IEEE 802.11a/b/g

Enterprise-class
Outdoor Multi-function Radio

External / Integral Antenna Terminal

KymaStar: KS5X-2301-EXT / I23 / I20
KS5X-1501-I14
KS24-2302-EXT / I18
KS24-2702-EXT / I18

USER MANUAL

Version 1.0.4.W2

WNI GLOBAL

Website: www.wnint.com
Address : 2146 Bering Drive, San Jose, CA 95131, USA
TEL : +1-408-432-8892, FAX : +1-408-432-8896

August 2007

Table of Contents

Copyright

Preface

About This Manual

This manual details the installation, operation, and troubleshooting of the enterprise-class IEEE 802.11a or 802.11b/g outdoor radio.

ANATEL

Although this radio operates in 5,2 GHz to 5,8 GHz frequency bands, it is certified with ANATEL for operating in Brazil in the 5725 – 5850 MHz (5,8 GHz) band. All other bands are disabled to avoid wrong radio settings that do not comply with ANATEL.

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 this manual.

CAUTION This symbol means ***reader use caution.*** 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 harm. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

NOTE:

1. **This manual uses 5.X GHz IEEE 802.11a product as example.**
2. **2.4 GHz IEEE 802.11g/b is same as 802.11a except where noted.**
3. **KymaLite is a lower powered KymaStar in a smaller package and is available with integral antenna only.**

Chapter 1. Introduction

Thank you for choosing this Enterprise-class IEEE 802.11a or 802.11b/g outdoor multi-function 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. We also provide details of the hardware, system requirements and basic installation.

1-1 Overview

802.11a/b/g-compliant, VLAN functionality allows a single network AP to serve as 8 virtual network APs. 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 conditions.

This Access point can serve as a 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.

This Access Point can be configured and monitored using the command-line interface,(CLI), the browser-based management system, or Simple Network Management Protocol, (SNMP).

This radio currently can support a data rate of up to 108Mbps. (In Super A or Super G mode)

The instructions in this Guide will help you connect the outdoor radio, set it up, and configure it.

1-2 Key Features

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

• IEEE 802.11a or 802.11b/g

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

• WEP Support

The radio supports WEP 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 also be configured as a client and obtain information from your DHPC server.

• RADIUS Accounting

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

• SNMP

The radio supports 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

• VAP (Virtual Access Point), or VLAN

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

• 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

Power levels can be set to full, half, quarter, eighth, and minimum.

•Atheros Super A (5.X GHz)or Super G (2.4 GHz) Mode

Super A mode enables over the air transmission rates of up to 108Mbps.

• Multiple security settings per VLAN with up to 8 VLANs

Security settings for up to eight VLANs can be set individually, thus offering high level security where it is needed.

•Hidden Mode

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

•Access Control

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

1-3 Additional Materials Required

Before installing the radio, make sure you have the following materials

- Category 5 UTP straight through Ethernet cable with RJ-45 connector for connection between your network or PC and the PoE injector
- Category 5 **SFTP** (Shielded) straight through Ethernet cable with weather-proof RJ-45 connector for connection between the PoE injector and the radio.
- A 100~240 V, 50~60 Hz AC power source
- A PC with a Web browser such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above for configuration.

What's In the Box?

- 802.11 a or 802.11b/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 part is missing or damaged, please contact WNI Global, Inc. or your local reseller.

1-4 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.

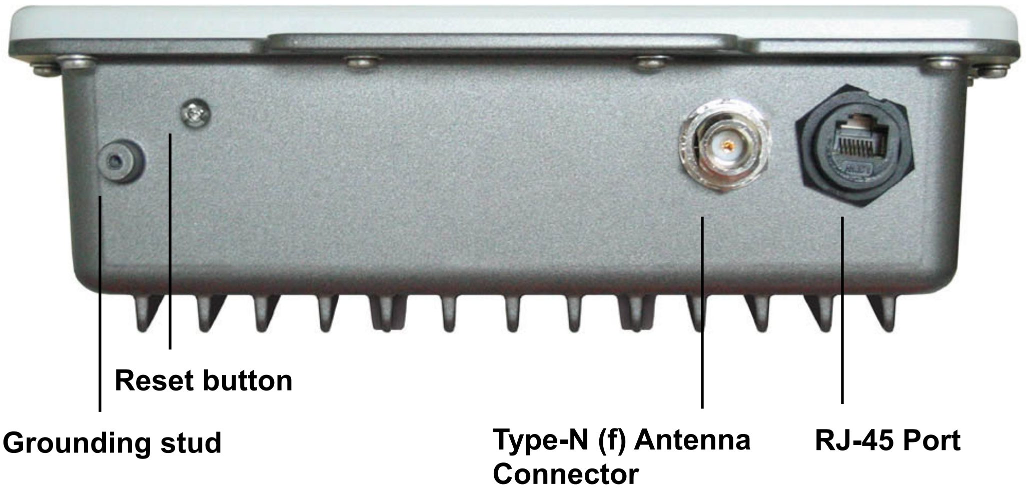


Figure 1-1A Outdoor Multi-function Radio for External Antenna

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	**Type-N (f) Antenna Connector**	For connecting external antenna. Please contact WNI Global, Inc. for recommended antenna selection.
3	**Grounding stud**	Connect to the ground conductor using a minimum of 6 AWG copper wire or braid.
4	**Reset button**	Remove this screw and insert a paper clip to press in and hold the reset button for 5~10 seconds to reset the radio to factory default settings.

WARNING

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.

ODU –Integral Antenna Unit

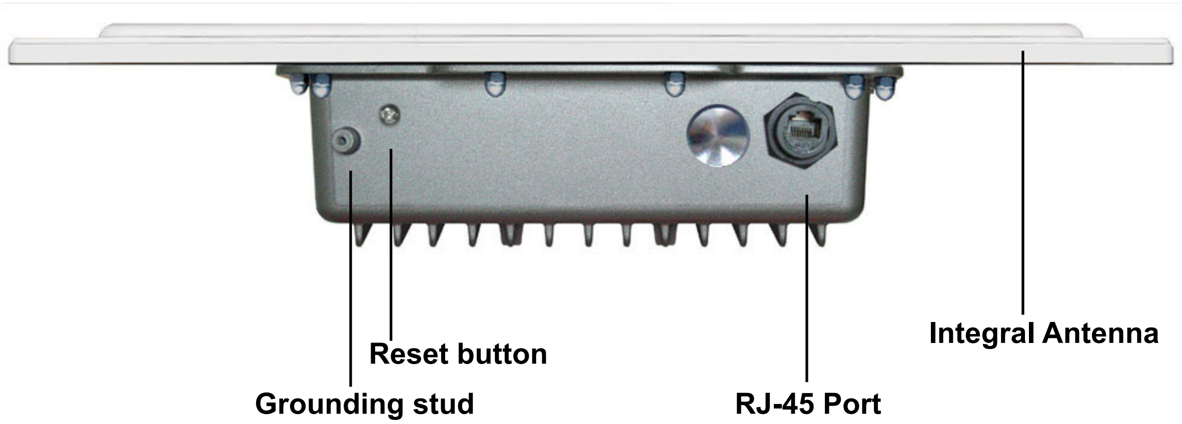


Figure 1-1B Outdoor Multi-Function Radio with Integral Antenna

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	**Grounding Stud**	Connect to the ground conductor using a minimum of 6 AWG copper wire or braid.
3	**Reset Button**	Remove this screw and insert a paper clip to press in and hold the reset button for 5~10 seconds to reset the radio to factory default settings.

PoE (Power over Ethernet)

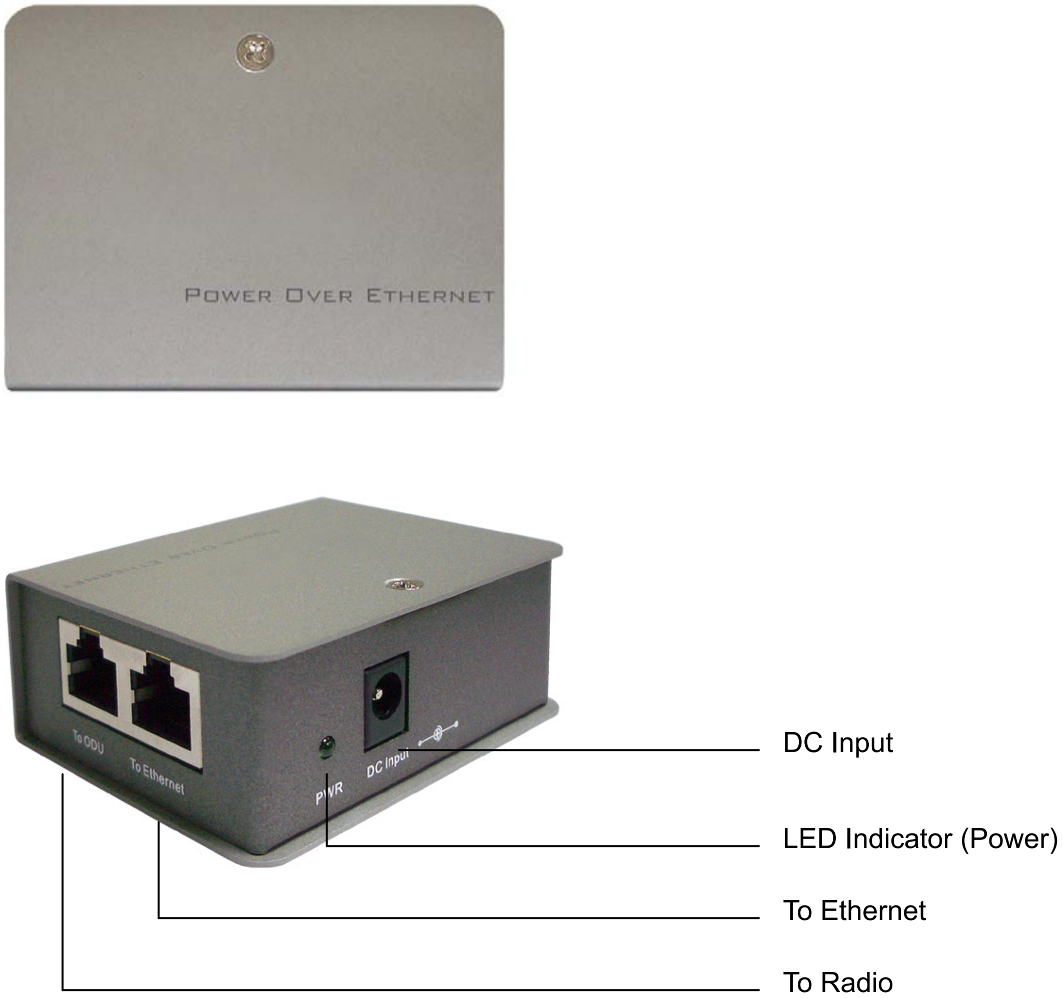


Figure 1-2 Power over Ethernet injector

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 DC input.
4	**LED Indicator**	Power LED

WARNING

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.

CAUTION

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

CAUTION

Power Over Ethernet Injector is not a waterproof unit and should not be used outdoors.

1-5 Hardware Installation

The Outdoor Multi-function Radio operates in a license free frequency band in most countries, and is therefore susceptible to interfering signals from other devices in the area. Taking some simple precautions can reduce the likelihood of poor link performance due to interfering signals.

- Check to see if there are other radios operating in the same frequency band on the same structure or nearby. If the operating channels of these devices can be determined, set your radio to a no-overlapping channel.
- Make sure that there is direct line of sight to the receiving radio. Trees and other obstructions can reduce signal levels and cause poor link performance.

■ Site Surveys

It is advisable to conduct a site survey prior to the installation. The survey should include checking availability of power, grounding systems, proper mounting structure, grounding of mounting structure, line of sight, fresnel zone clearance, and any other issues that may affect the installation.

It is a good practice to configure and verify the 802.11a Outdoor Multi-function Radio operation before you mount the radio in a remote location.

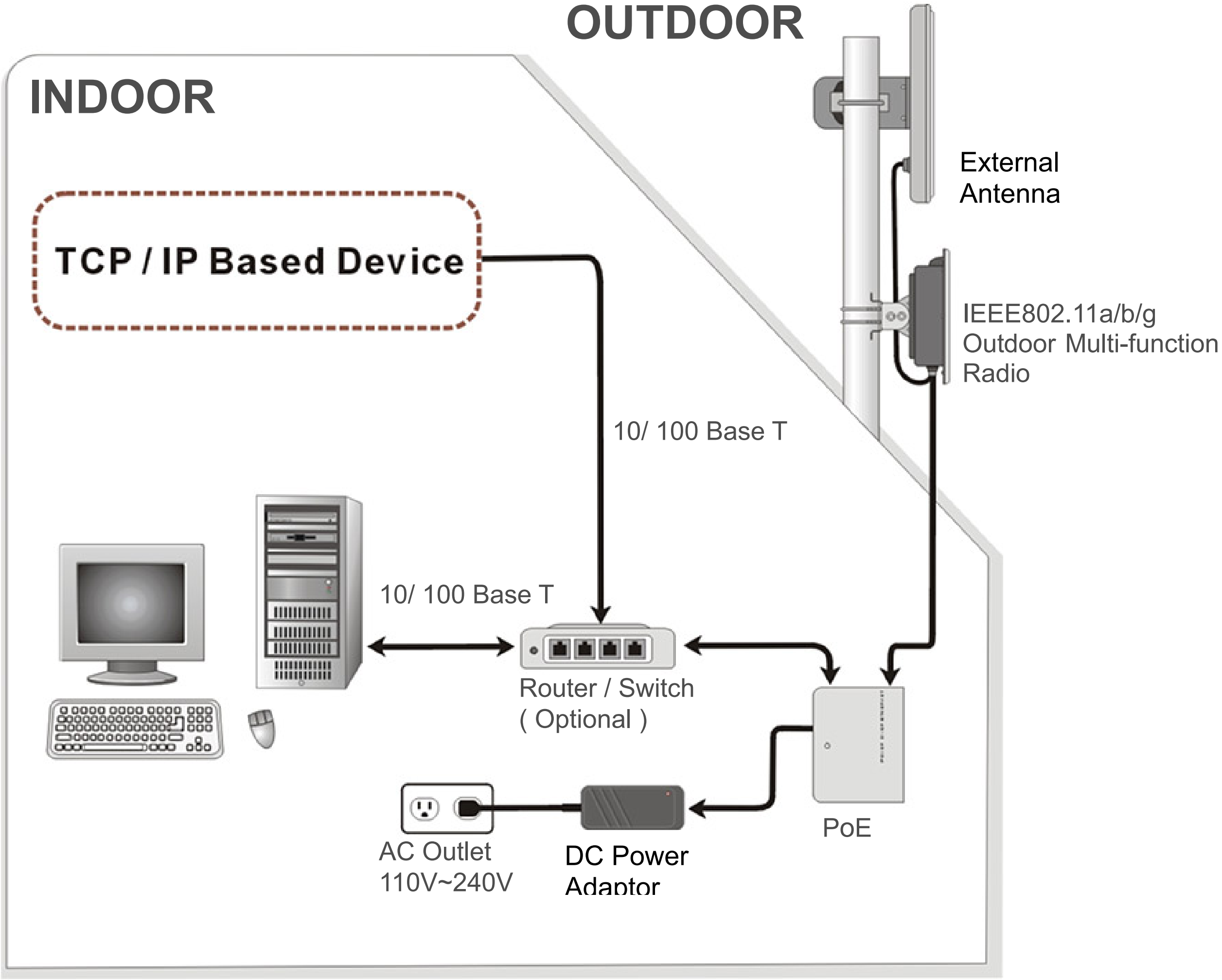


Figure 1-3A: Hardware Installation with External Antenna

Power Over Ethernet Injector is not a waterproof unit, should not be used outdoors

- **Connect the Ethernet Cable**

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

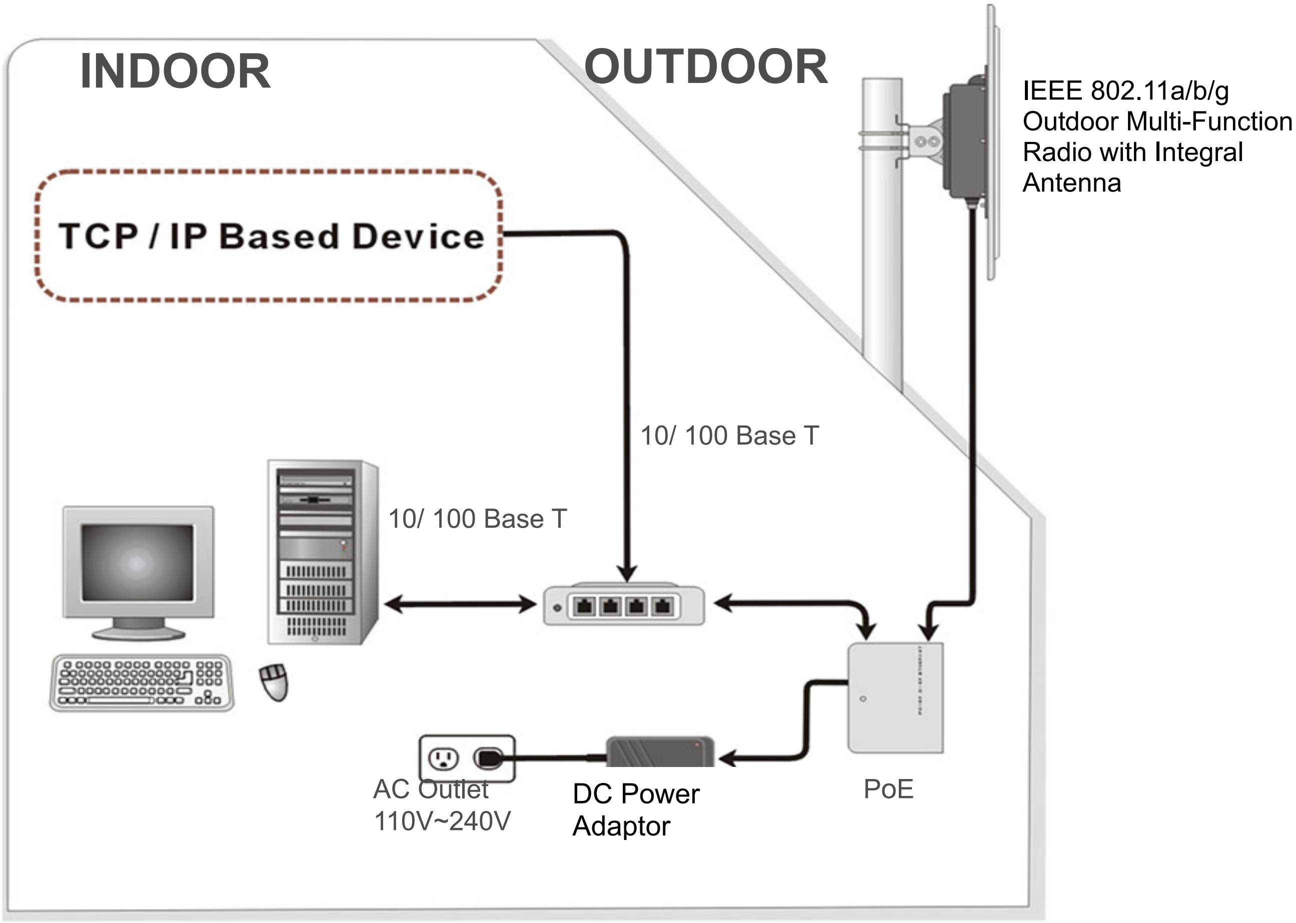


Figure 1-3B: Hardware Installation with Integral Antenna Radio

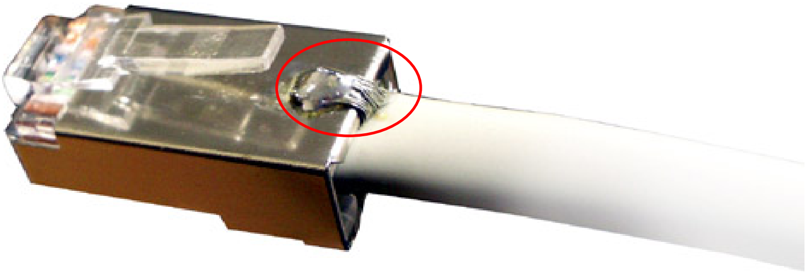


Figure 1-4 Solder the RJ-45 connector with the SFTP cable

Solder the SFTP cable as the Figure 2-4, make sure the solder bead is NOT bigger than that shown in the figure, or it may affect the function of the waterproof RJ-45 connector.

- **Attach the antenna**

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

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

- **Connect the Power Cable**

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

- **Mounting the 802.11a 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**.**

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

⚠ CAUTION **FCC Part 15.247(i) System operating under the provisions of this section shall be operated in a manner that ensures that the public is not exposed to radio frequency levels in excess of the comissions guidelines.**

Limit S = 1 mW / cm^2 from section 1.3107(b)(1) Table 1

Note to professional installer: **At the location of transmitters, the minimum MPE safe distance, is at least 420 cm with an antenna having a gain of 34.5 dBi.**

⚠ CAUTION **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 procedures.**

- **Connect the ground stud**

  Connect a minimum 6 AWG Wire to the ground stud on the ODU, and connect the other end to a suitable ground using the shortest and most direct route.

This equipment must be grounded. Never 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.

Chapter 2. Security

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

Radio default factory settings are detailed 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 (IEEE 802.11a or 802.11/b/g)
Channel / Frequency	52 / 5260 MHz or 11 / 2412 MHz

2-2 Getting to Know Radio Wireless Security Options

WNI Global, Inc. 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 that may be taken 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 the WEP encryption keys periodically.

To ensure network security, steps one through four should be followed at a minimum.

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 still 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 your 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 computers, servers, etc., on the Ethernet.

1. SET UP THE AP

Tip: Before mounting the radio in a high location, first set up and test the radio and 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 the Cat.5 SFTP cable from the radio to the POE.

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

e. 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 is on.

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 will open:

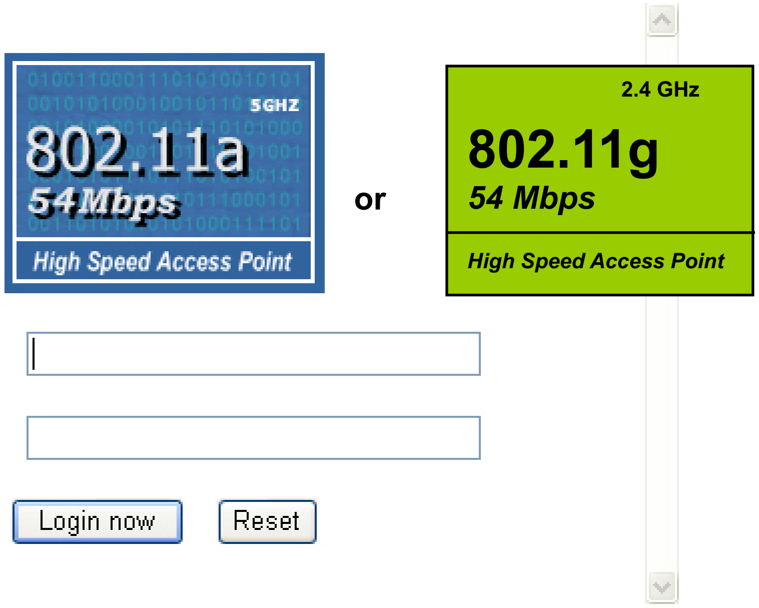
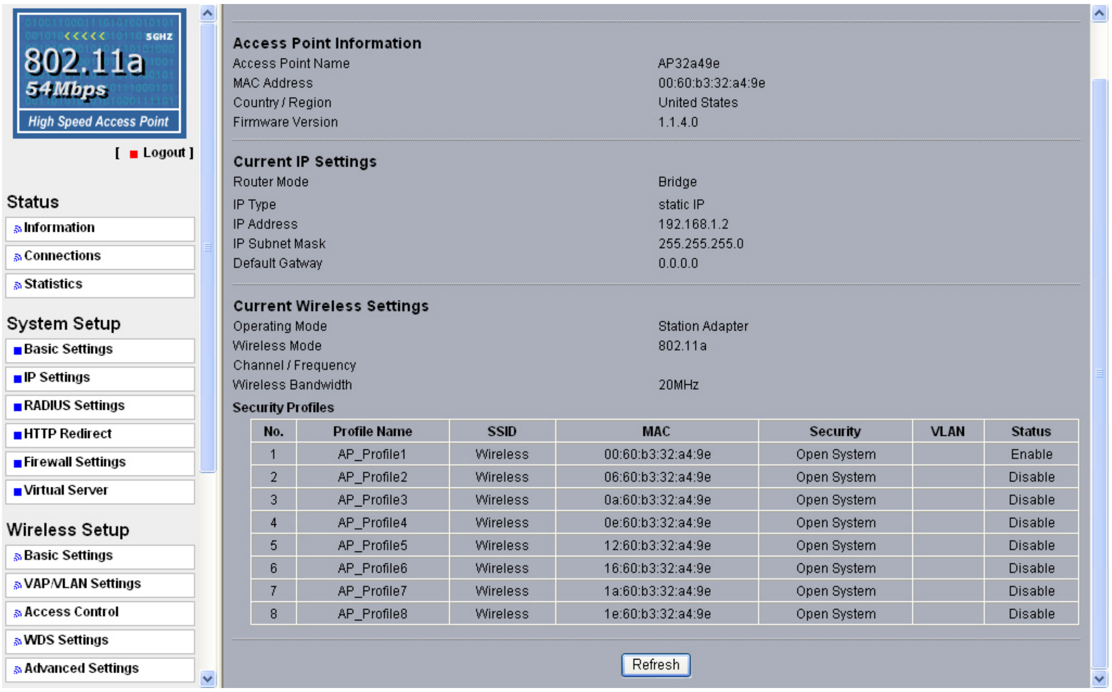


Figure: 2-1 AP log in window

When prompted, please enter **admin** for Name and **password** for password, both in lower case.

3. Clicking Login now will navigate you into this radio's homepage. This page contains General Information as shown below.



Access Point Information

Access Point Name	AP32a49e
MAC Address	00:60:b3:32:a4:9e
Country / Region	United States
Firmware Version	1.1.4.0

Current IP Settings

Router Mode	Bridge
IP Type	static IP
IP Address	192.168.1.2
IP Subnet Mask	255.255.255.0
Default Gatway	0.0.0.0

Current Wireless Settings

Operating Mode	Station Adapter
Wireless Mode	802.11a
Channel / Frequency	
Wireless Bandwidth	20MHz

Security Profiles

No.	Profile Name	SSID	MAC	Security	VLAN	Status
1	AP_Profile1	Wireless	00:60:b3:32:a4:9e	Open System		Enable
2	AP_Profile2	Wireless	06:60:b3:32:a4:9e	Open System		Disable
3	AP_Profile3	Wireless	0a:60:b3:32:a4:9e	Open System		Disable
4	AP_Profile4	Wireless	0e:60:b3:32:a4:9e	Open System		Disable
5	AP_Profile5	Wireless	12:60:b3:32:a4:9e	Open System		Disable
6	AP_Profile6	Wireless	16:60:b3:32:a4:9e	Open System		Disable
7	AP_Profile7	Wireless	1a:60:b3:32:a4:9e	Open System		Disable
8	AP_Profile8	Wireless	1e:60:b3:32:a4:9e	Open System		Disable

Figure: 2-2 AP general information page

Chapter 3. General Information

General information gives you basic information regarding the configuration of the radio..

3-1 Information

The information displayed is as follows:

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.

.

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: Acts as a standard 802.11a or 802.11g. This is the default mode.

•Station: Performs as a client station associated to other APs.

•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. It is advisable to use WEP in order to protect this data from intruders.

•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 another wireless bridge. Or you can use a common SSID to communicate with another wireless station. WEP should be used to protect this communication.

Inter-building: Under Unique to KymaStar WDS 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.

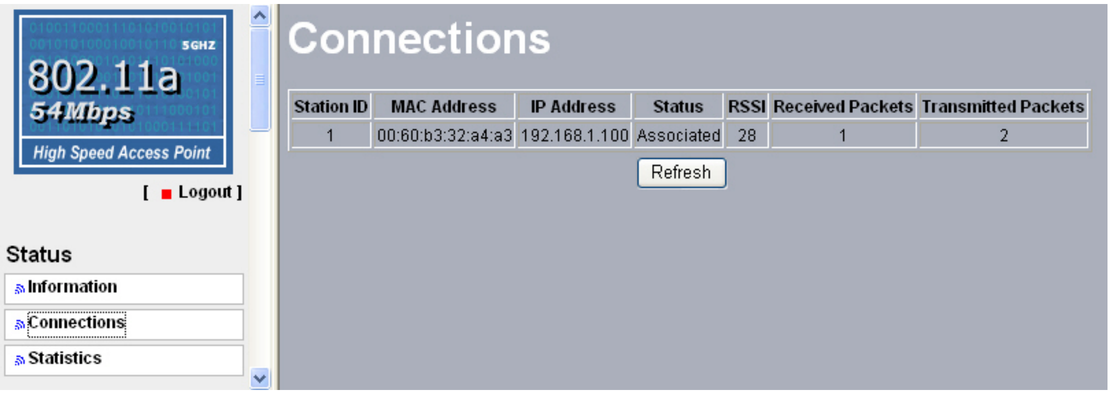
Wireless Mode: Select the desired wireless operating mode. The default mode is 802.11a.

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 as shown below.



Connections

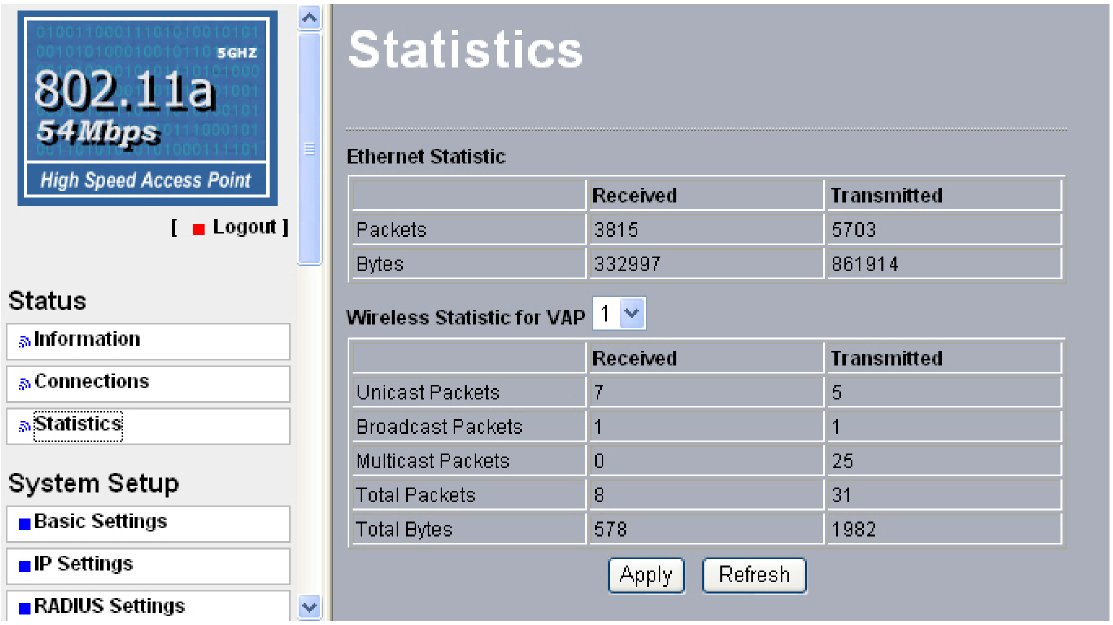
Station ID	MAC Address	IP Address	Status	RSSI	Received Packets	Transmitted Packets
1	00:60:b3:32:a4:a3	192.168.1.100	Associated	28	1	2

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 page provides various LAN and WAN statistics.



Statistics

Ethernet Statistic

	Received	Transmitted
Packets	3815	5703
Bytes	332997	861914

Wireless Statistic for VAP 1

	Received	Transmitted
Unicast Packets	7	5
Broadcast Packets	1	1
Multicast Packets	0	25
Total Packets	8	31
Total Bytes	578	1982

Figure: 3-2 statistics

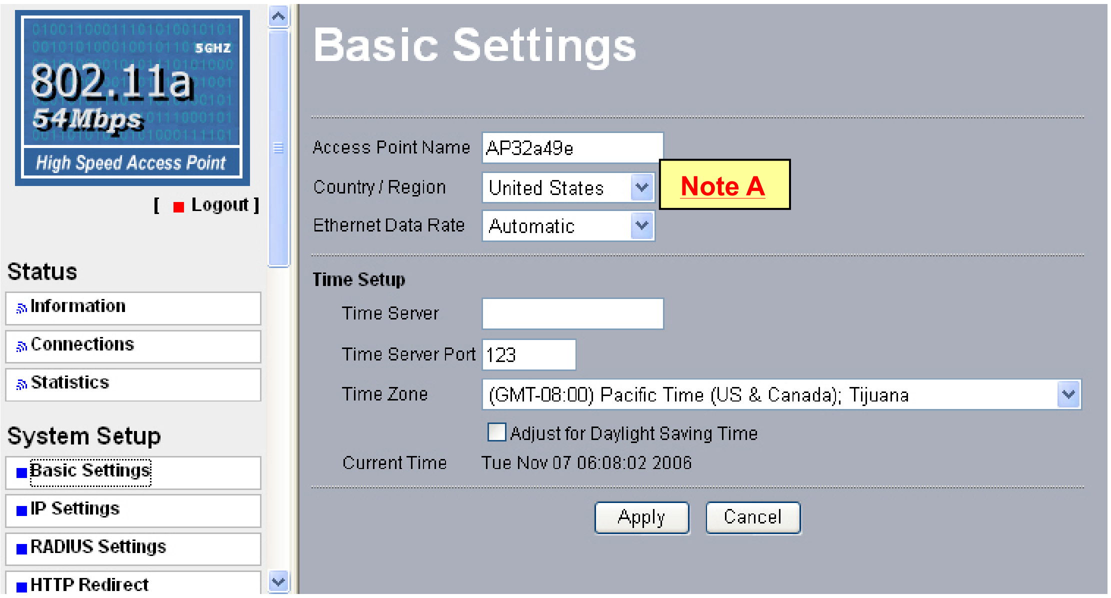
Field		Description
Wired Ethernet	Packets	The number of packets sent since the AP was restarted.
	Bytes	The number of bytes sent since the AP was restarted.
Wireless	Unicast Packets	The Unicast packets sent since the AP was restarted.
	Broadcast Packets	The Broadcast packets sent since the AP was restarted.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

The versatile radio provides many useful functions.

4-1 Time Server

By clicking on Basic Settings, the “Basic Settings” page will appear as shown below.



Basic Settings

Access Point Name: AP32a49e

Country / Region: United States

Ethernet Data Rate: Automatic

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: Tue Nov 07 06:08:02 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. The time Server provides the current time in any world time zone. 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, such as 123.

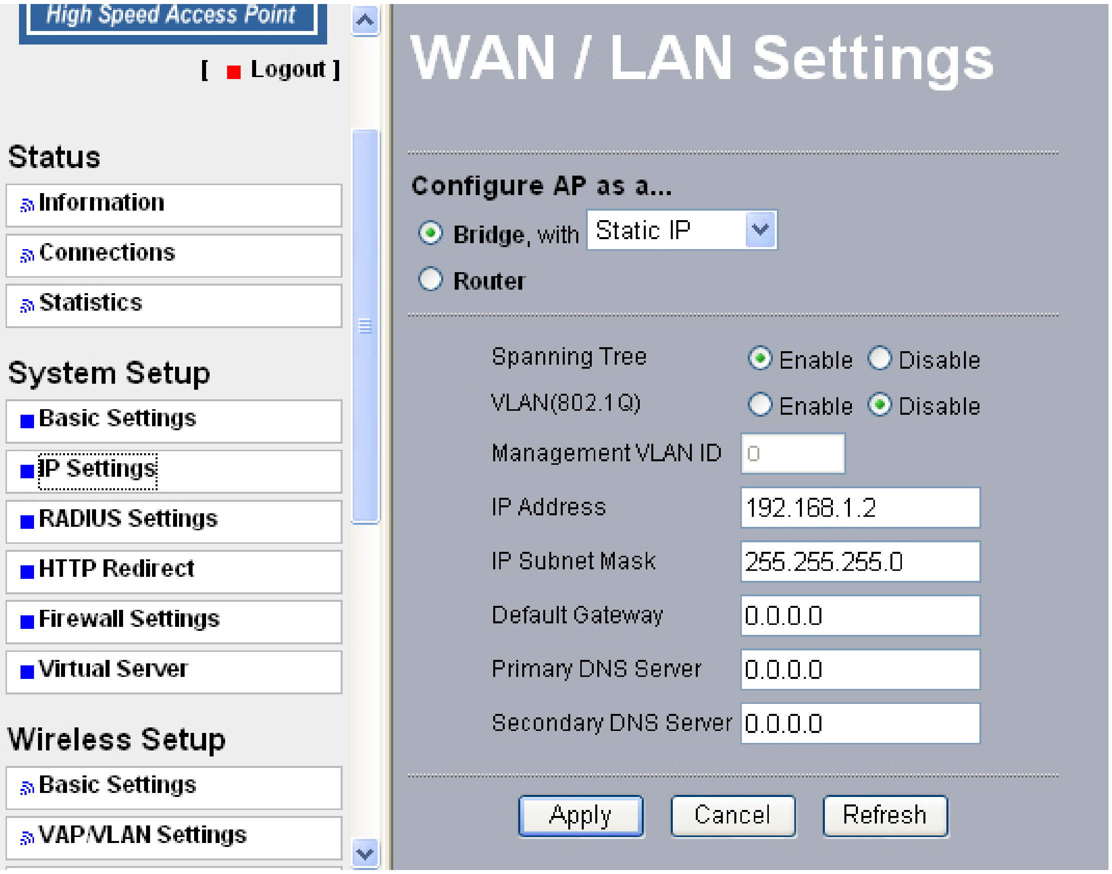
Time Zone: Select the time zone location for your setting.

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

Note A If the country you are operating this product in is not listed, please select a country which has the same Channel Plan as the operating country.

4-2 Bridge/Router Mode

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



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	192.168.1.2
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 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

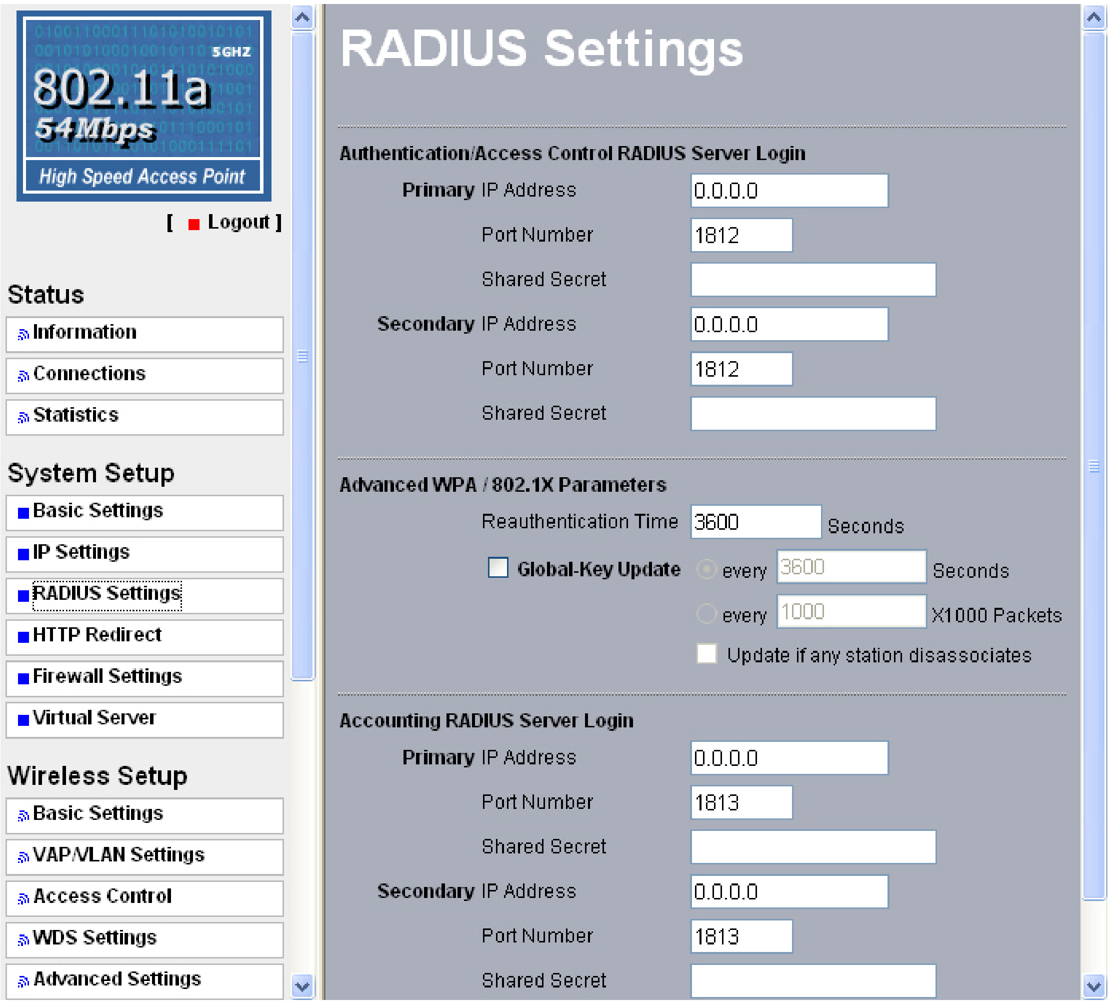
In Router Mode, the radio has two ports, a WAN port and a LAN port.

This is the page where you will set the IP address, subnet mask, default gateway, ans DNS servers for you're the radio. Remember to click Apply to save your changes.

4-3 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.



RADIUS Settings

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:

Figure: 4-3 AP Radius settings

You will need 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

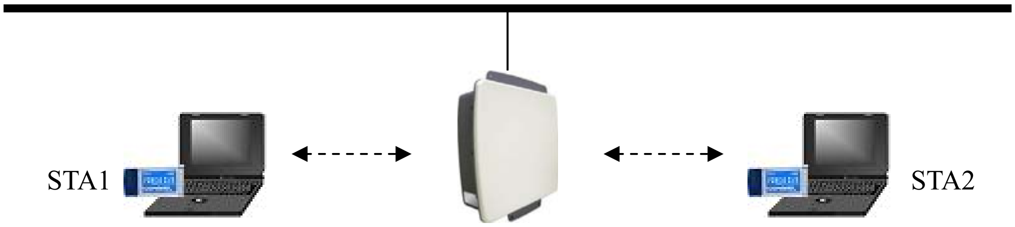
.

•Radius Accounting Option

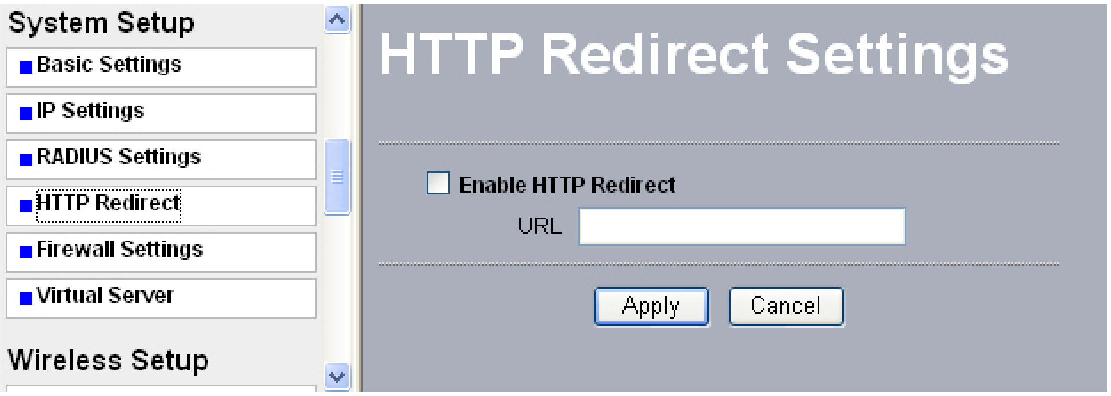
The Radius Accounting option can be enabled in order to track information such as, who connected to the network, when they connected, how long they were connected, how much network traffic they generated, etc..

4-4 HTTP Redirect

This feature allow you to direct anyone that logs on to this access point, to a website of your choosing. This is useful for billing, advertising, and many other purposes.



The following are the HTTP Redirect Settings.



HTTP Redirect Settings

□ Enable HTTP Redirect

URL

Apply Cancel

Figure: 4-4 AP HTTP Redirect settings

URL

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

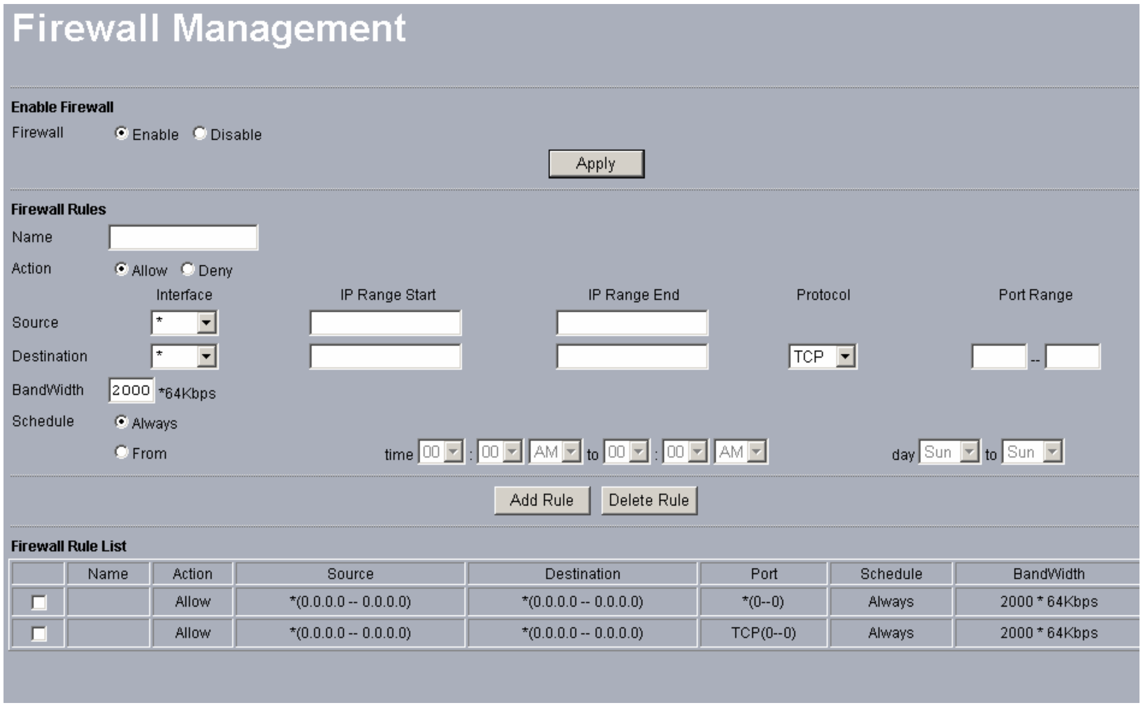
4-5 Firewall Management

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) has an excellent firewall management feature..

Please see the diagram below. Acting as a firewall, the radio will filter your undesired data and protocols, only delivering the “wanted” to your network.

Click the firewall link and you’ll be navigated to the 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’ll need to enable the firewall.

Here we’ll discuss the Firewall.

• Name

Enter your desired firewall rule name in this field

.

• Allow

This field allows you to specify a range of IP addresses that will be allowed access to your network.

.

- **Deny**

  This field allows you to specify a range of IP addresses that will be denied access to your network.

- **Interface**

  This is where you select the source and destination interfaces of the packets to which this rule will apply.

•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 where you can select specific protocols that will be affected by this rule.

•Port Range

This you select the range of ports that will be affected by this rule.

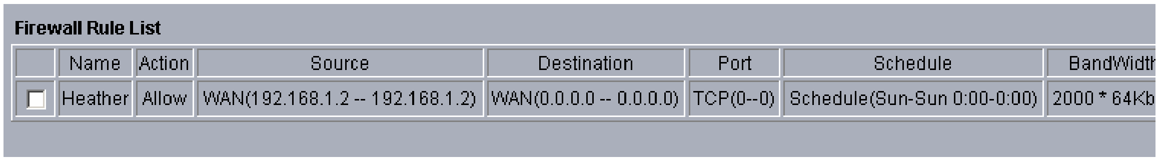
•Schedule

Here you can select a specific time period that will be affected by this rule, or you can click "Always" for the rule to be in effect all of the time.

•Bandwidth

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

After completing a firewall rule configuration, please click Add Rule. The Firewall Rule List will appear below.



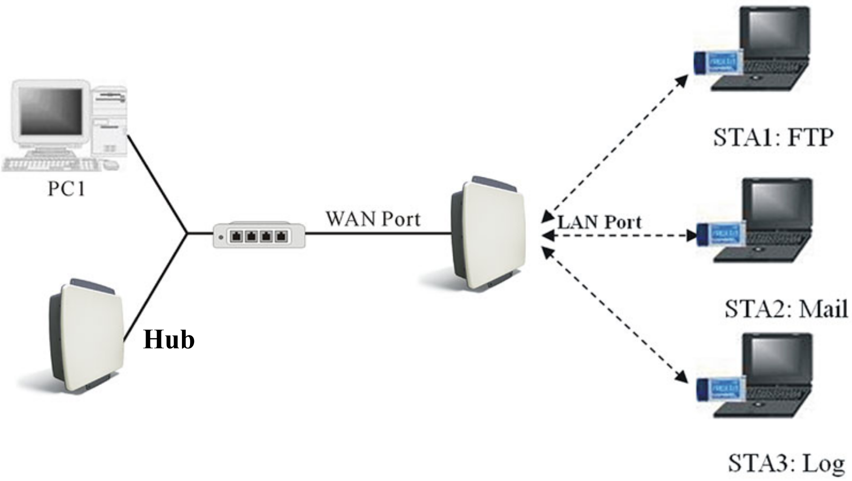
Firewall Rule List

	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

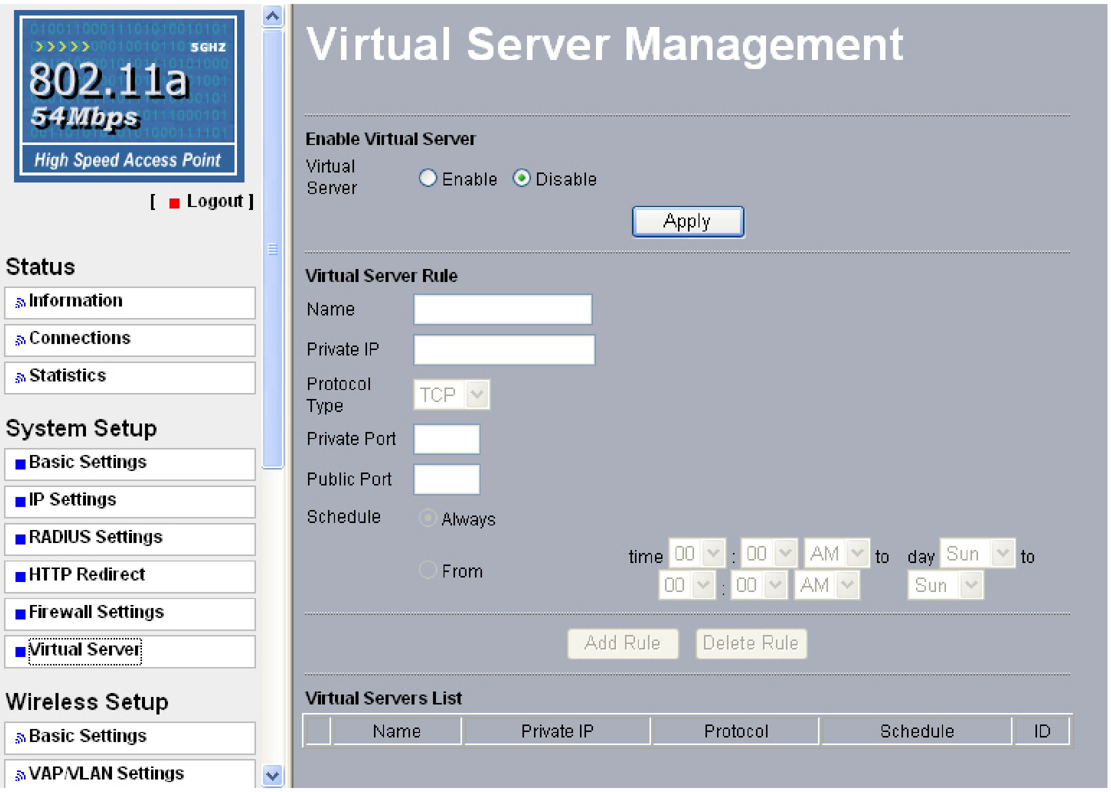
Figure: 4-6 Firewall list

4-6 Virtual Server

Virtual server can be enabled only in router mode.



The radio (which is set as an AP), can act as a virtual server, allowing clients access to multiple servers as in the diagram above.



Virtual Server Management

Enable Virtual Server

Virtual Server ○ Enable ● Disable

Virtual Server Rule

Name

Private IP

Protocol Type TCP

Private Port

Public Port

Schedule ○ Always

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

Virtual Servers List

	Name	Private IP	Protocol	Schedule	ID

Figure: 4-7 AP virtual server management

Below are the elements included in the Virtual Server Management page.

•Name

Enter the name of the virtual in this field.

•Private IP

This specifies the IP Address of the server in your LAN.

•Protocol Type

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 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.