Chapter 5. Wireless Setup

This chapter focuses on the radio's powerful wireless functions.

5-1 Basic Settings

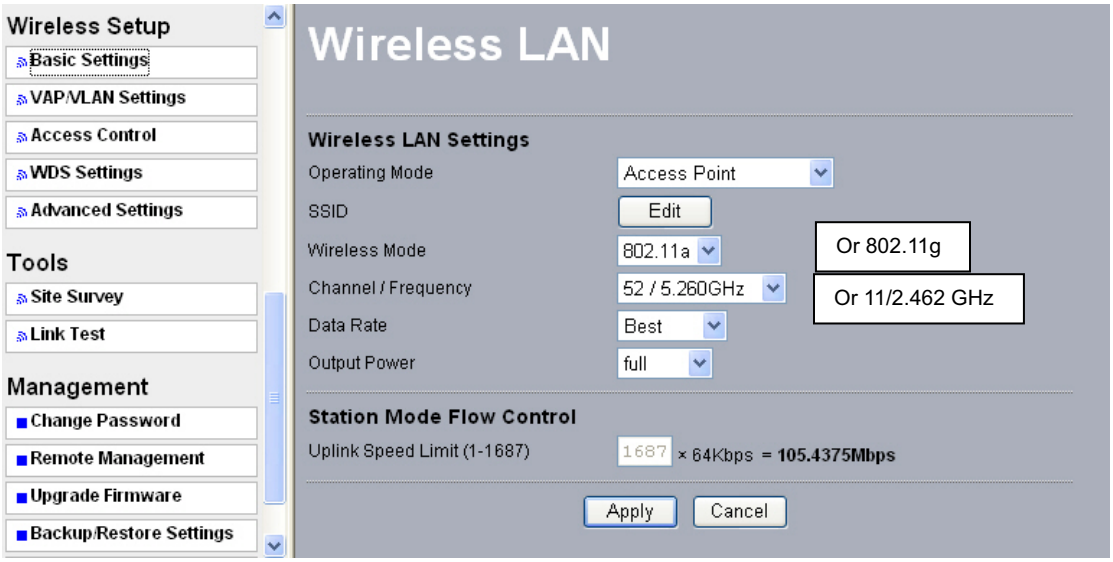


Figure: 5-1 Basic Settings

• Operating Mode:

The AP is capable of five operating modes, as defined below.

•Access Point

Any 802.11a/b/g wireless station can communicate with it by using the correct SSID and security settings.

•Station adapter: Performs as a client, and can associate to other APs. The client must be programmed with the correct SSID and security settings in order to associate to a particular AP.

•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".

•

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

Under unique to ***KymaStar*** WDS mode, radio will automatically connect to each other without manually entering MAC address.

• 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 from the pull down menu.

• Channel.

This field identifies which operating frequency will be used. You can use the site survey feature discussed in chapter six to help you select a channel that is not being used by other AP’s in the area.

• 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 co-located using the same channel frequency. The default is Full.

• Station Mode Flow Control

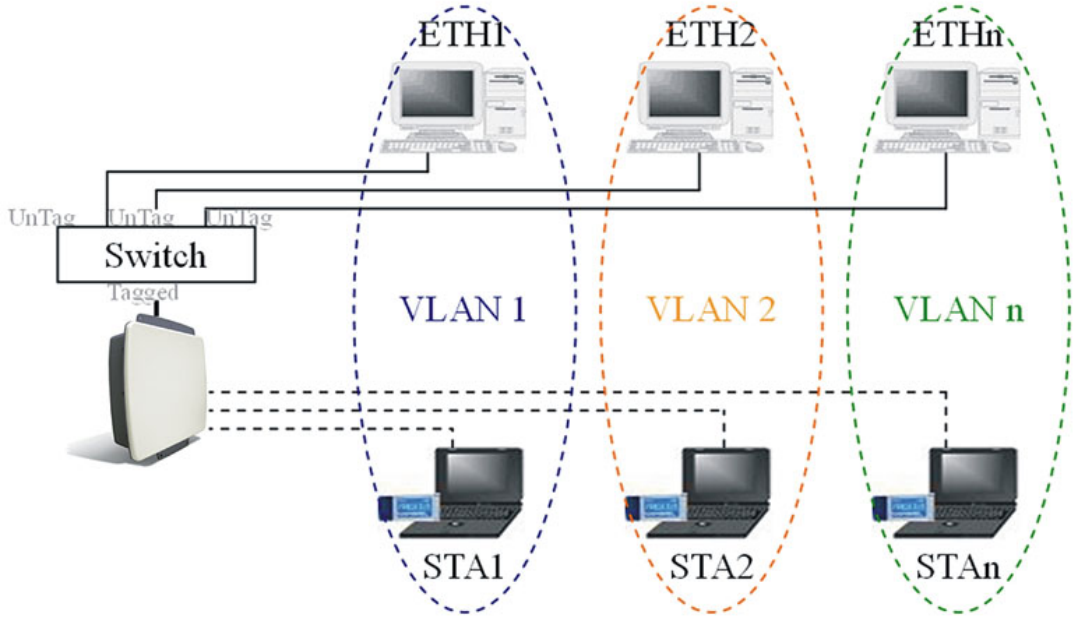
This limits the uplink speed. Select a value between 1 and 1687.

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. Using the VLAN feature it is possible for these multiple devices to function as in different networks without the need for multiple physical network APs.

See the diagram below.



In this mode, this radio can behave as 8 virtual Wireless LAN infrastructures. You can specify a unique SSID for each of these different virtual networks. 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 separate networks. The AP does this by assigning each of the 8 VLANs its own SSID.

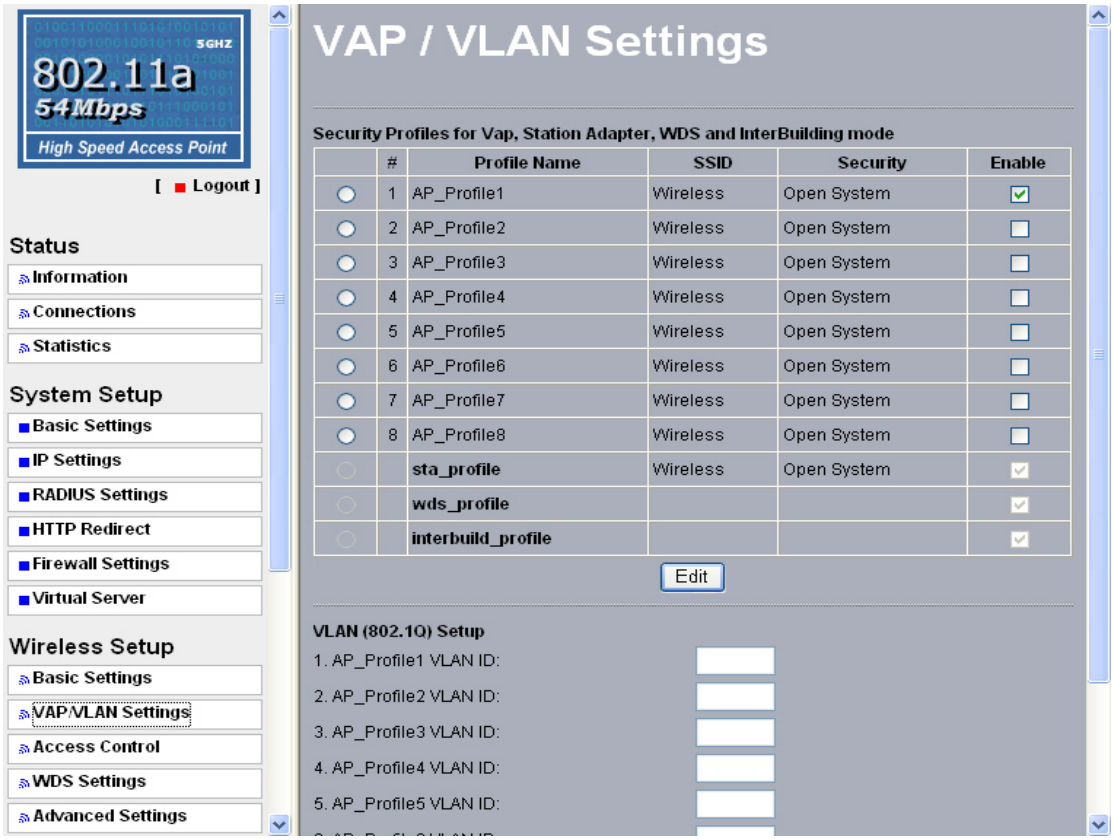


Figure 5-2 VAP / VLAN Settings

You can configure each profile by clicking “Edit”.

Figure 5-3 Security profile for Vap x

5-3 Understanding WEP/WPA Security Options

The following elaborate WEP/WPA security options.

Field	Description
Network Authentication	You have two authentication options. • Open System: This allows any properly configured client to establish a secure connection 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 for you 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.

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.

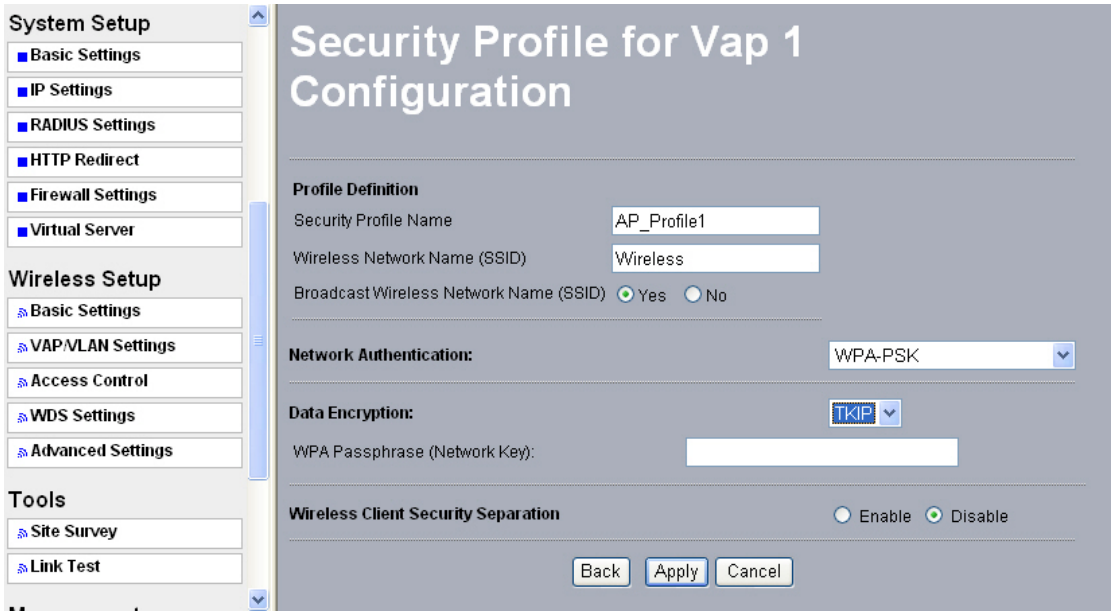


Figure 5-4 Security profile with WPA-PSK

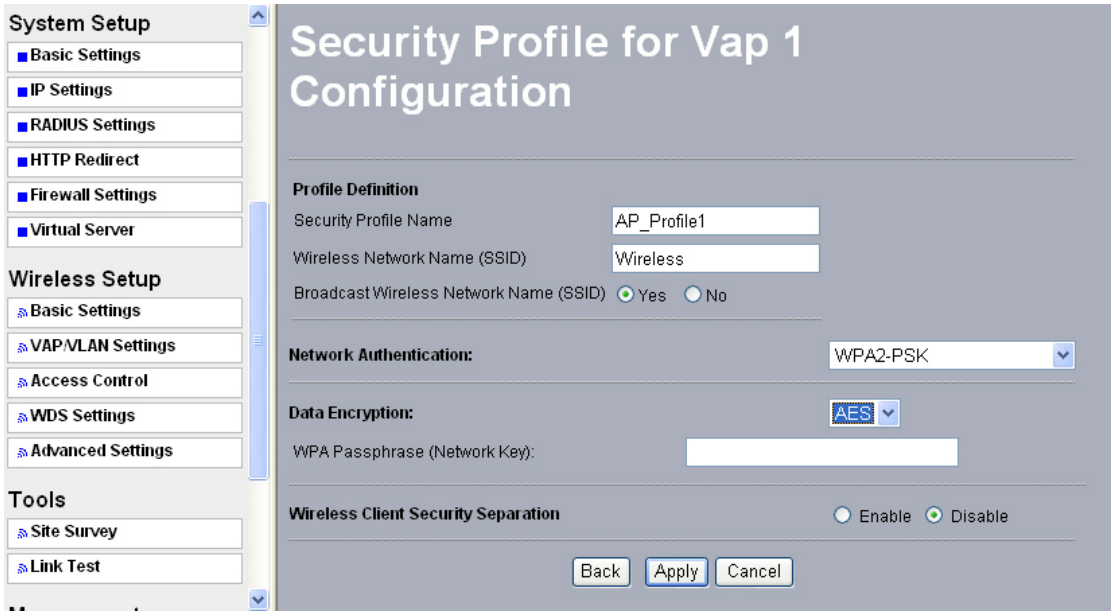


Figure 5-5 Security profile with WPA2-PSK

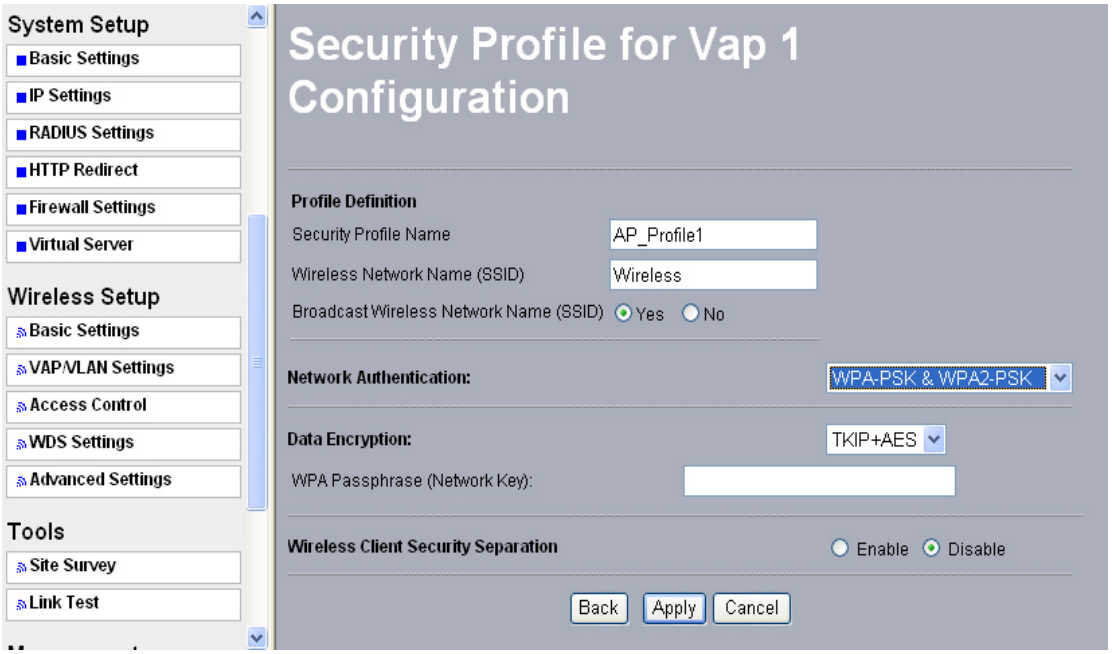


Figure 5-6 Security profile with WPA-PSK & WPA2-PSK

5-4 Access Control

This feature allows you to enter a list of client MAC addresses that will be allowed wireless access to your network. Clients with a MAC address that is not on the list will be denied access.

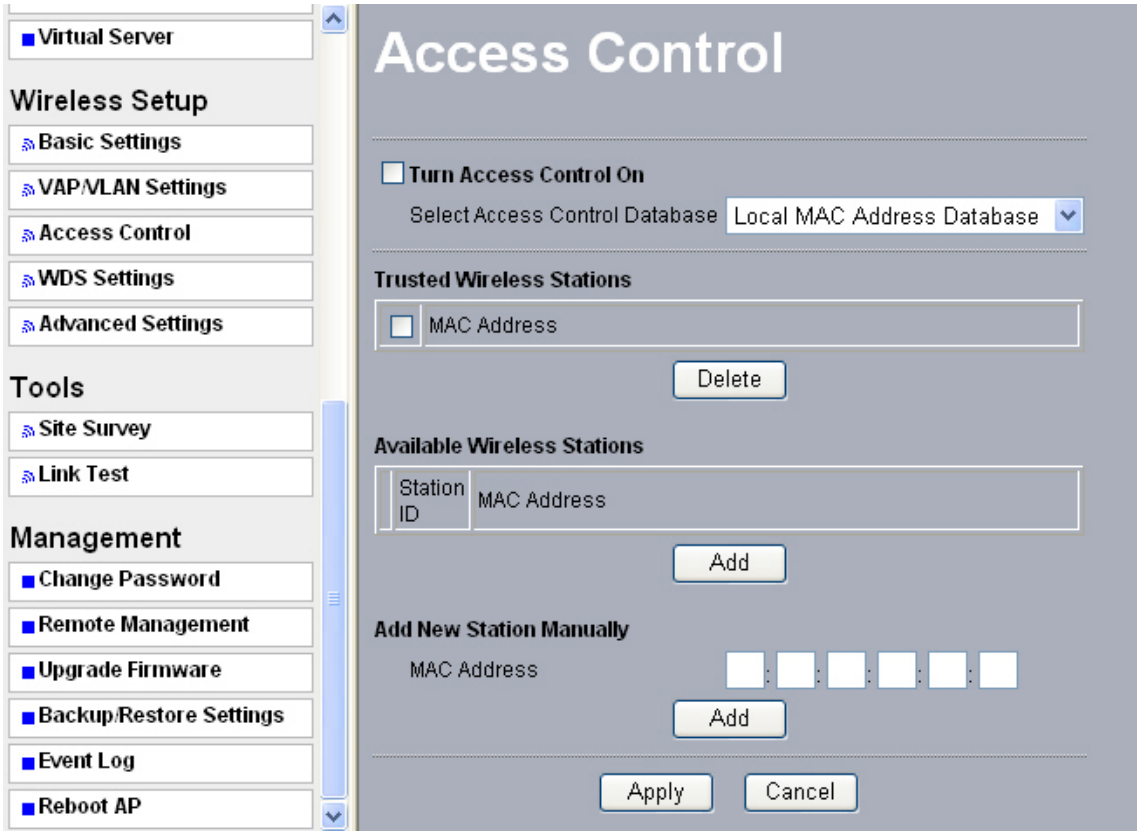


Figure: 5-8 Access Control

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.

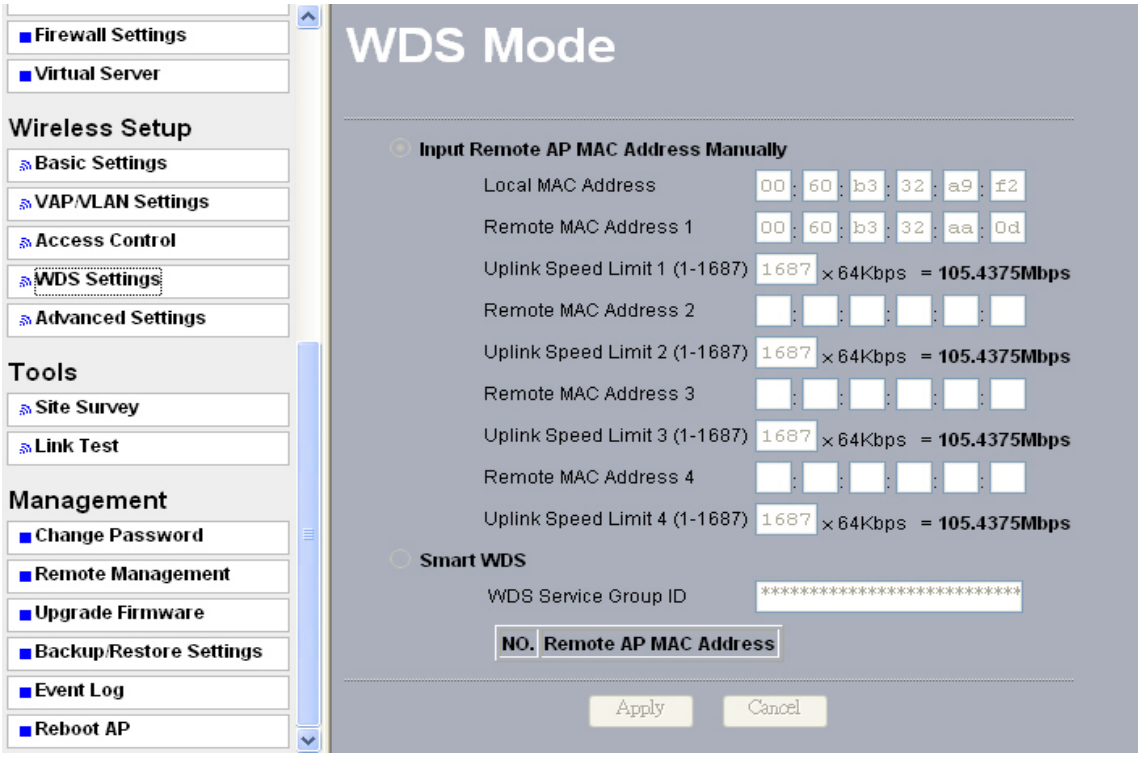


Figure: 5-9 WDS mode

• Local MAC Address:
Enter the MAC address of the local AP

• 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 highest speed available is 1687 ×64Kbps=105.4375Mbps

5-6 Smart WDS

• WDS Service Group ID

If two radios share the same group ID, they will be automatically connected.

Smart WDS can be activated only when the radio is configured in AP mode.

5-7 Advanced Settings

The advanced wireless LAN parameters can be configured to make the AP more efficient for the type of traffic that it will be carrying.

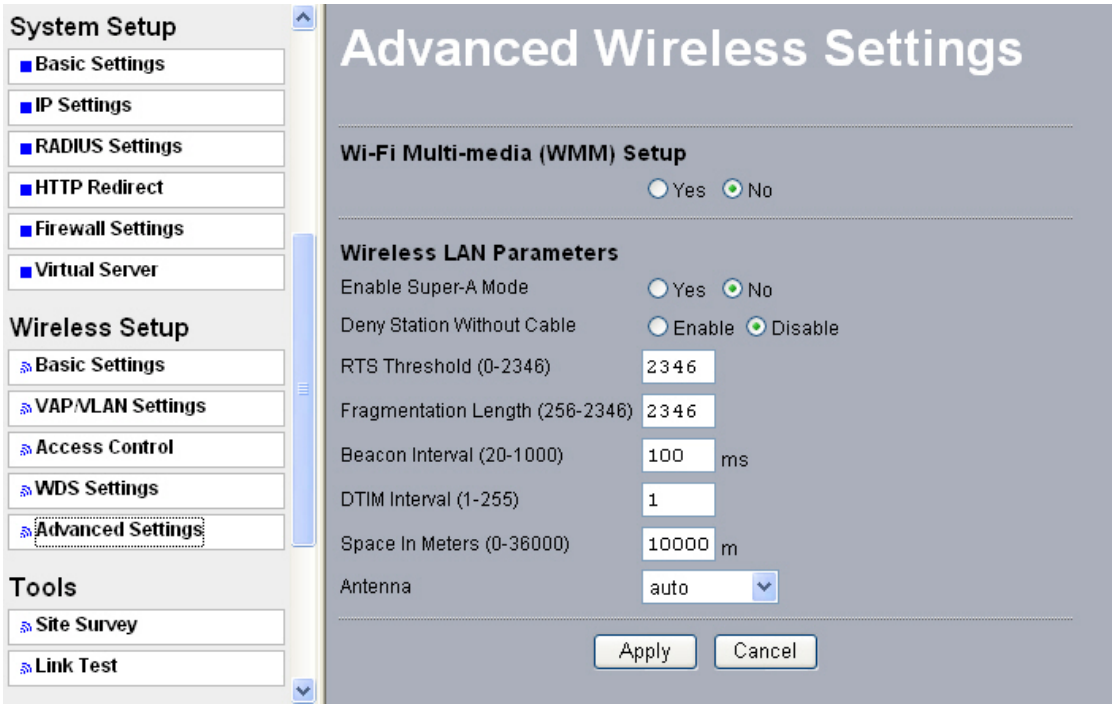


Figure: 5-10 Advanced Wireless Settings

• 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.

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

• Super A or Super G and wireless parameters

Enabling super A, 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 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. **“Auto” is the default setting for 5.X GHz System. “Primary” is the default setting for 2.4 GHz System.**

Chapter 6. Managing and Testing Your AP

6-1 Site Survey

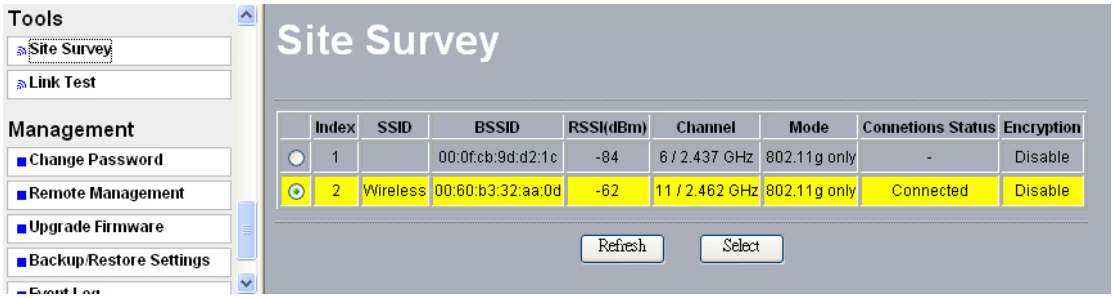


Figure: 6-1 Site survey

Site Survey provides you with a table of adjacent APs discovered by your radio when it acts as a station. For each AP within range, Site Survey displays some 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.

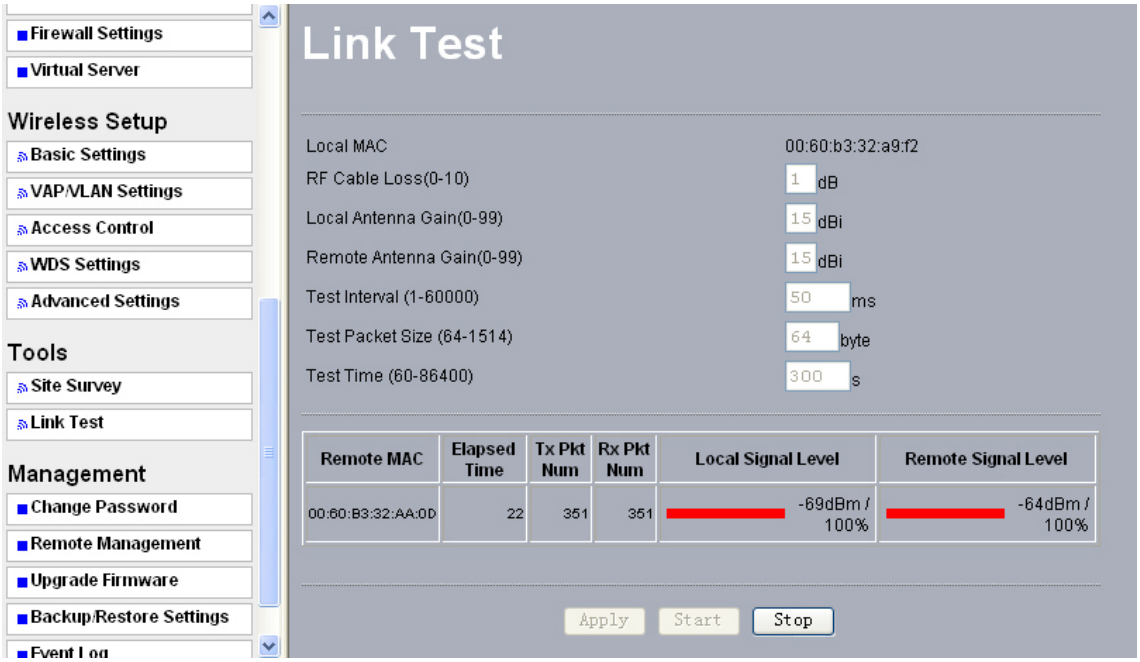


Figure: 6-2 Link test

Below are the parameters used in the Link Test:

• RF Cable Loss (0-10):

Enter the loss in dB of the cable and connectors between the Local radio and its antenna.

• Local Antenna Gain (0-99):

Enter the gain in dB of the local antenna.

• Remote Antenna Gain (0-99):

Enter the gain in dB of the remote antenna

• Wireless local area network (WLAN).ranging from o to 99.

• Test Interval (1-60000): This provides testing time in seconds

• 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

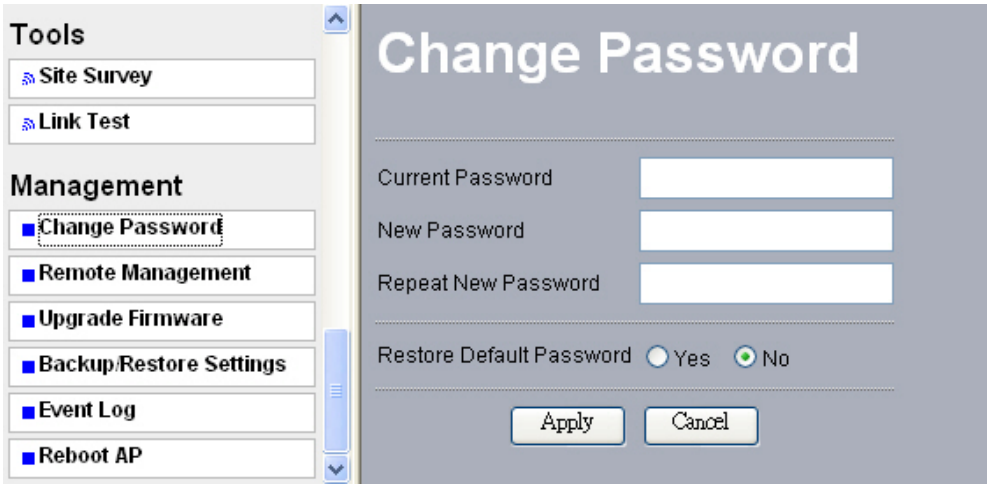


Figure: 7-1 Change Password

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

.

You can also restore the factory-set password. Just click “Yes”, and then “Apply”.

..

7-2 Remote Management

This radio provides remote management to manage and diagnose your network.

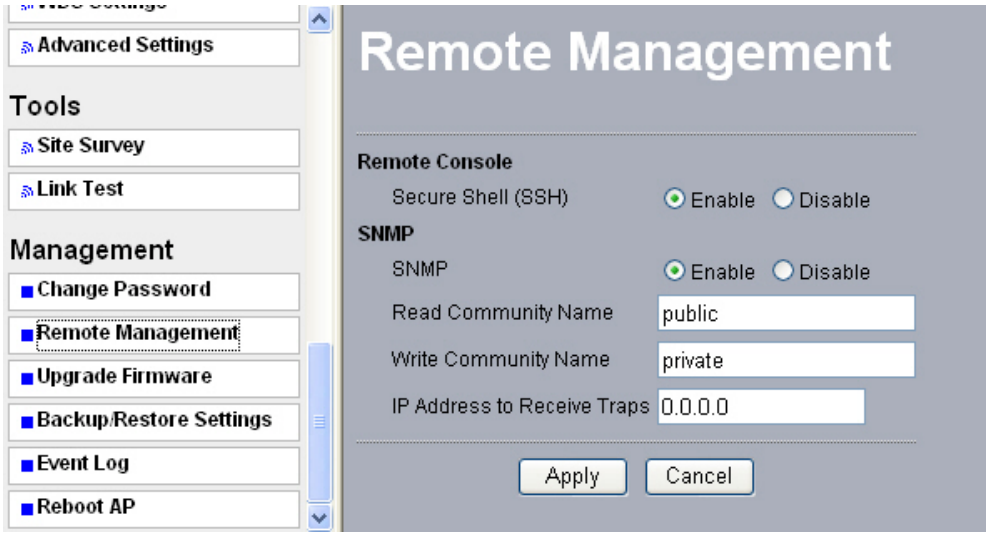


Figure: 7-2 Remote Management

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.

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.

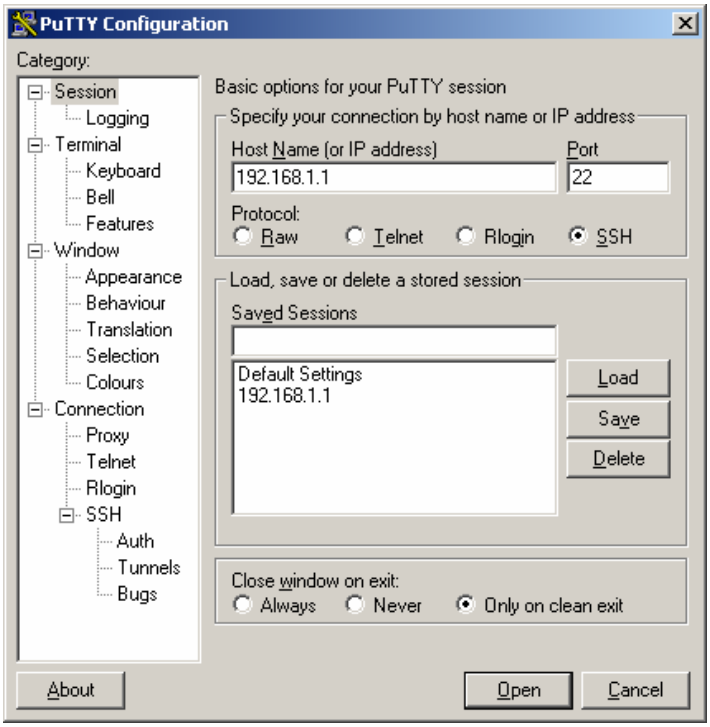


Figure: 7-3 PuTTY configuration utility

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

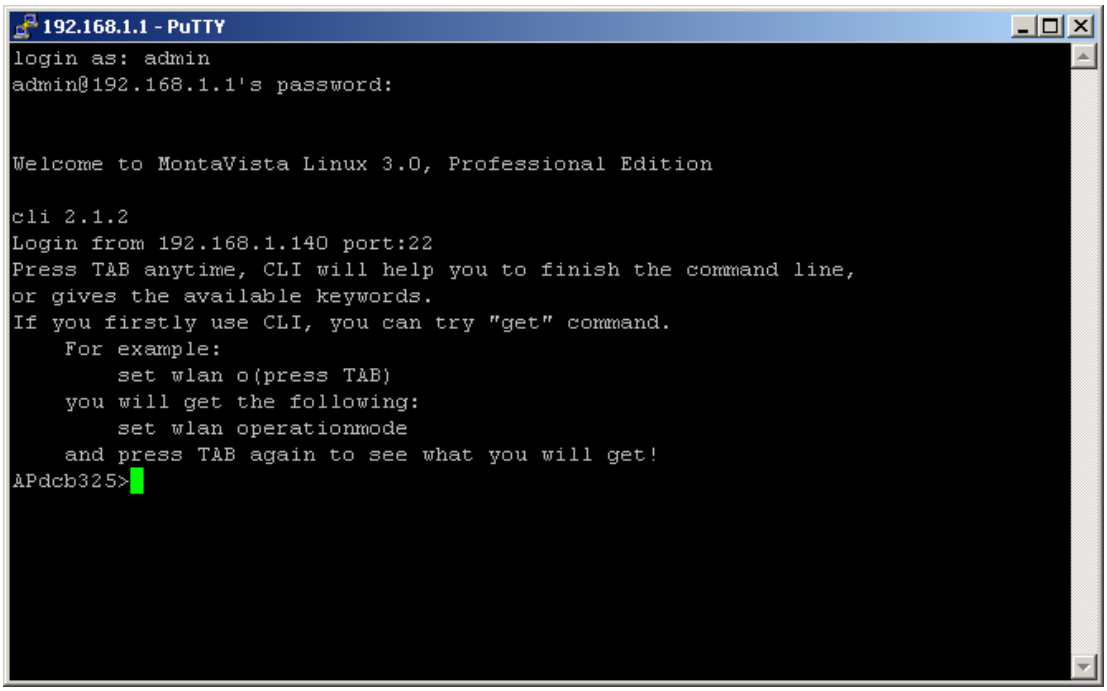


Figure: 7-4 Putty configuration page

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 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 completely 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 below.
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.

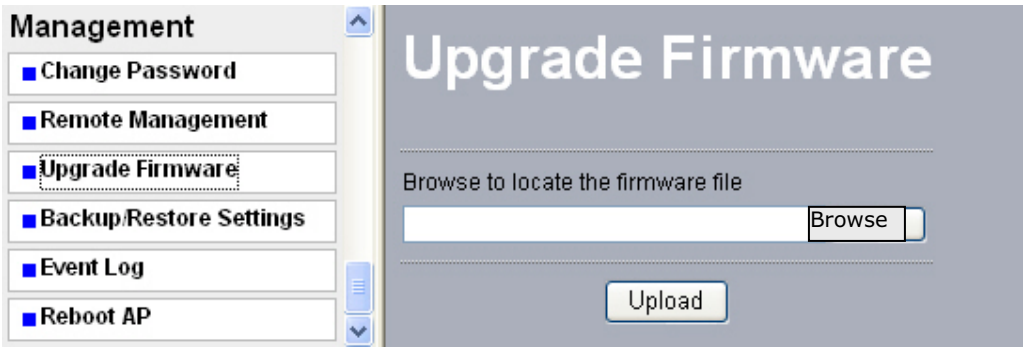


Figure: 7-5 Upgrade Firmware

7-4 Backup / Restore Settings

Radio provides backup and restore for file management.

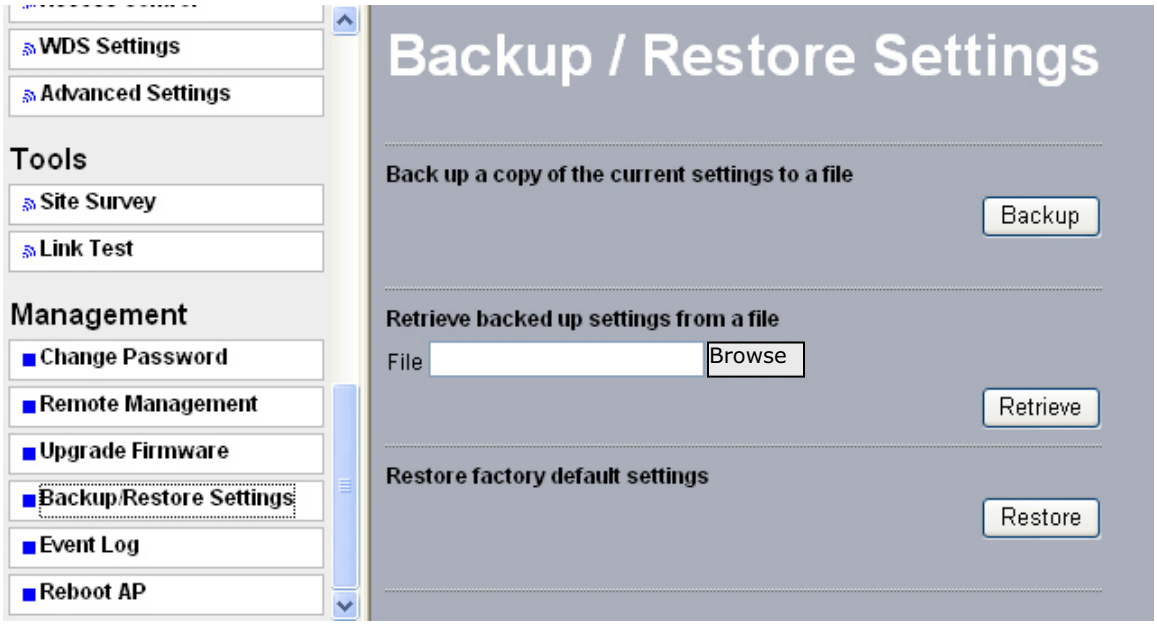


Figure: 7-6 Backup / Restore Settings

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.

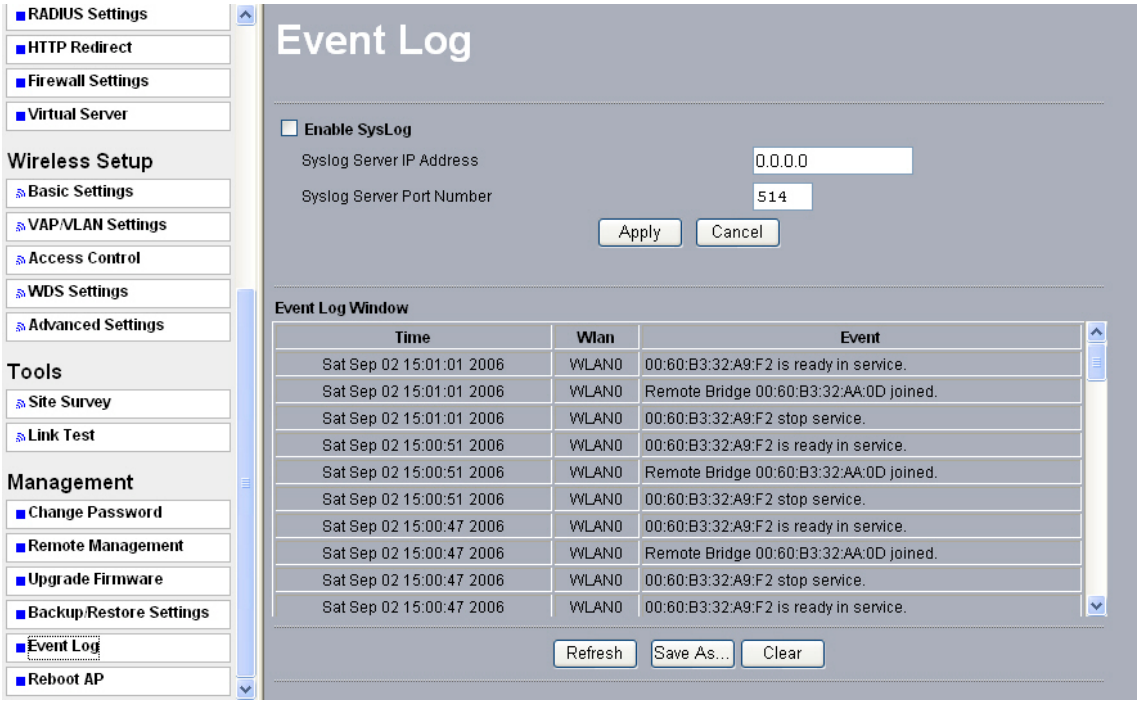


Figure: 7-7 Event log

• 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 default port number configured in the SysLog server is 514.

7-6 Reboot AP

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

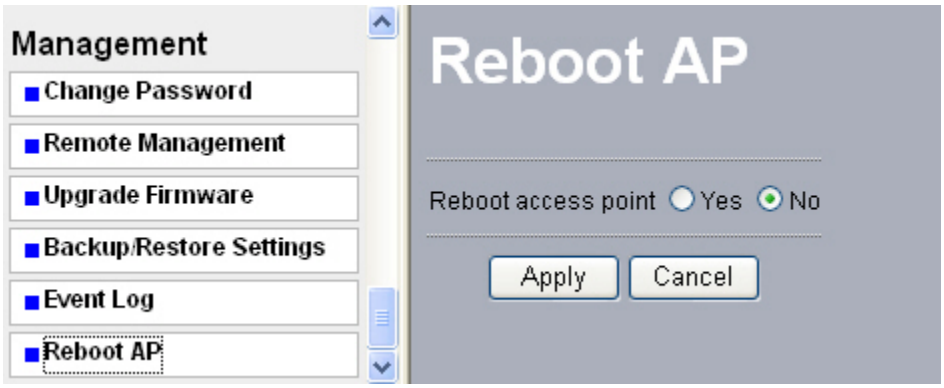


Figure: 7-8 Reboot AP

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. Use the following procedure.

- With the radio powered up, unscrew the screw next to the grounding stud.
- Use a paper clip or similar object to depress the reset button inside the radio for 10 seconds.
- This will delete any configurations you have entered, and restore all factory default configurations

Figure: 7-8 Tool used to unscrew the screw covering the reset button.

Chapter 8. Troubleshooting

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 check that the installation and configuration are done according to the guidance in this manual. In some cases, rebooting the unit can clear the problem.

8-1 General Descriptions

This section will show you how an Outdoor Multi-function radio could be analyzed in the case of “no link”, or there is no traffic being passed. The four main reasons that a link may not work are listed below:

- Configuration
- Path issues such as distance, obstructions, RF reflection, etc.
- Incorrect connection
- Hardware (includes the radio, cable and connectors, etc. In some cases, the radio cannot communicate with the laptop or PC.
- Environment (anything that is outside the equipment and not part of the path itself)

General Check

Two general checks are recommended before taking any action:

- Check whether the software version at both sides the same and 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 a spectrum analyzer. By turning the antenna 360 degrees, you can locate the sources of any interference and the frequencies on which they transmit.

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 to the opposite polarization of the interferer.
- A narrower beam antenna may help. Careful planning is necessary in this case. The replacement antenna must have sufficient beam width to cover the locations of all of your clients, yet narrow enough to eliminate sources of interference.

8-2 Connection Issues

This section describes several common troubles the customer might have while installing and configuring the radios.

Radio Does Not Boot

When the Radio does not boot, follow these steps to check the whole system:

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

Cannot use the Web Interface

If the radio boots, but can't be entered 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 the IP address is correct. If there is response, the Ethernet connection is working properly, go to 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 (including the cables and the connectors). Use a known good unit to ensure that the network connection is properly functioning.

8-3 Configuration Issues

The following relates to setup and configuration problems.

Some basic configurations might make the link fail, below are the major ones:

- RF Channel
- SSID
- IP address
- MAC address filter rules
- Check security settings (such as WEP or WPA)
- Authentication rules, such as settings of radius server and 802.1x
- Check configuration of WDS

8-4 Communication Issues

If two radios can link when they are close to each other, there are two possible reasons that wireless connectivity is not possible when the Outdoor Multi-function radios are at their desired locations:

- RF path problems such as bad antenna alignment, obstructions in the path, defective coaxial cables and connectors, or even defective antennas or feeders. Check all cables and connection for the presence of water. Water in connectors, antennas and feeders can have a dramatic effect on signal level.
- Interference caused by a high signal level from another unit in the area can interrupt communications between your radios. The interference problem can be corrected by changing the frequency checking performance until a suitable frequency can be found. You can also try changing the polarization of the antenna as a way of avoiding the interfering signal.

Chapter 9.1; DATASHEET:

Table 9.1: KS5X-2301-EXT / I23 / I20

RADIO					
Standards	IEEE 802.11a (20 MHz RF Channel)				
Frequency Band	5.150 to 5.850 GHz ; Customized to meet regulatory requirements				
Data Rate	**Modulation**	**Tx Pwr Output****	**Rcvr Sensitivity***	**Net Throughput***	**Range***
OFDM, 54 Mbps	64 QAM	+29(±1.5) dBm	-70 dBm	Up to 23.4 Mbps	Up to 11 Km
OFDM, 36 Mbps	16 QAM	+29(±1.5) dBm	-75 dBm	Up to 18.6 Mbps	Up to 15 Km
OFDM, 16 Mbps	QPSK	+29(±1.5) dBm	-80 dBm	Up to 10.2 Mbps	Up to 19 Km
OFDM, 6 Mbps	BPSK	+29(±1.5) dBm	-87 dBm	Up to 4.7 Mbps	Up to 27 Km
Note :	* **Range** : Path distance, with 23 dBi Integral Antenna at both ends for 99.7% availability at ideal conditions. **Rcvr Sensitivity :** measured at Laboratory conditions for 10^{-6} BER. **** = Peak Power Output**				
Operating Data Rate selection	54/48/36/24/18/12/9/6 Mbps				
INTERFACES					
RF (connect to the antenna)	Type N, female				
Ethernet	IEEE 802.3(10 Base-T) / IEEE 802.3u(100 Base-TX) / IEEE 802.1d (spanning tree protocol) / IEEE 802.1Q (VLAN)				
MANAGEABLILITY					
Management and setup	Web-based configuration				
Configurable Operating mode	AP / CPE / WDS (Bridge) / Repeater / Inter-Building private LAN				
SNMP agents	MIB II				
Protocol	TCP/IP, IPX/SPX, NetBEUI				
Operating System	Windows 98 / 2000 / NT / XP				
Network Architecture	Hotspot / Point to point / Point to multi-point / Repeater				
Data bandwidth Control, QoS	Uplink speed limiting (n x 64 Kbps); VQoS Class: VoIP, Video, Best Effort, Background				
IP Routing	Enable any IP				
Other Features	HTTP Redirect / Virtual Servers				
DHCP supports	DHCP client				
SECURITY					
Data Encryption	WEP 64 / 128 / 152 bits or AES-128 bits encryption				
	WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)				
	WPA2				
Authentication	802.1x Auth.(EAP)				
Authorization	MAC Access Control				
Advanced Security	Disable broadcast SSID				
	Firewall				
	Client Isolation (Layer 2 Isolation)				
ENVIRONMENT					
Operating Temperature	-20°C to +55°C				
Storage Temperature	-30°C to +70°C				
Humidity	95% non-condensing				
POWER SUPPLY					
AC 100-264 V, DC 24 V, 50-60Hz; Power Consumption; 7.5 Watts					
PHYSICAL	**KS5X-2301-EXT**	**KS5X-2301-I23**	**KS5X-2301-I20**		
Dimension	259 (L) × 250 (W) × 75 (H) mm 10.2 x 9.8 x 2.9 in	335(L) x 335(W) x 81(H) mm 13.2 x 13.2 x 3.2 in	330(L) x 295(W) x 91(H)mm 13.0 x 11.6 x 3.6 in		
Weight	1.8 Kg; 4.0 lb	2.9 Kg, 6.4 lb	3.5 Kg, 7.7 lb		
WARRANTY					
1 Year					
ORDER INFORMATION					
KS5X-2301-EXT	5.X GHz, 200mW, AP, CPE, Bridge, Repeater, Private LAN, for External Antenna				
KS5X-2301-I20 (Special Order)	5.X GHz, 200mW, AP, CPE, Bridge, Repeater, Private LAN, 20 dBi Integral ANT, EIRP=43dBm				
KS5X-2301-I23	5.X GHz, 200mW, AP, CPE, Bridge, Repeater, Private LAN, 23 dBi Integral ANT, EIRP=46dBm				

Table 9.2: KS5X-1501-I14

RADIO					
Standards	IEEE 802.11a (20 MHz RF Channel)				
Frequency Band	5.150 to 5.850 GHz ; Customized to meet regulatory requirements				
Data Rate	**Modulation**	**Tx Pwr Output****	**Recvr Sensitivity***	**Net Throughput***	**Range***
OFDM, 54 Mbps	64 QAM	+19(±1.5) dBm	-70 dBm	Up to 23.4 Mbps	Up to 5.2 Km
OFDM, 36 Mbps	16 QAM	+21(±1.5) dBm	-75 dBm	Up to 18.6 Mbps	Up to 7.0 Km
OFDM, 16 Mbps	QPSK	+21(±1.5) dBm	-80 dBm	Up to 10.2 Mbps	Up to 9.0 Km
OFDM, 6 Mbps	BPSK	+21(±1.5) dBm	-87 dBm	Up to 4.7 Mbps	Up to 13.0 Km
Note :	* **Range** : Path distance, with 14 dBi Integral Antenna at both ends for 99.7% availability at ideal conditions. **Recvr Sensitivity:** measured at Laboratory conditions for 10^{-6} BER. **** = Peak Power Output**				
Operating Data Rate selection	54/48/36/24/18/12/9/6 Mbps				
INTERFACES					
RF Output	Internally connected to 14 dBi Integral antenna				
Ethernet	IEEE 802.3(10 Base-T) / IEEE 802.3u(100 Base-TX) / IEEE 802.1d (spanning tree protocol) / IEEE 802.1Q (VLAN)				
MANAGEABLILITY					
Management and setup	Web-based configuration				
Configurable Operating mode	AP / CPE / WDS (Bridge) / Repeater / Inter-Building private LAN				
SNMP agents	MIB II				
Protocol	TCP/IP, IPX/SPX, NetBEUI				
Operating System	Windows 98 / 2000 / NT / XP				
Network Architecture	Hotspot / Point to point / Point to multi-point / Repeater				
Data bandwidth Control, QoS	Uplink speed limiting (n x 64 Kbps); VQoS Class: VoIP, Video, Best Effort, Background				
IP Routing	Enable any IP				
Other Features	HTTP Redirect / Virtual Servers				
DHCP supports	DHCP client				
SECURITY			**INTEGRAL ANTENNA**		
Data Encryption	WEP 64 / 128 / 152 bits or AES-128 bits encryption		RF Band	5.150 ~ 5.875 GHz	
	WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)				
	WPA2		Efctv Gain	14 dBi	
Authentication	802.1x Auth.(EAP)		Beam width	H33.4°; E36.9°	
Authorization	MAC Access Control		VSWR	≦2.0 : 1	
Advanced Security	Disable broadcast SSID		R/B Ratio	>40 dB	
	Firewall		Impedance	50 ohms	
	Client Isolation (Layer 2 Isolation)				
ENVIRONMENT					
Operating Temperature	-20°C to +55°C				
Storage Temperature	-30°C to +70°C				
Humidity	95% non-condensing				
POWER SUPPLY					
AC 100-264 V, DC 24 V, 50-60Hz; Power Consumption; 7.5 Watts					
PHYSICAL					
Dimension	197 (L) × 197 (W) × 70 (H) mm; 7.8 x7.8 x 2.8 in				
Weight	0.8 Kg; 1.8 lb				
WARRANTY					
1 Year					
ORDER INFORMATION					
KS5X-1501-I14	5.X GHz, 200mW, AP, CPE, Bridge, Repeater, Private LAN, 14 dBi Integral ANT, EIRP=29dBm				

Table 9.3: KS24-2302-EXT / I18: KS24-2702-EXT / I18

RADIO						
Standards	IEEE 802.11g/b, Super G (20 MHz RF Channel)					
Frequency	2.400 to 2.4835 GHz Bands ; Customized to meet local reguratory requirements					
IEE 802.xx Standard & Data Rate	**Modulation**	**2305 Pwr Out****	**2705 Pwr Out**	**Rcvr Sensitivity***	**Net Throughput***	**Range***
11g, OFDM, 54 Mbps	64 QAM	27 (±1.5) dBm	24 (±1.5) dBm	-72 (±2) dBm	23.1 Mbps	Up to 15 Km
11g, OFDM, 36 Mbps	16 QAM	29 (±1.5) dBm	26 (±1.5) dBm	-77 (±2) dBm	18.6 Mbps	Up to 20 Km
11g, OFDM, 16 Mbps	QPSK	29 (±1.5) dBm	26 (±1.5) dBm	-82 (±2) dBm	10.3 Mbps	Up to 25 Km
11g, OFDM, 6 Mbps	BPSK	29 (±1.5) dBm	26 (±1.5) dBm	-89 (±2) dBm	5.5 Mbps	Up to 35 Km
11g/Super G, OFDM, 108 Mbps	64 QAM	21 (±1.5) dBm	24 (±1.5) dBm	-72 (±2) dBm	34.0 Mbps	Up to 15 Km
11b, DSSS, 5 Mbps, 5 MHz CH	BPSK	29 (±1.5) dBm	30 (±1.5) dBm	-92 (±2) dBm	4.5 Mbps	Up to 45 Km
Note :	**Range** : Path distance, with 18 dBi Integral Antenna at both ends for 99.97% availability at Ideal conditions. **Net Throughput** : ' Up to ' figures under ideal conditions. **Rcvr Sensitivity** : at 10^{-6} BER. ****=Peak Pwr Output**					
INTERFACES						
RF (External Antenna Port)	Type N, female					
Ethernet	IEEE 802.3(10 Base-T) / IEEE 802.3u(100 Base-TX) / IEEE 802.1d (spanning tree protocol) / IEEE 802.1Q (VLAN)					
MANAGEABLILITY						
Management and setup	Web-based configuration					
Operating mode	AP / CPE / WDS (Bridge) / Repeater / Inter-Building Private LAN					
SNMP agents	MIB II					
Protocol	TCP/IP, IPX/SPX, NetBEUI					
Operating System	Windows 98 / 2000 / NT / XP					
Network Architecture	Hotspot / Point to point / Point to multi-point / Repeater					
IP Routing	Enable any IP					
Other Features	HTTP Redirect / Virtual Servers					
DHCP supports	DHCP client					
SECURITY						
Data Encryption	WEP 64/128/152 bits or AES-128 encryption					
	WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)					
	WPA2					
Authentication	802.1x Auth.(EAP)					
Authorization	MAC Access Control					
Advanced Security	Disable broadcast SSID					
	Firewall					
	Client Isolation (Layer 2 Isolation)					
ENVIRONMENT						
Operating Temperature	-20°C~55°C					
Storage Temperature	-30°C ~70°C					
Humidity	95% non-condensing					
POWER SUPPLY						
AC 100-264 V, DC 24 V, 50-60Hz: Power Consumption: KS24-2302 = 9.7 Watts, KS24-2702 = 15 Watts						
PHYSICAL	**KS24-2302-EXT**		**KS24-2702-EXT**		**KS24-XX02-I18**	
Dimension	259(L) x 250(W) x 75(H) mm 10.2 x 9.9 x 3.0 in		259(L) x 250(W) x 75(H) mm 10.2 x 9.9 x 3.0 in		330(L) x 295(W) x 91(H) mm 13.0 x 11.6 x 3.6 in	
Weight	1.8 Kg, 4.0 lb		2.9 Kg, 6.4 lb		Add 1.7 Kg (3.8lb) to EXT Opt.	
WARRANTY						
1 Year						
ORDERING INFORMATION						
KS24-2302-I18	2.4GHz, EIRP=41dBm OFDM/DSSS, AP, CPE, Bridge, Repeater, Private LAN, with 18dBi Integral Ant.					
KS24-2702-I18	2.4GHz, EIRP=45dBm OFDM/DSSS, AP, CPE, Bridge, Repeater, Private LAN, with 18dBi Integral Ant					
KS24-2302-EXT	2.4GHz, 200mW OFDM/DSSS, AP, CPE, Bridge, Repeater, Private LAN, for External Antenna					
KS24-2702-EXT	2.4GHz, 500mW OFDM/DSSS, AP, CPE, Bridge, Repeater, Private LAN, for External Antenna					

Chapter 9.2; WNI Global, Contact Information

WNI GLOBAL, Inc.

Contact Information:

Address: 2146 Bering Drive
San Jose, CA 95131, USA

Tel: +1-408-432-8892
Fax: +1-408-432-8896
or +1-408-432-8897
E-Mail: sales@wnint.com
Web Site: www.wnint.com

WNI GLOBAL, Inc.
2146 Bering Drive
San Jose, CA 95131, USA
Tel: +1(408)432-8892
Fax: +1(408)432-8896

WNI GLOBAL, Inc.
2146 Bering Drive
San Jose, CA 95131, USA
Tel: +1(408)432-8892
Fax: +1(408)432-8896