LANPRO
THE NATURAL CHOICE IN NETWORKING

LP-993

LP933_UG_ENB01W

Outdoor Multi-function Radio

USER MANUAL

Version 1.0.1

www.lanpro.com

Copyright

About This Manual

This manual includes install, configuration and trouble shooting for the WLAN outdoor radios. It helps you in avoiding the unforeseen problems and using the outdoor radio correctly.

Technical Support

If you have difficulty resolving the problem while installing or using the Wireless LAN ODU, please contact the LanPro supplier for support.

Conventions

This publication uses the following conventions to convey instructions and information:

This symbol means ***reader take note*.** Notes contain helpful suggestions or references to materials not contained in this manual.

This symbol means ***reader be careful*.** In this situation, you might do something that could result in equipment damage or loss of data.

This warning symbol means ***danger***. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

Chapter 1 Overview

The 802.11g WLAN outdoor radio – 54Mbps Wireless Outdoor Unit, are specially designed for Point-to-Point / Point-to-Multipoint bridge and Hotspot applications, offering long distance connections between buildings at a speed of up to 54Mbps. Fully compliant with LP-993 standard, the Outdoor Unit (ODU) provides powerful features such as the Windows-based configuration utility, MAC access control, WEP, WPA-PSK, WPA, hidden SSID and wireless isolation, WDS application and more.

The Following contents of this chapter will show you

- **Features and Benefits**
- Applications

1-1 Features and Benefits

- Provides the easy installation and cost effective outdoor hotspot and PTP / PTMP solution up to 15 KM .
- The ODU act as bridge and access point at the same time with the WDS function.
- With a data rate up to 54Mbps, the system is faster than an E1/T1 data link.
- Features 54Mbps data rate by incorporating OFDM (Orthogonal Frequency Division Multiplexing) technology.
- Fully LP-993 compatible. Allow inter-operation among multiple vendors.
- Technique operating in the unlicensed 2.4GHz ISM band.
- Seamless roaming within the 802.11 & 802.11b/g wireless LAN infrastructure.

- Provides the highest available level of WEP / WAP-PSK / WPA as well as MAC access control to increase security.
- Advanced security mechanism such as 802.1x auth. Hidden SSID and wireless isolation.
- Provides Window-based configuration utility.
- IP-68 rated weatherproof housing

1-2 Applications

The outdoor radio offers a fast, reliable, high-speed, and high security solution for wireless clients access to the network. It's easier and more cost effective to deploy the wireless access environment with the Wireless Distribution System (WDS) technology. Saving 30% ~ 50% cost for telecom operators, ISPs and enterprises. It's really an ideal solution for enterprise / campus connectivity, Hotspot and next-generation broadband wireless Access.

The 802.11g WLAN outdoor radio offers a fast, reliable, cost-effective solution for wireless client access to the network in applications like these:

1. **Remote Access to Corporate Network Information**
   E-mail, file transfer and terminal emulation.
2. **Difficult-to-Wire Environments**
   Historical or old buildings, asbestos installations, and open area where wiring is difficult to deploy.
3. **Frequently Changing Environments**
   Retailers, manufacturers and those who frequently rearrange the workplace and change location.
4. **Temporary LANs for Special Projects or Peak Time**

C1- Trade shows, exhibitions and construction sites where a temporary network will be practical.

C2- Retailers, airline and shipping companies need additional workstations during peak period.

C3- Auditors requiring workgroups at customer sites.

5. Access to Database for Mobile Workers

Doctors, nurses, retailers, accessing their database while being mobile in the hospital, retail store or office campus.

6. High Security Connection

The secure wireless network can be installed quickly and provide flexibility.

Chapter 2 Hardware Installation

This chapter describes warning, safety information and guideline to install the Outdoor Multi-function Radio. Please make sure to read all the contents of this chapter then start to install this radio.

- **Warnings**
- **Package Contents**
- **System Requirements**
- **Mechanical Description**
- **Hardware Installation**

2-1 Warnings

In order to comply with international radio frequency (RF) exposure limits, dish antennas should be laced at a minimum of 8.7 inches (22 cm) from the bodies of all persons. Other antennas should be laced a minimum of 7.9 inches (20 cm) from the bodies of all persons.

Do not work on the system or connect or disconnect cables during periods of lightning activity.

This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Ultimate disposal of this product should be handled according to all national laws and regulations.

Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.:NFPA 70, National Electrical Code, Article 810, in Canada: Canadian Electrical Code, Section 54).

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

To meet regulatory restrictions, the radio and the external antenna must be professionally installed. The network administrator or other IT professional responsible for installing and configuring the unit is a suitable professional installer. Following installation, access to the unit should be password protected by the network administrator to maintain regulatory compliance.

The Outdoor Multi-function radio and POE injector can be damaged by incorrect power application. Read and carefully follow the installation instructions before connecing the system to its power source.

Follow the guidelines in this chapter to ensure correct operation and safe use of the 802.11g outdoor radio.

2-2 Package Contents

The package you have received should contain the following items:

- 802.11g Outdoor Multi-function Radio ……x1
- PoE Injector. ……x1
- AC Power Code ……x1
- 15V Power adaptor……x1
- Mounting Kit ……x1
- Product CD……x1
- Quick Installation Guide……x1

If any item on the above list is not included or damaged, please contact your local vendor for support.

2-3 System Requirements

Before installing the 802.11g Outdoor Multi-function Radio, please make sure that these requirements have been met:

- A 10/100 Mbps Local Area Network device such as a hub or switch. (optional)
- Category 5 UTP or STP networking cable. (From the PC to POE)

- Category 5 SSTP or SFTP networking cable. (From the radio to POE)
- A Web browser for configuration: Microsoft IE 5.0 or later, or Netscape Navigator 5.0 or later version.
- Installing TCP/IP protocol to the computer.

2-4 Mechanical Description

Please refer to the following table for the meaning of each feature.

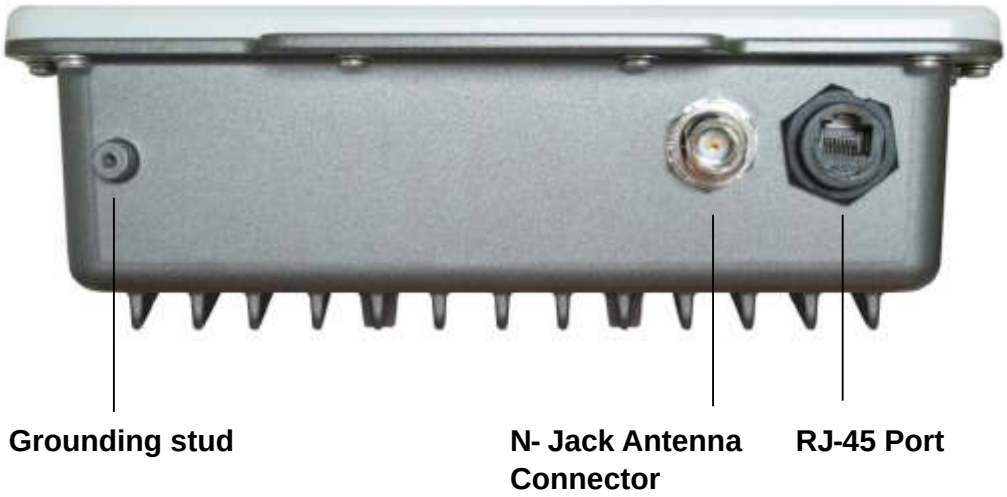
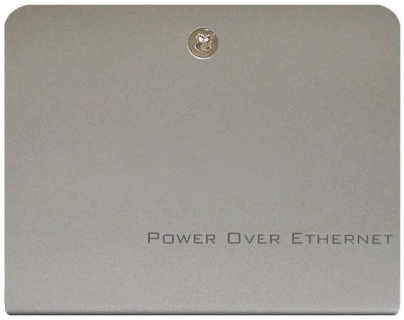
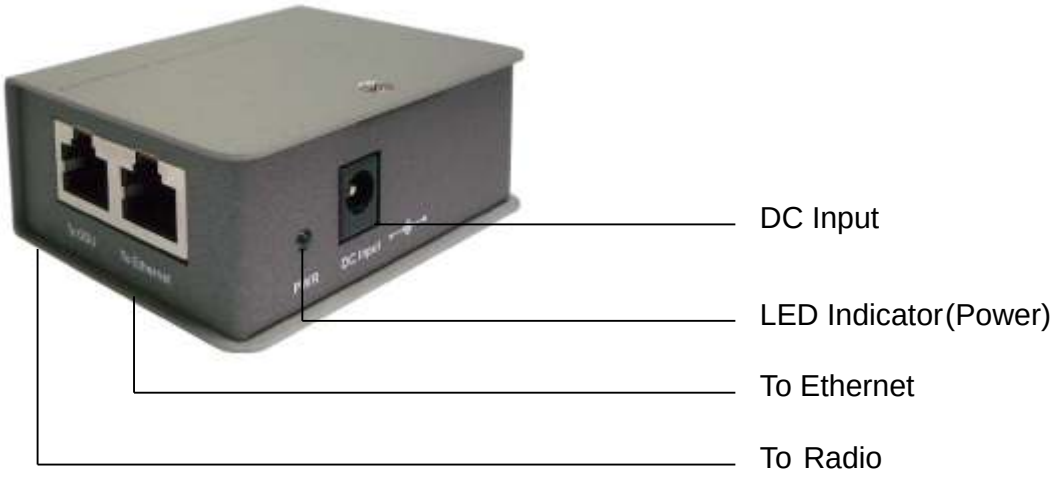


Figure 2-1 Outdoor Multi-function Radio

1	**RJ-45 Port**	Use the SFTP cat.5 cable with weatherproof connector to connect to the “To ODU” side of PoE injector.

2	**N- Jack Antenna Connector**	Here you can attach the proper antenna with the Outdoor Multi-function Radio to wirelessly connect to the 802.11g networks. In order to improve the RF signal radiation of your antenna, proper antenna installation is necessary.
3	**Grounding stud**	Connect to the ground conductor with the ground wire.





1	**To Ethernet**	Here you can attach the proper antenna with the Outdoor Multi-function Radio to wirelessly connect to the 802.11g networks. In order to improve the RF signal radiation of your antenna, proper antenna installation is necessary.
2	**To ODU**	RJ-45 port used to connect to the ODU..
3	**DC Input**	Connect to the Power adaptor for 15V DC input.
4	**LED Indicator**	Power LED.

This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

The Outdoor Multi-function radio and POE injector can be damaged by incorrect power application. Read and carefully follow the installation instructions before connecing the system to its power source.

Power Over Ethernet Injector is not a waterproof unit, should not be exposed to outdoor without any protection.

2-5 Hardware Installation

The Outdoor Multi-function Radio is a radio device, so it is susceptible to common causes of interference that can reduce throughput and range. Follow these basic guidelines to ensure the best possible performance:

- IF there is any other 2.4GHz RF device deployed around the outdoor radio, try to set the channel to the non overlapping one.
- Install the bridge at a height sufficient place where structures, trees, or hills do not obstruct radio signals to and from the unit. A clear line-of-sight path can guarantee the performance of the RF link

Site Surveys

Clear and flat area provide better RF range and data rate, on the contrary, physical obstructions such as trees, electric tower, hills or buildings can reduce the performance of RF devices. Do not deploy your radios in the location where there is any obstacle between the antennas.

Configure and verify the 802.11g Outdoor Multi-function Radio operations first before you mount the radio in a remote location.

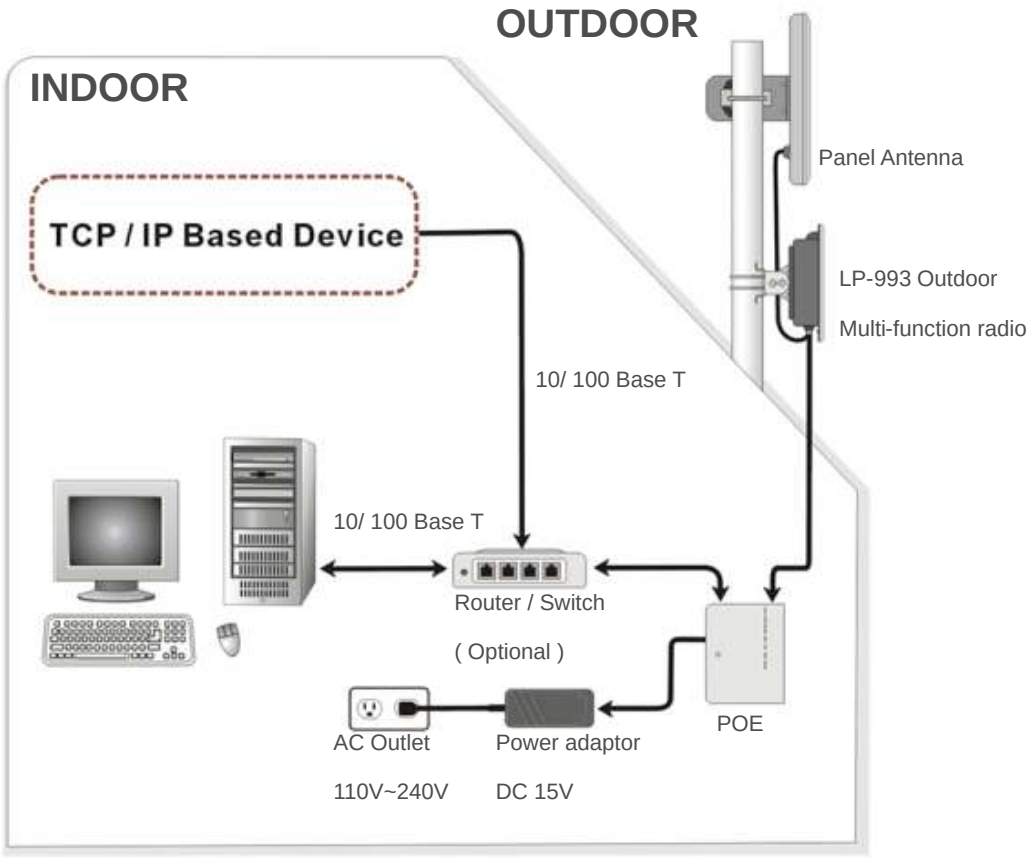


Figure 2-3 Hardware Installation Figure

Power Over Ethernet Injector is not a waterproof unit, should not be exposed to outdoor without any protection.

Connect the Ethernet Cable

The Outdoor Multi-function Radio support 10/100M Ethernet connection. Attach your SFTP / SSTP cat.5 Ethernet cable with waterproof connector to the RJ-45 connector on the ODU enclosure. Then connect the other end of the cable to the “To ODU” side on PoE injector.

Welding the shielding parts of the SFTP cable and the RJ-45 connector well to ensure the performance of the system and avoid the moisture leak into the radio.

Figure 2-4 Weld the RJ-45 connector with the SFTP cable

Weld the SFTP cable as the Figure 2-4, make sure the welding parts NOT bigger than the figure, or it will affect the function of waterproof RJ-45 connector.

Attached the antenna

You can attach the proper antenna to the N-type connector on the Outdoor Multi-function Radio.

To meet regulatory restrictions, the outdoor radio and the external antenna must be professionally installed.

Connect the Power Cable

Connect the 15V power adapter to the POE injector, and plug the other end of the electrical outlet (AC 110V~240V).

We cannot assume the responsibility for the damage from using with the other power adapter supplier.

You should read and carefully follow the installation instructions before connecting the system to its power source. The outdoor radio and power injector can be damaged by incorrect power application.

Connect the ground stud

Connect the ground stud on the ODU enclosure with the ground wire.

This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Mounting the 802.11g Outdoor Multi-function Radio

The outdoor radio is usually installed on a rooftop, tower, wall, or a suitable flat surface. For detailed

mounting instructions, please refer to the Quick Installation Guide.

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Wind the water-resistant adhesive tape around the RJ-45 and N-type connector on the outdoor radio enclosure as the last step of the mounting procdures.

Chapter 3 Configuring the 802.11g Radio

This chapter describes the LanPro web-browser interface that you can use to configure the Outdoor Multi-function Radio. The web browser interface contains management pages that you use to change the settings, upgrade firmware, monitor and configure other wireless devices on the network.

This chapter contains these sections:

- Start-up and Log in
- IP Setup
- Wireless Setup
- Status
- Management

3-1 Using the Web Management

The built-in LanPro Web Management provides you with a user-friendly graphical user interface (web pages) to manage your 802.11g WLAN outdoor radio.

3-1-1 How to access the web-browser configuration utility?

1. Connect your computer to the wireless adapter either through wireless or wired connection. Please set a fixed IP address, within the range of 192.168.1.X (X can't be 2), to your computer.
2. Activate your browser, then type this 802.11g WLAN outdoor radio's address (e.g. **http://192.168.1.2**), in the Location (for IE) or Address field and press Enter.

3. Key in the system password (the default setting is “default”) and click on the “**Login**” button. You will see the main page.

3-1-3 Configuration

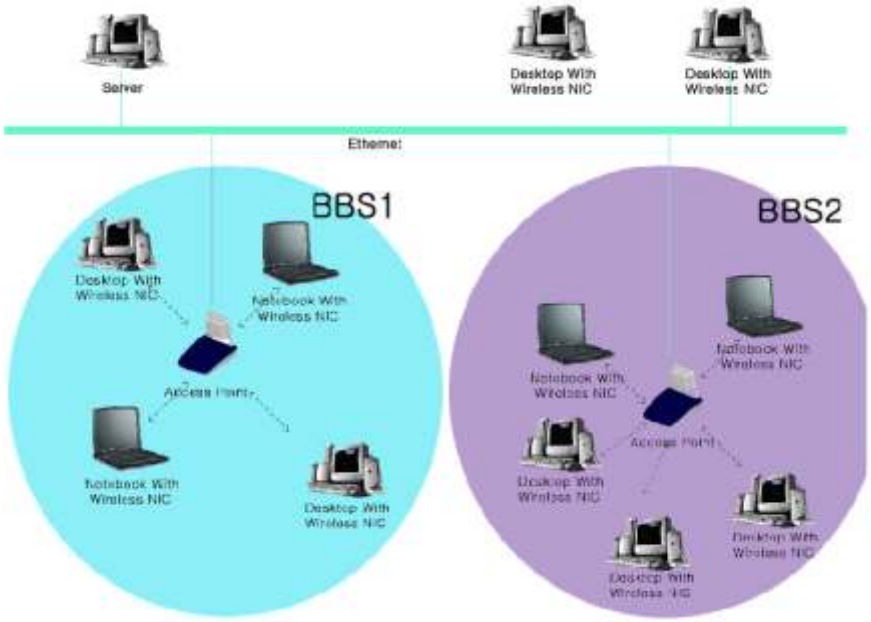
General Page

You may make the settings on your 802.11g WLAN outdoor radio such as Access Point Name, Wireless Mode, Network Type, ESSID, Rate, Country/Region and Channel.

Access Point Name: In this field, you may enter any name. This will enable you to manage your 802.11g WLAN outdoor radio more easily if you have multiple 802.11g WLAN outdoor radios on the network. Besides, **Access Point Name** can be used to prevent you from forgetting an IP Address and fail to access the website. Try to type the nickname you like to identify the website, then press the button of **"Apply"** to reboot.

Wireless Mode: The default wireless operating mode of the 802.11g WLAN outdoor radio is Access Point (AP) mode. To switch to Station mode, select the desired mode from the down-arrow menu. Click Apply. The board will reboot into the desired mode..

AP Mode: The LanPro system can be configured to work as a wireless network access point. Note that the 802.11g WLAN outdoor radio acts only as a layer 2 bridge and does not act as a DHCP server. In other words, it does not supply dynamic IP addresses and instead relies on the network to supply them. The implementation can be shown as below:



Station Mode: When configuring as a station mode, the device is now acting as a wireless client. The 802.11g WLAN outdoor radio will associate to an AP within its range in infrastructure mode, or join with another device in Client mode in an ad-hoc network.

Network Type: There are 2 network types for the wireless station adapter to operate. If you need to access company network or Internet via Access Point, select "**Infrastructure**". To set up a group of wireless stations for files and printer sharing, select "**Ad-Hoc**" (without Access Point). For **Ad-Hoc** operation, the *same ESSID* is required to set for the wireless stations.

ESSID: The ESSID is a unique ID used by Access Points and Stations to identify a wireless LAN. Wireless clients associating to any Access Point must have the same ESSID. The default ESSID is ANY. The ESSID can have up to 32 characters.

Channel: Select a clear and available channel as an operational channel for your wireless station adapter when it performs as Ad-Hoc mode or AP with repeating mode.

Mode: There are three different wireless modes to operate, "B Only Mode", "G Only Mode", and "B/G Mixed Mode". In B/G Mixed Mode, the wireless station adapter is compatible with a mix of both 802.11g and 802.11b clients. You will see that the factory-set default "B/G Mixed Mode" will prove the most efficient. B Only Mode is compatible with 802.11b clients only. This mode can be used only if you do not allow any 802.11g clients to join a network. G Only Mode is compatible with 802.11g clients only. This mode can be used only if you do not allow any 802.11b clients to access to the network. To switch the mode, select the desired mode from the pull-down menu of "**Mode**".

Rate: The wireless station adapter provides various data rate options for you to choose. Data rates options include **Auto, 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48 and 54. The default setting is Auto.**

Country/Region: Allows you to select country domain in case there is any chances that you would use wireless network in other countries. There are a total of 11 countries for you to select. They are Africa, Asia, Australia, Canada, Europe, France, Israel, Japan, Mexico, South America, and USA. Note that if your AP and station adapter are in different standards, please use the **"Country/Region"** item to switch the standards of the station adapter (For example, when set to client mode, if your Access Point is America standard but your station adapter is Japanese standard, you can pull down the **"Country/Region"** option to switch your station adapter from Japanese standard to American standard.). As long as you change the country domain, the

Click **"Apply"** if you have made any changes.

Security Page

Various encryption and authentication build highly security mechanism for this 802.11g radio, such as WEP, WPA-PSK, WPA, 802.1x…etc.

Data encryption: This LanPro 802.11g WLAN outdoor radio allows you to create up to 2 data encryption keys to secure your data from being eavesdropping by unauthorized wireless users. To enable the encryption, all devices on the network must share the same WEP key.

Disable: Allows the wireless station to communicate with the Access Point without any data encryption.

WEP40: Requires the wireless station adapter to use data encryption with 40-bit algorithm when communicating with the Access Point.

WEP128: Allows the wireless station adapter to communicate with the Access Point with data 128-bit encryption algorithm.

<u>For 40-bit encryption you may choose:</u>

ASCII: *Enter **5 characters*** (case sensitive) ranging from “a-z”, “A-Z” and “0-9” (e.g. **MyKey**).
Hex: Alternatively, you may enter **10 *hexadecimal digits*** in the range of “A-F”, “a-f” and “0-9” (e.g. **11AA22BB33**).

For 128-bit encryption you may choose:

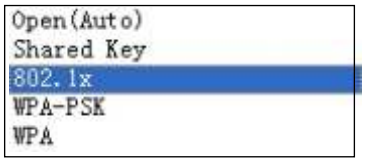
ASCII: *Enter **13 characters*** (case sensitive) ranging from "a-z", "A-Z" and "0-9" (e.g. **MyKey12345678**).

Hex: Alternatively, you may enter **26 *hexadecimal digits*** in the range of "A-F", "a-f" and "0-9" (e.g. **00112233445566778899AABBCC**).

After entering the WEP keys in the key field, select one key as active key.

Alternatively, you may create encryption keys automatically by using Passphrase. From the Passphrase field, type a character string and click "**Generate**". As you type, the 802.11g WLAN outdoor radio will use an algorithm to generate 4 keys automatically. Select one key from the 4 WEP keys.

Network authentication: Moreover, the 802.11g WLAN outdoor radio provides five types of authentication services: Open System (Auto), Shared Key, 802.1x, WPA-PSK and WPA.



Open (Auto)：The default authentication type is Open System (Auto), requires no authentication since it allows any device to join a network without performing any security check.

Shared Key: If you require higher security for wireless access, you may select Shared Key. Note that when Shared Key is selected, a WEP key is required and must be the same between the Access Point and client.

802.1x: The 802.1x authentication (EAP) is designed to enhance the security of wireless networks. The 802.1x provides an authentication framework for wireless LANs, allowing a user to be authenticated by a central authority. For wireless LANs, it also provides centralized, server-based authentication of end users. The standard is flexible enough to allow multiple authentication algorithms, and because it is an open standard, multiple vendors can innovate and offer enhancements.

For wireless LANs, the 802.1x authentication has three main components: The supplicant (usually the client software, such as zero configuration in window XP), the authenticator (usually the access point), and the authentication server (usually a Remote Authentication Dial-In User Service server, although RADIUS although 802.1X does not specify it).

The advanced security describes how to control authorized access to the Access Point with Remote Authentication Dial-In User Service (RADIUS). To enable 802.1x based authentication, please select 802.1x. Moreover, you may enable the radius account function by check Enable Radius Account in the check box. To configure the Authentication and Account Server function, the parameter of Radius Authentication Server and Radius Account Server must set to the same with the Authentication Server and Account Server.

Note: The Password is up to 16 bytes.

Otherwise, you may select disable auth mode that adjusts to the 802.11 legacy network.

For setting 802.1x Based Auth:

1. Enable 802.1x by clicking the “802.1x Based Auth” radio button.
2. Configure the IP address and port number and set the parameters the same as RADIUS server. (Default port number is 1812)
3. Configure the password and set it the same as RADIUS server. (Security key)
4. Enable the Radius Account when you needed to use Radius account service. (Default port number is 1813)
5. You can also configure the 802.1x parameters through web-based management.
6. On the client side, you'll need to set the security setting, as well as the authentication method (MD5/TLS is supported by Windows XP) , user name, password or certificate. For detail setting, you can refer to documentation of windows XP.

WPA-PSK: Allows the wireless station adapter to communicate with the Access Point with a more secure data protection than the WEP. Here you can select the WPA with PSK mode to improve the data security and privacy during wireless transmission. The present WPA supplied with this 802.11g WLAN outdoor radio is used in a pre-shared key mode, which does not require an authentication (Radius) server.

For WPA-PSK mode you may choose:

In the WPA-PSK field, you may input 8-63 characters ranging from “a-z”, “A-Z” and “0-9”. If you require that access to the Internet or other wireless network services are allowed only when the pre-shared key

of the LanPro 802.11g WLAN outdoor radio matches that of the device you want to communicate.

WPA (Wi-Fi Protected Access): Currently one of the highest levels of security a wireless network can achieve. Wi-Fi Protected Access is a subset of the security specification and has been introduced as an interim solution for most known security weaknesses in relation to plain WEP. TKIP, the successor to WEP, includes enhancements that eliminate the known vulnerabilities of WEP. Enterprises that already have RADIUS authentication in place can use WPA with 802.1x (WPA-EAP / Enterprise Mode). Small business and home wireless LAN can use WPA without 802.1x (WPA-PSK / Pre-Shared Key).

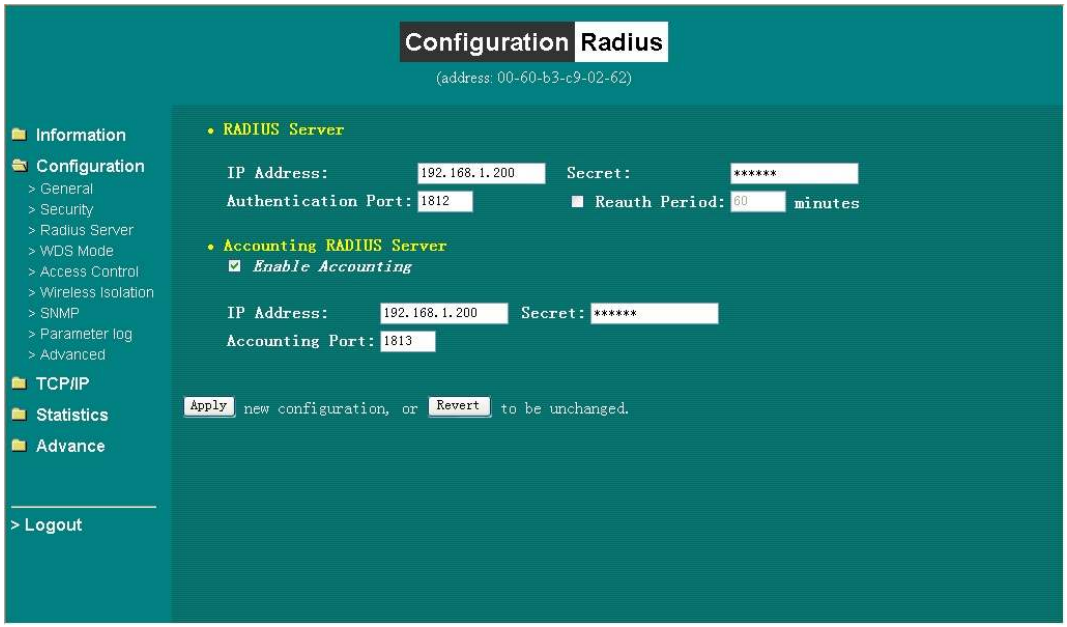
In cooperation with RADIUS, systems with WPA-EAP will be used with a new encryption method called Temporal Key Integrity Protocol (TKIP) implementation with 802.1x dynamic key exchange.

Note:

1. **Supports AES (Advanced Encryption Standard) in WPA-PSK and WPA mode.**
2. **When the radio is set to be station mode, 802.1x and WPA are not available.**

Click the **"Apply"** button on the Configuration tab to make the setting take effect.

Radius Server Page



RADIUS (Remote Authentication Dial-In User Service) plays a central role in the network to provide the capabilities of authenticating, authorizing, accounting, auditing and alarming…etc and allows an organization to maintain user profiles in a central database that all remote servers can share. Since RADIUS is relatively complex to explain, we will focus here on how it acts as an 802.1x authentication server (EAP-aware RADIUS) and assists in enhancing security.

RADIUS performs the authentication function required to check the credentials of users and intermediate Access Points and indicates whether the users are authorized to access the Access Points. Enabling RADIUS is therefore the first step toward building up an 802.1x-capable environment. Even more, it is also a must-do to accommodate the recently introduced Wi-Fi protected access (WPA-EAP) to wireless networks.

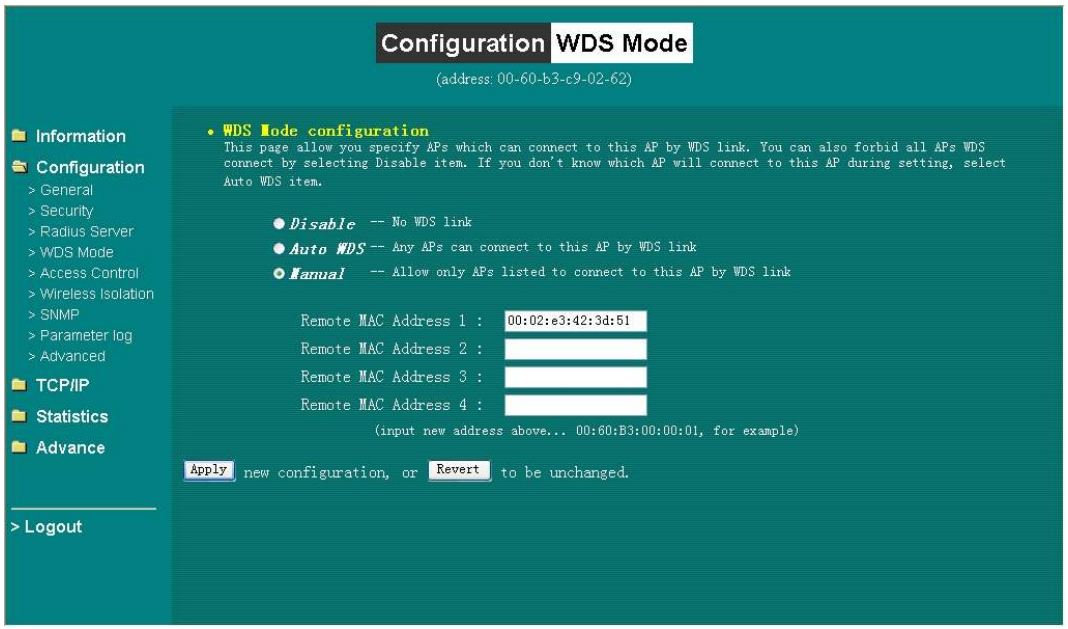
Setting up RADIUS information in your Access Point is quite simple; just input the IP address of the RADIUS server and its port number, which is usually set to 1812, as well as the secret key, which is identified with the given key in RADIUS. Press **"Apply"** to apply the settings.

When you finish adding RADIUS information, return to the Security page, where you will be allowed to continue configuring 802.1x and WPA-EAP. You can choose to have either 802.1x with static WEP or with dynamic WEP and WPA-EAP to ensure even higher security in your wireless network.

Note: before setting the RADIUS Server, select 802.1x or WPA first in the Security Page.

WDS Mode Page

WDS Mode: In this mode, you can extend the range of a wireless network. Wireless clients can associate with the repeater to communicate with each client on your network. Note that all the Access Points' IP address must be set in the same network and make sure that Channel is set the same for all of your devices. There are three modes in this page: **Disable, Auto WDS and Manual.**



Disable

Auto WDS—Any radio can connect to this radio by WDS link

Manual—Only allows the radio on the flowing MAC address list can connect to this radio by WDS link.

Access Control Page

When configuring the LanPro 802.11g WLAN outdoor radio with AP mode operation, the Access Control is a powerful security feature that allows you to specify which wireless stations are allowed or denied in the list including:

Open: Allows any wireless station to access the network.

Allow: Any wireless station in this list attempting to access the network is allowed.

Deny: Any wireless station in this list will be denied access.

To add the Mac address of each wireless station on your network by entering the Mac address of the client you desire to add into the list. Click **"Add"**, and then **"Apply"** to save the settings. To delete a Mac address from the list, select the Mac address you want to delete by clicking **"Del"** and then **"Apply"** to save the settings.

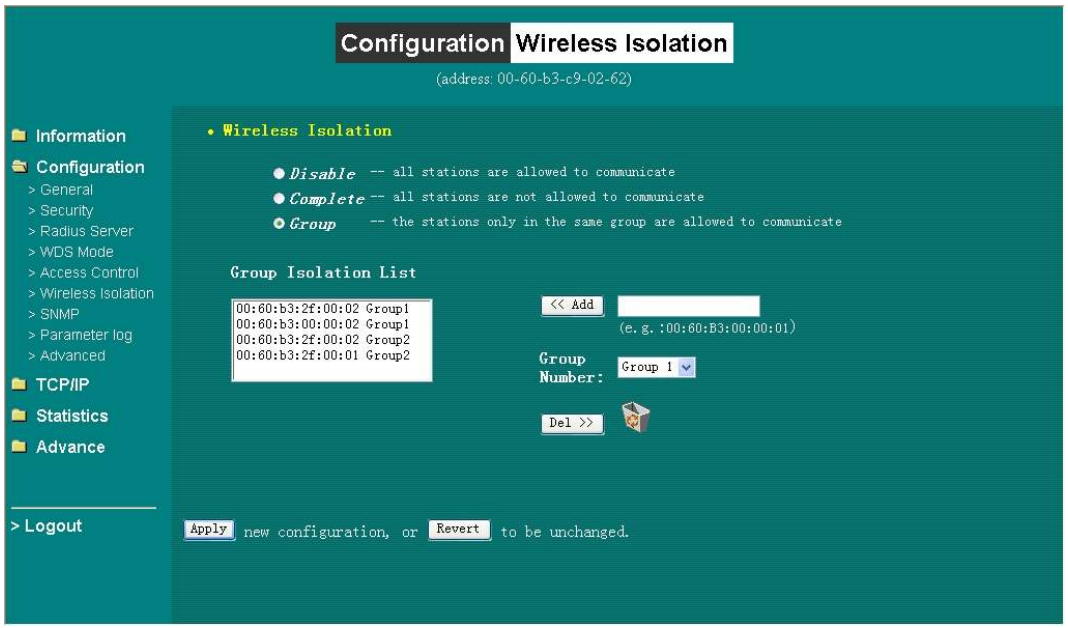
Wireless Isolation Page

Only AP mode is available for the configuration of **"Wireless Isolation"** and **"Hidden AP"**.
Enabling the parameter, the wireless clients will not be able to virtually "see" any others who associated with the same access point. Remark: supposedly there are two clients associated with the same access point, client A and B. In this case, the wireless client A will not be able to talk to the client B in any level of network protocol and vice versa. The function can prohibit users from accessing the unauthorized resources in your wireless network but can't prevent users from accessing your wired network though. To disable the function, the protection on the access point will be also disabled. There are two modes here as below:

Complete: all stations are not allowed to communicate.

Group: the stations only in the same group are allowed to communicate.

When you have done your selection, please press the **"Apply"** button to have the function take effect. The default value is "disable".



IN DEPTH: The function will only refine the efficient isolation on the area of a same BSS. It won't work out the same protection for those clients who associated with different access points (in different BSS). In this case, to adopt virtual LAN may be a wonderful solution.

SNMP Page

Enable SNMP to allow the SNMP network management software to manage the outdoor radio via SNMPv2 protocol.

Trap Server: The IP address of the SNMP manager to receive traps sent from the outdoor radio.

Read-Only Community: Allow the SNMP manager to read only the MIB objects of the outdoor radio. The default setting is "public".

Read-Write Community: Allow the SNMP manager to read/write the MIB objects of the outdoor radio. The default setting is "private".

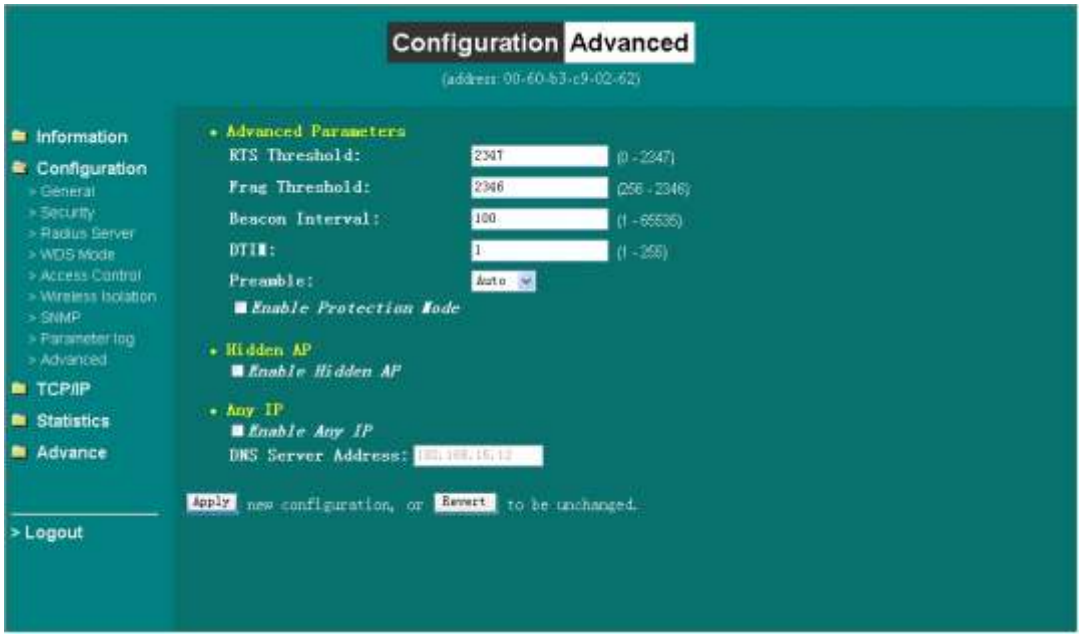
Click "**Apply**" if you make any changes.

Parameter log Page

The Parameter log item allows you to save settings to the local hard drive by clicking **"Save"**. When you click the **"Browse"** button, you can select the saved setting files. To click **"Load"**, the saved settings will be loaded back.

Advanced Page

The LanPro Advanced page lets you set Parameters for the outdoor radio such as, RTS Threshold, Frag Threshold, Beacon Interval, DTIM, and Preamble.



RTS Threshold: RTS Threshold is a mechanism implemented to prevent the “Hidden Node” problem. If the size of the packet transmitted is larger than the value you set, the RTS will be enabled. When the RTS is activated, the station and its Access Point will use a (RTS/CTS) mechanism for data transmission. The setting range is 0-2347.

Frag Threshold: LanPro Fragmentation mechanism is used for improving the efficiency when there is high traffic within the wireless network. If you transmit large files in a wireless network, you can enable the Fragmentation Threshold and specify the packet size. This specifies the maximum size a data packet will be before splitting and creating a new packet. The setting range is 256-2346. For example: If you set value as 256, it means the packet will be fragmented into “256” bytes while transmitting.

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

Beacon Interval: This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the outdoor radio to keep the network synchronized. A beacon includes the wireless LAN service area, the outdoor radio address, the Broadcast destination addresses, a time stamp, Delivery Traffic

Indicator Maps, and the Traffic Indicator Message (TIM).

Preamble: The Preamble defines the length of the PLCP synchronization field for communication between the Access Point and Network Card. Select the appropriate preamble type and press the Apply button to set it. The default setting is 'Auto'.

Enable Protection: If enabled, the system will send out RTS/CTS packet from the outdoor radio.

Hidden AP: Only AP mode is available for the configuration of **“Wireless Isolation”** and **“Hidden AP”**. Enabling the function, the AP will stop processing the connecting request of the clients (in active scan mode) who aren't aware of the identity (SSID) of the wireless network (AP). In the case, the identity (SSID) must be given for a successful access to your network in advance. When you have done your selection, please press the “Apply” button to have the function take effect. The default value is “disable”.

> **IN DEPTH: The hidden function can bring up a natural protection that wireless standard naturally introduced, to implement it will be able to prohibit access point from responding the connecting request of the client who carries the known SSID. The protection is very preliminary and can setup a basic secured network in parallel with access control and WEP security.**

Click “**Apply**” if you make any changes.

3-1-4 TCP/IP

You may assign a proper IP address to your 802.11g WLAN outdoor radio manually. If you would like the 802.11g WLAN outdoor radio to obtain the IP address from the DHCP server on your network automatically, enable the DHCP client function.

Click the **"Apply"** button to make it effect. The default IP Address is 192.168.1.2.

3-1-5 Statistics

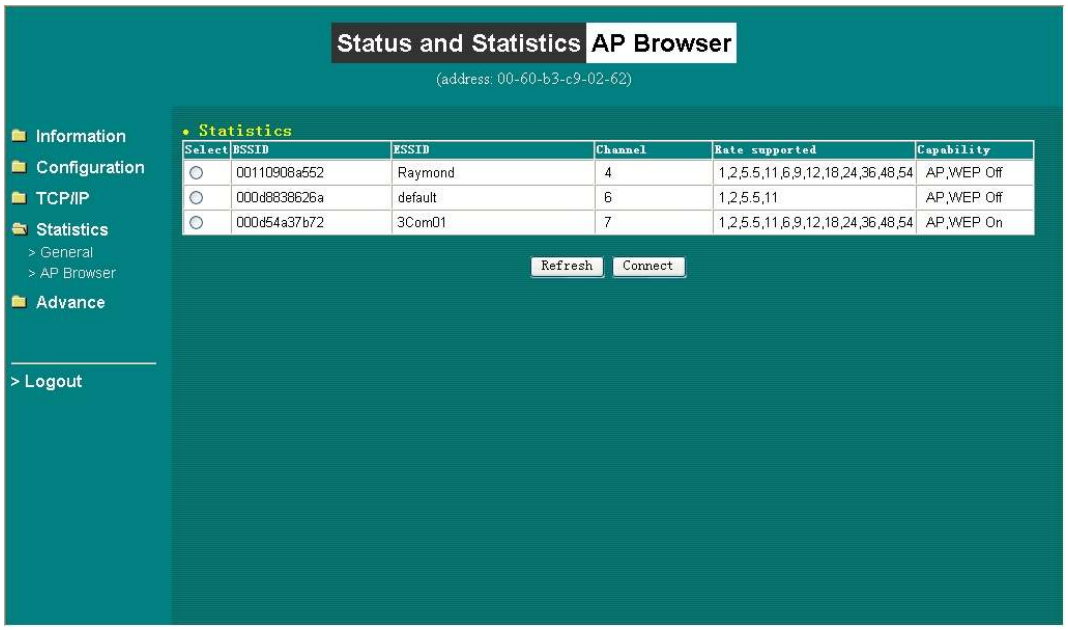
This item will allow you to monitor the connection status when set to AP mode such as the Mac Address, Link Status, Rate Type as well as RX/TX from Ethernet packets.

General Page

When set to station mode, you may also open the **General** page to view the available Access Points around your environment. The status includes Link Status, ESSID, BSSID, Channel and Signal as well as RX/TX from Ethernet packets.

AP Browser Page

This LanPro AP Browser shows only when configuring your 802.11g WLAN outdoor radio as Station mode. By clicking the **"Refresh"** button, the AP Browser will reload and display available Access Points around the working environment. Besides showing the BSSID of each Access Point, it also displays ESSID, Channel, Support Rate and Capability. To connect one of displayed Access Points, just select the Access Point you desire and then click the **"Connect"** button to make the connection.



3-1-6 Advance

Firmware upgrade Page

Here, you can upload the latest firmware of the LanPro 802.11g WLAN outdoor radio. You may either enter the file name in the entry field or browse the file by clicking the **"Browse"** button. Then click the **"Apply"** button to begin to upgrade the new firmware.

Password Change Page

Here allow you to change the LanPro outdoor radio's password. Changing password for the outdoor radio is as easy as typing the password into the New Password field. Then, type it again into the Confirm Change Field to confirm. Click the **"Apply"** button to save the setting.

Note: After you change password, please take note of your new password. Otherwise, you will not able to access the Wireless Access Point setup. If you forget the password, you could pressing the Reset button on the back panel of your WLAN outdoor Radio for at least 3 second – and all previous configurations will need to be input again.

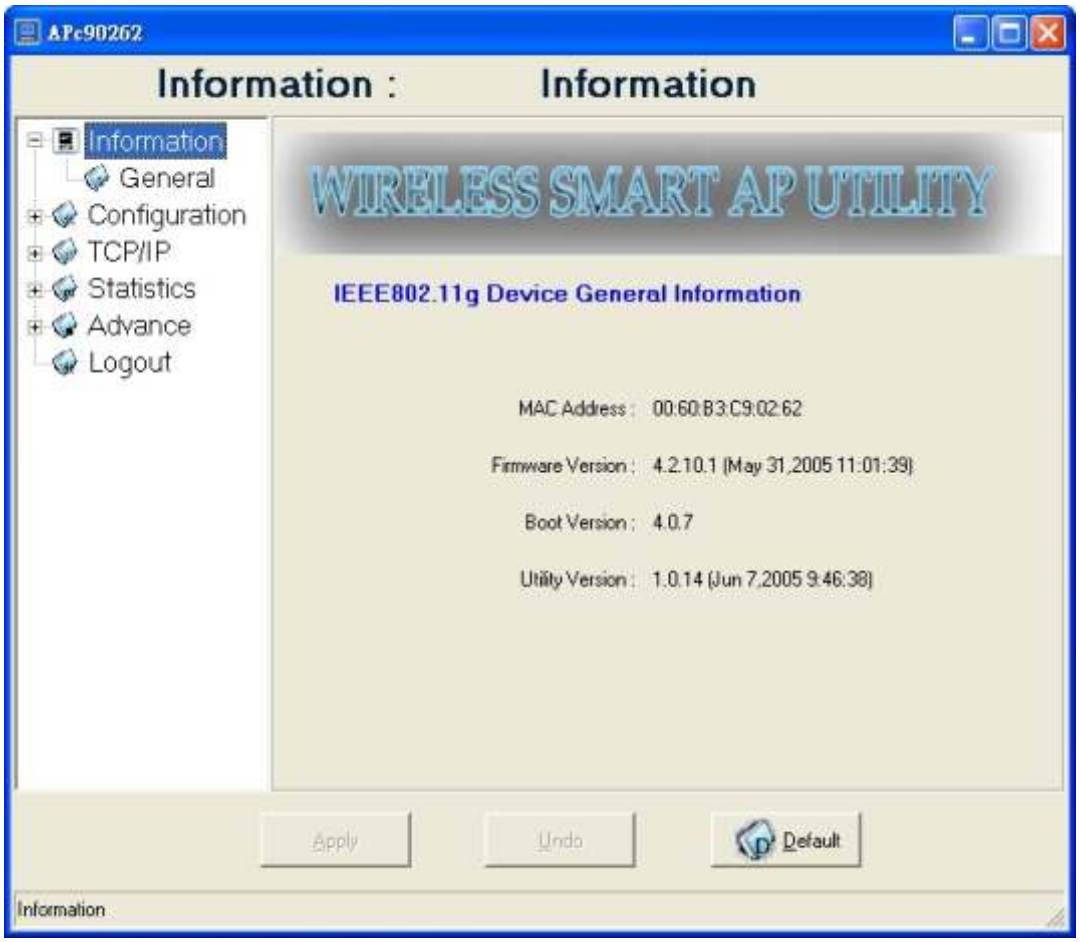
3-2 Using the Smart Utility

Install the LP993 802.11g WALN outdoor Radio on your Windows 95/98/NT/ME/2000 desktop computer, the Windows-based utility **"Wireless Smart AP Utility"** provides an easy-setup interface. The smart Utility enables you to configure your 802.11g WLAN outdoor radio on the network more easily than ever before, especially when you don't know the IP address of the radio. The following gives instructions guiding you through the installations of the Outdoor Radio Utility. All the configurations are almost the same as via the Web.

1. Insert the Installation CD that came with your LP993 product kit into the corresponding drive on your computer.
2. Go to the 802.11g / Wireless Smart AP utility folder and click **Setup.exe**. The installation screen will show up Click **Next** to continue.
3. Follow the on-screen instructions to install the Smart Utility.
4. Upon completion, go to start menu and execute the Wireless Utility. It will begin to browse the 802.11g WLAN outdoor radio on the network.

5. Double-click the icon to access the property dialog box. Enter the password in the entry field. The default password is **"default"** .

5 After entering the correct password, a main window appears. You will see the basic information of the 802.11g WLAN outdoor radio, such as MAC Address, Firmware, Boot and Utility version.



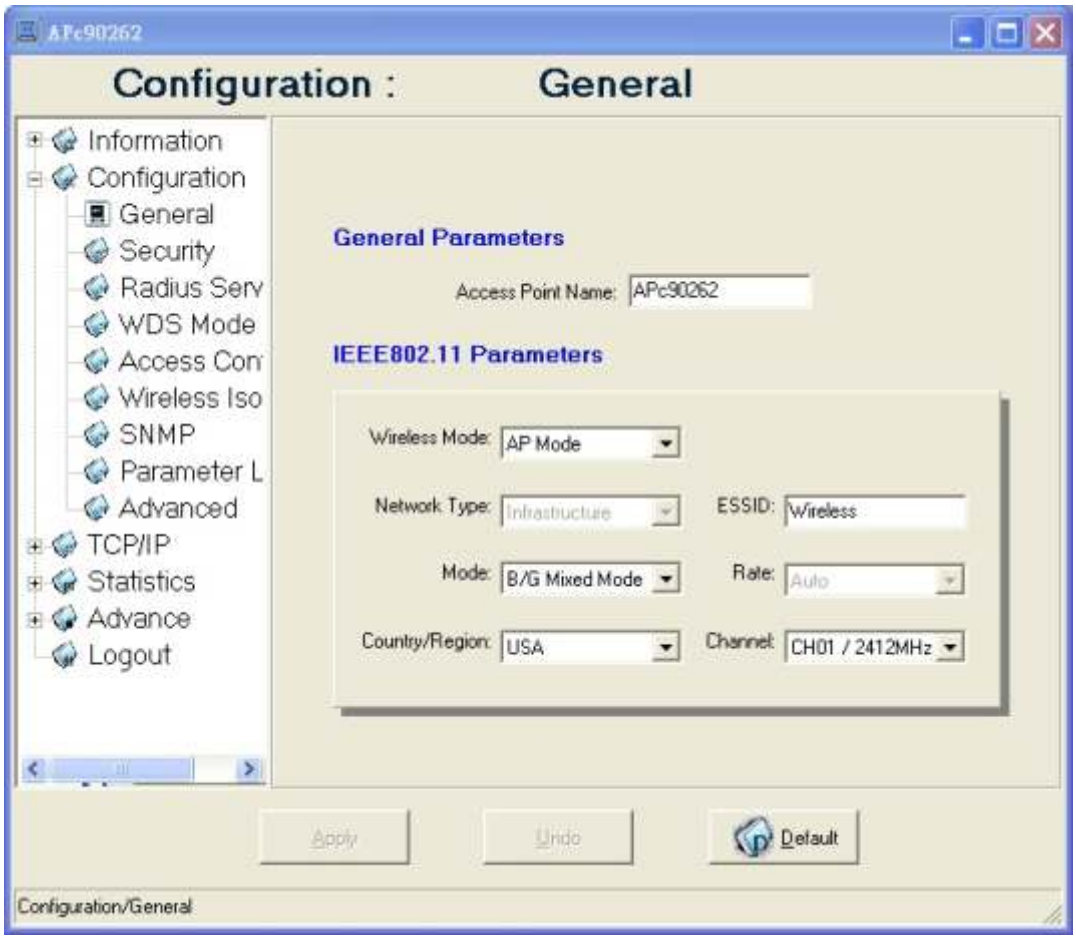
MAC Address: It is a hardware identification number that distinguishes the unit from others.

Firmware Version: Displays the firmware version that is equipped with your hardware.

3-2-1 Configuration

General

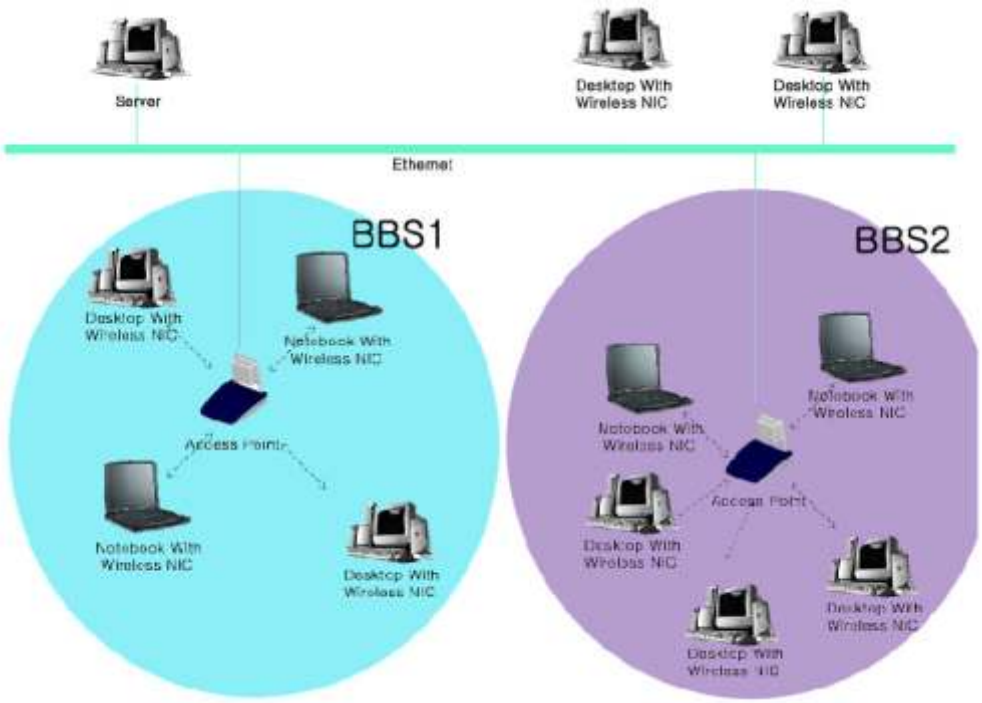
You may make the settings on your 802.11g WLAN outdoor radio such as Access Point Name, Wireless Mode, Network Type, ESSID, Rate, Country/Region and Channel.



Access Point Name: In this field, you may enter any name. This will enable you to manage your 802.11g WLAN outdoor radio more easily if you have many 802.11g WLAN outdoor radios on the network. Besides, **Access Point Name** can be used to prevent you from forgetting an IP Address and fail to access the website. Try to type the nickname you like to identify the website, then press the button of **"Apply"** to reboot.

- **Wireless Mode: The default wireless operating mode of the 802.11g WLAN outdoor radio is Access Point (AP) mode. To switch to Station mode, select the desired mode from the down-arrow menu. Click Apply. The board will reboot into the desired mode**

- **.AP Mode: The system can be configured to work as a wireless network access point. Note that the 802.11g WLAN outdoor radio acts only as a layer 2 bridge and does not act as a DHCP server. In other words, it does not supply dynamic IP addresses and instead relies on the network to supply them. The implementation can be shown as below:**



Station Mode: When configuring as a station mode, the device is now acting as a wireless client. The 802.11g WLAN outdoor radio will associate to an AP within its range in infrastructure mode, or join with another device in Client mode in an ad-hoc network.

Network Type: There are 2 network types for the wireless station adapter to operate. If you need to access company network or Internet via Access Point, select "**Infrastructure**". To set up a group of wireless stations for files and printer sharing, select "**Ad-Hoc**" (without Access Point). For **Ad-Hoc** operation, the *same ESSID* is required to set for the wireless stations.

ESSID: The ESSID is a unique ID used by Access Points and Stations to identify a wireless LAN. Wireless clients associating to any Access Point must have the same ESSID. The default ESSID is ANY. The ESSID can have up to 32 characters.

Channel: Select a clear and available channel as an operational channel for your wireless station adapter when it performs as Ad-Hoc mode or AP with repeating mode.

Mode: There are three different wireless modes to operate, "B Only Mode", "G Only Mode", and "B/G Mixed Mode". In B/G Mixed Mode, the wireless station adapter is compatible with a mix of both 802.11g and 802.11b clients. You will see that the factory-set default "B/G Mixed Mode" will prove the most efficient. B Only Mode is compatible with 802.11b clients only. This mode can be used only if you do not allow any 802.11g clients to join a network. G Only Mode is compatible with 802.11g clients only. This mode can be used only if you do not allow any 802.11b clients to access to the network. To switch the mode, select the desired mode from the pull-down menu of "**Mode**".

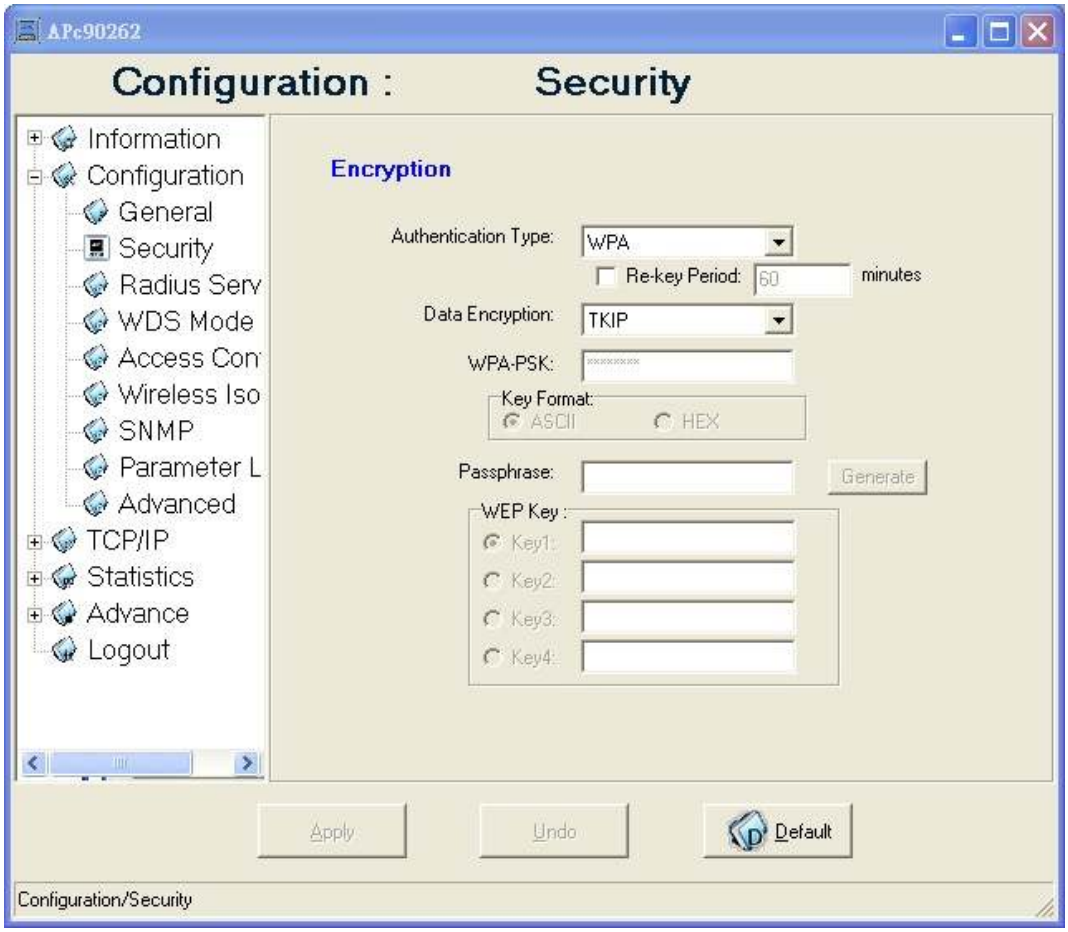
Rate: The wireless station adapter provides various data rate options for you to choose. Data rates options include **Auto, 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48 and 54. The default setting is Auto.**

Country/Region: Allows you to select country domain in case there is any chances that you would use wireless network in other countries. There are a total of 11 countries for you to select. They are Africa, Asia, Australia, Canada, Europe, France, Israel, Japan, Mexico, South America, and USA. Note that if your AP and station adapter are in different standards, please use the **"Country/Region"** item to switch the standards of the station adapter (For example, when set to client mode, if your Access Point is America standard but your station adapter is Japanese standard, you can pull down the **"Country/Region"** option to switch your station adapter from Japanese standard to American standard.). As long as you change the country domain, the channel will switch to correspond with the country you changed.

Click **"Apply"** if you have made any changes.

Security

Various encryption and authentication build highly security mechanism for this 802.11g radio, such as WEP, WPA-PSK, WPA, 802.1x…etc.



Data encryption: This 802.11g WLAN outdoor radio allows you to create up to 2 data encryption keys to secure your data from being eavesdropping by unauthorized wireless users. To enable the encryption, all devices on the network must share the same WEP key.

Disable: Allows the wireless station to communicate with the Access Point without any data encryption.

WEP40: Requires the wireless station adapter to use data encryption with 40-bit algorithm when communicating with the Access Point.

WEP128: Allows the wireless station adapter to communicate with the Access Point with data 128-bit encryption algorithm.

For 40-bit encryption you may choose:

ASCII: *Enter **5 characters*** (case sensitive) ranging from "a-z", "A-Z" and "0-9" (e.g. **MyKey**).

Hex: Alternatively, you may enter **10 *hexadecimal digits*** in the range of "A-F", "a-f" and "0-9" (e.g. **11AA22BB33**).

For 128-bit encryption you may choose:

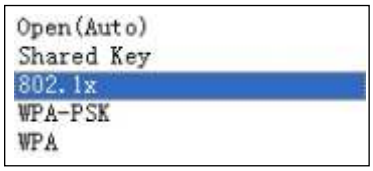
ASCII: *Enter **13 characters*** (case sensitive) ranging from "a-z", "A-Z" and "0-9" (e.g. **MyKey12345678**).

Hex: Alternatively, you may enter **26 *hexadecimal digits*** in the range of "A-F", "a-f" and "0-9" (e.g. **00112233445566778899AABBCC**).

After entering the WEP keys in the key field, select one key as active key.

Alternatively, you may create encryption keys automatically by using Passphrase. From the Passphrase field, type a character string and click "**Generate**". As you type, the 802.11g WLAN outdoor radio will use an algorithm to generate 4 keys automatically. Select one key from the 4 WEP keys.

Network authentication: Moreover, the 802.11g WLAN outdoor radio provides five types of authentication services: Open System (Auto), Shared Key, 802.1x, WPA-PSK and WPA.



Open (Auto)：The default authentication type is Open System (Auto), requires no authentication since it allows any device to join a network without performing any security check.

Shared Key: If you require higher security for wireless access, you may select Shared Key. Note that when Shared Key is selected, a WEP key is required and must be the same between the Access Point and client.

802.1x: The 802.1x authentication (EAP) is designed to enhance the security of wireless networks. The 802.1x provides an authentication framework for wireless LANs, allowing a user to be authenticated by a central authority. For wireless LANs, it also provides centralized, server-based authentication of end users. The standard is flexible enough to allow multiple authentication algorithms, and because it is an open standard, multiple vendors can innovate and offer enhancements.

For wireless LANs, the 802.1x authentication has three main components: The supplicant (usually the client software, such as zero configuration in window XP), the authenticator (usually the access point), and the authentication server (usually a Remote Authentication Dial-In User Service server, although RADIUS although 802.1X does not specify it).

The advanced security describes how to control authorized access to the Access Point with Remote Authentication Dial-In User Service (RADIUS). To enable 802.1x based authentication, please select 802.1x. Moreover, you may enable the radius account function by check Enable Radius Account in the check box. To configure the Authentication and Account Server function, the parameter of Radius Authentication Server and Radius Account Server must set to the same with the Authentication Server and Account Server.

Note: The Password is up to 16 bytes.

Otherwise, you may select disable auth mode that adjusts to the 802.11 legacy network.

For setting 802.1x Based Auth:

1. Enable 802.1x by clicking the “802.1x Based Auth” radio button.
2. Configure the IP address and port number and set the parameters the same as RADIUS server. (Default port number is 1812)
3. Configure the password and set it the same as RADIUS server. (Security key)
4. Enable the Radius Account when you needed to use Radius account service. (Default port number is 1813)
5. You can also configure the 802.1x parameters through web-based management.
6. On the client side, you'll need to set the security setting, as well as the authentication method (MD5/TLS is supported by Windows XP) , user name, password or certificate. For detail setting, you can refer to documentation of windows XP.

WPA-PSK: Allows the wireless station adapter to communicate with the Access Point with a more secure data protection than the WEP. Here you can select the WPA with PSK mode to improve the data security and privacy during wireless transmission. The present WPA supplied with this 802.11g WLAN outdoor radio is used in a pre-shared key mode, which does not require an authentication (Radius) server.

For WPA-PSK mode you may choose:

In the WPA-PSK field, you may input 8-63 characters ranging from “a-z”, “A-Z” and “0-9”. If you require that access to the Internet or other wireless network services are allowed only when the pre-shared key of the 802.11g WLAN outdoor radio matches that of the device you want to communicate.

WPA (Wi-Fi Protected Access): Currently one of the highest levels of security a wireless network can achieve. Wi-Fi Protected Access is a subset of the security specification and has been introduced as an interim solution for most known security weaknesses in relation to plain WEP. TKIP, the successor to WEP, includes enhancements that eliminate the known vulnerabilities of WEP. Enterprises that already have RADIUS authentication in place can use WPA with 802.1x (WPA-EAP / Enterprise Mode). Small business and home wireless LAN can use WPA without 802.1x (WPA-PSK / Pre-Shared Key).

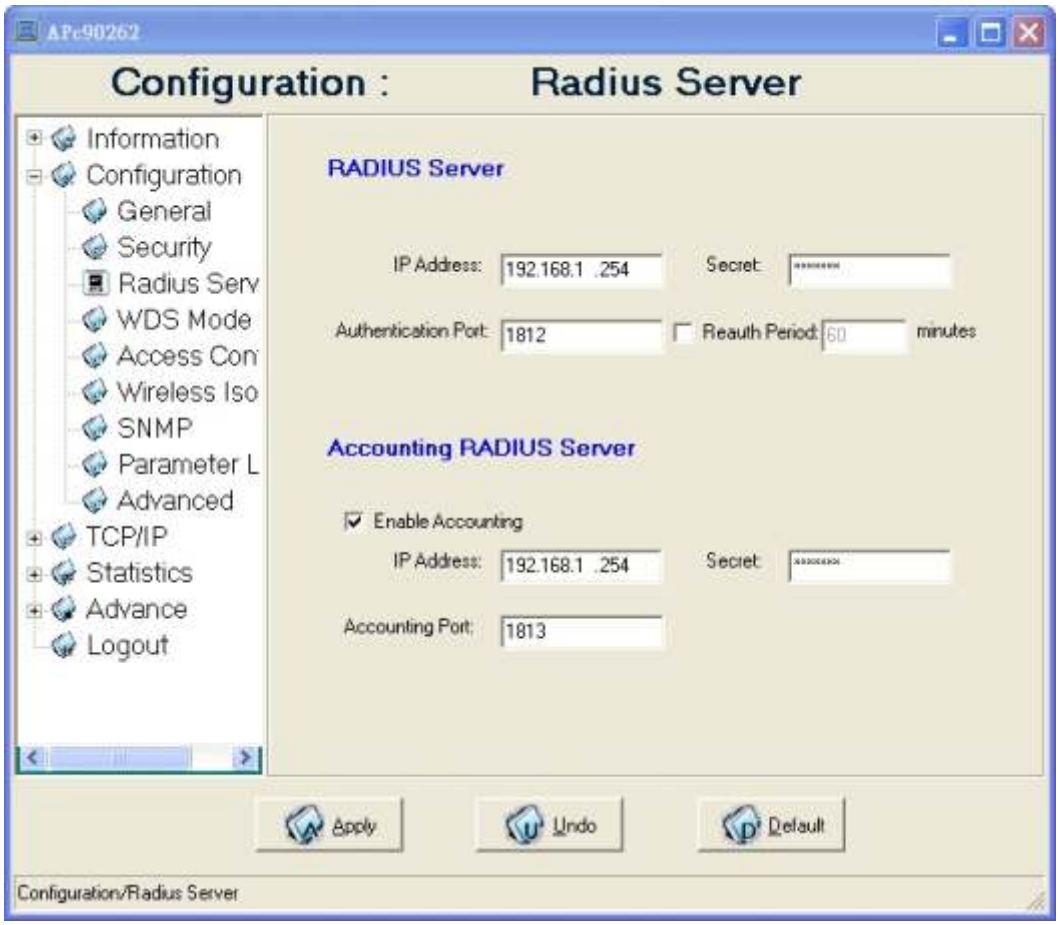
In cooperation with RADIUS, systems with WPA-EAP will be used with a new encryption method called Temporal Key Integrity Protocol (TKIP) implementation with 802.1x dynamic key exchange.

Note:

1. **Supports AES (Advanced Encryption Standard) in WPA-PSK and WPA mode.**
2. **When the radio is set to be station mode, 802.1x and WPA are not available.**

Click the **“Apply”** button on the Configuration tab to make the setting take effect.

Radius Server



RADIUS (Remote Authentication Dial-In User Service) plays a central role in the network to provide the capabilities of authenticating, authorizing, accounting, auditing and alarming…etc and allows an organization to maintain user profiles in a central database that all remote servers can share. Since RADIUS is relatively complex to explain, we will focus here on how it acts as an 802.1x authentication server (EAP-aware RADIUS) and assists in enhancing security.

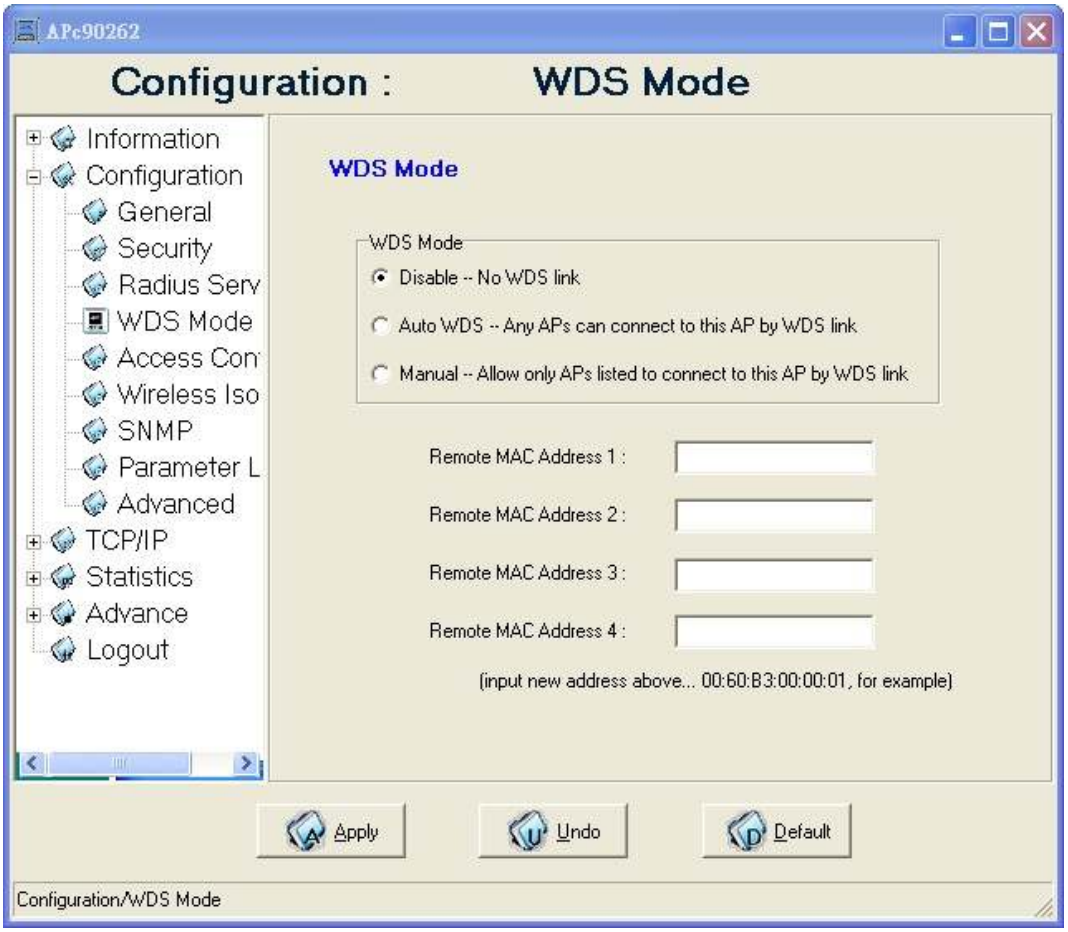
RADIUS performs the authentication function required to check the credentials of users and intermediate Access Points and indicates whether the users are authorized to access the Access Points. Enabling RADIUS is therefore the first step toward building up an 802.1x-capable environment. Even more, it is also a must-do to accommodate the recently introduced Wi-Fi protected access (WPA-EAP) to wireless networks.

Setting up RADIUS information in your Access Point is quite simple; just input the IP address of the RADIUS server and its port number, which is usually set to 1812, as well as the secret key, which is identified with the given key in RADIUS. Press **"Apply"** to apply the settings.
When you finish adding RADIUS information, return to the Security page, where you will be allowed to continue configuring 802.1x and WPA-EAP. You can choose to have either 802.1x with static WEP or with dynamic WEP and WPA-EAP to ensure even higher security in your wireless network.

Note: before setting the RADIUS Server, select 802.1x or WPA first in the Security Page.

WDS Mode

WDS Mode: In this mode, you can extend the range of a wireless network. Wireless clients can associate with the repeater to communicate with each client on your network. Note that all the Access Points' IP address must be set in the same network and make sure that Channel is set the same for all of your devices. There are three modes in this page: **Disable, Auto WDS** and **Manual.**



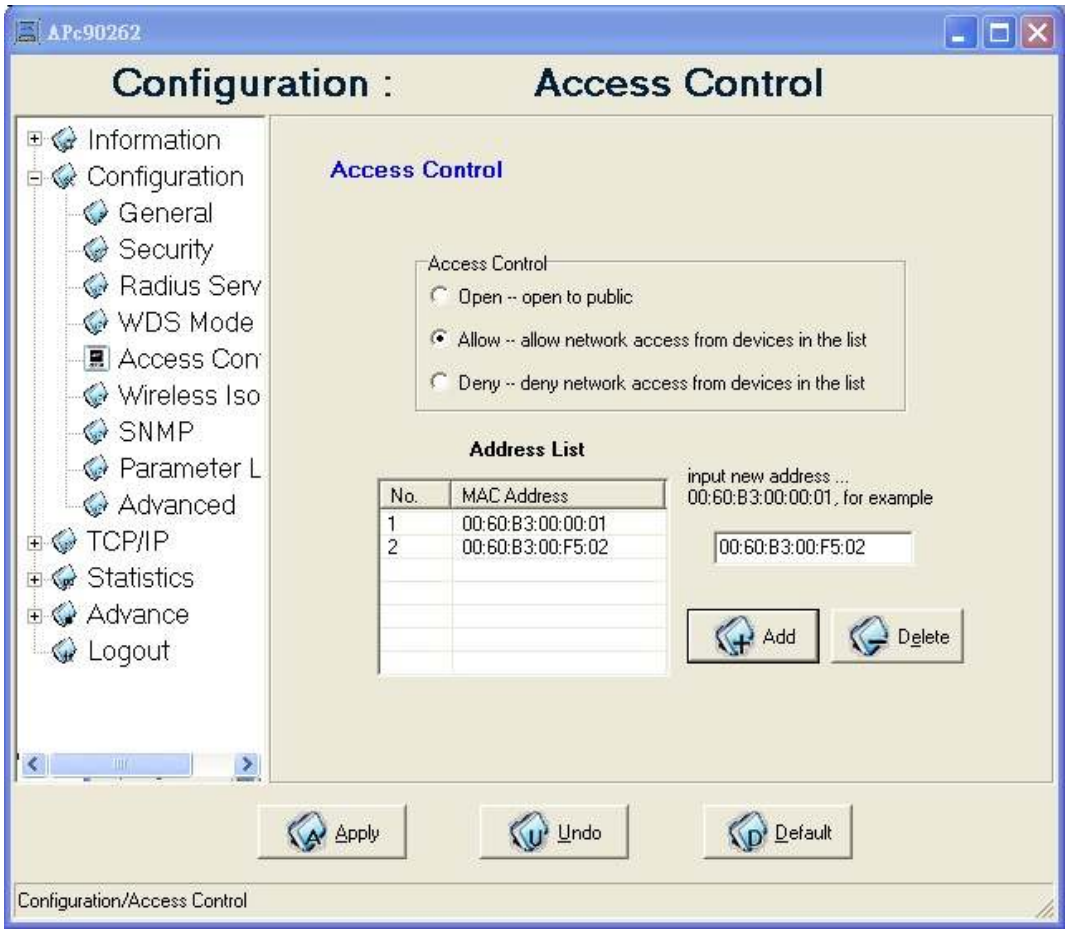
Disable

Auto WDS—Any radio can connect to this radio by WDS link

Manual—Only allows the radio on the flowing MAC address list can connect to this radio by WDS link.

Access Control

When configuring the LP993 802.11g WLAN outdoor radio with AP mode operation, the Access Control is a powerful security feature that allows you to specify which wireless stations are allowed or denied in the list including:



Open: Allows any wireless station to access the network.

Allow: Any wireless station in this list attempting to access the network is allowed.

Deny: Any wireless station in this list will be denied access.

To add the Mac address of each wireless station on your network by entering the Mac address of the client you desire to add into the list. Click **"Add"**, and then **"Apply"** to save the settings. To delete a Mac address from the list, select the Mac address you want to delete by clicking **"Del"** and then **"Apply"** to save the settings.

Wireless Isolation

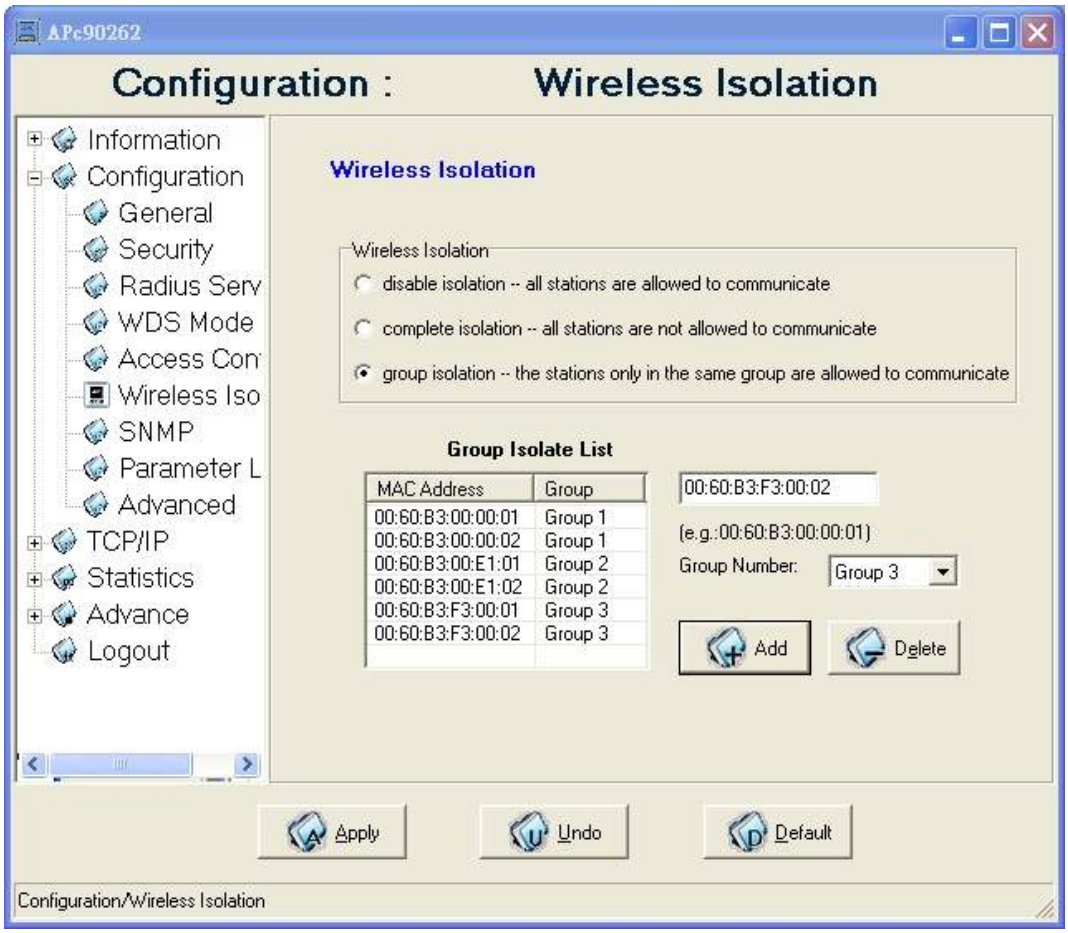
Only AP mode is available for the configuration of **"Wireless Isolation"** and **"Hidden AP"**.
Enabling the parameter, the wireless clients will not be able to virtually "see" any others who associated with

the same access point. Remark: supposedly there are two clients associated with the same access point, client A and B. In this case, the wireless client A will not be able to talk to the client B in any level of network protocol and vice versa. The function can prohibit users from accessing the unauthorized resources in your wireless network but can't prevent users from accessing your wired network though. To disable the function, the protection on the access point will be also disabled. There are two modes here as below:

Complete: all stations are not allowed to communicate.

Group: the stations only in the same group are allowed to communicate.

When you have done your selection, please press the **"Apply"** button to have the function take effect. The default value is "disable".

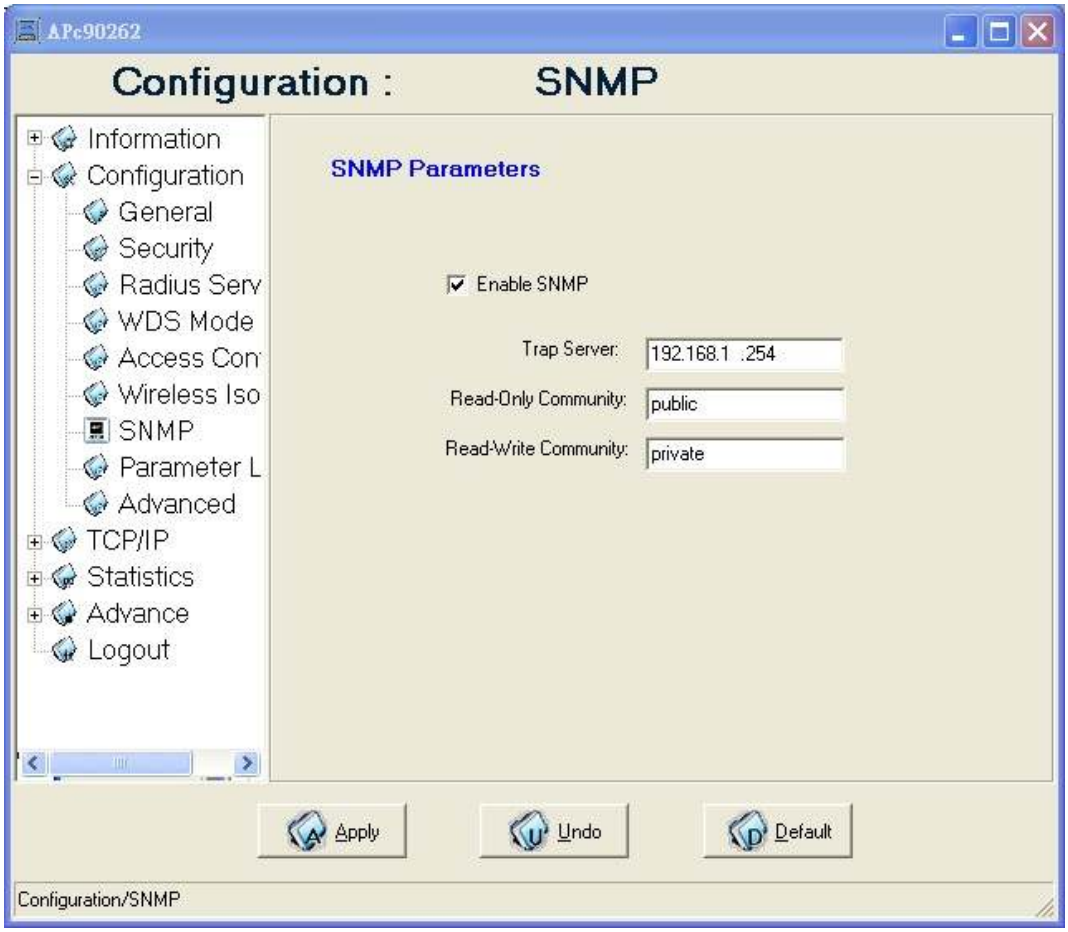


IN DEPTH: The function will only refine the efficient isolation on the area of a same BSS. It won't work out

the same protection for those clients who associated with different access points (in different BSS). In this case, to adopt virtual LAN may be a wonderful solution.

SNMP

Enable SNMP to allow the SNMP network management software to manage the outdoor radio via SNMPv2 protocol.



Trap Server: The IP address of the SNMP manager to receive traps sent from the outdoor radio.

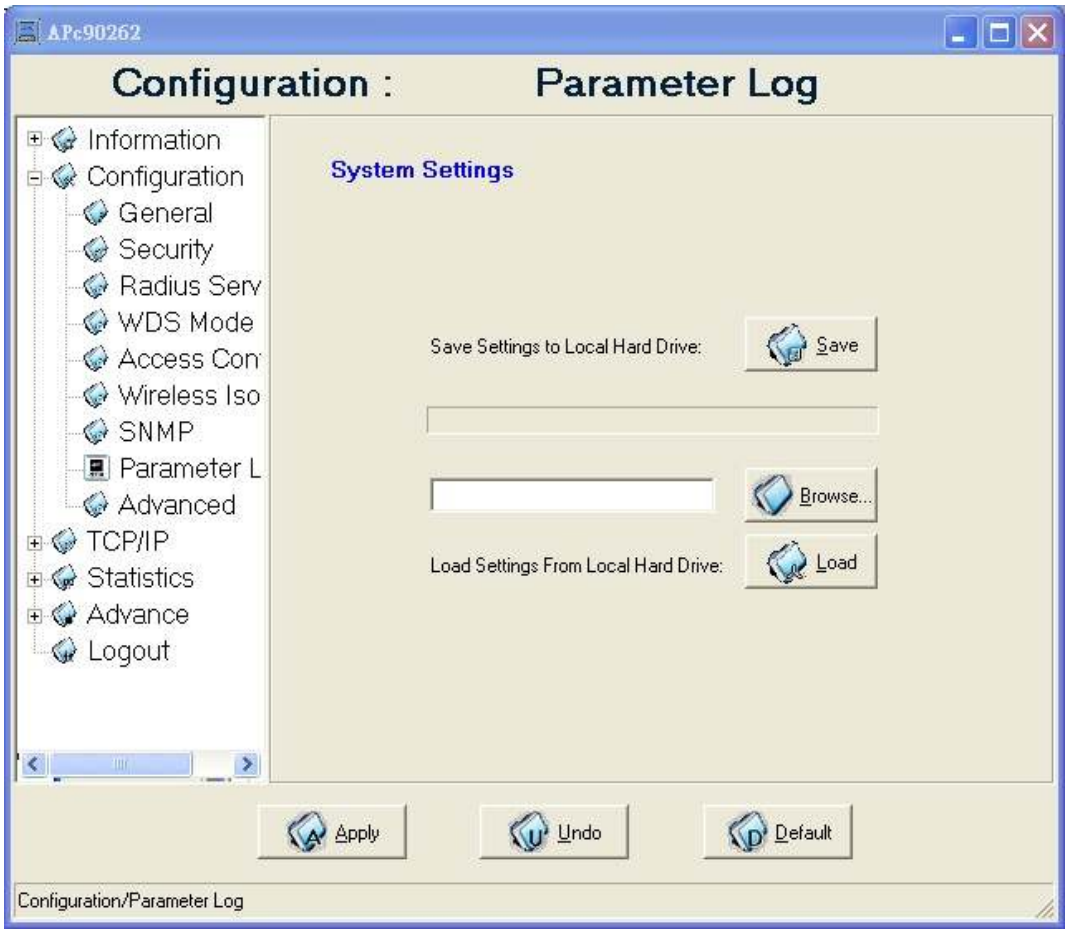
Read-Only Community: Allow the SNMP manager to read only the MIB objects of the outdoor radio. The default setting is "public".

Read-Write Community: Allow the SNMP manager to read/write the MIB objects of the outdoor radio. The default setting is "private".

Click "**Apply**" if you make any changes.

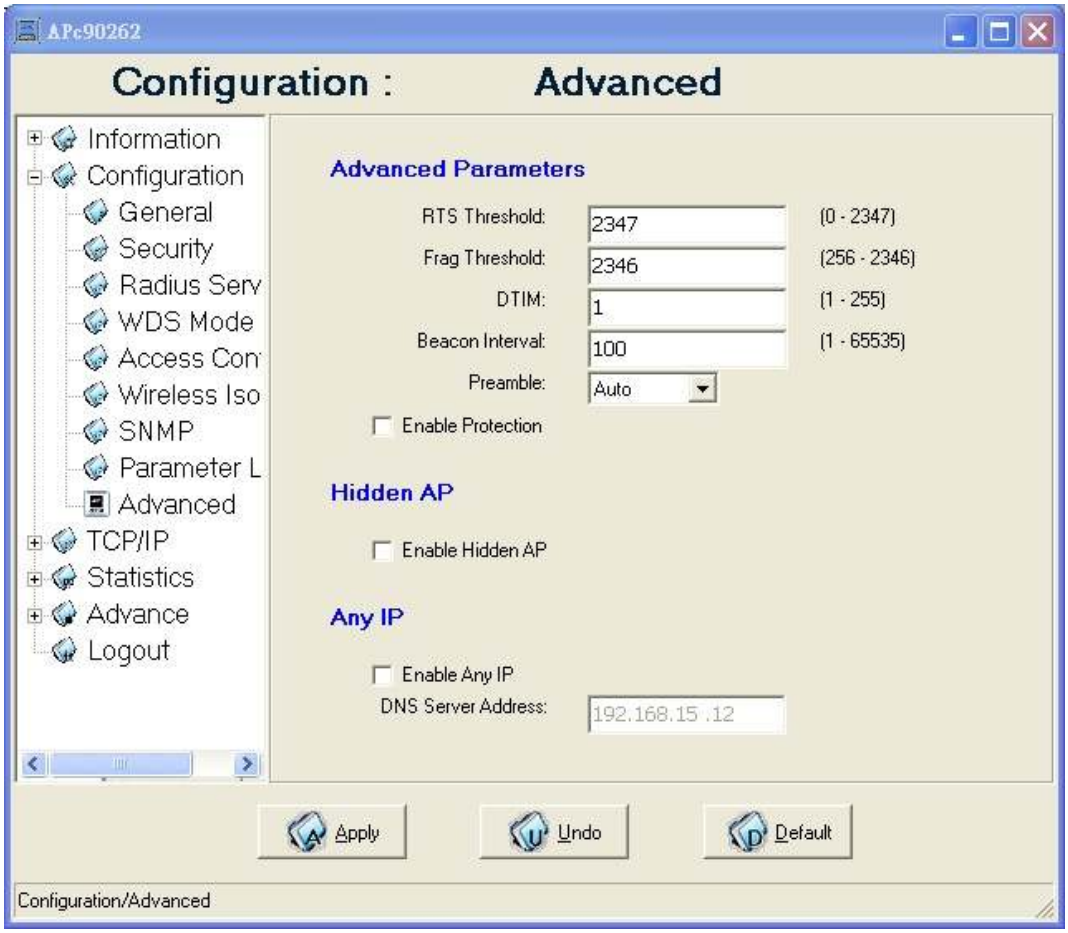
Parameter log

The Parameter log item allows you to save settings to the local hard drive by clicking **"Save"**. When you click the **"Browse"** button, you can select the saved setting files. To click **"Load"**, the saved settings will be loaded back.



Advanced

The Advanced page lets you set Parameters for the outdoor radio such as, RTS Threshold, Frag Threshold, Beacon Interval, DTIM, and Preamble.



RTS Threshold: RTS Threshold is a mechanism implemented to prevent the "Hidden Node" problem. If the size of the packet transmitted is larger than the value you set, the RTS will be enabled. When the RTS is activated, the station and its Access Point will use a (RTS/CTS) mechanism for data transmission. The setting range is 0-2347.

Frag Threshold: Fragmentation mechanism is used for improving the efficiency when there is high traffic within the wireless network. If you transmit large files in a wireless network, you can enable the Fragmentation Threshold and specify the packet size. This specifies the maximum size a data packet will be before splitting and creating a new packet. The setting range is 256-2346. For example: If you set value as 256, it means the packet will be fragmented into "256" bytes while transmitting.

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

Beacon Interval: This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the outdoor radio to keep the network synchronized. A beacon includes the wireless LAN service area, the outdoor radio address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

Preamble: The Preamble defines the length of the PLCP synchronization field for communication between the Access Point and Network Card. Select the appropriate preamble type and press the Apply button to set it. The default setting is 'Auto'.

Enable Protection: If enabled, the system will send out RTS/CTS packet from the outdoor radio.

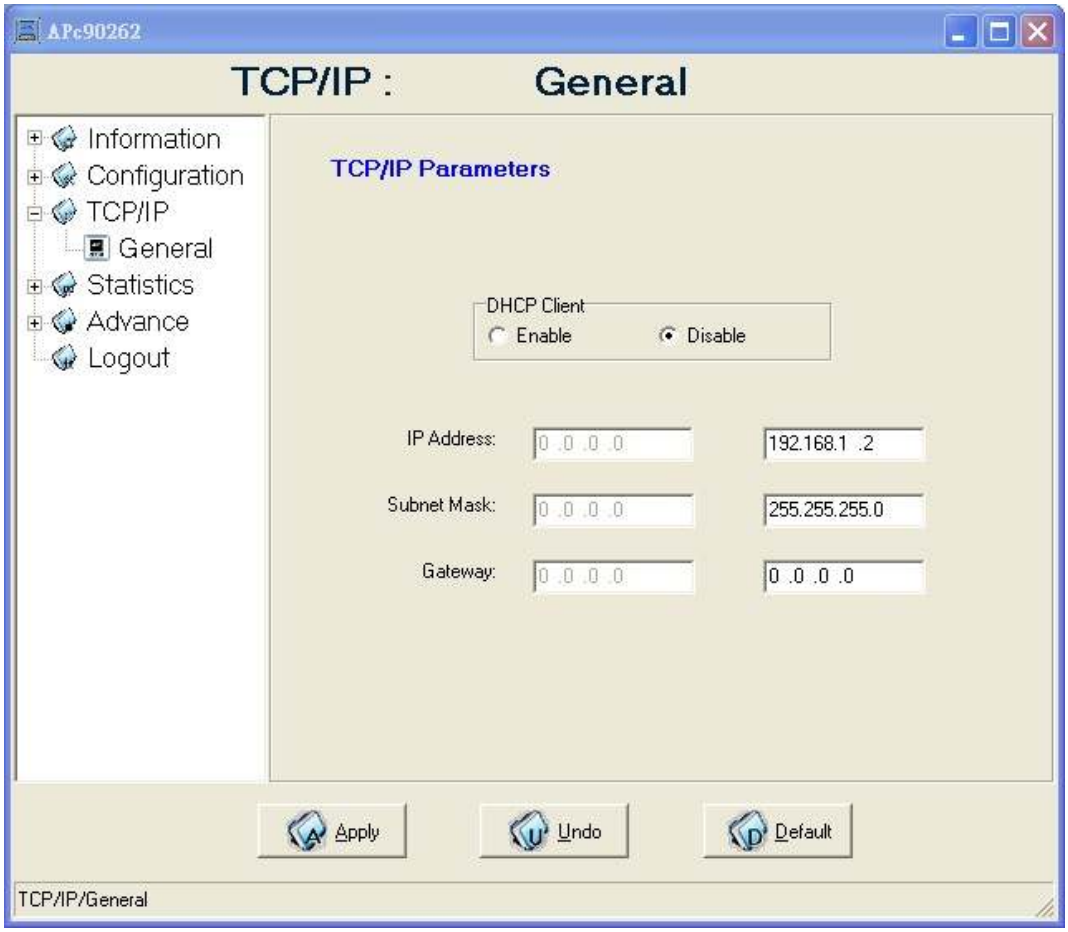
Hidden AP: Only AP mode is available for the configuration of **"Wireless Isolation"** and **"Hidden AP"**. Enabling the function, the AP will stop processing the connecting request of the clients (in active scan mode) who aren't aware of the identity (SSID) of the wireless network (AP). In the case, the identity (SSID) must be given for a successful access to your network in advance. When you have done your selection, please press the "Apply" button to have the function take effect. The default value is "disable".

> **IN DEPTH: The hidden function can bring up a natural protection that wireless standard naturally introduced, to implement it will be able to prohibit access point from responding the connecting request of the client who carries the known SSID. The protection is very preliminary and can setup a basic secured network in parallel with access control and WEP security.**

Click "**Apply**" if you make any changes.

3-2-2 TCP/IP

You may assign a proper IP address to your LP993 802.11g WLAN outdoor radio manually. If you would like the 802.11g WLAN outdoor radio to obtain the IP address from the DHCP server on your network automatically, enable the DHCP client function.



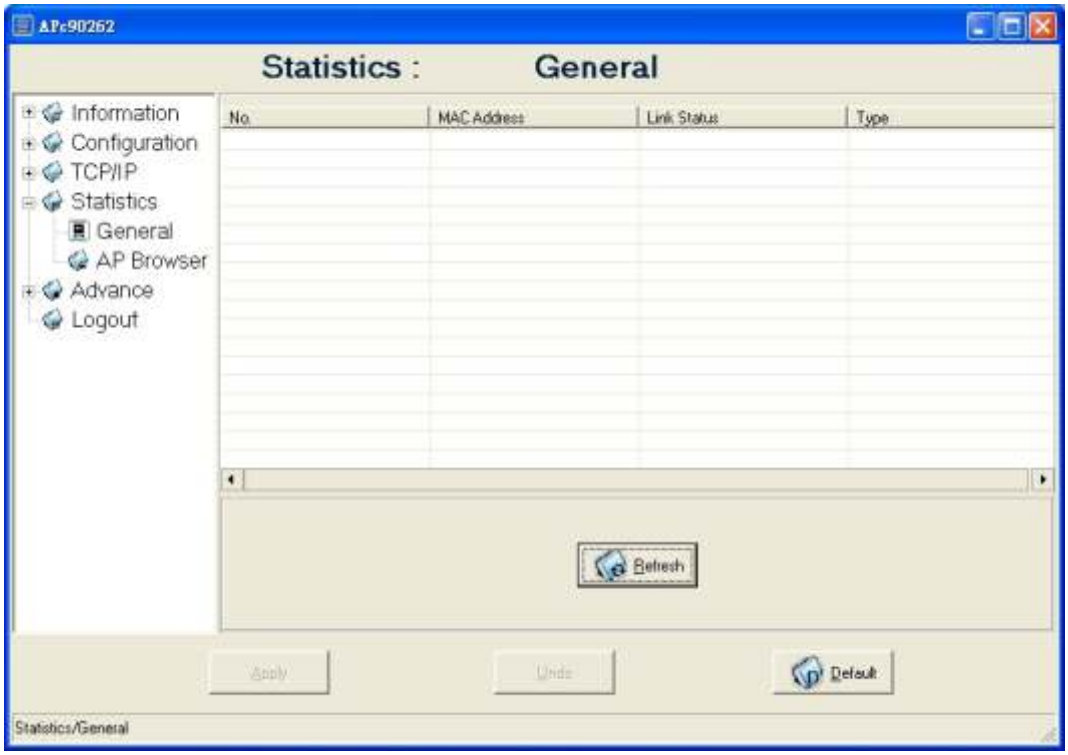
Click the **"Apply"** button to make it effect. The default IP Address is 192.168.1.2.

3-2-3 Statistics

This item will allow you to monitor the connection status when set to AP mode such as the Mac Address, Link Status, Rate Type as well as RX/TX from Ethernet packets.

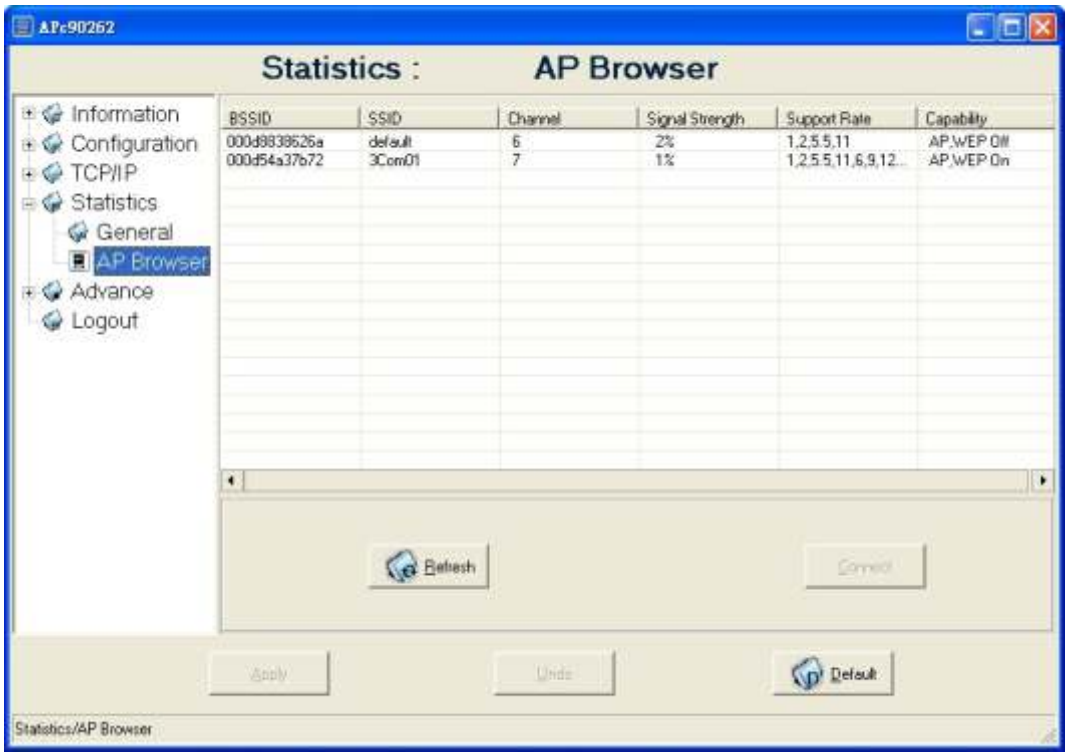
General

When set to station mode, you may also open the General page to view the available Access Points around your environment. The status includes Link Status, ESSID, BSSID, Channel and Signal as well as RX/TX from Ethernet packets



AP Browser

This LP993 LanPro AP Browser shows only when configuring your 802.11g WLAN outdoor radio as Station mode. By clicking the **"Refresh"** button, the AP Browser will reload and display available Access Points around the working environment. Besides showing the BSSID of each Access Point, it also displays ESSID, Channel, Support Rate and Capability. To connect one of displayed Access Points, just select the Access Point you desire and then click the **"Connect"** button to make the connection.

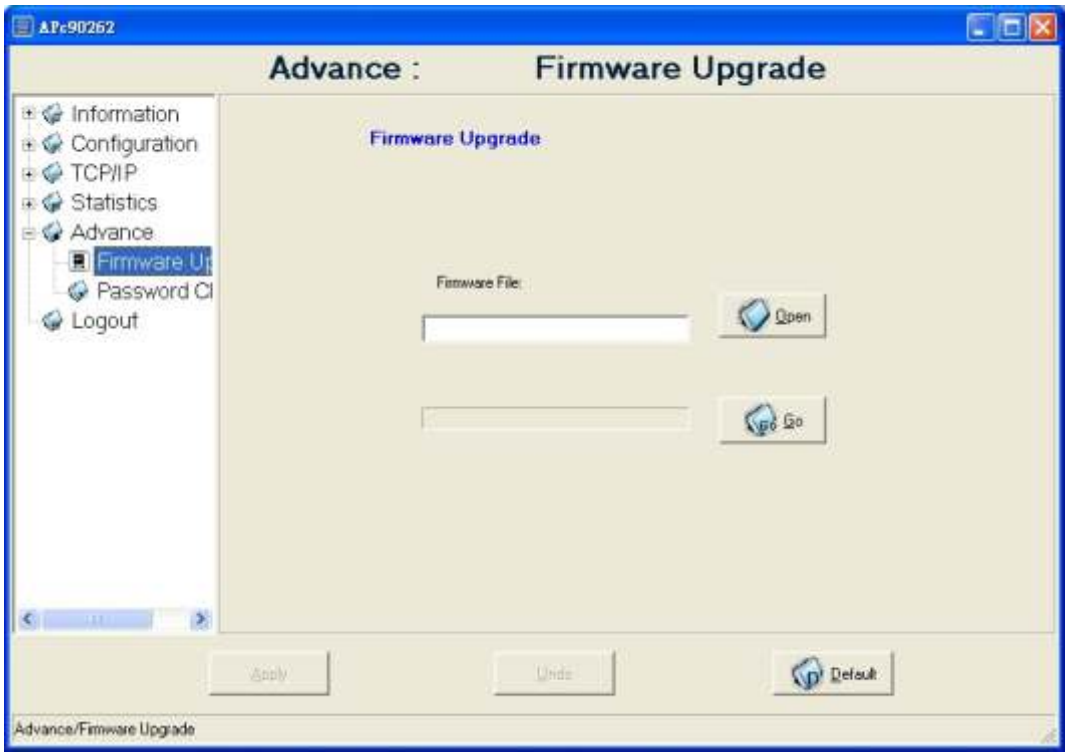


3-2-4 Advanced

This item is used for uploading the newest firmware of the 802.11g WLAN outdoor radio. You may either enter the file name in the entry field or browse the file by clicking the "**Open**" button and then click "**Go**" to run the upgrading. For information about the release of the newest firmware, please contact your local reseller.

Firmware Upgrade:

This item is used for uploading the newest firmware of the Outdoor Radio. You may either enter the file name in the entry field or browse the file by clicking the "Open" button and then click "Go" to run the upgrading. For information about the release of the newest firmware, please contact your local reseller.



Password Change:

Here allow you to change the outdoor LP993 radio's password. Changing password for the outdoor radio is as easy as typing the password into the New Password field. Then, type it again into the Confirm Change Field to confirm. Click the “Apply” button to save the setting.

Note: After you change password, please take note of your new password. Otherwise, you will not able to access the Wireless Access Point setup. If you forget the password, you could pressing the Reset button on the back panel of your WLAM outdoor Radio for at least 3 second – and all previous configurations will need to be input again.

Chapter 4 Trouble Shooting

This chapter helps you to isolate and solve the problems with the LanPro LP993 Outdoor Multi-function Radio. Before you start troubleshooting, it is important that you have checked the details in the product user manual and QIG.

In some cases, rebooting the unit clears the problem. If the radio still can't work well, please try to contact your local vendor or supplier.

4-1 General Descriptions

To successfully use the radios, engineers must be able to troubleshoot the system effectively. This section will show you how an LP993 Outdoor Multi-function radio could be analyzed in the case of "no link," usually, we thinks that the link is down because there is no traffic being passed. The four main reasons that a link may not work are list as below:

- Configuration
- Path issues (such as distance, obstacles, RF reflection…)
- Personal reasons (careless mounting or the incorrectly connection.)
- Hardware (includes the radio, cable and connectors…etc. In few cases, the radio will conflict with the laptop or PC)

Environment (anything that is outside the equipment and not part of the path itself)

After verified the correct configuration, double-checked the path terms, ensure no personal reasons and the hardware works well in the office, but the user still report that the link does not work. Most likely, the problem reported is caused by the environment or by improper tests to verify the connection. Assumes that the test

method, cabling, antennas, and antenna alignment have been checked, (Always ensure this before checking the environment.) then you can do the follow to check the environment.

General Check

Two general checks are recommended before taking any action:

Check whether the software version at both sides is the most current

Check for any reported alarm messages in the Event Log

Analyzing the Spectrum

The best way to discover if there is a source of interference is to use the spectrum analyzer. By turning the antenna 360 degrees, you can find out which direction is the interference coming from. it will also show the frequencies and the level of signal is detected.

Avoiding Interference

When a source of interference is identified and when the level and frequencies are known, the next step is to avoid the interference. Some of the following actions can be tried:

Change the RF channel to the one away from the interference source

Change the polarization of the antenna; try to change to a polarization different from the interferer.

A small beam antenna may helps. (Such as some grid or dish antenna, align the antenna in to the particular direction will reduce the affects from the interference source) This solution cannot help when the source of interference is right behind the remote site.

Before checking for interference, ensure all the hardware works well and configurations are correct. The path analysis, cabling and antennas should be checked as well.

4-2 Connection Issues

This section describes several common troubles the customer might have while setting the radios.

Radio Does Not Boot

When the Radio does not Boot, do the following steps to check your whole system:

1. Ensure that the power supply is properly working and correctly connected.
2. Ensure that all cables are workable and connected correctly.
3. Check the power source.

Cannot use the Web Interface

If the radio boot, but can't enter it via the Web site.

1.Open a command prompt window and enter **ping <ip address unit>** (for example: **`ping 192.168.1.2`**). If ther is no response from the radio, make sure that you the IP address is correct. If there is response, the Ethernet connection is working properly, do the next step.

2. Make sure that you are using one of the following Web browsers:

Microsoft Internet Explorer version 5.0 or later
Netscape version 5.0 or later.

3. Ensure that you are not using a proxy server for the connection with your Web browser.
4. Double-check the physical network connections (includes the cables and the connectors). Use a well-known unit to ensure the network connection is properly functioning.

4-3 Configuration Issues

- The following problems relate to setup and configuration problems.
- Some basic configurations might make the link fail, below are the major ones:
- RF Channel
- SSID
- IP address

- Rule of MAC address filte
- Rule of security settings (such as WEP or WPA)
- Rule of authentication (such as settings of radius server and 802.1x)
- Configurations of WDS page

Please check the detail configuration in Chapter 3 “Configuring the 802.11g Radio”

4-4 Communication Issues

- If the links of the two radios works within close distance of each other, then there are two possible reasons why wireless connectivity is not possible while the Outdoor Multi-function radios are at their desired locations
- RF path, for example, a bad antenna alignment, the tower is not tall enough when the radios are installed in a long distance or the connector do not attachment well…etc (these are the most common problems in installations
- Interference problem caused by a high signal level from another unit. The interference can be checked by changing the frequency and then see if another channel works better. Or you can change the polarization of the antenna as a way of avoiding the interfering signal. To know in advance how much interference is present in a given environment, a Spectrum Analyzer can be attached to a (temporary) antenna for measuring the signal levels on all available Channels.

If the link still not works after resetting the configurations, checking the connectors and cables, double-check the path and environment issues, then the problem is possible a hardware problem. Acquiring a third radio and then testing it amongst the existing units will help to find out the broken unit.

Please contact your local vendor for advance technical support or

support@lan-products.com