LOHU 5158P V2

Outdoor Wireless AP/Bridge

User Manual
Version 1.3

LohuisNetworks

Voltlaan 408 – 2681 TV Monster – Netherlands
Tel : +31208080743
Email : Info@lohuisnetworks.com
Website : www.lohuisnetworks.com

International Numbers:

Dubai :	+97142280111
United States:	+12123812983
United Kingdom:	+442033557669
France :	+33170612716
Italy:	+390662207084
Japan:	+81345506867
Argentina:	+541152391407
Brazil :	+552135219853
Pakistan:	+92217019804

Chapter 1. Introduction

Thank you for choosing this 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 Overview

802.11a-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 radio 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 radio 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 802.11a 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. Station Adapter
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 802.11a 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 7

●**Atheros Super G Mode**

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 broadcasted; assuring only clients configured with the correct SSID can connect.

1-4 System Requirements

Before installing the radio, make sure your system meets these requirements

• The Category 5 UTP straight through Ethernet cable with RJ-45 connector. (Between switch and POE). Category 5 UTP cross-over is required between PC and POE.

• 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

Chapter 2. Basic Installation and Security

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

3-1 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
- 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 802.11a
- Channel / Frequency 52 / 5260 MHz
-

3-2 Wireless Security Options

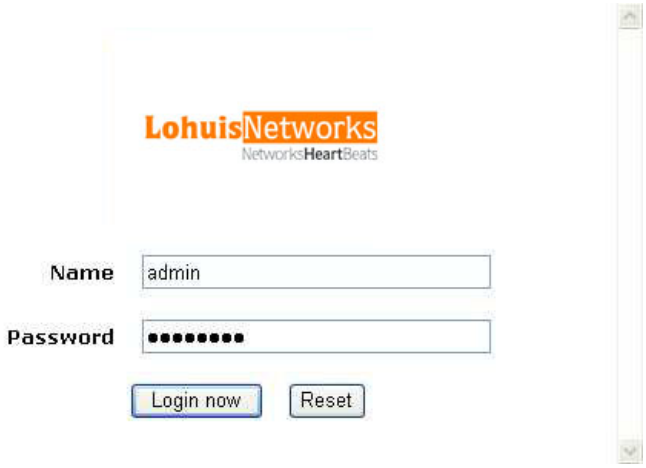
To make wireless networking as safe and easy as possible, this radio provides several network security features, but requires specific programming and setup.

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. A very strong authentication key 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 **disabled**.

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

Before installing, you should make sure that Ethernet network is working perfectly. You will be connecting the radio to the Ethernet network so that computers with 10/100 Fast Ethernet adapters will communicate with other computers on the Ethernet.
1. SET UP THE AP:
Before mounting the radio in a high location, first set up and test the radio to verify wired network connectivity at ground level or indoors.
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:



AP log 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.

Figure: 3-2 AP general information

Chapter 3. General Information

General information gives you a basic concept of the radio.

4-1 Information

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 LOHU.
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 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
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 802.11a access point. 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 (Point-to-Point) 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 bridges or use SSID to communicate with other wireless station. WEP should be used to protect this communication mode.
Inter-building This is the LOHU's own brand of WDS mode. In this mode, the AP will automatically connect to another LOHU Radio which is set to inter-building mode, without

manually entering MAC address for each other. This creates a unique link to LOHU radios only.

Wireless Mode The only option available is 802.11a.

Channel This field identifies which operating frequency will be used.

Security Profiles This provides a list of other APs with proper identification data.

4-2 Connection

Under the Information heading, click the connection link to view the connection status shown below. This information is useful for identifying clients on the network.

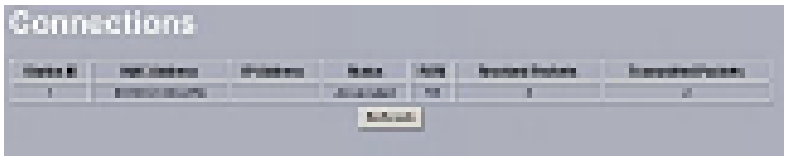


Figure: 4-1 AP connection status

Statistics

The statistics provide various LAN and WAN statistics.

Figure: 4-2 statistics

Chapter 4. Added Functionalities

5-1 Time Server

By click Basic Settings, the "Basic Settings" will appear shown below.

Figure: 5-1 AP Basic settings

The AP allows you to synchronize the time between your network and time server by using an NTP Time Server.
The Time Sever provides correct and current time in any world time zone, country or major city. Accurate adjustments for Daylight Saving Time are made according to eachlocation'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.

5-2 Bridge/Router Mode

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

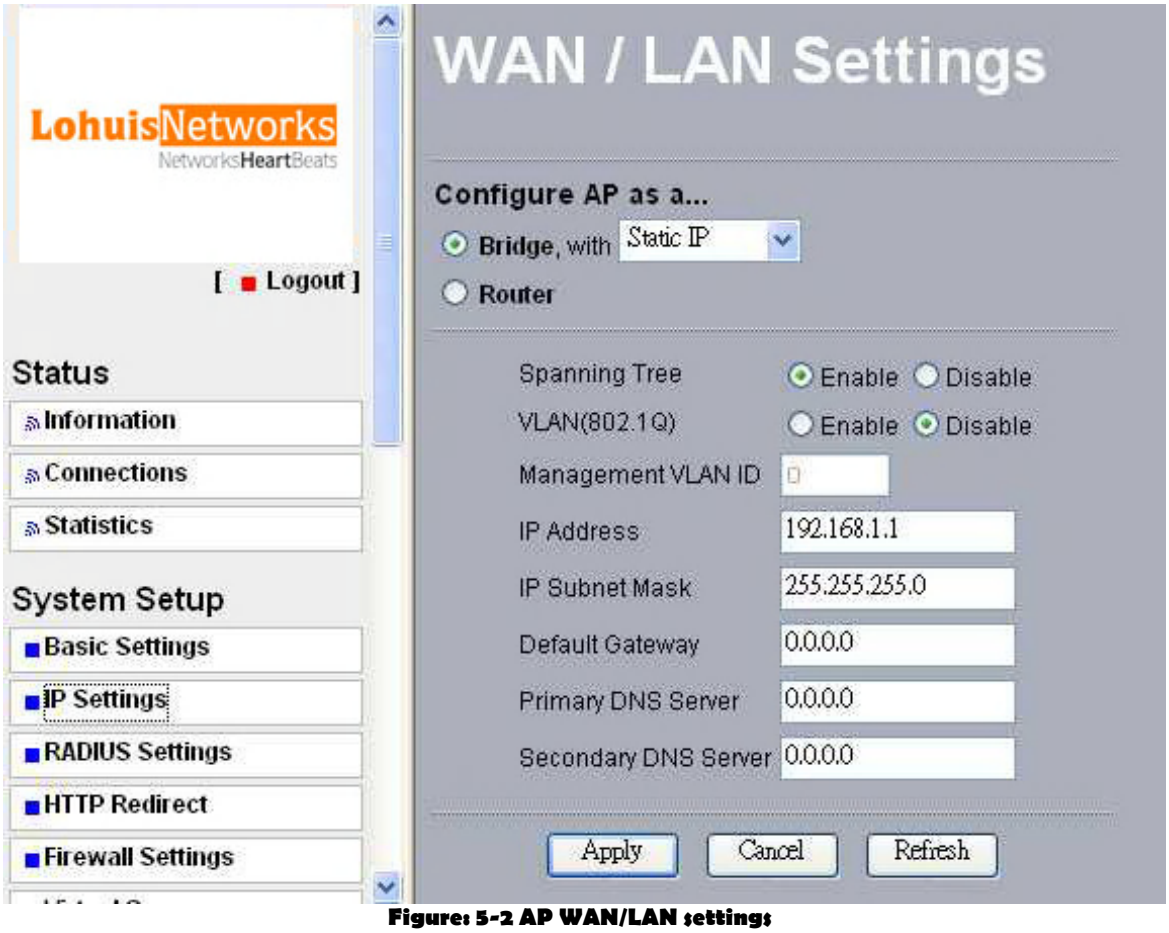


Figure: 5-2 AP WAN/LAN settings

The LOHU Series Radio can be configured in bridge mode or router mode.

Bridge Mode

In Bridge Mode, the AP will act as a pass-through bridging your network, by associating with various devices. This can extend the 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

In 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.

5-3 Any IP

If the IP address has slipped your mind, any IP functionality can offer peace of mind.

Enabling any IP, you'll feel free to enter IP Address, IP Subnet Mask and Gateway, enjoying internet surf.
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

5-4 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.

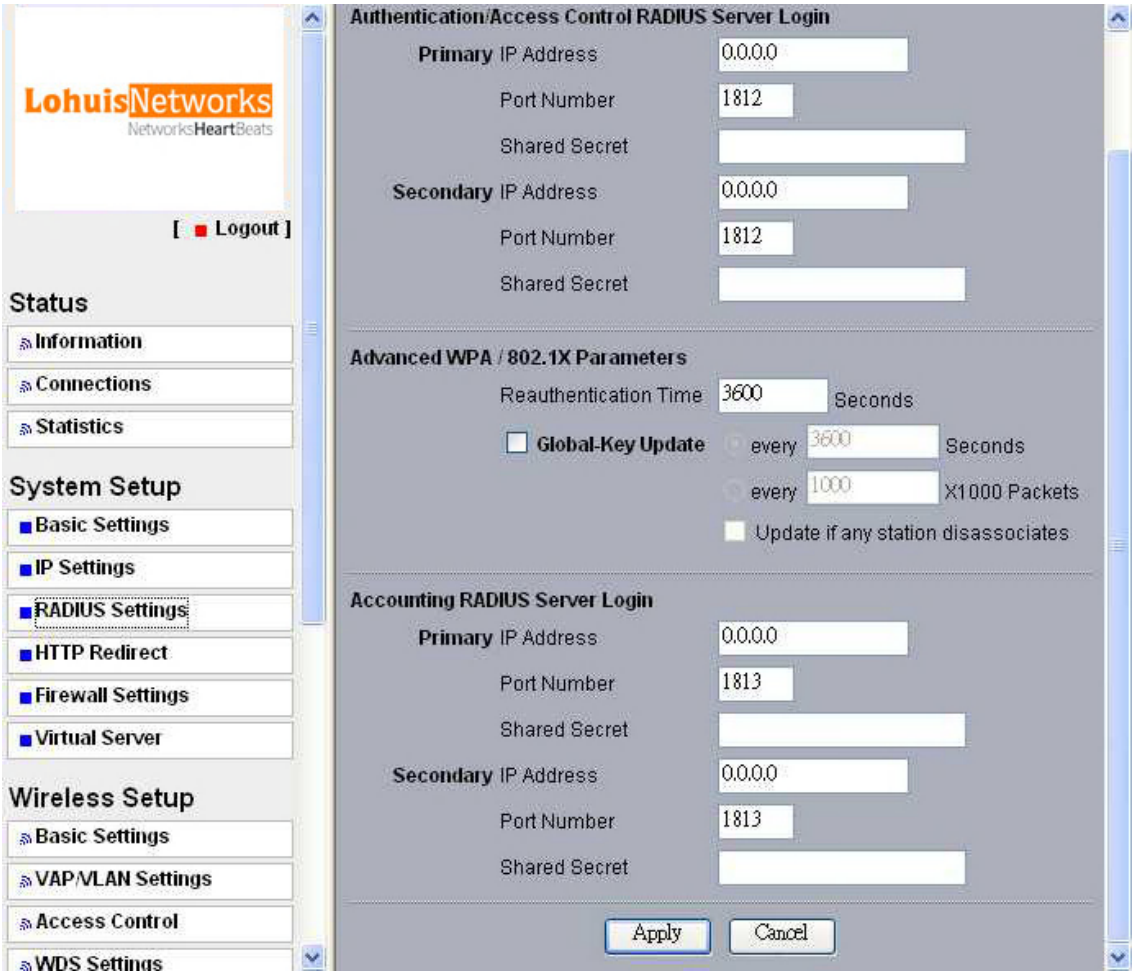


Figure: 5-3 AP Radius settings

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.

5-5 HTTP Redirect

Enabling HTTP redirect, you can enter a corporate URL (for example, (http://www.yourcompany.com). It is your desired web page that first appears when someone is surfing the internet, via a station connected to your radio (which is set to be an AP).
The following is the HTTP Redirect Settings.

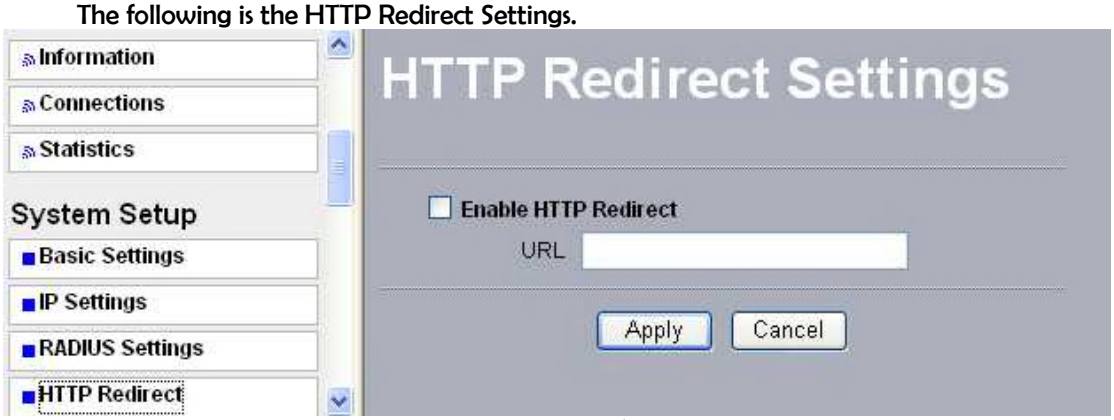


Figure: 5-4 AP HTTP Redirect settings

URL
Enter your desired website in this field. Be sure to click "Apply" to save the configuration.
Be sure your AP is connected to the internet when using HTTP Redirect.

5-6 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. This radio (access point) is also qualified for firewall management , Acting as a firewall, the radio will filter your undesired data and protocols, only delivering the wanted information to your PC.

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

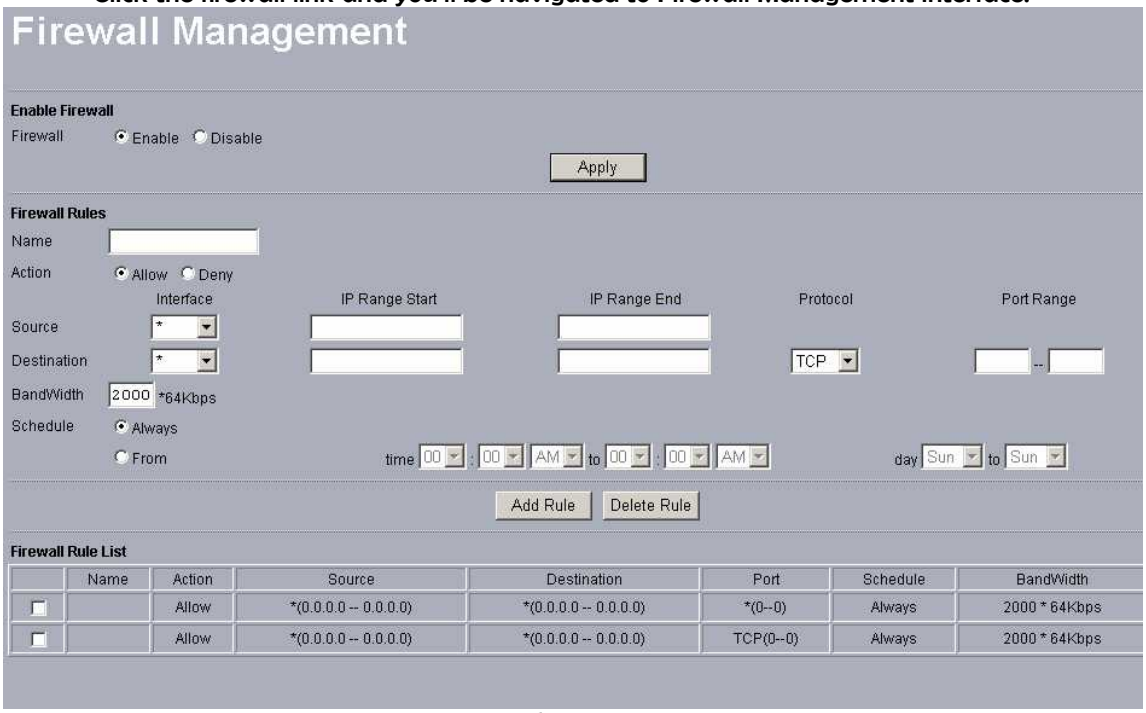


Figure: 5-5 AP firewall management

Before applying the firewall management, you need to enable the 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".

Using an asterisk (*) indicates any protocol may be allowed or denied.

Port Range

This specifies your IP port range.

Schedule

You can set the 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: 5-6 Firewall list

5-7 Virtual Server

Virtual server can only be enabled while the radio is in 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.

In 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, or enjoy e-mails, only via your PC.

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. Select TCP or UDP.

Private Port

This specifies your LAN port.

Public Port

This specifies your WAN port.

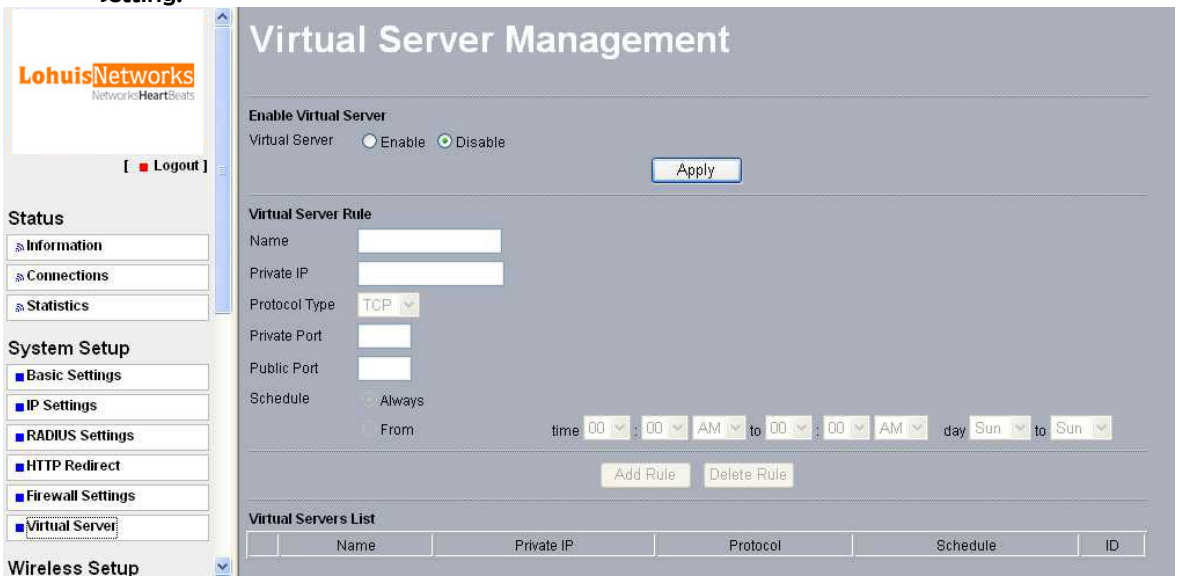
Schedule

You can set a time-limit when your AP acts as a virtual server, by enabling "from". Alternatively, if you desire your AP to always act as a virtual server, 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

6-1 Basic Settings

The versatile LOHU Series Radio provides up to five operating modes for your various purposes.

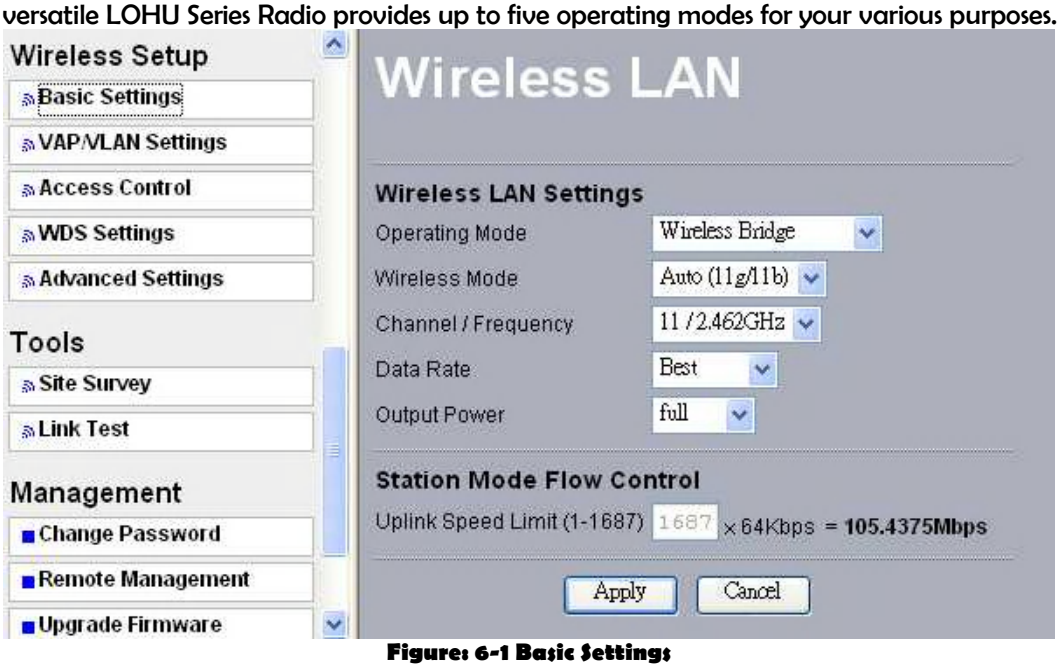


Figure: 6-1 Basic Settings

Operating Mode

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

Access Point

Any 802.11a wireless station can communicate with it by 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 secure all data.

Inter-building

This is the LOHU's own brand of WDS mode. In this mode, the AP will automatically connect to another LOHU Radio which is set to inter-building mode, without manually entering MAC address for each other. This creates a unique link to LOHU radios only.

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

Only 802.11a is available.

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 Speed Limit (1-1687): It indicates the transmission rate.

6-2 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. The LOHU's VLAN (Virtual Local Area Network) technology can help overcome this difficulty. Now it is possible for these multi devices in function without the need for multiple physical network APs. See the diagram below:

Under this mode, this radio can behave as (up to) 8 virtual Wireless LAN infrastructures. You can specify unique SSIDs for these virtual 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 essentially, you'll be seeing up to 8 different wireless networks.

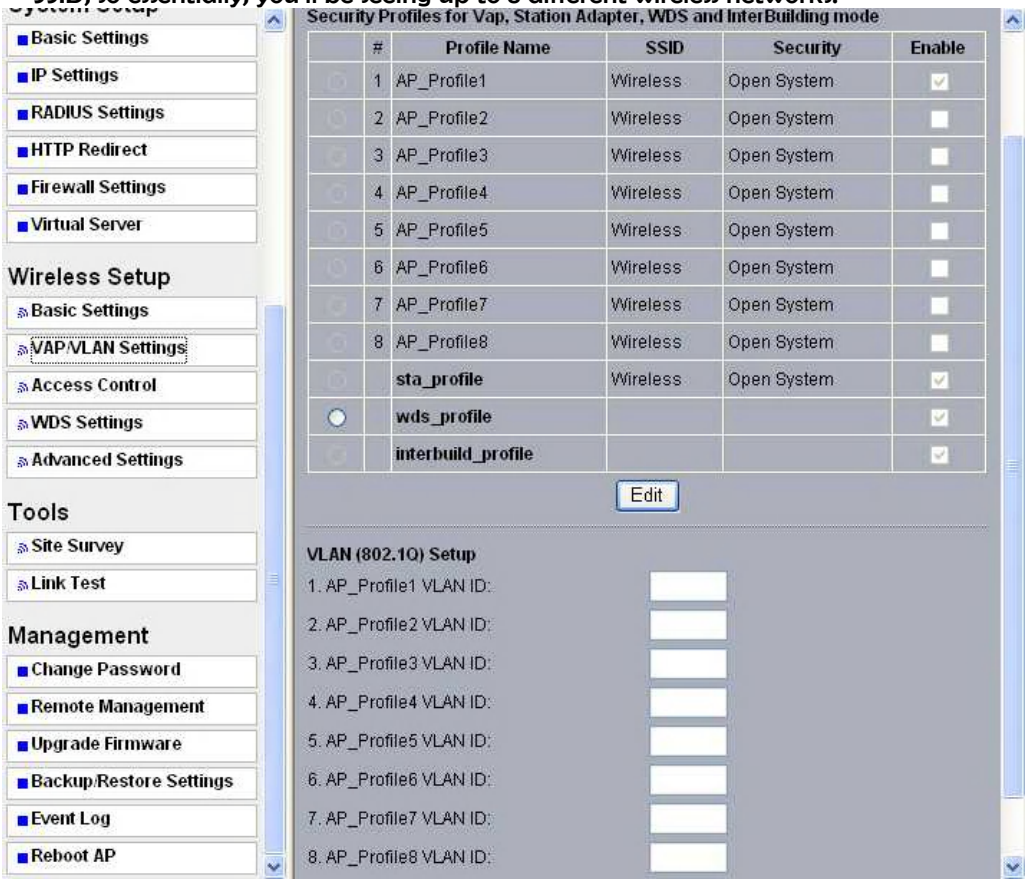


Figure 6-2 VAP / VLAN Settings

You can configure each profile by clicking "Edit". Such configuration as configuring profile name, SSID, enabling "broadcast SSID", or doing security.

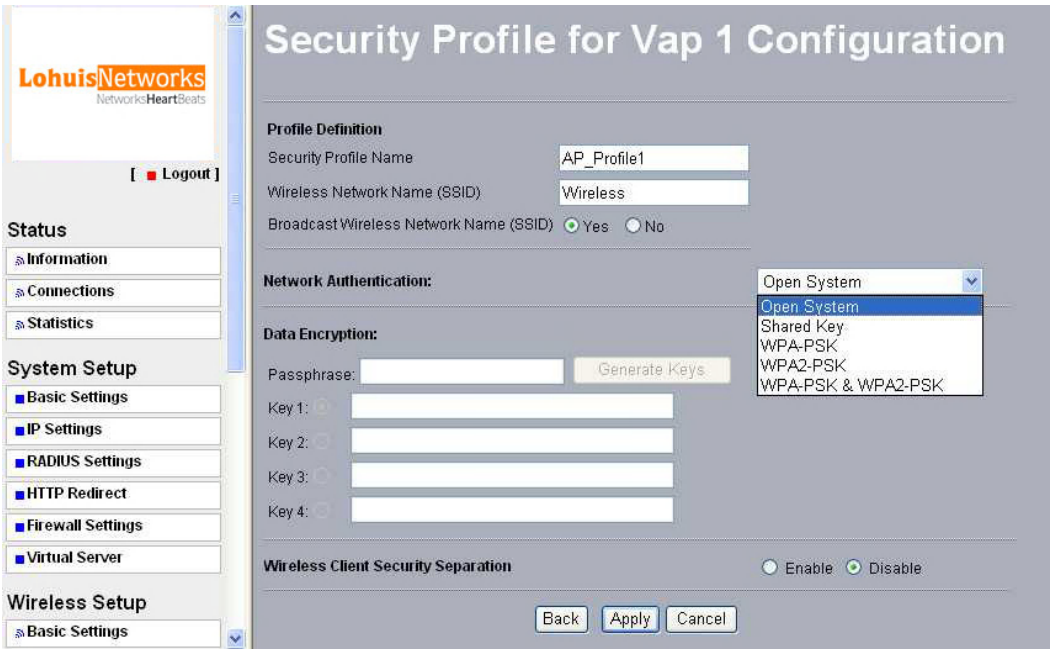


Figure 6-3 Security profile for Vap x

6-3 Understanding WEP/WPA Security Options

Network Authentication:

You have two authentication options.

• Open System:

No authentication is imposed on 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 :

With WEP enabled, you can manually enter the four data encryption keys or use a passphrase to generate the keys automatically. These values must be matched between all clients and access points on 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 IntegrityProtocol (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.

WPA 2-PSK:

Identical to WPA-PSK with the exception of the way to encryption keys.
WPA2-PSK uses Advanced Encryption Standard (AES) for encryption 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.

Figure 6-4 Security profile with WEP encryption

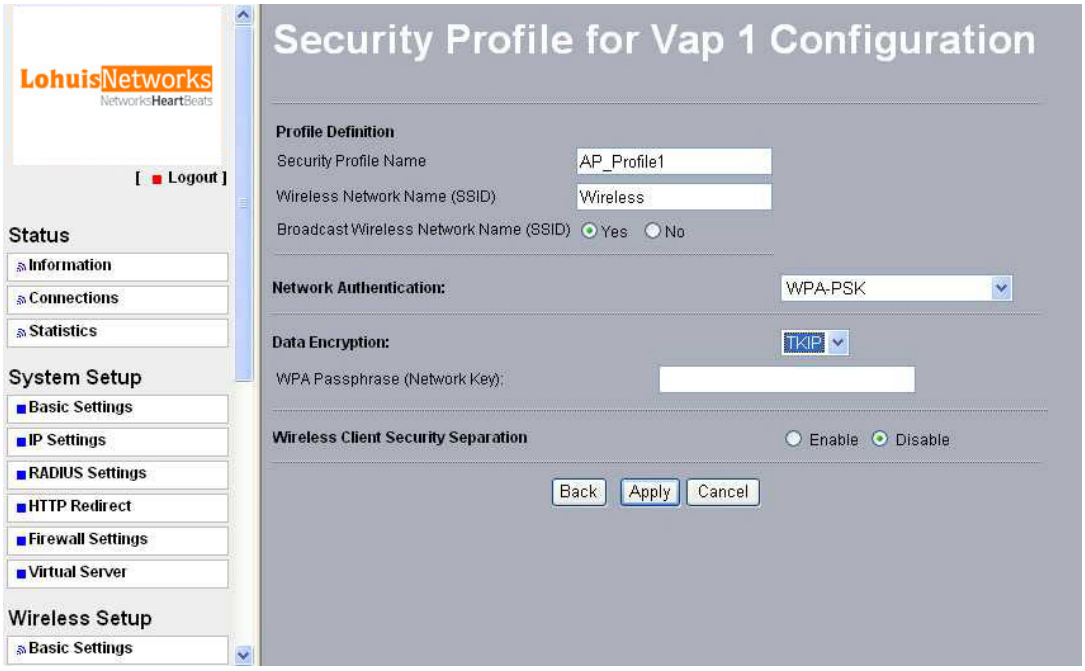


Figure 6-5 Security profile with WPA-PSK

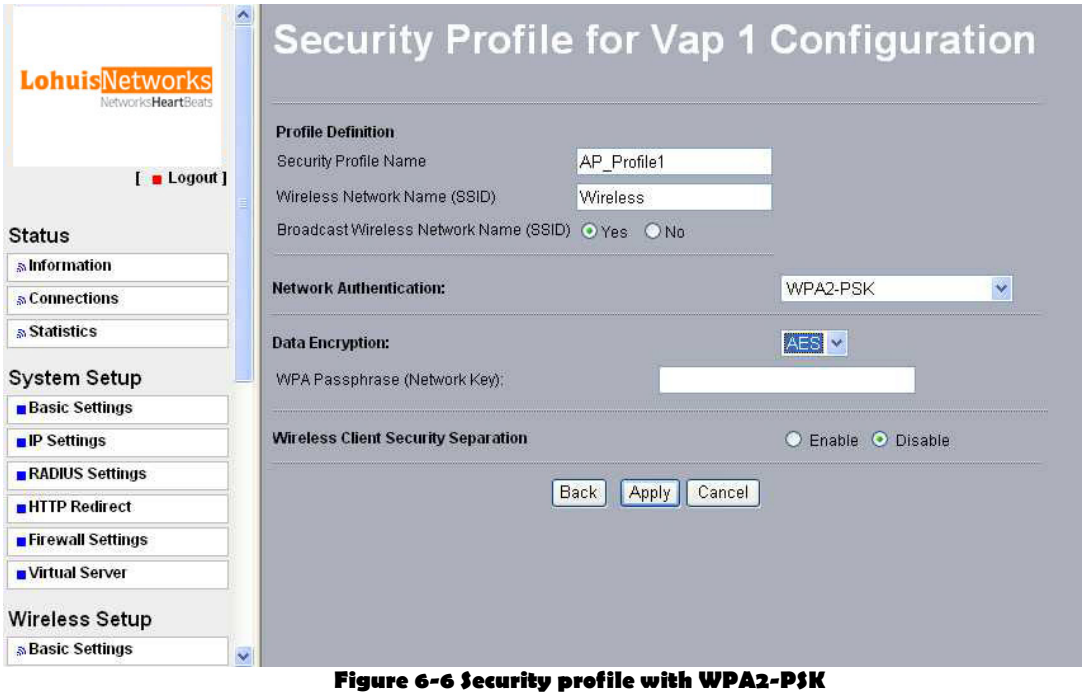


Figure 6-6 Security profile with WPA2-PSK

Figure 6-7 Security profile with WPA-PSK & WPA2-PSK

6-4 Access Control

Authentication by username and password is only part of the story. Many times 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.

Figure: 6-8 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 the MAC Addresses of new stations, you can manually add the stations to allow them to be connected to the radio.

6-5 WDS Mode

In 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.

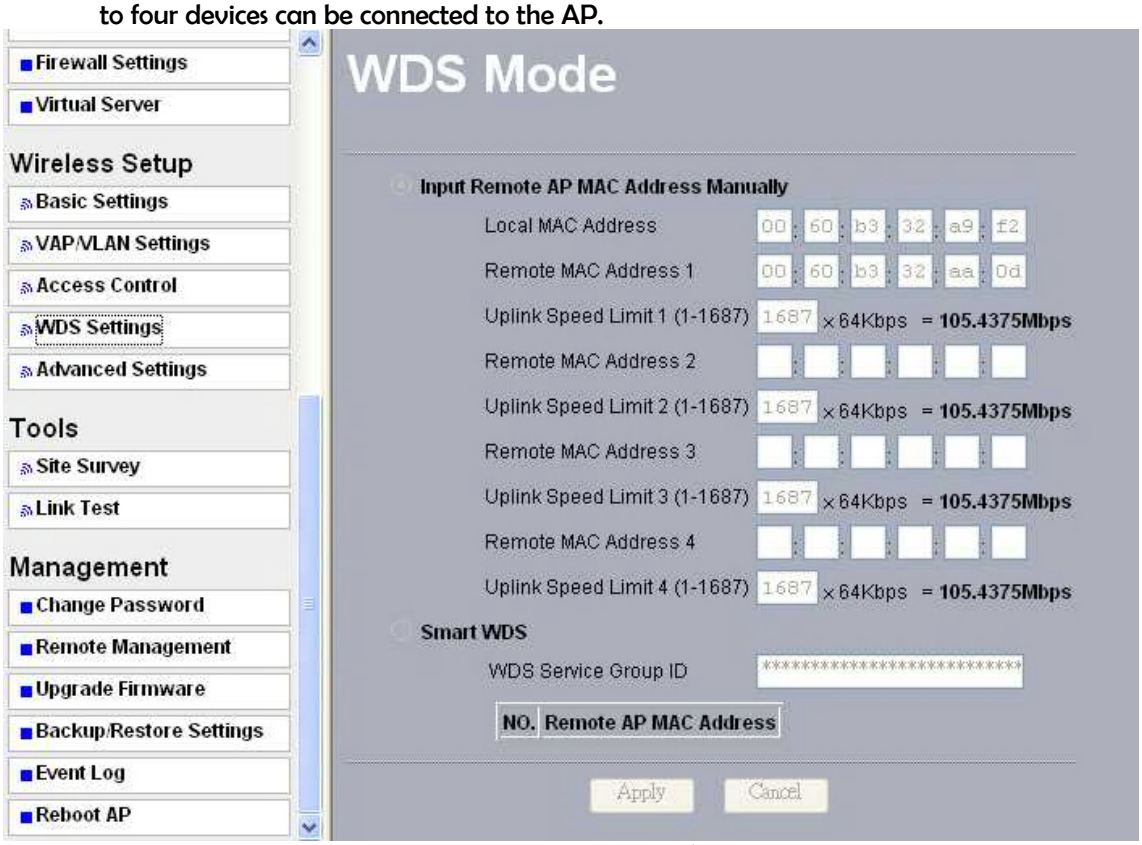


Figure: 6-9 WDS mode

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 a value in uplink speed limit. The most speed available is 1687 × 64Kbps = 105.4375Mbps

6-6 Smart WDS

In bridge mode, enabling Smart WDS, the radio 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 is set to be AP mode.

6-7 Advanced Settings

The default advanced wireless LAN parameters usually streamline your work.

Figure: 6-10 Advanced Wireless Settings

Wi-Fi Multi-media (WMM)

Currently interest and demand for multimedia applications and advanced capabilities is growing quickly. In the residential market, Voice over Internet Protocol (VoIP), video streaming, music streaming, and interactive gaming are among the fastest growing 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 connects to the AP, you can enjoy high-quality multimedia prioritization on your LAN by enabling WMM.

Before enabling WMM, make sure your CPEs also support WMM.

Windows XP, Service Pack 2 is required to fully utilize WMM.

Super G and wireless parameters

Enabling Super G, your transmission rate could reach up to 108Mbps.

The following describes the advanced wireless parameters.

Field Description

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 Your AP

7-1 Site Survey

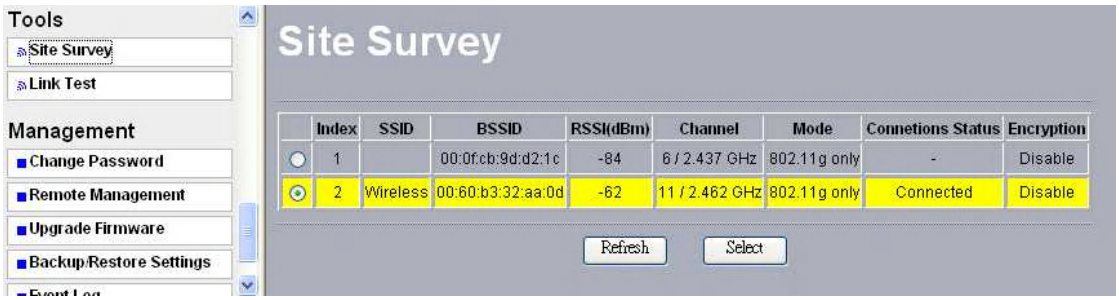


Figure: 7-1 Site survey

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 network information, including SSID, BSSID, RSSI, channel mode, connection status and encryption.

7-2 Link Test

To optimize the communication on your LAN, the Link Test is designed to test the parameters that indicate communication quality.

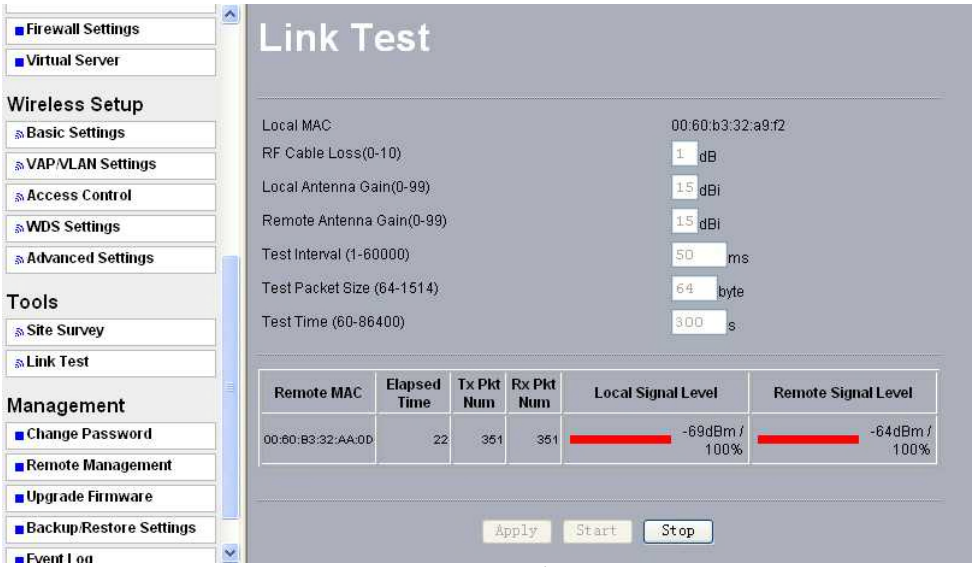


Figure: 7-2 Link test

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 802.11a wireless local area network (WLAN), ranging from 0 to 99.

Remote Antenna Gain (0-99)

This indicates extended coverage provided by the remote AP, for an existing 802.11a Wireless local area network (WLAN).ranging from 0 to 99.

Test Interval (1-60000)

This provides testing time interval in milliseconds.

Test Packet Size (64-1514)

This tests the size of packets transmitted between the two radios, ranging from 64 to 1,514

Test Time (60-86400)

This specifies how long the link test will last ranging from 60 to 86,400 seconds.

Chapter 7. Management

8-1 Change Password

Figure: 8-1 Change Password

Here you can make adjustments to your current or default password.
Take the following steps to change the password:
1. Enter your currently-used password in the Current Password field.
2. Enter your new password in the New Password field.
3. Re-enter the new password to confirm it in the Repeat New Password field.
4. 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.

8-2 Remote Management

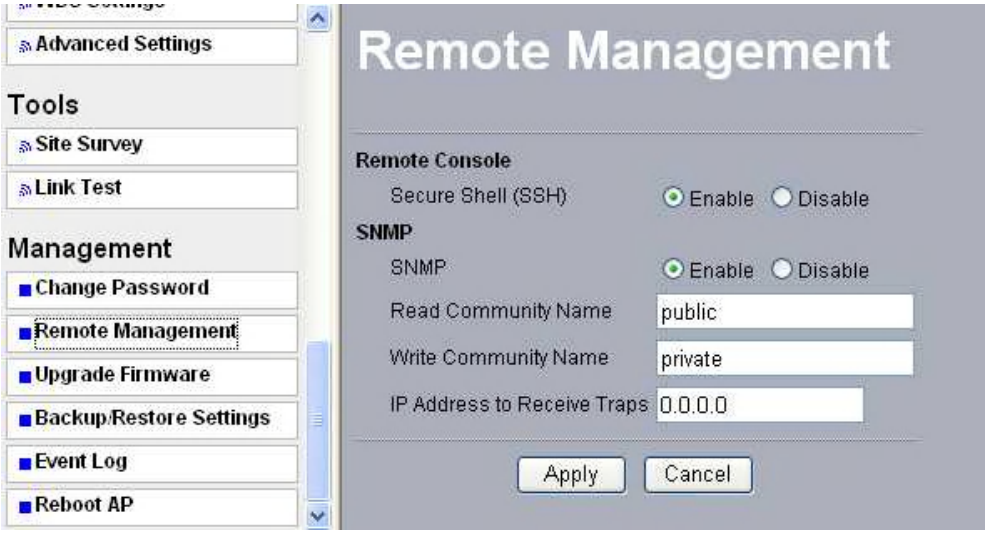


Figure: 8-2 Remote Management

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 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.
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 the IP address in host name field and port number in port field. Also, select SSH as protocol.

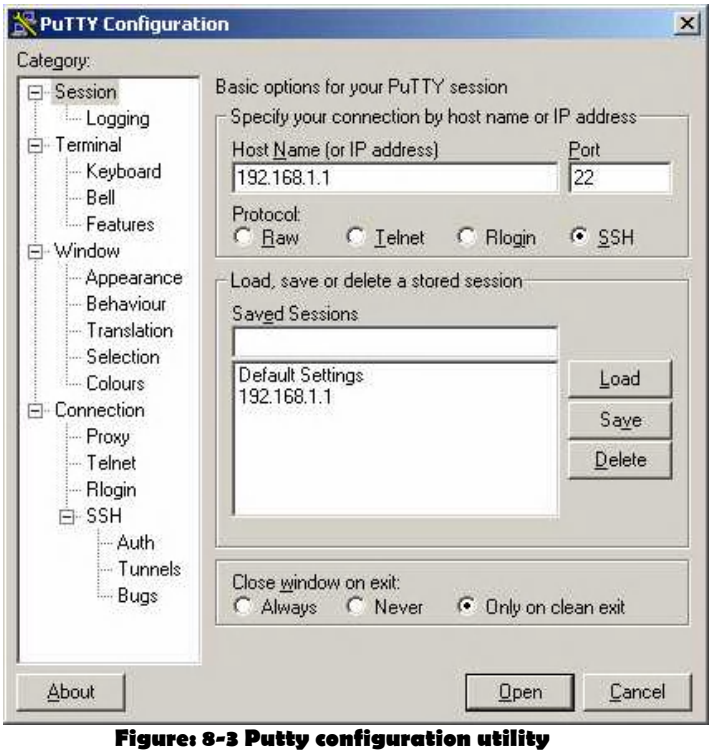


Figure: 8-3 Putty configuration utility

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

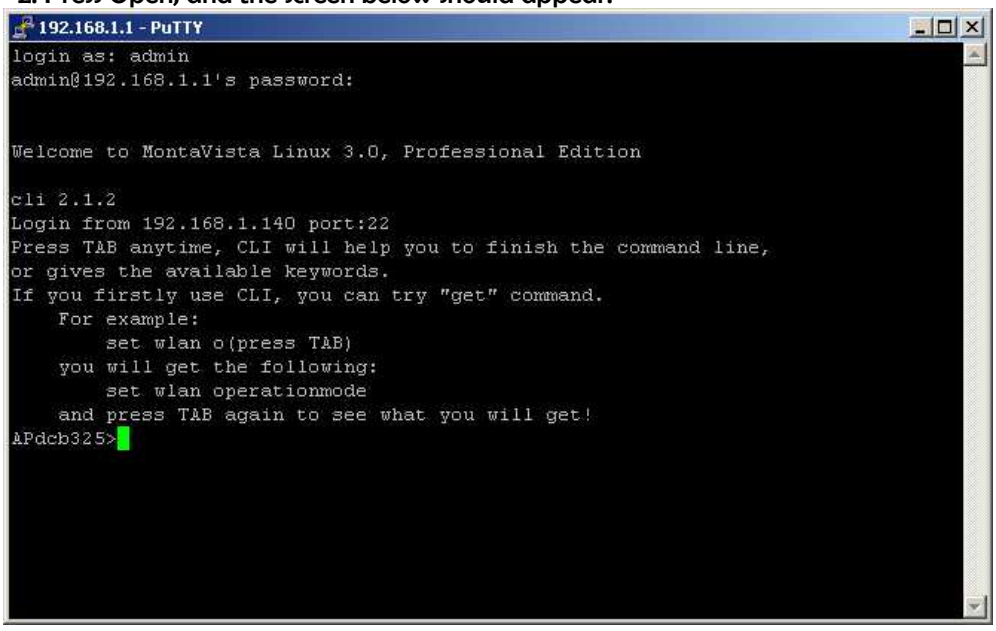


Figure: 8-4 Putty configuration page

The login name is **admin** and **password** is the default password. After successful login, the screen should prompt **LOHU>**. In this example, the **LOHU** 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.

8-3 Upgrade Firmware

When uploading software to the AP 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 inoperable.

The software of the radio is stored in FLASH memory, and can be upgraded as new software is released. 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: 8-5 Upgrade Firmware

8-4 Backup / Restore Settings

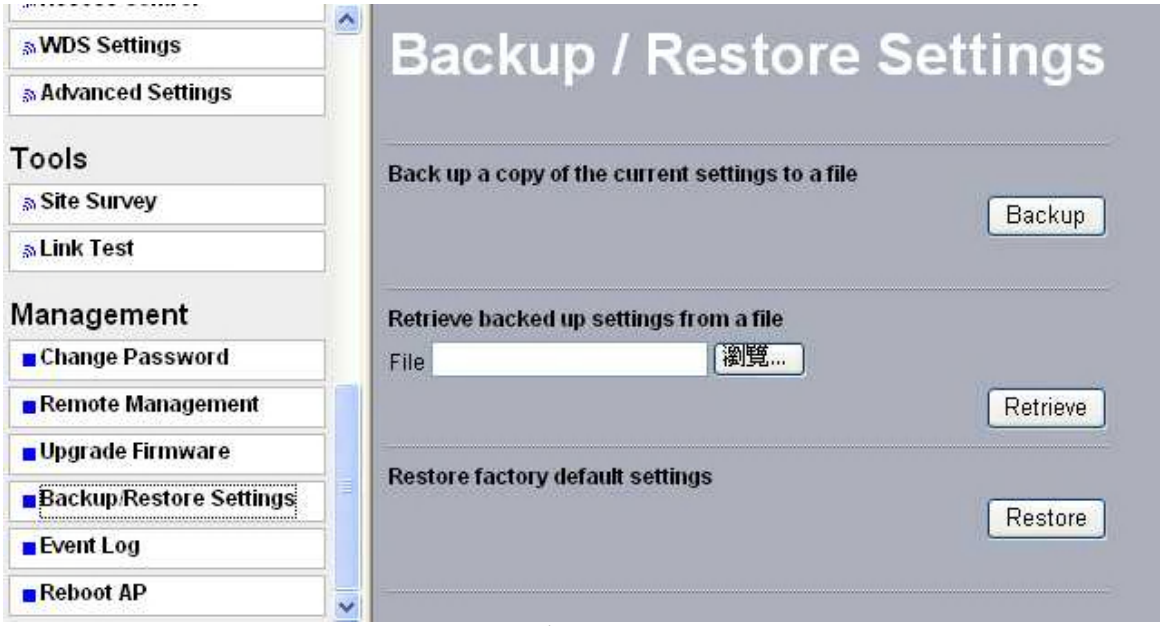


Figure: 8-6 Backup / Restore Settings

Backup

Allows you to save all of the radio's settings in a file that can be stored on any computer.

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.

8-5 Event Log

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

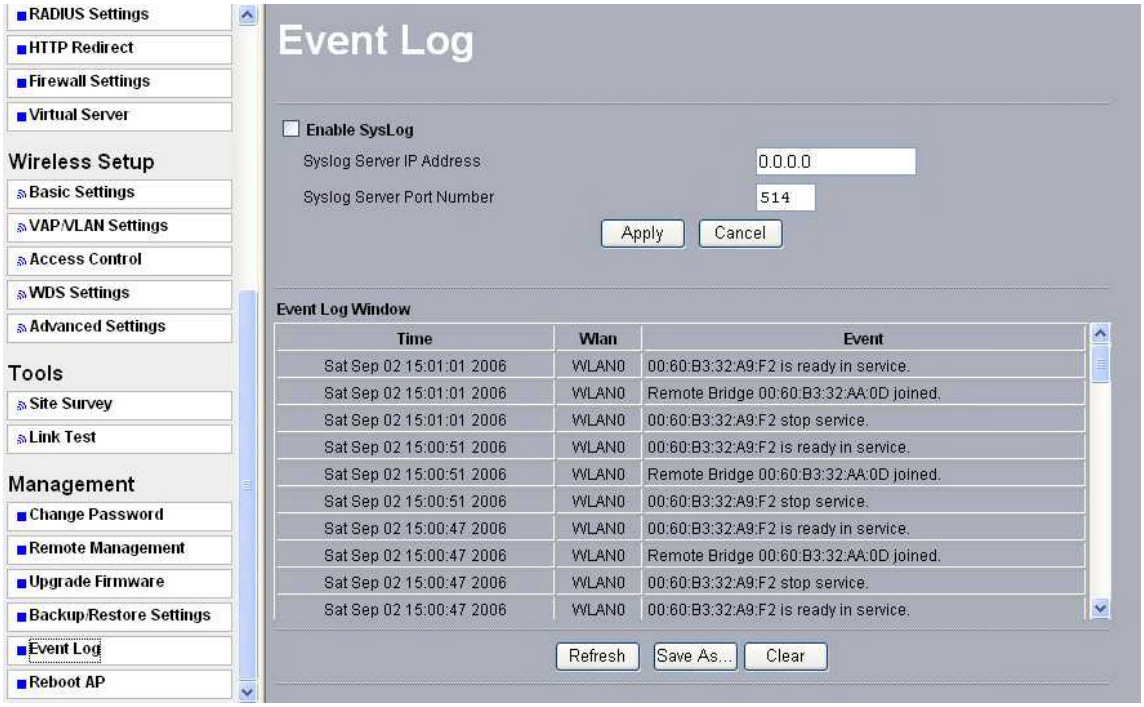


Figure: 7-7 Event log

- **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

8-6 Reboot AP

If you want to reboot AP, click Yes and then apply. AP will reboot.

Figure: 8-8 Reboot AP

Chapter 8. Troubleshooting

This chapter helps you to isolate and solve common problems that may arise during setup.
Before you start troubleshooting, it is important that you have checked the details in the product user manual and quick installation guide.
In some cases, rebooting the unit clears the problem. If the radio still doesn't perform as expected, please try the following options.

9-1 General Descriptions

To successfully use the radios, engineers must be able to troubleshoot the system effectively. This section will show you how a LOHU Series Radio could be analyzed when you are experiencing link problems. 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) If you verify that your configuration is correct, but the user still report that the link does not work, the most likely, the problem is environmental interference or an improper connection. Assuming that the testing 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 versions at both ends of the link are up-to-date.
☐ Check for any reported alarm messages in the radio's Event Log

Analyzing the Spectrum

The best way to discover if there is a source of interference is to use a 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 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 performed:

☐ Switch the RF channel away from the interference source.
☐ Change the polarization of the antenna; try to change to a polarization different from the incoming interference.

☐ A small beam antenna may help (such as a grid or dish antenna). Aligning the antenna properly will reduce the effects of the interference. This solution won't help when the source of interference is extremely close the remote site.
Before checking for interference, ensure all of your hardware is working properly and your configurations are correct. The path analysis, cabling and antennas should be checked as well.

9-2 Connection Issues

This section describes several common problems you might have while setting the radios.

Radio Does Not Boot

When the radio does not boot, use the following steps to check your 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 boots properly, but remains inaccessible via the web interface:
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.

9-3 Configuration Issues

The following problems relate to setup and configuration problems:
These are some basic configurations might make the link fail:
☐ 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

9-4 Communication Issues

If two radios work within close distance of each other and do not work while separated, then there are two possible reasons why wireless connectivity isn't working properly:

☐ An RF path problem is one possibility. For example, poor antenna alignment, the tower is not tall enough when the radios are installed at a long distance or the connectors are not seated properly, etc (these are the most common problems in installations).

☐ The other possibility is interference problems caused by high signal levels from another unit. The interference can be checked by changing the frequency and then seeing 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.