11n Dual Band
Wireless Access Point

User's Guide

TABLE OF CONTENTS

P/N:

Document Version: 1.0

Chapter 1

Introduction

This Chapter provides an overview of the Wireless Access Point's features and capabilities.

Congratulations on the purchase of your new Wireless Access Point. The Wireless Access Point links your Wireless Stations to your wired LAN. With the Wireless Access Point, you can select either 2.4 GHz or 5 GHz radio bands, which provides the flexibility to manage a graceful transition from networks. The Wireless stations and devices on the wired LAN are then on the same network, and can communicate with each other without regard for whether they are connected to the network via a Wireless or wired connection.

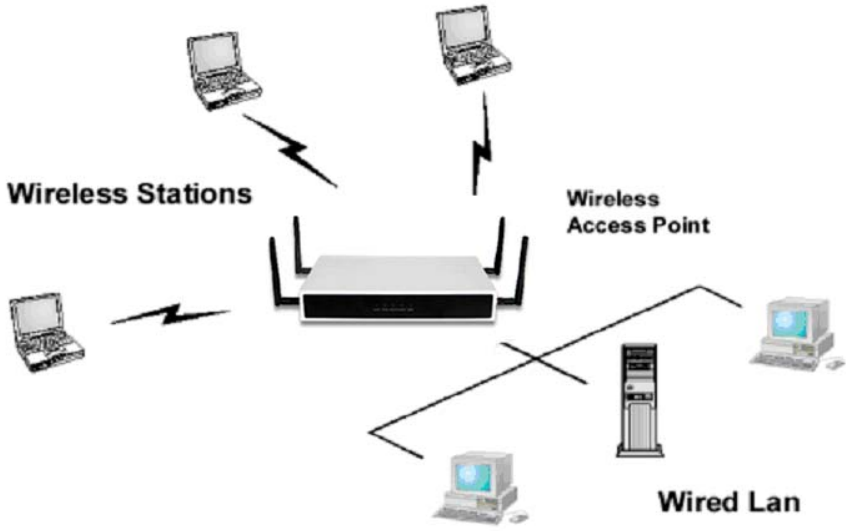

Figure 1: Wireless Access Point

Features of your Wireless Access Point

The Wireless Access Point incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

- ***Standards Compliant.*** The Wireless Access Point complies with the IEEE802.11g and IEEE802.11n draft 2.0 specifications for Wireless LANs.
- ***Supports 11n Wireless Stations.*** The 802.11n Draft standard provides for backward compatibility with the 802.11b standard, so 802.11n, 802.11a, 802.11b and 802.11g Wireless stations can be used simultaneously. The Wireless Access Point supports both the 2.4GHz and 5.0GHz (802.11a) bands.
- ***DHCP Client Support.*** **D**ynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The Wireless Access Point can act as a **DHCP Client**, and obtain an IP address and related information from your existing DHPC Server.

- ***Upgradeable Firmware.*** Firmware is stored in a flash memory and can be upgraded easily, using only your Web Browser.
- ***PoE Support.*** You can use PoE (Power over Ethernet) to provide power to the Wireless Access Point, so only a single cable connection is required.

Security Features

- ***Virtual APs.*** For maximum flexibility, wireless security settings are stored in Virtual AP. Up to 16 Virtual APs can be defined and used as any time.
- ***Multiple BSSIDs.*** Because each Virtual AP has it own SSID and beacon, and up to 16 Virtual APs can be active simultaneously, multiple SSIDs are supported. Different clients can connect to the Wireless Access Point using different SSIDs, with different security settings.
- ***Virtual APs Isolation.*** If desired, PCs and devices connecting to different Virtual APs can be isolated from each other.
- ***VLAN Support.*** The 802.1Q VLAN standard is supported, allowing traffic from different sources to be segmented. Combined with the multiple SSID feature, this provides a powerful tool to control access to your LAN.
- ***WEP support.*** Support for WEP (Wired Equivalent Privacy) is included. The 64 Bit, 128 Bit and 152 Bit keys are supported.
- ***WPA support.*** Support for WPA is included. WPA is more secure than WEP, and should be used if possible. Both TKIP and AES encryption methods are supported.
- ***802.1x Support.*** Support for 802.1x mode is included, providing for the industrial-strength wireless security of 802.1x authentication and authorization.
- ***Radius Client Support.*** The Wireless Access Point can login to your existing Radius Server (as a Radius client).
- ***Radius MAC Authentication.*** You can centralize the checking of Wireless Station MAC addresses by using a Radius Server.
- ***Rogue AP Detection.*** The Wireless Access Point can detect unauthorized (Rouge) Access Points on your LAN.
- ***Access Control.*** The Access Control feature can check the MAC address of Wireless clients to ensure that only trusted Wireless Stations can use the Wireless Access Point to gain access to your LAN.
- ***Password - protected Configuration***. Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings.

Advanced Features

- ***Command Line Interface.*** If desired, the command line interface (CLI) can be used for configuration. This provides the possibility of creating scripts to perform common configuration changes.
- ***Auto Configuration.*** The Wireless Access Point can perform self-configuration by copying the configuration data from another Access Point. This feature is enabled by default.
- ***Auto Update.*** The Wireless Access Point can automatically update its firmware, by downloading and installing new firmware from your FTP server.
- ***Radius Accounting Support.*** If you have a Radius Server, you can use it to provide accounting data on Wireless clients.
- ***Syslog Support.*** If you have a Syslog Server, the Wireless Access Point can send its log data to your Syslog Server.

- ***SNMP Support.*** SNMP (Simple Network Management Protocol) is supported, allowing you to use a SNMP program to manage the Wireless Access Point. When stores the configuration, will not affect the operation of SNMP and CLI.
- ***VPN Pass – through.*** Do not affect related application operation (such as ICMP, FTP, HTTP, Etc.) when in IP network, and support VPN Pass - through function.

Package Contents

The following items should be included:

- Wireless Access Point
- Power Adapter
- Two 5G Detachable Antennas
- Two 2.4G Detachable Antennas
- Quick Start Guide
- CD-ROM containing the on-line manual

If any of the above items are damaged or missing, please contact your dealer immediately.

Physical Details

Front Panel LEDs

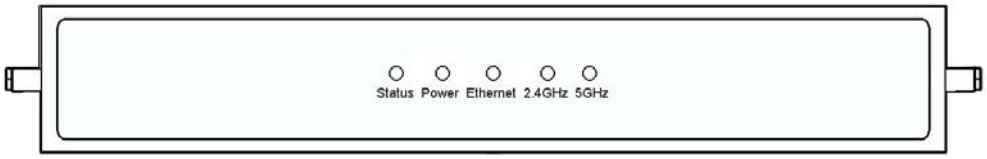

Figure 2: Front Panel

Antenna Ports (Left Side)	Attach the 5G antennas here.
Status	**On** - Error condition.
	Off - Normal operation.
	Blinking - During start up, and when the Firmware is being upgraded.
Power	**On** - Normal operation.
	Off - No power
Ethernet	**On** - Corresponding LAN (hub) port is active.
	Off - No active connection on the corresponding LAN (hub) port.
	Flashing - Data is being transmitted or received via the corresponding LAN (hub) port.
2.4 GHz	**On** - Wireless connection is available in 2.4GHz mode.
	Off - Wireless connection is not available in 2.4GHz mode.
	Flashing - Data is being transmitted or received via the Wireless access point. Data includes "network traffic" as well as user data.
5 GHz	**On** - Wireless connection is available in 5GHz mode.
	Off - Wireless connection is not available in 5GHz mode.
	Flashing - Data is being transmitted or received via the Wireless access point. Data includes "network traffic" as well as user data.
Antenna Ports (Right Side)	Attach the 2.4G antennas here.

Rear Panel

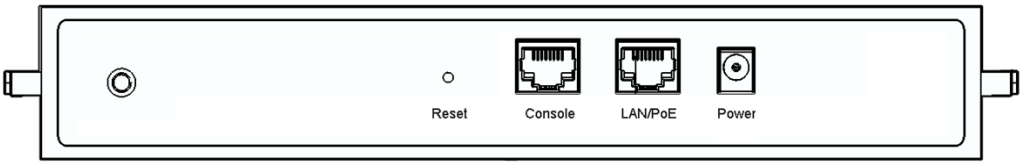

Figure 3: Rear Panel

Reset Button

This button has two (2) functions:

- **Reboot**. When pressed and released, the Wireless Access Point will reboot (restart).
- **Reset to Factory Defaults**. This button can also be used to clear ALL data and restore ALL settings to the factory default values.

To Clear All Data and restore the factory default values:

1. Hold the Reset Button until the Status (Red) LED blinks TWICE, usually more than 5 seconds.
2. Release the Reset Button.
   The factory default configuration has now been restored, and the Access Point is ready for use.

Console port — This port allows root access to the router via a dumb terminal interface.

LAN/PoE — Use a standard LAN cable (RJ45 connectors) to connect this port to a 10/100/1000BaseT hub/switch on your LAN.

Power port — Connect the supplied power adapter (12V) here.

Wall Mount Template

The following image illustrates the mounting slots on the bottom of the device.

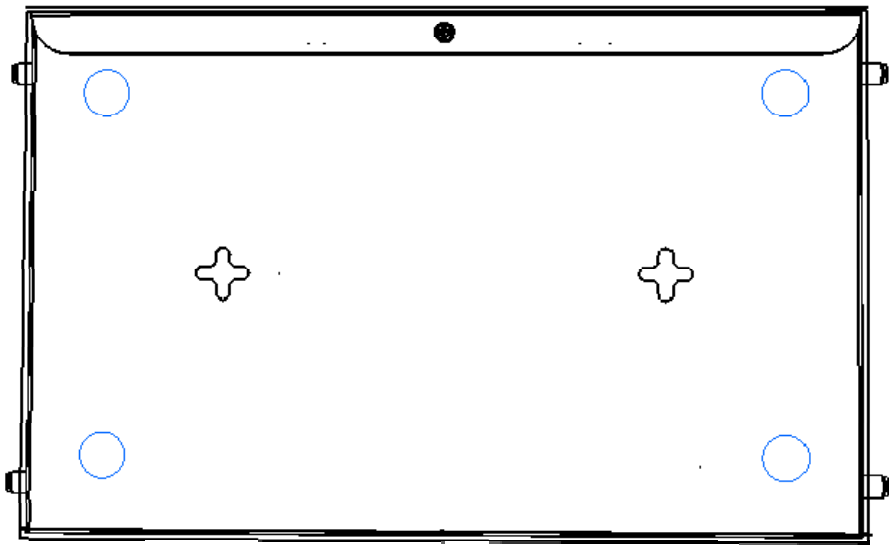

Figure 4: Wall Mount

Chapter 2

Installation

This Chapter covers the physical installation of the Wireless Access Point.

Requirements

Requirements:

- TCP/IP network
- Ethernet cable with RJ-45 connectors
- Installed Wireless network adapter for each PC that will be wirelessly connected to the network.

Procedure

1. Select a suitable location for the installation of your Wireless Access Point. To maximize reliability and performance, follow these guidelines:
   - Use an elevated location, such as wall mounted or on the top of a cubicle.
   - Place the Wireless Access Point near the center of your wireless coverage area.
   - If possible, ensure there are no thick walls or metal shielding between the Wireless Access Point and Wireless stations. Under ideal conditions, the Wireless Access Point has a range of around 150 meters (450 feet). The range is reduced, and transmission speed is lower, if there are any obstructions between Wireless devices.

Figure 5: Installation Diagram

2. Use a standard LAN cable to connect the "LAN" port on the Wireless Access Point to a 10/100/1000BaseT hub/switch on your LAN.
3. Connect the supplied power adapter to the Wireless Access Point and a convenient power outlet, and power up.
4. Check the LEDs:
   - The *Status* LED should flash, then turn OFF.
   - The *Power* and *Ethernet* LEDs should be ON.

   For more information, refer to *Front Panel LEDs* in Chapter 1.

Using PoE (Power over Ethernet)

The Wireless Access Point supports PoE (Power over Ethernet). To use PoE:

1. Do not connect the supplied power adapter to the Wireless Access Point.
2. Connect one end of a standard (category 5) LAN cable to the Ethernet port on the Wireless Access Point.
3. Connect the other end of the LAN cable to the powered Ethernet port on a suitable PoE Adapter.
4. Connect the unpowered Ethernet port on the PoE adapter to your Hub or switch.
5. Connect the power supply to the PoE adapter and power up.
6. Check the LEDs on the Wireless Access Point to see it is drawing power via the Ethernet connection.

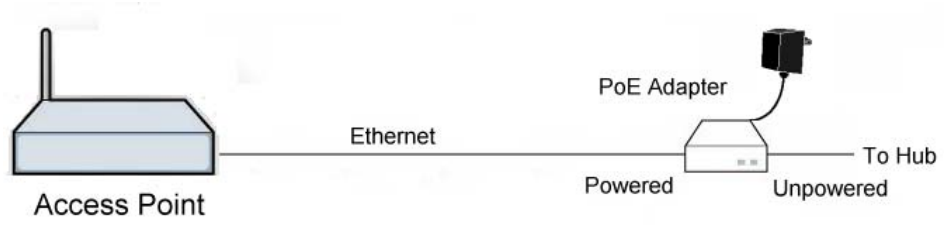

Figure 6: Using PoE (Power over Ethernet)

Chapter 3

Access Point Setup

This Chapter provides details of the Setup process for Basic Operation of your Wireless Access Point.

Overview

This chapter describes the setup procedure to make the Wireless Access Point a valid device on your LAN, and to function as an Access Point for your Wireless Stations.

Wireless Stations may also require configuration. For details, see *Chapter 4 - PC and Server Configuration*.

The Wireless Access Point can be configured using your Web Browser.

Setup using a Web Browser

Your Browser must support JavaScript. The configuration program has been tested on the following browsers:

- Chrome
- Firefox
- Internet Explorer 7 or later

Setup Procedure

Before commencing, install the Wireless Access Point in your LAN, as described previously.

1. Check the Wireless Access Point to determine its *Host Name*. This is shown on a label on the base or rear, and is in the following format:

   APxxxxxx

   Where `xxxxxx` is the last 6 Hex characters (0 ~ 9, and A ~ F) of the MAC address.
2. Use a PC which is already connected to your LAN, either by a wired connection or another Access Point.
   - Until the Wireless Access Point is configured, establishing a Wireless connection to it may be not possible.
   - If your LAN contains a Router or Routers, ensure the PC used for configuration is on the same LAN segment as the Wireless Access Point.
3. Start your Web browser.
4. In the *Address* box, enter "HTTP://" and the IP Address of the 11N Wireless Access Point, as in this example, which uses the Wireless Access Point's default IP Address:

   `HTTP://192.168.0.228`
5. You should then see a login prompt, which will ask for a *User Name* and *Password*. Enter **`admin`** for the *User Name*, and **`password`** for the *Password*.
   These are the default values. The password can and should be changed. Always enter the

current user name and password, as set on the *Administration-Management-Account* screen.

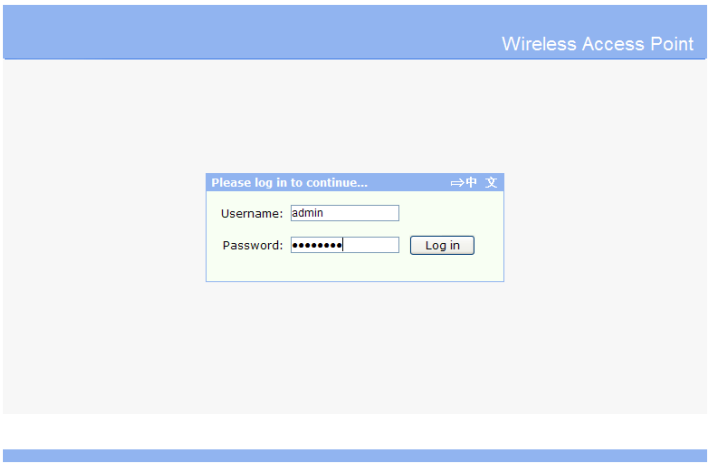

Figure 7: Password Dialog

6. You will then see the *Status* screen, which displays the current settings and status. No data input is possible on this screen. See Chapter 5 for details of the *Status* screen.
7. From the menu, check the following screens, and configure as necessary for your environment. Details of these screens and settings are described in the following sections of this chapter.
8. Use the **Apply** and **Logout** buttons on the menu to apply your changes and exit the Wireless Access Point.

Setup is now complete.

Wireless stations must now be set to match the Wireless Access Point. See Chapter 4 for details.

If you can't connect:

It is likely that your PC's IP address is incompatible with the Wireless Access Point's IP address. This can happen if your LAN does not have a DHCP Server. The default IP address of the Wireless Access Point is 192.168.0.228, with a Network Mask of 255.255.255.0.

If your PC's IP address is not compatible with this, you must change your PC's IP address to an unused value in the range 192.168.0.1 ~ 192.168.0.254, with a Network Mask of 255.255.255.0. See ***Appendix C - Windows TCP/IP*** for details for this procedure.

System - Basic Settings Screen

Click *Basic Settings* on the System menu to view a screen like the following.

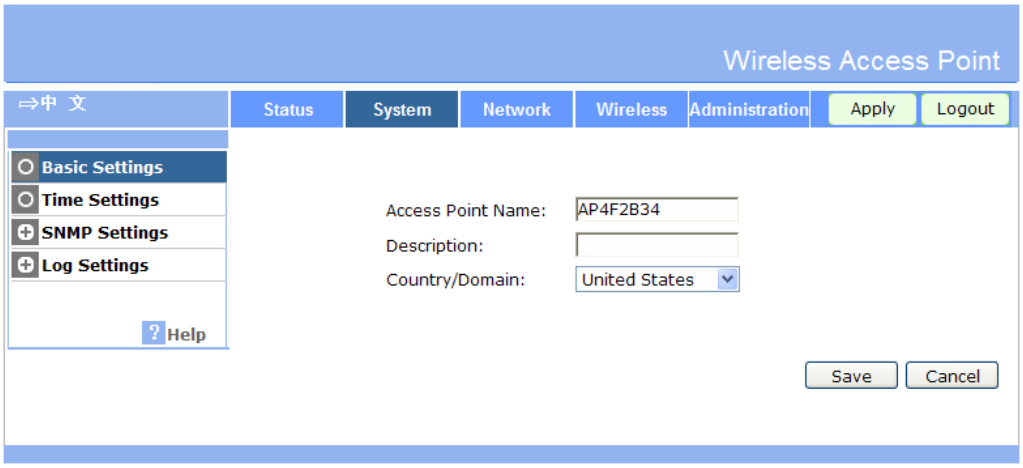

Figure 8: Basic Settings Screen

Data - Basic Settings Screen

Basic Settings	
Access Point Name	It displays the default host name of the device. Enter a suitable name for this Access Point if required.
Description	If desired, you can enter a description for the Access Point.
Country/Domain	The country or domain which is matching your current location.

System - Time Settings Screen

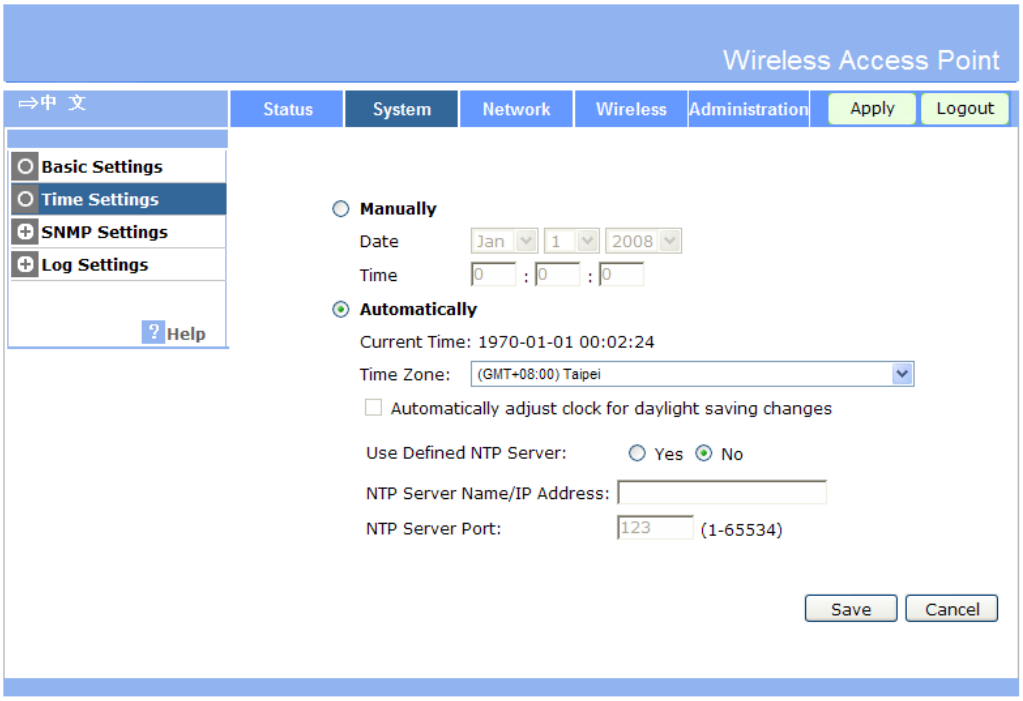

Figure 9: Time Settings Screen

Data - Time Settings Screen

TimeZone	

Time Settings	Select either Manually or Automatically
	• Manually
	  • Date - Select the date to match your location.
	  • Time - Enter the correct time.
	• Automatically
	  • Current Time - It displays the current date and time.
	  • Time Zone - Choose the Time Zone for your location from the drop-down list. If your location is currently using Day-light Saving, enable the **Automatically adjust for daylight saving changes** checkbox.
	You must UNCHECK this checkbox when Daylight Saving Time finishes.
	  • Use Defined NTP Server - If you prefer to use a particular NTP server as the primary server, check this checkbox and enter the Server's IP address in the fields provided. If this setting is not enabled, the default NTP Server is used.
	  • NTP Server Name/IP Address - Enter the server name or IP address of the NTP.
	  • NTP Server Port - Enter the port for the NTP server.

System - SNMP Settings

SNMP (Simple Network Management Protocol) is only useful if you have a SNMP program on your PC. To reach this screen, select *SNMP* in the **System** section of the menu.

Basic Screen

Figure 10: Basic Screen

Data - Basic Screen

Basic	
SNMP v1/v2/v3	Use this to enable or disable SNMP as required.
Contact	The identification of the contact person.
Device Name	Enter the desired name for the device.
Location	The physical location of this node.
Read Only community	Data can be read, but not changed.
Read/Write Community	Data can be read and changed.

SNMPv3

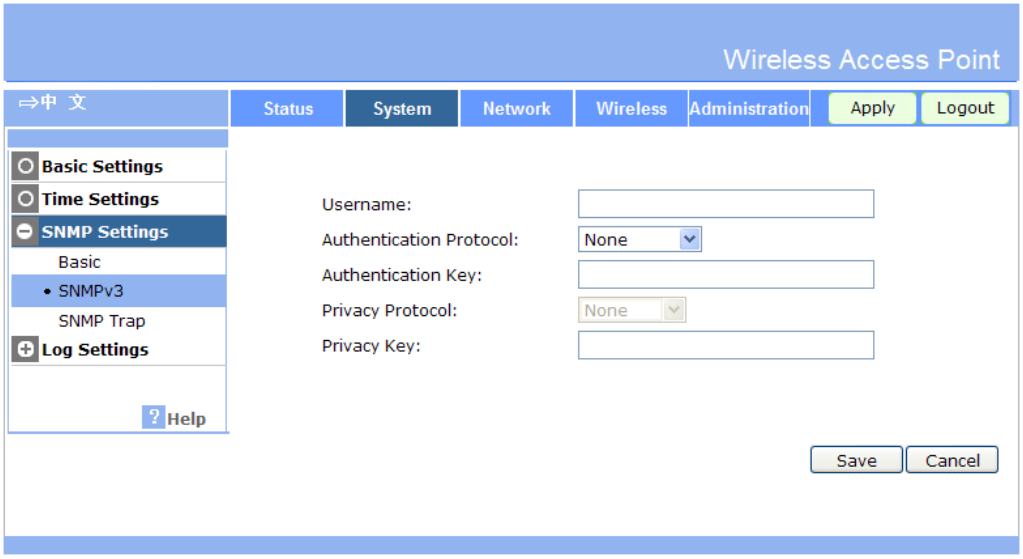

Figure 11: SNMPv3 Screen

Data - SNMPv3 Screen

SNMPv3	
User Name	Enter the user name for SNMPv3.
Authentication Protocol	Select the authentication protocol used by SNMPv3.
Authentication Key	Enter the authentication key required by SNMPv3.
Privacy Protocol	Select the private protocol as required.
Privacy Key	Enter the private key here.

SNMP Trap

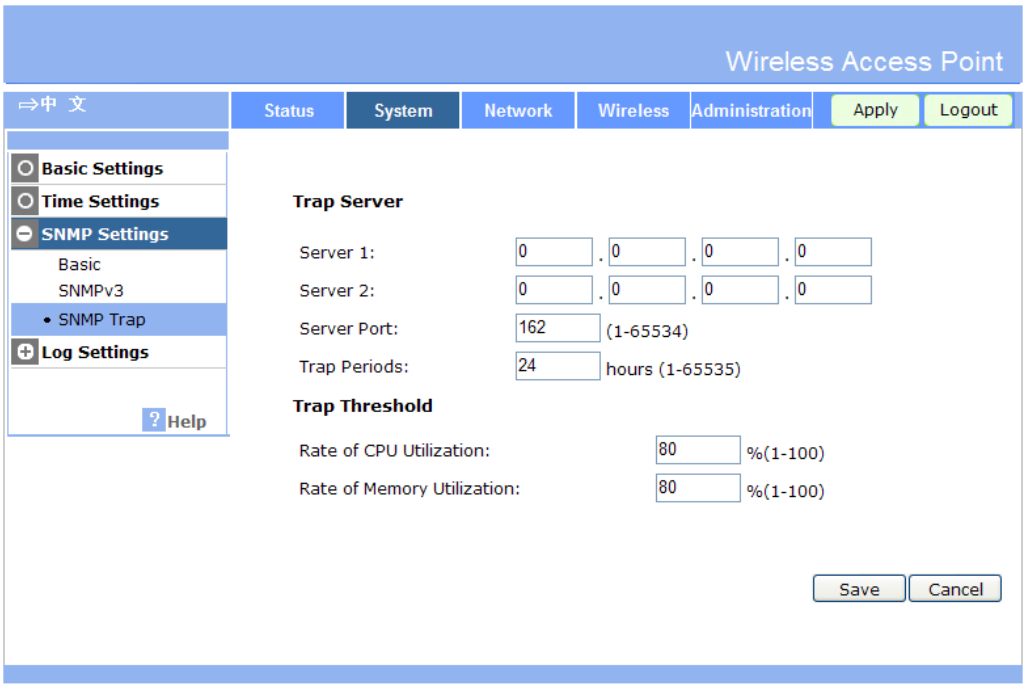

Figure 12: SNMP Trap Screen

Data - SNMP Trap Screen

SNMP Trap	
Server 1	Enter the IP address of the server 1.
Server 2	Enter the IP address of the server 2 in case the server 1 is not available.
Server Port	Enter the port number for the server.
Trap Periods	Enter the desired hours (1 ~ 65535).
Trap Threshold	
Rate of CPU Utilization	When Rate of CPU Utilization reaches the threshold, then one SNMP trap will be sent out.
Rate of Memory Utilization	When Rate of Memory Utilization reaches the threshold, then one SNMP trap will be sent out.

System - Log Settings

If you have a Syslog Server on your LAN, this screen allows you to configure the Access Point to send log data to your Syslog Server.

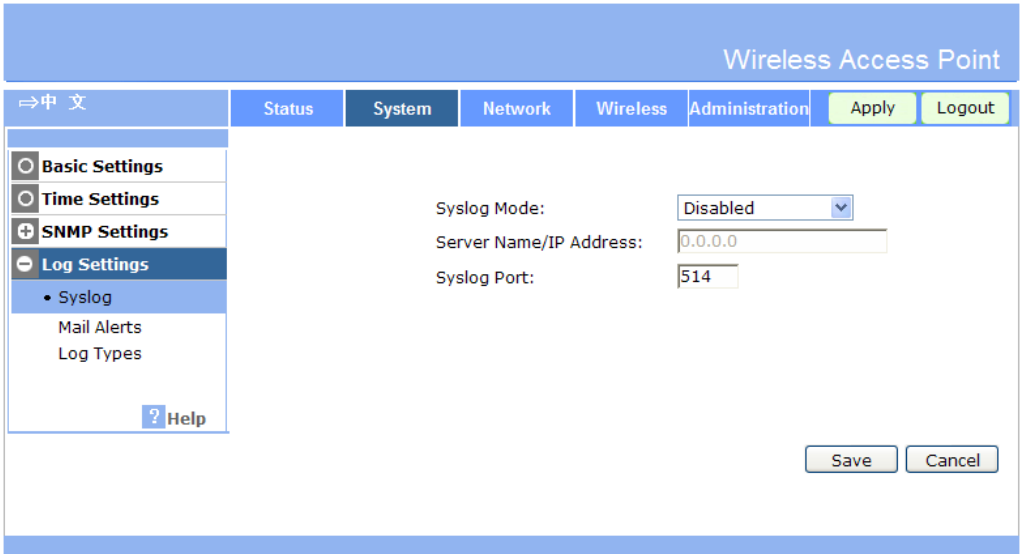

Figure 13: Syslog Settings Screen

Data - Syslog Settings Screen

Syslog Mode	Select the desired Option: • **Disabled** - Syslog server is not used. • **Broadcast** - Syslog data is broadcast. Use this option if different PCs act as the Syslog server at different times. • **Unicast** - Select this if the same PC is always used as the Syslog server. If selected, you must enter the server address in the field provided.
Server Name/IP Address	Enter the name or IP address of your Syslog Server.
Syslog Port	Enter the port for the Syslog Server.

Mail Alerts

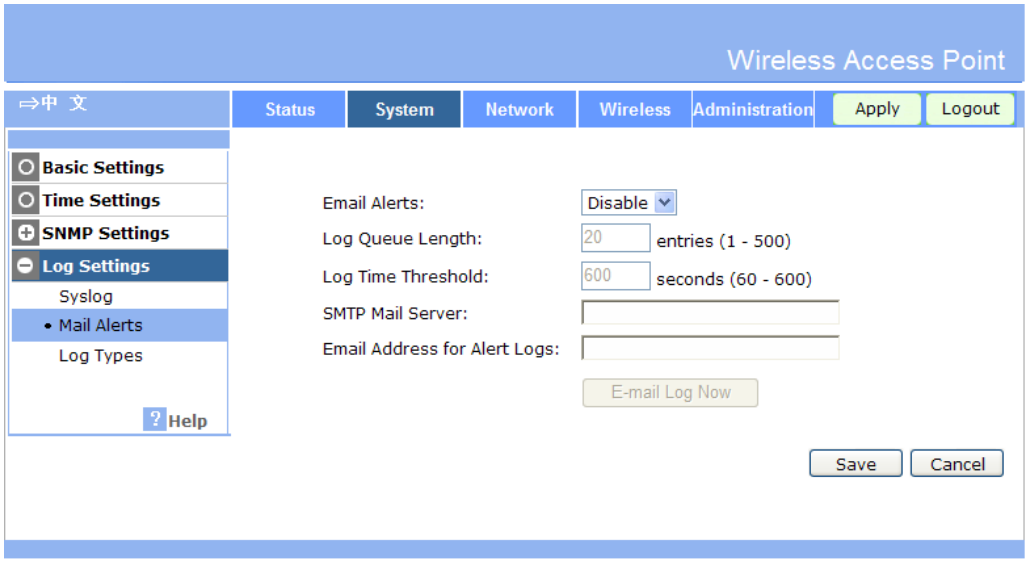

Figure 14: Mail Alerts Screen

Data - Mail Alerts Screen

Email Alerts	
Email Alerts	If enabled, an E-mail will be sent. If enabled, the e-mail address information (below) must be provided.
Log Queue Length	Enter the desired length of the log queue. The default is 20 entries.
Log Time Threshold	Enter the preferred value between 60 and 600, which determine how often the log will be emailed to you. Normally, this can be left at the default value. The default is 600 seconds.
SMTP Mail Server	Enter the domain name or IP address of the SMTP (Simple Mail Transport Protocol) server you use for sending e-mails.
Email Address for Alert Logs	Enter the e-mail address the log is to be sent to.
E-mail Log Now	Press this button to let the log to be e-mailed immediately.

Log Types

Figure 15: Log Types Screen

Data - Log Types Screen

Log Types	
Log Types	Use these checkboxes to determine which events are included in the log. Checking all options will increase the size of the log, so it is good practice to disable any events which are not really required. • **Unauthorized Login Attempt** - If checked, the unauthorized users who attempted to login to the Access Point are logged. • **Authorized Login** - If checked, this will log the authorized login TO this Access Point. • **Unauthorized Wireless Attempt** - If checked, the unauthorized wireless attempted will be login to the Access Point are logged. • **Authorized Wireless Connection** - If checked, this will log the authorized wireless connection to this Access Point. • **System Error Messages** - If checked, the system error message will be logged. • **Web Access and Configuration Changes** - If checked, the changes of configuration will be logged. • **Firewall Log** - If checked, the firewall message will be logged.

Wireless - Basic Settings Screen

The settings on this screen must match the settings used by Wireless Stations.

WLAN

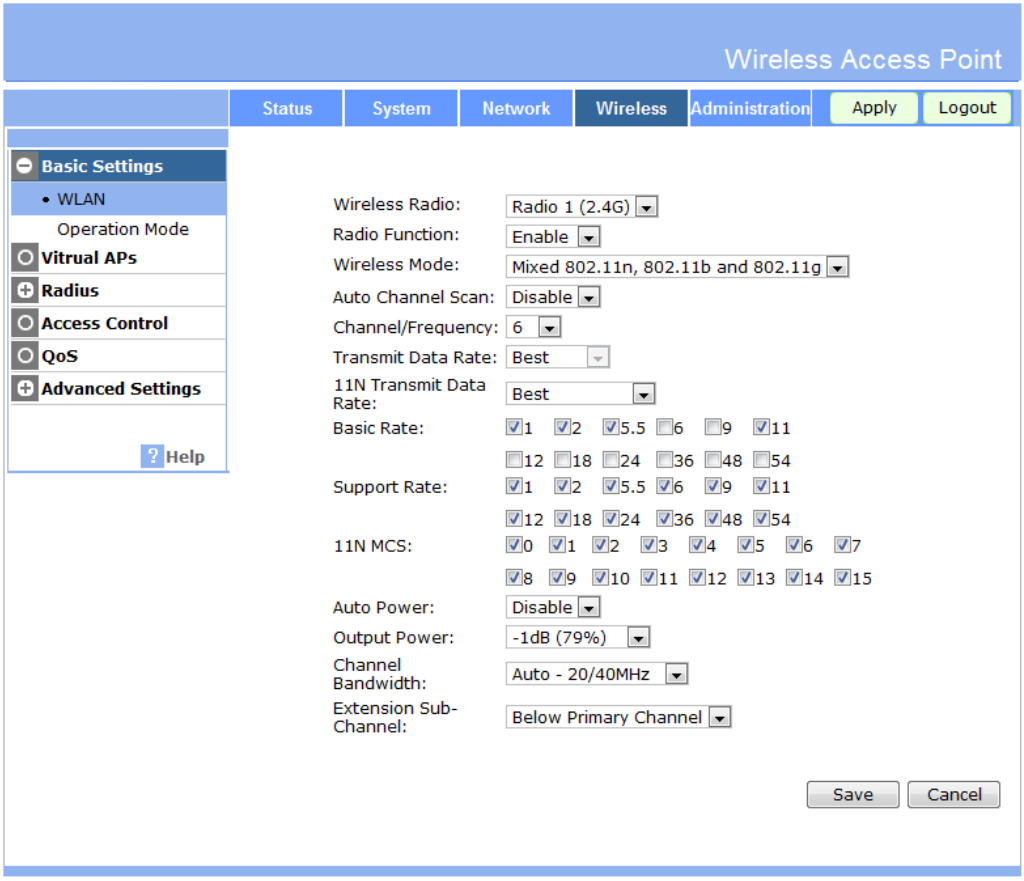

Figure 16: WLAN Settings Screen

Data - WLAN Settings Screen

Operation	
Wireless Radio	Select the either Radio 1 or Radio 2 for the wireless feature.
Radio Function	Enable this to use the wireless feature.

Wireless Mode	For 5G, select the desired option: • **802.11a Only (5G)** - only 802.11a connections are allowed. If you only have 802.11a, selecting this option may provide a performance improvement over using the default setting. • **802.11n Only (5G)** - only 802.11n connections are allowed. If you only have 802.11n, selecting this option may provide a performance improvement over using the default setting. • **802.11a and 802.11n (5G)** - this will allow connections by both 802.11a and 802.11n wireless stations. For 2.4G, select the desired option: • **802.11b only (2.4G)** - if selected, only 802.11b connections are allowed. 802.11g wireless stations will only be able to connect if they are fully backward-compatible with the 802.11b standard. • **802.11g only (2.4G)** - only 802.11g connections are allowed. If you only have 802.11g, selecting this option may provide a performance improvement over using the default setting. • **802.11n only (2.4G)** - only 802.11n connections are allowed. If you only have 802.11n, selecting this option may provide a performance improvement over using the default setting. • **802.11b and 802.11g (2.4G)** - this will allow connections by both 802.11b and 802.11g wireless stations. • **802.11n and 802.11g (2.4G)** - this will allow connections by both 802.11n and 802.11g wireless stations. • **Mixed 802.11n/802.11b/802.11g (2.4G)** - this is the default, and will allow connections by 802.11n, 802.11b and 802.11g wireless stations.
Auto Channel Scan	If "Enable" is selected, the Access Point will select the best available Channel.
Channel /Frequency	If you experience interference (shown by lost connections and/or slow data transfers) you may need to experiment with manually setting different channels to see which one is better.
Transmit Data Rate	Select the desired rate from the drop-down list as required.
11N Transmit Data Rate	Select the desired rate for 802.11N from the list.
Basic Rate	It is the rate that the WAP device will advertise to the network for setting up communication with other access points and client stations on the network.
Support Rate	This indicates the rates that the WAP device supports. Multiple rates can be selected. The WAP device will automatically choose the most efficient rate based on error rates and distance of client stations.
11N MCS	Select the MCS index below. The WAP device supports MCS indexes from 0 to 15, which allows a maximum transmission rate of 300 Mbps.
Auto Power	Select the desired option. The default is Disable.
Output Power	Select the desired power output. Can support -1dB~-15dB, step 1dB. Higher levels will give a greater range, but are also more likely to

	cause interference with other devices.
Channel Bandwidth	Select the desired bandwidth from the list.
Extension Sub-Channel	Select Above or Below Primary Channel from the list.

Operation Mode

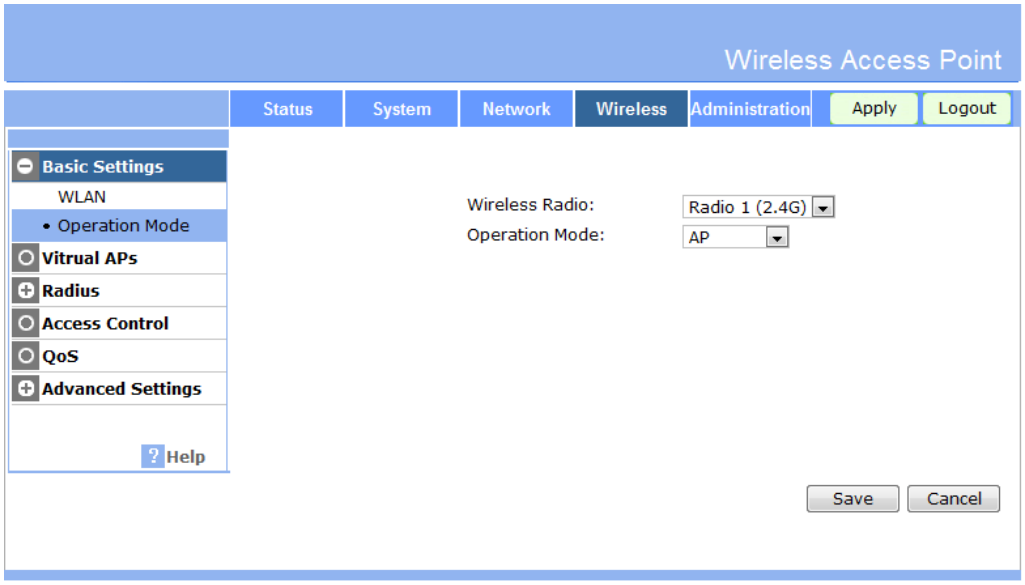

Figure 17: Operation Mode

Data - Operation Mode Settings Screen

Operation	
Wireless Radio	Select the either Radio 1 or Radio 2 for the wireless feature.
Operation Mode	Select the desired option from the list: • AP: Choose this to make the device act as a normal AP. • AP+WDS: Select this mode and make configurations in Vitrual APs pages. In WDS mode, you can choose which interface to be worked as a root AP or WDS client. Select only one interface to be worked as a root AP for the device is recommended. A root AP is the "Master" for a group of Bridge-mode APs. The other Bridge-mode APs must be set to Point-to-Point Bridge mode (WDS Client) with the AP's MAC address.

Wireless - Virtual APs Screen

Clicking the *Virtual APs* link on the Wireless menu will result in a screen like the following.

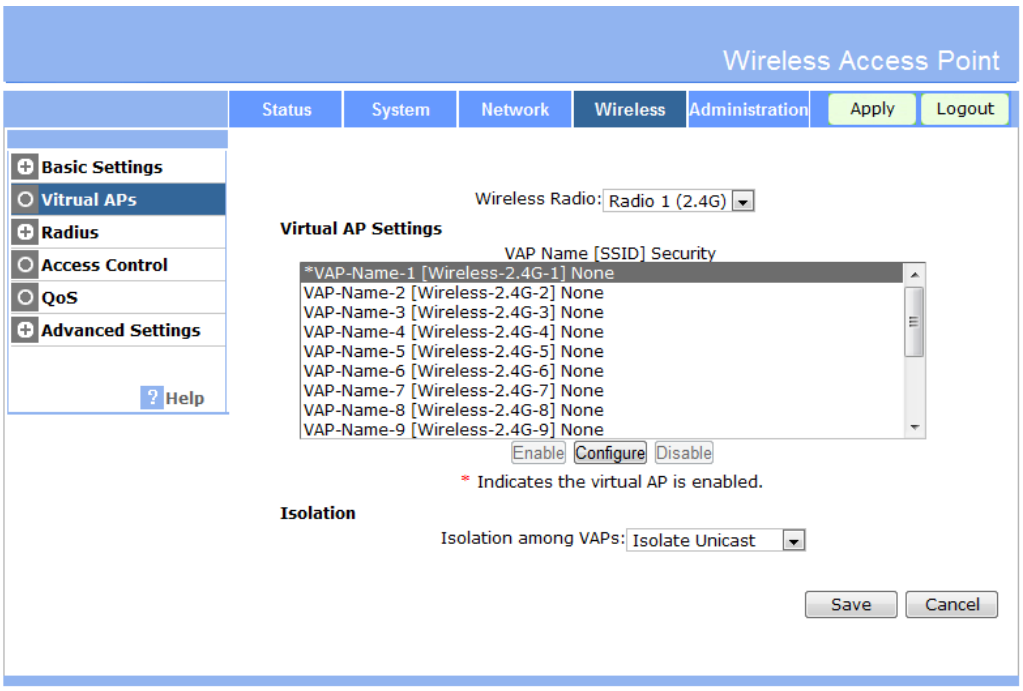

Figure 18: Virtual APs Settings

Data - Virtual APs Settings Screen

VAPs	
Wireless Radio	Select the either Radio 1 or Radio 2 for the wireless feature.
VAP List	All available VAPs are listed. Up to 16 VAPs/Radios can be supported. For each VAP, the following data is displayed: • * If displayed before the name of the VAP, this indicates the VAP is currently enabled. If not displayed, the VAP is currently disabled. • VAP Name The current VAP name is displayed. • [SSID] The current SSID associated with this VAP. • Security System The current security system (e.g. WPA-PSK) is displayed.
Enable Button	Enable the selected VAP.
Configure Button	Change the settings for the selected VAP.
Disable Button	Disable the selected VAP.
Isolation	
Isolation among VAPs	Select the desired option from the list. If this option is enabled, wireless clients using different VAPs (different SSIDs) are isolated from each other, so they will NOT be able to communicate with each other. They will still be able to communicate with other clients using the same profile, unless the "Wireless

	Separation" setting on the "Advanced" screen has been enabled.

Virtual AP Screen

This screen is displayed when you select a VAP on the Virtual AP Settings screen, and click the *Configure* button.

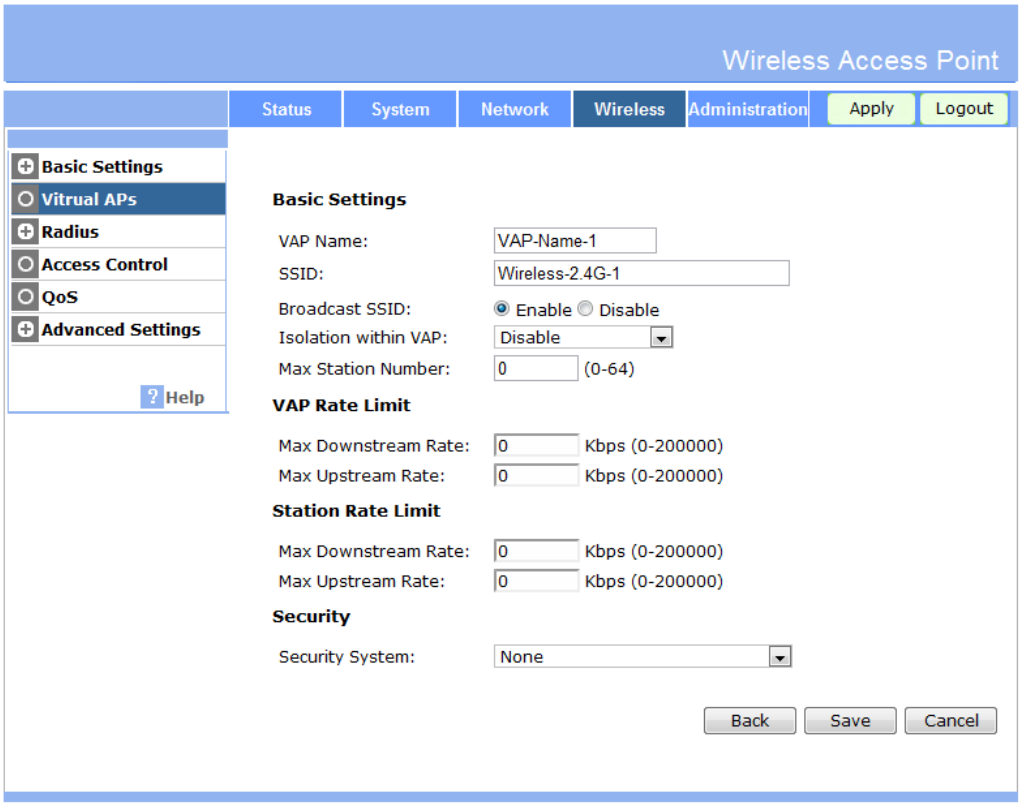

Figure 19: Virtual VAP Screen

Data - Virtual VAP Screen

Basic Settings	
VAP Name	Enter a suitable name for this VAP.
SSID	Enter the desired SSID. Each VAP must have a unique SSID.
Broadcast SSID	If Disabled, no SSID is broadcast. If enabled, the SSID will then be broadcast to all Wireless Stations. Stations which have no SSID (or a "null" value) can then adopt the correct SSID for connections to this Access Point.
Isolation within VAP	If enabled, then each Wireless station using the Access Point is invisible to other Wireless stations. In most business stations, this setting should be Disabled.
Max Station Number	Enter the number between 0 and 64.
VAP Rate Limit	
Max Downstream Rate	Enter the maximum downstream rate for the VAP. "0" means no limit.

Max Upstream Rate	Enter the maximum upstream rate for the VAP. "0" means no limit.
Station Rate Limit	
Max Downstream Rate	Enter the maximum downstream rate for each wireless station. "0" means no limit.
Max Upstream Rate	Enter the maximum upstream rate for each wireless station. "0" means no limit.
Security	
Security System	Choose the security method from the drop-down list. Refer to the following section for more details.

Security Settings

Select the desired option, and then enter the settings for the selected method.

The available options are:

- **None** - No security is used. Anyone using the correct SSID can connect to your network.
- **WEP** - The 802.11b standard. Data is encrypted before transmission, but the encryption system is not very strong.
- **WPA-PSK** - Like WEP, data is encrypted before transmission. WPA is more secure than WEP, and should be used if possible. The PSK (Pre-shared Key) must be entered on each Wireless station. The 256Bit encryption key is derived from the PSK, and changes frequently.
- **WPA2-PSK** - This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption.
- **WPA-PSK and WPA2-PSK** - This method, sometimes called "Mixed Mode", allows clients to use EITHER WPA-PSK (with TKIP) OR WPA2-PSK (with AES).
- **WPA with Radius** - This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard.

  If this option is selected:

  - This Access Point must have a "client login" on the Radius Server.
  - Each user must have a "user login" on the Radius Server.
  - Each user's wireless client must support 802.1x and provide the login data when required.
  - All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required.
- **WPA2 with Radius** - This version of WPA2 requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA2 standard.

  If this option is selected:

  - This Access Point must have a "client login" on the Radius Server.
  - Each user must authenticate on the Radius Server. This is usually done using digital certificates.
  - Each user's wireless client must support 802.1x and provide the Radius authentication data when required.

- All data transmission is encrypted using the WPA2 standard. Keys are automatically generated, so no key input is required.

- **WPA and WPA2 with Radius** - EITHER WPA or WPA2 require a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using EITHER WPA or WPA2 standard.

  If this option is selected:

  - This Access Point must have a "client login" on the Radius Server.
  - Each user must authenticate on the Radius Server. This is usually done using digital certificates.
  - Each user's wireless client must support 802.1x and provide the Radius authentication data when required.
  - All data transmission is encrypted using EITHER WPA or WPA2 standard. Keys are automatically generated, so no key input is required.

- **802.1x** - This uses the 802.1x standard for client authentication, and WEP for data encryption.

  If this option is selected:

  - This Access Point must have a "client login" on the Radius Server.
  - Each user must have a "user login" on the Radius Server.
  - Each user's wireless client must support 802.1x and provide the login data when required.
  - All data transmission is encrypted using the WEP standard. You only have to select the WEP key size; the WEP key is automatically generated.

Security Settings - None

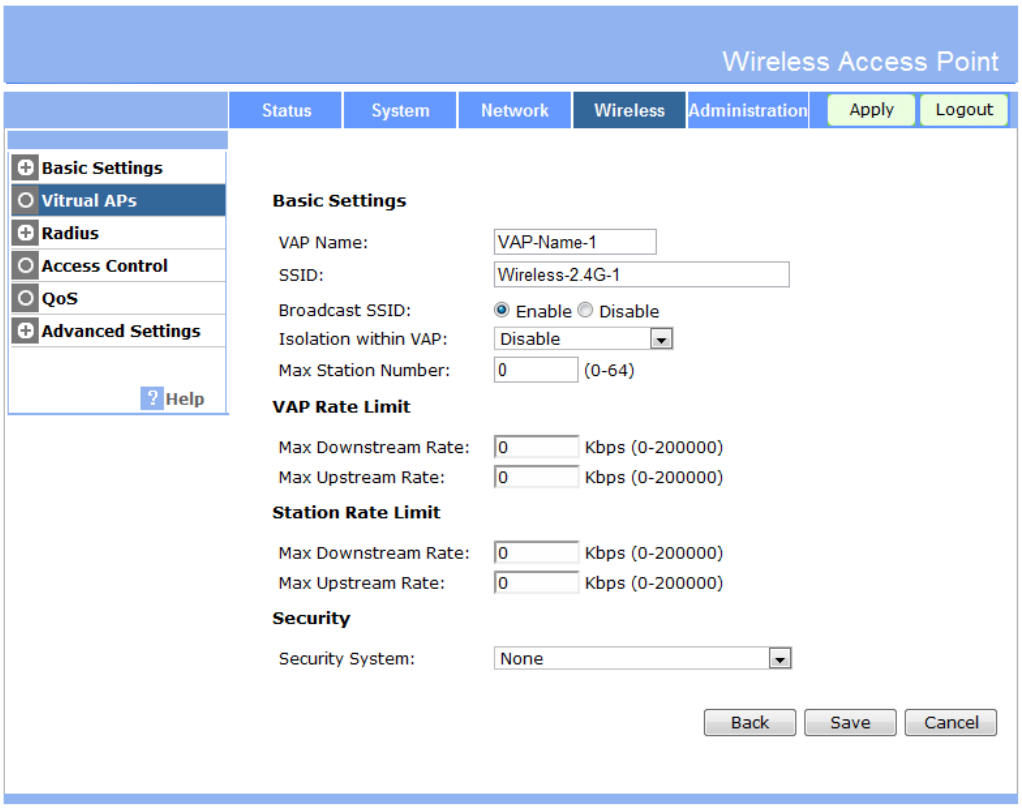

Figure 20: Wireless Security - None

No security is used. Anyone using the correct SSID can connect to your network.

Security Settings - WEP

This is the 802.11b standard. Data is encrypted before transmission, but the encryption system is not very strong.

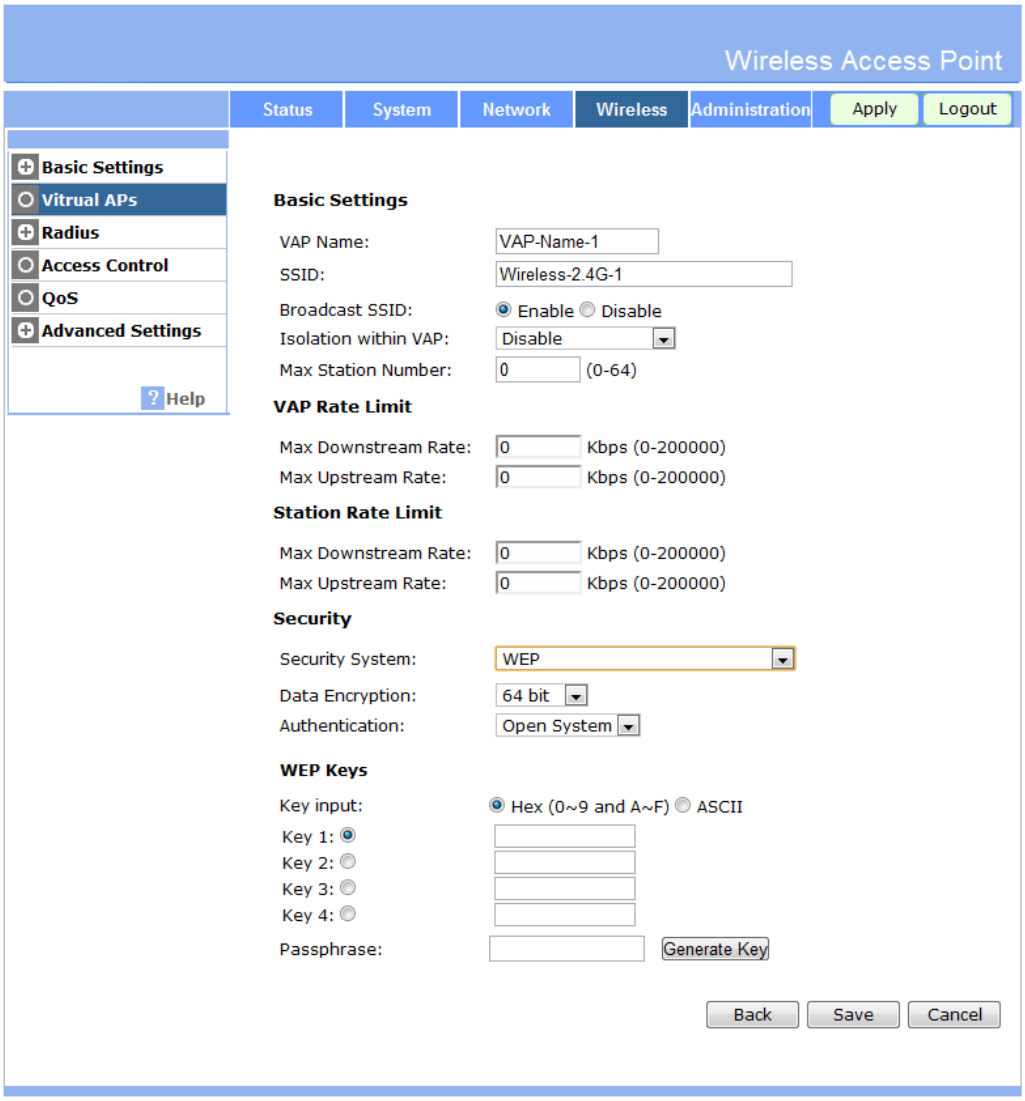

Figure 21: WEP Screen

Data - WEP Screen

WEP	
Data Encryption	Select the desired option, and ensure your Wireless stations have the same setting: • **64 Bit Encryption** - Keys are 10 Hex (5 ASCII) characters. • **128 Bit Encryption** - Keys are 26 Hex (13 ASCII) characters. • **152 Bit Encryption** - Keys are 32 Hex (16 ASCII) characters.

Authentication	Normally, you can leave this at “Automatic”, so that Wireless Stations can use either method ("Open System" or "Shared Key".). If you wish to use a particular method, select the appropriate value - "Open System" or "Shared Key". All Wireless stations must then be set to use the same method.
Key Input	Select "Hex" or "ASCII" depending on your input method. (All keys are converted to Hex, ASCII input is only for convenience.)
Key Value	Enter the key values you wish to use. The default key, selected by the radio button, is required. The other keys are optional. Other stations must have matching key values.
Passphrase	Use this to generate a key or keys, instead of entering them directly. Enter a word or group of printable characters in the Passphrase box and click the "Generate Key" button to automatically configure the WEP Key(s).

Security Settings - WPA-PSK

Like WEP, data is encrypted before transmission. WPA is more secure than WEP, and should be used if possible. The PSK (Pre-shared Key) must be entered on each Wireless station. The 256Bit encryption key is derived from the PSK, and changes frequently.

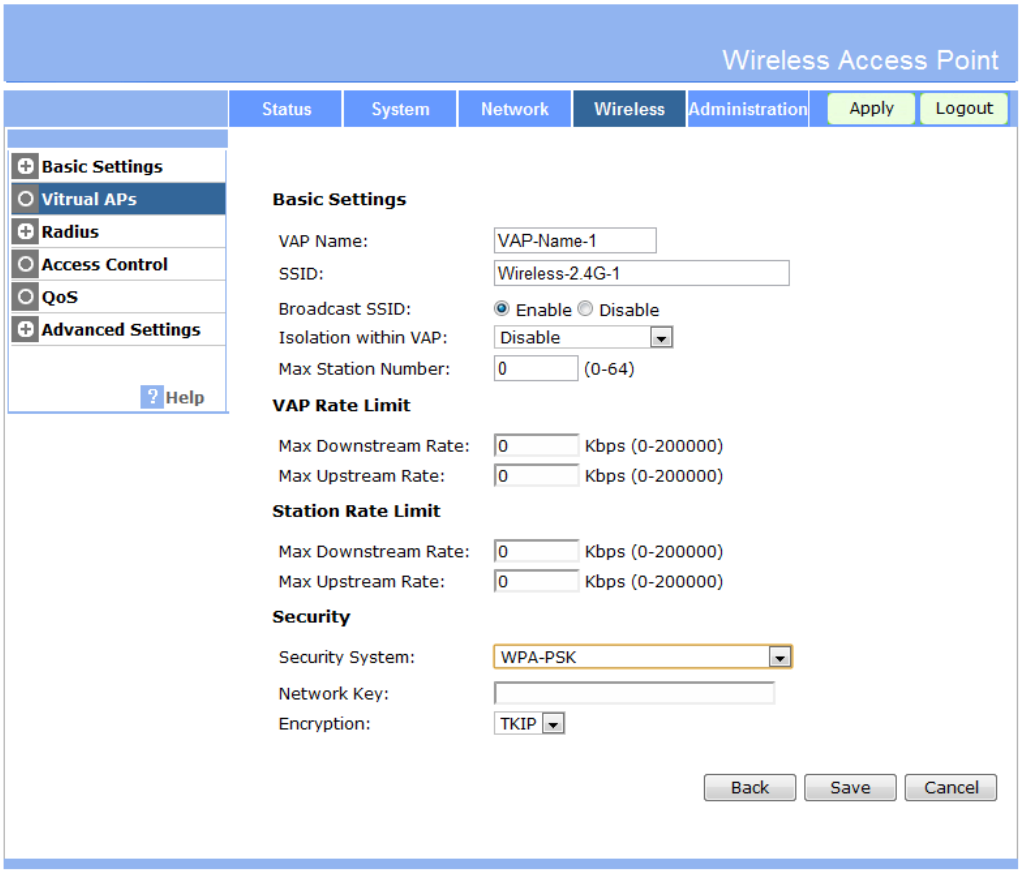

Figure 22: WPA-PSK Screen

Data - WPA-PSK Screen

WPA-PSK	
Network Key	Enter the key value. Data is encrypted using a 256Bit key derived from this key. Other Wireless Stations must use the same key.
Encryption	The encryption method is TKIP. Wireless Stations must also use TKIP.

Security Settings - WPA2-PSK

This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption.

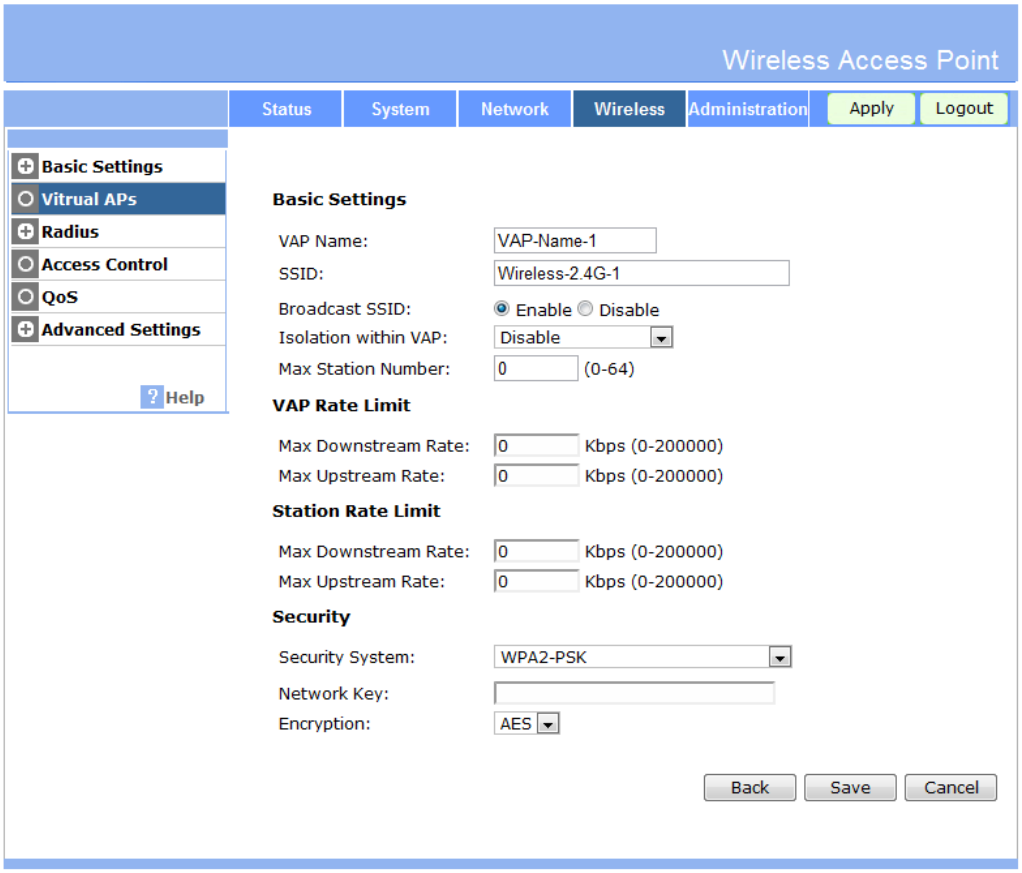

Figure 23: WPA2-PSK Screen

Data - WPA2-PSK Screen

WPA2-PSK	
Network Key	Enter the key value. Data is encrypted using a 256Bit key derived from this key. Other Wireless Stations must use the same key.
Encryption	The encryption method is AES. Wireless Stations must also use AES.

Security Settings - WPA-PSK and WPA2-PSK

This method, sometimes called "Mixed Mode", allows clients to use EITHER WPA-PSK (with TKIP) OR WPA2-PSK (with AES).

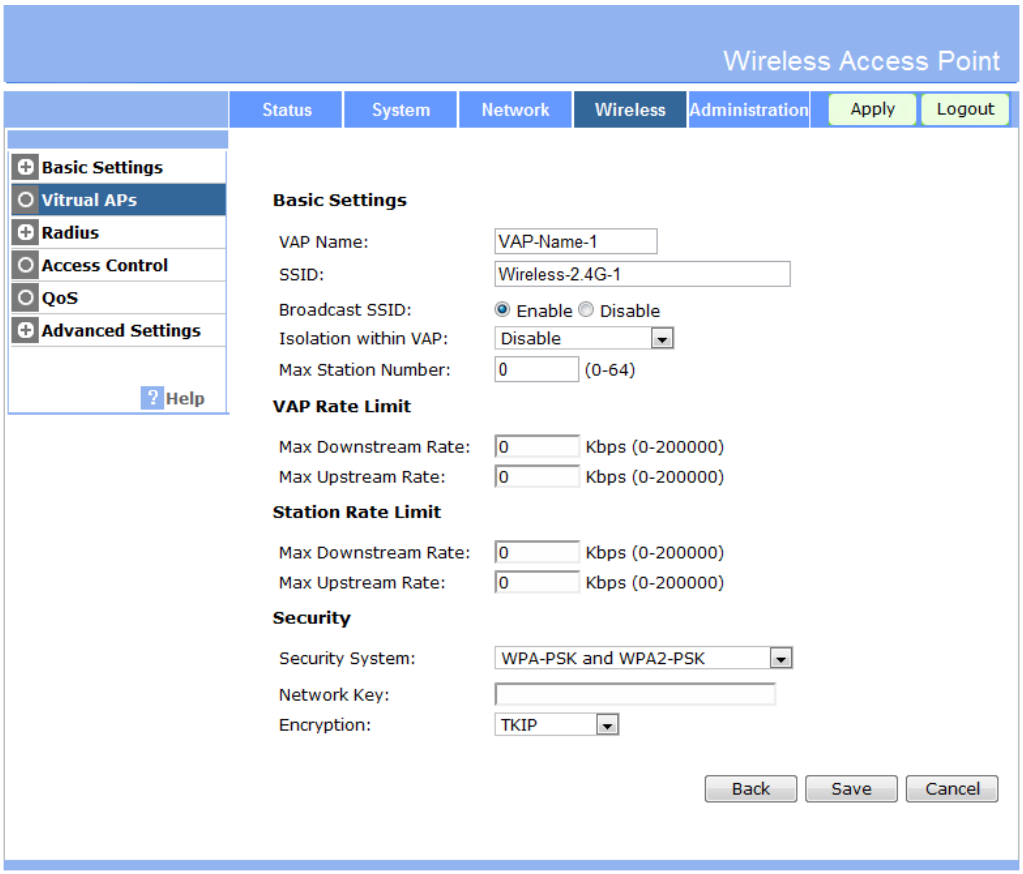

Figure 24: WPA-PSK and WPA2-PSK Screen

Data - WPA-PSK and WPA2-PSK Screen

WPA-PSK and WPA2-PSK	
Network Key	Enter the key value. Data is encrypted using this key. Other Wireless Stations must use the same key.
Encryption	Select the desired encryption method from the list.

Security Settings - WPA with Radius

This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard.

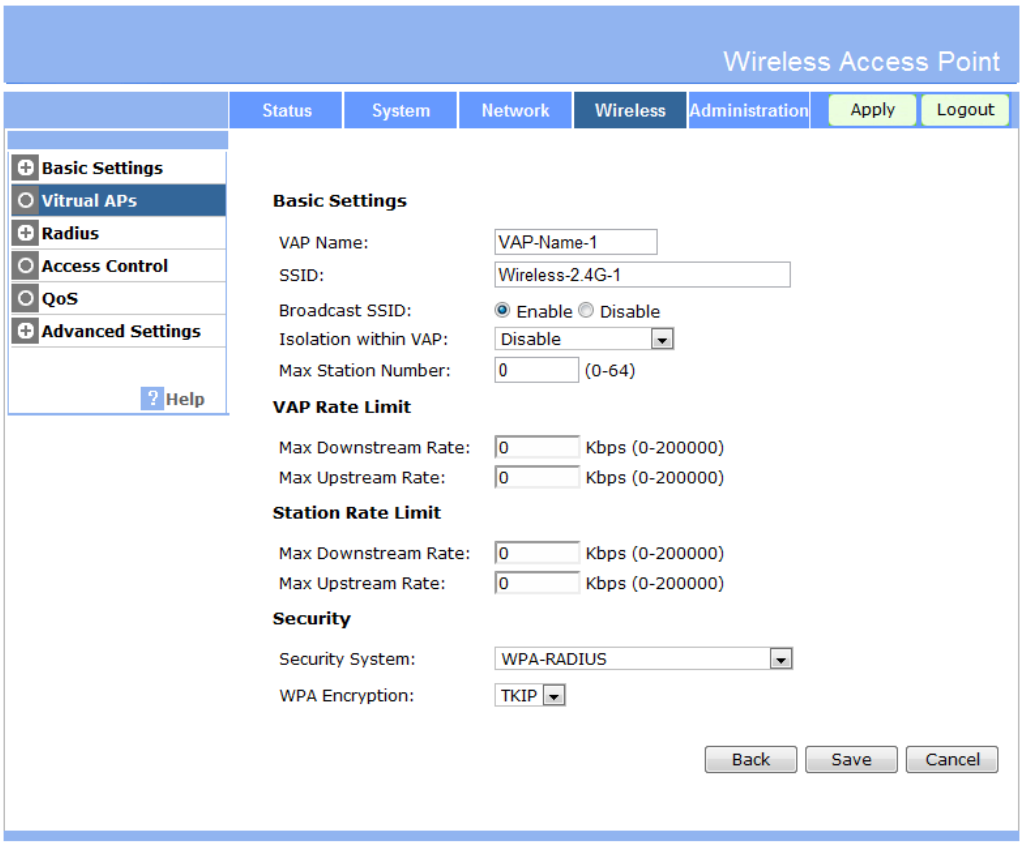

Figure 25: WPA with Radius Screen

Data - WPA with Radius Screen

WPA with Radius	
WPA Encryption	The encryption method is TKIP. Wireless Stations must also use TKIP.

Security Settings - WPA2 with Radius

This version of WPA2 requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA2 standard.

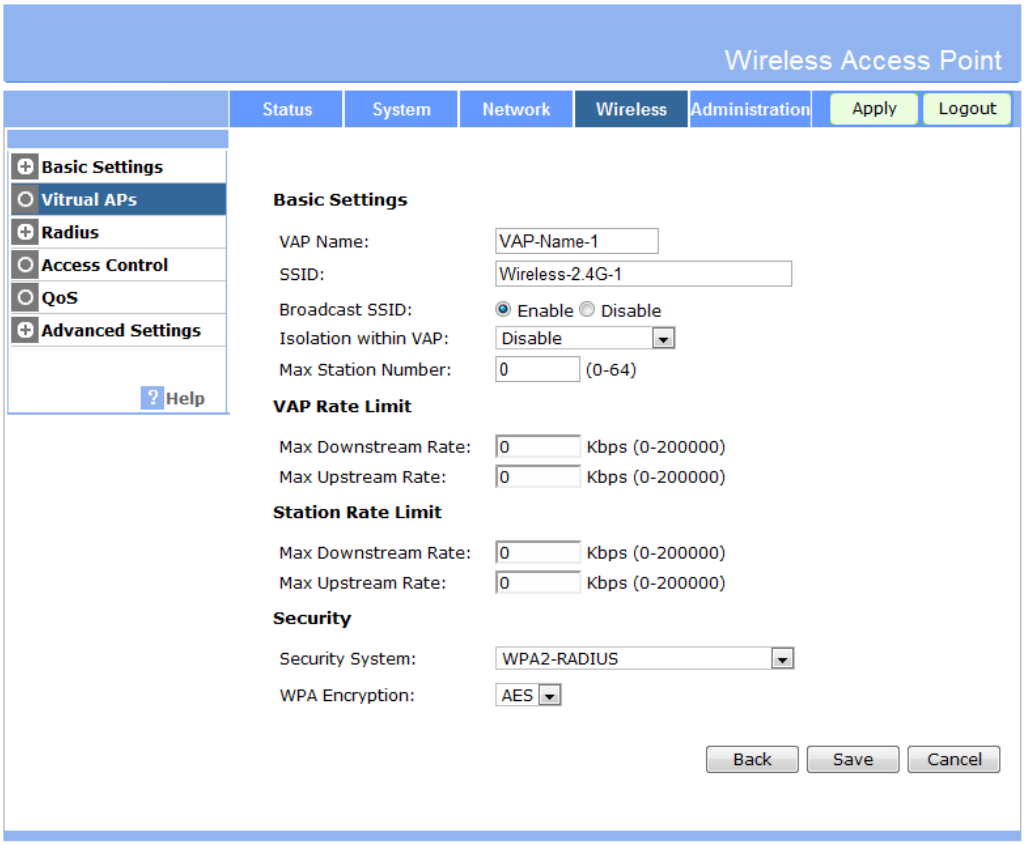

Figure 26: WPA2 with Radius Screen

Data - WPA2 with Radius Screen

WPA2 with Radius	
WPA Encryption	The encryption method is AES. Wireless Stations must also use AES.

Security Settings - WPA and WPA2 with Radius

EITHER WPA or WPA2 require a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using EITHER WPA or WPA2 standard.

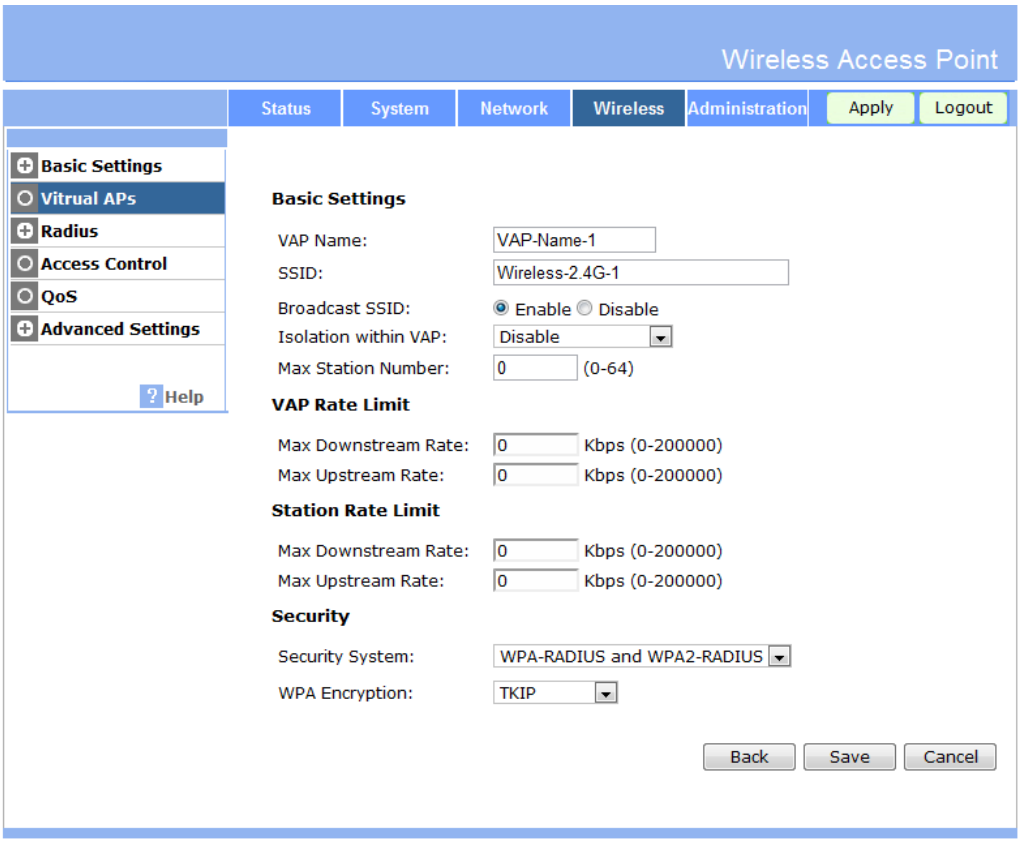

Figure 27: WPA and WPA2 with Radius Screen

Data - WPA and WPA2 with Radius Screen

WPA and WPA2 with Radius	
WPA Encryption	Select the desired encryption method from the list.

Security Settings - 802.1x

This uses the 802.1x standard for client authentication, and WEP for data encryption. If this option is selected:

- This Access Point must have a "client login" on the Radius Server.
- Each user must have a "user login" on the Radius Server. Normally, a Certificate is used to authenticate each user. See Chapter4 for details of user configuration.
- Each user's wireless client must support 802.1x.
- All data transmission is encrypted using the WEP standard. You only have to select the WEP key size; the WEP key is automatically generated.

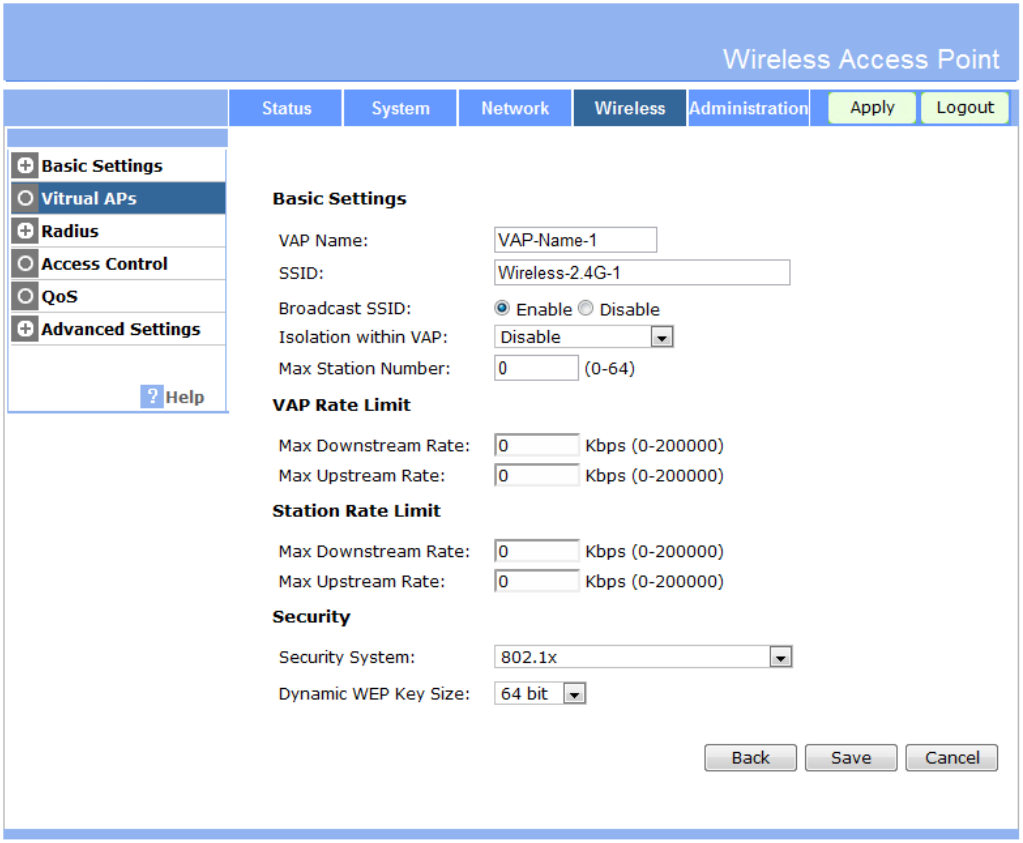

Figure 28: 802.1x Screen

Data - 802.1x Screen

802.1x	
Dynamic WEP Key Size	Select the desired option: • **64 Bit** - Keys are 10 Hex (5 ASCII) characters. • **128 Bit** - Keys are 26 Hex (13 ASCII) characters. • **152 Bit** - Keys are 32 Hex (16 ASCII) characters.

Wireless - Radius Settings

Clicking the *Radius* link on the Wireless menu will result in a screen like the following.

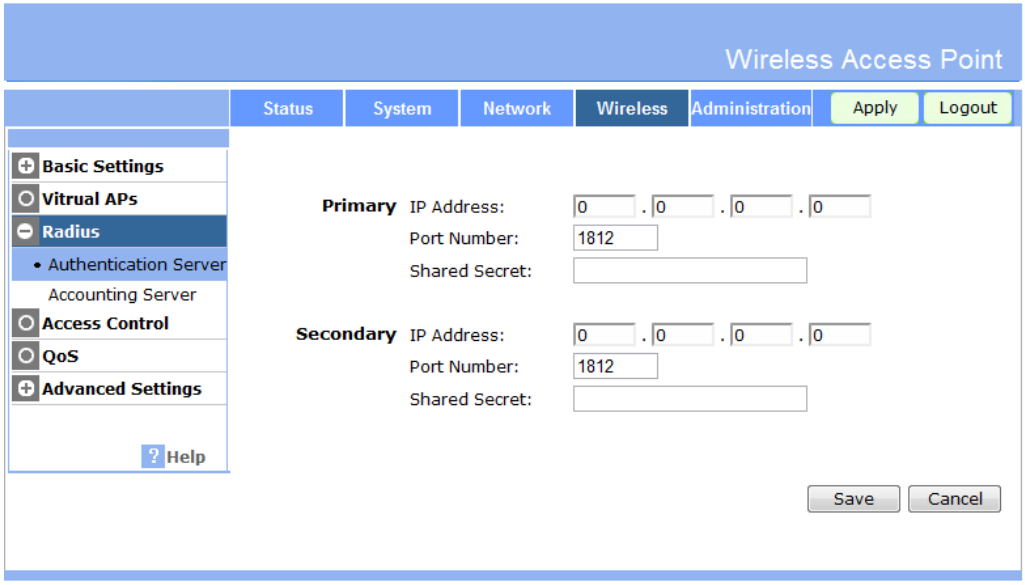

Figure 29: Authentication Server Settings

Data - Authentication Server Screen

Authentication Server	
Primary IP Address	Enter the name or IP address of the Radius Server on your network.
Port Number	Enter the port number used for connections to the Radius Server.
Shared Secret	Enter the key value to match the Radius Server.
Secondary IP Address	The Secondary Authentication Server will be used when the Primary Authentication Server is not available.

Accounting Server

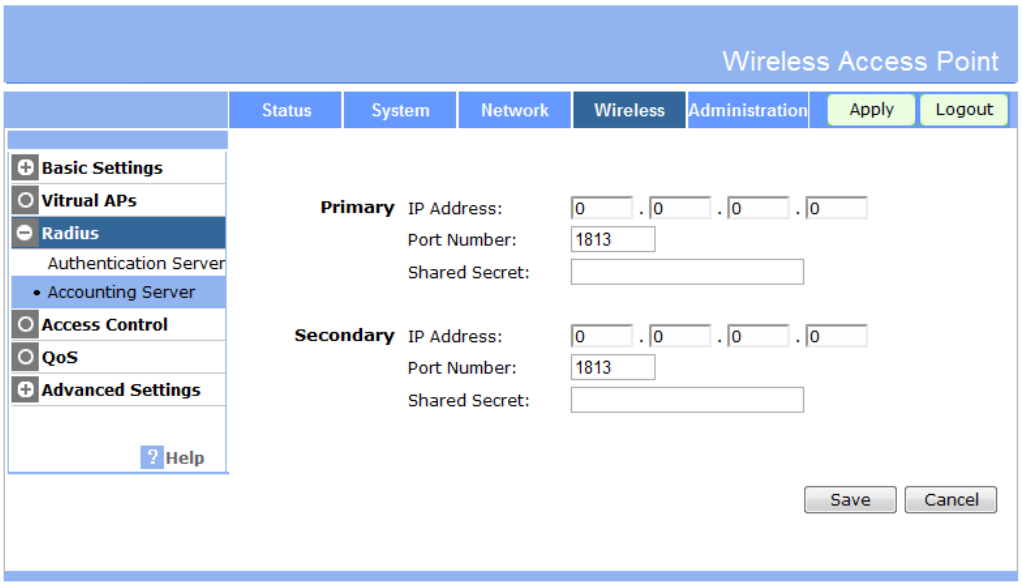

Figure 30: Accounting Server Screen

Data - Accounting Server Screen

Accounting Server	
Primary IP Address	Enter the IP address in the following fields if you want this Access Point to send accounting data to the Radius Server.
Port Number	The port used by your Radius Server must be entered in the field.
Shared Secret	Enter the key value to match the Radius Server.
Secondary IP Address	The Secondary Accounting Server will be used when the Primary Accounting Server is not available.

Wireless - Access Control

This feature can be used to block access to your LAN by unknown or untrusted wireless stations.

Click *Access Control* on the Wireless menu to view a screen like the following.

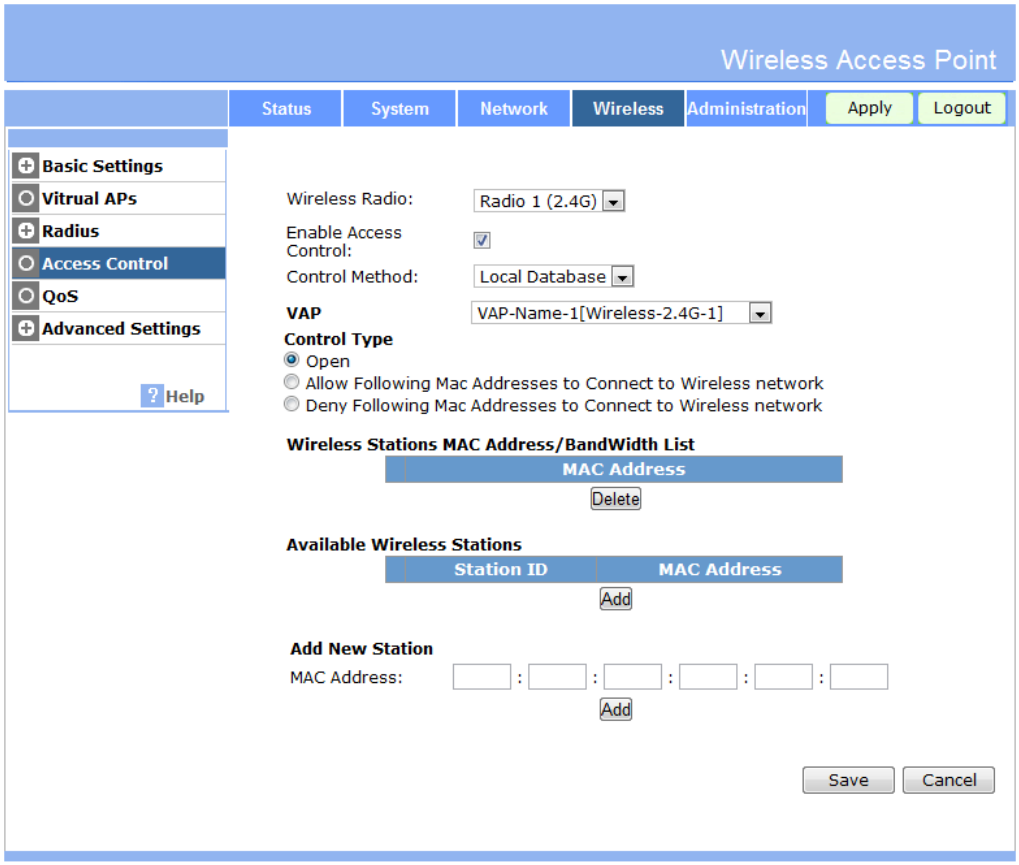

Figure 31: Access Control Screen

Data - Access Control Screen

Wireless Radio	Select the either Radio 1 or Radio 2 for the wireless feature.
Enable Access Control	Enable or Disable the Access Control feature as required.
Control Method	Select the desired option, as required • **Local Database**- The device will use the local MAC address table for Access Control. • **RADIUS Server**- The Access Point will use the MAC address table located on the external Radius server on the LAN for Access Control. **Warning !** Ensure your own PC is in the "Trusted Wireless Stations" list before enabling this feature.

Control Type	There are three options: • **Open** • **Allow Following MAC Addresses to Connect to Wireless network** - It's only used for Access Control with Local Database. If selected, then clients with MAC Addresses in Local Database can connect to the wireless network. • **Deny Following MAC Addresses to Connect to Wireless network** - It's only used for Access Control with Local Database. If selected, then clients with MAC Addresses in Local Database cannot connect to the wireless network.
Wireless Stations MAC Address List	All Wireless Stations defined in Local Database are listed here. Use the "Delete" button to delete the items from the list.
Available Wireless Stations	All Wireless Stations connecting to the device are listed here. You can choose some stations from the list and click "Add" button to add them into Local Database.

Wireless - QoS Settings

QoS Screen

Clicking the *QoS* link on the Wireless menu will result in a screen like the following.

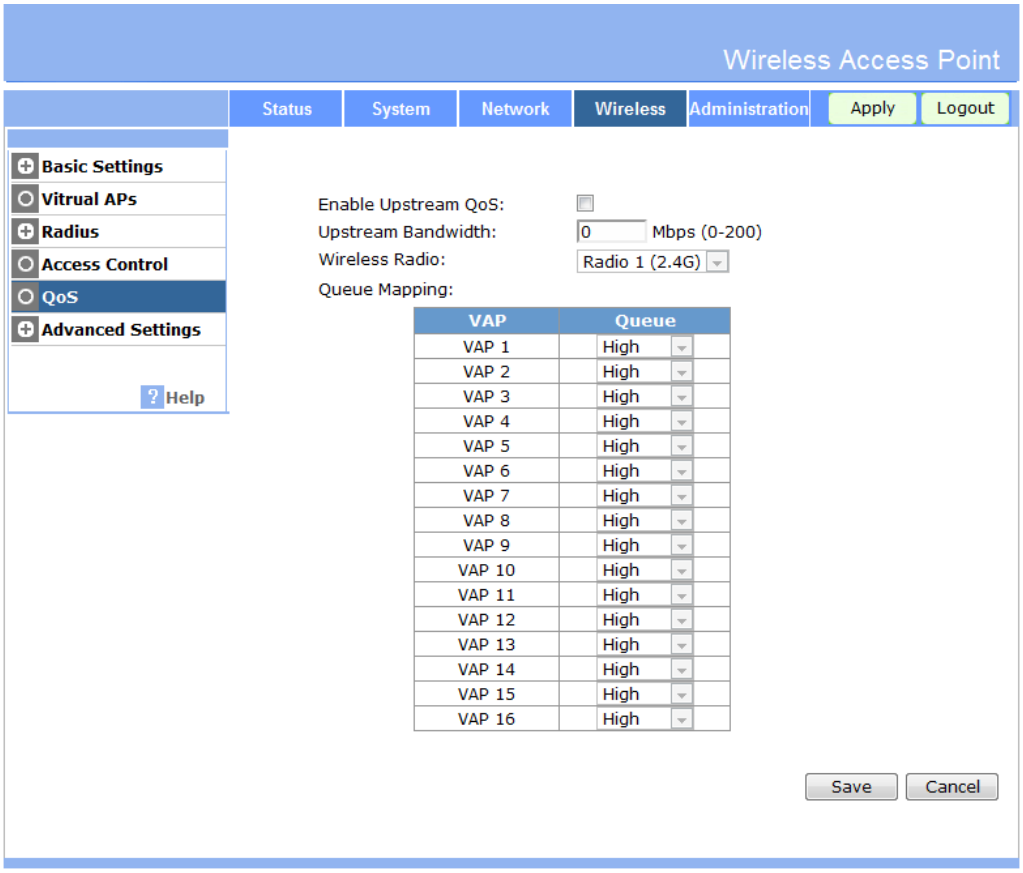

Figure 32: QoS Screen

Data - QoS Screen

Parameters	
Enable Upstream QoS	Enable or Disable upstream QoS of Ethernet Port. The QoS includes four outbound priority queues. The packets from high priority queue will be processed first.
Upstream Bandwidth	Specify the maximum upstream bandwidth of the AP.
Wireless Radio	Select the desired radio to configure the queue mappings.
Queue Mapping	Define the mapping for the queues.

Wireless - Advanced Settings

Parameters Screen

Clicking the *Parameters* link on the Wireless menu will result in a screen like the following.

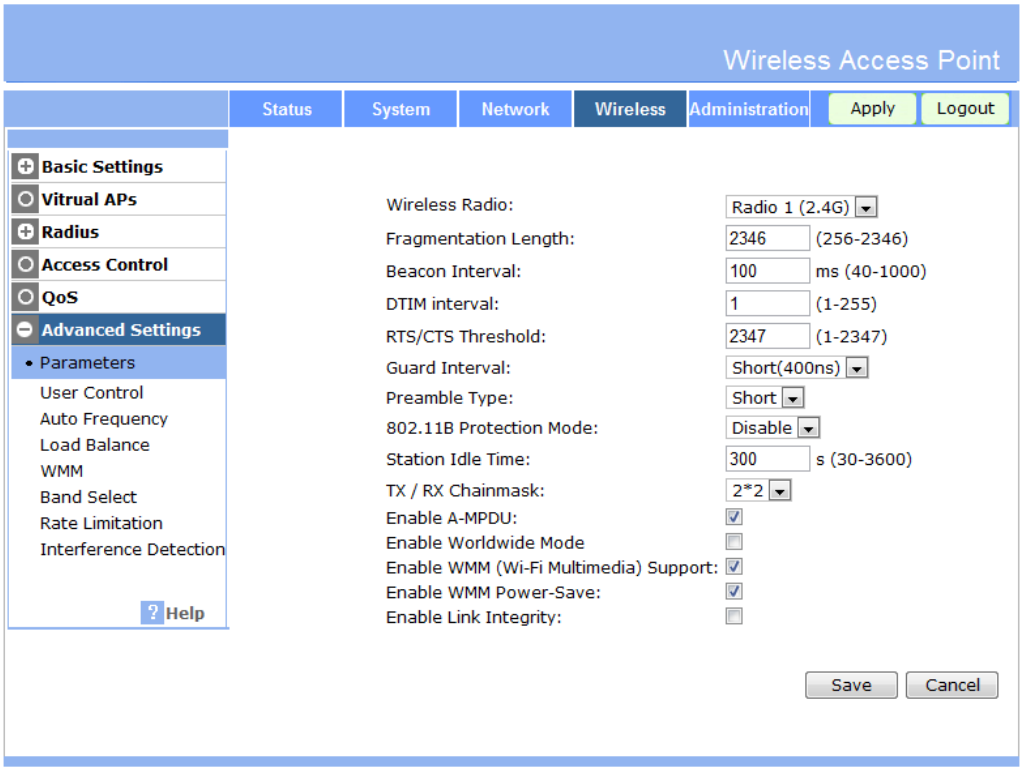

Figure 33: Parameters Screen

Data - Parameters Screen

Parameters	
Wireless Radio	Select the either Radio 1 or Radio 2 for the wireless feature.
Fragmentation Length	Enter the preferred setting between 256 and 2346. Normally, this can be left at the default value.
Beacon Interval	Enter the preferred setting between 20 and 1000. Normally, this can be left at the default value.
DTIM Interval	Enter the preferred setting between 1 and 255. Normally, this can be left at the default value.
RTS/CTS Threshold	Enter the preferred setting between 1 and 2347. Normally, this can be left at the default value.
Guard Interval	Select the guard interval manually for Wireless-N connections. The two options are Short (400ns) and Long (800ns).
Preamble Type	Select the desired option. The default is "Long". The "Short" setting takes less time when used in a good environment.

802.11b Protection Mode	The Protection system is intended to prevent older 802.11b devices from interfering with 802.11g transmissions. (Older 802.11b devices may not be able to detect that the 802.11g transmission is in progress.)
Station Idle Time	This indicates the time (seconds) of the station whose node will be deleted from AP if there is no traffic for the link.
TX/RX Chainmask	Select the desired TX/RX chainmask.
Enable A-MPDU	Enable this setting if you wish to use this feature.
Enable Worldwide Mode	Enable this setting if you want to use this mode, and your Wireless stations also support this mode.
Enable WMM (Wi-Fi Multimedia) Support	Check this to enable WMM (Wi-Fi Multimedia) support in the Access Point. If WMM is also supported by your wireless clients, voice and multimedia traffic will be given a higher priority than other traffic.
Enable WMM Power-Save	Enable or Disable WMM Power-Save feature.
Enable Link Integrity	If enabled, the device can detect the plugging or unplugging of the Ethernet cable and start/stop the related services correspondingly.

User Control Screen

Click *User Control* on the Wireless menu to view a screen like the following:

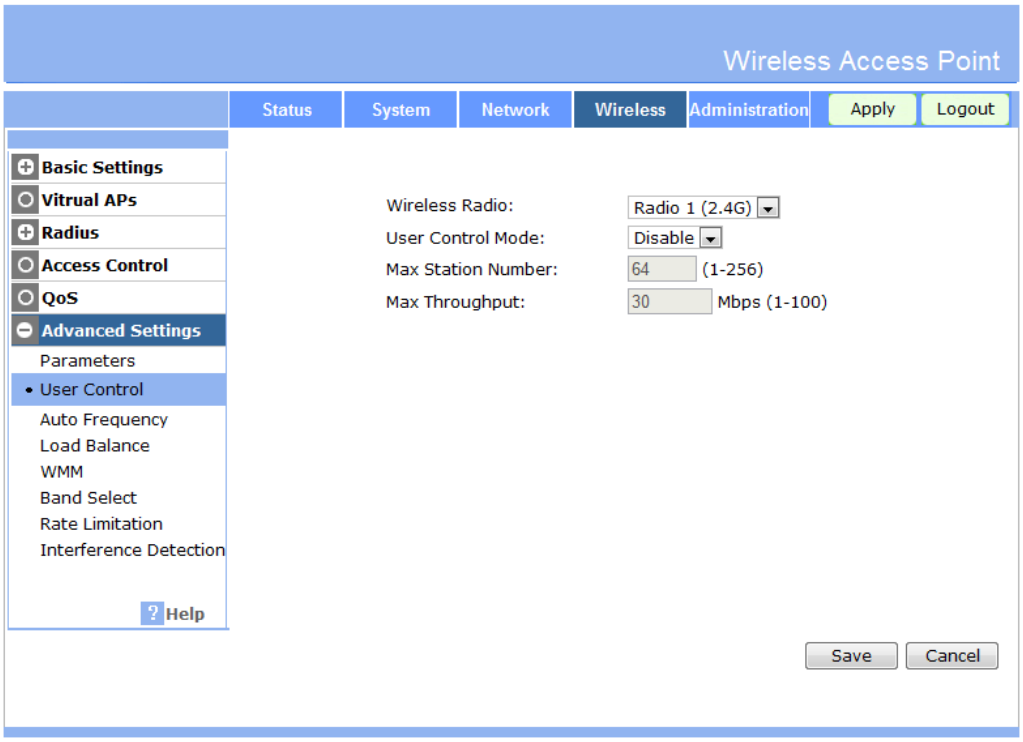

Figure 34: User Control Screen

Data - User Control Screen

User Control	
Wireless Radio	Select the either Radio 1 or Radio 2 for the wireless feature.
User Control Mode	Select the method of controlling the Wireless Stations. It can be one of following options: • Disable - This function is disabled. • Users - In this mode, number of Wireless Stations that can connect this device is limited to the specified value. • Flux - In this mode, if total throughput of the device reaches the specified value, the Wireless Stations will refuse to connect the device.
Max Station Number	Enter the maximum number (1~256) of wireless stations connecting to the device.
Max Throughput	Enter the desired number between 1 and 100 for the maximum throughput.

Auto Frequency Screen

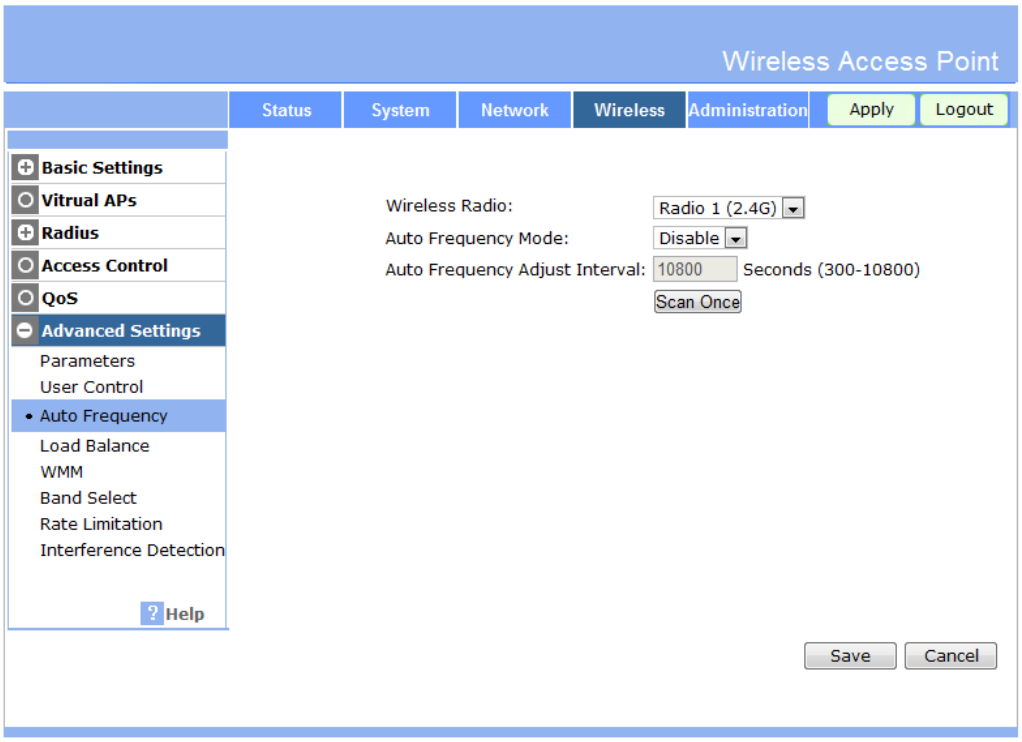

Figure 35: Auto Frequency Screen

Data - Auto Frequency Screen

Auto Frequency	
Wireless Radio	Select the either Radio 1 or Radio 2 for the wireless feature.
Auto Frequency Mode	If enabled, the device can adjust its wireless channel at a specified interval.
Auto Frequency Adjust Interval	Specify the interval at which the device will scan and adjust its wireless channel.

Load Balance Screen

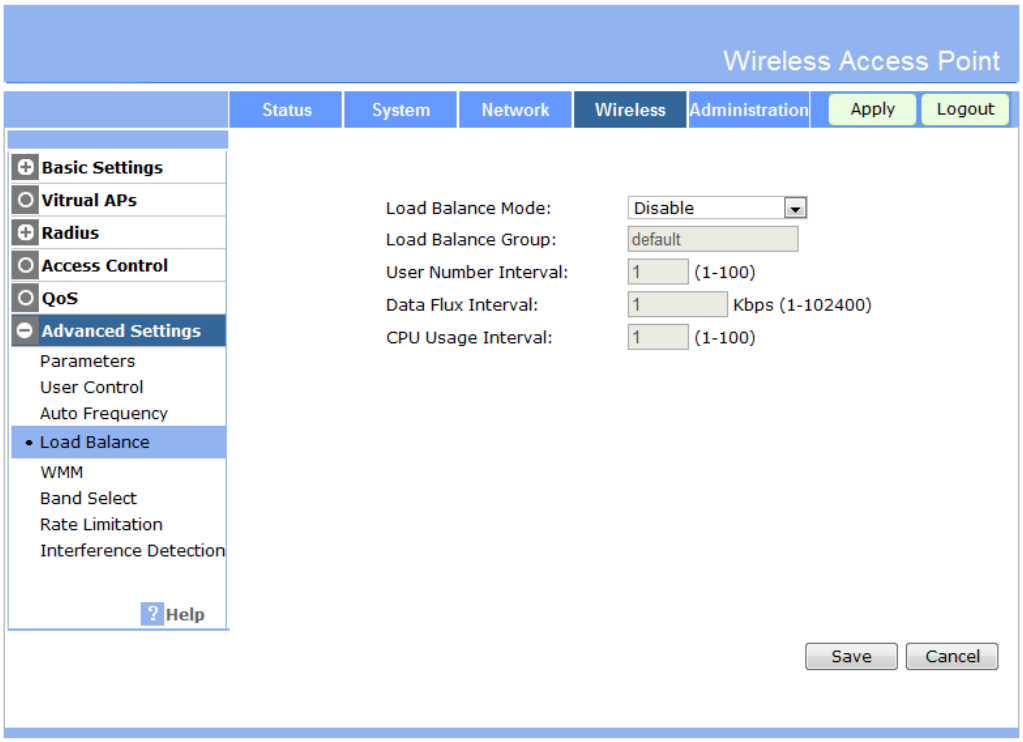

Figure 36: Load Balance Screen

Data - Load Balance Screen

Load Balance	
Load Balance Mode	Enable or disable this function.
Load Balance Group	Specify the group name. The feature will only work with the Access Points that are in same group.
User Number Interval	Specify the User Number Interval. When user number difference of Access Points reaches the interval, the new client will connect to the Access Point with fewer users.
Data Flux Interval	Specify the Data Flux Interval here. When data flux difference of Access Points reach the interval, the new client will connect to the Access Point with fewer data flow.
CPU Usage Interval	Specify the CPU Usage Interval. When CPU usage difference of Access Points reaches the interval, the new client will connect to the Access Point with fewer users.

WMM Screen

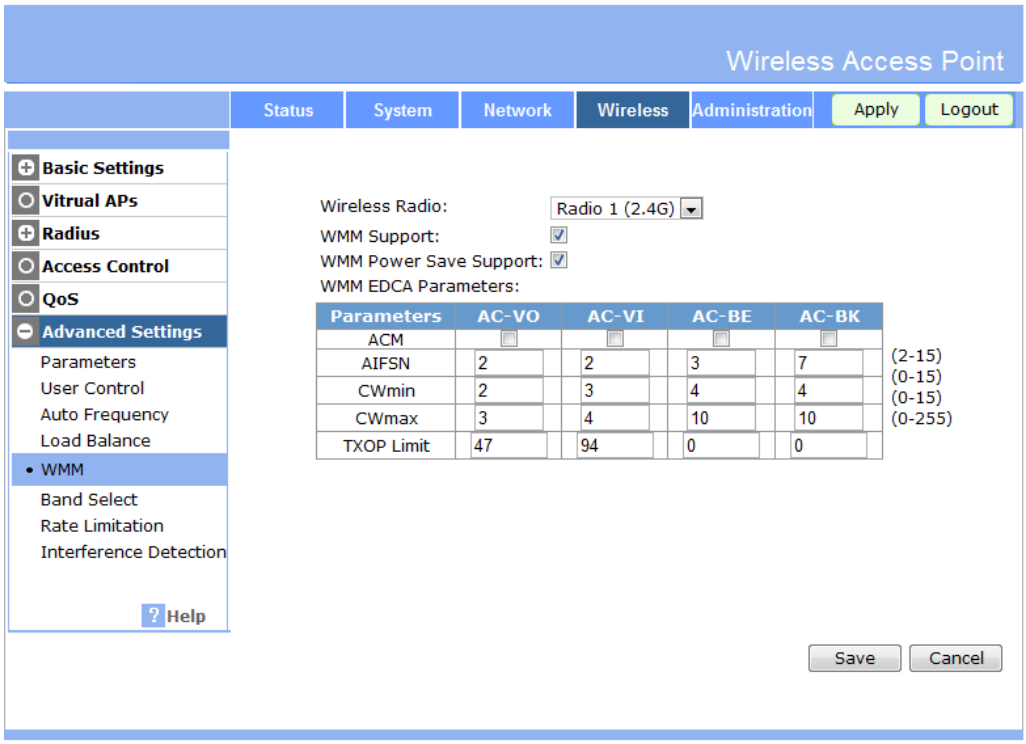

Figure 37: WMM Screen

Data - WMM Screen

WMM	
Wireless Radio	Select the desired radio option from the list.
WMM Support	Check this to enable WMM (Wi-Fi Multimedia) support. This feature is also supported by your wireless clients, whose voice and multimedia traffic will be given a higher priority than other traffic.
WMM Power Save Support	Enable or disable WMM Power-Save feature
WMM EDCA Parameters (When the Number of Spatial Streams≥ 2，Can support static and dynamic Spatial Multiplexing Power Saving.	
ACM	ACM (Admission Control Mandatory) is used to restrict stations from using a specific AC.
AIFSN	Specify the AIFSN (Arbitration Interframe Space) of the AC here. The idle duration increases as the AIFSN value increases.
CWmin/CWmax	CWmin (Minimum Contention Windows) and CWmax (Maximum Contention Windows) determine the average backoff slots, which increases as the two values increase. CWMax value must be greater than or equal to CWMin.

TXOPlimit	Transmission opportunity limit (TXOPLimit) indicates the maximum time, which a user can use a channel after a successful contention. The greater the TXOPLimit is, the longer the user can use the channel. The value 0 indicates that the user can send only one packet each time when it uses the channel.

Band Select Screen

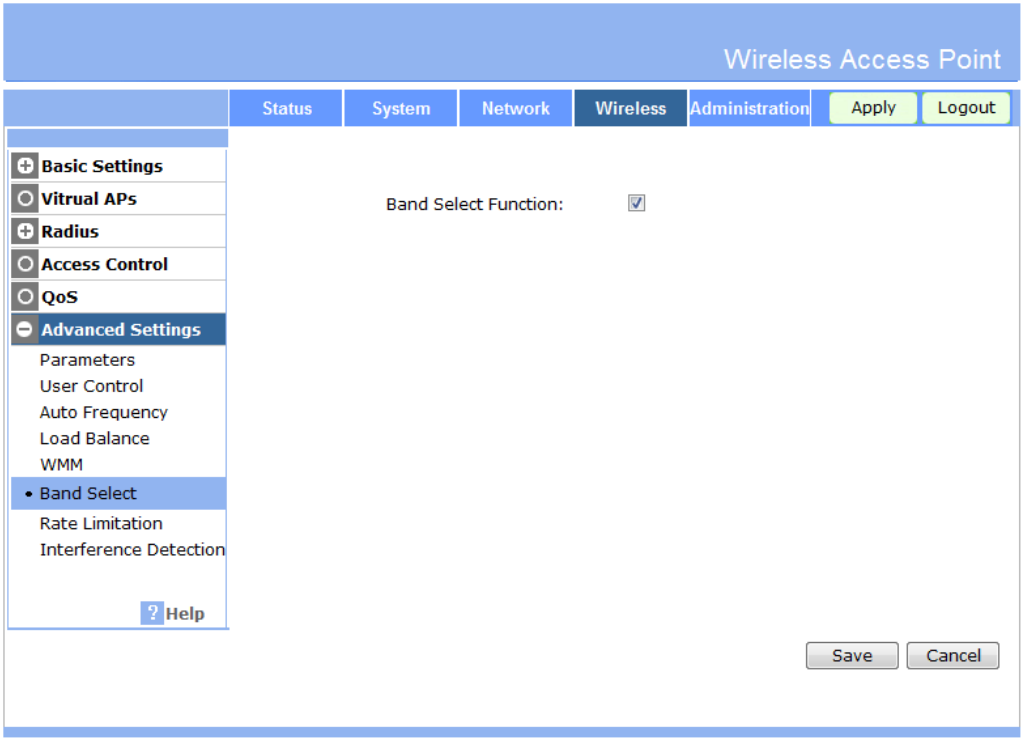

Figure 38: Band Select Screen

Data - Band Select Screen

Band Select	
Band Select Function	When 2.4G radio and 5G radio are both enabled, and both have the same SSIDs, this function will force dual band (2.4G & 5G) clients to connect with 5G channel.

Rate Limitation Screen

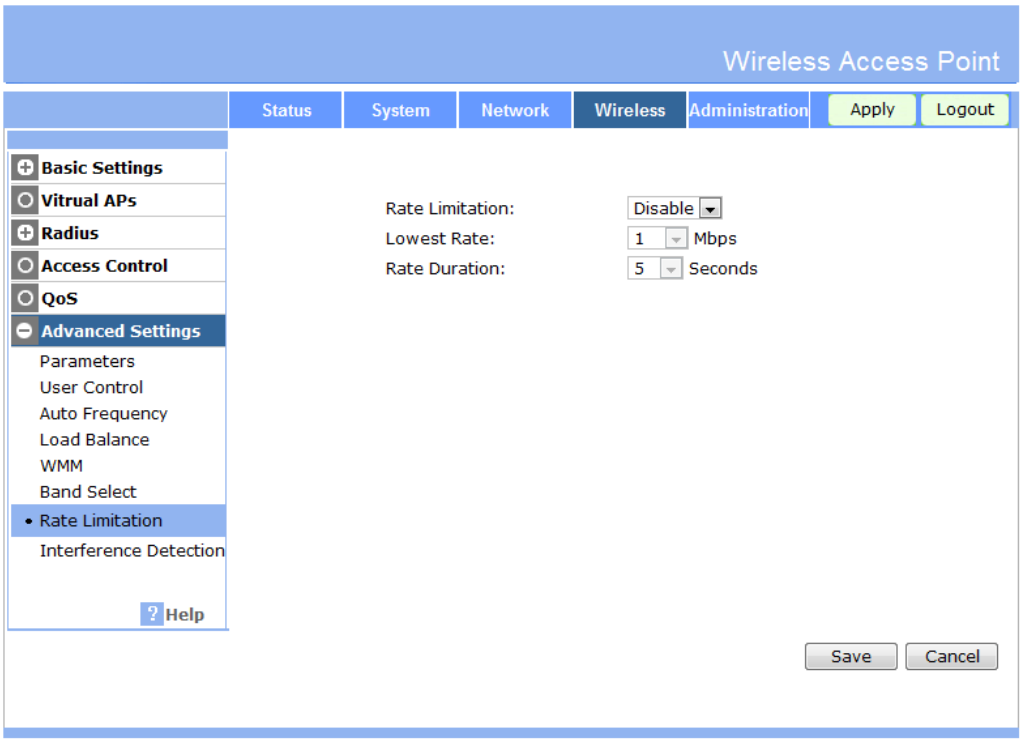

Figure 39: Rate limitation Screen

Data - Rate limitation Screen

Rate limitation	
Rate Limitation	If this feature is enabled, it will be disconnected when one wireless client's link rate is lower than the specified lowest rate in a specified duration.
Lowest Rate	Select the lowest rate from the list.
Rate Duration	Choose the desired duration from the drop-down list.

Interference Detection Screen

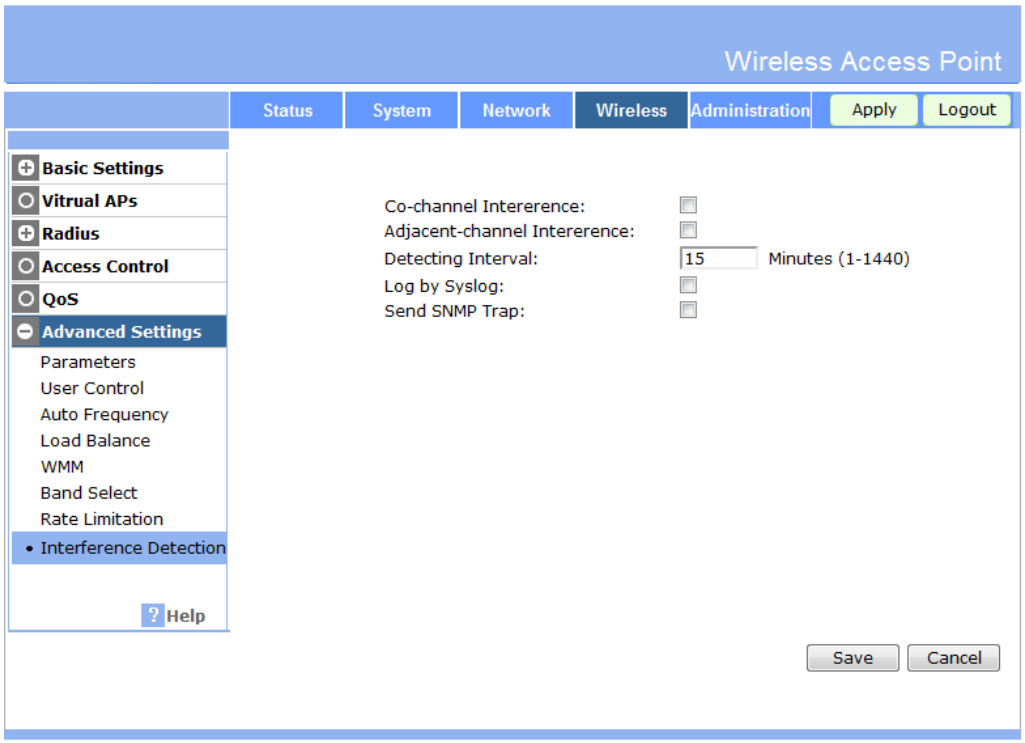

Figure 40: Interference Detection Screen

Data - Interference Detection Screen

Interference Detection	
Co-channel Interference	Check it to enable the detecting interference of APs with same channels.
Adjacent-channel Interference	Check it to enable the detecting interference of APs with adjacent channels.
Detecting Interval	Specify the interval for detecting.
Log by Syslog	Enable it if you want to use this function.
Send SNMP Trap	Send the results of interference by SNMP trap if enabled.

Network - Device Mode Screen

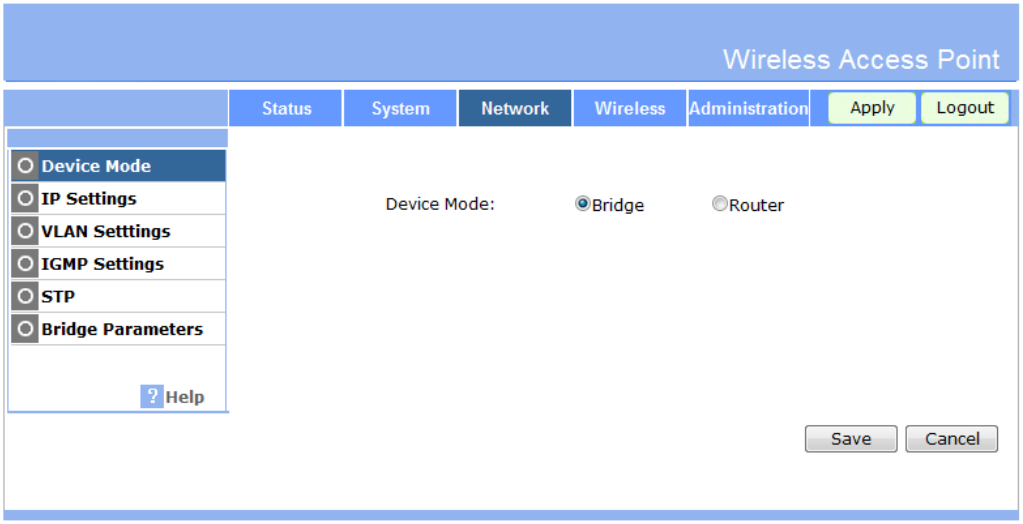

Figure 41: Device Mode Screen

Data - Device Mode Screen

Device Mode	If bridge mode is selected, then the device will act as an Access Point. If router mode is selected, then the device will act as a router.

Network - IP Settings Screen

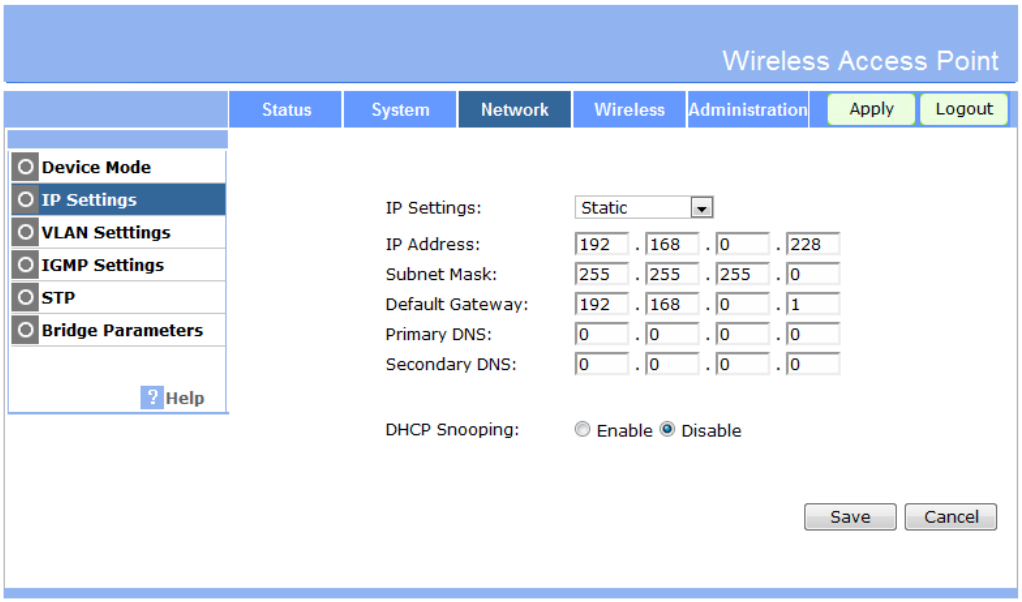

Figure 42: IP Settings Screen

Data - IP Settings Screen

IP Settings	

IP Settings	Select the desired option from the drop-down list.
	• Static - Select it if you want to configure one static IP Address for the Access Point. You need input following settings:
	  • IP Address: The IP Address of this device.
	  • Subnet Mask: The Network Mask associated with the IP |Address above.
	  • Default Gateway: The IP Address of your Gateway or Router.
	  • Primary DNS: Specify a primary DNS here. It's necessary for functions like NTP Client, E-Mail alert and so on.
	  • Secondary DNS: Specify a secondary DNS here. It's optional.
	• DHCP Client - Select it if you want the device to obtain an IP address automatically.
	• PPPoE Client - This is the most common login method, widely used with DSL modems.
	  • **Username** - The user name (or account name) provided by your ISP.
	  • **Password** - Enter the password for the login name above.
	  • **Timeout** - Enter the desired value in seconds for the timeout period.
	  • **Retry** - Enter the retry times for the PPPoE connection.
	  • **Auth-Type** - Choose the desired option from the list.
	  • **MTU** - Enter the number between 128 and 1492 for MTU.

AC IP Address	Enter the IP address for the AC. It's necessary when the IP Settings is "Static".
AC DNS Name 1	Enter the primary DNS name for the AC.
AC DNS Name 2	Enter the secondary DNS name for the AC. It is optional.

Network - VLAN Settings Screen

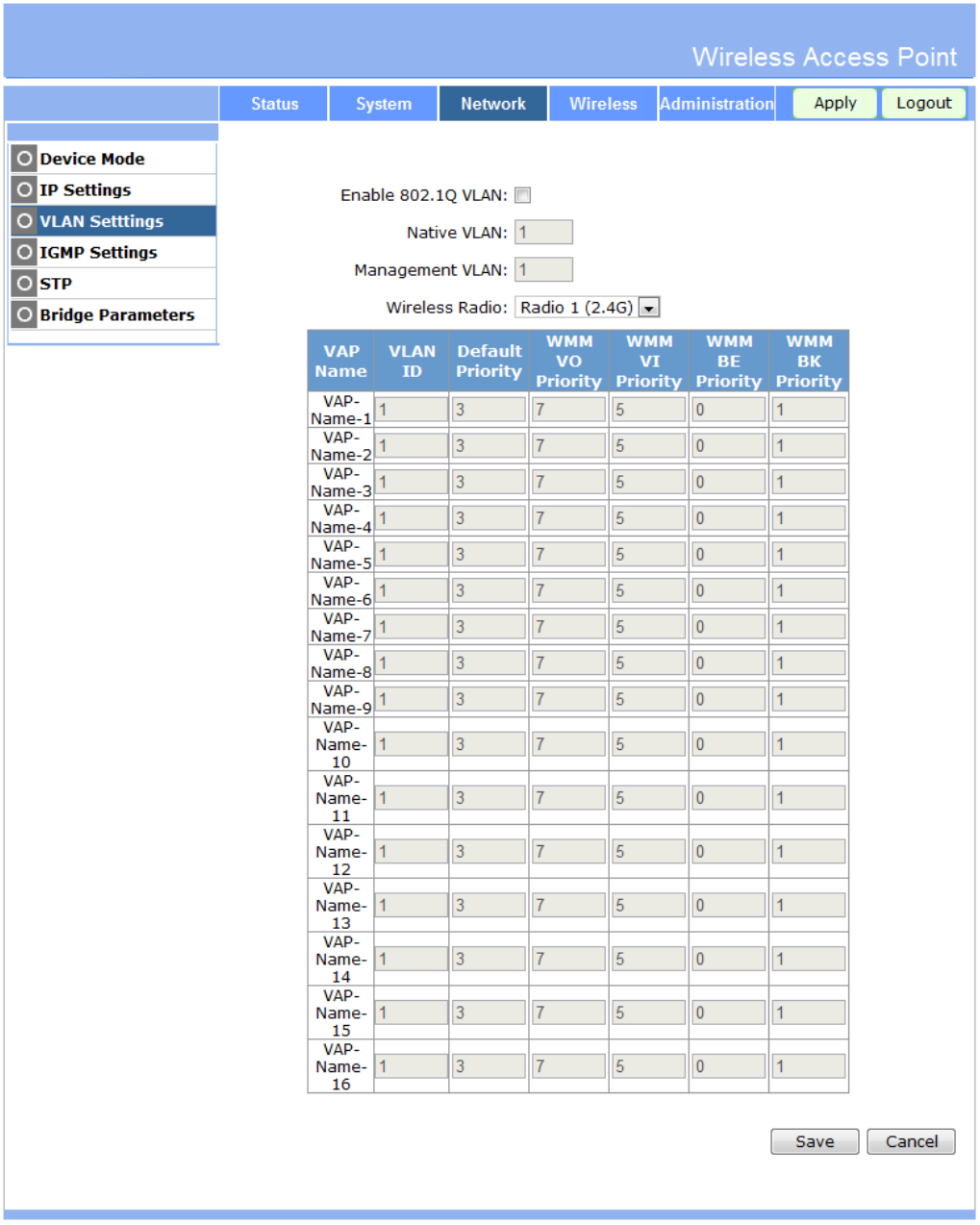

Figure 43: VLAN Settings Screen

Data - VLAN Settings Screen

VLAN Settings	
Enable 802.1Q VLAN	This option is only useful if the hubs/switches on your LAN support the VLAN standard.
Native VLAN	Enter the value for Native VLAN.

Management VLAN	Define the VLAN ID used for management.
Wireless Radio	Select the desired option from the list.
VLAN Table	802.1p setting: Enter the values for VLAN ID, Default Priority, WMM VO Priority, WMM VI Priority, WMM BE Priority, WMM BK Priority in the table.

Network - IGMP Settings Screen

Figure 44: IGMP Settings Screen

Data - IGMP Settings Screen

IGMP Settings	
IGMP Snooping	This option is only useful if the hubs/switches on your LAN support the VLAN standard.

Network - STP Screen

Figure 45: STP Screen

Data - STP Screen

STP	
Enable Spanning Tree Protocol	Enable this if you want to use this feature.

Network - Bridge Parameters Screen

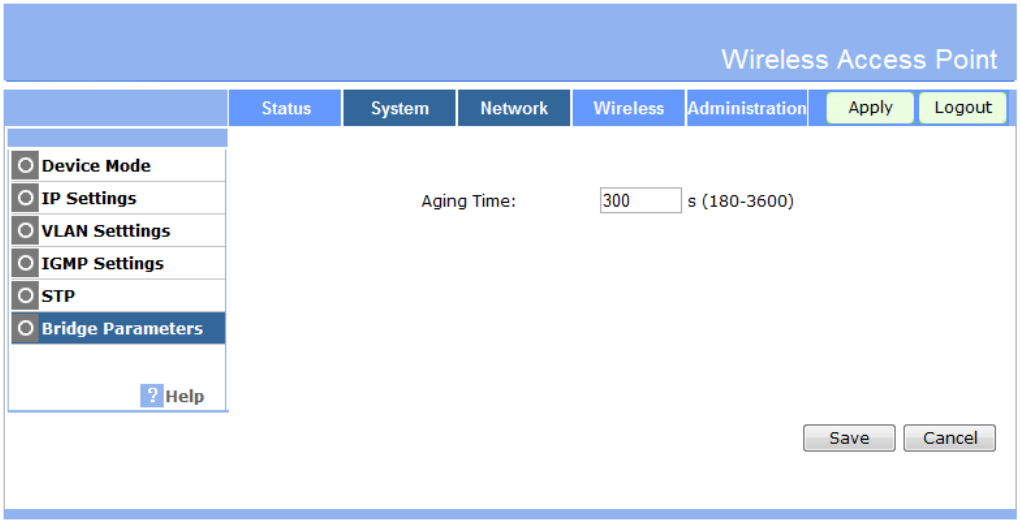

Figure 46: Bridge Parameters Screen

Data - Bridge Parameters Screen

Bridge Parameters	
Ageing Time	This value indicates the ageing time on the bridge. If it is timeout, this station will be removed from the bridge table.

Chapter 4

PC and Server Configuration

This Chapter details the PC Configuration required for each PC on the local LAN.

Overview

All Wireless Stations need to have settings which match the Wireless Access Point. These settings depend on the mode in which the Access Point is being used.

- If using WEP or WPA-PSK, it is only necessary to ensure that each Wireless station's settings match those of the Wireless Access Point, as described below.
- For 802.1x modes, configuration is much more complex. The Radius Server must be configured correctly, and setup of each Wireless station is also more complex.

Using WEP

For each of the following items, each Wireless Station must have the same settings as the Wireless Access Point.

Mode	On each PC, the mode must be set to ***Infrastructure***.
SSID (ESSID)	This must match the value used on the Wireless Access Point. The default value is **`wireless`** **Note! The SSID is case sensitive.**
Wireless Security	• Each Wireless station must be set to use WEP data encryption. • The Key size (64 bit, 128 bit, 152 bit) must be set to match the Access Point. • The keys values on the PC must match the key values on the Access Point. **Note**: On some systems, the key sizes may be shown as 40bit, 104bit, and 128bit instead of 64 bit, 128 bit and 152bit. This difference arises because the key input by the user is 24 bits less than the key size used for encryption.

Using WPA-PSK/WPA2-PSK

For each of the following items, each Wireless Station must have the same settings as the Wireless Access Point.

Mode	On each PC, the mode must be set to ***Infrastructure***.
SSID (ESSID)	This must match the value used on the Wireless Access Point. The default value is **`wireless`** **Note! The SSID is case sensitive.**
Wireless Security	On each client, Wireless security must be set to WPA-PSK. • The **Pre-shared Key** entered on the Access Point must also be entered on each Wireless client. • The **Encryption** method (e.g. TKIP, AES) must be set to match the Access Point.

Using WPA-Enterprise

This is the most secure and most complex system.

WPA-Enterprise mode provides greater security and centralized management, but it is more complex to configure.

Wireless Station Configuration

For each of the following items, each Wireless Station must have the same settings as the Wireless Access Point.

Mode	On each PC, the mode must be set to ***Infrastructure***.
SSID (ESSID)	This must match the value used on the Wireless Access Point. The default value is **`wireless`** **Note! The SSID is case sensitive.**
802.1x Authentication	Each client must obtain a Certificate which is used for authentication for the Radius Server.
802.1x Encryption	Typically, EAP-TLS is used. This is a dynamic key system, so keys do NOT have to be entered on each Wireless station. However, you can also use a static WEP key (EAP-MD5); the Wireless Access Point supports both methods simultaneously.

Radius Server Configuration

If using **WPA-Enterprise** mode, the Radius Server on your network must be configured as follow:

- It must provide and accept **Certificates** for user authentication.
- There must be a **Client Login** for the Wireless Access Point itself.
  - The Wireless Access Point will use its Default Name as its Client Login name. (However, your Radius server may ignore this and use the IP address instead.)
  - The *Shared Key*, set on the *Security* Screen of the Access Point, must match the *Shared Secret* value on the Radius Server.
- **Encryption** settings must be correct.

802.1x Server Setup (Windows 2000 Server)

This section describes using *Microsoft Internet Authentication Server* as the Radius Server, since it is the most common Radius Server available that supports the EAP-TLS authentication method.

The following services on the Windows 2000 Domain Controller (PDC) are also required:

- dhcpd
- dns
- rras
- webserver (IIS)
- Radius Server (Internet Authentication Service)
- Certificate Authority

Windows 2000 Domain Controller Setup

1. Run *dcpromo.exe* from the command prompt.
2. Follow all of the default prompts, ensure that DNS is installed and enabled during installation.

Services Installation

1. Select the *Control Panel - Add/Remove Programs*.
2. Click *Add/Remove Windows Components* from the left side.
3. Ensure that the following components are activated (selected):
   - *Certificate Services*. After enabling this, you will see a warning that the computer cannot be renamed and joined after installing certificate services. Select *Yes* to select certificate services and continue
   - *World Wide Web Server*. Select *World Wide Web Server* on the *Internet Information Services* (IIS) component.
   - From the *Networking Services* category, select *Dynamic Host Configuration Protocol* (DHCP), and *Internet Authentication Service* (DNS should already be selected and installed).

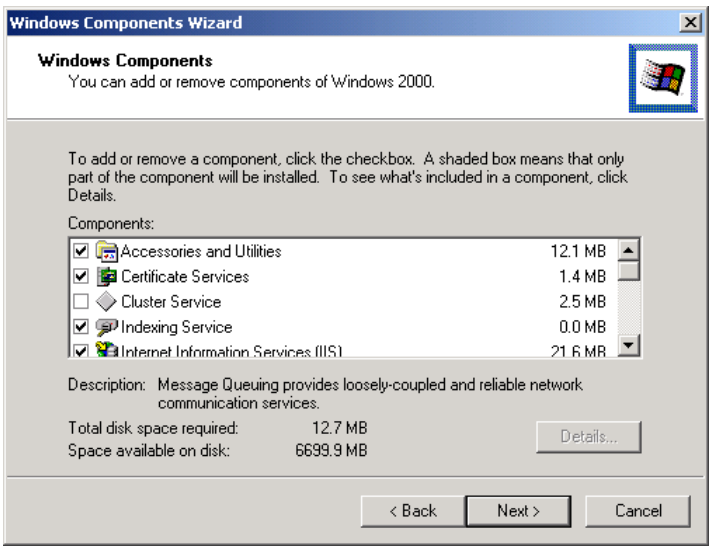

Figure 47: Components Screen

4. Click *Next*.
5. Select the *Enterprise root CA*, and click *Next*.

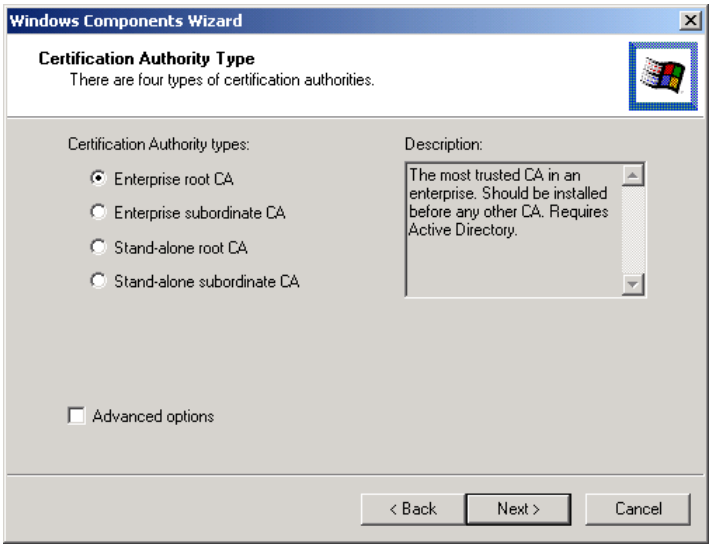

Figure 48: Certification Screen

6. Enter the information for the Certificate Authority, and click *Next*.

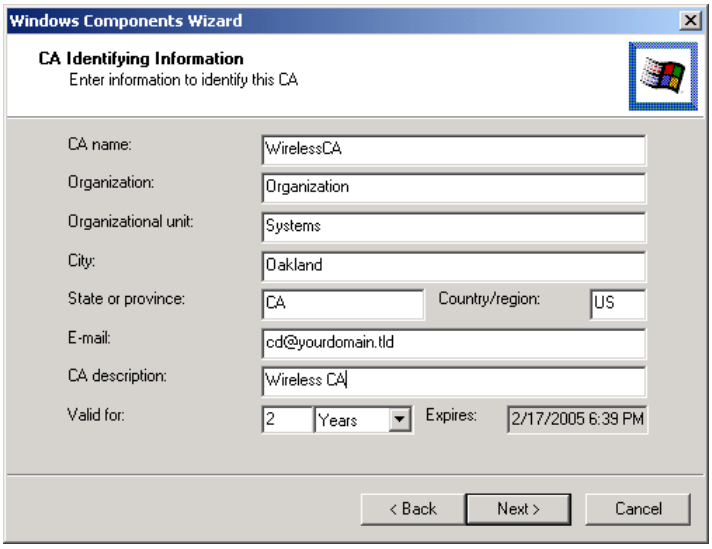

Figure 49: CA Screen

7. Click *Next* if you don't want to change the CA's configuration data.
8. Installation will warn you that Internet Information Services are running, and must be stopped before continuing. Click *Ok*, then *Finish*.

DHCP server configuration

1. Click on the *Start - Programs - Administrative Tools - DHCP*
2. Right-click on the server entry as shown, and select *New Scope*.

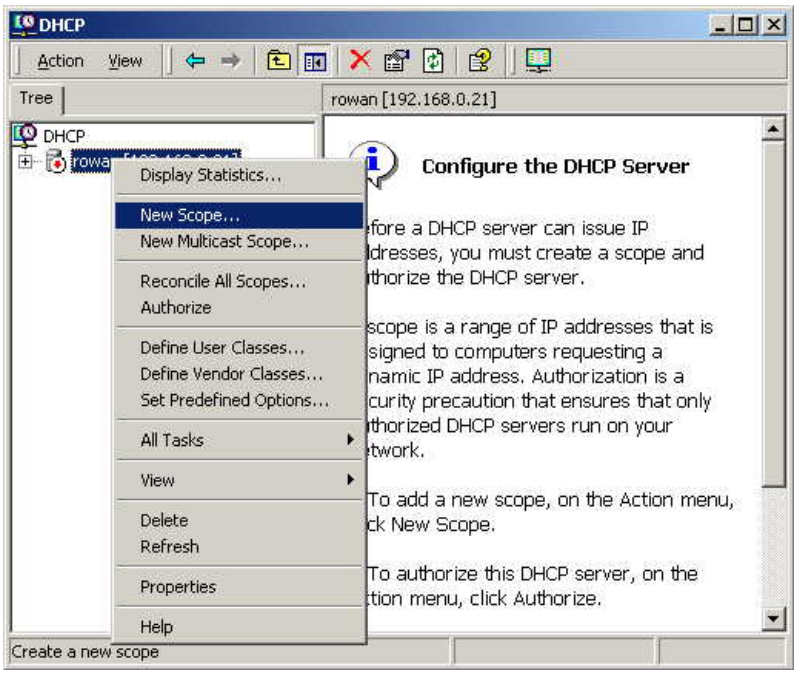

Figure 50: DHCP Screen

3. Click *Next* when the New Scope Wizard Begins.
4. Enter the name and description for the scope, click *Next*.
5. Define the IP address range. Change the subnet mask if necessary. Click *Next*.

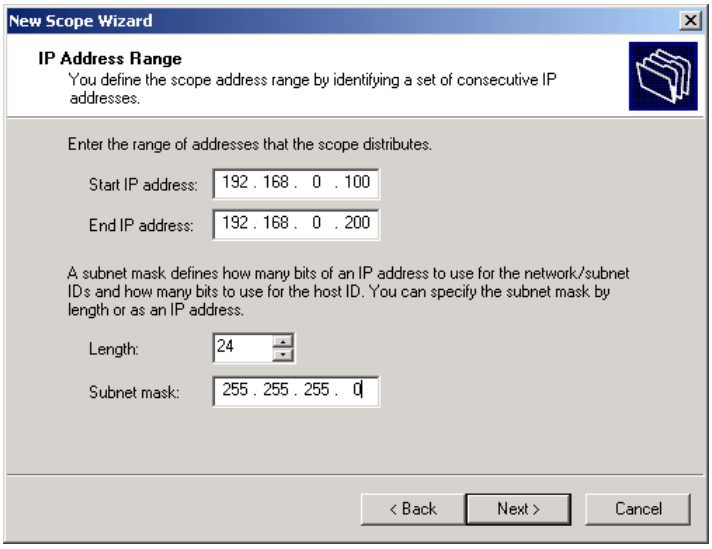

Figure 51: IP Address Screen

6. Add exclusions in the address fields if required. If no exclusions are required, leave it blank. Click *Next*.
7. Change the *Lease Duration* time if preferred. Click *Next*.
8. Select *Yes, I want to configure these options now*, and click *Next*.
9. Enter the router address for the current subnet. The router address may be left blank if there is no router. Click *Next*.
10. For the Parent domain, enter the domain you specified for the domain controller setup, and enter the server's address for the IP address. Click *Next*.

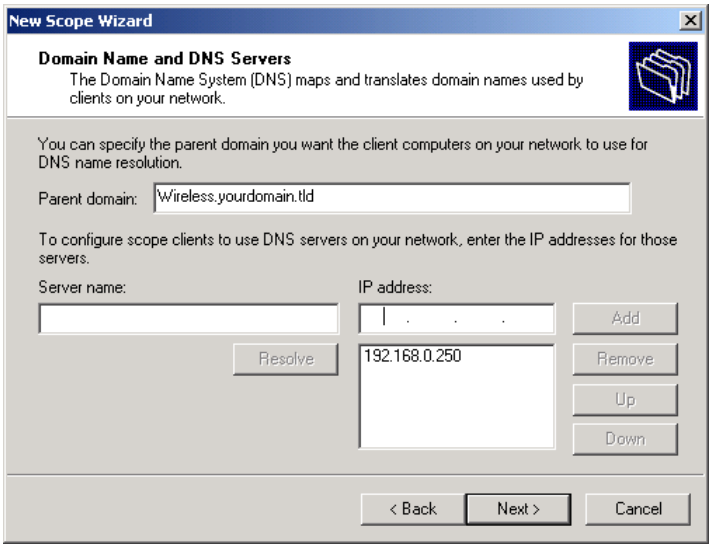

Figure 52: DNS Screen

11. If you don't want a WINS server, just click *Next*.
12. Select *Yes, I want to activate this scope now*. Click *Next*, then *Finish*.
13. Right-click on the server, and select *Authorize*. It may take a few minutes to complete.

Certificate Authority Setup

1. Select *Start - Programs - Administrative Tools - Certification Authority*.
2. Right-click *Policy Settings*, and select *New - Certificate to Issue*.

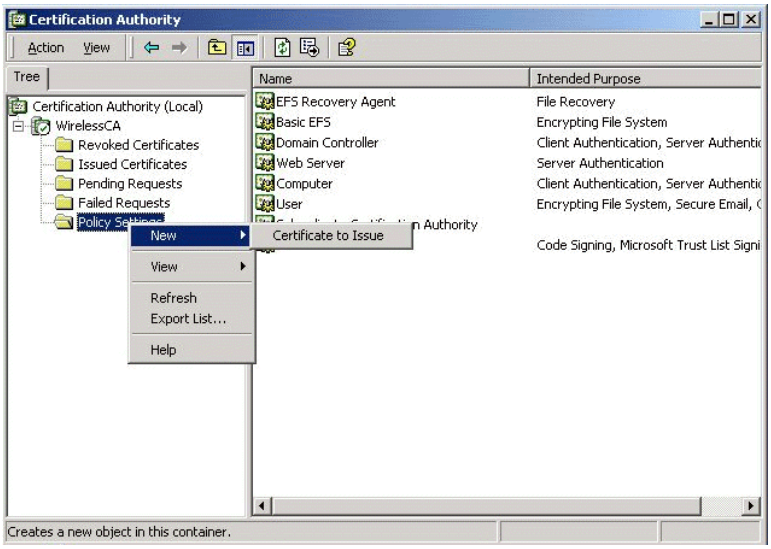

Figure 53: Certificate Authority Screen

3. Select *Authenticated Session* and *Smartcard Logon* (select more than one by holding down the Ctrl key). Click *OK*.

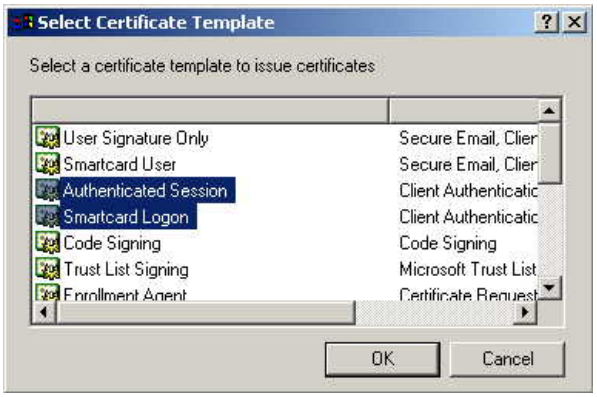

Figure 54: Template Screen

4. Select *Start - Programs - Administrative Tools - Active Directory Users and Computers*.
5. Right-click on your active directory domain, and select *Properties*.

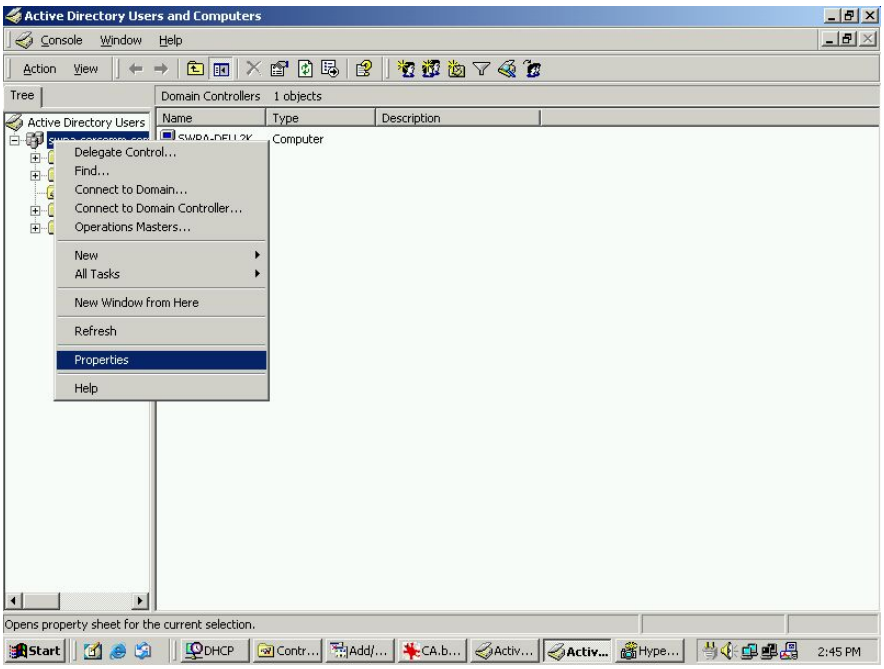

Figure 55: Active Directory Screen

6. Select the *Group Policy* tab, choose *Default Domain Policy* then click *Edit*.

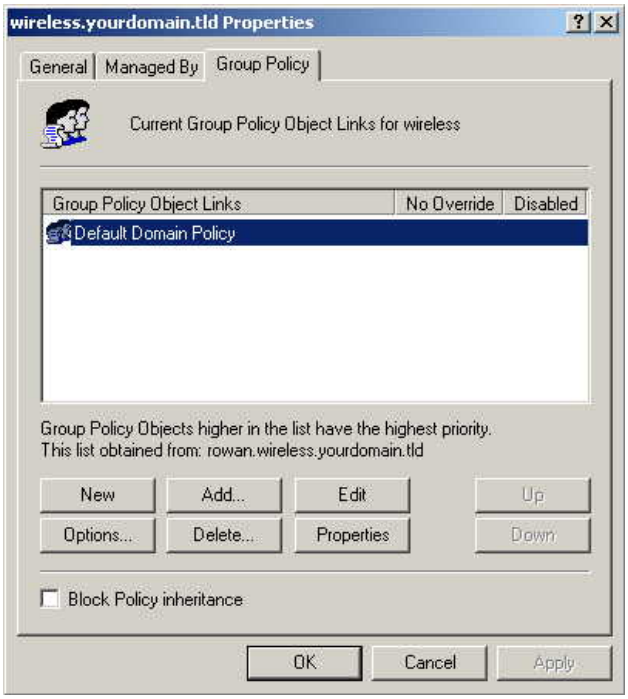

Figure 56: Group Policy Tab

7. Select *Computer Configuration - Windows Settings - Security Settings - Public Key Policies*, right-click *Automatic Certificate Request Settings - New - Automatic Certificate Request*.

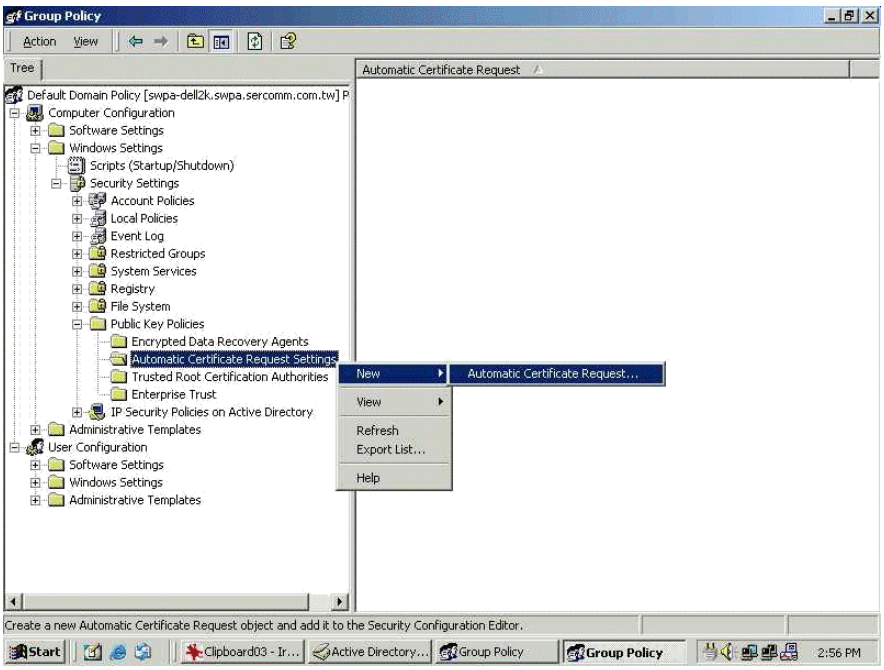

Figure 57: Group Policy Screen

8. When the Certificate Request Wizard appears, click *Next*.
9. Select *Computer*, then click *Next*.

Figure 58: Certificate Template Screen

10. Ensure that your certificate authority is checked, then click *Next*.
11. Review the policy change information and click *Finish*.
12. Click *Start* - *Run*, type *cmd* and press enter.
    Enter `secedit /refreshpolicy machine_policy`
    This command may take a few minutes to take effect.

Internet Authentication Service (Radius) Setup

1. Select *Start - Programs - Administrative Tools - Internet Authentication Service*
2. Right-click on *Clients*, and select *New Client*.

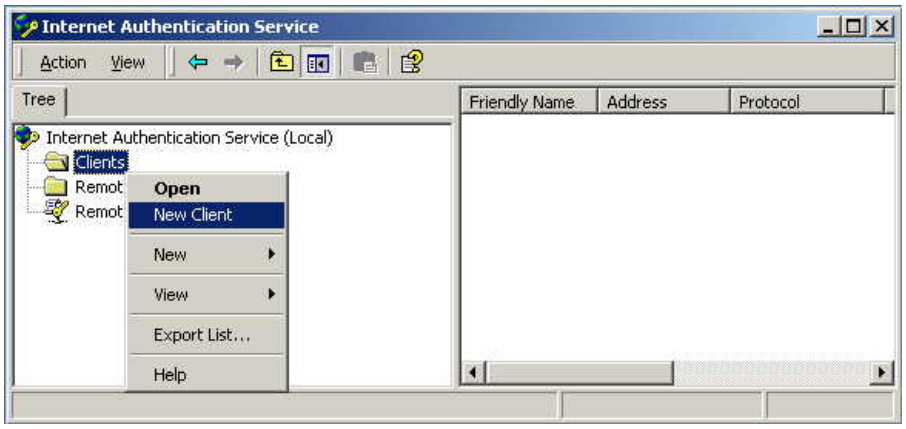

Figure 59: Service Screen

3. Enter a name for the access point, click *Next*.
4. Enter the address or name of the Wireless Access Point, and set the shared secret, as entered on the *Security Settings* of the Wireless Access Point.
5. Click *Finish*.
6. Right-click on *Remote Access Policies*, select *New Remote Access Policy*.
7. Assuming you are using EAP-TLS, name the policy `eap-tls`, and click *Next*.
8. Click *Add...*
   If you don't want to set any restrictions and a condition is required, select *Day-And-Time-Restrictions*, and click *Add...*

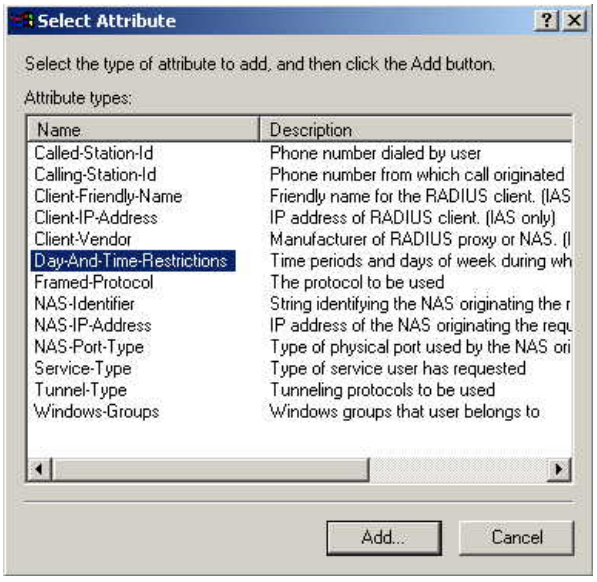

Figure 60: Attribute Screen

9. Click *Permitted*, then *OK*. Select *Next*.
10. Select *Grant remote access permission*. Click *Next*.

11. Click *Edit Profile...* and select the *Authentication* tab. Enable *Extensible Authentication Protocol*, and select *Smart Card or other Certificate*. Deselect other authentication methods listed. Click *OK*.

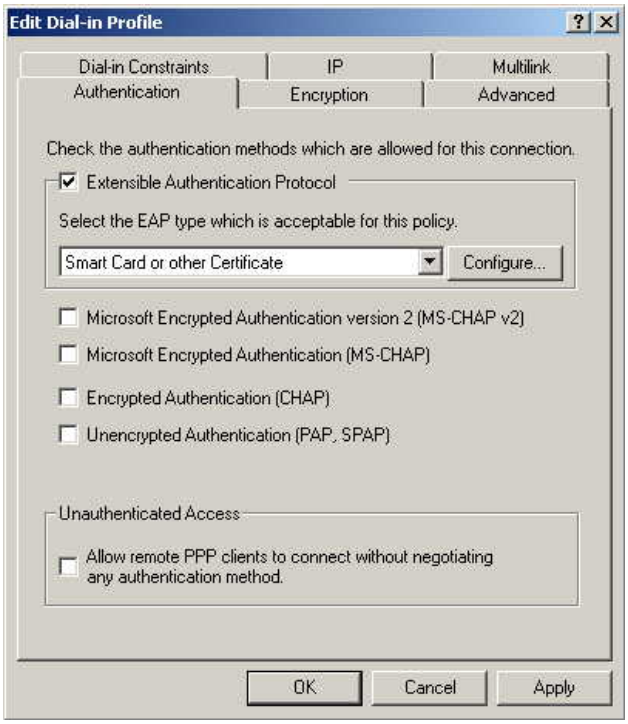

Figure 61: Authentication Screen

12. Select *No* if you don't want to view the help for EAP. Click *Finish*.

Remote Access Login for Users

1. Select *Start - Programs - Administrative Tools- Active Directory Users and Computers*.
2. Double click on the user who you want to enable.
3. Select the *Dial-in* tab, and enable *Allow access*. Click *OK*.

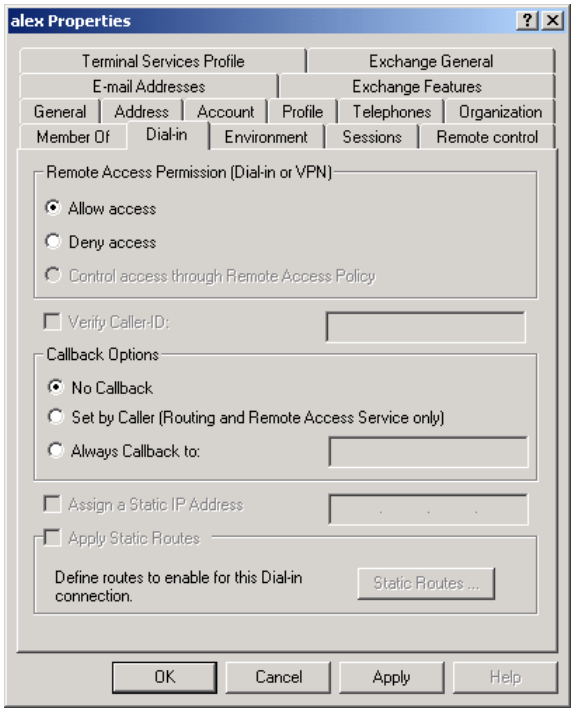

Figure 62: Dial-in Screen

Using 802.1x Mode (without WPA)

This is very similar to using WPA-Enterprise.

The only difference is that on your client, you must NOT enable the setting *The key is provided for me automatically*.

Instead, you must enter the WEP key manually, ensuring it matches the WEP key used on the Access Point.

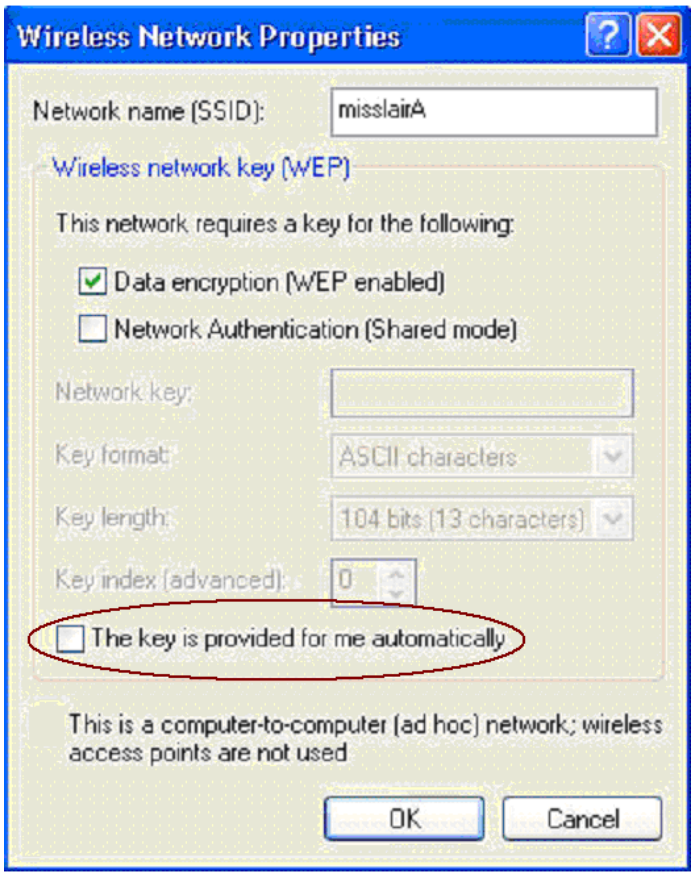

Figure 63: Properties Screen

Note:

On some systems, the "64 bit" WEP key is shown as "40 bit" and the "128 bit" WEP key is shown as "104 bit". This difference arises because the key input by the user is 24 bits less than the key size used for encryption.

Chapter 5

Operation and Status

This Chapter details the operation of the Wireless Access Point and the status screens.

Status Screen

Use the ***Status*** link on the main menu to view this screen.

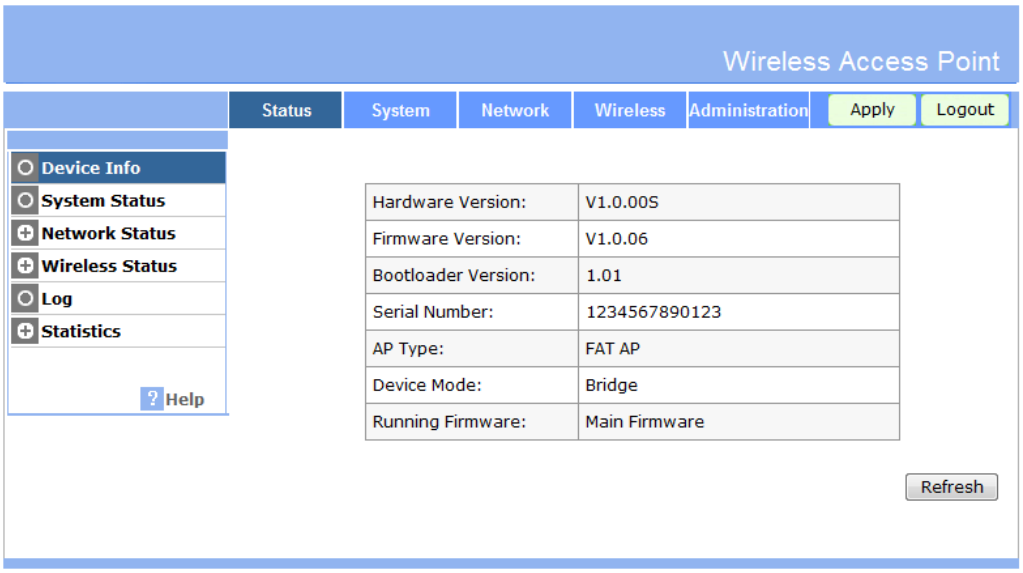

Figure 64: Device Info Screen

Data - Device Info Screen

Access Point	
Hardware Version	The version of the hardware currently used.
Firmware Version	The version of the firmware currently installed.
Bootloader Version	The version of the bootloader currently used.
Serial Number	The serial number of the device.
AP Type	The current AP type is displayed.
Device Mode	The current Device mode is displayed
Running Firmware	The currently running firmware is displayed.

System Status

This screen is displayed when the *System Status* button is clicked.

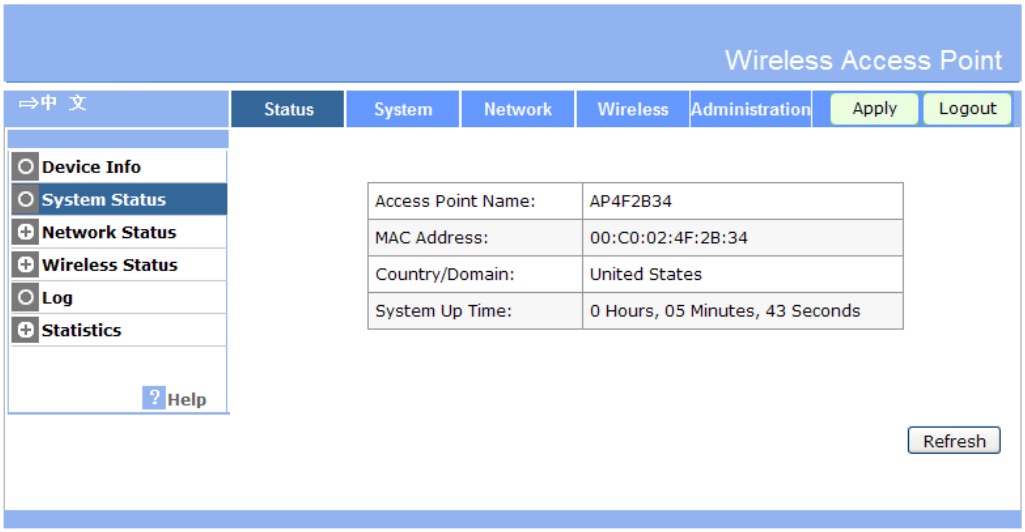

Figure 65: System Status Screen

Data - System Status Screen

Access Point Name	The current name will be displayed.
MAC Address	The MAC (physical) address of the Wireless Access Point.
Country/Domain	The region or domain, as selected on the System screen.
System Up Time	This indicates how long the system has been running since the last restart or reboot.

Network Status

This screen is displayed when the *Network Status* button is clicked.

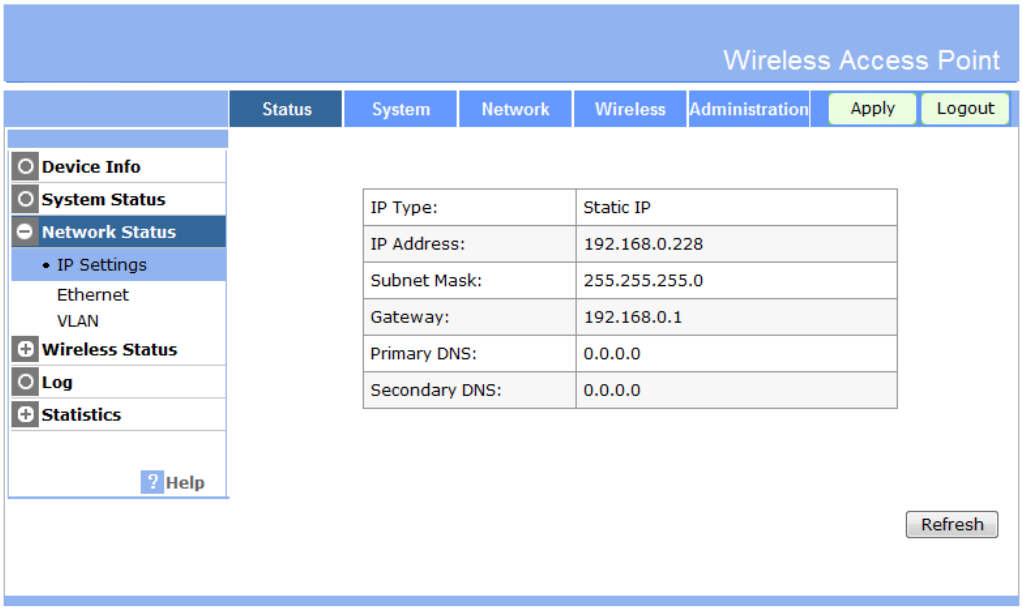

Figure 66: IP Settings Screen

Data - IP Settings Screen

TCP/IP	
IP Type	The current IP type is displayed.
IP Address	The IP Address of the Wireless Access Point.
Subnet Mask	The Network Mask (Subnet Mask) for the IP Address above.
Gateway	Enter the Gateway for the LAN segment to which the Wireless Access Point is attached (the same value as the PCs on that LAN segment).
Primary DNS	Enter the IP Address of the DNS (Domain Name Servers) here. These DNS will be used only if the primary DNS is unavailable.
Secondary DNS	The Secondary DNS will be used only if the primary DNS is unavailable.

Ethernet

This screen is displayed when the *Ethernet* button is clicked.

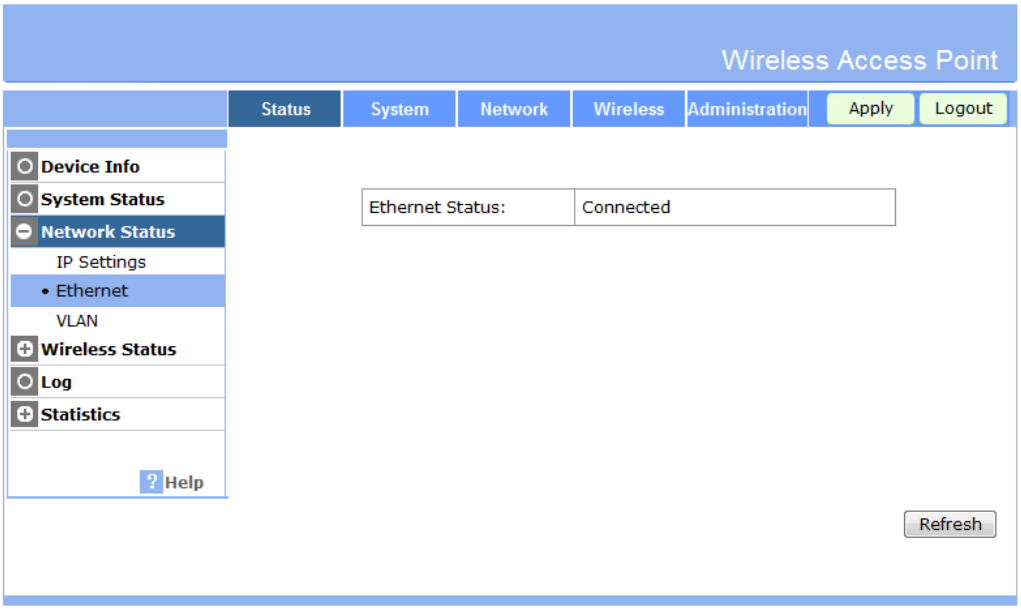

Figure 67 Ethernet Screen

Data - Ethernet Screen

Ethernet	
Ethernet Status	The current Ethernet status is displayed.

VLAN

This screen is displayed when the *VLAN* button is clicked.

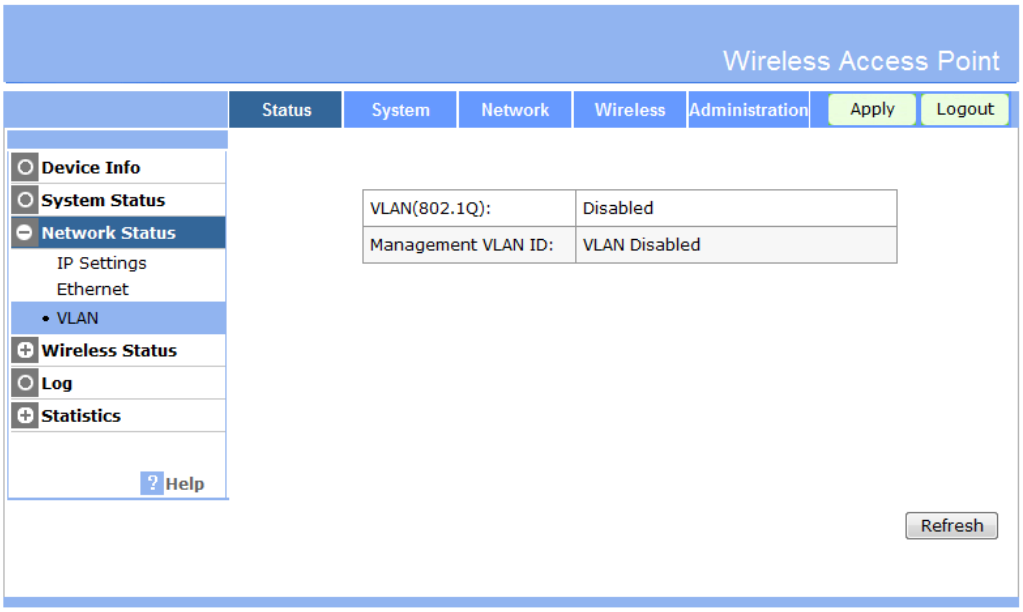

Figure 68: VLAN Screen

Data - VLAN Screen

VLAN	
VLAN	The current VLAN status is displayed.
Management VLAN ID	It displays the VLAN ID of Management VLAN.

Wireless Status

Basic Screen

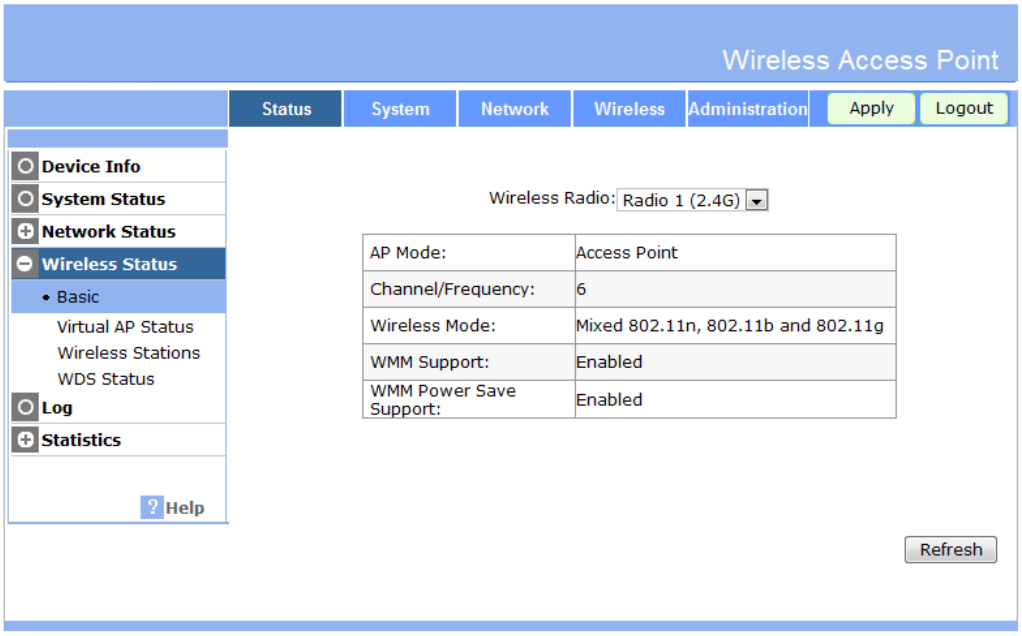

Figure 69: Basic Screen

Data - Basic Screen

Basic	
AP Mode	The current Access Point mode is displayed.
Channel/Frequency	The Channel currently in use is displayed.
Wireless Mode	The current mode (e.g. 802.11g) is displayed.
WMM Support	"Enabled" or "Disabled" is displayed for the WMM status.
WMM Power Save Support	"Enabled" or "Disabled" is displayed for the WMM Power Save status.

Virtual AP Status Screen

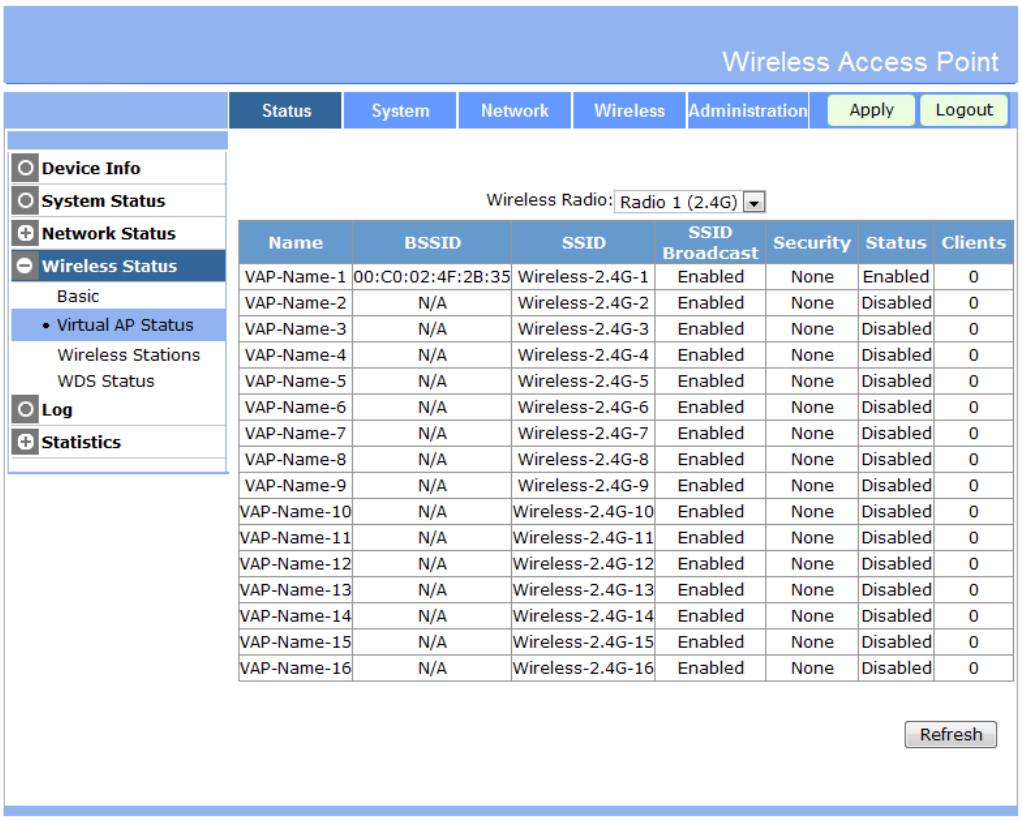

Figure 70: Virtual AP Status Screen

Data - Virtual AP Status Screen

Virtual AP Status	
Wireless Radio	Select the desired band (2.4 GHz or 5 GHz) used by this profile.
Name	The name you gave to this profile; if you didn't change the name, the default name is used.
BSSID	The BSSID assigned to this profile.
SSID	The SSID assigned to this profile.
SSID Broadcast	Indicates whether or not the SSID is broadcast.
Security	The security method used by this profile.
Status	Indicates whether or not this profile is enabled or currently used.
Clients	The number of wireless stations currently using accessing this Access Point using this profile. If the profile is disabled, this will always be zero.

Wireless Stations Screen

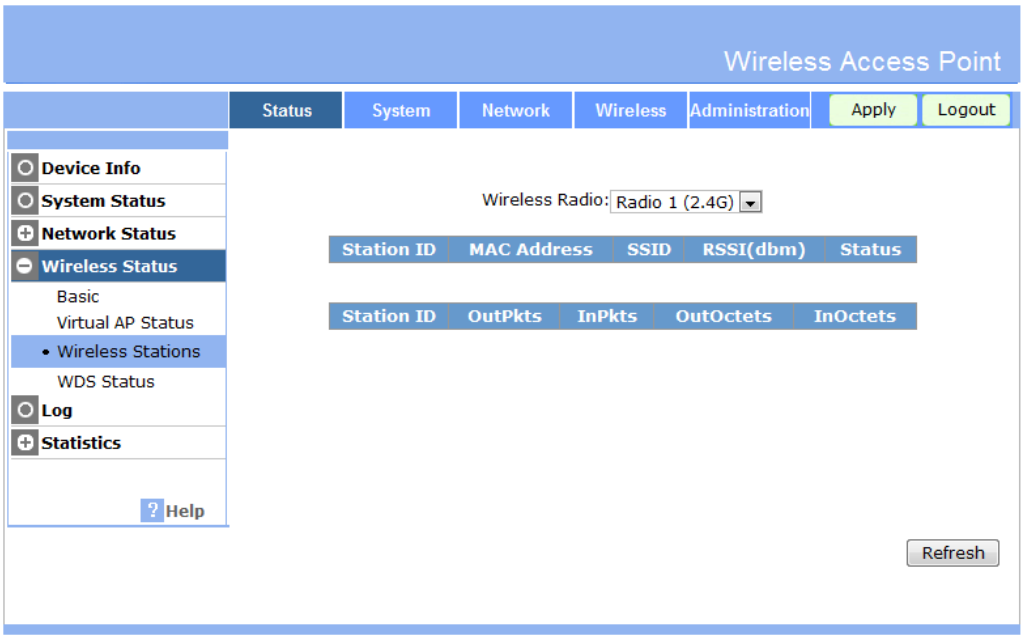

Figure 71: Wireless Stations Screen

Data - Wireless Station Screen

Station List	
Wireless Radio	Select the desired band (2.4 GHz or 5 GHz) used by this profile.
Station ID	The ID of each Wireless Station is displayed. If the ID is not known, "unknown" will be displayed.
MAC Address	The MAC (physical) address of each Wireless Station is displayed.
SSID	This displays the SSID used by the Wireless station. Because the Wireless Access Point supports multiple SSIDs, different PCs could connect using different SSIDs.
RSSI	It displays the RSSI (received signal strength indicator) of received radio signal
Status	This indicates the current status of each Wireless Station.
OutPkts	Number of valid Data packets transmitted to Wireless Stations
InPkts	Number of valid Data packets received from Wireless Stations.
OutOctets	Number of octests transmitted to Wireless Stations
InOctets	This indicates the current status of each Wireless Station.
Refresh Button	Update the data on screen.

WDS Status Screen

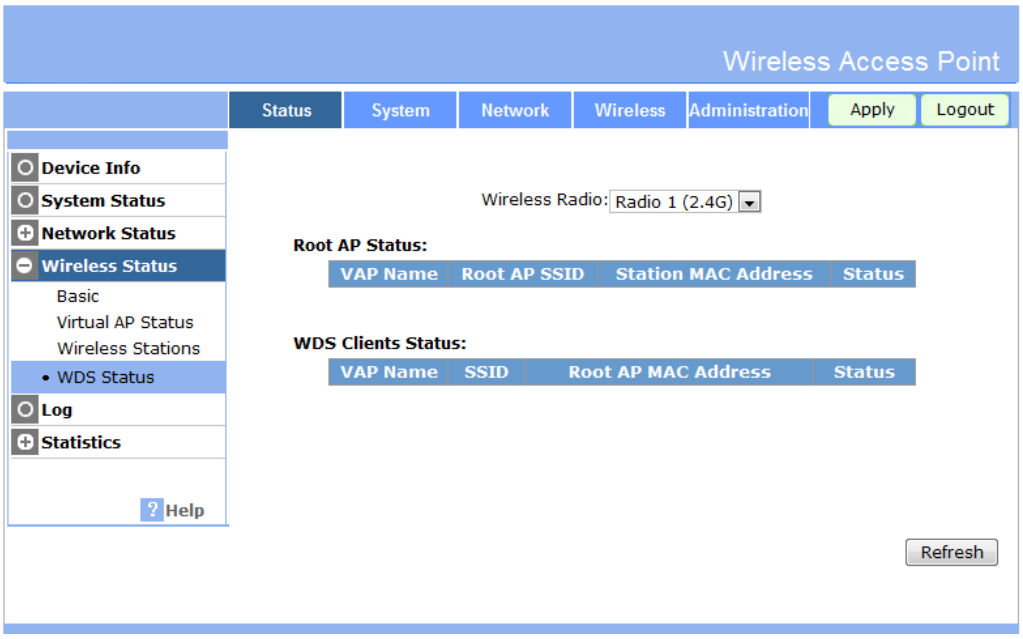

Figure 72: WDS Status Screen

Data - WDS Status Screen

Wireless Radio	Select the desired band (2.4 GHz or 5 GHz) used by this profile.
Root AP Status	The following table shows the current status of the root AP.
WDS Client Status	The following table shows the current status of the WDS Client.

Log Screen

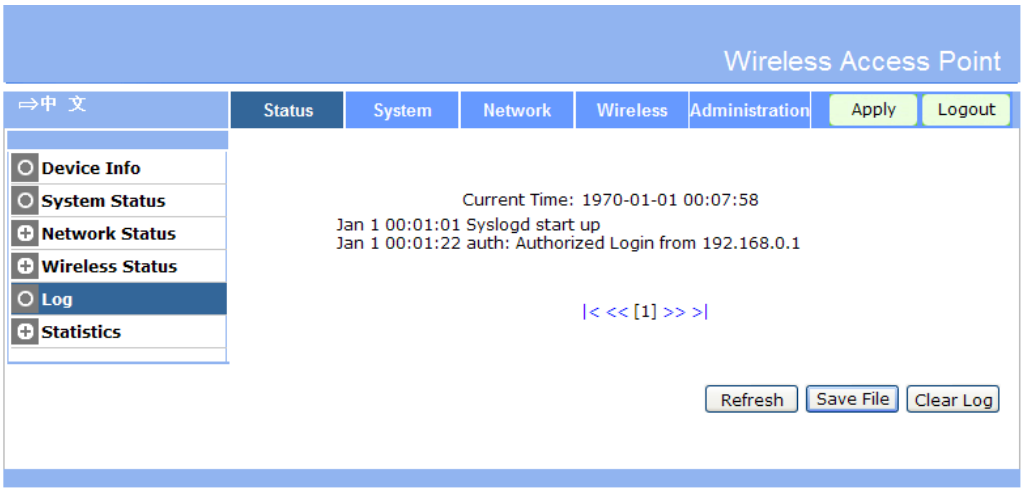

Figure 73: Log Screen

Data - Log Screen

Data	
Current Time	The system date and time is displayed.
Log	The Log shows details of the connections to the Wireless Access Point.
Buttons	
Refresh	Update the data on screen.
Save File	Save the log to a file on your pc.
Clear Log	This will delete all data currently in the Log. This will make it easier to read new messages.

Statistics Screen

Ethernet Screen

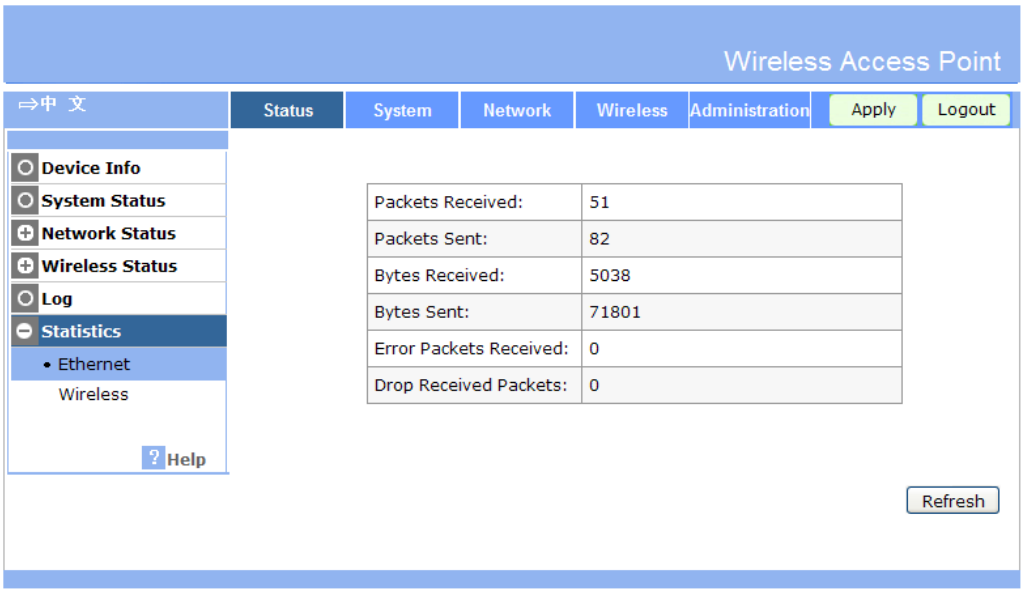

Figure 74: Ethernet Screen

Data - Ethernet Screen

Ethernet	
Packets Received	The number of packets received by the Access Point.
Packets Sent	The number of packets sent by the Access Point.
Bytes Received	The number of bytes received by the Access Point.
Bytes Sent	The number of bytes sent by the Access Point.
Error Packets Received	The number of error packets received.
Drop Received Packets	The number of drop packets received.

Wireless Screen

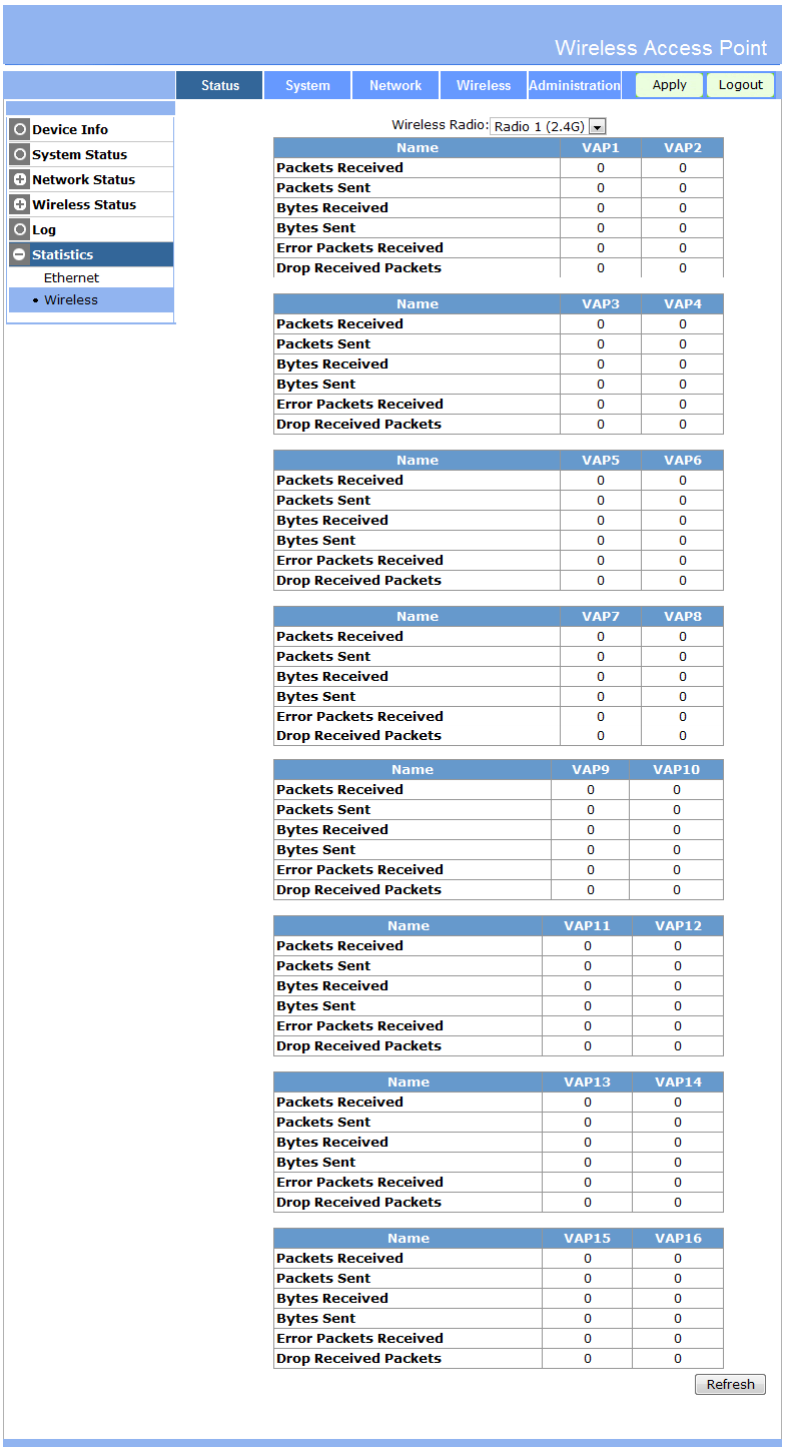

Figure 75: Wireless Screen

Data - Wireless Screen

VAP1~VAP16	
Wireless Radio	Select the desired band (2.4 GHz or 5 GHz) used by this profile.

Packets Received	The number of packets received by the Access Point.
Packets Sent	The number of packets sent by the Access Point.
Bytes Received	The number of bytes received by the Access Point.
Bytes Sent	The number of bytes sent by the Access Point.
Error Packets Received	The number of error packets received.
Drop Received Packets	The number of drop packets.

Chapter 6

Access Point Management

This Chapter explains when and how to use the Wireless Access Point's "Administration" Features.

Overview

This Chapter covers the following features, available on the Wireless Access Point's ***Administration*** menu.

- AP Type
- Management
- Auto Config
- Config File
- Ping Test
- Auto Reboot
- Firmware Upgrade

AP Type

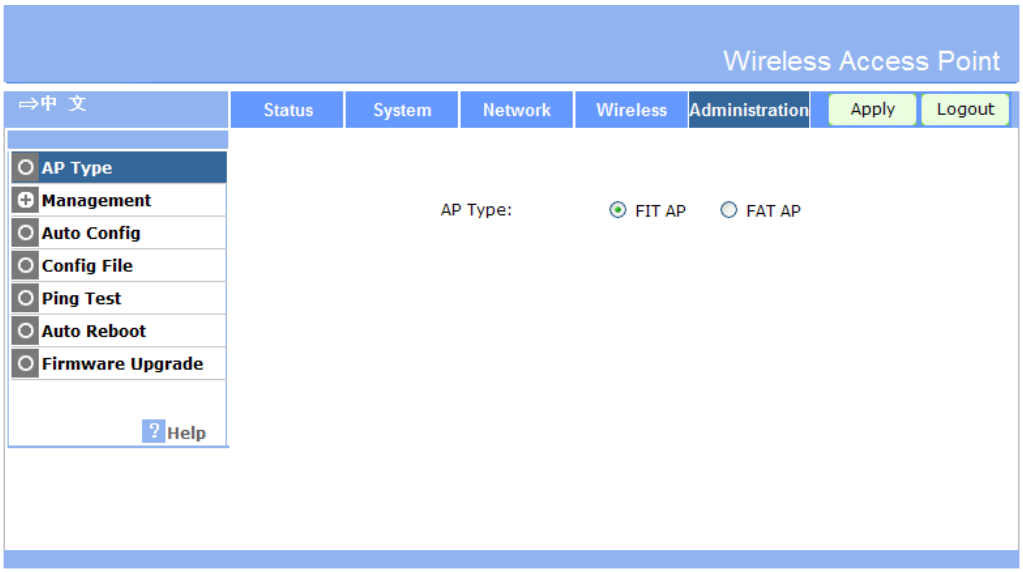

Figure 76: AP Type Screen

Data - AP Type Screen

Account	
AP Type	Select the AP type as required.

Management Screen

Account Screen

The Account screen allows you to assign or modify the names and passwords for the administrator and maintainer. It is recommended that this be changed, using this screen.

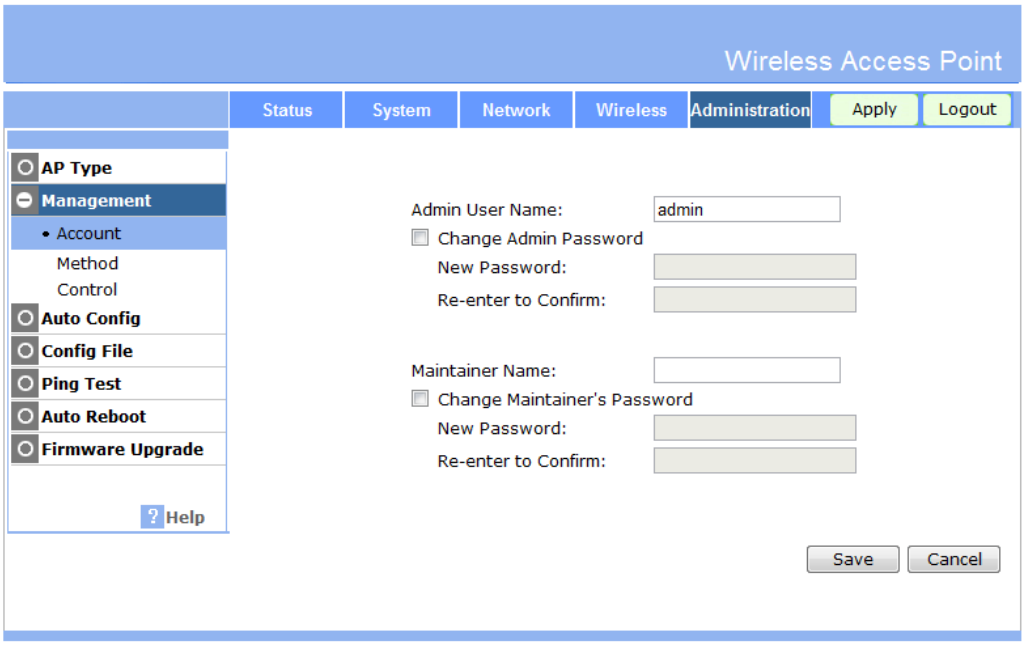

Figure 77: Account Screen

Data - Account Screen

Account	
Admin User Name	Enter the login name for the Administrator. The administrator has the maintenance and operation for all the functions.
Change Admin Password	If you wish to change the Admin password, check this field and enter the new login password in the fields below.
New Password	Enter the desired login password.
Re-enter to Confirm	Re-enter the desired login password.
Maintainer	
Maintainer Name	Enter the login name for the maintainer. This account can only be allowed to use some functions (such as Firmware Upgrade, Auto Reboot, Config file, AP Type, Device Mode and Wireless).
Change Maintainer's Password	If you wish to change the password, check this field and enter the new login password in the fields below.
New Password	Enter the desired login password.

Re-enter to Confirm	Re-enter the desired login password.

Method Screen

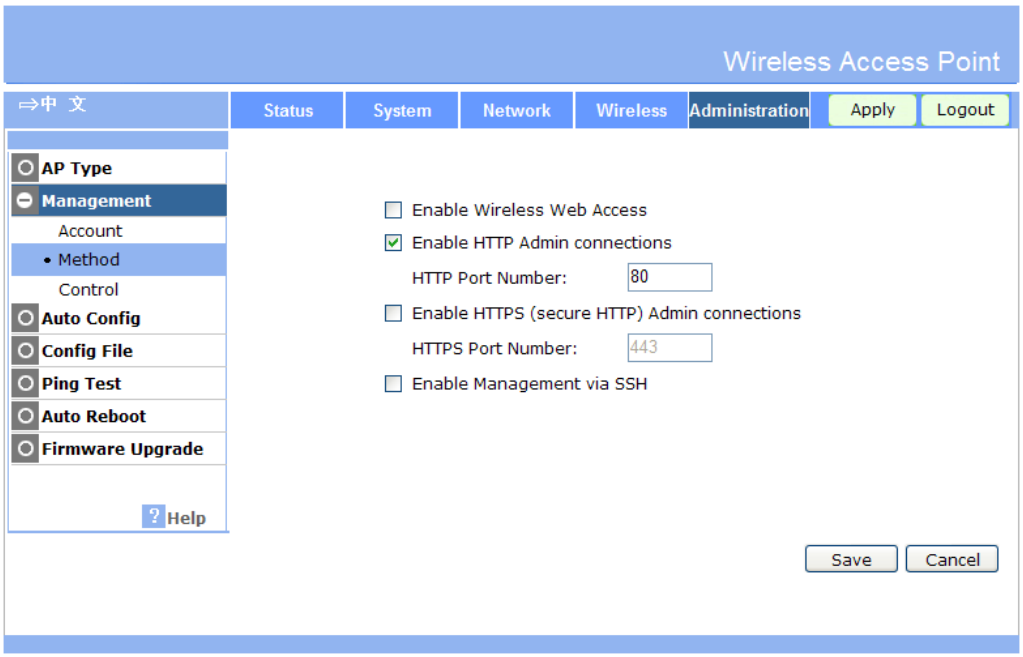

Figure 78: Method Screen

Data - Method Screen

Method	
Enable Wireless Web Access	Enable this to allow wireless client access the device.
Enable HTTP	Enable this to allow admin connections via HTTP. If enabled, you must provide a port number in the field below. Either HTTP or HTTPS must be enabled.
HTTP Port Number	Enter the port number to be used for HTTP connections to this device. The default value is 80.
Enable HTTPS	Enable this to allow admin connections via HTTPS (secure HTTP). If enabled, you must provide a port number in the field below. Either HTTP or HTTPS must be enabled.
HTTPS Port Number	Enter the port number to be used for HTTPS connections to this device. The default value is 443.
Enable Management via SSH	If desired, you can enable this option. If enabled, you will able to connect to this AP using a SSH client.

Control Screen

This feature can be used to block access to your LAN by unknown or untrusted wireless stations.

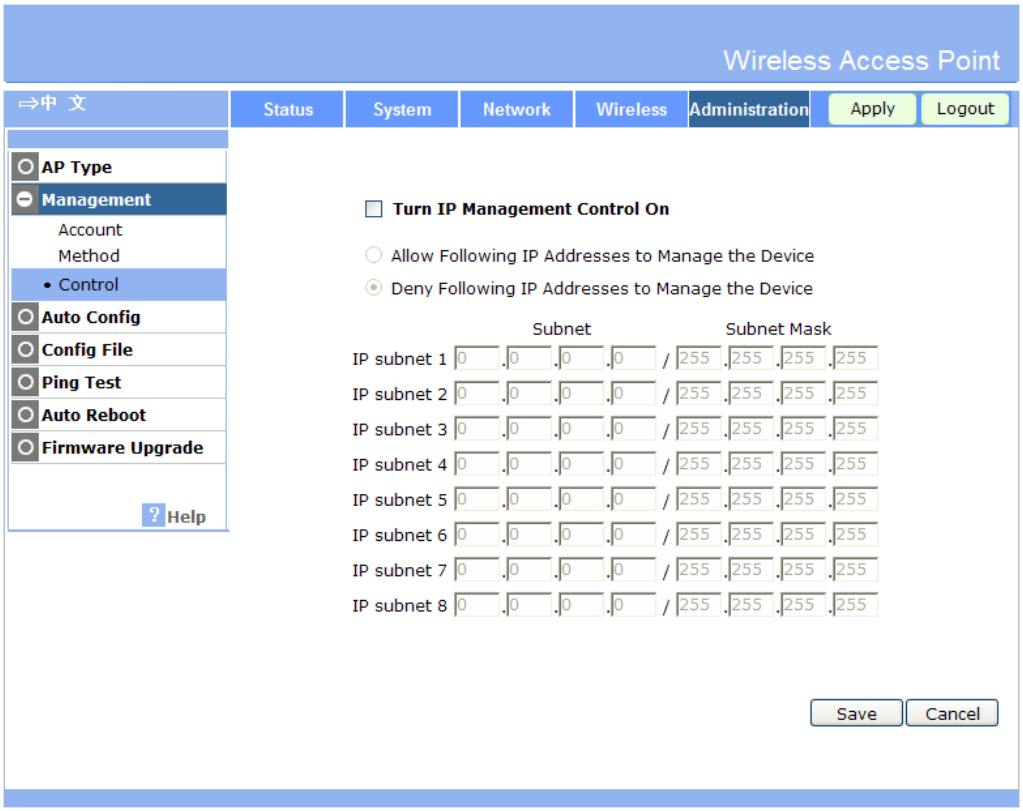

Figure 79: Control Screen

Data - Control Screen

Turn IP Management Control On	Select the desired option, as required • Enable or Disable the Management Control feature. • Select either *Allow following IP addresses to Manage the Device* or *Deny following IP addresses to Manage the Device*. • Enter the physical IP address and Subnet Mask of each Wireless station.

Auto Config

To reach this screen, select *Auto Config* in the **Administration** section of the menu.

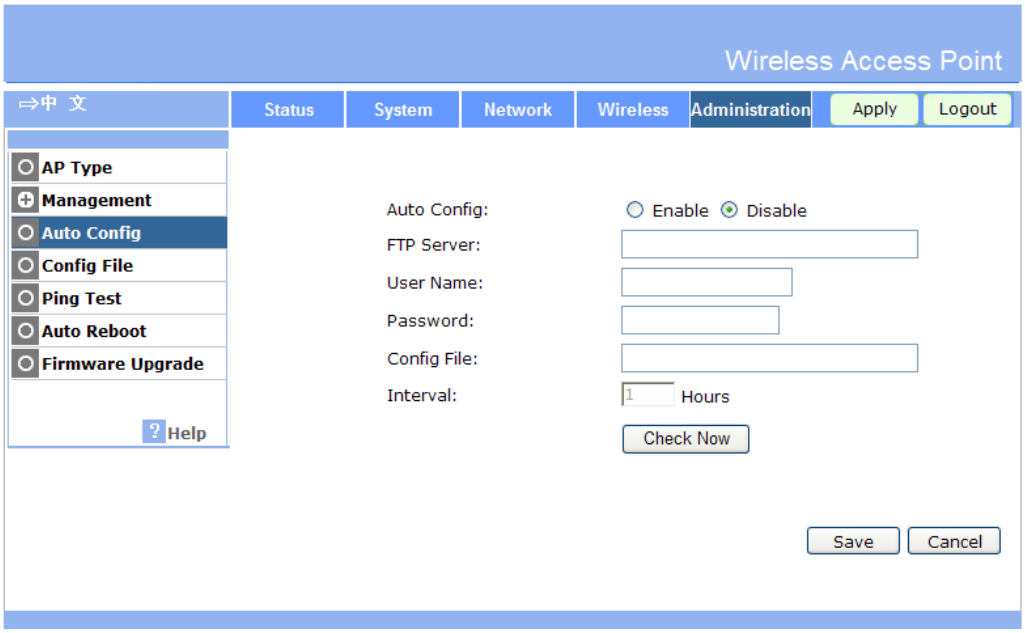

Figure 80: Auto Config Screen

Data - Auto Config Screen

Auto Config	
Auto Config	If enabled, this AP will perform Auto Configuration.
FTP Server	Enter the address for the FTP server.
User Name	Enter the login name for the FTP server.
Password	Enter the login password for the FTP server.
Config File	Enter the full path of the firmware in the FTP server.
Interval	If enabled, the device will check the config file in the time interval. Enter the desired time in the field.

Config File

This screen allows you to Backup (download) the configuration file, and to restore (upload) a previously-saved configuration file.

You can also set the Wireless Access Point back to its factory default settings.

To reach this screen, select *Config File* in the **Management** section of the menu.

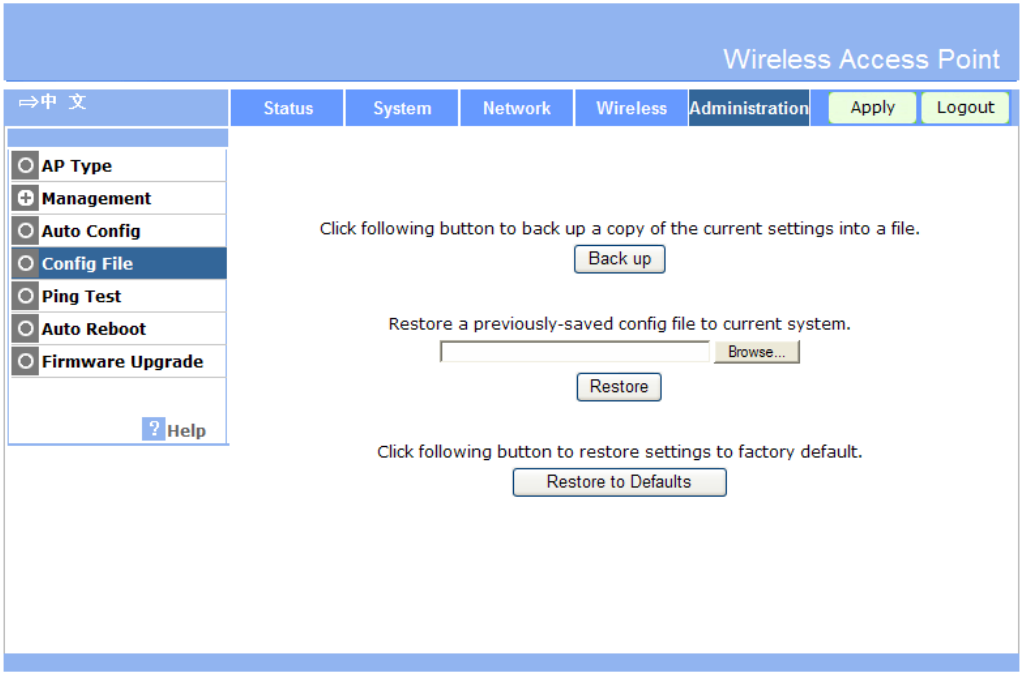

Figure 81: Config File Screen

Data - Config File Screen

Backup	
Back up a copy of the current settings to a file	Once you have the Access Point working properly, you should back up the settings to a file on your computer. You can later restore the Access Point's settings from this file, if necessary. To create a backup file of the current settings: • Click **Back up**. • If you don't have your browser set up to save downloaded files automatically, locate where you want to save the file, rename it if you like, and click **Save**.
Restore	
Restore saved settings from a file	To restore settings from a backup file: 1. Click **Browse**. 2. Locate and select the previously saved backup file. 3. Click **Restore.**

Defaults	
Revert to factory default settings	To erase the current settings and restore the original factory default settings, click **Restore to Defaults** button. **Note!** • This will terminate the current connection. The Access Point will be unavailable until it has restarted. • By default, the Access Point will act as a DHCP client, and automatically obtain an IP address. You will need to determine its new IP address in order to re-connect.

Ping Test

This screen allows you to perform a "Ping". These activities can be useful in solving network problems.

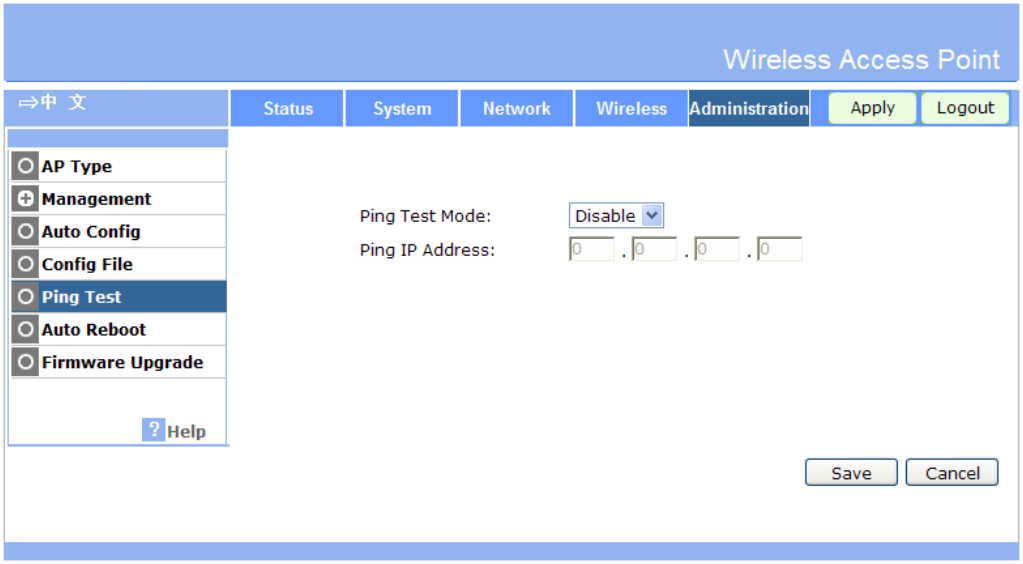

Figure 82: Ping Test Screen

Data - Ping Test Screen

Ping	
Ping Test Mode	Select the desired option from the drop-down list.
Ping IP Address	Enter the IP address you wish to ping. The IP address can be on your LAN, or on the Internet. Note that if the address is on the Internet, and no connection currently exists, you could get a "Timeout" error. In that case, wait a few seconds and try again.

Auto Reboot

If you have a Syslog Server on your LAN, this screen allows you to configure the Access Point to send log data to your Syslog Server.

Figure 83: Auto Reboot Screen

Data - Auto Reboot Screen

Auto Reboot Mode	Select the desired Option: • **Disable** - Auto Reboot feature is not used. • **Enable** - Auto Reboot feature is in use.
Reboot Interval	Enter the desired time for reboot interval.

Firmware Upgrade

The firmware (software) in the Wireless Access Point can be upgraded using your Web Browser.

You must first download the upgrade file, and then select *Upgrade Firmware* in the **Management** section of the menu. You will see a screen like the following.

Figure 84: Firmware Upgrade Screen

To perform the Firmware Upgrade:

1. Click the *Browse* button and navigate to the location of the upgrade file.
2. Select the upgrade file. Its name will appear in the *Firmware File* field.
3. Click the *Upgrade* button to commence the firmware upgrade.

The Wireless Access Point is unavailable during the upgrade process, and must restart when the upgrade is completed. Any connections to or through the Wireless Access Point will be lost.

Chapter 7

Access Point Mode

This Chapter explains configuration and operation when in "Access Point".

Overview

There are two modes available on the ***Device Mode*** screen.

- **Router** - In this mode, this device can provide shared Internet Access to all your LAN users. Also, by default, it acts a DHCP Server, providing an IP address and related information to all Wireless and LAN users.
- **Bridge** - The device links your Wireless Stations to your wired LAN. The Wireless stations and devices on the wired LAN are then on the same network, and can communicate with each other without regard for whether they are connected to the network via a Wireless or wired connection.

This Chapter describes operation while in **Access Point Mode**.

Management Connections

- You need to have a DHCP Server on your LAN to provide IP addresses to the Wireless clients using this Access Point.
- This AP must be a valid device on your LAN, to allow management connections. You must assign a (fixed) IP address which is within the address range used on your LAN, but not within the address range used by your DHCP server.

When you connect in future, just connect normally, using the IP address you assigned.

1. Start your WEB browser.
2. In the *Address* box, enter "HTTP://" and the current IP Address of the Wireless ADSL Modem, as in this example, which uses the Wireless ADSL Modem's default IP Address:

   `HTTP://192.168.0.228`
3. When prompted for the User name and Password, enter `admin` for the user name, and the current password, as set on the password screen. (The password is the same regardless of the mode.)

Home Screen

If in Access Point mode, the home screen will look like the example below.

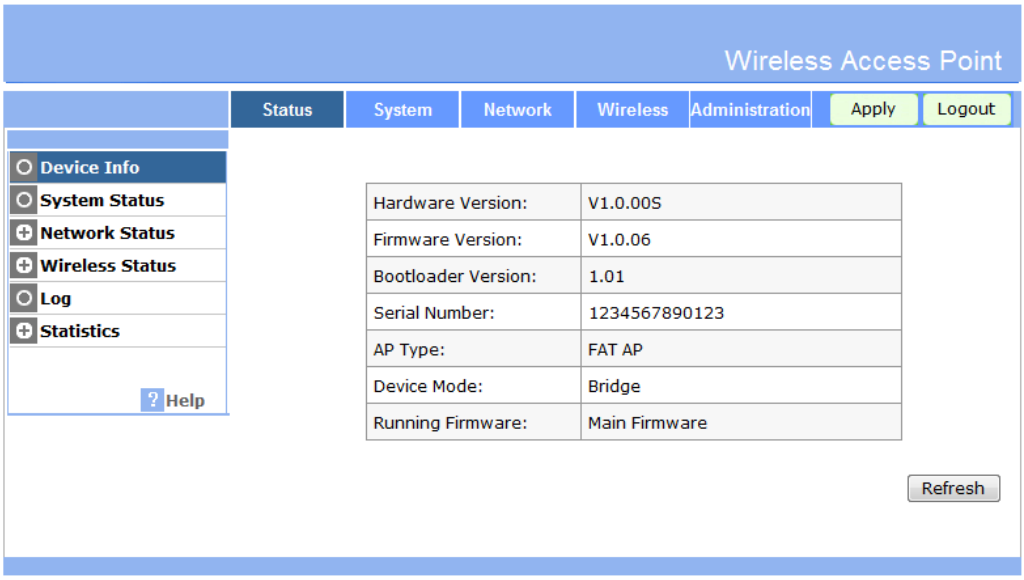

Figure 85: Home Screen - Bridge Mode

Note that the menu has changed, many of the options in Router mode are the same as Bridge mode. The screens available are:

- **Device Mode** - change back to Router mode, if desired.
- **System** - this screen and related sub-screens are the same as in Router mode.
- **Wireless** - this screen and related sub-screens are the same as in Router mode.
- **Administration** - this screen and related sub-screens are the same as in Router mode.
- **Status** - displays current settings and status. See the following section for details.

The following section only describes the screens that are different than those in Router mode.

Device Mode Screen

This screen is used to change back to Router mode, if desired.

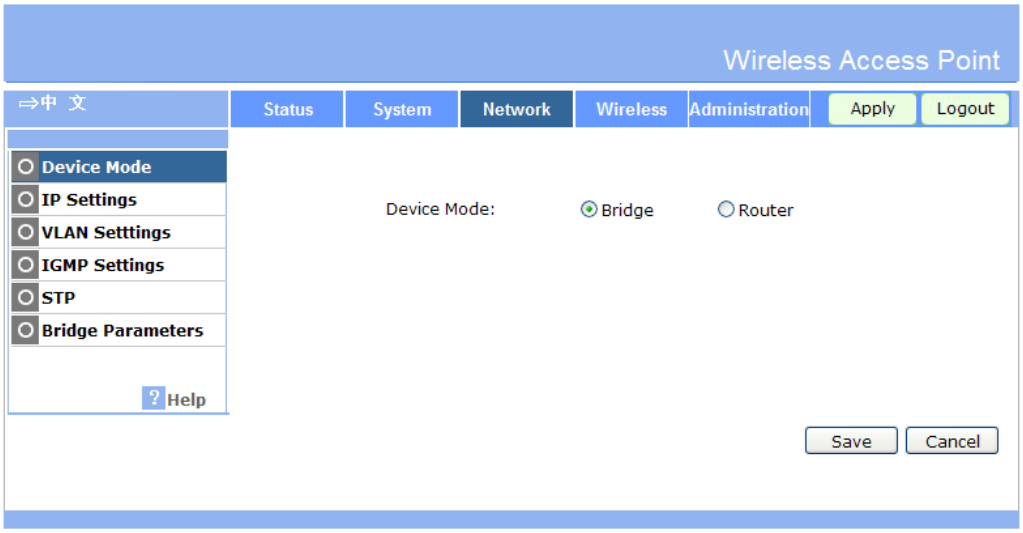

Figure 86: Device Mode Screen

Data - Device Mode Screen

Device Mode	Select the desired device mode for the router: • **Router** - In this mode, this device can provide shared Internet Access to all your LAN users. Also, by default, it acts a DHCP Server, providing an IP address and related information to all Wireless and LAN users. • **Bridge** - The device links your Wireless Stations to your wired LAN. The Wireless stations and devices on the wired LAN are then on the same network, and can communicate with each other without regard for whether they are connected to the network via a Wireless or wired connection. After changing the mode, this device will restart, which will take a few seconds. The menu will also change, depending on the mode you are in.

Status Screen

In Access Point mode, the Status screen looks like the example below.

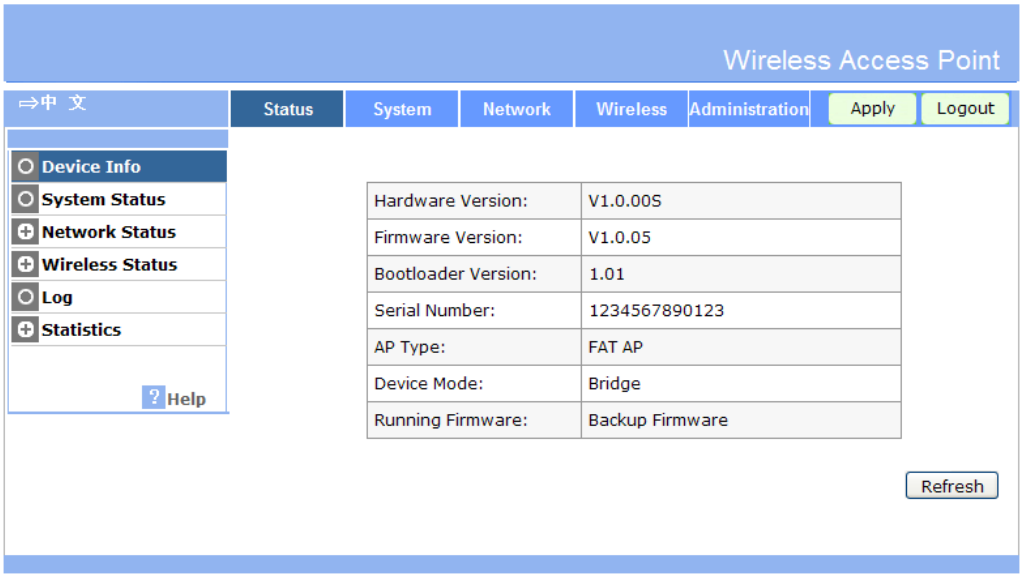

Figure 87: Device Info Screen - Bridge Mode

Data - Device Info Screen (Bridge Mode)

Device Info	
Hardware Version	The version of the hardware currently used.
Firmware Version	The version of the firmware currently installed.
Bootloader Version	The version of the bootloader currently used.
Serial Number	The serial number of the device.
AP Type	The current AP type is displayed.
Device Mode	The current device mode is displayed.
Running Firmware	The currently running firmware is displayed.

VLAN Screen

In Access Point mode, the VLAN screen looks like the example below.

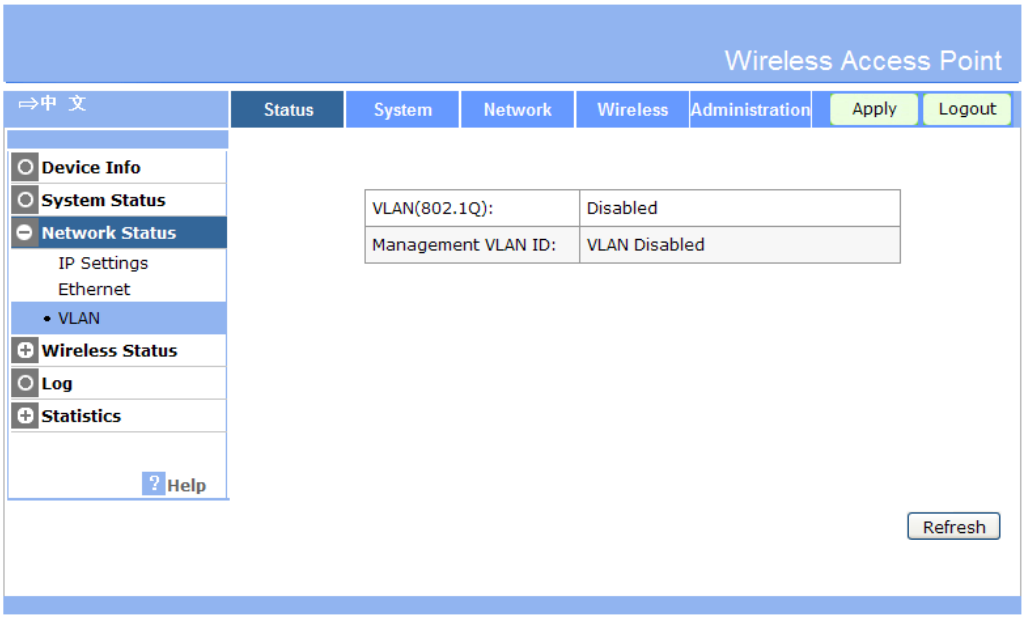

Figure 88: VLAN Screen

Data - VLAN Screen

VLAN	
VLAN(802.1Q)	It displays the status (Enabled or disabled) of VLAN.
Management VLAN ID	It displays the VLAN ID of Management VLAN.

Appendix A

Specifications

Wireless Access Point

Hardware Specifications

LAN port	1 x RJ45 auto-sensing 10/100/1000BASE-TX Ethernet with 802.3af+ PoE. Can support Full Duplex and Half Duplex transfer function.
Antennae	4 external omni antennas
Operating Temperature	-10° C to 50° C
Operating Humidity	10% - 90% non-condensing
Power Adapter	12V/1A External
Console Port	1 x RJ45-base Console

Wireless Interface

Standards	IEEE 802.11a/b/g/n 2.4GHz/5GHz
Radio Chains	2x2
Spatial Streams	2
Channelization	20MHz and/or 40MHz
Frequency Band	2.4 – 2.484 GHz and 5.15 – 5.85 GHz
Operating Channels	US/Canada: 1-11 Europe/China/Japan: 1-13 5GHz channels: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165
BSSID	Up to 16 per Radios (32 total)
Power Save	Supported
Wireless Security	WEP, WPA-PSK, WPA-TKIP, WPA2 AES, 802.11i
RF Power	20dBm at max
Receive Sensitivity	-91dBm @802.11b -89dBm @802.11a/g -83dBm @802.11n
Performance	160Mbps per band

Connectivity	Up to 128 clients per band (256 total)

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operation.

FCC RF Radiation Exposure Statement

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

Appendix B

Troubleshooting

Overview

This chapter covers some common problems that may be encountered while using the Wireless Access Point and some possible solutions to them. If you follow the suggested steps and the Wireless Access Point still does not function properly, contact your dealer for further advice.

General Problems

Problem 1: **Can't connect to the Wireless Access Point to configure it.**

Solution 1: Check the following:

- The Wireless Access Point is properly installed, LAN connections are OK, and it is powered ON. Check the LEDs for port status.
- Ensure that your PC and the Wireless Access Point are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- You can use the following method to determine the IP address of the Wireless Access Point, and then try to connect using the IP address, instead of the name.

To Find the Access Point's IP Address

1. Open a MS-DOS Prompt or Command Prompt Window.
2. Use the Ping command to “ping” the Wireless Access Point. Enter `ping` followed by the Default Name of the Wireless Access Point. e.g.

   ```
   ping SC003318
   ```

3. Check the output of the ping command to determine the IP address of the Wireless Access Point, as shown below.

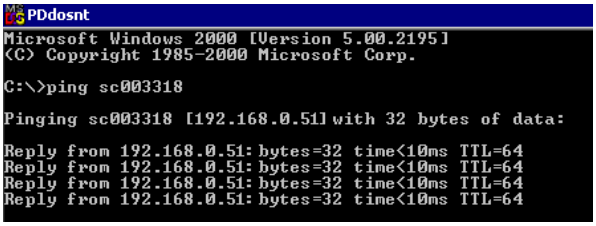

Figure 89: Ping

If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address which is compatible with the Wireless Access Point. (If no DHCP Server is found, the Wireless Access Point will default to an IP Address and Mask of 192.168.0.228 and 255.255.255.0.) On Windows PCs, you can use *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Problem 2: **My PC can't connect to the LAN via the Wireless Access Point.**

Solution 2 Check the following:

- The SSID and WEP settings on the PC match the settings on the Wireless Access Point.
- On the PC, the wireless mode is set to "Infrastructure"
- If using the *Access Control* feature, the PC's name and address is in the *Trusted Stations* list.
- If using 802.1x mode, ensure the PC's 802.1x software is configured correctly. See Chapter 4 for details of setup for the Windows XP 802.1x client. If using a different client, refer to the vendor's documentation.

Appendix C

About Wireless LANs

Overview

Wireless networks have their own terms and jargon. It is necessary to understand many of these terms in order to configure and operate a Wireless LAN.

Wireless LAN Terminology

Modes

Wireless LANs can work in either of two (2) modes:

- Ad-hoc
- Infrastructure

Ad-hoc Mode

Ad-hoc mode does not require an Access Point or a wired (Ethernet) LAN. Wireless Stations (e.g. notebook PCs with wireless cards) communicate directly with each other.

Infrastructure Mode

In Infrastructure Mode, one or more Access Points are used to connect Wireless Stations (e.g. Notebook PCs with wireless cards) to a wired (Ethernet) LAN. The Wireless Stations can then access all LAN resources.

Access Points can only function in "Infrastructure" mode, and can communicate only with Wireless Stations which are set to "Infrastructure" mode.

SSID/ESSID

BSS/SSID

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).

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).

ESS/ESSID

A group of Wireless Stations, and multiple Access Points, all using the same ID (ESSID), form an Extended Service Set (ESS).

Different Access Points within an ESS can use different Channels. To reduce interference, it is recommended that adjacent Access Points SHOULD use different channels.

As Wireless Stations are physically moved through the area covered by an ESS, they will automatically change to the Access Point which has the least interference or best performance. This capability is called **Roaming**. (Access Points do not have or require Roaming capabilities.)

Channels

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. For 802.11g, 13 channels are available in the USA and Canada, but 11channels are available in North America if using 802.11b.
- If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference. The recommended Channel spacing between adjacent Access Points is 5 Channels (e.g. use Channels 1 and 6, or 6 and 11).
- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)
- If using "Ad-hoc" mode (no Access Point), all Wireless stations should be set to use the same Channel. However, most Wireless stations will still scan all Channels to see if there is an existing "Ad-hoc" group they can join.

WEP

WEP (Wired Equivalent Privacy) is a standard for encrypting data before it is transmitted. This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.

If WEP is used, the Wireless Stations and the Wireless Access Point must have the same settings.

WPA-PSK

Like WEP, data is encrypted before transmission. WPA is more secure than WEP, and should be used if possible. The PSK (Pre-shared Key) must be entered on each Wireless station. The 256Bit encryption key is derived from the PSK, and changes frequently.

WPA2-PSK

This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption.

WPA-Enterprise

This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard.

If this option is used:

- The Access Point must have a "client login" on the Radius Server.
- Each user must have a "user login" on the Radius Server.
- Each user's wireless client must support 802.1x and provide the login data when required.

All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required.

802.1x

This uses the 802.1x standard for client authentication, and WEP for data encryption. If possible, you should use WPA-Enterprise instead, because WPA encryption is much stronger than WEP encryption.

If this option is used:

- The Access Point must have a "client login" on the Radius Server.
- Each user must have a "user login" on the Radius Server.
- Each user's wireless client must support 802.1x and provide the login data when required.
- All data transmission is encrypted using the WEP standard. You only have to select the WEP key size; the WEP key is automatically generated.

Appendix D

Command Line Interface

Overview

If desired, the Command Line Interface (CLI) can be used for configuration. This creates the possibility of creating scripts to perform common configuration changes. The CLI requires a Telnet connection to the Wireless Access Point.

Using the CLI - Telnet

1. Start your Telnet client, and establish a connection to the Access Point.
   e.g.
   ```
   Telnet 192.168.0.228
   ```
2. You will be prompted for the user name and password. Enter the same login name and password as used for the HTTP (Web) interface.
   The default values are **admin** for the User Name, and **password** for the Password.
3. Once connected, you can use any of the commands listed in the following **Command Reference**.

Command Reference

The following commands are available.

config vap	Config Virtual AP X
?	Display CLI Command List
help	Display CLI Command List
get 11nampdu	Set 11n A-MPDU Aggregation Mode
get 11namsdu	Set 11n A-MSDU Aggregation Mode
get 11nguardinterval	Set 11n Guard Interval Mode
get 11nsubchannel	Set 11n Extension Sub-Channel
get 11nradioband	Set 11n Radio Band
get 802.11d	Display 802.11d Mode
get acctserver	Display Accounting Server
get acctport	Display Accounting Port
get acctsecret	Display Accounting Secret
get acl	Display Access Control Status
get active	Display VAP Active (up) Mode
get aging	Display Idle Timeout Interval
get authentication	Display Authentication Type of WEP

get beaconinterval	Display Beacon Interval
get channel	Display Radio Channel
get country	Display Country/Domain
get defaultkey	Display Default Key Index
get description	Display Access Point Description
get dhcp	Display DHCP Mode
get dhcpserverendip	Display DHCP Server End IP Address
get dhcpserverstartip	Display DHCP Server start IP Address
get dnsserver	Display IP Address of DNS Server
get dot1xdynkeyupdate	Display 802.1x Dynamic Key Update Mode
get dot1xdynkeylife	Display 802.1x Dynamic Key Life Time (in Minutes)
get dot1xkeytype	Display 802.1x Distribute Key Method
get fragthreshold	Display Fragment Threshold
get gateway	Display Gateway IP Address
get gtkupdate	Display Group Key Update Mode
get gtkupdateinterval	Display Group Key Update Interval (in Seconds)
get http	Display HTTP Mode
get httpport	Display HTTP Port Number
get https	Display HTTPS Mode
get httpsport	Display HTTPS Port Number
get ipaddr	Display IP Address
get ipmask	Display IP Subnet Mask
get isolation	Display Isolate All Virtual APs State
get key	Display WEP Key Value
get keylength	Display WEP Key Length
get lltd	Display LLTD Mode
get md5supplicant	Display 802.1x MD5 Supplicant Mode
get md5suppname	Display 802.1x Supplicant MD5 Name
get md5supppassword	Display 802.1x Supplicant MD5 Password
get md5supptype	Display 802.1x MD5 Supplicant Type
get nativevlanid	Display Native VLAN ID
get ntp	Display NTP Server IP Address
get operationmode	Display Operation Mode
get password	Display Login Password

get psk	Display Pre-shared Key
get radiusserver	Display RADIUS Server IP Address
get radiusport	Display RADIUS Port Number
get radiussecret	Display RADIUS Shared Secret
get remoteptmp	Display PTMP's Remote MAC Address List
get remoteptp	Display PTP's Remote MAC Address
get roguedetect	Display Rogue AP Detection Mode
get rogueinteval	Display Interval of Every Rogue AP Detection
get roguelegal	Display Legal AP List of Legal AP
get roguetrap	Display Rogue AP Detection Send SNMP Trap Mode
get roguetype	Display Rogue AP Definition
get rtsthreshold	Display RTS/CTS Threshold
get security	Display Wireless Security Mode
get shortpreamble	Display Short Preamble Usage
get snmpreadcommu-nity	Display SNMP Read Community
get snmpwritecommu-nity	Display SNMP Write Community
get snmpmode	Display SNMP Mode
get snmpmanagemode	Display SNMP Manager Mode
get snmptrapmode	Display SNMP Trap Mode
get snmptrapversion	Display SNMP Trap Version
get snmpv3username	Display SNMP v3 User Name
get snmpv3authproto	Display SNMP v3 Authentication Protocol
get snmpv3authkey	Display SNMP v3 Authentication Key
get snmpv3privproto	Display SNMP v3 Private Protocol
get snmpv3privkey	Display SNMP v3 Private Key
get ssid	Display Service Set ID
get ssidbroadcast	Display SSID Broadcast Mode
get stp	Display STP Mode
get strictgtkupdate	Display Group Key Update Strict Status
get syslog	Display Syslog Mode
get syslogport	Display Syslog Port
get syslogserver	Display Unicast Syslog Server Address
get syslogseverity	Display Syslog Severity Level

get systemname	Display Access Point System Name
get telnet	Display Telnet Mode
get time	Display Current System Time
get timezone	Display Time Zone Setting
get uptime	Display Access Point Up Time
get username	Display Login User Name
get vapname	Display Virtual AP Name
get version	Display Firmware Version
get vlan	Display VLAN Operational State
get vlanid	Display the VLAN ID
get wirelessmode	Display Wireless LAN Mode
get wirelessseparate	Display Wireless Separate Mode
get wmm	Display WMM Mode
get wmmnoack	Display WMM No Acknowledgement status
set 11nampdu	Set 11n A-MPDU Aggregation Mode
set 11namsdu	Set 11n A-MSDU Aggregation Mode
set 11nguardinterval	Set 11n Guard Interval Mode
set 11nsubchannel	Set 11n Extension Sub-Channel
set 11nradioband	Set 11n Radio Band
set 802.11d	Set 802.11d Mode
set acctserver	Set Accounting Server
set acctport	Set Accounting Port
set acctsecret	Set Accounting Secret
set acl	Set Access Control
set active	Set Active (up) Mode
set aging	Set Idle Timeout Interval
set authentication	Set Authentication Type of WEP
set beaconinterval	Set Beacon Interval
set channel	Set Radio Channel
set country	Set Country/Domain
set defaultkey	Set Default Key Index
set description	Set Access Point Description
set dhcp	Set DHCP Mode
set dhcpserverendip	Set DHCP Server End IP Address
set dhcpserverstartip	Set DHCP Server start IP Address

set dnsserver	Set DNS Server IP Address
set dot1xdynkeyupdate	Set 802.1x Dynamic Key Update Mode
set dot1xdynkeylife	Set 802.1x Dynamic Key Life Time (in Minutes)
set dot1xkeytype	Set 802.1x Distribute Key Method
set fragthreshold	Set Fragment Threshold
set gateway	Set Gateway IP Address
set groupkeyupdate	Set Group Key Update Mode
set groupkeyupdatein-terval	Set Group Key Update Interval (in Minutes)
set http	Set HTTP Mode
set httpport	Set HTTP Port Number
set https	Set HTTPS Enable/Disable
set httpsport	Set HTTPS Port Number
set ipaddr	Set IP Address
set ipmask	Set IP Subnet Mask
set isolation	Set Isolate All Virtual APs State
set key	Set WEP Key Value
set keylength	Set WEP Key Length
set lltd	Set LLTD Mode
set md5supplicant	Set 802.1x MD5 Supplicant Mode
set md5suppname	Set 802.1x Supplicant MD5 Name
set md5supppassword	Set 802.1x Supplicant MD5 Password
set md5supptype	Set 802.1x MD5 Supplicant Type
set nativevlanid	Set Native VLAN ID
set ntp	Set NTP Server IP Address
set operationmode	Set operation Mode
set password	Modify Login Password
set psk	Modify Pre-shared Key
set radiusserver	Set RADIUS IP Address
set radiusport	Set RADIUS Port Number
set radiussecret	Set RADIUS Shared Secret
set remoteptmp	Set PTMP's Remote MAC Address List
set remoteptp	Set Remote PTP MAC Address
set roguedetect	Set Rogue AP Detection Mode
set rogueinteval	Set Interval of Rogue AP Detection (Range: 3 ~ 99)

set roguelegal	Add/Delete Legal AP MAC/OUI
set roguesnmp	Set Rogue AP Detection SNMP Trap Mode
set roguetype	Set Rogue AP Definition
set rtsthreshold	Set RTS/CTS Threshold
set security	Set Wireless Security Mode
set shortpreamble	Set Short Preamble
set snmpreadcommunity	Set SNMP Read Community
set snmpwritecommunity	Set SNMP Write Community
set snmpmode	Set SNMP Mode
set snmpmanagemode	Set SNMP Manager Mode
set snmptrapmode	Set SNMP Trap Mode
set snmptrapversion	Set SNMP Trap Version
set snmpv3username	Set SNMP v3 User Name
set snmpv3authproto	Set SNMP v3 Authentication Protocol
set snmpv3authkey	Set SNMP v3 Authentication Key
set snmpv3privproto	Set SNMP v3 Private Protocol
set snmpv3privkey	Set SNMP v3 Private Key
set ssid	Set Service Set ID
set ssidsuppress	Set SSID Broadcast Mode
set stp	Set STP Mode
set strictgtkupdate	Set Group Key Update Strict Status
set syslog	Set Syslog Mode
set syslogport	Set Syslog Port
set syslogserver	Set Unicast Syslog Server Address
set syslogseverity	Set Syslog Severity Level
set systemname	Set Access Point System Name
set telnet	Set Telnet Mode
set timezone	Set Time Zone Setting
set username	Modify Login User Name
set vlan	Set VLAN Operational State
set vlanid	Set the VLAN Tag
set wirelessmode	Set Wireless LAN Mode
set wirelessseparate	Set Wireless Separate Mode

set wmm	Set WMM Mode
set wmmnoack	Set WMM No Acknowledge
factoryrestore	Restore to Default Factory Settings
apply	To make the changes take effect
exit	Quit the telnet