LP-348 USER GUIDE

LP348_UG_ENB02W

www.lanpro.com

Table of Content

Copyright

Preface

About This Manual.
This manual explains the LP-348 enterprise-class 802.11g outdoor radio.

Document Conventions

This publication uses the following conventions to convey instructions and Information:
STA refers to a station

ETH refers to a PC

NOTE This symbol means reader take note. Notes contain helpful suggestions or references to materials not contained in thismanual.

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

WARNING 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.

Bold: Indicates the function, important words, and so on.

Chapter 1. Introduction

Thank you for choosing the LP-348 Enterprise-class outdoor radio (hereafter called radio). This radio provides a secure, affordable, and easy-to-use wireless LAN solution that combines mobility and flexibility with the enterprise-class features required by networking Professionals.

This chapter gives an overview of the enterprises-class radio, as well as its key features. In addition, we detail about the hardware descriptions, system requirements and basic Installation.

1-1 LP-348 Overview

802.11a/b/g-compliant, Vlan functionality allows a single network AP to behave as “8” number of virtual network APs. This does away with the limitation by the sheer number of Ethernet connections that need APs acting as a proxy. WMM prioritizes traffic demands from different applications and extends Wi-Fi’s high quality end-user experience from data connectivity to voice, music, and video applications under a wide variety of environment.
This Access points serves as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network.
You can configure and monitor the 348 using the command-line interface (CLI), the browser-based management system, or Simple Network Management Protocol (SNMP).
This radio currently can support data rate up to 108Mbps.
Use the instructions in this Guide to help you connect the outdoor radio, set it up, and configure it to bridge your different networks. These instructions should be all you need to get the most out of the radio

1-2 Key Features

The LP-348 is user-friendly and provides solid wireless and networking support. The following standards and conventions are supported:

• Standards Compliant

The Wireless Access Point complies with the IEEE 802.11b/g for Wireless LANs.

• WEP support

Support for WEP is included. 64-bit, 128-bit, and 152-bit keys.

• DHCP Client Support

DHCP Server provides a dynamic IP address to PCs and other devices upon request. The radio can act as a client and obtain information from your DHPC server.

• RADIUS Accounting

Enable accounting on the access point to send accounting data about wireless client devices to a RADIUS server on your network.

• SNMP Support

Support for Simple Network Management Protocol (SNMP) Management Information Base (MIB) management.

• Multiple operating modes

1. Access point
2. StationAdapter
3. Point-to-Point Bridge.
4. Wireless Repeater
5. Inter-building

• Repeater mode

Configure the radio as a wireless repeater to extend the coverage area of your wireless Network.

• VAPs (VLAN)

Assign Multi-SSIDs on your radio (one SSID per VAP) to differentiate policies and services among users forming a wide variety of VLANs.

• QoS

Use this feature to support quality of service for prioritizing traffic from the Ethernet to the access point.

• Wi-Fi Multi-media (WMM)

Radio also supports the voice-prioritization schemes by using the 802.11b/g wireless phones via enable the WMM application.

•Transmit Power Control

Supports settable transmit power levels to adjust coverage cell size, ranging from full, half(50%), quarter(25%) eighth(12.5%) and min.

There are several versions power versions of the LanPro 348, ranging from 0.2W, 0.5W to 1W of full output power. The 0.5W and 1W contain an aditional high performance b/g amplifier inside the Nema4 sealed enclosure. Ask your distributor for details.

•Atheros Super G Mode

Atheros is a world lider in telecomm chipsets.
Selected by companies as IBM and Toshiba among many others.
LanPro uses Atheros to assure best performance and compatiibility with current modern systems. Super G mode enables the transmission up to 108Mbps

• Multiple security settings per VLAN with up to 8 VLANs

Security settings for multiple groups; so employees, guests and contractors now easily and securely share the same infrastructure.

•Access Control

The Access Control MAC address filtering feature can ensure that only trusted wireless stations can use the radio to gain access to your LAN.

•Hidden Mode

The SSID is not broadcast, assuring only clients configured with the correct SSID can Connect.

1-3 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.

WARNING

To meet regulatory restrictions, the LP-348 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.

CAUTION

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.

1-4 System Requirements

Before installing the LP-348, make sure your system meets these requirements

- The Category 5 UTP straight through Ethernet cable with RJ-45 connector. (Between PC and POE) . We recommend to use LanPro networking cable cat5e.

- The Category 5 SFTP straight through Ethernet cable with weather-proof RJ-45 connector. (Between POE and radio)

- A 100~240 V, 50~60 Hz AC power source

- A Web browser for configuration such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above

- At least one computer with the TCP/IP protocol installed

What's In the Box?

- 802.11 b/g Outdoor radio * 1

- Power adapter and cord * 1

- Power over Ethernet (POE) * 1

- Quick Installation Guide * 1

- Installation CD for the radio *1

- Mounting kit *1

- RJ-45 weather-proof connector for the SFTP cable * 1

If any missing or damaged, please contact your local seller.

1-5 Hardware Description

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

MECHANICAL DESCRIPTION

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

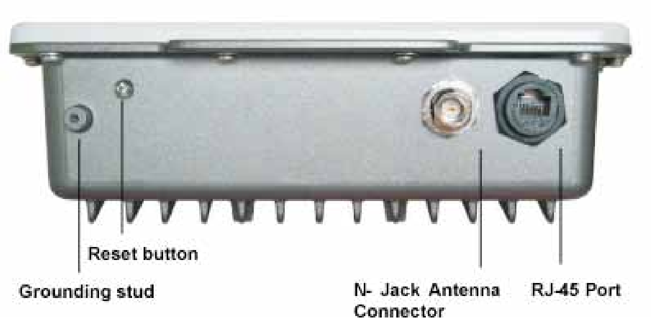


Figure 1-1 Outdoor Multi-function Radio Figure

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

2 N- Jack Antenna Connector — Here you can attach the proper antenna with the outdoor radio to wirelessly connect to the 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.

4 Reset button — Screw off this screw and insert a stick to press in and hold the reset button for 5~10 seconds, the radio will back to factory default Settings.
PS. The spec of the screw is “Button head socket cap screw 4*6 iso”.

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.

POE (Power over Ethernet)

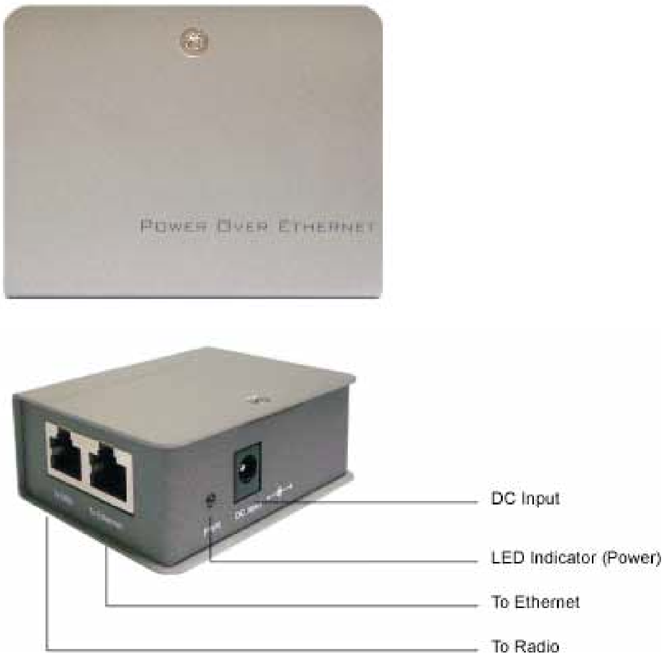


Figure 1-2 Power over Ethernet injector

1 **To Ethernet** RJ-45 port used to connect to the 10/100 Base T complied device such as switch, router or PC.

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.

1-6 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.

NOTE

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

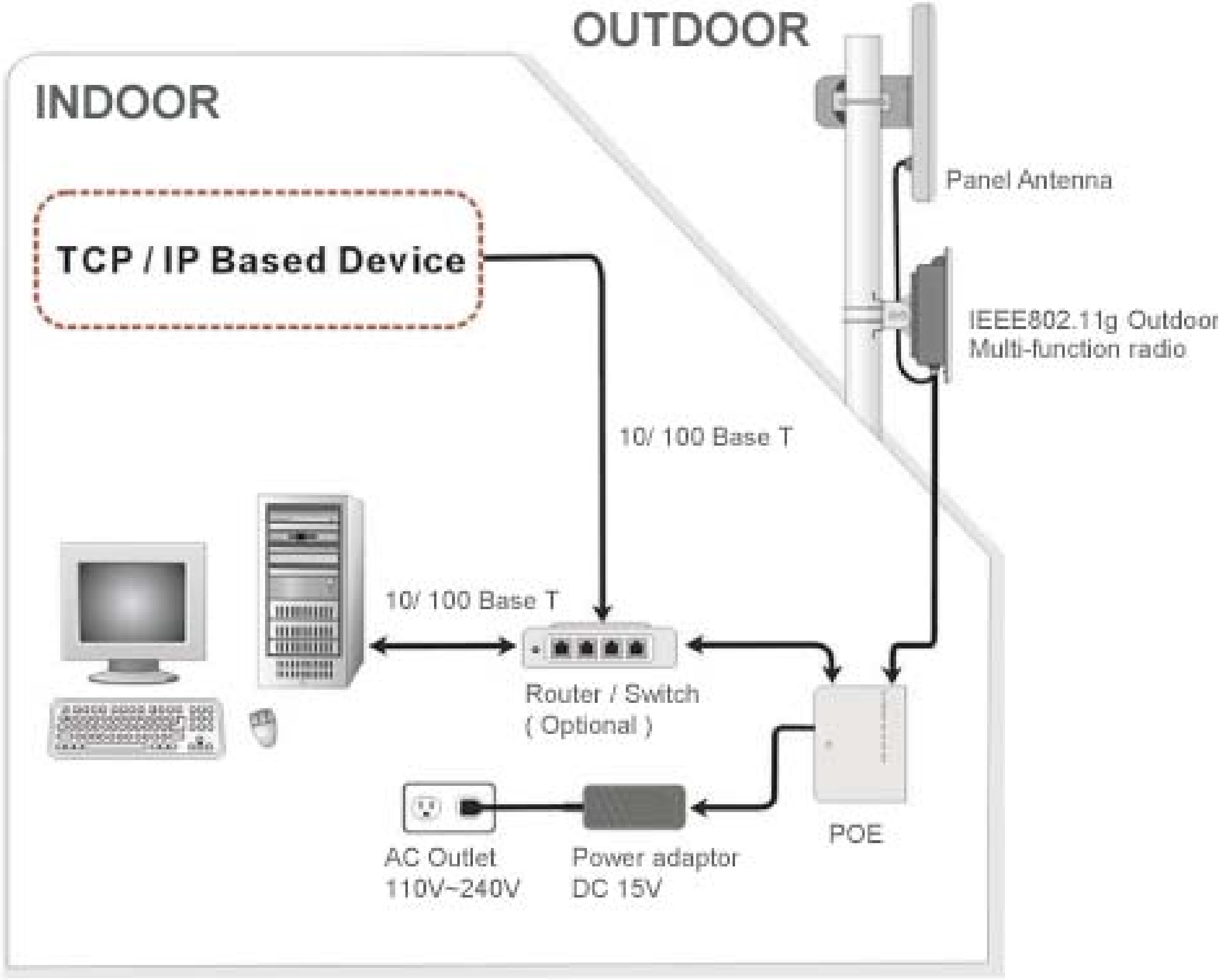


Figure 1-3 Hardware Installation Figure

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

Connect the Ethernet Cable

The LP-348 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.

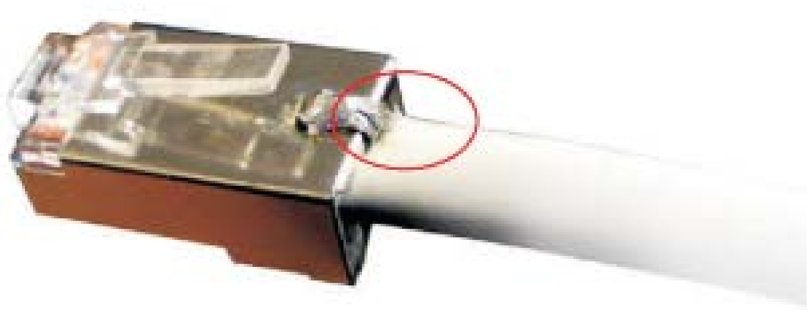


Figure 1-4 Weld the RJ-45 connector with the SFTP cable

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 2. Basic Installation and Securities

This chapter explains how to place and connect the outdoor radio. In addition, the radio's security features are elaborated.

2-1 Default Factory Settings

We'll detail about radio default factory settings below. Factory Default Restore will enable you to restore these defaults.

FEATURE	FACTORY DEFAULT SETTINGS
User Name (case sensitive)	admin
Password (case sensitive)	password
radio Name	APxxxxxx(xxxxxx represents the last 6 digits of MAC address)
Country / Region	United States
Router Mode	Bridge
IP Type	static IP
IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Operating Mode	Access Point
Wireless Mode	Auto (802.11g/b)
Channel / Frequency	1 / 2.412 Ghz

2-2 Getting to Know radio Wireless Security Options

If wants to make wireless networking as safe and easy for you as possible. This radio provides several network security features, but they require specific action on your part for Implementation.

Security Precautions

The following is a complete list of security precautions to take as shown in this User's Manual.

1. Change the default SSID.
2. Disable SSID Broadcast.
3. Change the default password for the Administrator account.
4. Enable MAC Address Filtering.
5. Change the SSID periodically.
6. Use the highest encryption algorithm possible. Use WPA if it is available. Please note that this may reduce your network performance.
7. Change theWEP encryption keys periodically.

To ensure network security, steps one through four should be followed at least. Wireless networks are easy to find. Hackers know that in order to join a wireless network, wireless networking products first listen for "beacon messages". These messages can be easily decrypted and contain much of the network's information, such as the network's SSID (Service Set Identifier).

Security Options

There are several ways you can enhance the security of your wireless network:

• Restrict Access Based on MAC address. You can restrict access to only trusted clients so that unknown clients cannot wirelessly connect to the radio. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.

• **Use WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper.

• **Use WPA or WPA-PSK.** Wi-Fi Protected Access (WPA) data encryption provides data security. The very strong authentication along with dynamic per frame re-keying of WPA makes it virtually impossible to compromise.

• **Enable Wireless Security Separator.**The associated wireless clients will not be able to communicate with each other if this feature is enabled. The default setting is disabling.

2-3 Installing the radio as an AP (Access Point)

Before installing, you should make sure that Ethernet network is perfectly working. You will be connecting the radio to the Ethernet network so that computers with 10/100 Fast Ethernet adapters will communicate computers on the Ethernet.

1. SET UP THEAP Tip:

Before mounting the radio in a high location, first set up and test the radio to verify wired network connectivity.

a. Prepare a computer with an Ethernet adapter. If this computer is already part of your network, record its TCP/IP configuration settings.

b. Configure the computer with a static IP address of 192.168.1.x (x cannot be 1) and 255.255.255.0 for the Subnet Mask.

c. Connect a Cat.5 SFTP cable from the radio to the POE.

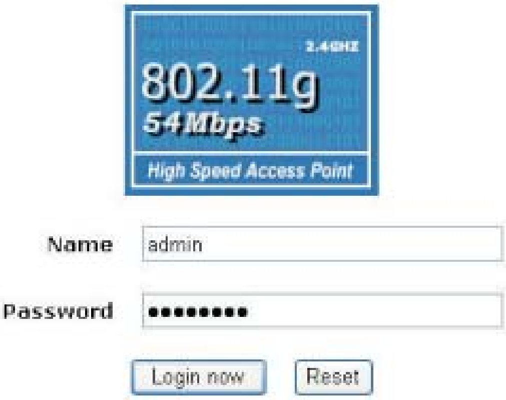
d. Connect a Cat.5 UTP cable from the POE to computer.

e. Turn on your computer, connect the power adapter to the AP and verify the following:
– The power light of the POE goes on.
– The LAN light of the Ethernet port on computer goes on too. (or the lan status which showed on the windows linked)

2. To CONFIGURE LAN AND WIRELESS ACCESS

a. Configure the AP Ethernet port for LAN access

• Connect to the AP by opening your browser and entering http://192.168.1.1 in the address field. A login window like the one shown below opens:



Name admin

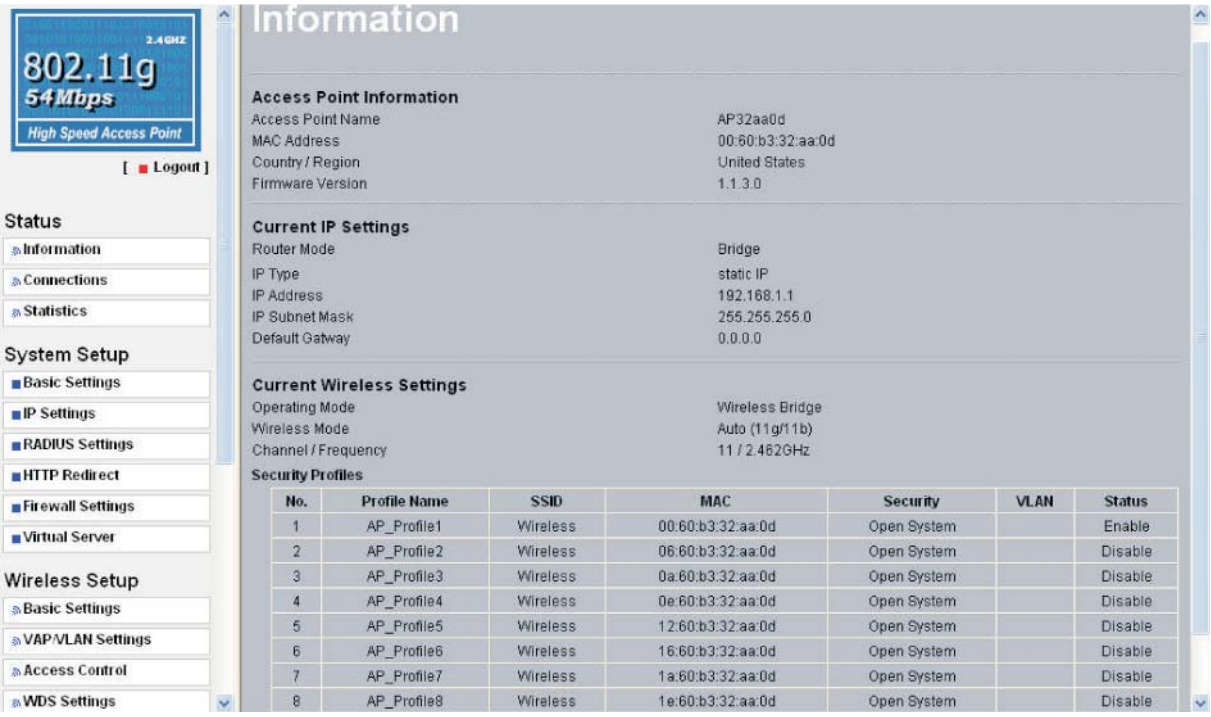
Password ●●●●●●●●●

Figure: 2-1 APlog in window

When prompted, please enter admin for Name and password for password, both in

low cases.

3. Clicking Login now, it will navigate you into this radio's homepage-----General Information will be shown below.



Information

Access Point Information

Access Point Name	AP32aa0d
MAC Address	00:60:b3:32:aa:0d
Country / Region	United States
Firmware Version	1.1.3.0

Current IP Settings

Router Mode	Bridge
IP Type	static IP
IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
Default Gatway	0.0.0.0

Current Wireless Settings

Operating Mode	Wireless Bridge
Wireless Mode	Auto (11g/11b)
Channel / Frequency	11 / 2.462GHz

Security Profiles

No.	Profile Name	SSID	MAC	Security	VLAN	Status
1	AP_Profile1	Wireless	00:60:b3:32:aa:0d	Open System		Enable
2	AP_Profile2	Wireless	06:60:b3:32:aa:0d	Open System		Disable
3	AP_Profile3	Wireless	0a:60:b3:32:aa:0d	Open System		Disable
4	AP_Profile4	Wireless	0e:60:b3:32:aa:0d	Open System		Disable
5	AP_Profile5	Wireless	12:60:b3:32:aa:0d	Open System		Disable
6	AP_Profile6	Wireless	16:60:b3:32:aa:0d	Open System		Disable
7	AP_Profile7	Wireless	1a:60:b3:32:aa:0d	Open System		Disable
8	AP_Profile8	Wireless	1e:60:b3:32:aa:0d	Open System		Disable

Chapter 3. General Information

General information gives you a basic concept of the radio.

3-1 Information

Understanding General Information Settings
We'll elaborate the information from this radio's homepage.

Access Point Name: You may assign any device name to the Access Point. This name is only used by the Access Point administrator for identification purposes. Unique, memorable names are helpful, especially if you are employing multiple access points on the same network. The default name is Apxxxxxx.

MAC Address: Short for Media Access Control address, a hardware address that uniquely identifies each node of a network.

Country/Region: This field identifies the region where the AP can be used. It may not be legal to operate the wireless features of the wireless access point in a region other than one of those identified in this field. The default country is the United States.

Firmware Version: Firmware is stored in a flash memory and can be upgraded easily, using your Web browser, and can be upgraded via ftp server. The currently available version of AP is 1.1.3.0.

IP Type: By default, the LP-348 AP is configured as static IP Address.

IP Address: The IP address must be unique to your network. The default IP address is 192.168.1.1

⚠ **To associate the access point to your PC, make sure the PC IP address need to be matched the AP. For instance, the AP is 192.168.1.1, and your PC IP should Be 192.168.1. X.**

Subnet Mask: The Subnet Mask must be the same as that set on the LAN that your Access Point is connected to. The default is 255.255.255.0.

Operating Mode: AP provides five modes, Access Point, Station, bridge, repeater and Inter-building.

•**Access Point:** Act as a standard 802.11b/g. The default mode is Access Point.

•**Station:** Perform as a client station associated to other APs. Be sure that they share the same SSID when connected.

•**Wireless bridge:** In this mode, the AP only communicates with another bridge-mode wireless station. You Must enter the MAC address (physical address) of the other bridge-mode wireless station in the field provided. WEP should be used to protect this communication.

•Point to Multi-Point Bridge

Select this only if this AP is the “Master” for a group of bridge-mode wireless stations. The other bridge-mode wireless stations must be set to Point-to-Point Bridge mode, using this AP MAC address. They then send all traffic to this “Master”, rather than communicate directly with each other.WEP should be used to protect this traffic.

•Wireless Repeater: In this mode, the AP can communicate with another wireless station or wireless bridge. You can enter the MAC address of both adjacent repeaters in the fields provided to communicate with other wireless bridge or use SSID to communicate with other wireless station. WEP should be used to protect this communication.

•Inter-building

This is own brand of WDS mode. Under this mode, AP will automatically connect to our 11b radio which is set to inter-building mode too, without manually entering MAC address for each other.

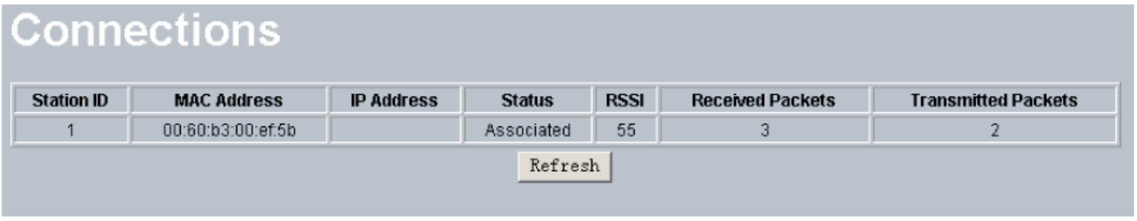
Wireless Mode: Select the desired wireless operating mode. The default mode is Auto(802.11g/b).

Channel: This field identifies which operating frequency will be used.

Security Profiles: This provides a list of virtual APs derived from AP Virtual AP, spelling out profile name, SSID, MAC, security, and status.

3-2 Connection

Under the Information heading, click the connection link to view the connection status shown below.



Connections

Station ID	MAC Address	IP Address	Status	RSSI	Received Packets	Transmitted Packets
1	00:60:b3:00:ef:5b		Associated	55	3	2

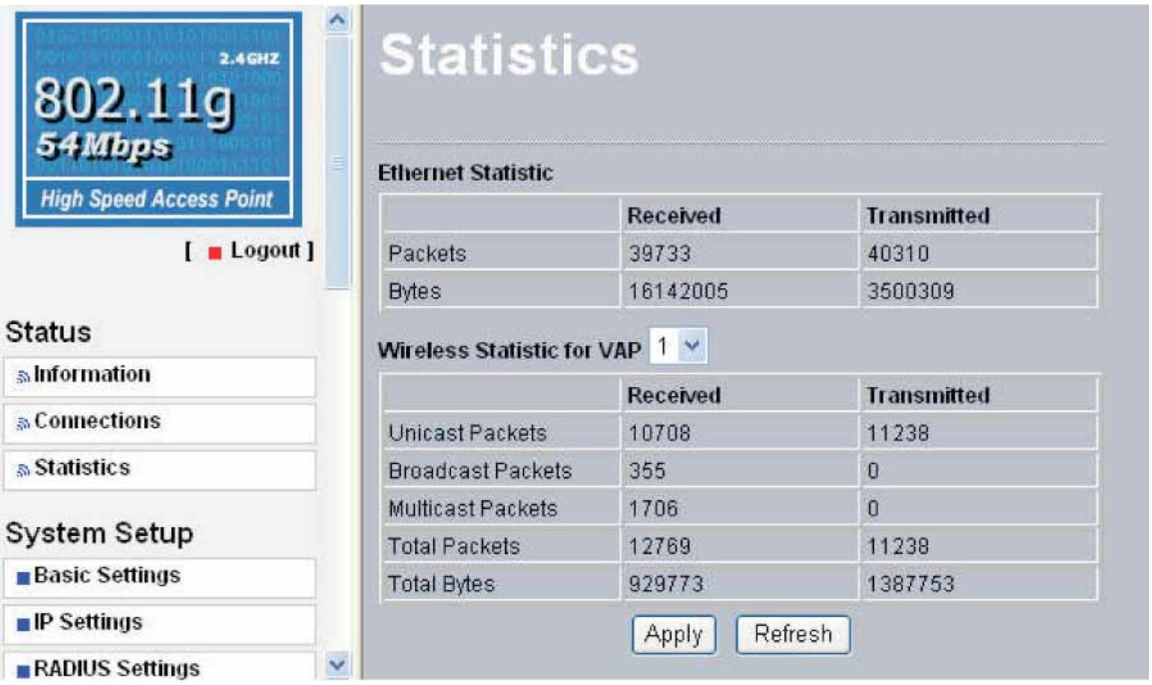
Figure: 3-1 AP connection status

If the wireless access point is rebooted, the table data is lost until the wireless Access point rediscovers the devices.

Statistics

The statistics provide various LAN and WAN statistics.

.



Statistics

Ethernet Statistic

	Received	Transmitted
Packets	39733	40310
Bytes	16142005	3500309

Wireless Statistic for VAP 1

	Received	Transmitted
Unicast Packets	10708	11238
Broadcast Packets	355	0
Multicast Packets	1706	0
Total Packets	12769	11238
Total Bytes	929773	1387753

Figure: 3-2 statistics

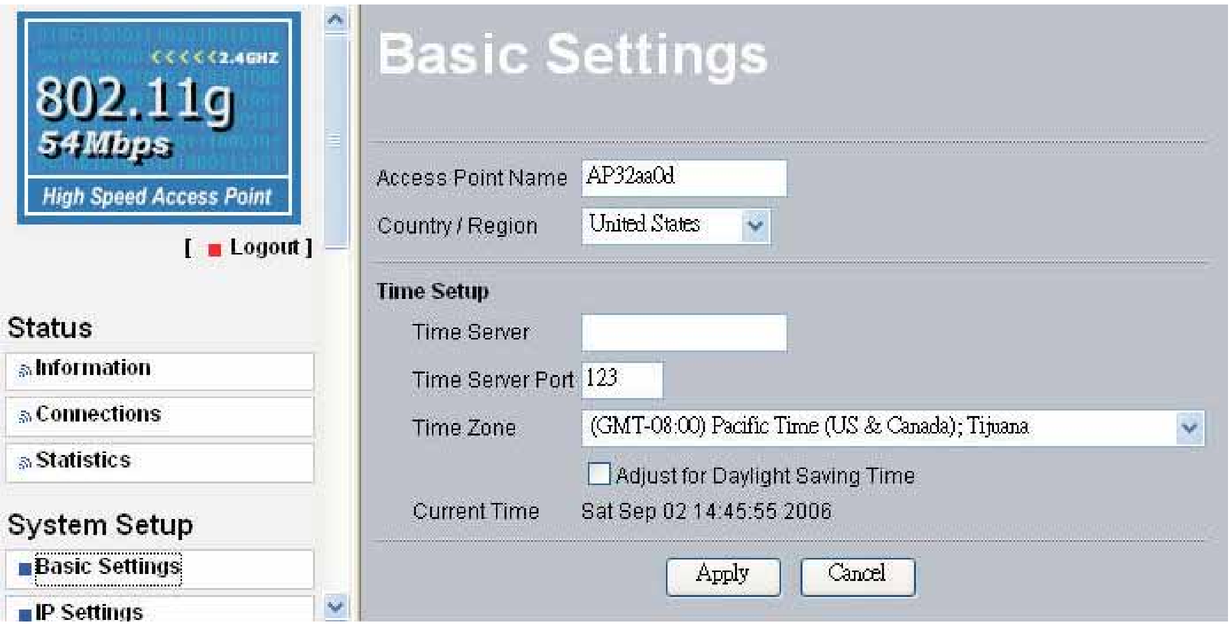
Field		Description
Wired Ethernet	Packets	The number of packets sent since the AP was restarted.
	Bytes	The number of bytes sent since the AP was restarted.
Wireless	Unicast Packets	The Unicast packets sent since the AP was restarted.
	Broadcast Packets	The Broadcast packets sent since the AP was restarted.
	Multicast Packets	The Multicast packets sent since the AP was restarted.
	Total Packets	The Wireless packets sent since the AP was restarted.
	Total Bytes	The Wireless bytes sent since the AP was restarted.

Chapter 4. Copious Functionalities

The versatile radio provides various, applicable functions.

4-1 Time Server

By click Basic Settings, the “Basic Settings” will appear shown below.



Access Point Name: AP32aa0d

Country / Region: United States

Time Setup

Time Server:

Time Server Port: 123

Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana

□ Adjust for Daylight Saving Time

Current Time: Sat Sep 02 14:45:55 2006

Figure: 4-1 AP Basic settings

The AP allows you to synchronize the time between your network and time server by using NTP Time Server.

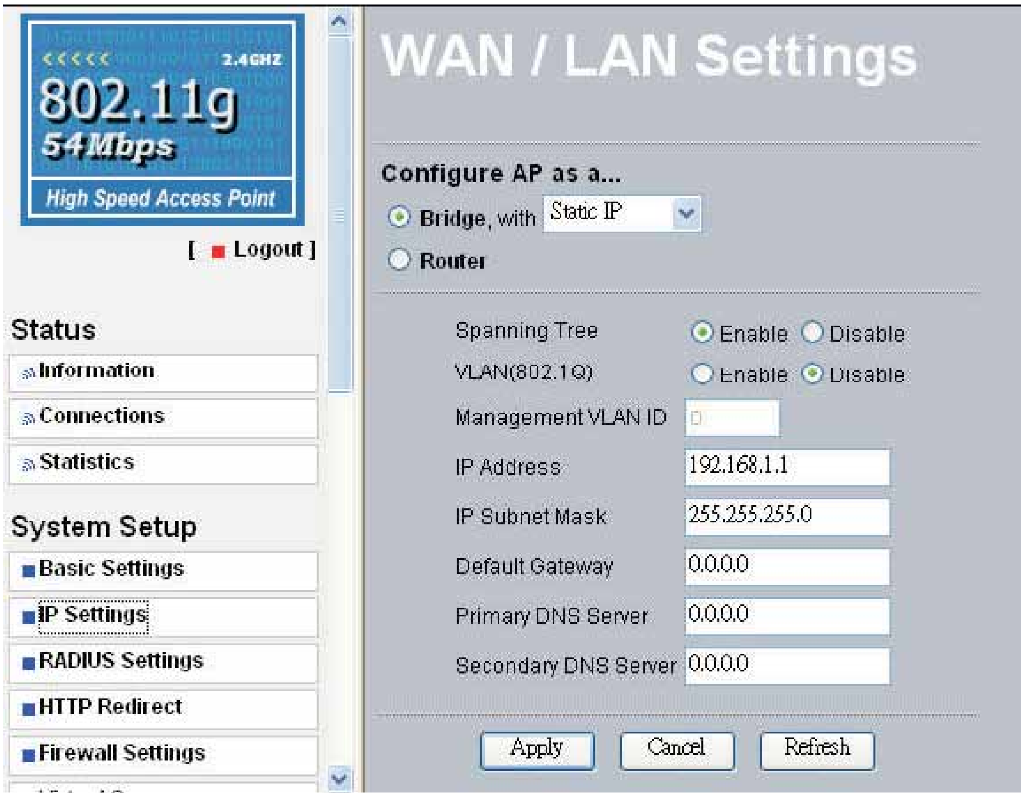
Time Sever provides correct and current time in any world time zone, country or major city. Accurate adjustments for Daylight Saving Time (or Summer Time) are made according to each location's rules and laws.

Time Server Port: This field identifies the time server port like 123.
Time Zone: Select the time zone location for your setting.

Current Time: This field identifies the current time in your specific time Zone.

4-2 Bridge/Router Mode

From the system setup, click IP Settings, you’ll be navigated into the WAN/LAN Settings.



WAN / LAN Settings

Configure AP as a...

● Bridge, with Static IP

○ Router

Spanning Tree ● Enable ○ Disable

VLAN(802.1Q) ○ Enable ● Disable

Management VLAN ID 0

IP Address 192.168.1.1

IP Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

Primary DNS Server 0.0.0.0

Secondary DNS Server 0.0.0.0

Figure: 4-2 AP WAN/LAN settings

This radio can be figured as bridge mode and router mode.

Bridge Mode

Under Bridge Mode, the AP will act as a pass-through bridging your network, by associating with various devices. This can extend your radius of your network.
Spanning Tree: Enabling spanning tree can prevent undesirable loops in the network, ensuring a smooth running network. By default, the function is enabled.

Router Mode

Under Router Mode, the radio has two ports, WAN port and LAN ports.
If your network has a requirement to use a different IP addressing scheme, you can make those changes in this menu. These settings are only required if the Refresh” is chosen. Remember to click Apply to save your changes.

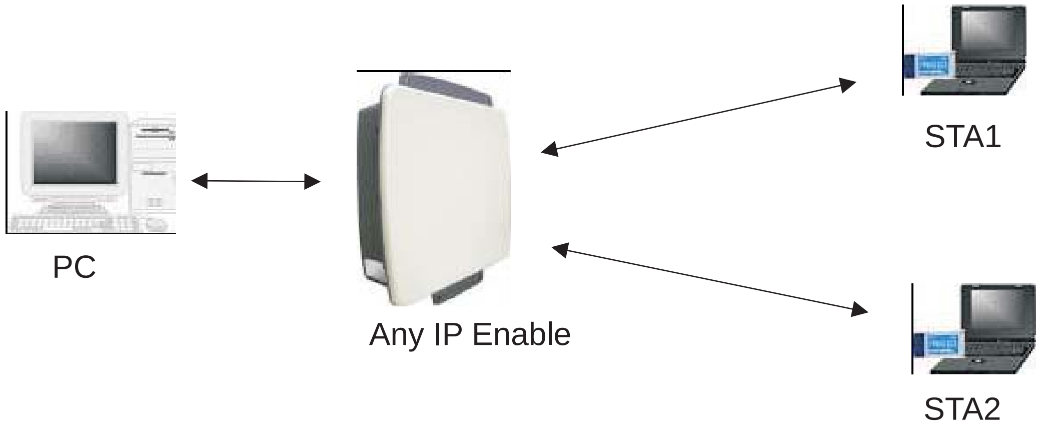
4-3 Any IP

If IP address has slipped your mind, any IP functionality can relieve your anxiety. Enabling any IP, you'll feel free to enter IP Address, IP Subnet Mask and Gateway, enjoying internet surf.

Please refer to the diagram below.

Take the steps to activate the functionality.

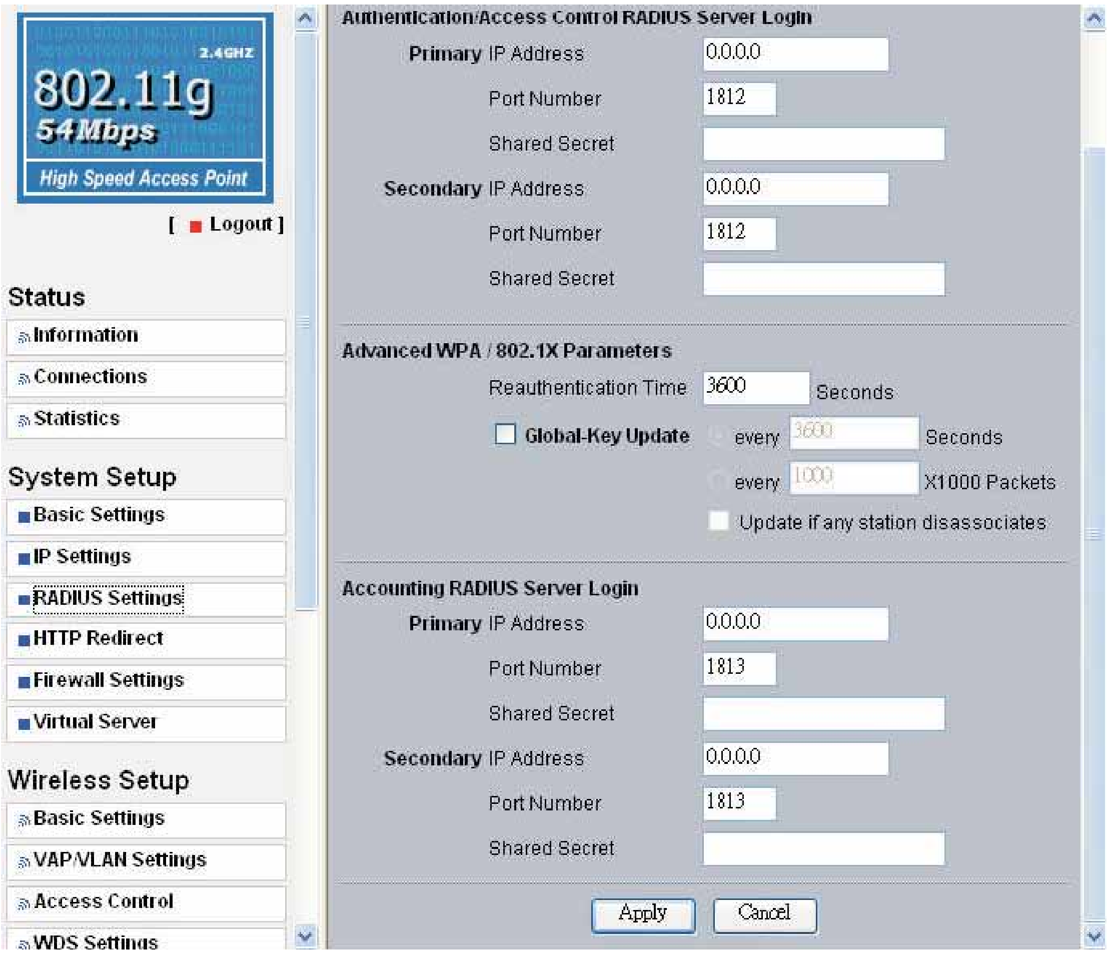
1. Configure the AP as router mode.
2. Make sure your station connected to the AP.
3. Set correct IP parameters for the AP.
4. Enable any IP



4-4 Understanding RADIUS Settings

RADIUS is a server for remote user authentication and accounting. It can be used on any network that needs a centralized authentication and/or accounting service for its Workstations.

From the system Setup, click Radius Settings, the RADIUS Settings will display as below.



Authentication/Access Control RADIUS Server Login

Primary IP Address: 0.0.0.0
Port Number: 1812
Shared Secret:
Secondary IP Address: 0.0.0.0
Port Number: 1812
Shared Secret:

Advanced WPA / 802.1X Parameters

Reauthentication Time: 3600 Seconds
□ Global-Key Update ○ every 3600 Seconds
○ every 1000 X1000 Packets
□ Update if any station disassociates

Accounting RADIUS Server Login

Primary IP Address: 0.0.0.0
Port Number: 1813
Shared Secret:
Secondary IP Address: 0.0.0.0
Port Number: 1813
Shared Secret:

You will also have to fill in the following Radius server settings:

• Primary Radius Server IP Address
This field is required. Enter the IP address of the Radius Server on your LAN or WAN..
• Secondary Radius Server IP Address
This field is optional. Enter the IP address of the Secondary Radius Server on your LAN.
• Radius Port
Enter the port number used for connections to the Radius Server.
• Radius Shared Key
Enter the desired value for the Radius shared key. This key enables the AP to log in to the Radius server and must match the value used on the Radius server.

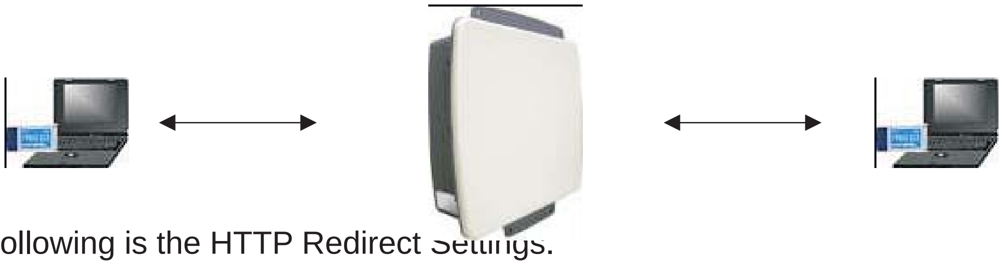
•Radius Accounting Option

The Radius Accounting option can be enabled so that you can track various information like who connected to the network, when they connected, how long they were connected, how much network traffic they generated, and so on.

4-5 HTTP Redirect

Currently market campaign has a stake in the future of your company, so that plugging your products on website is a basic step for your goods.

This radio has insight into your need. Enabling HTTP redirect, you can enter the company website (for example, http://www.google.com). It is your desired web that first appears when someone is surfing on internet, via a station connected to your radio (which is set to be anAP) for internet surf.



The following is the HTTP Redirect Settings.

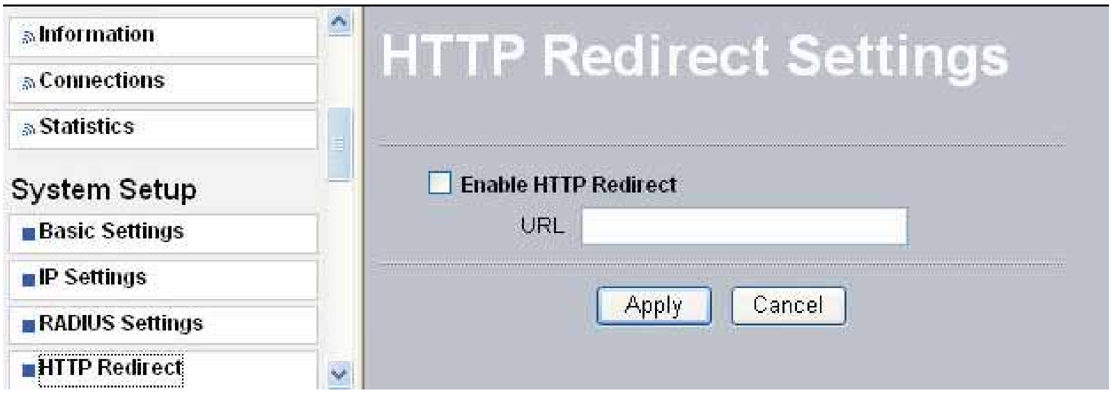


Figure: 4-4 AP HTTP Redirect settings

URL

Enter your desired website in this field. Be sure to click “Apply” to save the configuration.

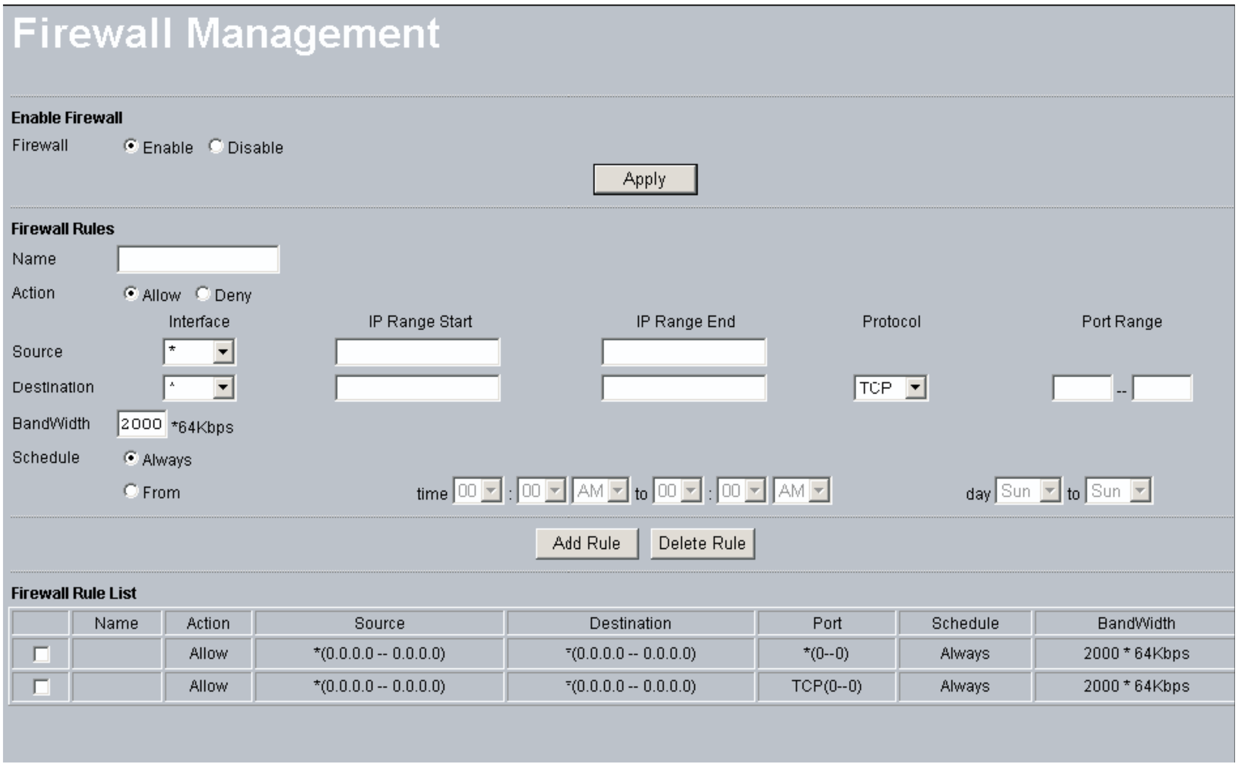
Be sure to your AP connected to the internet when using HTTP Redirect.

4-6 Firewall Management

Today's companies rely on highly networked, secure computing environments to efficiently and safely conduct business. Firewalls are a key component of any secure network. Firewalls are configured to allow "desired" traffic in and to keep "undesired" traffic out. The LP-348 (access point) is also qualified for firewall management.
Please see the diagram below.

Acting as a firewall, the radio will filter your undesired data and protocols, only delivering the "wanted" for your PC.

Click the firewall link and you'll be navigated to Firewall Management interface.



Firewall Management

Enable Firewall

Firewall ● Enable ○ Disable

Firewall Rules

Name

Action ● Allow ○ Deny

	Interface	IP Range Start	IP Range End	Protocol	Port Range
Source	*				
Destination	*			TCP	--

BandWidth 2000 *64Kbps

Schedule ● Always

○ From time 00 : 00 AM to 00 : 00 AM day Sun to Sun

Firewall Rule List

	Name	Action	Source	Destination	Port	Schedule	BandWidth
☐		Allow	*(0.0.0.0 -- 0.0.0.0)	*(0.0.0.0 -- 0.0.0.0)	*(0--0)	Always	2000 * 64Kbps
☐		Allow	*(0.0.0.0 -- 0.0.0.0)	*(0.0.0.0 -- 0.0.0.0)	TCP(0--0)	Always	2000 * 64Kbps

Figure: 4-5 AP firewall management

Before applying the firewall management, you need enable firewall.
Here we'll discuss Firewall.

• Name

Enter your desired firewall rule name in this field.

• Allow

This field identifies which packets have IP addresses specified by you, are allowed to transmit at your LAN.

• Deny

This field identifies which packets have IP addresses specified by you, are banned to transmit at your LAN.

• Interface

This is optional, WAN or LAN.

Destination

This specifies where packets are bound for.

•IP Range Start

This specifies the starting-point of your specific IP addresses.

•IP Range End

This specifies the ending-point of your specific IP addresses.

•Protocol

This is optional, TCP, DCP, ICMP or *. Select which protocol you want to perform “Allow” or “Deny”.

⚠ **indicates you restrict no protocol to perform “Allow” or “Deny”.**

•Port Range

This specifies your IP port range.

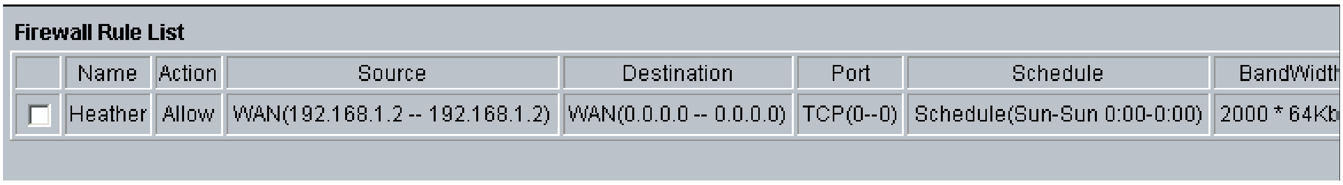
•Schedule

You can set time when your AP performs firewall management, by enabling “from”. Alternatively, if you desire your AP to perform firewall management for a long time, please enable “always”.

•Bandwidth

You can set the bandwidth with n*64Kb / per second to limit the data flow.

When completing all firewall rules configuration, please click Add Rule. Firewall Rule List will appear below.



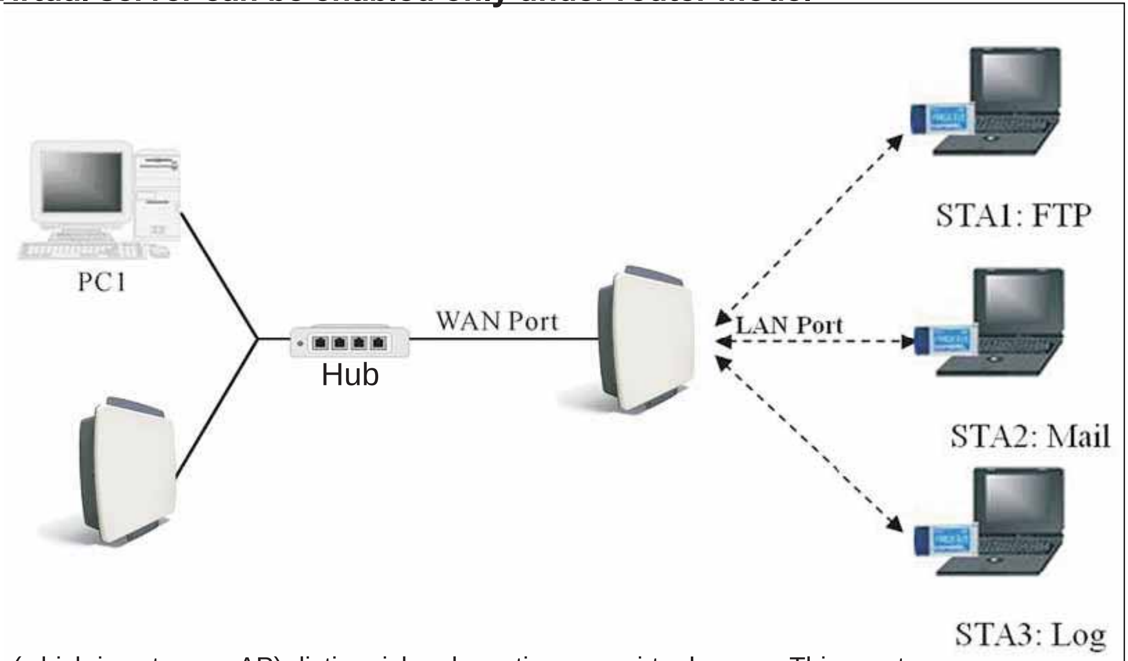
Firewall Rule List

	Name	Action	Source	Destination	Port	Schedule	BandWidth
□	Heather	Allow	WAN(192.168.1.2 -- 192.168.1.2)	WAN(0.0.0.0 -- 0.0.0.0)	TCP(0--0)	Schedule(Sun-Sun 0:00-0:00)	2000 * 64Kb

Figure: 4-6 Firewall list

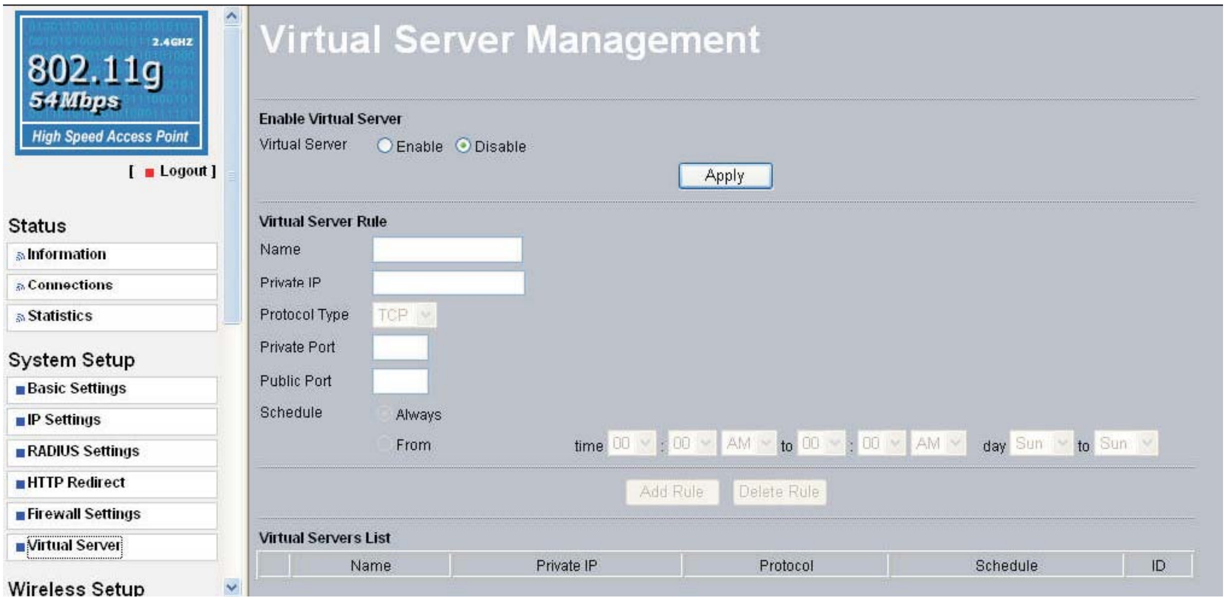
4-7 Virtual Server

Virtual server can be enabled only under router mode.



The radio (which is set as an AP) distinguishes by acting as a virtual server. This most cost-effective server virtualization technology is engineered for heterogeneous network. Please refer to the following diagram.

Under router mode, designed for the virtual server, the AP is wirelessly coupled to FTP server, mail server and log server on LAN port; on WAN port, the AP is coupled to PC. The AP is the virtual server, so that you have access to download files, enjoy e-mails or undertake others, only via your PC.



Virtual Server Management

Enable Virtual Server

Virtual Server ○ Enable ● Disable

Apply

Virtual Server Rule

Name

Private IP

Protocol Type TCP

Private Port

Public Port

Schedule ○ Always

○ From time 00 : 00 AM to 00 : 00 AM day Sun to Sun

Add Rule Delete Rule

Virtual Servers List

	Name	Private IP	Protocol	Schedule	ID

Figure: 4-7 APvirtual server management

We'll discuss virtual elements below.

•Name

Enter the virtual server’s name in this field.

•Private IP

This specifies the IP Address at your LAN.

•Protocol Type

This field is optional. SelectTCP or UDP.

•Private Port

This specifies your LAN port.

•Public Port

This specifies your WAN port.

•Schedule

You can set time-limit when your AP acts as a virtual server, by enabling “from”. Alternatively, if you desire your AP to act as a virtual server for a long time, please enable “Always”.

•Virtual Server List

This provides you with the detailed list of virtual servers.

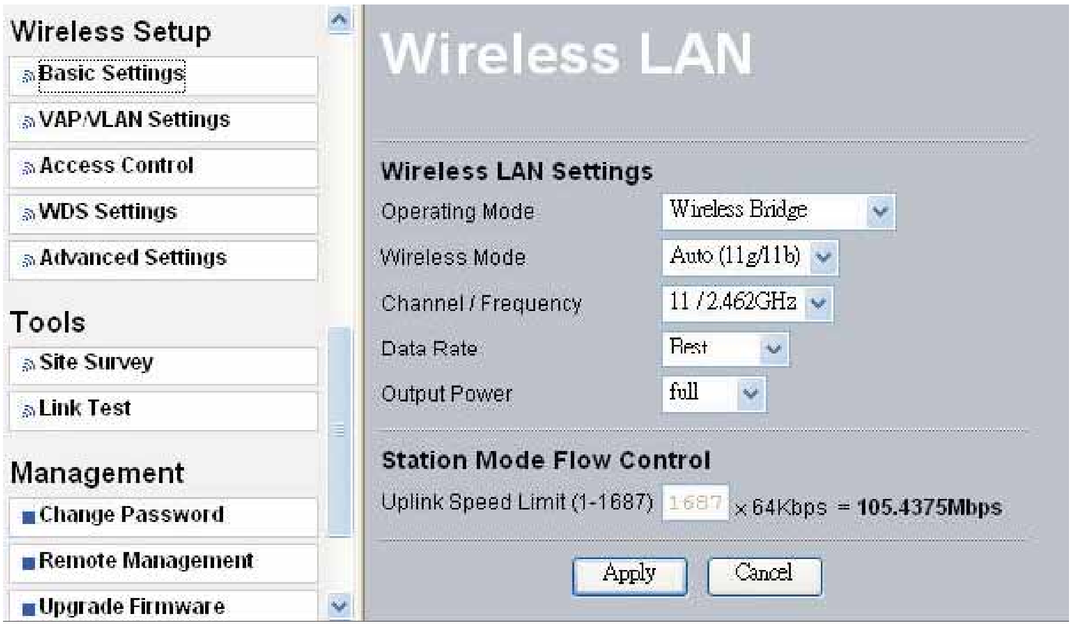
When completing configuration of your virtual server, please click “Add Rule” to save the Setting.

Chapter 5. Wireless Setup

This chapter focuses on the LP-348 powerful wireless function.

5-1 Basic Settings

The versatile outdoor radio provides adequate to five operating modes for your various Purposes.



Wireless LAN Settings

Operating Mode: Wireless Bridge

Wireless Mode: Auto (11g/11b)

Channel / Frequency: 11 / 2.462GHz

Data Rate: Best

Output Power: full

Station Mode Flow Control

Uplink Speed Limit (1-1687): 1687 x 64Kbps = 105.4375Mbps

Figure: 5-1 Basic Setting

• Operating Mode:

AP is capable of five operating modes, access point, station adapter, wireless bridge, wireless repeater, and wireless inter-building.

•Access Point

Any 802.11 b/g wireless station can communicate with it by correct SSID.
•Station: Perform as a client station associated to other APs. Be sure that they share the same SSID and secure settings when connected.

•Wireless bridge

In this mode, the radio only communicates with another bridge-mode wireless station. You must enter the MAC address (physical address) of the other bridge-mode wireless station in the field provided. WEP should be used to protect this communication.

•Point to Multi-Point Bridge

Select this only if this radio is the “Master” for a group of bridge-mode wireless stations. The other bridge-mode wireless stations must be set to Point-to-Point Bridge mode, using this radio MAC address. They then send all traffic to this “Master”, rather than communicate directly with each other.

• Wireless Repeater.

In this half-duplex mode, the radio can communicate with another wireless bridge and wireless station. You must enter the MAC address of both adjacent wireless bridges in the fields provided. WEP should be used to protect this communication.

- Inter-building

This is own brand of WDS mode. Under this mode, radio will automatically connect to our 11b outdoor radio without manually entering MAC address for each other.

- **SSID**

The SSID is the unique name shared among all devices in a wireless network. It is case-sensitive, must not exceed 32 alphanumeric characters, and may be any keyboard character. Make sure this setting is the same for all devices in your wireless network. The default SSID name is wireless.

- **BSSID**

A group of Wireless Stations and a single access point, all using the same ID (SSID), form a Basic Service Set.
Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other. However, some access points allow connections from wireless stations which have their SSID set to “any” or whose SSID is blank (null).

- **Wireless Mode**

Select the desired wireless operating mode. The options are:
Auto (11g/b) – Both 802.11g and 802.11b wireless stations can be used.
11gonly - Only 802.11g wireless stations can be used.
11bonly - All 802.11b wireless stations can be used. 802.11g wireless stations can still be used if they can operate in 802.11b mode.

- **Channel.**

This field identifies which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems or setting up the AP near another access point.

- **Data Rate.**

Shows the available transmit data rate of the wireless network. The default is “Best”.

- **Output Power.**

Set the transmit signal strength of the radio. The options are full, half, quarter, eighth, and min. Decrease the transmit power if more than one AP is collocated using the same channel frequency. The default is Full.

- **Station Mode Flow Control**

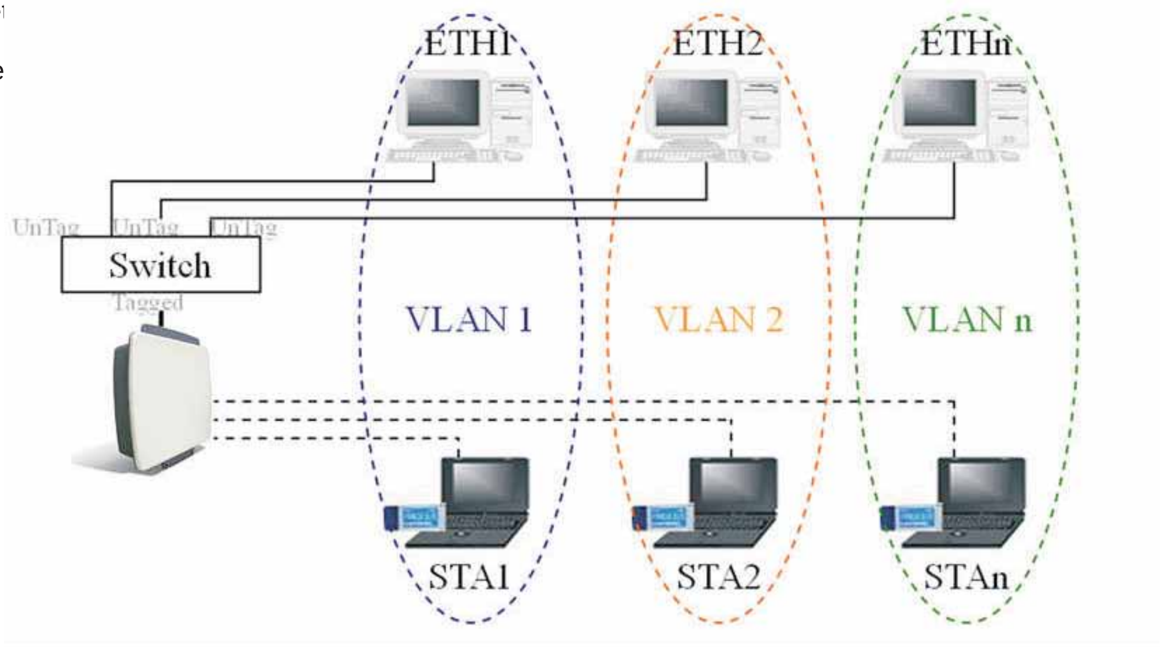
Uplink SpeedLimit (1-1687): It indicates the transmission rate.

5-2 VAP / VLAN Settings

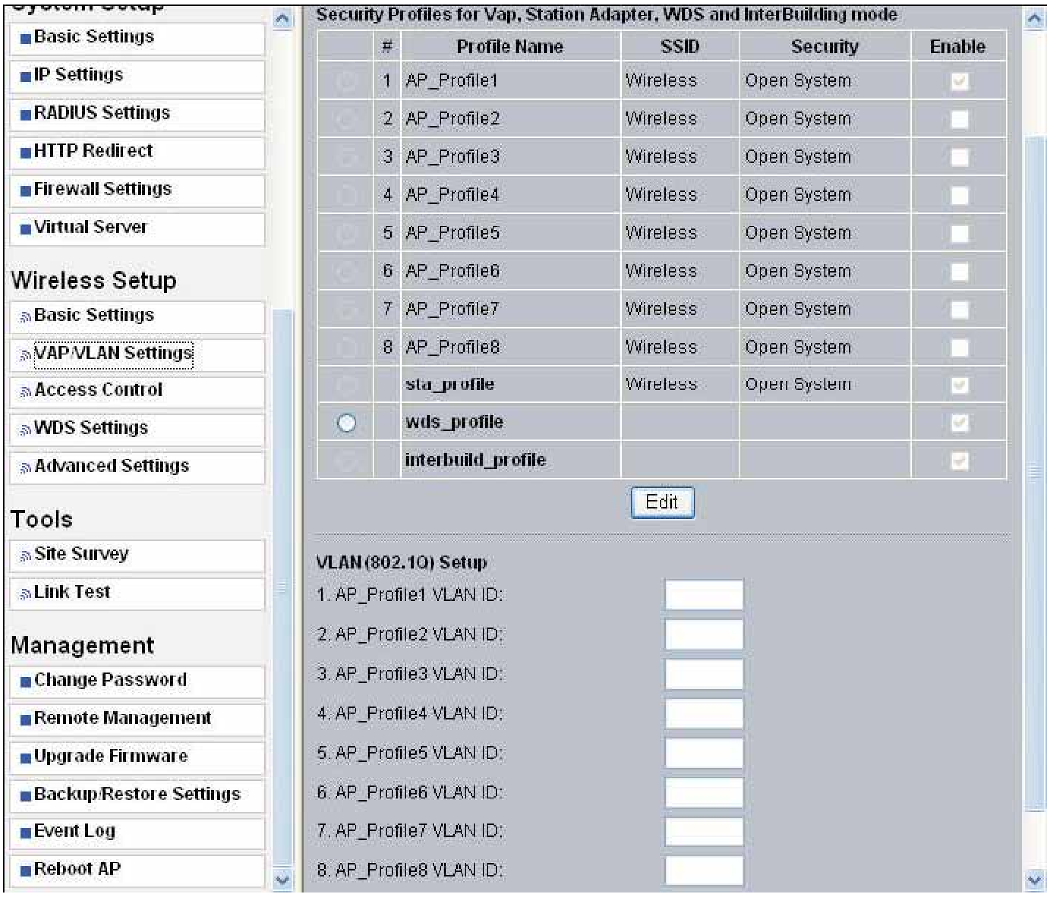
Overview

As the number of data-based systems increase, it becomes more and more difficult to provide the network infrastructure (due to the sheer number of Ethernet connections that need to be provided) from the perspective of cost, space, and wire management. Luckily, the advent technology called VLAN (Virtual Local Area Network) can achieve her mission. Now it is possible for these multi devices in function without the need for multiple physical ne

Se



Under this mode, this radio can behave as 8 virtual Wireless LAN infrastructures. You can specify unique SSID for these different infrastructures. For example, VLAN1 contains ETH1 and STA1,VLAN2 contains ETH2 and STA2, and so on. However, they all share the same AP and undertake different tasks. Some VLANs can be used for guest Internet access, others for enterprise users, and administrators can be put on a high security VLAN with enhanced firewall permissions. All this can be achieved using a single infrastructure to emulate up to 8 infrastructures. The AP does this by assigning each of the 8 VLANs it’s own SSID, so you will think you are looking at up to 8different wireless Networks.



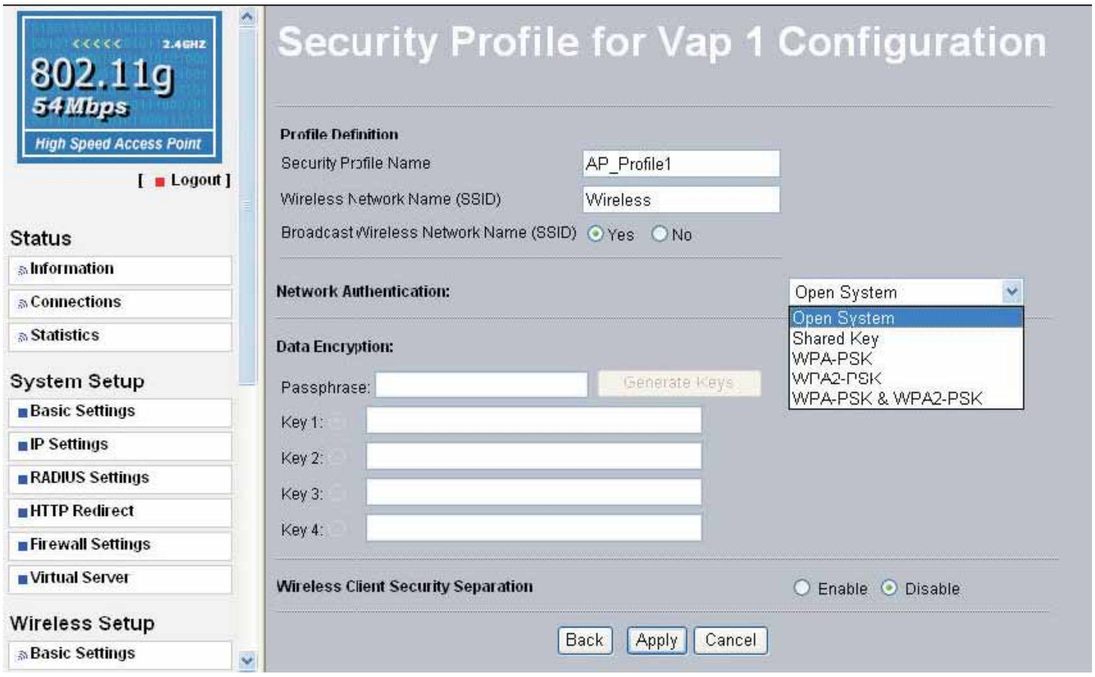
Security Profiles for Vap, Station Adapter, WDS and InterBuilding mode

	#	Profile Name	SSID	Security	Enable
○	1	AP_Profile1	Wireless	Open System	☑
○	2	AP_Profile2	Wireless	Open System	□
○	3	AP_Profile3	Wireless	Open System	□
○	4	AP_Profile4	Wireless	Open System	□
○	5	AP_Profile5	Wireless	Open System	□
○	6	AP_Profile6	Wireless	Open System	□
○	7	AP_Profile7	Wireless	Open System	□
○	8	AP_Profile8	Wireless	Open System	□
○		sta_profile	Wireless	Open System	☑
○		wds_profile			☑
○		interbuild_profile			☑

VLAN (802.1Q) Setup

1. AP_Profile1 VLAN ID:
2. AP_Profile2 VLAN ID:
3. AP_Profile3 VLAN ID:
4. AP_Profile4 VLAN ID:
5. AP_Profile5 VLAN ID:
6. AP_Profile6 VLAN ID:
7. AP_Profile7 VLAN ID:
8. AP_Profile8 VLAN ID:

You can configure each profile by clicking “Edit”. Such configuration as configuring profile name, SSID, enabling “broadcast SSID”, or doing security.
Figure 5-3 Security profile for Vap x



Security Profile for Vap 1 Configuration

Profile Definition

Security Profile Name: AP_Profile1

Wireless Network Name (SSID): Wireless

Broadcast Wireless Network Name (SSID) ● Yes ○ No

Network Authentication: Open System

Data Encryption:

Passphrase:

Key 1: ○

Key 2: ○

Key 3: ○

Key 4: ○

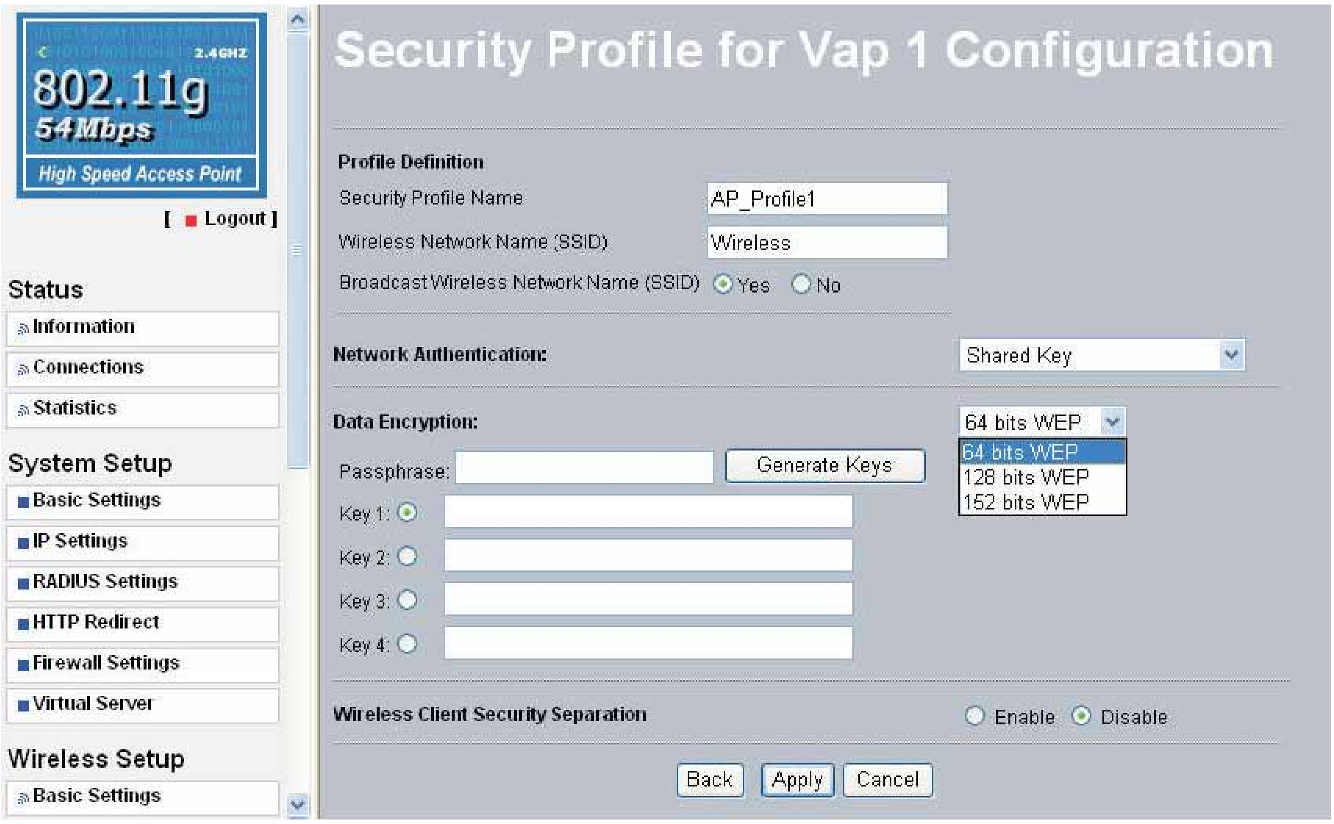
Wireless Client Security Separation ○ Enable ● Disable

5-3 Understanding WEP/WPASecurity Options

The following elaborate WEP/WPA security options.

Field	Description
Network Authentication	You have two authentication options. • Open System: No authentication is imposed to the radio. However, if the 802.1x option is configured, authentication of connections can be performed by a RADIUS server. • Shared: this is for shared key authentication. Data is encrypted.
Encryption Strength	You can select the following data encryption options: Disabled 64- 128- or 152-bit WEP With Open System Authentication and 64- 128- or 152-bit WEP Data Encryption with Shared Key authentication
Security Encryption (WEP) Keys	WEP enabled, you can manually enter the four data encryption keys or enable Passphrase to generate the keys automatically. These values must be matched between all Clients and access points at your LAN (key 1 must be the same for all, key 2 must be the same for all, etc.) Two ways to create WEP encryption keys: • Passphrase. Passphrase functions as automatically case-sensitive characters. However, not all wireless adapters support passphrase key generation. • Manual. These values are not case sensitive. 64-bit WEP: enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F). 128-bit WEP: enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F). 152-bit WEP: enter 32 hexadecimal digits (any combination of 0-9, a-f, or A-F).
WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)	WPA Pre-Shared-Key uses a pre-shared key to perform the authentication and generate the initial data encryption keys. Then, it dynamically varies the encryption key. It uses Temporal Key Integrity Protocol (TKIP) for encryption keys. However not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also

	support WPA.
WPA2-PSK	Identical to WPA-PSK with the exception of the way to Encryption keys. WPA2-PSK uses Advanced EncryptionStandard (AES) forencryption keys.
WPA-PSK& WPA 2-PSK	You may have the option of WPA-PSK associated with TKIP. Alternatively, you can select WPA2-PSK associated with AES.



Security Profile for Vap 1 Configuration

Profile Definition

Security Profile Name: AP_Profile1

Wireless Network Name (SSID): Wireless

Broadcast Wireless Network Name (SSID): ● Yes ○ No

Network Authentication: Shared Key

Data Encryption: 64 bits WEP (64 bits WEP / 128 bits WEP / 152 bits WEP)

Passphrase: [Generate Keys]

Key 1: ●

Key 2: ○

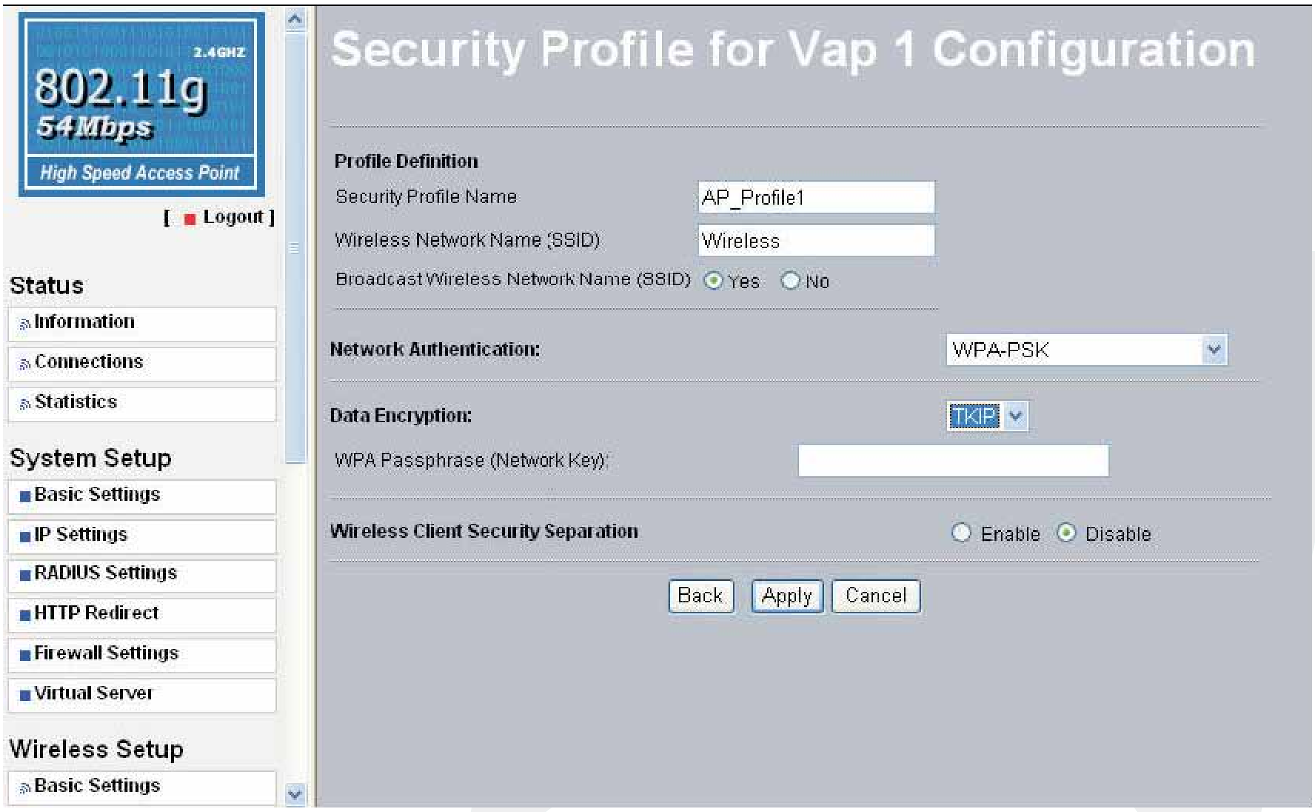
Key 3: ○

Key 4: ○

Wireless Client Security Separation: ○ Enable ● Disable

[Back] [Apply] [Cancel]

Figure 5-4 Security profile with WEP encryption



Security Profile for Vap 1 Configuration

Profile Definition

Security Profile Name: AP_Profile1

Wireless Network Name (SSID): Wireless

Broadcast Wireless Network Name (SSID) ● Yes ○ No

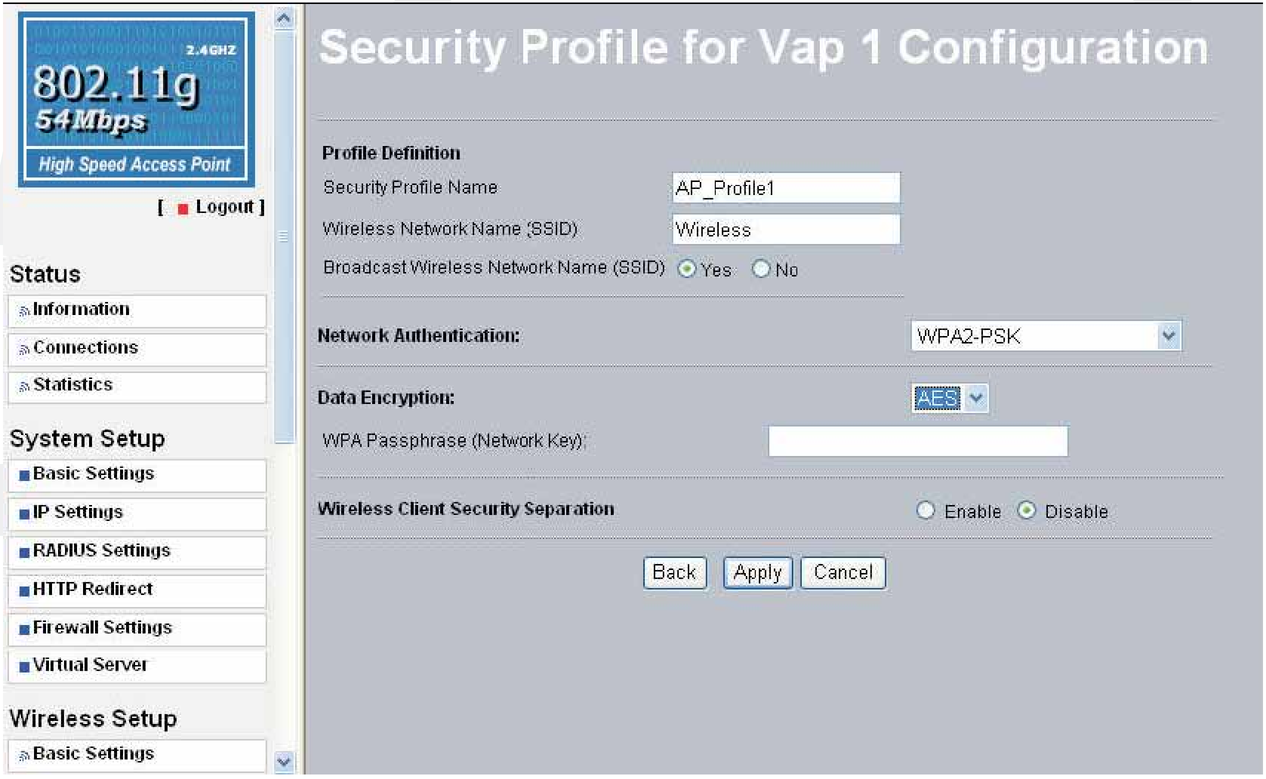
Network Authentication: WPA-PSK

Data Encryption: TKIP

WPA Passphrase (Network Key):

Wireless Client Security Separation ○ Enable ● Disable

Figure 5-5 Security profile with WPA-PSK



Security Profile for Vap 1 Configuration

Profile Definition

Security Profile Name: AP_Profile1

Wireless Network Name (SSID): Wireless

Broadcast Wireless Network Name (SSID) ● Yes ○ No

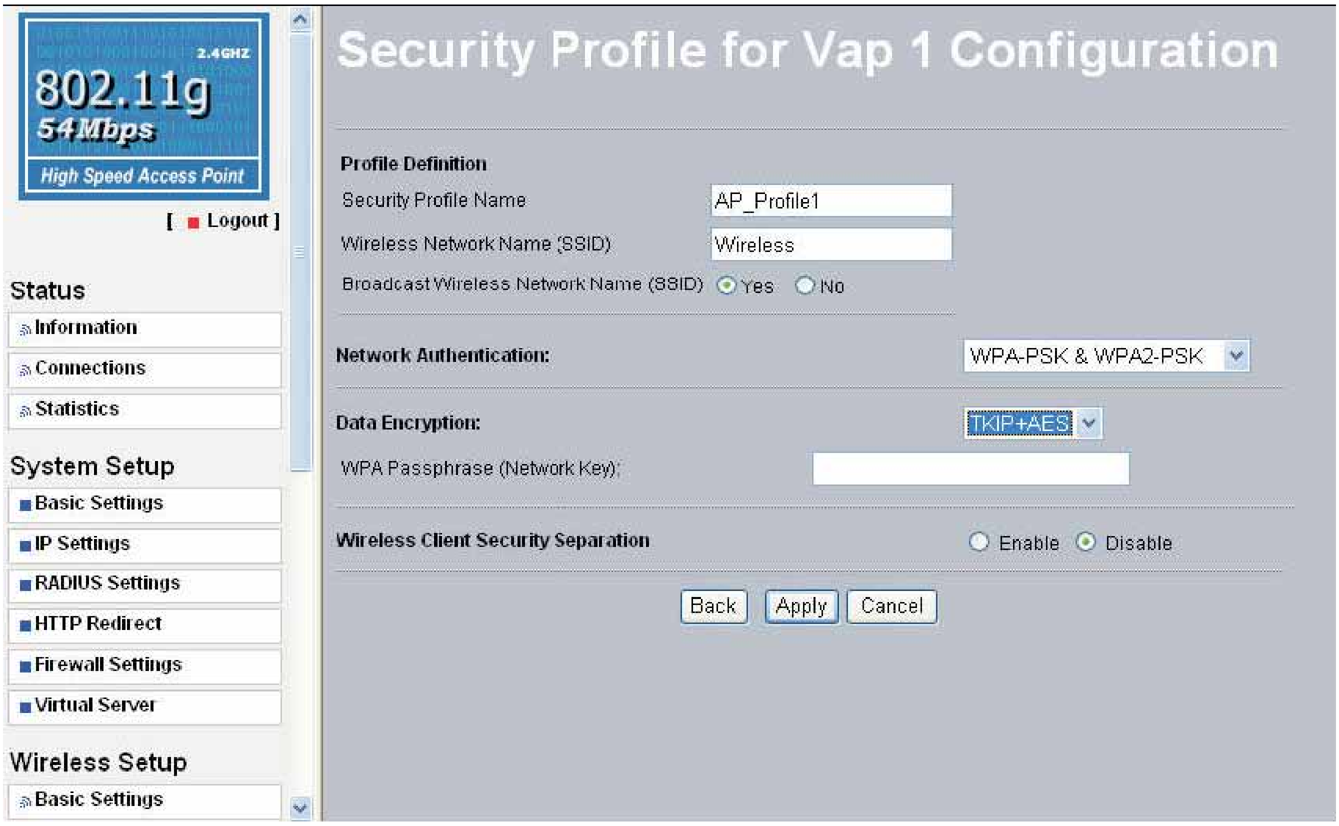
Network Authentication: WPA2-PSK

Data Encryption: AES

WPA Passphrase (Network Key):

Wireless Client Security Separation ○ Enable ● Disable

Figure 5-6 Security profile with WPA2-PSK



Security Profile for Vap 1 Configuration

Profile Definition

Security Profile Name: AP_Profile1

Wireless Network Name (SSID): Wireless

Broadcast Wireless Network Name (SSID): ● Yes ○ No

Network Authentication: WPA-PSK & WPA2-PSK

Data Encryption: TKIP+AES

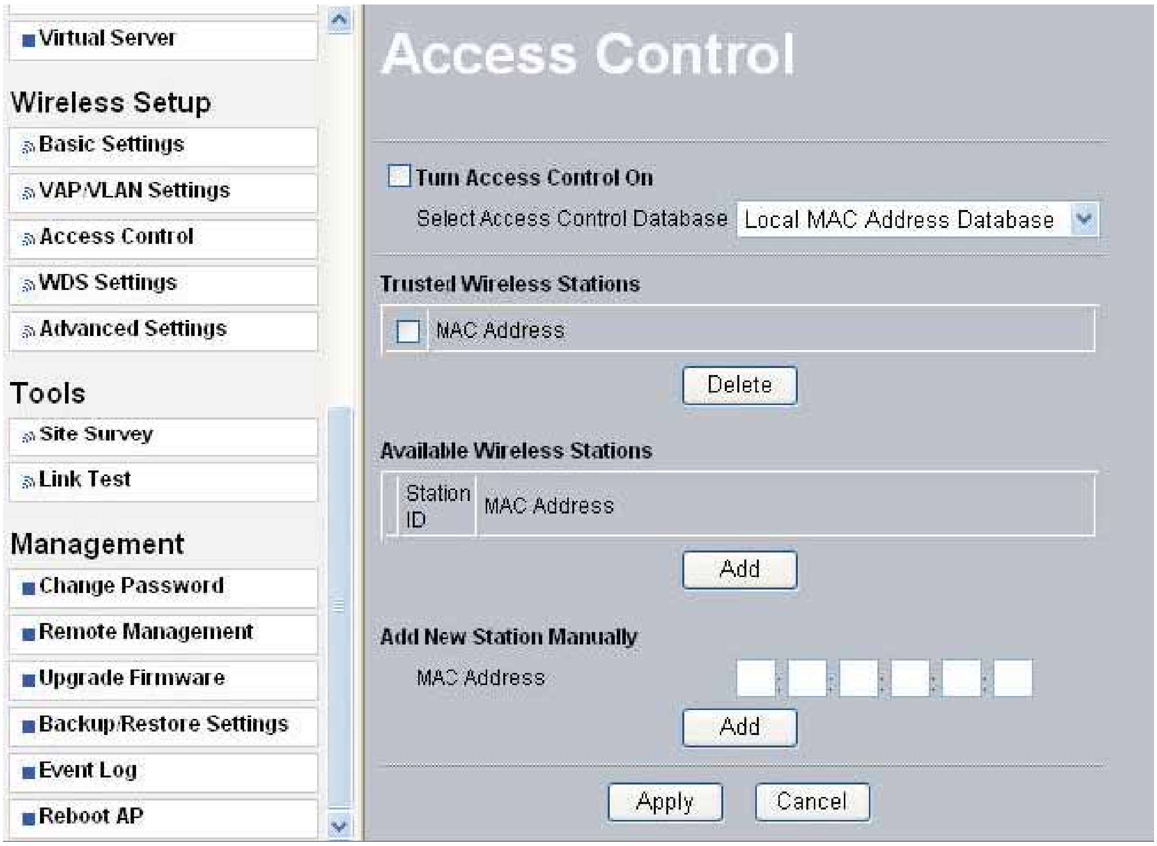
WPA Passphrase (Network Key):

Wireless Client Security Separation ○ Enable ● Disable

Figure 5-7 Security profile with WPA-PSK & WPA2-PSK

5-4 Access Control

Authentication by username and password is only part of the story. Frequently you want to let people in based on something other than who they are. Something such as where they are coming from. Restricting access based on something other than the identity of the user is generally referred to as Access Control.



Access Control

□ Turn Access Control On

Select Access Control Database: Local MAC Address Database

Trusted Wireless Stations

□	MAC Address

Available Wireless Stations

Station ID	MAC Address

Add New Station Manually

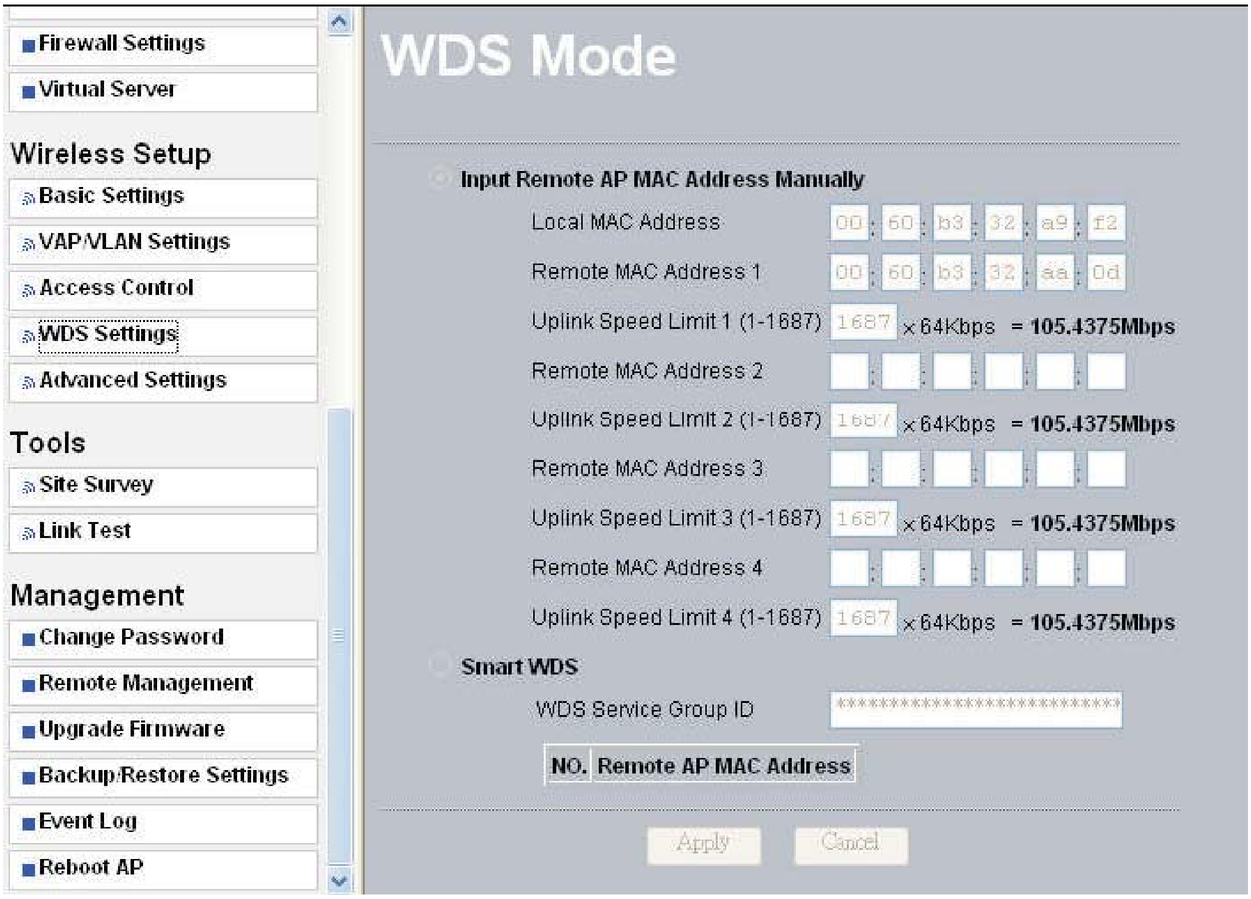
MAC Address: __ : __ : __ : __ : __ : __

Figure: 5-8 Access Control

You can restrict access to only trusted STAs so that those unknown STAs cannot wirelessly connect to the AP by turning Access Control on.
By entering MAC Address of new stations, you can manually add the stations to allow them to be connected to the radio.

5-5 WDS Mode

In a Wireless Distribution System (WDS) mode, multiple radios can be configured to operate in the WDS mode to inter-connect wired LAN segments that are attached to the radio. Up to four devices can be connected to the AP.



WDS Mode

○ Input Remote AP MAC Address Manually

Local MAC Address 00 : 60 : b3 : 32 : a9 : f2

Remote MAC Address 1 00 : 60 : b3 : 32 : aa : 0d

Uplink Speed Limit 1 (1-1687) 1687 ×64Kbps = 105.4375Mbps

Remote MAC Address 2 : : : : :

Uplink Speed Limit 2 (1-1687) 1687 ×64Kbps = 105.4375Mbps

Remote MAC Address 3 : : : : :

Uplink Speed Limit 3 (1-1687) 1687 ×64Kbps = 105.4375Mbps

Remote MAC Address 4 : : : : :

Uplink Speed Limit 4 (1-1687) 1687 ×64Kbps = 105.4375Mbps

○ Smart WDS

WDS Service Group ID ****************************

NO.	Remote AP MAC Address

- Local MAC Address:

This field provides the MAC address.

- Remote MAC Address:

Enter the MAC Address of your desired devices connected to the AP in WDS Mode.

- Uplink Speed Limit:

You can specify the transmission rate between the AP and other devices by entering the value in uplink speed limit. The most speed available is 1687 ×64Kbps=105.4375Mbps

5-6 Smart WDS

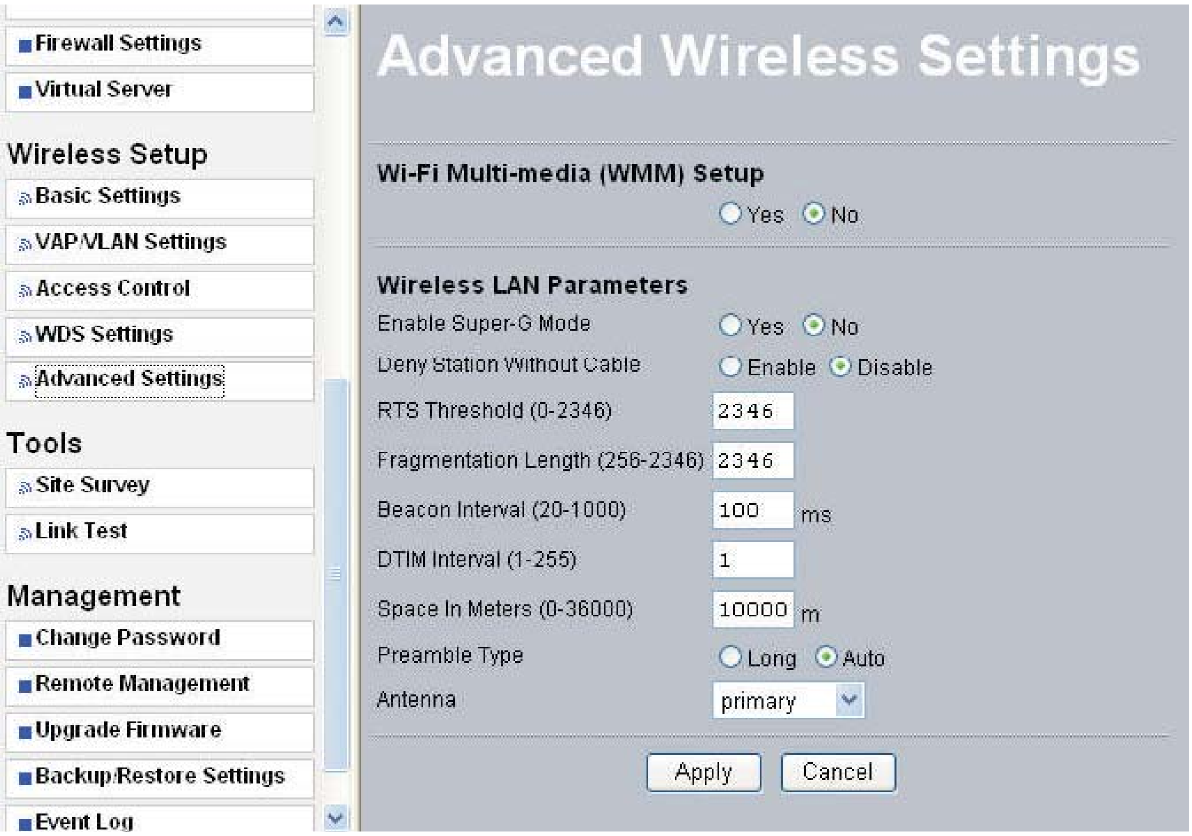
Under bridge mode, enabling smart WDS, the LP-348 can sniff other bridge mode radio around it and automatically connect those that work in the same channel.

- **WDS Service Group ID**

If two radios share the same group ID, they will be automatically connected.
Smart WDS can be activated on the premise that the radio must set to be AP mode.

5-7 Advanced Settings

The default advanced wireless LAN parameters usually streamline your work.



Advanced Wireless Settings

Wi-Fi Multi-media (WMM) Setup

○ Yes ● No

Wireless LAN Parameters

Enable Super-G Mode ○ Yes ● No

Deny Station Without Cable ○ Enable ● Disable

RTS Threshold (0-2346) 2346

Fragmentation Length (256-2346) 2346

Beacon Interval (20-1000) 100 ms

DTIM Interval (1-255) 1

Space In Meters (0-36000) 10000 m

Preamble Type ○ Long ● Auto

Antenna primary

• Wi-Fi Multi-media (WMM)

Currently interest and demand for multimedia applications and advanced capabilities are growing quickly. In the residential market, Voice over Internet Protocol (VoIP), video streaming, music streaming, and interactive gaming are among the most anticipated applications. In enterprise and public networks, support for VoIP, real time streaming of audio and video content, as well as traffic management, allows network owners to invent advanced methods to offer a richer and more diverse set of services.

WMM prioritizes traffic demands from different applications and extends Wi-Fi’s high quality end-user experience from data connectivity to voice, music, and video applications under a wide variety of environment and traffic conditions. WMM defines four access categories (voice, video, best effort, and background) that are used to prioritize traffic so that these applications have access to the necessary network resources. When your STA connect to the AP, you can enjoy high-quality multimedia function at your LAN, by enabling WMM.

Before enabling WMM, make sure your stations must also support WMM. Further, your operating system must be Windows XP with Service Pack 2.

- Super G and wireless parameters

Enabling super G, your transmission rate could reach up to 108Mbps.
The following describes the advanced wireless parameters.

RTS Threshold

The packet size used to determine whether it should use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) or the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) mechanism for packet transmission.

Fragmentation Length

This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value.

Beacon Interval

This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Access Point to keep the network synchronized. A beacon includes the wireless LAN service area, the AP address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM). Specifies the data beacon rate between 20 and 1000.

DTIM Interval

This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the 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.

Space in meters

This space in meter is used for extending ACK time-out destination. The setting range is 0-36000.

Preamble Type

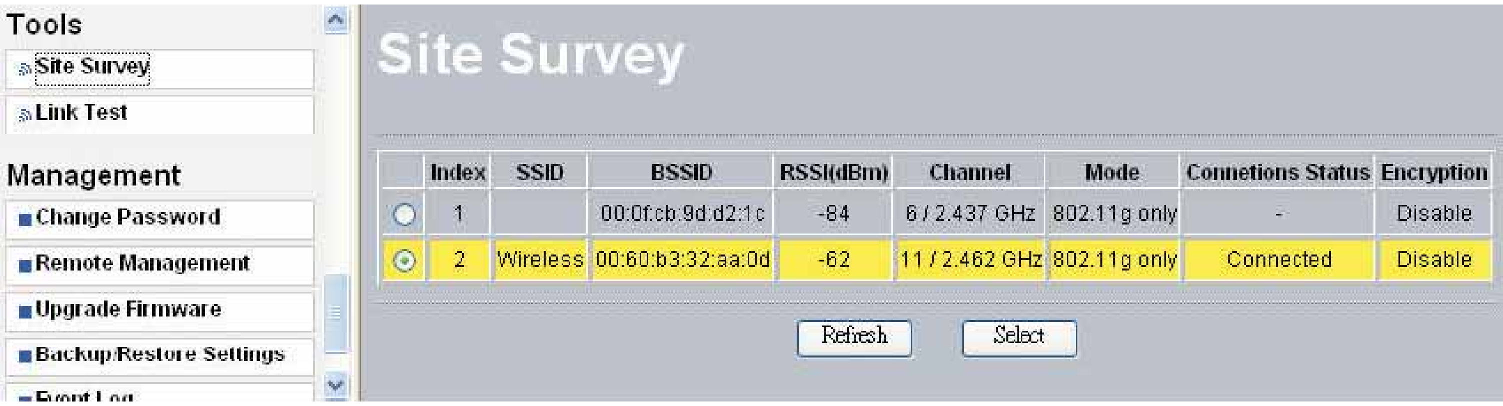
A long transmit preamble may provide a more reliable connection or slightly longer range. A short transmit preamble gives better performance. Auto is the default

Antenna

Select the desired antenna for transmitting and receiving. “Primary” is the default and must.

Chapter 6. Managing and Testing YourAP

6-1 Site Survey



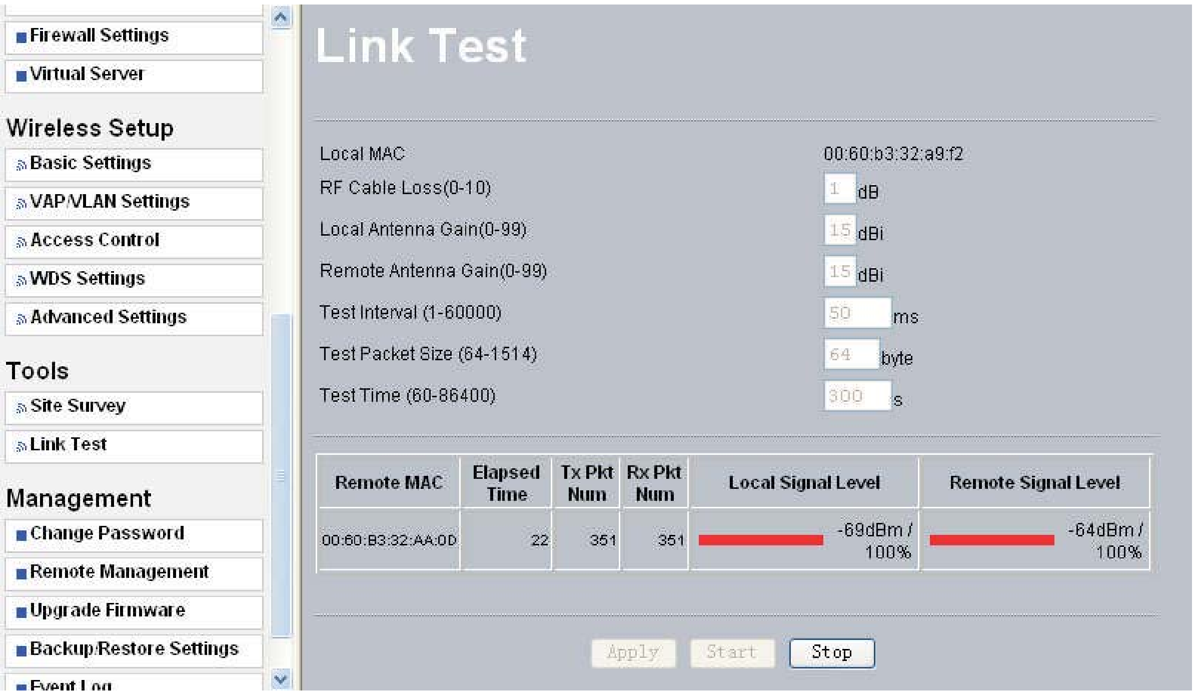
	Index	SSID	BSSID	RSSI(dBm)	Channel	Mode	Connetions Status	Encryption
○	1		00:0f.cb:9d:d2:1c	-84	6 / 2.437 GHz	802.11g only	-	Disable
●	2	Wireless	00:60:b3:32:aa:0d	-62	11 / 2.462 GHz	802.11g only	Connected	Disable

Figure: 6-1 Site survey

Site Survey provides you with a table of adjacent APs discovered by your radio when it acts as a station. In terms of each connected AP, Site Survey offers you their personal information, including SSID, BSSID, RSSI, channel mode, connection status and Encryption.

6-2 Link Test

To optimize the communication between your LAN, link test is designed to test the parameters that indicates communication quality.



Link Test

Local MAC 00:60:b3:32:a9:f2
RF Cable Loss(0-10) 1 dB
Local Antenna Gain(0-99) 15 dBi
Remote Antenna Gain(0-99) 15 dBi
Test Interval (1-60000) 50 ms
Test Packet Size (64-1514) 64 byte
Test Time (60-86400) 300 s

Remote MAC	Elapsed Time	Tx Pkt Num	Rx Pkt Num	Local Signal Level	Remote Signal Level
00:60:B3:32:AA:0D	22	351	351	🟥 -69dBm / 100%	🟥 -64dBm / 100%

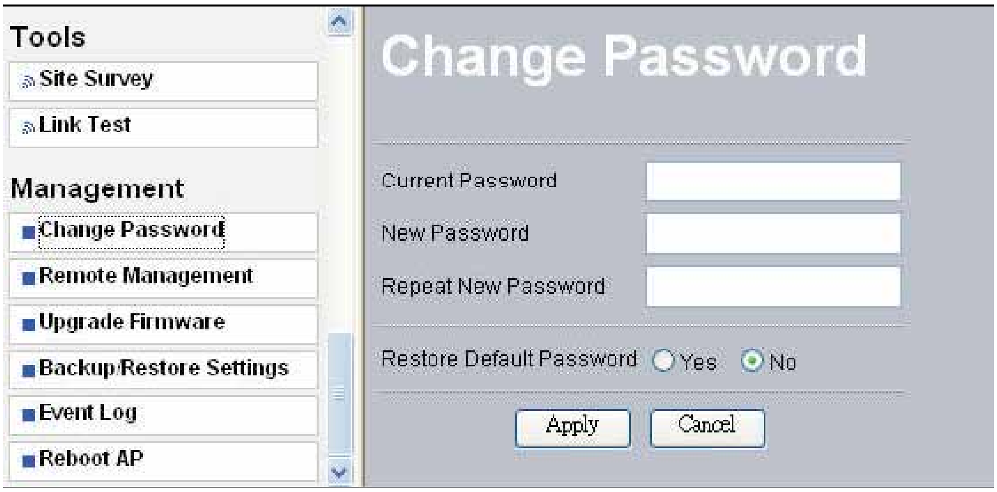
Figure: 6-2 Link test

We'll discuss parameters in link test.
• RF Cable Loss (0-10):
This indicates RF loss in cables, ranging from 0 to 10.
• Local Antenna Gain (0-99):
This indicates extended coverage provided by the local AP, for an existing 802.11 b/g wireless local area network (WLAN), ranging from o to 99.
• Remote Antenna Gain (0-99):
This indicates extended coverage provided by the remote AP, for an existing 802.11a/b/g
•Wireless local area network (WLAN).ranging from o to 99.
• Test Interval (1-60000): This provides testing time
• Test Packet Size (64-1514):
This test the size of packet transmitted between the two radios, ranging from 64 to 1514
• Test Time (60-86400):
This specifies how long the link test will last ranging from 60 to86400.

Chapter 7. Management

This chapter describes how to manage your radio.

7-1 Change Password



Current Password
New Password
Repeat New Password
Restore Default Password ○ Yes ● No

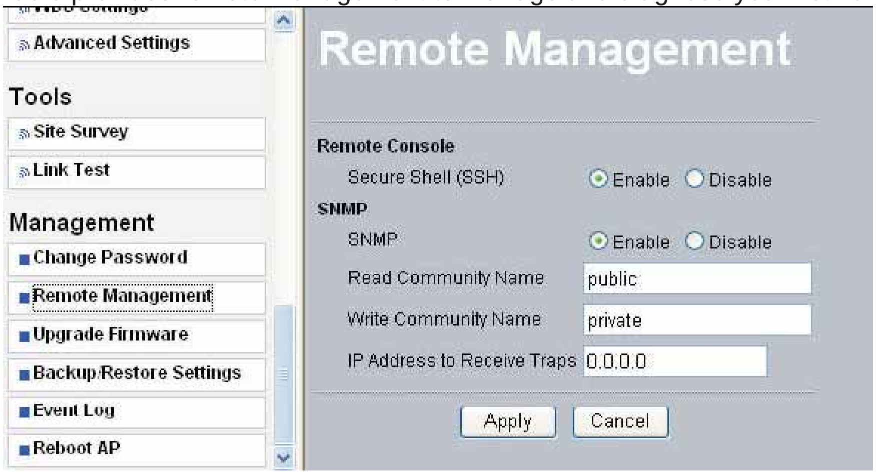
Figure: 7-1 Change Password

You can have your desired password by changing password.
Take the following steps to change password.
• Enter your currently-used password in the current field.
• Enter your new password in the New Password field.
• Re-enter the new password to confirm it in the Repeat New Password field.
Finally, click “Apply” to save the change.
Also, if you desire to restore to the factory-set password, please click “Yes”.
The default setting is disabled.

7-2 Remote Management

This radio provides remote management to manage and diagnose your network

.



Remote Management

Remote Console

Secure Shell (SSH) ● Enable ○ Disable

SNMP

SNMP ● Enable ○ Disable

Read Community Name: public

Write Community Name: private

IP Address to Receive Traps: 0.0.0.0

Figure: 7-2 Remote Management

SSH

Secure Shell (SSH) is a program that provides a cryptographically secure replacement for Telnet that is considered the de facto protocol for remote logins. SSH runs in the Application Layer of the TCP/IP stack. SSH provides a secure connection over the Internet providing strong user authentication. SSH protects the privacy of transmitted data (such as passwords, binary data, and administrative commands) by encrypting it. SSH clients make SSH relatively easy to use and are available on most computers including those that run Windows or a type of UNIX. SSH clients are also available on some handheld devices.

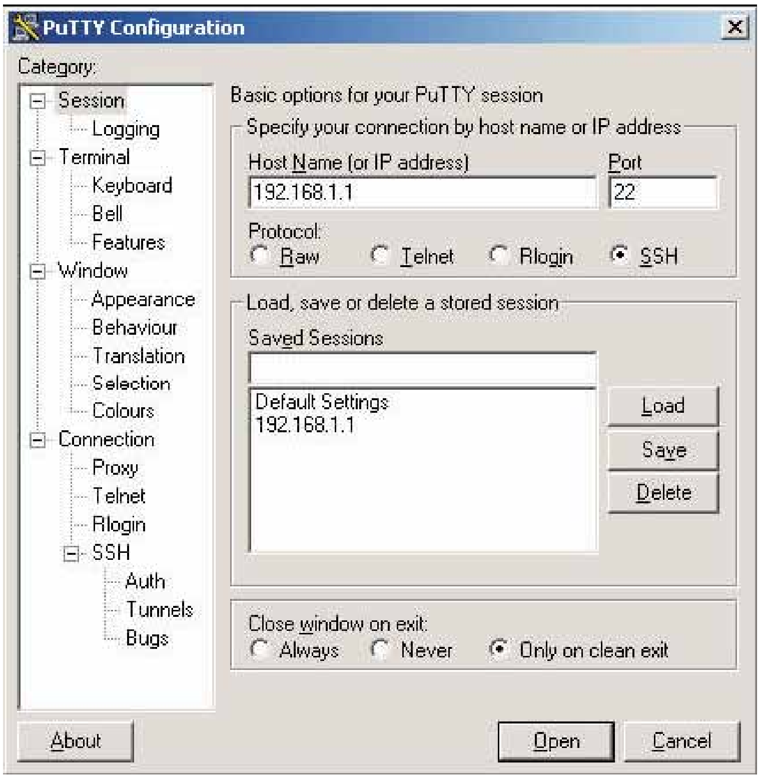
SSH on the radio is enabled by default. When user manager is enabled, SSH uses the same usernames and passwords established by the user manager.

The applicability of SSH for the radio allow you to have insight into your LAN.

If your computer does not have the SSH client installed, you must procure and install it before you can proceed. You can download the latest SSH client from the following site: http://ssh.com/.

Take the following steps to manage this radio via SSH:

1. From the Putty Configuration, enter IP address in host name field and port number in port field. Also, select SSH as protocol.



Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address): 192.168.1.1

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Load, save or delete a stored session

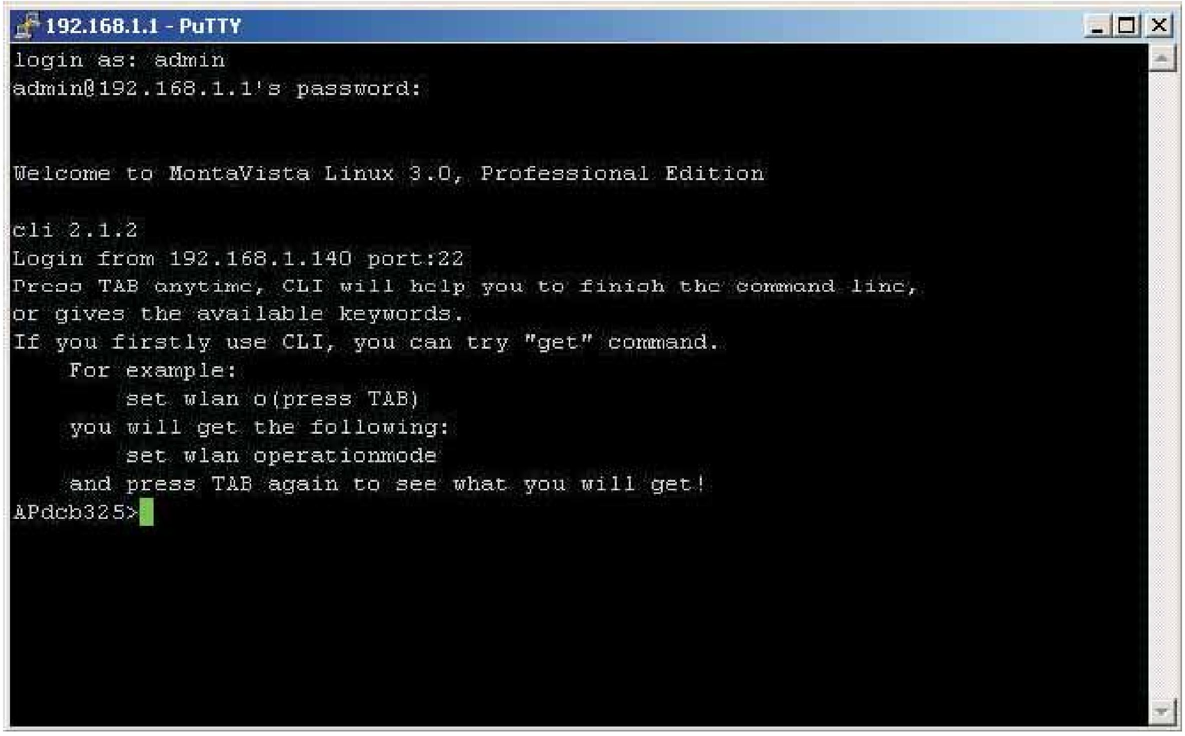
Saved Sessions

Default Settings
192.168.1.1

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure: 7-3 Putty configuration utility

2. Press Open, and the screen below should appear.



```
login as: admin
admin@192.168.1.1's password:


Welcome to MontaVista Linux 3.0, Professional Edition

cli 2.1.2
Login from 192.168.1.140 port:22
Press TAB anytime, CLI will help you to finish the command line,
or gives the available keywords.
If you firstly use CLI, you can try "get" command.
    For example:
        set wlan o(press TAB)
    you will get the following:
        set wlan operationmode
    and press TAB again to see what you will get!
APdcb325>
```

Figure: 7-4 Putty configuration page

The login name is admin and password is the default password. After successful login, the screen should show the APdcb325>. In this example, the APdcb325 is the radio name.. Enter help to display the SSH command help.

SNMP

SNMP (simple network management protocol) is a distributed-management protocol. Via SNMP, you have access to administrate your AP remotely.

Read Community Name: You have access to read rather than write. The default name is public.

Write Community Name: The default name is private.

7-3 Upgrade Firmware

When uploading software to the LP-348 Access Point, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, the upload may fail, corrupt the software, And render the AP completely inoperable.

The software of the radio is stored in FLASH memory, and can be upgraded as new software is released by. The upgrade file can be sent via your browser.

The Web browser used to upload new firmware into the AP must support HTTP uploads, such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above.

1. Download the new software file and save it to your hard disk.

2. From the main menu Management section, click the Upgrade Firmware link to display the screen above.

3. In the Upgrade Firmware menu, click the Browse button and browse to the location of the image (.RMG) upgrade file.

4. Click Upload. When the upload completes, your wireless access point will automatically restart. The upgrade process typically takes about 150 seconds. In some cases, you may need to reconfigure the wireless access point after upgrading.

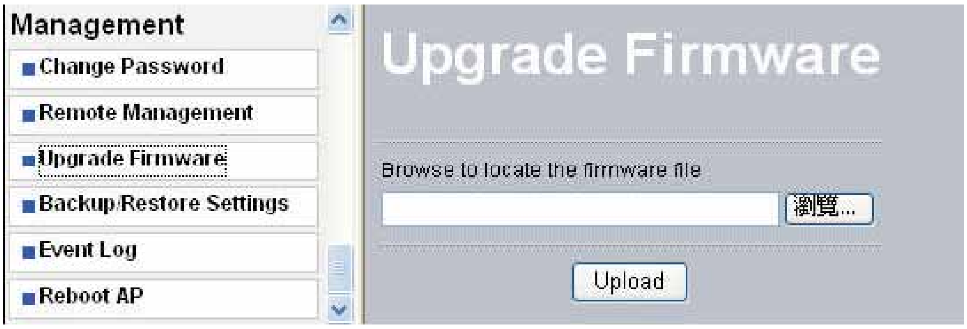
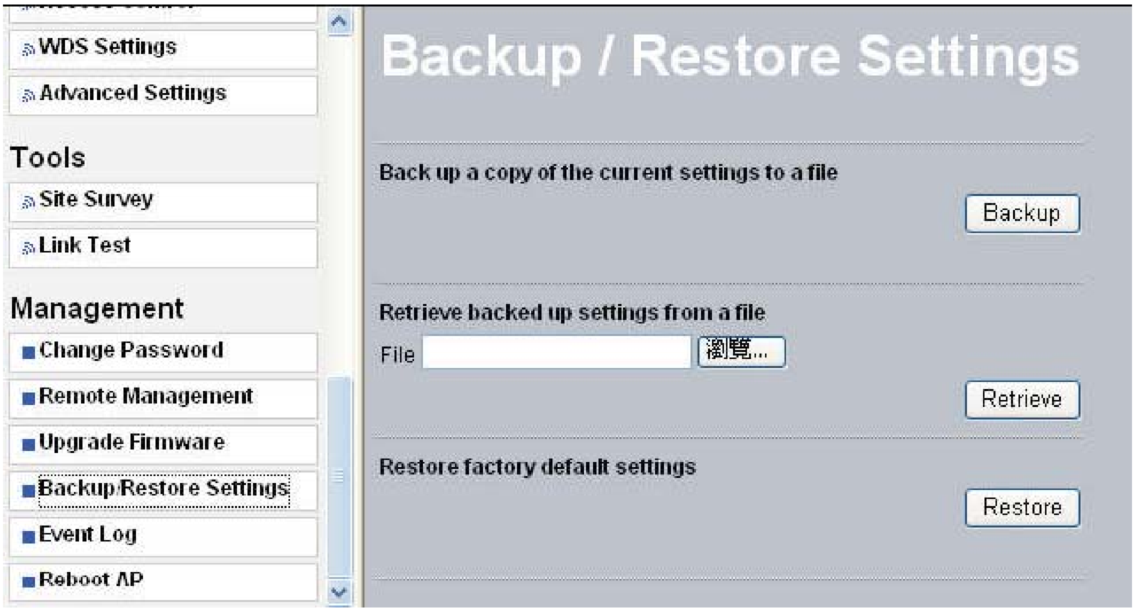


Figure: 7-5 Upgrade Firmware

7-4 Backup / Restore Settings

Radio provides backup and restore for file management.



Backup / Restore Settings

Back up a copy of the current settings to a file

Retrieve backed up settings from a file

File

Restore factory default settings

Figure: 7-6 Backup / Restore Settings

Backup

You have access to back up the currently settings by enabling radio ‘s Backup function.

Retrieve:

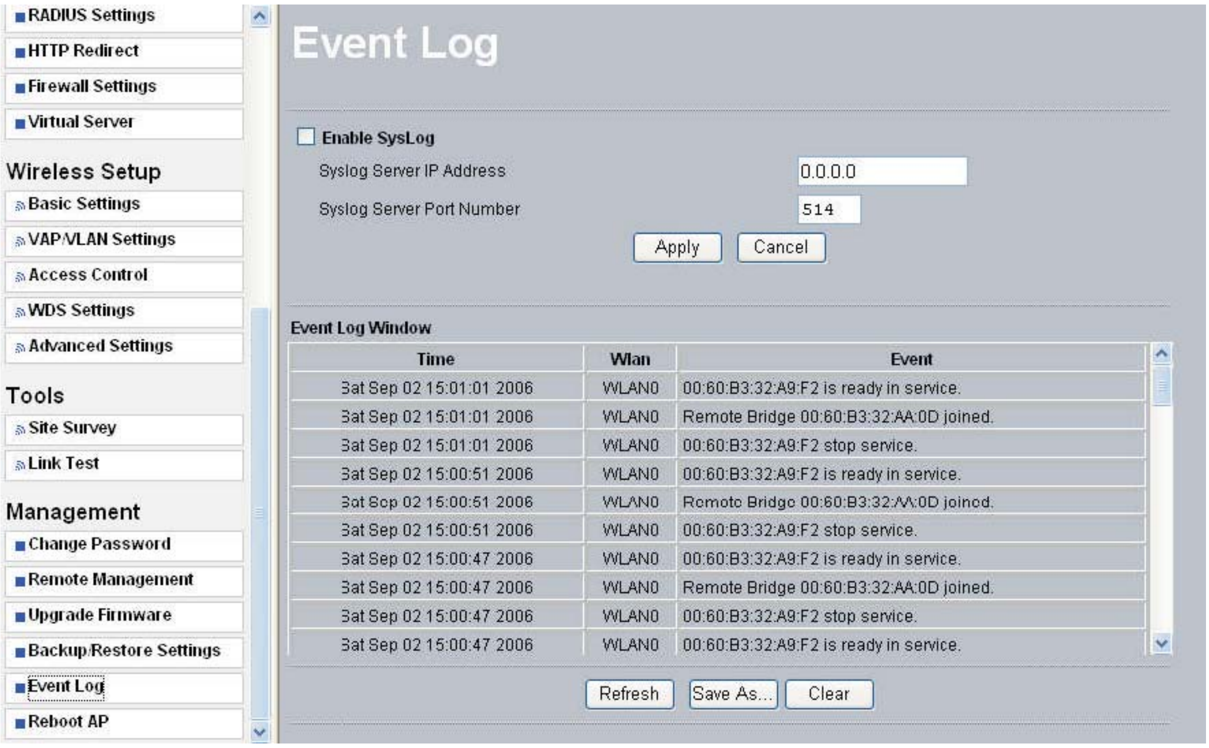
Retrieve button allows you to retrieve your backup files.

Restore:

This button can be used to clear ALL data and restore ALL settings to the factory default Values.

7-5 Event Log

If you have a SysLog server on your LAN, enable the SysLog option. Event Log offers you activity log information.



Event Log

□ Enable SysLog

Syslog Server IP Address 0.0.0.0

Syslog Server Port Number 514

Event Log Window

Time	Wlan	Event
Sat Sep 02 15:01:01 2006	WLAN0	00:60:B3:32:A9:F2 is ready in service.
Sat Sep 02 15:01:01 2006	WLAN0	Remote Bridge 00:60:B3:32:AA:0D joined.
Sat Sep 02 15:01:01 2006	WLAN0	00:60:B3:32:A9:F2 stop service.
Sat Sep 02 15:00:51 2006	WLAN0	00:60:B3:32:A9:F2 is ready in service.
Sat Sep 02 15:00:51 2006	WLAN0	Remote Bridge 00:60:B3:32:AA:0D joined.
Sat Sep 02 15:00:51 2006	WLAN0	00:60:B3:32:A9:F2 stop service.
Sat Sep 02 15:00:47 2006	WLAN0	00:60:B3:32:A9:F2 is ready in service.
Sat Sep 02 15:00:47 2006	WLAN0	Remote Bridge 00:60:B3:32:AA:0D joined.
Sat Sep 02 15:00:47 2006	WLAN0	00:60:B3:32:A9:F2 stop service.
Sat Sep 02 15:00:47 2006	WLAN0	00:60:B3:32:A9:F2 is ready in service.

Figure: 7-7 Event log

- SysLog Server IP address:

The radio will send all the SysLog to the specified IP address if SysLog option is enabled.

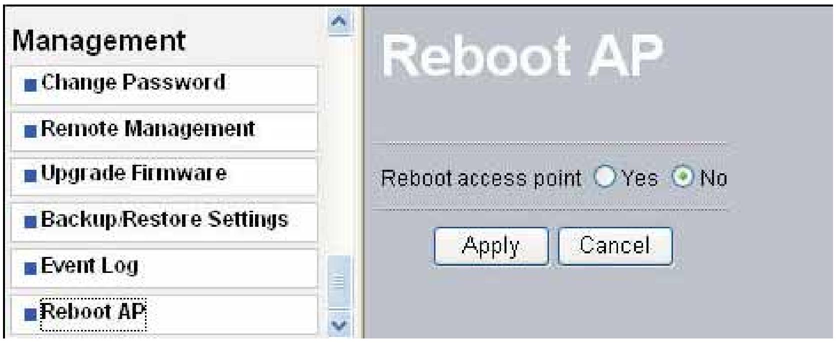
Default: 0.0.0.0

- Syslog Server Port Number:

The port number configured in the SysLog server on your network. Default: 514

7-6 Reboot AP

In some cases, if you want to reboot AP, click Yes and then apply. AP will reboot.



Reboot access point ○ Yes ● No

Figure: 7-8 Reboot AP

7-7 Hardware reset

If your Web User Interface stops responding, ping the IP address of the radio to check whether “reply” is obtained, or unplug and then plug back in the power supply of the Wireless AP Access Point. This will reboot the Wireless AP Access Point. If you are still unable to communicate with the Web User Interface, screw off the screw next to the grounding stud. Then use a stick to press in and hold the RESET button for five to ten seconds. This will reset the WirelessAP Access Point to the factory default settings. If you applied any personal configuration settings, you will need to make the changes again. Below is the tool to revolve the screws and press the reset button for your reference: Figure: 7-8 Tool to screw off the screw of reset button.

Chapter 8. Trouble Shooting

This chapter helps you to isolate and solve the problems with the 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.

8-1 General Descriptions

To successfully use the radios, engineers must be able to troubleshoot the system effectively. This section will show you how an 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.

8-2 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 192.168.1.1). If there 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.

8-3 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 filter
*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

NOTE

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

8-4 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.

NOTE 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.

NOTE Please contact your local vendor for advance technical support or Support@lan-products.com