# VX-AP320NA 11n Dual Band Wireless Access Point

# **User's Guide**

CHAPTER 1 INTRODUCTION	1
Features of your Wireless Access Point	1
Package Contents	3
Physical Details	4
CHAPTER 2 INSTALLATION	7
Requirements	
Procedure	7
CHADTED 3 ACCESS DOINT SETUD	0
Ovorviow	9
Over view	9
Setup using a web blowser Systam Basic Sattings Screen	
System - Dask Settings Screen	11
System - SNMP Settings	13
System I og Sattings	15
Wiralass – Rosic Sattings Screen	10
Wireless - Dasie Settings Sereen Wireless - Virtual APs Screen	····· 17 22
Wireless - Virtual AI's Scittings	37
Wireless - Access Control	
Wireless - Advanced Settings	
Natwork ID Sattings Screen	
Network - II Settings Screen	 51
Network - VLAN Settings Screen	51 52
Network - STT Screen	
Network - Reidae Peremeters Screen	55
Retwork - Druge rarameters Screen	
CHAPTER 4 PC AND SERVER CONFIGURATION	55
Overview	55
Using WEP	55
Using WPA-PSK/WPA2-PSK	56
Using WPA-Enterprise	
802.1x Server Setup (Windows 2000 Server)	58
Using 802.1x Mode (without WPA)	68
CHAPTER 5 OPERATION AND STATUS	69
Status Screen	69
CHAPTER 6 ACCESS POINT MANAGEMENT	79
Overview	79
АР Туре	79
Management Screen	81
Auto Čonfig	84
Config File	85
Ping Test	87
Auto Reboot	88
Firmware Upgrade	89
CHAPTER 7 ACCESS POINT MODE	90
Overview	90
Management Connections	90
Home Screen	
Device Mode Screen	
Status Screen	
ADDENDLY A SDECIEICATIONS	
Windows A previrt Data Daint	
wireless Access Point	

APPENDIX B TROUBLESHOOTING	
Overview	
General Problems	
APPENDIX C ABOUT WIRELESS LANS	
Overview	
Wireless LAN Terminology	
APPENDIX D COMMAND LINE INTERFACE	
Overview	
Command Reference	

P/N: VX-AP320NA

Copyright © 2013. All Rights Reserved.

Document Version: 1.0

All trademarks and trade names are the properties of their respective owners.

# Chapter 1 Introduction



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

Congratulations on the purchase of your new VX-AP320NA 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.





#### 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.** Dynamic Host Configuration Protocol 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.

# Package Contents

The following items should be included:

- Wireless Access Point
- Two 5G Detachable Antennas
- Two 2.4G Detachable Antennas
- Quick Start Guide

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	<b>On</b> - Error condition.
	Off - Normal operation.
	Blinking - During start up, and when the Firmware is being upgraded.
Power	<b>On</b> - Normal operation.
	Off - No power
Ethernet	<b>On</b> - Corresponding LAN (hub) port is active.
	Off - No active connection on the corresponding LAN (hub) port.
	<b>Flashing</b> - Data is being transmitted or received via the corresponding LAN (hub) port.
2.4 GHz	<b>On</b> - Wireless connection is available in 2.4GHz mode.
	<b>Off</b> - Wireless connection is not available in 2.4GHz mode.
	<b>Flashing</b> - Data is being transmitted or received via the Wireless access point. Data includes "network traffic" as well as user data.
5 GHz	<b>On</b> - Wireless connection is available in 5GHz mode.
	Off - Wireless connection is not available in 5GHz mode.
	<b>Flashing</b> - 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.

8	Ô		O Reset	Console		Power	
		]	Figure 3	: Rear Pa	nel		

**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 ٠ ALL data and restore ALL settings to the factory default values. To Clear All Data and restore the factory default values: Hold the Reset Button until the Status (Red) LED blinks TWICE, 1. 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, and 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:

#### APxxxxx

Where  $\times \times \times \times \times \times$  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.

		,	Wireless Access Point
Please log in	to continue	⇒中文	
Username:	admin		
Password:	•••••	Log in	

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  $192.168.0.1 \sim 192.168.0.254$ , 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.

					Wireles	s Acces	s Point	
⇒中文	Status	System	Network	Wireless	Administration	Apply	Logout	
O Basic Settings O Time Settings O SNMP Settings C Log Settings	Access Point Name Description: Country/Domain:			AP4F2B34 United States				
? Help					C	Save	Cancel	

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

					Wirele	ss Acces	s Point		
⇔中 文	Status	System	Network	Wireless	Administratio	n Apply	Logout		
O Basic Settings									
O Time Settings	C	) Manually							
SNMP Settings		Date	Jan 🗡 1	✓ 2008 ✓					
Log Settings		Time	0:0	: 0					
	۲	Automatically							
2 Help		Current Time	e: 1970-01-01	00:02:24					
		Time Zone:	(GMT+08:00) Ta	aipei		~			
		Automat	tically adjust cl	ock for dayli <u>c</u>	ght saving chan	ges			
		Use Define	d NTP Server:	O Yes	s 💿 No				
		NTP Server	Name/IP Addr	-ess.		_			
		NTD Server	Port:	123	(1 65524)				
		INTE Server	Port.	125	(1-05554)				
						Save	Cancel		

Figure 9: 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.						
	<ul> <li>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.</li> </ul>						
	• 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**

					Wireles	s Acces	s Point		
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout		
O Basic Settings									
O Time Settings	SN	MP v1/v2c/v3:		Enable 💌					
SNMP Settings	Co	ntact:							
• Basic	De	vice Name:		AP4F2B34 public					
SNMPv3 SNMP Trap	Lo	cation:							
Log Settings	Re	ad Only Comm	nunity:						
? Help	Re	ad/Write Com	munity:	private					
						Save	Cancel		

#### Figure 10: 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.

#### **Data - Basic Screen**

#### SNMPv3

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
<ul> <li>Basic Settings</li> <li>Time Settings</li> <li>SNMP Settings</li> <li>Basic</li> <li>SNMPV3</li> <li>SNMP Trap</li> <li>Log Settings</li> </ul>	Us Au Pri Pri	ername: thentication Pr thentication Kr vacy Protocol: vacy Key:	rotocol: ey:	None			
? Help							
						Save	Cancel

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.
<b>Privacy Protocol</b>	Select the private protocol as required.
Privacy Key	Enter the private key here.

# SNMP Trap

						VVireles	s Acces	s Point
⇒中 文	Status	System	Netv	vork	Wireless	Administration	Apply	Logout
O Basic Settings								
O Time Settings	Trap 9	Server						
SNMP Settings	-		1	•	0			
Basic	Serve	er 1:		0	. 0			
SNMPv3	Serve	er 2:		0	. 0	. 0 . 0		
SNMP Trap	Serve	r Port:		162	(1-65534	L)		
Log Settings	Trap I	Periods:	ĺ	24	hours (1-	-65535)		
2 Help	Trap	[hreshold						
	Rate	of CPU Utilizat	tion:		80	%(1-100	)	
	Rate	of Memory Util	lization		80	%(1-100	)	
						ſ	Save	Cancel
						L		Cancer

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 $(1 \sim 65535)$ .
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.

					Wirele	ss Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
<ul> <li>Basic Settings</li> <li>Time Settings</li> <li>SNMP Settings</li> <li>Log Settings</li> <li>Syslog</li> <li>Mail Alarta</li> </ul>		S) Se S)	rslog Mode: erver Name/IP rslog Port:	Address:	Disabled 0.0.0.0 514	×	
Log Types						Save	Cancel

Figure 13: Syslog Settings Screen

#### **Data - Syslog Settings Screen**

Syslog Mode	Select the desired Option:				
	• <b>Disabled</b> - Syslog server is not used.				
	• <b>Broadcast</b> - 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**

⇒中 文	Status	System	Network	Wireless	Wireles	s Acces	s Point
O Basic Settings	Fm	ail Alorta		Disphle M			
	EIII	all Alerts:		Disable 💌			
SNMP Settings	Log	g Queue Leng	th:	20 ent	ries (1 - 500)		
Log Settings	Loc	Time Thresh	old:	600 sec	onds (60 - 600)		
Syslog						-	
Mail Alerts	SM	IP Mall Server	r:			_	
Log Types	Em	ail Address fo	r Alert Logs:				
? Help				E-mail Lo	ng Now	Save	Cancel

Figure 14: 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 deter- mine 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.

#### Data - Mail Alerts Screen

# Log Types

→中 文	Status	System	Network	Wireless	Wireles	Acces	s Point
<ul> <li>Basic Settings</li> <li>Time Settings</li> <li>SNMP Settings</li> <li>Log Settings</li> <li>Syslog Mail Alerts</li> </ul>	♥ Un ♥ Un ♥ Sy: ♥ Fire	authorized Lo authorized Wi stem Error Me: ewall Log	gin Attempt reless Attempt ssages	☑ Authori t ☑ Authori ☑ Web Ac	zed Login zed Wireless Cor ccess and Configu	nnection uration Chan	iges
<ul> <li>Log Types</li> </ul>							
? Help					C	Save	Cancel

Figure 15: 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 unauthor- ized users who attempted to login to the Access Point are logged.
	• Authorized Login - If checked, this will log the author- ized 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.
	• <b>Firewall Log</b> - If checked, the firewall message will be logged.

## Data - Log Types Screen

# Wireless - Basic Settings Screen

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

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

					Wireless	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O Basic Settings							
O Vitrual APs	Wir	eless Radio:	Radio 1 (2	2.4G) 🔽			
Radius	Rad	lio Function:	Disable 💌	•			
O Access Control	Wir	eless Mode:	Mixed 802		b and 802.11g 🔽		
Advanced Settings	Aut	o Channel Sca	n: Disable 🛛				
	Cha	annel/Frequen	cy: 6 🗸				
? Help	Tra	nsmit Data Ra	te: Best	~			
	11N Rat	l Transmit Dat e:	a Best	*			
	Bas	ic Rate:	⊻1 ⊻:	2 🗹 5.5 🗌	6 9 11	L	
	Sup	port Rate:		18 ⊇ 24 2 ⊻ 5.5 ⊻	36 48 54 6 ⊻9 ⊻11	↓ ↓	
	11N	MCS:	<ul> <li>✓ 12</li> <li>✓ 12</li> <li>✓ 0</li> <li>✓ 1</li> <li>✓ 8</li> <li>✓ 9</li> </ul>	18 ⊻ 24 ⊻ . ⊻ 2 ⊻ 3 . ▼ 10 ▼ 1	136 ⊻48 ⊻54 3 ⊻4 ⊻5 11 ⊻12 ⊻13	₩ 16 ₩ 7 14 ₩ 1	5
	Aut	o Power:	Disable V	1			-
	Out	put Power:	-1dB (79%	6) 🗸			
	Cha Bar	annel idwidth:	Auto - 20/	40MHz 🚩			
	Ext Cha	ension Sub- annel:	Above Pri	mary Channe	I 🕶		
						Save	Cancel

Figure 16: Basic Settings Screen

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

Wireless Mode	For 5G, select the desired option:
	• <b>802.11a Only (5G)</b> - 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.
	• <b>802.11n Only (5G)</b> - 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.
	• <b>802.11a and 802.11n (5G)</b> - this will allow connections by both 802.11a and 802.11n wireless stations.
	For 2.4G, select the desired option:
	• <b>802.11b only (2.4G)</b> - 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.
	• <b>802.11g only (2.4G)</b> - 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.
	• <b>802.11n only (2.4G)</b> - 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.
	• <b>802.11b and 802.11g (2.4G)</b> - this will allow connections by both 802.11b and 802.11g wireless stations.
	• <b>802.11n and 802.11g (2.4G)</b> - 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. Higher levels will give a greater range, but are also more likely to cause interference with other devices. Can support -1dB~-16dB, step is 1dB.

Channel Bandwidth	Select the desired bandwidth from the list.
Extension Sub-Channel	Select Above or Below Primary Channel from the list.

# Wireless - Virtual APs Screen

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

					Wireless	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
<ul> <li>⇒ ₱ 文</li> <li>Basic Settings</li> <li>∨itrual APs</li> <li>Radius</li> <li>Access Control</li> <li>Advanced Settings</li> <li>? Help</li> </ul>	Status Virtual VAP VAP VAP VAP VAP VAP VAP VAP	System AP Settings P-Name-1 [Wire -Name-2 [Wire -Name-5 [Wire -Name-7 [Wire -Name-7 [Wire -Name-8 [Wire -Name-9 [Wire -Name-9 [Wire -Name-9 [Wire -Name-9 [Wire	Network Wireless Ra VAP Nar reless-2.4G-2] Neless-2.4G-3 Neless-2.4G-4 Neless-2.4G-6 Neless-2.4G-6 Neless-2.4G-6 Neless-2.4G-9 N	Wireless dio: Radio 1 me [SSID] Se None None None None None None None Configure ne virtual AP	Administration (2.4G) (	Apply	Cancel

Figure 17: 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	<ul> <li>All available VAPs are listed. Up to 16 VAPs/Radios can be supported. For each VAP, the following data is displayed: <ul> <li>*</li> <li>If displayed before the name of the VAP, this indicates the VAP is currently enabled. If not displayed, the VAP is currently disabled.</li> <li>VAP Name The current VAP name is displayed.</li> <li>[SSID] The current SSID associated with this VAP.</li> <li>Security System The current security system (e.g. WPA-PSK) is dis-</li> </ul> </li> </ul>		
	played.		
Enable Button	Enable the selected VAP.		
<b>Configure Button</b>	Change the settings for the selected VAP.		
<b>Disable Button</b>	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 communi- cate 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.

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
<ul> <li>⇒中文</li> <li>● Basic Settings</li> <li>○ Vitrual APs</li> <li>● Radius</li> <li>○ Access Control</li> <li>● Advanced Settings</li> <li>? Help</li> </ul>	Status Basic Se VAP Nar SSID: Broadca Isolation Max Sta Number VAP Rat Max Ups Station Max Ups Security	System ettings me: ast SSID: n within VAP: tion : te Limit wnstream Rate: Rate Limit wnstream Rate: stream Rate: y System:	VAP-Nam         Wireless-2 <ul> <li>Enabl</li> <li>Disable</li> <li>0</li> </ul> 0         e:       0         0       0         e:       0         0       0         o       0         o       0         o       0         o       0         o       0         o       0	Wireless           e-1           2.4G-1           e         Disable           (0-64)           Kbps (0-2000           Kbps (0-2000           Kbps (0-2000           Kbps (0-2000	Administration 000) 000) 000) 000) Back	Apply	Logout

Figure 18: 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.
<b>Broadcast SSID</b>	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 Setting	ys - 1101	Ie							
					Wireless	s Acces	s Point		
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout		
O Basic Settings									
O Vitrual APs	Basic S	ettings							
Radius	VAP Nar	ne:	VAP-Nam	e-1					
O Access Control	CCID		Wiroloss	1					
Advanced Settings	SSID:		Wireless-	1					
	Broadcast SSID:		Enable	💿 Enable 🔘 Disable					
? Help	Isolation within VAP:		Disable	Disable 💌					
	Max Station Number:		0	0 (0-64)					
	VAP Rat	te Limit							
	Max Dov	wnstream Rate	e: 0	Kbps (0-200	000)				
	Max Ups	stream Rate:	0	Kbps (0-200	000)				
	Station	Rate Limit							
	Max Dov	wnstream Rate	2: 0	Kbps (0-200	000)				
	Max Upstream Rate:		0	Kbps (0-200	000)				
	Security	/							
	Security	System:	None		*				
					Back	Save	Cancel		

#### **Security Settings - None**

Figure 19: 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.

					Wireless	s Access	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O Basic Settings O Vitrual APs	Basic S	ettings					
Radius Access Control Advanced Settings Help	VAP Nar SSID: Broadca Isolatio Max Sta Number <b>VAP Ra</b> t Max Do Max Up:	ne: ast SSID: n within VAP: ition : <b>te Limit</b> wnstream Rate:	VAP-Nam Wireless- © Enabl Disable 0 ::: 0 0	e-1 1 e O Disable v (0-64) Kbps (0-200 Kbps (0-200	90000)		
	Station Max Do Max Up Security Security Data En Authent	Rate Limit wnstream Rate: stream Rate: y v System: cryption: cication:	2: 0 0 WEP 64 bit 1 Open Sys	Kbps (0-200 Kbps (0-200 • •	0000) 0000) V		
	WEP Ke Key inpu Key 1: Key 2: Key 3: Key 4: Passphi	eys ut: ⊙ ⊙ rase:	<ul> <li>Hex (0</li> <li>12345674</li> <li>12345674</li> <li>12345674</li> <li>12345674</li> </ul>	I~9 and A~F) 890 890 890 890	Generate Key	Save	Cancel

Figure 20: 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.
	• <b>128 Bit Encryption</b> - Keys are 26 Hex (13 ASCII) characters.
	• <b>152 Bit Encryption</b> - 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.

					Wireles	s Acces	s Point
⇔中 文	Status	System	Network	Wireless	Administration	Apply	Logout
➡ 中 文 ● Basic Settings ● Vitrual APs ● Radius ● Access Control ● Advanced Settings ? Help	Status Basic Se VAP Nar SSID: Broadca Isolation Max Sta Number VAP Rat Max Dov Max Ups Station Max Ups Station Max Ups	System ettings me: nst SSID: n within VAP: tion : te Limit wnstream Rate stream Rate: Rate Limit wnstream Rate stream Rate:	Network VAP-Nam Wireless-1 © Enable 0 c: 0 c: 0 void void void void void void void void	Wireless           e-1           l           e         Disable           (0-64)           Kbps (0-200           Kbps (0-200           Kbps (0-200           Kbps (0-200           Kbps (0-200	Wireless Administration	Apply	s Point Logout
	Network	Key:					
	Liciypo				Back	Save	Cancel

Figure 21: WPA-PSK Screen

Data -	- WF	PA-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.

					Wireless	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O Basic Settings O Vitrual APs	Basic S	ettings					
Access Control     Advanced Settings	VAP Nar SSID: Broadca	ne: est SSID:	VAP-Nam Wireless-	e-1 I e 🔿 Disable			
? Help	Isolation Max Sta Number	n within VAP: tion :	Disable 0	(0-64)			
	VAP Rat	te Limit					
	Max Dov Max Ups	wnstream Rate stream Rate:	e: 0 0	Kbps (0-200 Kbps (0-200	000) 000)		
	Station	Rate Limit					
	Max Dov Max Ups	wnstream Rate stream Rate:	e: 0 0	Kbps (0-200 Kbps (0-200	000) 000)		
	Security Network Encrypti	y System: Key: Jon:	WPA2-PS	SK	<b>~</b>		
					Back	Save	Cancel

Figure 22: 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).

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
<ul> <li>⇒中文</li> <li>Basic Settings</li> <li>Vitrual APs</li> <li>Radius</li> <li>Access Control</li> <li>Advanced Settings</li> <li>? Help</li> </ul>	Status Basic Selection VAP Nar SSID: Broadca Isolation Max Sta Number VAP Rat Max Dov Max Ups Station Max Dov Max Ups Station Max Dov Max Ups Security Network Encrypti	System ettings me: me: st SSID: n within VAP: tion te Limit winstream Rate: Rate Limit winstream Rate: stream Rate: y System: < Key: ion:	Network VAP-Nam Wireless-1 © Enable 0 c c c c c c c c c c c c c c c c c c	Wireless           e-1           I           e         Disable           v           (0-64)           Kbps (0-200)           Kbps (0-200)	Administration Administration 0000) 0000) 0000) 0000) 0000) 0000	Apply	Logout
					Back	Save	Cancel

Figure 23: 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.

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
<ul> <li>Basic Settings</li> <li>Vitrual APs</li> <li>Radius</li> <li>Access Control</li> <li>Advanced Settings</li> </ul>	Basic So VAP Nar SSID:	<b>ettings</b> ne:	VAP-Nam Wireless-*	e-1			
? Help	Broadca Isolation Max Sta Number	nst SSID: n within VAP: tion :	<ul> <li>Enable</li> <li>Disable</li> <li>0</li> </ul>	e O Disable			
	VAP Rat	te Limit					
	Max Dov Max Ups	wnstream Rate stream Rate:	e: 0 0	Kbps (0-200) Kbps (0-200)	000) 000)		
	Station Max Dov	Rate Limit	2: 0	Kbps (0-2000	000)		
	Security Security	<b>y</b> System:	WPA-RAD		v		
	WPA En	cryption:					
					Back	Save	Cancel

Figure 24: 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.

					Wireless	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
<ul> <li>⇒中文</li> <li>Basic Settings</li> <li>Vitrual APs</li> <li>Radius</li> <li>Access Control</li> <li>Advanced Settings</li> <li>? Help</li> </ul>	Status Basic S VAP Nar SSID: Broadca Isolation Max Sta Number VAP Rat Max Don Max Up Station Max Don Max Don Station Max Don Security Security WPA En	System ettings me: inst SSID: in within VAP: tion te Limit winstream Rate: Rate Limit winstream Rate: ream Rate: y stream Rate:	Network VAP-Nam Wireless- © Enable 0 c c 0 0 c 0 v PA2-RA AES  V	Wireless	Wireless Administration	Access Apply	S Point
					Back	Save	Cancel

Figure 25: 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.

□●中文       Status       System       Network       Wireless       Administration       Apply       Logout         ● Basic Settings       ●       Vitrual APs       Basic Settings         ● Radius       VAP Name:       VAP-Name-1         ● Access Control       ●       SID:       Wireless-1         ● Advanced Settings       ■       ■       ■         ● Help       ■       ■       ■       ■         ■ Help       ■       ■       ■       ■       ■         ● Help       ■       ■       ■       ■       ■         ● Help       ■       ■       ■       ■       ■       ■         ● Help       ■       ■       ■       ■       ■       ■       ■         ● Help       ■						Wireless	s Acces	s Point
● Basic Settings   ● Vitrual APs   ● Radius   ● Access Control   ● Access Control   ● Access Control   ● Access Control   ● Advanced Settings   Broadcast SSID:   ● Enable ● Disable   Isolation within VAP:   Disable   Isolation within VAP:   Max Station   Number:   0   (0-64)   VAP Rate Limit Max Downstream Rate:    Max Downstream Rate:   0   Kbps (0-20000)   Max Upstream Rate:   0   Kbps (0-20000)   Max Downstream Rate:   0   Kbps (0-20000)	⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
Back Save Cancel	<ul> <li>⇒中文</li> <li>○ Basic Settings</li> <li>○ Vitrual APs</li> <li>④ Radius</li> <li>○ Access Control</li> <li>④ Advanced Settings</li> <li>? Help</li> </ul>	Status Basic Si VAP Nar SSID: Broadca Isolation Max Sta Number VAP Rat Max Dor Max Ups Station Max Ups Security WPA En	System ettings me: ast SSID: n within VAP: ition te Limit wnstream Rate: Rate Limit wnstream Rate: stream Rate: y y System: cryption:	VAP-Nam Wireless-1 © Enable 0 2: 0 0 2: 0 0 0 WPA-RAE TKIP	Wireless e-1	Administration Administration 000) 000) 000) A2-RADIUS 🗸	Apply	Logout

Figure 26: WPA and WPA2 with Radius Screen

Data - WPA and WPA2 with Radius Scree
---------------------------------------

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.

					Wireles	s Acces	s Point
⇒中文	Status	System	Network	Wireless	Administration	Apply	Logout
Basic Settings     Vitrual APs     Radius     Access Control     Advanced Settings     Phelp	Status Basic Sel VAP Nar SSID: Broadca Isolation Max Sta Number VAP Rat Max Dov Max Ups Station Max Dov Max Ups Security Security Dynamic	System ettings ne: st SSID: n within VAP: tion tion te Limit wnstream Rate stream Rate: Rate Limit wnstream Rate: System: System: WEP Key Size	VAP-Nam Wireless-1 © Enable 0 2: 0 0 2: 0 0 802.1x 2: 64 bit	Wireless e-1 i e O Disable v i (0-64) Kbps (0-2000 Kbps (0-200 Kbps (0-2000 Kbps (0-2000 Kbps (0-2000 Kbps (0-2000 Kbps (0	Administration 0000) 0000) 0000)	Apply	Cancel

Figure 27: 802.1x Screen

#### Data - 802.1x Screen

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

					Wireless	Acces	s Point
⇒中文	Status	System	Network	Wireless	Administration	Apply	Logout
<ul> <li>Basic Settings</li> <li>Vitrual APs</li> <li>Radius         <ul> <li>Authentication Server</li> <li>Accounting Server</li> </ul> </li> </ul>	р	<b>rimary</b> IP Ac Port Shar	ddress: Number: ed Secret:	0.0	. 0 . 0		
Advanced Settings	Sec	ondary <sub>IP Ac</sub> Port Shar	ldress: Number: ed Secret:	0.0	. 0 . 0		
						Save	Cancel

Figure 28: Authentication Server Settings

Data - A	Authenti	cation	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

					Wireles	s Acces	s Point
⇒中文	Status	System	Network	Wireless	Administration	Apply	Logout
<ul> <li>Basic Settings</li> <li>Vitrual APs</li> <li>Radius         <ul> <li>Authentication Server</li> <li>Accounting Server</li> <li>Access Control</li> <li>Advanced Settings</li> </ul> </li> </ul>	P	rimary IP AG Port Shar ondary IP AG Port Shar	ddress: Number: red Secret: ddress: Number: red Secret:	0 . 0 1813 0 . 0 1813	.  0 .  0		
						Save	Cancel

Figure 29: 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 Prima- ry 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.

					Wirelee		e Doint
					vvireles	S Acces	SPOIN
⇒中文	Status	System	Network	Wireless	Administration	Apply	Logout
O Basic Settings							
O Vitrual APs	Wireles	s Radio:	Radio 1 (2.4	4G) 💌			
🕀 Radius	Enable	Access					
O Access Control	Control	l: Method:	Local Datab				
Advanced Settings		incentra in	Local Datab				
	VAP	-	VAP-Name-1	[Wireless-1]	~		
? Help	Control	Туре					
		w Following M	ac Addresses (	to Connect to	o Wireless netwo	rk	
		Anow Following Mac Addresses to Connect to Wireless network     Depy Following Mac Addresses to Connect to Wireless network					
	0 00.	.,					
	Wirele	ss Stations M	AC Address/B	andWidth Li	ist		
			M	AC Addres	iS		
				Delete			
	Availal	ole Wireless S	Stations				
			Station ID	М	AC Address		
				Add			
	Add No	ew Station				,	
	MAC A	ddress:	:		:	:	
				Add			
					Г	Save	Cancel

Figure 30: 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.
<b>Control Method</b>	Select the desired option, as required
	• <b>Local Database</b> - The device will use the local MAC address table for Access Control.
	• <b>RADIUS Server-</b> The Access Point will use the MAC address table located on the external Radius server on the LAN for Access Control.
	<b>Warning !</b> Ensure your own PC is in the "Trusted Wireless Stations" list before enabling this feature.

<b>Control Type</b>	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 Data- base. 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 - Advanced Settings

### **Parameters Screen**

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

Figure 31: Parameters Screen

Data -	Ρ	aramete	rs 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.
<b>RTS/CTS Threshold</b>	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:

					Wireless	Acces	s Point
⇒中文	Status	System	Network	Wireless	Administration	Apply	Logout
<ul> <li>Basic Settings</li> <li>Vitrual APs</li> <li>Radius</li> <li>Access Control</li> <li>Advanced Settings         <ul> <li>Parameters</li> <li>User Control</li> <li>Auto Econyana</li> </ul> </li> </ul>		Wireless User Cor Max Stat Max Thro	Radio: htrol Mode: ion Number: hughput:	Radio Disab 64 30	1 (2.4G) ▼ le ▼ (1-256) Mbps (1-100)		
Auto Frequency Load Balance WMM Band Select Rate Limitation						Save	Cancel

Figure 32: 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 $(1\sim256)$ of wireless stations connecting to the device.
Max Throughput	Enter the desired number between 1 and 100 for the maximum throughput.

# Auto Frequency Screen

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O Basic Settings							
O Vitrual APs		Wireless	Radio:	Ra	dio 1 (2.4G) 🗸		
Radius		Auto Fre	auency Mode:	Dis	sable 💙		
O Access Control		Auto Fro	auonay Adjust	Interval: 108	300 <b>C</b> araanda	(600 10000)	
Advanced Settings		Autorres	quericy Aujust	incervan roo	Seconds	(000-10800)	
Parameters		Min Signa	al Level Interva	al: 0	dBm (-90- :	10)	
User Control				9	Scan Once		
<ul> <li>Auto Frequency</li> </ul>							
Load Balance							
WMM							
Band Select							
Rate Limitation							
9							
2 Help							
						Save	Cancel

Figure 33: 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.
Min signal Level Interval	Enter the desired dBm between -90 and 10 here.

# Load Balance Screen

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
<ul> <li>Basic Settings</li> <li>Vitrual APs</li> <li>Radius</li> <li>Access Control</li> <li>Advanced Settings</li> <li>Parameters</li> <li>User Control</li> <li>Auto Frequency</li> <li>Load Balance</li> <li>WMM</li> <li>Band Select</li> <li>Rate Limitation</li> </ul>		Load Bal Load Bal User Nun Data Flu CPU Usa	ance Mode: ance Group: nber Interval: < Interval: ge Interval:	Disab default 1 1	le v (1-100) Kbps (1-10) (1-100)	02400) Save	Cancel

Figure 34: 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

					Wir	eless Ac	cess Point
⇒中文	Status	System	Network	Wirel	ess Administ	ration Ap	ply Logout
O Basic Settings O Vitrual APs	Wirel WMM WMM	less Radio: I Support: I Power Save	F Support: [	Radio 1 (2.4 2 2	G) 💙		
Parameters User Control Auto Frequency Load Balance • WMM Band Select Rate Limitation ? Help		ACM ACK AIFSN CWmin CWmax COP Limit	AC-VO	AC-VI	AC-BE	AC-BK	(2-15) (0-15) (0-15) (0-255) Cancel

Figure 35: 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 Parameter	rs
ACM	ACM (Admission Control Mandatory) is used to restrict stations from using a specific AC.
No Ack	When the No ACK policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the envi- ronment where communication quality is fine and interference is weak. Also the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communica- tion quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.
	When the Normal ACK policy is used, the recipient acknowl- edges each received unicast packet.

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 (Maxi- mum Contention Windows) determine the average backoff slots, which increases as the two values in- crease. 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**

					Wireles	s Acces	s Point
⇒中文	Status	System	Network	Wireless	Administration	Apply	Logout
<ul> <li>○ Basic Settings</li> <li>○ Vitrual APs</li> <li>➡ Radius</li> <li>○ Assess Control</li> </ul>		Band Sel	ect Function:	V			
Access Control     Advanced Settings     Parameters     User Control     Auto Frequency     Load Balance     WMM							
• Band Select Rate Limitation ? Help					C	Save	Cancel

Figure 36: Band Select Screen

Data - I	Band S	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**

					Wireles	ss Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O Basic Settings							
O Vitrual APs		Rate Limi	itation:	Disabl	e 💙		
Radius		Lowest R	ate:	1 🗸	Mbps		
O Access Control		Rate Dur	ation	5 1	Seconds		
Advanced Settings		nace bai			Seconda		
Parameters							
User Control							
Auto Frequency							
Load Balance							
WMM Rand Select							
Bate Limitation							
0							
7 Help							
					(	Save	Cancel

Figure 37: 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.				

### **Data - Rate limitation Screen**

# **Network - IP Settings Screen**

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O IP Settings O VLAN Setttings O STP O IGMP Settings O Bridge Parameters		IP Settin AC IP Ad AC DNS 1	gs: dress: Name 1:	DHCP Client			
? Help		AC DNS I	Name 2:				
						Save	Cancel

Figure 38: 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.						
	• <b>Password</b> - Enter the password for the login name above.						
	• <b>Timeout</b> - Enter the desired value in seconds for the timeout period.						
	• <b>Retry</b> - 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".						

### Data - IP Settings Screen

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

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O IP Settings O VLAN Setttings O STP O IGMP Settings O Bridge Parameters		Enable 8 Manager	802.1Q VLAN: ment VLAN:		0 (1-4094)		
						Save	Cancel

Figure 39: 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.
Management VLAN	Define the VLAN ID used for management.

# Network - STP Screen

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
<ul> <li>IP Settings</li> <li>VLAN Setttings</li> <li>STP</li> <li>IGMP Settings</li> <li>Bridge Parameters</li> </ul>		Enat	ole Spanning 1	Tree Protocol:			
					C	Save	Cancel

### Figure 40: STP Screen

### Data - STP Screen

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

# Network - IGMP Settings Screen

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O IP Settings							
O VLAN Setttings		IGMP S	Snooping:	0 е	nable 💿 Disabl	e	
O STP							
O IGMP Settings							
O Bridge Parameters							
? Help							
	•				ſ	Sava	Cancel
					L	Jave	Cancer

Figure 41: 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 - Bridge Parameters Screen

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O IP Settings							
O VLAN Setttings		Agein	g Time:	300	s (180-3600)		
O STP							
O IGMP Settings							
O Bridge Parameters							
? Help							
					ſ	Save	Cancel
					Ľ	Jave	Cancer

Figure 42: 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 <i>Infrastructure</i> .
SSID (ESSID)	This must match the value used on the Wireless Access Point.
	The default value is <b>wireless</b>
	Note! The SSID is case sensitive.
Wireless	• Each Wireless station must be set to use WEP data encryption.
Security	• 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 <i>Infrastructure</i> .
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	On each client, Wireless security must be set to WPA-PSK.
Security	• The <b>Pre-shared Key</b> entered on the Access Point must also be entered on each Wireless client.
	• The <b>Encryption</b> 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 <i>Infrastructure</i> .
SSID (ESSID)	This must match the value used on the Wireless Access Point.
	The default value is <b>wireless</b>
	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).

indows Components Wizard			×
Windows Components You can add or remove components o	Windows 2000.		<b>H</b>
To add or remove a component, click t part of the component will be installed. Details.	ne checkbox. A s To see what's inc	haded box means t luded in a compone	hat only nt, click
Components:			
🗹 📻 Accessories and Utilities		12.1	1 MB 🔺
🗹 🝺 Certificate Services		1.4	4 мв 🛄
Cluster Service		2.5	5 MB
🗹 💬 Indexing Service		0.0	О МВ
Internet Information Services (I)	51	21.6	Б МВ 🔳
Description: Message Queuing provid communication services.	s loosely-coupled	l and reliable networ	k
Total disk space required: 12 Space available on disk: 6699	.7 MB .9 MB	D	etails
	< Back	Next >	Cancel

Figure 43: Components Screen

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

Windows Components Wizard		×
Certification Authority Type There are four types of certification authorities.		
Certification Authority types:	Description:	
<ul> <li>Enterprise root CA</li> </ul>	The most trusted CA in an	<b>A</b>
C Enterprise subordinate CA	before any other CA. Requires	
Stand-alone root CA	Active Directory.	
C Stand-alone subordinate CA		-
C Advanced options		
L	< Back Next >	Cancel

### Figure 44: Certification Screen

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

Windows Components Wizard	×
CA Identifying Information Enter information to identify	this CA
CA name:	WirelessCA
Organization:	Organization
Organizational unit:	Systems
City:	Dakland
State or province:	CA Country/region: US
E-mail:	cd@yourdomain.tld
CA description:	Wireless CA
Valid for:	2 Years Expires: 2/17/2005 6:39 PM
	< Back Next > Cancel

Figure 45: 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.

Action <u>V</u> i	ew 📋 🗢 🤿 💽 🔃	🗡 🖼   😫   ] 🖳
Tree		rowan [192.168.0.21]
2 DHCP	Display Statistics	Configure the DHCP Server
	New Scope New Multicast Scope	fore a DHCP server can issue IP
	Reconcile All Scopes Authorize	ithorize the DHCP server.
	Define User Classes Define Vendor Classes Set Predefined Options	scope is a range of IP addresses that is signed to computers requesting a namic IP address. Authorization is a curity precaution that ensures that only
	All Tasks	thorized DHCP servers run on your twork.
	View	To add a new scope, on the action menu
	Delete Refresh	ck New Scope.
	Properties	To authorize this DHCP server, on the tion menu, click Authorize.
	Help	

#### Figure 46: 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.

New Scope Wizard	×
IP Address Range You define the scope address range by identifying a set of consecutive IP addresses.	<b>S</b>
Enter the range of addresses that the scope distributes.	
Start IP address: 192 . 168 . 0 . 100	
End IP address: 192 . 168 . 0 . 200	
A subnet mask defines how many bits of an IP address to use for the network/subne IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.	et
Length: 24	
Subnet mask: 255 . 255 . 0	
< Back Next > 0	ancel

**Figure 47: 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*.

New Scope Wizard		×
Domain Name and DNS Servers The Domain Name System (DNS) maps a clients on your network.	nd translates domain names used	
You can specify the parent domain you want t DNS name resolution.	he client computers on your netwo	rk to use for
Parent domain: Wireless.yourdomain.tld		
To configure scope clients to use DNS server servers.	s on your network, enter the IP add	dresses for those
Server name:	IP address:	
		Add
Resolve	192.168.0.250	Remove
		Up
		Down
	,	
	< Back Next >	Cancel

### Figure 48: 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.

Tree	Name	Intended Purpose
Certification Authority (Local)     WirelessCA     Revoked Certificates     Issued Certificates     Issued Certificates     Failed Requests     Policy Setting     New     View     Refresh     Export List     Help	Certificate to Issue	File Recovery Encrypting File System Client Authentication, Server Autheni Server Authentication Client Authentication, Server Autheni Encrypting File System, Secure Email, Code Signing, Microsoft Trust List Sig

Figure 49: Certificate Authority Screen

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

🗱 User Signature Only	Secure Email, Clier
🗱 Smartcard User	Secure Email, Clier
🐺 Authenticated Session	Client Authenticatic
🙀 Smartcard Logon	Client Authenticatic
🙀 Code Signing	Code Signing
😨 Trust List Signing	Microsoft Trust List
Enrollment Agent	Certificate Request

Figure 50: 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 51: Active Directory Screen** 

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

Cum	ent Group Policy	Object Links for	wireless	
Group Policy 0	Ibject Links		No Override	Disabled
🚮 Default Don	nain Policy			
		r.1 .1 .1		
Group Policy Ob This list obtained	jects higher in the I from: rowan.wire	a list have the hi eless.yourdomair	ghest priority. .tld	
Group Policy Obi This list obtained	jects higher in the from: rowan.wire Add	a list have the hi eless.yourdomair Edit	ghest priority. . tid	UP
Group Policy Ob This list obtained New Options	jects higher in the I from: rowan.wire Add Delete	a list have the hi eless.yourdomair Edit Properties	ghest priority. Ltld	Up Down

#### Figure 52: 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 53: Group Policy Screen

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

A certificate template is a set of pro	edefined properties for certificates issued to	
computers. Select a template from	the following list.	
Certificate templates:	Intended Purposes	
Computer	Client Authentication, Server Authenticatio	
Domain Controller	Client Authentication, Server Authenticatio	
Enrollment Agent (Computer)	Certificate Request Agent	
IPSEC	1.3.6.1.5.5.8.2.2	

#### Figure 54: 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.

+		L3		
e		Friendly Name	Address	Protocol
Internet Aut	hentication Service (Local)			
Remot	Open			
💐 Remot	New Client			
	New 🕨			
	View 🕨			
	Export List			

Figure 55: 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*...

Name	Description
Called-Station-Id	Phone number dialed by user
Calling-Station-Id	Phone number from which call originated
Client-Friendly-Name	Friendly name for the RADIUS client. (IA
Client-IP-Address	IP address of RADIUS client. (IAS only)
Client-Vendor	Manufacturer of RADIUS proxy or NAS.
Day-And-Time-Restrictions	Time periods and days of week during w
Framed-Protocol	The protocol to be used
NAS-Identifier	String identifying the NAS originating the
NAS-IP-Address	IP address of the NAS originating the rec
NAS-Port-Type	Type of physical port used by the NAS o
Service-Type	Type of service user has requested
Tunnel-Type	Tunneling protocols to be used
Windows-Groups	Windows groups that user belongs to
•1	

Figure 56: 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*.

	IP		Multilink
Authentication	Encryption	1	Advanced
heck the authentication m	ethods which are allov	ved for	this connecti
🔽 Extensible Authenticat	ion Protocol		
Select the EAP type which	n is acceptable for this	policy.	
Smart Card or other Certif	icate	-	Configure
Microsoft Encrypted A	uthentication version 2	2 (MS-C	HAP v2)
Microsoft Encrypted A	uthentication (MS-CH/	λP)	
Encrypted Authenticat	ion (CHAP)		
Encrypted Authenticat     Unencrypted Authenti	ion (CHAP) cation (PAP, SPAP)		
Encrypted Authenticat     Unencrypted Authenti     Unencrypted Authenti     Unauthenticated Access	ion (CHAP) cation (PAP, SPAP)		
Encrypted Authenticat     Unencrypted Authenti     Unauthenticated Access     Allow remote PPP clier     any authentication me	ion (LHAP) cation (PAP, SPAP) nts to connect without thod.	negotia	ating
Encrypted Authenticat     Unencrypted Authentic     Unauthenticated Access     Allow remote PPP clier     any authentication me	ion (LHAP) cation (PAP, SPAP) nts to connect without thod.	negolia	ating

Figure 57: 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*.

alex Properties	? ×
Terminal Services Profile Exchange I E-mail Addresses Exchange Fe General Address Account Profile Telephones Member Of Dial-in Environment Sessions F	General atures Organization Remote control
Remote Access Permission (Dial-in or VPN) C Allow access Deny access C Control access through Remote Access Policy	
Verify Caller/D:     Callback Options     No Callback     Set by Caller (Routing and Remote Access Service only)     Always Callback to:	
Assign a Static IP Address     Apply Static Routes     Define routes to enable for this Dial-in     connection.	tes
OK Cancel Apply	Help

Figure 58: 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.

Wireless Network Pro	perties (	? 🛛
Network name (SSID):	misslairA	
Wireless network key (W	(EP)	
This network requires a l	key for the following:	
Data encryption (W	/EP enabled)	
Network Authentic	ation (Shared mode)	
Network key:		
Key format	ASCII characters	~
Key length:	104 bits (13 characters)	~
Key index (advanced)	0 0	
The key is provided f	or me automatically	
This is a computer-to-co	omputer (ad hoc) network; w	vireless
access points are not u	ised	
	OK Cano	el

**Figure 59: 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.

					Wireless	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O Device Info							
O System Status		Service Pro	ovider:	Sercomm			
Network Status		Hardware	Version:	V1.0.00S			
Wireless Status		Firmware	Version:	V1.0.05			
O Log		Bootloade	r Version:	1.01			
Statistics		Serial Num	ber:	123456789	90123		
2 Help		AP Type:		FIT AP			
- Holp		Running Fi	rmware:	Backup Firr	mware		
						(	Refresh

Figure 60: Device Info Screen

Access Point	
Service Provider	The name of the service provider will be displayed.
Hardware Version	The version of the hardware currently used.
Firmware Version	The version of the firmware currently installed.
<b>Bootloader Version</b>	The version of the bootloader currently used.
Serial Number	The serial number of the device.
АР Туре	The current AP type is displayed.
Running Firmware	The currently running firmware is displayed.

#### Data - Device Info Screen

## System Status

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

					Wireless	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O Device Info							
O System Status		Access Po	int Name:	AP4F2B34			
Network Status		MAC Addre	ess:	00:C0:02:4	4F:2B:34		
Wireless Status		Country/D	omain:	United Stat	tes		
O Log		System Up	o Time:	0 Hours, 0	5 Minutes, 43 Seco	onds	
Statistics							
? Help						(	Refresh

Figure 61: 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.

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O Device Info							
O System Status		IP Type:		DHCP Clien	t		
Network Status		IP Address	:	192.168.0.	228		
IP Settings		Subnet Ma	sk:	255.255.25	5.0		
Wireless Status		Gateway:		192.168.0.	1		
O Log		Primary DN	IS:	0.0.00			
G Statistics		Secondary	DNS:	0.0.0.0			
2 Help						(	Refresh

Figure 62: IP Settings Screen

Data - IF	Settings	Screen
-----------	----------	--------

TCP/IP	
<b>IP</b> Туре	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.

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O Device Info							
O System Status		Ethernet S	status:	Connected			
Network Status							
IP Settings							
Ethernet							
Wireless Status							
O Log							
Statistics							
? Help							
						l	Refresh

#### Figure 63 Ethernet Screen

#### Data - Ethernet Screen

Ethernet	
Ethernet Status	The current Ethernet status is displayed.

#### Wireless Status

#### **Basic Screen**

					Wireless	s Acces	s Point
⇒中文	Status	System	Network	Wireless	Administration	Apply	Logout
O Device Info O System Status			Wireless F	Radio: Radio	1 (2.4G) 💙		
Wireless Status		AP Mode:	0.00000	Access Point	t		
Basic     Virtual AP Status		Wireless M	ode:	o Disabled			
O Log		WMM Supp	ort: er Save	Enabled Enabled			
Statistics		Support:		<u></u>			Refresh

Figure 64: 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

							Wireles	ss Acc	ess Po
⇒中 文	Status	System	Ne	twork	Wi	ireless /	Administration	Appl	y Log
				Wireless F	Radio	Radio 1	(2.4G) 💙		
O Device Info	_								
O System Status		Name	BSSID	SSID	E	SSID Broadca	st Security	Status	Clients
Network Status	V	AP-Name-1	N/A	Wireless	-1	Enabled	None	Disabled	0
Wireless Status	V	AP-Name-2	N/A	Wireless	-2	Enabled	None	Disabled	0
Racio	V	AP-Name-3	N/A	Wireless	-3	Enabled	None	Disabled	0
Dabic Vistual AD Chatura	V	AP-Name-4	N/A	Wireless	-4	Enabled	None	Disabled	0
Virtual AP Status	V	AP-Name-5	N/A	Wireless	-5	Enabled	None	Disabled	0
Wireless Stations	V	AP-Name-6	N/A	Wireless	-6	Enabled	None	Disabled	0
O Log	V	AP-Name-7	N/A	Wireless	-7	Enabled	None	Disabled	0
Statistics	V	AP-Name-8	N/A	Wireless	-8	Enabled	None	Disabled	0
	V	AP-Name-9	N/A	Wireless	-9	Enabled	None	Disabled	0
	VA	P-Name-10	N/A	Wireless-	-10	Enabled	None	Disabled	0
	VA	P-Name-11	N/A	Wireless-	-11	Enabled	None	Disabled	0
	VA	P-Name-12	N/A	Wireless-	-12	Enabled	None	Disabled	0
	VA	P-Name-13	N/A	Wireless-	-13	Enabled	None	Disabled	0
	VA	P-Name-14	N/A	Wireless-	-14	Enabled	None	Disabled	0
	VA	P-Name-15	N/A	Wireless-	-15	Enabled	None	Disabled	0
	VA	P-Name-16	N/A	Wireless-	-16	Enabled	None	Disabled	0
									Refre

Figure 65: 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.
SSID Broadcast	Indicates whether or not the SSID is broadcast.
SSID	The SSID assigned to this profile.
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.

#### **Data - Virtual AP Status Screen**

#### Wireless Stations Screen

					Wirele	ss Acces	s Point
⇒中 文	Status	System	Network	Wirele	ss Administratio	n Apply	Logout
O Device Info							
O System Status			Wireless Ra	adio: Radi	io 1 (2.4G) ⊻		
Network Status							
Wireless Status		Station ID	MAC Addre	ss SS	ID RSSI(dbm)	) Status	
Basic							
Virtual AP Status		Station ID	OutPkts	InPkts	OutOctets	InOctets	
Wireless Stations							
O Log							
Statistics							
2 Holp							
neip						-	
						l	Refresh

Figure 66: Wireless Stations 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.
<b>Refresh Button</b>	Update the data on screen.

#### Data - Wireless Station Screen

## Log Screen

					Wireles	s Acces	s Point	
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout	
O Device Info								
O System Status			Current Time:	1970-01-01	00:07:58			
Network Status	Jan 1 00:01:01 Syslogd start up Jan 1 00:01:22 auth: Authorized Login from 192.168.0.1							
Wireless Status								
O Log		< << [1] >> >						
Statistics								
	L							
					Refresh	Save File	Clear Log	

#### Figure 67: 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.

#### Data - Log Screen

#### **Statistics Screen**

#### **Ethernet Screen**

					Wireless	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O Device Info							
O System Status		Packets Re	eceived:	51			
Network Status		Packets Sent:		82			
Wireless Status		Bytes Received:		5038			
O Log		Bytes Sent:		71801			
Statistics		Frror Packets Received:		0			
• Ethernet		Dress Deserved Deducter		0			
Wireless		Drop Recei	veu Packets.	U			
? Help						ſ	Refresh

#### Figure 68: 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

						Nireless	Access	e Point
⇒中 文	Status	System	Network	Wireless	Admi	inistration	Apply	Logout
			Wireles	s Radio: Radi	io 1 (2.	.4G) 🗸		
O Device Info							1	
O System Status			Name			VAPO	VAP1	
Network Status		Packets Re	eceived			0	0	_
O utivelese Status		Packets Se	ent			0	0	
Wireless Status		Bytes Rec	eivea			0	0	
O Log		Error Dack	t otc Pocoivor	4		0	0	_
Statistics		Drop Pack	ived Packete			0	0	_
Ethernet		ыор кесе	Ived Fackets	•		0	0	
• Wireless			Name			VAP2	VAP3	
		Packets Re	eceived			0	0	
		Packets Se	ent			0	0	
		Bytes Rec	eived			0	0	
		Bytes Sen	t			0	0	
		Error Pack	ets Received	1		0	0	_
		Drop Rece	ived Packets	;		0	0	
							MARE	
		De electe De	Name			VAP4	VAP5	
		Packets Re	eceived			0	0	_
		Packets Se	aivod			0	0	
		Bytes Ket	t			0	0	_
		Error Pack	ets Receiver	1		0	0	_
		Drop Rece	ived Packets			0	0	
						_	_	
			Name			VAP6	VAP7	
		Packets Re	eceived			0	0	
		Packets Se	ent			0	0	
		Bytes Rec	eived			0	0	
		Bytes Sen	t			0	0	_
		Error Pack	ets Received	1		0	0	_
		Drop Rece	ived Packets	;		0	0	
								Refresh

Figure 69: Wireless Screen

#### Data - Wireless Screen

VAP0~VAP7	
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

АР Туре							
					Wireless	s Acces	s Point
⇒中文	Status	System	Network	Wireless	Administration	Apply	Logout
<ul> <li>AP Type</li> <li>Management</li> <li>Auto Config</li> <li>Config File</li> <li>Ping Test</li> <li>Auto Reboot</li> <li>Firmware Upgrade</li> <li>2 Help</li> </ul>		AF	у Туре:	⑥ FIT AI	P 🔘 FAT AP		

Figure 70: AP Type Screen

Data	- AP	Type	Screen
------	------	------	--------

Account	
АР Туре	Select the AP type as required. If "FAT AP -> Bridge Mode" is selected, please refer to the <i>Chapter 7 Access Point Mode</i> for more details.

## Management Screen

#### **Account Screen**

The Account screen allows you to assign a password to the Wireless Access Point. This password limits access to the configuration interface. The default password is *password*. It is recommended that this be changed, using this screen.

					Wireles	s Acces	s Point
⇔中 文	Status	System	Network	Wireless	Administration	Apply	Logout
<ul> <li>AP Type</li> <li>Management</li> <li>Account</li> <li>Method Control</li> <li>Auto Config</li> <li>Config File</li> <li>Ping Test</li> <li>Auto Reboot</li> <li>Firmware Upgrade</li> <li>? Help</li> </ul>		Admin Use Chang New F Re-en	er Name: ge Admin Pass Password: Iter to Confirm	admin word		] ] Save [	Cancel

Figure 71: Account Screen

#### **Data - Account Screen**

Account	
Admin User Name	Enter the login name for the Administrator.
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.
<b>Re-enter to Confirm</b>	Re-enter the desired login password.

#### **Method Screen**

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
О АР Туре							
😑 Management		Enabl	e Wireless We	b Access			
Account		Enabl	e HTTP Admin	connections			
Method							
Control		HTTP	Port Number:	80			
O Auto Config		📃 Enabl	e HTTPS (secu	re HTTP) Adn	nin connections		
O Config File		HTTPS	6 Port Number	443			
O Ping Test		🗌 Enabl	e Managemen	t via SSH			
O Auto Reboot							
O Firmware Upgrade							
? Help							
	-				Г	Save	Cancel

Figure 72: 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.

							Wirele	ess	Acces	s Point
⇒中 文	Status	System	Netwo	rk	Wirel	ess	Administratio	n	Apply	Logout
AP Type     Management     Account     Method		Turn IP Allow Follow Follow	<b>Managen</b> Ilowing IP	nent (	<b>Control</b>	On o Mar	nage the Devi	ce		
Control		Deny Fol	lowing IP	Addr	esses t	o Mar	nage the Devi	ce		
<ul> <li>Auto Config</li> <li>Config File</li> <li>Ping Test</li> <li>Auto Reboot</li> <li>Firmware Upgrade</li> </ul>		IP subnet 1 IP subnet 2 IP subnet 3 IP subnet 4	2 0. 0. 0. 0	Subne .0 .0	et .0 .0 .0	2   2   2   2	Subnet M 255 255 2 255 255 2 255 255 2 255 255 2	1ask 55 . 55 .	255 255 255 255	
? Help		IP subnet 5 IP subnet 6 IP subnet 7 IP subnet 8		0. 0. 0. 0.	.0 .0 .0	2   2   2   2	255 255 2 55 255 2 55 255 2 55 255 2 55 255 2	55. 55.	255 255 255 255	
									Save (	Cancel

Figure 73: Control Screen

#### **Data - Control Screen**

Turn IP Management Control On	<ul> <li>Select the desired option, as required</li> <li>Enable or Disable the Management Control feature.</li> <li>Select either <i>Allow following IP addresses to Manage the Device</i> or <i>Deny following IP addresses to Manage the Device</i>.</li> <li>Enter the physical IP address and Subnet Mask of each Wireless attained.</li> </ul>
	station.

## Auto Config

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

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O AP Type		Auto Cor	ıfia:	O Ena	able 💿 Disable		
O Auto Config O Config File O Ping Test		FTP Serve User Nan	er: ne:				]
O Auto Reboot O Firmware Upgrade		Config Fil	le:	1	Hours		]
? Help				Cheo	ck Now		
					C	Save	Cancel

Figure 74: Auto Config Screen

Data - A	uto Co	nfig S	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.

					Wireles	s Acces	s Point
⇒中文	Status	System	Network	Wireless	Administration	Apply	Logout
<ul> <li>AP Type</li> <li>Management</li> <li>Auto Config</li> <li>Config File</li> <li>Ping Test</li> </ul>	Clic	k following bu	itton to back u	p a copy of t Back up	he current setting	js into a file	
O Auto Reboot O Firmware Upgrade	Restore a previously-saved config file to current system. Browse Restore						
<b>⊻</b> Heip		Click follov	wing button to	restore sett store to Defaul	ings to factory de ts	fault.	

Figure 75: Config File Screen

#### Data - Config File Screen

-	
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 <b>Save</b> .
Restore	
<b>Restore saved settings</b>	To restore settings from a backup file:
Restore saved settings from a file	To restore settings from a backup file: 1. Click <b>Browse</b> .
Restore saved settings from a file	<ul><li>To restore settings from a backup file:</li><li>1. Click <b>Browse</b>.</li><li>2. Locate and select the previously saved backup file.</li></ul>

\_\_\_\_

Defaults	
Revert to factory default settings	To erase the current settings and restore the original factory default settings, click <b>Restore to Defaults</b> 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.

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
<ul> <li>AP Type</li> <li>Management</li> <li>Auto Config</li> <li>Config File</li> <li>Ping Test</li> <li>Auto Reboot</li> <li>Firmware Upgrade</li> <li>? Help</li> </ul>		Ping Test Mo Ping IP Addr	ode: ress:	Disable V	. 🖸 . 🛛	Save	Cancel

Figure 76: 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.

					Wireles	ss Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
<ul> <li>AP Type</li> <li>Management</li> <li>Auto Config</li> <li>Config File</li> <li>Ping Test</li> <li>Auto Reboot</li> <li>Firmware Upgrade</li> <li>? Help</li> </ul>		Auto Rebool Reboot Inte	t Mode: rval:	Disable v 24 H	ours 💟 (1-1000)	) Save	Cancel

Figure 77: Auto Reboot Screen

#### Data - Auto Reboot Screen

Auto Reboot Mode	Select the desired Option:
	• <b>Disable</b> - Auto Reboot feature is not used.
	• <b>Enable</b> - 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.

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
О АР Туре							
Management		Firmware F	ile:			Browse	ə
O Auto Config							
O Config File							
O Ping Test							
O Auto Reboot							
O Firmware Upgrade							
? Help							
						Upgrade	Cancel

#### Figure 78: 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.
- 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.

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O Device Info							
O System Status		Hardware	Version:	V1.0.00S			
O Network Status		Firmware	Firmware Version:				
Wireless Status		Bootloade	Bootloader Version:				
		Serial Num	Serial Number:		90123		
Statistics		AP Type:	АР Туре:				
9 Uala		Device Mo	de:	Bridge			
: neip		Running Fi	irmware:	Backup Firr	mware		
						(	Refresh

#### Figure 79: Home Screen - Access Point 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.

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O Device Mode IP Settings VLAN Settings IGMP Settings STP Bridge Parameters		Device M	ode:	⊕ Bridge	() Router		
<b>Heip</b>					[	Save	Cancel

Figure 80: Device Mode Screen

#### Data - Device Mode Screen

<b>Device Mode</b>	Select the desired device mode for the router:					
	• <b>Router</b> - 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.					
	• <b>Bridge</b> - 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.

					Wireles	s Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O Device Info							
O System Status		Hardware	Version:	V1.0.00S			
Network Status		Firmware	Version:	V1.0.05			
Wireless Status		Bootloader Version:		1.01			
O Log		Serial Num	ber:	12345678	90123		
Statistics		AP Type:		FAT AP			
		Device Mo	dor	Pridao			
? Help		Device Mo	ue.				
		Running Fi	rmware:	Backup Fin	mware		
						(	Refresh

Figure 81: Device Info Screen - Access Point Mode

## Data - Device Info Screen (Access Point Mode)

Device Info	
Hardware Version	The version of the hardware currently used.
Firmware Version	The version of the firmware currently installed.
<b>Bootloader Version</b>	The version of the bootloader currently used.
Serial Number	The serial number of the device.
АР Туре	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.

					Wireless	Acces	s Point
⇒中 文	Status	System	Network	Wireless	Administration	Apply	Logout
O Device Info							
O System Status		VLAN(802.	1Q):	Disabled			
Network Status		Manageme	ent VLAN ID:	VLAN Disab	led		
IP Settings Ethernet							
VLAN							
Wireless Status							
O Log							
Statistics							
? Help							
						(	Refresh

Figure 82: 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
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

<u>C( 1 1</u>	
Standards	$\frac{11212}{12} \frac{112}{12} \frac{112}{$
	2.4002/3002
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 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.

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

#### **FCC Radiation Exposure Statement**

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.

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

(1) This device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

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

## 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 83: 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 snmpreadcommu- nity	Set SNMP Read Community
set snmpwritecommu- nity	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

## VX-AP320NA Wireless Access Point User Guide

factoryrestore	Restore to Default Factory Settings
apply	To make the changes take effect
exit	Quit the telnet