all of the boxes on the following Local area network Internet Configuration screen are unchecked.
6. Check the "No" option when prompted "Do you want to set up an Internet mail account now?"
7. Click *Finish* to close the Internet Connection Wizard. Setup is now completed.

For Windows XP

1. Select Start Menu - Control Panel - Network and Internet Connections.
2. Select *Set up or change your Internet Connection*.
3. Select the *Connection* tab, and click the *Setup* button.
4. Cancel the pop-up "Location Information" screen.
5. Click *Next* on the "New Connection Wizard" screen.
6. Select "Connect to the Internet" and click *Next*.
7. Select "Set up my connection manually" and click *Next*.
8. Check "Connect using a broadband connection that is always on" and click *Next*.
9. Click *Finish* to close the New Connection Wizard. Setup is now completed.

Accessing AOL

To access AOL (America On Line) through the Wireless Router, the *AOL for Windows* software must be configured to use TCP/IP network access, rather than a dial-up connection. The configuration process is as follows:

1. Start the *AOL for Windows* communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
2. Click the *Setup* button.
3. Select *Create Location*, and change the location name from "New Locality" to "Wireless Router".

4. Click *Edit Location*. Select *TCP/IP* for the *Network* field. (Leave the *Phone Number* blank.)
5. Click *Save*, then *OK*.
6. Configuration is now complete.
7. Before clicking "Sign On", always ensure that you are using the "Wireless Router" location.

Macintosh Clients

From your Macintosh, you can access the Internet via the Wireless Router. The procedure is as follows.

1. Open the TCP/IP Control Panel.
2. Select *Ethernet* from the *Connect via* pop-up menu.
3. Select *Using DHCP Server* from the *Configure* pop-up menu. The DHCP Client ID field can be left blank.
4. Close the TCP/IP panel, saving your settings.

Note:

If using manually assigned IP addresses instead of DHCP, the required changes are:

- Set the *Router Address* field to the Wireless Router's IP Address.
- Ensure your DNS settings are correct.

Linux Clients

To access the Internet via the Wireless Router, it is only necessary to set the Wireless Router as the "Gateway".
Ensure you are logged in as "root" before attempting any changes.

Fixed IP Address

By default, most Unix installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.

- Set your "Default Gateway" to the IP Address of the Wireless Router.
- Ensure your DNS (Domain Name server) settings are correct.

To act as a DHCP Client (Recommended)

The procedure below may vary according to your version of Linux and X -windows shell.

1. Start your X Windows client.
2. Select *Control Panel – Network.*
3. Select the "Interface" entry for your Network card. Normally, this will be called "eth0".
4. Click the *Edit* button, set the "protocol" to "DHCP", and save this data.
5. To apply your changes:
   - Use the "Deactivate" and "Activate" buttons, if available.
   - OR, restart your system.

Other Unix Systems

To access the Internet via the Wireless Router:

- Ensure the "Gateway" field for your network card is set to the IP Address of the Wireless Router.
- Ensure your DNS (Name Server) settings are correct.

Wireless Station Configuration

- This section applies to all wireless stations wishing to use the wireless router's access point, regardless of the operating system that is used on the client.
- To use the wireless portable router in the wireless router, each wireless station must have compatible settings, as following:

Mode	The mode must be set to *Infrastructure*.
SSID (ESSID)	This must match the value used on the Wireless Router. ***Note! The SSID is case sensitive.***
Open System / Shared Key	If there is no security is enabled on the Wireless Router, the security of each station should be disabled as well. And, you can connect the Wireless Router without security, but it is not recommended.
WEP	By default, WEP on the Wireless Router is disabled. • If WEP remains disabled on the Wireless Router, all stations must have WEP disabled. • If WEP is enabled on the Wireless Router, each station must use the same settings as the Wireless Router.
WPA-PSK/ WPA2-PSK/ WPA-RADIUS/ WPA2-RADIUS	WPA-PSK (TKIP/AES)/ WPA2-PSK (TKIP/AES)/ WPA-RADIUS (TKIP/AES)/ WPA2 -RADIUS (TKIP/AES): If one of these securities is enabled on the Wireless Router, each station must use the same settings as the Wireless Router.

Note: By default, the Wireless Router will allow both 802.11b and 802.11g connections.

A

APPENDIX A: TROUBLESHOOTING

Overview

This chapter covers some common problems that may be encountered while using the Wireless Router and some possible solutions to them. If you follow the suggested steps and the Wireless Router still does not function properly, contact your dealer for further advice.

General Problems

Problem 1:	Can't connect to the Wireless Router to configure it.
Solution 1:	Check the following: • Check the Wireless Router is properly installed, LAN connections are OK, and it is powered ON. • Ensure that your PC and the Wireless Router are on the same network segment. (If you don't have a router, this must be the case.) • If your PC is set to "Obtain an IP Address automatically" (DHCP client), please restart it. • If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.1.1 to 192.168.1.253 and thus compatible with the Wireless Router's default IP Address of 192.168.1.254. Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Router. In Windows, you can check these settings by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Internet Access

Problem 1:	When I enter a URL or IP address I get a time out error.
Solution 1:	A number of things could be causing this. Try the following troubleshooting steps. • Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address. • If the PCs are configured correctly, but still not working, check the

	Wireless Router. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.) • If the Wireless Router is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.
Problem 2:	Some applications do not run properly when using the Wireless Router.
Solution 2:	The Wireless Router processes the data passing through it, so it is not transparent. Use the *Special Applications* feature to allow the use of Internet applications, which do not function correctly. If this does solve the problem you can use the *DMZ* function. This should work with almost every application, but: • It is a security risk, since the firewall is disabled. • Only one (1) PC can use this feature.

Wireless Access

Problem 1:	My PC can't locate the Wireless Portable Router.
Solution 1:	Check the following: • Your PC is set to *Infrastructure Mode*. (Access Points are always in *Infrastructure Mode*) • The SSID on your PC and the Wireless Portable Router are the same. Remember that the SSID is case-sensitive. So, for example "**W**orkgroup" does NOT match "**w**orkgroup". • Both your PC and the Wireless Router must have the same setting for security. The default setting for the Wireless Router security is disabled, so your wireless station should also have security disabled. • If security is enabled on the Wireless Router, your PC must have security enabled, and the key must match. • If the Wireless Router's *Wireless* screen is set to *Allow LAN access to selected Wireless Stations only*, then each of your Wireless stations must have been selected, or access will be blocked. • To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Router. Remember that the connection range can be as little as 100 feet in poor environments.
Problem 2:	Wireless connection speed is very slow.
Solution 2:	The wireless system will connect at the highest possible speed, depending on the distance and the environment. To obtain the highest possible

	connection speed, you can experiment with the following: • Wireless Router location. Try adjusting the location and orientation of the Wireless Router. • Wireless Channel. If interference is the problem, changing to another channel may show a marked improvement. • Radio Interference. Other devices may be causing interference. You can experiment by switching other devices off, and see if this helps. Any "noisy" devices should be shielded or relocated. • RF Shielding. Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Wireless Router.

APPENDIX B: ABOUT WIRELESS LANS

BSS

BSS

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).

Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other.

Channels

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channel are available. If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference.
- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)

Note to US model owner: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.

Security

WEP

WEP (Wired Equivalent Privacy) is a standard for encrypting data before it is transmitted. This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.

If WEP is used, the Wireless Stations and the Access Point must have the same settings for each of the following:

WEP	64 Bits, 128 Bits.
Key	For 64 Bits encryption, the Key value must match. For 128 Bits encryption, the Key value must match.
WEP Authentication	Open System or Shared Key.

WPA/WPA2

WPA/WPA2 (Wi-Fi Protected Access) is more secure than WEP. It uses a “Shared Key” which allows the encryption keys to be regenerated at a specified interval. There are several encryption options: **TKIP, AES, TKIP-AES** and additional setup for **RADIUS** is required in this method.

WPA-PSK/ WPA2-PSK

WPA/WPA2 (Wi-Fi Protected Access using Pre-Shared Key) is recommended for users who are not using a RADIUS server in a home environment and all their clients support WPA/WPA2. This method provides a better security.

Encryption	**WEP Key 1~4**	**Passphrase**
TKIP	**NOT REQUIRED**	**8-63 characters**
AES		

802.1x

With **802.1x** authentication, a wireless PC can join any network and receive any messages that are not encrypted, however, additional setup for **RADIUS** to issue the WEP key dynamically will be required.

Wireless LAN Configuration

To allow Wireless Stations to use the Access Point, the Wireless Stations and the Access Point must use the same settings, as follows:

Mode	On client Wireless Stations, the mode must be set to "Infrastructure". (The Access Point is always in "Infrastructure" mode.)
SSID (ESSID)	Wireless Stations should use the same SSID (ESSID) as the Access Point they wish to connect to, but the SSID can not set to be null (blank).
WEP	The Wireless Stations and the Access Point must use the same settings for WEP (None, 64 Bit, 128 Bit). WEP Key: If WEP is enabled, the Key must be the same on the Wireless Stations and the Access Point. WEP Authentication: If WEP is enabled, all Wireless Stations must use the same setting as the Access Point (either "Open System" or "Shared Key").
WPA-PSK/ WPA2-PSK/ WPA-RADIUS/ WPA2-RADIUS	WPA-PSK (TKIP/AES)/ WPA2-PSK (TKIP/AES)/ WPA-RADIUS (TKIP/AES)/ WPA2 -RADIUS (TKIP/AES): If one of these securities is enabled on the Wireless Router, each station must use the same settings as the Wireless Router. If there is no security is enabled on the Wireless Router, the security of each station should be disabled as well.