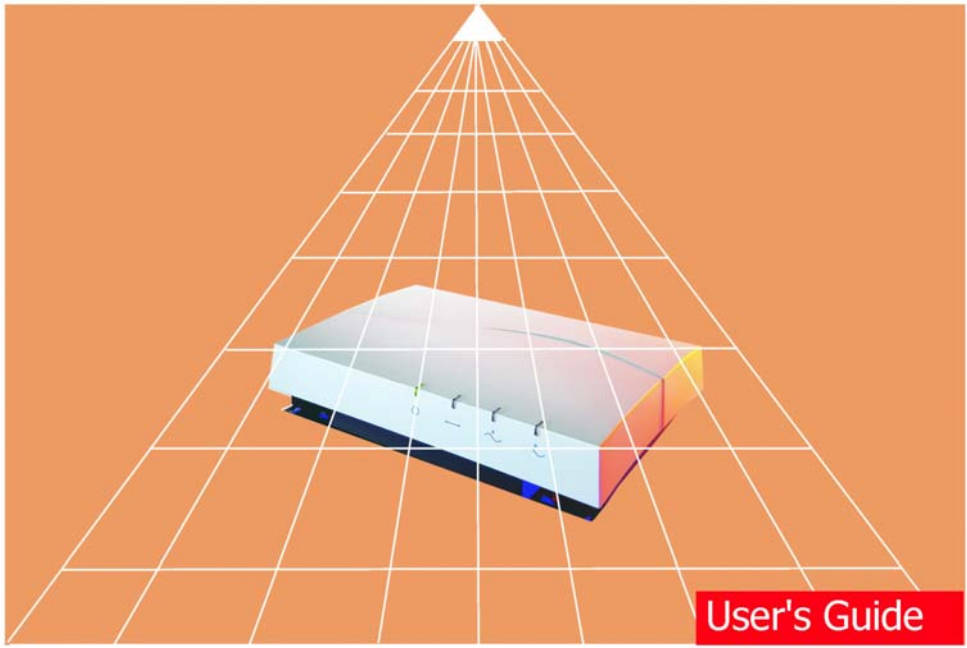


User's Guide

Avaya Wireless AP-3

AVAYA

Copyrights

- Avaya is a registered trademark of Avaya Inc.
- Microsoft Windows is a registered trademark of the Microsoft Corporation.
- All trademarks mentioned herein belong to their respective owners.

Publication Information

Date: December, 2002.

Document No.: 555-301-706

Avaya Wireless AP-3 User's Guide
Table of Contents

Chapter 1: Introduction

Chapter 2: Configuring the AP-3

Chapter 3: AP-3 Device Management

Chapter 4: Advanced Features

Chapter 5: Troubleshooting

Chapter 6: Using the Command Line Interface

Appendix A: Record Configuration Settings

Appendix B: Specifications

Introduction 1

In This Chapter

Wireless Networking Concepts

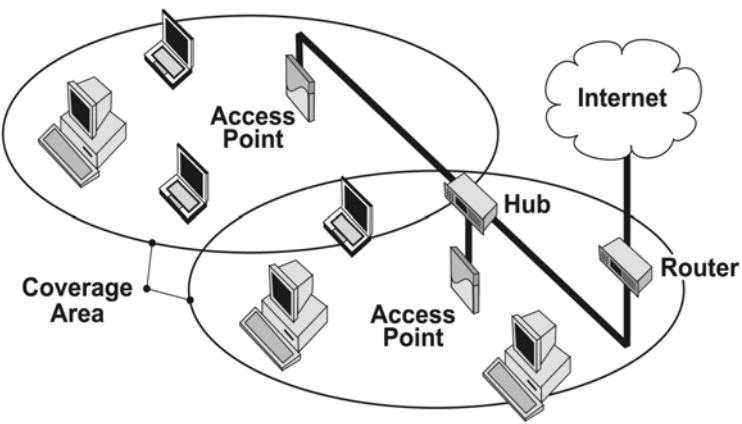
The AP-3 provides wireless access to network infrastructures. As wireless clients move from one coverage cell to another, AP-3 units automatically allow client roaming within the same subnet.

To determine the best location for the Base Station units, it is recommended that you conduct a Site Survey before placing the devices in their final locations. For information about how to conduct a Site Survey, contact your local reseller.

Before the AP-3 unit can be configured for your specific networking requirements, it must first be initialized so that you can recognize it once it is located in your network. Initialization consists of setting

- a static IP address and
- the appropriate IP mask.

Figure 3-2: Standalone wireless network access infrastructure



The network administrator can configure each unit according to the requirements for the network. The Access Point 3 (AP-3) functions as a wireless network access point to data networks. AP-3 networks provide:

- Seamless client roaming
- Easy installation and operation
- Over-the-air encryption of data
- High speed network links

To be fully operational, the AP-3 needs at least one Avaya Wireless PC Card.

Note: PC Cards are not included with your kit and must be ordered as separate items. Note that you cannot insert an Avaya Wireless 802.11a/b Card into the AP-3.

Management and Monitoring Capabilities

To configure the AP-3 for your needs, set your specific network, wireless interface, and bridge parameters. The HTTP (web browser) Interface provides easy configuration and management.

Wireless clients (computers connected to your network through a radio PC Card) use configuration software for network access. Once connected, users can roam from one coverage cell to another while maintaining their connection.

There are three management and monitoring interfaces available to the network administrator to configure and manage the AP-3 device(s) in the network:

- HTTP Interface
- Command Line Interface
- SNMP configuration capabilities

HTTP Interface

The HTTP Interface (Web browser Interface) provides easy access to configuration settings and network statistics from any computer in the network. Use the HTTP Interface through your LAN (switch, hub, etc.), through the Internet, or with a “crossover” Ethernet cable connected directly to your computer’s Ethernet Port.

Command Line Interface

The Command Line Interface (CLI) represents a set of keyboard commands and parameters used for configuring and managing the AP-3.

Users enter Command Statements, composed of CLI Commands and their associated parameters. Statements may be issued from one of the following:

- The keyboard for real time control.
- Through scripts that automate configuration.

For example, when downloading a file, administrators enter the following on the command line:

- the **download** CLI Command along with
  - IP Address,
  - file name, and
  - file type parameters.

If necessary, use the CLI with your computer serial port to initialize the proper IP address for your network.

The CLI provides configuration and management access for most generic Telnet and Terminal clients. Use the CLI through your computer serial port, over your LAN, through the Internet, or with a “crossover” Ethernet cable connected directly to your computer.

Details of the CLI commands used to manage the AP-3 device along with syntax and specific parameters names can be found in Using the Command Line Interface.

SNMP Management

You can also manage and configure an AP-3 using the Simple Network Management Protocol (SNMP).

Note: This requires an SNMP manager program, like HP Openview™ or Castlerock™'s SNMPc.

The AP-3 supports several Management Information Base (MIB) files that describe the parameters that can be viewed and/or configured over SNMP:

- MIB-II (RFC 1213)
- Bridge MIB (RFC 1493)
- Ethernet-like MIB (RFC 1643)
- AP-3 Enterprise MIB

Avaya provides these MIB files on the AP-3 CD. You need to compile one or more of the above MIBs into your SNMP program's database before you can manage the AP-3. Refer to the documentation that came with your SNMP manager for instructions on how to compile MIBs.

The Enterprise MIB defines the read and read-write objects that can be viewed or configured using SNMP. These objects correspond to most of the settings and statistics that are available with the other management interfaces. Refer to the Enterprise MIB for more information; the MIB can be opened with any text editor, such as Microsoft Word or WordPad.

Note: This guide describes how to configure an AP-3 using the HTTP Web interface or the CLI interface. For information on how to manage devices using SNMP, refer to the documentation that came with your SNMP program. Also, refer to the MIB files for information on the parameters available via SNMP.

Active Ethernet

Some AP-3 units are equipped with an Active Ethernet module. Active Ethernet (AE) delivers both data and power to the access point. The AP-3 operates in the same way, the only difference is in the power source.

- The Active Ethernet (AE) integrated module adds ~48 VDC to unused (non-data) wires in standard Category 5 Ethernet cable.
- The cable length between the Ethernet network source and the AP-3 unit should not exceed 100 meters (approx 325 ft.).
- The AE module is not a repeater and does not amplify the Ethernet data signal.
- AP-3 devices with Active Ethernet should be connected to a grounding type AC outlet (100-240 VAC), using the standard power cord supplied.
- Output Power per Port is 11 Watts.

For additional information, see Appendix B, “Electrical Specifications”.

802.11b versus 802.11a Networks

The AP-3 supports 802.11 wireless connectivity using the following radio technologies:

- **802.11a-compliant 5 GHz.** The IEEE 802.11a standard adds support for a high-speed wireless physical layer in the 5 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard requires support for data rates of 6, 12, 24, and 54 Mbits/s. The AP-3 unit supports the following data rates: 6, 9, 12, 18, 24, 36, 54 Mbits/s.
- **802.11a Turbo Mode.** For 802.11a Turbo mode, support is provided for data rates of up to 108 Mbps.Turbo mode employs the same operating theory as 802.11a but uses twice the bandwidth to provide twice the data rate. The AP-3 unit supports the following data rates: 12, 18, 24, 36, 48, 72, and 108 Mbits/s.
- **802.11b-compliant 2.4 GHz.** The IEEE 802.11b standard supports wireless physical layer in the 2.4 GHz band using Direct Sequence Spread Spectrum (DSSS). The standard provides for data rates of 1, 2, 5.5, and 11 Mbits/s.

The AP-3 device can be used with any combination of 802.11a and 802.11b radio cards. The following configurations are supported:

- one or two 802.11b cards
- one 802.11a card, or
- one 802.11a and one 802.11b card.

Note: Only one 802.11a card with an antenna adapter can be plugged into the AP-3 unit at one time. You can have an 802.11a and an 802.11b card present in the AP-3 device at the same time and the 2.4 GHz and 5 GHz clients will be supported simultaneously. The 802.11a card can only be placed in the slot marked PC CARD A.

Feature List

The IEEE standards that governs wireless communications are different for the 2.4 GHz band and the 5 GHz band. The table below compares the software features supported for each type of card in the AP-3 device:

Feature	2.4 GHz (802.11b)	5 GHz (802.11a)	Comments
Number of stations per BSS	up to 250	up to 50	
HTTP Server	yes	yes	
Telnet / CLI	yes	yes	
SNMP Agent	yes	yes	
VLAN Support (2 User VLANs)	yes	yes	
Emergency Reset to Default Configuration	yes	yes	
DHCP Client	yes	yes	

Feature	2.4 GHz (802.11b)	5 GHz (802.11a)	Comments
DHCP Server	yes	yes	
TFTP	yes	yes	
RADIUS Access Control	yes	yes	
RADIUS Multiple MAC Address Formats	yes	yes	
RADIUS DNS Host Name Support	yes	yes	
RADIUS Start/Stop Accounting	yes	yes	
802.1X (EAP-MD5, EAP-TLS and EAP-TTLS)	yes	yes	
802.1d bridging	yes	yes	
MAC Access Control Table	yes	yes	
Protocol Filtering	yes	yes	
Multicast/Broadcast Storm Filtering	yes	yes	
Proxy ARP	yes	yes	
Configuration Support for MAC Features	yes	yes	
ICMP Echo Response	yes	yes	
Hardware Watchdog Timer	yes	yes	
Roaming	yes	yes	
Link Integrity	yes	yes	
Automatic Channel Select	yes	yes	
WEP	yes	yes	Key lengths supported for 802.11b: 64-bit and 128-bit Key lengths supported for 802.11a: 64-bit, 128-bit, and 152-bit (Note: Some products refer to 64-bit as “40-bit”, 128-bit as “104-bit”, and 152-bit as “128-bit”.)
WEP Plus (Weak Key Avoidance)	yes		No client support for 802.11a
WDS Relay	yes		
Remote Link Test	yes		

Feature	2.4 GHz (802.11b)	5 GHz (802.11a)	Comments
Link Test Responder	yes		No client support for 802.11a
Medium Density Distribution	yes		
Distance between APs	yes		
Ultra High Density	yes		
Closed System	yes		
Interference Robustness	yes		
Load Balancing	yes		No client support for 802.11a
AP List	yes		No client support for 802.11a
SpectraLink VoIP Support	yes		
Fragmentation	yes	yes	
Blocking Intra BSS Clients	yes	yes	
Packet Forwarding	yes	yes	
TCP/UDP Port Filtering	yes	yes	
Dynamic Frequency Selection		yes	For 802.11a products sold in Europe
Per User Per Session Encryption		yes	In conjunction with 802.1x
Syslog Messaging	yes	yes	
Turbo Mode		yes	Turbo mode provides twice the data rate of standard 802.11a mode; not available in all countries

Differences Between 802.11a and 802.11b Feature Sets

The following table provides detailed information on the differences between the 802.11a and 802.11b feature sets.

	2.4 GHz (802.11b)	5 GHz (802.11a)
Physical Layer Type (Modulation Type)	DSSS (Direct Sequence Spread Spectrum)	ODFM (Orthogonal Frequency Division Multiplexing)
Auto Channel Select	Enable (default) Disable	Enable (default) Disable Note: A user cannot manually select a channel for products sold in Europe; these products require automatic channel selection using DFS. See Dynamic Frequency Selection (DFS).

	2.4 GHz (802.11b)	5 GHz (802.11a)
Frequency Channel	1 - 2.412 GHz 2 - 2.417 GHz 3 - 2.422 GHz (default FCC, ETSI, Japan) 4 - 2.427 GHz 5 - 2.432 GHz 6 - 2.437 GHz 7 - 2.422 GHz 8 - 2.447 GHz 9 - 2.452 GHz 10 - 2.457 GHz 11 - 2.462 GHz 12 - 2.467 GHz (ETSI countries only) 13 - 2.472 GHz 14 - 2.477 GHz (Japan only) For France, channels 10-13 only	36 - 5.180 GHz 40 - 5.200 GHz 44 - 5.220 GHz 48 - 5.240 GHz 52 - 5.260 GHz (default FCC) 56 - 5.280 GHz 60 - 5.300 GHz 64 - 5.320 GHz Channels 36-64 are valid for products in the FCC and ETSI regulatory domains. The following channels are available in Japan: 34 - 5.170 GHz (default) 38 - 5.190 GHz 42 - 5.210 GHz 46 - 5.230 GHz For Turbo mode (not available in all countries), the following channels are available: 42 - 5.210 GHz 50 - 5.250 GHz 58 - 5.290 GHz
Regulatory Domain	USA (FCC) Canada (DOC) Europe (ETSI) Spain (SP) France (FR) Japan (MKK)	USA (FCC) Canada (DOC) Europe (ETSI) Japan (MKK)

	2.4 GHz (802.11b)	5 GHz (802.11a)
Transmit Rate	0 - Auto Fallback (default) 1 Mbit/sec 2 Mbits/sec 5.5 Mbits/sec 11 Mbits/sec	0 - Auto Fallback (default) 6 Mbit/sec 9 Mbits/sec 12 Mbits/sec 18 Mbits/sec 24 Mbits/sec 36 Mbits/sec 48 Mbits/sec 54 Mbits/sec For Turbo mode (not available in all countries): 0 - Auto Fallback (default) 12 Mbit/sec 18 Mbits/sec 24 Mbits/sec 36 Mbits/sec 48 Mbits/sec 72 Mbits/sec 96 Mbits/sec 108 Mbits/sec
Distance Between APs	large (default) medium small minicell microcell	N/A
Multicast Rate	1 Mbit/sec 2 Mbits/sec (default) 5.5 Mbits/sec 11 Mbits/sec Available options depend on **Distance Between APs** setting	N/A
Interference Robustness	Enable (default) Disable	N/A
Closed System	Enable Disable (default)	N/A
Load Balancing	Enable (default) Disable	N/A

	2.4 GHz (802.11b)	5 GHz (802.11a)
Medium Density Distribution	Enable (default) Disable	N/A

Cell Size and Coverage Area

The coverage area achieved with the 2.4 GHz card type is larger than that of a 5 GHz radio card. The transmit rate is higher in the smaller (5 GHz) cell than the larger (2.4 GHz cell). The following illustrations depict the difference in cell sizes and the way that cell size affects coverage area.

Figure 3-3: 802.11a (5 GHz) Cell Size

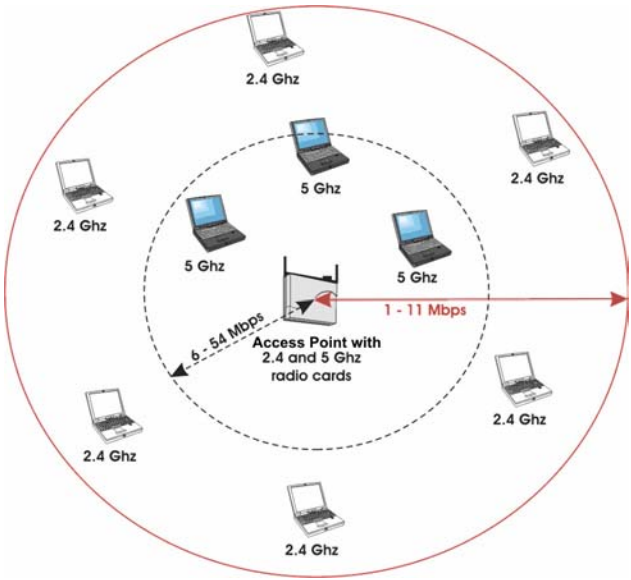
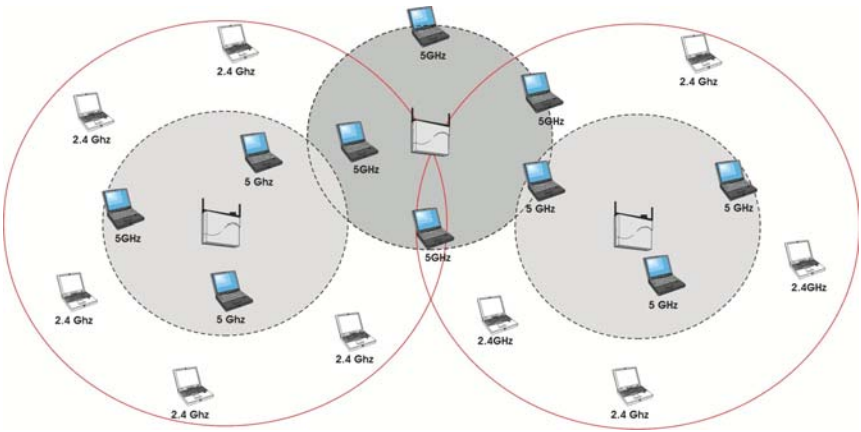


Figure 3-4: 802.11a versus 802.11b Coverage Area



Installation and Initialization

The AP-3 is designed to support both 2.4 GHz (IEEE 802.11b) radio cards and 5 GHz (IEEE 802.11a) radio cards. The Avaya Wireless 5 GHz kit for the AP-3 has an antenna adapter which snaps into place on the existing wall mounting bracket.

Refer to the Quick Start Guide for instructions on installing the Base Station hardware and initializing the unit for your network.

Configuring the AP-3

2

In This Chapter

Since each network is unique, the AP-3 must be configured to operate in your network environment.

Most administrators will only need to use the HTTP Interface (web browser) for configuration. This chapter explains how to configure using the HTTP Interface.

If you prefer to use the Command Line Interface (CLI), refer to Using the Command Line Interface.

In some scenarios described in this chapter, you need to make configuration choices (for example, which radio channel to use). This guide explains each choice. When in doubt, it is recommended that you accept the default values. It is recommended you perform the configuration functions in the order recommended in this chapter.

The following topics are found in this chapter:

Prerequisites

Before configuring the AP-3, you need to gather certain network information. The following section identifies the information you need. A form has been provided at the end of this guide for you to document the configuration settings of each of the AP-3 units in your network. Refer to Record Configuration Settings.

Network Name (SSID of the wireless cards)	Each wireless interface of an AP-3 must be given a Network Name before users can sign on. This is not the same as the System Name, which applies only to the AP-3 unit. This may apply to the isolated unit, the immediate, active network, or to multiple networks. The network administrator typically provides the Network Name(s).
(HTTP) Password	Each AP-3 requires a read/write password to access the web interface. The default password is “public”.
Authentication Method	A primary authentication server may be configured; a backup authentication server is also optional. The network administrator typically provides this information.
Authentication Server Shared Secret	This is a kind of password shared between the AP-3 and the RADIUS authentication server (so both passwords must be the same), and is typically provided by the network administrator.

Authentication Server Authentication Port	This is a port number (default is 1812) and is typically provided by the network administrator.
Client IP Address Pool Allocation Scheme	The AP-3 can automatically provide IP addresses to clients as they sign on. The network administrator typically provides the IP Pool range.
DNS Server IP Address	The network administrator typically provides this IP Address.

Note: Configuration software comes with the PC Cards used in wireless client computers. The current network profile on the wireless client must contain a valid Network Name. The Network Name is one of the case-sensitive Network Names defined in the AP-3's PC Card "Wireless Interface" properties. For more information, please refer to the PC Card documentation.

Step1: Initialize Units and Download Image Files

SCANTOOL Program

Use ScanTool to initialize units and download image files for any unit connected to the LAN subnet. You can set the IP Address, IP Address Type (Static or Dynamic), and other values. The **SCANTOOL.exe** application is included on the installation CD-ROM.

Note: ScanTool can be installed without prior bench initialization. To track units, you must record the MAC Address and physical location of each unit during installation. Since ScanTool identifies each unit by its MAC Address, you can install multiple units simultaneously and initialize them from ScanTool.

The factory default for the AP-3 is for DHCP operation. If you are using DHCP, the unit requests an IP Address from the DHCP server when rebooted or powered up. Since the IP Address could come from a large DHCP address pool, it may be difficult to identify the IP Address assigned to the unit.

Use the following procedure to open ScanTool and set AP-3 network parameters. You should have the AP-3 unit(s) and your computer connected to the same LAN subnet.

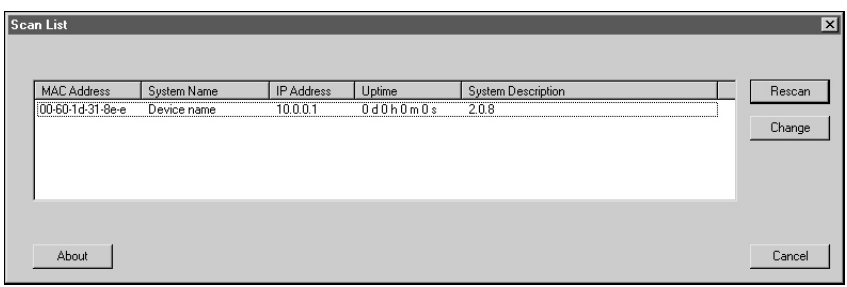
1. Install the AP-3 hardware and connect the unit(s) to the LAN.
2. Power up, reboot, or reset the AP-3.

   Result: If set for DHCP, the unit requests an IP Address from the network DHCP server.

3. Open ScanTool.

   Result: ScanTool scans the subnet and locates all AP-3 units. The ScanTool **Main** dialog appears. The dialog example below shows a single unit in the factory default state.

Figure 2-1: Scan Tool

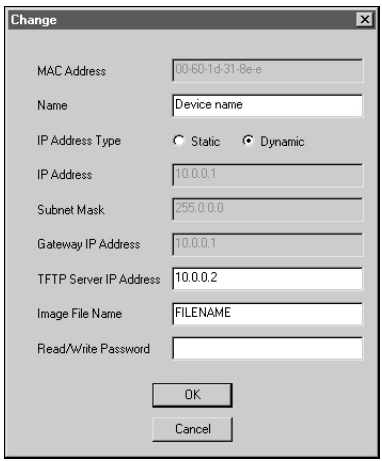


- To re-scan the network and update the display after changing values, click the **Rescan** button.

- To change values or download an AP Image, select the desired unit, and then click the **Change** button.

  Result: the ScanTool **Change** dialog appears, similar to the following example. Our example shows a unit with factory default settings.

Figure 2-2: Scan Tool Change Page



You may perform the following operations.

Note: Certain options are available only when selecting Static IP Address mode.

MAC Address	Displays the MAC Address of the selected unit. This is a **read-only** field.
Name	Enter the System Name of the unit. This is typically descriptive text, such as “Main Lobby”.
IP Address Type	• Select **Static** if you wish to enter the IP values manually. • Select **DHCP** to force the unit to request an IP Address from a DHCP server each time it is powered up or rebooted.
IP Address	If you selected **Static**, enter the IP Address.
Subnet Mask	If you selected **Static**, enter the Subnet Mask.
Gateway IP Address	If you selected **Static**, enter the IP Address of the Gateway.
TFTP Server IP Address	If you wish to download a new AP Image file, enter the IP Address of the TFTP server.

Image File Name	If you wish to download a new AP Image file, enter the full directory path and file name. If the file is located in the default TFTP directory, you only need to enter the file name.
Read/Write Password	Enter the read/write password. The default password is “public”.

To reboot the unit to make the changes effective,

- verify the entered values and
- click the **OK** button.

  Result: The unit will reboot and the new values will be in effect. To cancel the operation and return to the ScanTool **Main** dialog, click the **Cancel** button.

Step 2: Set Basic Configuration Parameters

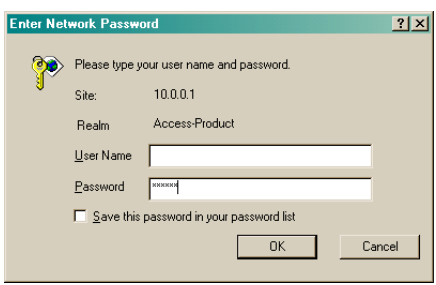
Once you have a valid IP Address assigned to the AP-3 and an Ethernet connection, use a web browser to configure the AP-3 through the Web Interface.

Log Into the AP-3 Unit using the Web Interface

1. Ensure any proxy servers are turned off. Open your browser and enter the IP Address. Press **Enter**.

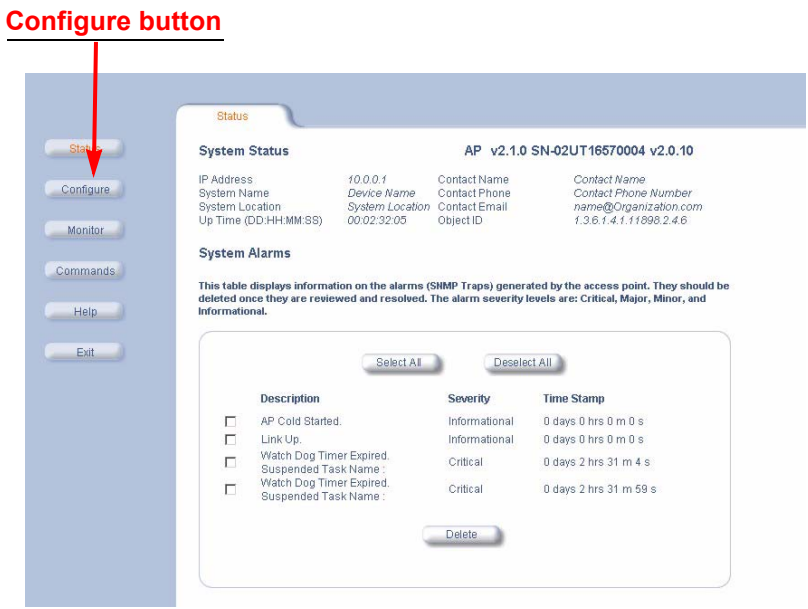
   Result: The AP-3 **Login** page appears.

2. Leave the **User Name** field empty
3. Enter **`public`** in the **Password** field.



   Result: The **System Status** dialog appears.

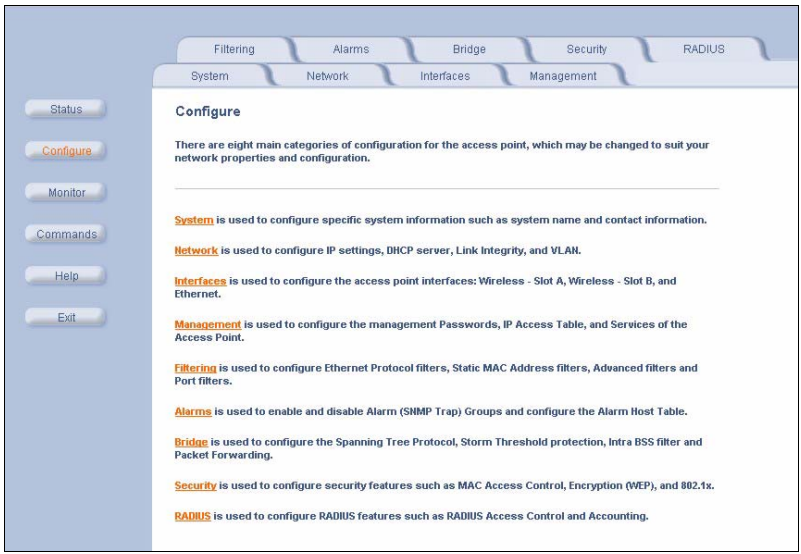
4. Click the **Configure** operation button.



Result: The **System Configuration** dialog appears. Each tab contains information for specific configuration categories.

5. Depending on your system, you can now configure each AP-3 category. In some cases, you do not have to make any changes. If you are in doubt about any setting, it is recommended that you use the default values.

Figure 2-3: Configuration Options



- To set properties for each category, click on the desired tab.

  Result: The selected configuration page appears. Each configuration page allows you to select options, or enter, edit, and delete information.

In some cases, the AP-3 reminds you that it must be rebooted for a change to take effect. **You can wait to reboot until all changes have been made.** After entering or editing information on configuration pages,

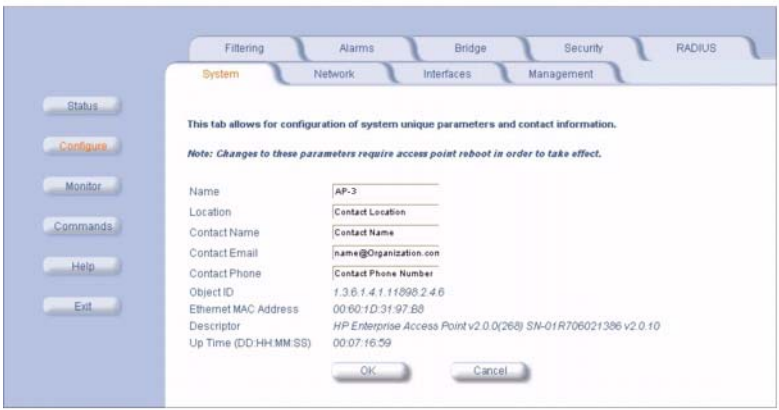
- click **OK** to save changes, or
- click **Cancel** to restore previous settings.

You will want to set up a few basic configuration parameters right away when you receive the AP-3 unit. For example:

- System name and location
- Contact information for network administrator
- IP Address
- Communication rules for your wireless interface(s)
- Passwords for the different management interfaces (SNMP, Telnet, HTTP)
- If you need to upload the latest software, you will also want to setup your TFTP server to communicate with the AP-3 device. This process is described in downloading the latest software, under Setup your TFTP Server.

Set System Name, Location and Contact Information

Figure 2-4: System Configuration



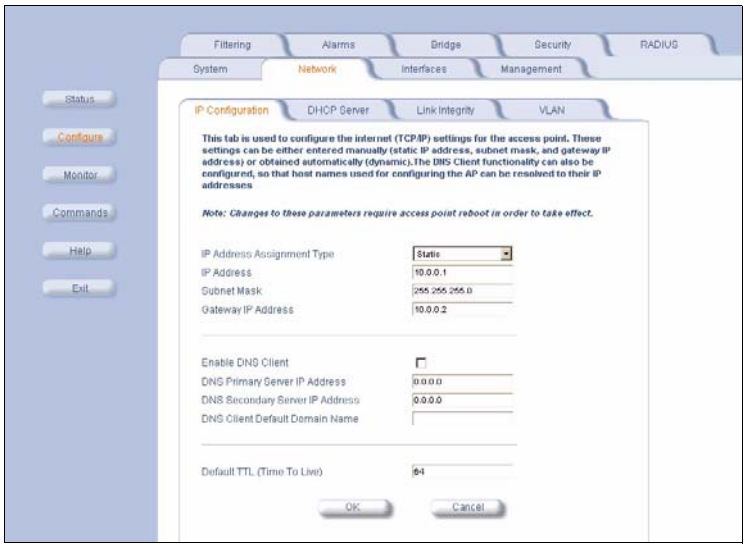
1. In the Web Interface, click the **Configure** button and select the **System** tab.

2. Enter the
   - name of the AP-3 device,
   - its location within your network or its physical location, such as “Front Lobby” or Engineering, and
   - name, phone number and e-mail address of the person responsible for this device.
3. Click **OK**.

Set a Static IP Address for the AP-3 Device

1. In the Web Interface, click the **Configure** button and select the **Network** tab.
2. Set the **IP Address Assignment Type** to **Static**.
3. Enter for the AP-3 unit the following:
   - fixed IP Address,
   - IP mask, and
   - default gateway IP Address.
4. The IP Mask of the AP-3 unit needs to match the IP Mask of your network. If you are setting up the AP-3 device from a client station, check the IP mask of your computer before proceeding.
5. Click **OK** when finished. The AP-3 unit will need to be rebooted for the changes to take effect.

Figure 2-5: Network IP Configuration



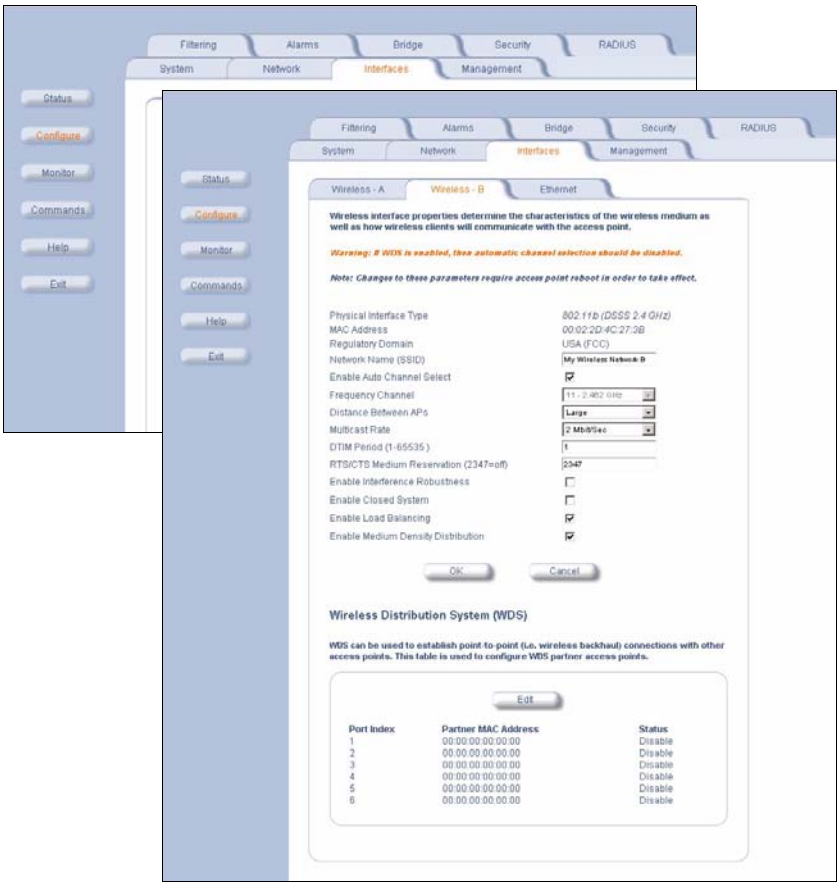
See Maintain 802.11b Client Connections using Link Integrity and Advanced Features for information on the other Network features.

Set Network Names

Client stations use the PC Card Network Name to connect to the network through the AP-3 unit. At power up or insertion of either a 2.4 GHz or 5 GHz radio card, the AP-3 software will automatically detect the card type.

The Configuration and Monitoring parameters displayed in the HTTP Interface will be updated accordingly and default values will be assigned.

Figure 2-6: Wireless Interface Configuration



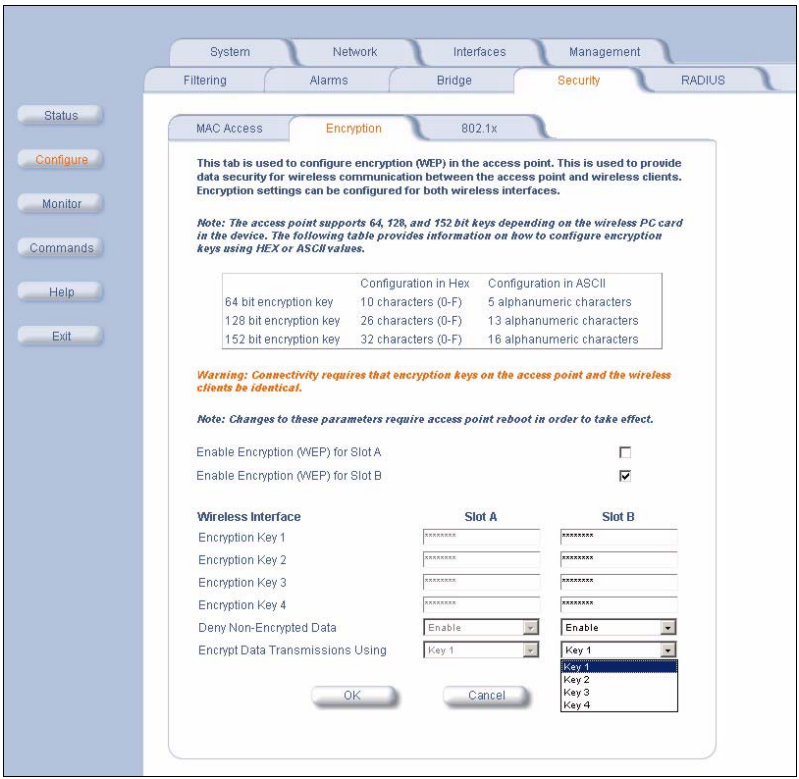
The AP-3 device can be used with any combination of 2.4 GHz (802.11b) and 5 GHz (802.11a) radio cards. Only one 802.11a adapter card can be plugged into the AP-3 unit at one time. You can have an 802.11a and an 802.11b card present in the AP-3 device at the same time, and 2.4 GHz and 5 GHz clients will be supported simultaneously.

Note: Not all software features available for the 802.11b cards are available for the 802.11a cards.

1. In the Web Interface, click the **Configure** button and select the **Interfaces** tab.
2. Select the **Wireless A** or the **Wireless B** tab.
3. Enter Network Names (SSID) for the PC Cards in wireless Slots A and/or B in the AP-3 device.
4. Select **OK**.

Set WEP Encryption for each Wireless Interface

Figure 2-7: WEP Encryption



1. In the Web Interface, click the **Configure** button and select the **Security** tab.

Note: If you want to use 802.1x security, see IEEE 802.1x Security Mode.

2. Select the **Encryption** sub-tab.
3. Click the check box to **enable Encryption (WEP)** on a wireless card.
4. Type in an **Encryption key** based on the type of card present in each slot. You can enter the key in either ASCII characters (a-z, A-Z, and 0-9) or hexadecimal digits (A-F, a-f, and 0-9).

Note: The AP-3 device supports 802.11b cards that use 64-bit or 128-bit encryption. For 802.11a, the AP-3 device supports 64-bit, 128-bit, or 152-bit encryption.

- 64-bit encryption supports key lengths of 5 alphanumeric characters or 10 hexadecimal digits.
- 128-bit encryption supports key lengths of 13 alphanumeric characters or 26 hexadecimal digits.
- 152-bit encryption supports key lengths of 16 alphanumeric characters or 32 hexadecimal digits.

About Encryption Keys: An Encryption Key is composed of the secret key (entered by the user) and a 24-bit Initialization Vector (IV). Some products report an Encryption Key Size with the IV and some report a Key Size without the IV. Therefore, 64-bit encryption is also referred to as “40-bit” encryption (without the IV), 128-bit encryption is also referred to as “104-bit” encryption (without the

IV), and 152-bit encryption is also referred to as “128-bit” encryption (without the IV).

5. Select a key to use for WEP encryption.

Note: Client stations must have the same encryption key to be able to communicate with the AP-3 device.

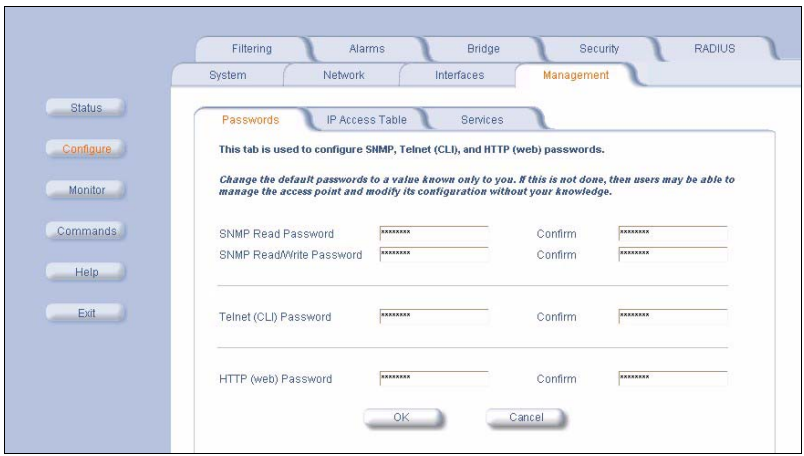
6. For 802.11b only, set **Deny Non-Encrypted Data** to **Enable** if you want to prevent clients that do not have WEP enabled and the proper keys configured from communicating with the network.

7. Select **OK**.

See Step 5: Change Your Wireless Interface Settings for information on the remainder of the wireless configuration parameters. Also, IEEE 802.1x Security Mode for additional security information.

Set and Change Passwords

Figure 2-8: Setting Interface Passwords



1. In the Web Interface, click the **Configure** button and select the **Management** tab.
2. Change the default passwords for the SNMP, Telnet/CLI, and HTTP interfaces.
   - **SNMP Read Password, Confirm**. Enter each password in both the **Read Password** field and the **Confirm** field. The default password is “public”.
   - **SNMP Read/Write Password, Confirm**. Enter the password in

both the **Read Password** field and the **Confirm** field. The default password is “public”.

- **Telnet (CLI) Password, Confirm**. Enter the password in both the **Read Password** field and the **Confirm** field. The default password is “public”.
- **HTTP (Web) Password, Confirm**. Enter the password in both the **Read Password** field and the **Confirm** field. The default password is “public”.

Note: For security purposes It is recommended that you **change ALL PASSWORDS** from the default “public” immediately to restrict access to your network devices to authorized personnel. You should document the AP-3 configuration using the worksheets provided for you in Record Configuration Settings. If you lose or forget your password settings, you can always perform the Reset to Factory Default Procedure.

Step 3: Download the Latest Software

Three types of files can be downloaded to the AP-3 from a TFTP server:

- img (AP software image or kernel)
- config (configuration file)
- bspbl (BSP/Bootloader firmware file)

The latest updates on software and documentation can be found on the Avaya Wireless web site at: www.avaya.com. Also, see SolarWind.net for the latest version of the TFTP server software.

Setup your TFTP Server

The “Trivial File Transfer Protocol” (TFTP) server allows you to transfer files across a network. You can

- upload files from the AP-3 for backup or copying, and
- download the files for configuration and AP Image upgrades.

The TFTP software is located on the Avaya Wireless AP-3 Installation CD-ROM.

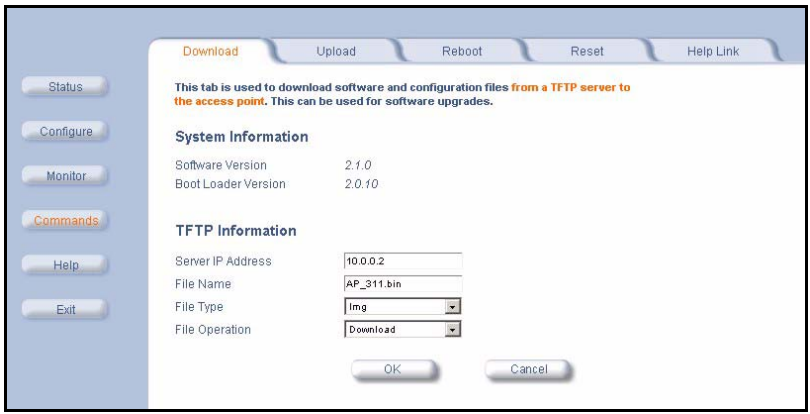
If a TFTP server is not configured and running, you will not be able to download and upload images and configuration files to/from the AP-3. Remember that the TFTP server does not have to be local, so long as you have a valid TFTP IP Address. TFTP does not have to be running for AP-3 operations that do not transfer files.

After the TFTP server is installed:

- Check to see that TFTP is configured to point to the directory containing the AP Image.
- Make sure you have the proper TFTP server IP Address, the proper AP Image file name, and that the TFTP server is connected.
- Make sure the TFTP server is configured to both Transmit and Receive files, with no automatic shutdown or time-out.

Download Updates from your TFTP Server

Figure 2-9: Download Software Image from TFTP Server



1. Make sure the TFTP server is running and pointing to the directory that contains the desired file.
2. In the Web Interface, click the **Commands** button and select the **Download** tab.
3. Type in the IP address of your TFTP server.
4. Type in the file name (including the file extension).

5. Select the file type from the pull down menu.
6. Reboot the unit in order for the changes to take effect.

Backup your AP-3 Configuration File

1. Make sure the TFTP server is running and pointing to the directory where you want to save the file.
2. In the Web Interface, click the **Commands** button and select the **Upload** tab.
3. Type in the IP address of your TFTP server.
4. Type in a descriptive name for your configuration file.
5. Select the file type as **config** from the pull down menu.
6. Click **OK** to upload this information from the AP-3 unit to the TFTP server. The information can be retrieved in the event you reset your AP-3 device to factory defaults.

Note: Record the name of this configuration file and the IP address of the AP-3 unit so you can easily find it if you need to download it.

Copy a Configuration File from Another AP-3 Unit

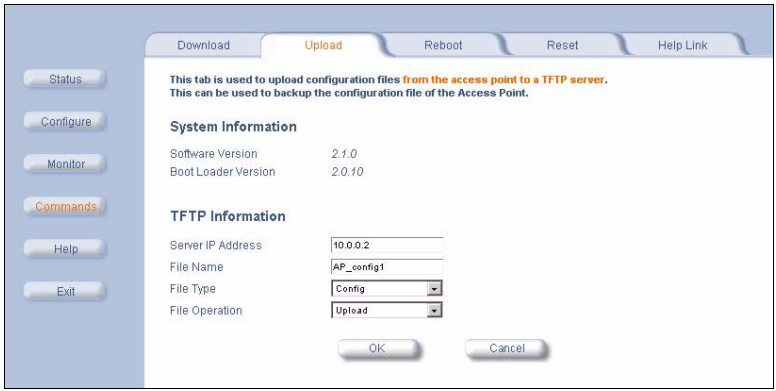
You can configure multiple units using the same configuration file by

- uploading the configuration file from one AP-3 unit to the TFTP server, and
- download the configuration file to other AP-3 units.

Caution: Do not use a static IP address in this configuration file, otherwise you will end up with duplicate IP addresses in your network!

1. Check to ensure Dynamic IP address is enabled by clicking the **Configure** button and selecting the IPConfig tab.
2. In the Web Interface, click the **Commands** button and select the **Upload** tab.
3. Enter the IP address of your TFTP server.

Figure 2-10: Upload Configuration File to TFTP Server



11. Enter the name of your configuration file and click **OK**.
12. Wait for the file to transfer from the AP-3 device to the TFTP server.
13. Access the AP-3 unit to which you will download the configuration. A system window will notify you when this process is complete. Confirm by clicking **OK**.
14. Click the **Commands** button, then select the **Download** tab.

15. Verify the IP address of your TFTP server and enter the name of the file you wish to transfer (see Step 3).
16. Set the file type to **config**, and click **OK**.
17. Click **Download**.
18. Reboot the unit for the changes to take effect.
19. Repeat this procedure for all the AP-3 units you want to configure using this specific file.

Step 4: Other Network Settings

You may want to set other configuration parameters for your AP-3 unit, such as:

- Configure the AP-3 device as a DHCP Server
- Maintain 802.11b client connections using Link Integrity
- Change your Wireless Interface settings
- Configure the physical interface that will be used to manage the AP-3 unit
- Control access to the AP-3 device using MAC Address authentication, WEP encryption, or 802.1x security settings

Refer to Advanced Features for more complex network settings.

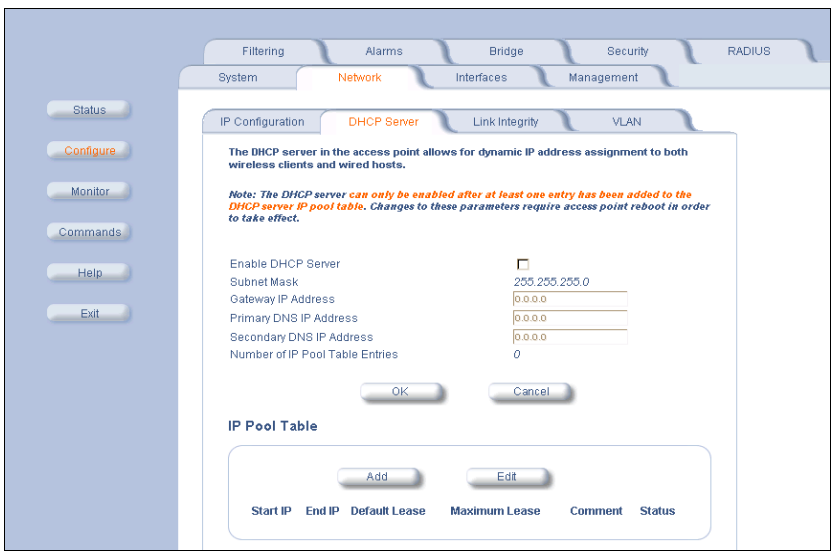
Configure the AP-3 Device as a DHCP Server

Warning: Make sure there is only one DHCP server on the network and **do not** enable the DHCP server without checking with your network administrator first. If you enable the server without checking with your administrator, it could bring down the entire network.

Use DHCP configuration to provide dynamic client IP Addresses from one or more IP Pool Tables. Enable the DHCP Server to allow the AP-3 to assign clients IP Addresses from IP Pool Tables. Deselect the Status check box to prevent client IP Address assignment from the AP-3.

Note: There must be at least one entry in the DHCP Server client IP Address assignment table before you can enable the DHCP Server Status feature.

Figure 2-11: Network Configuration Pages - DHCP Server



1. In the Web Interface, click the **Configure** button and select the **Network** tab.
2. Select the **DHCP Server** sub-tab.
3. Click the **Add** button in the IP Pool Table.
4. Enter the following information:
   - **Start IP Address**
   - **End IP Address**
   - **Default Lease Time (optional)** - the default time value for clients to retain the assigned IP Address. DHCP automatically renews IP Addresses without client notification. Default is 86400 seconds.
   - **Maximum Lease Time (optional)** - the maximum time value for clients to retain the assigned IP Address. DHCP automatically renews IP Addresses without client notification. Default is 86400 seconds.
   - Comment (optional)
   - **Status** - IP Pools are enabled upon entry in the table. Use the **Edit** button to disable or delete existing table entries.
5. Enter the **Default Gateway IP Address**, the **Primary** and **Secondary DNS IP Addresses**, and select the **Enable DHCP Server** check box.
6. Reboot the AP-3 unit for the changes to take affect.

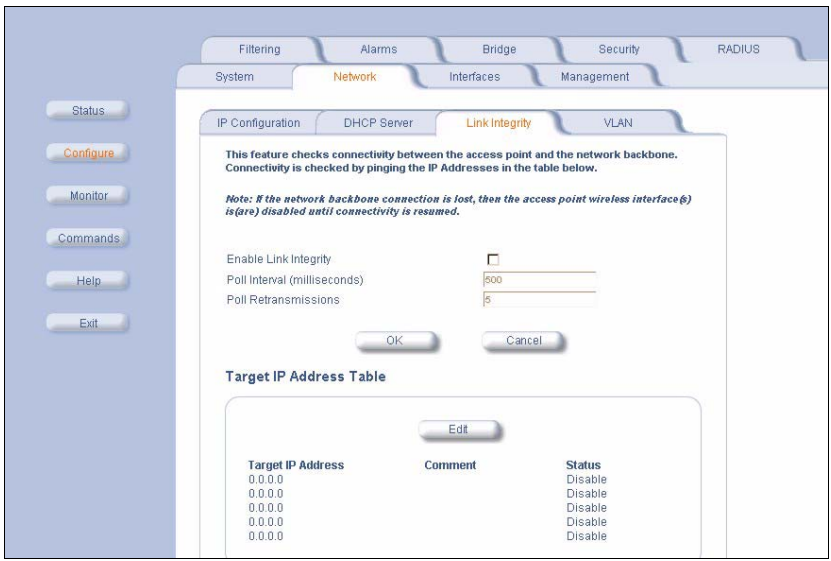
Maintain 802.11b Client Connections using Link Integrity

Note: This feature is only applicable to 2.4 GHz (802.11b) cards.

The Link Integrity feature checks the link between the AP-3 and the nodes on the backbone. These nodes are listed by their IP address on the Link Integrity IP Address Table, and serve as backup. If the link goes down, the client will connect to another AP-3 in your network that still communicates with the server.

Configure Link Integrity

Figure 2-12: Link Integrity



1. In the Web Interface, click the **Configure** button and select the **Network** tab.
2. Select the **Link Integrity** sub-tab.
3. Click the **Edit** button in the **Target IP Address Table**.

4. Enter the IP Address of the host computer you want to check, and add comments to identify the computer if you wish. This Target IP Address is enabled as soon as it is entered in the table. Click **OK**.
5. Set the following parameters as needed:
   - **Poll Interval** - the interval between link integrity checks. Range is 500 - 15000 ms in increments of 500 ms. The default is 500 ms.
   - **Poll Retransmissions** - the number of times a poll should be retransmitted before the link is considered down.
6. Click to select the **Enable Link Integrity** check box.

Disable Link Integrity

- To disable Link Integrity check for all clients, deselect the **Enable Link Integrity** check box.
- To disable Link Integrity check to a certain host computer, click the **Edit** button in the **Target IP Address Table** and set the **Status** to **Disable**.

Step 5: Change Your Wireless Interface Settings

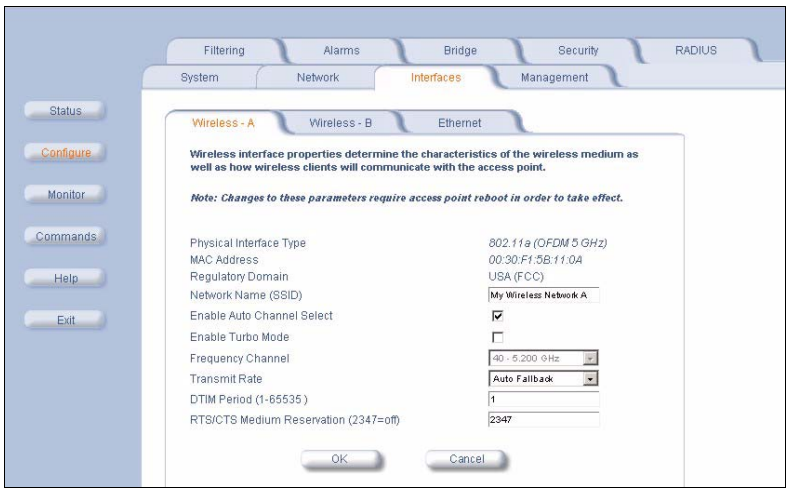
Depending on the type of wireless PC Card installed in the AP-3 device, the configuration options will be different. Some parameters are the same for 802.11a and 802.11b cards. Others are unique to each card type.

You can setup an AP-3 unit using the following combinations of wireless cards:

- single 802.11a card with the attached antenna adapter
- single 802.11b card
- two 802.11b cards (one in each slot)
- one 802.11a card with attached antenna and one 802.11b card

802.11a Wireless Interface Card

Figure 2-13: 802.11a Wireless Interface Options



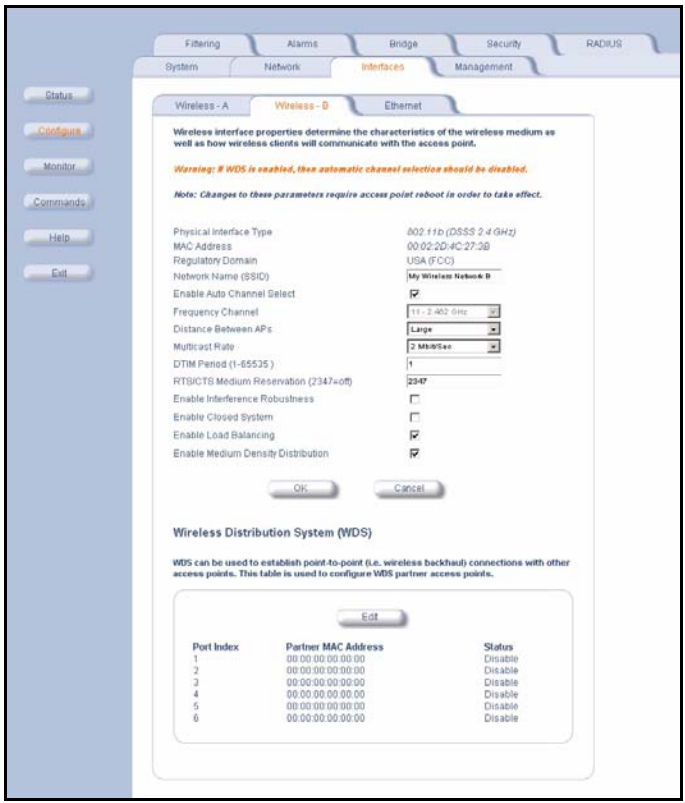
Field	Description
Network Name	Enter a Network Name for each PC Card. This is the same name used on client machines to connect using the client configuration software. • Range is 1 - 31 characters. • **Default** is “My Wireless Network A” for card in Slot A and “My Wireless Network B” for card in Slot B.
Enable Auto Channel Select (ACS)	By **default** this feature is enabled. The AP-3 device • scans the area for other AP-3 devices and • selects a free or relatively unused communication channel. This helps prevent interference problems and increases network performance. **Note:** This option is not available for 802.11a products in Europe. See Dynamic Frequency Selection (DFS) for more information.

Field	Description
Turbo Mode	An 802.11a card supports an extension of the IEEE 802.11a standard that provides twice the data rate. By **default**, Turbo mode is disabled. **Note:** Turbo mode is not defined in the IEEE 802.11a specification. Turbo mode is not available in all countries including European countries and Japan.
Frequency Channel	If Auto Channel Select is disabled, use the pull-down menu to select the desired card frequency. Ensure nearby devices do not use the same frequency. The Frequency Channels available will depend on the following: • card type, • card mode (standard mode or Turbo mode), and • country of use. Refer to Radio Specifications for details.

Field	Description
Transmit Rate	Use the pull-down menu to select a specific transmit rate for the 802.11a card. Choose between 6, 9, 12, 18, 24, 36, 48, 54 Mbits/s, or Auto Fallback for standard 802.11a mode. If Turbo mode is enabled, choose between 12, 18, 24, 36, 48, 72, 98, 108 Mbits/s, or Auto Fallback. The Auto Fallback feature allows the AP-3 unit to select the best transmit rate based on the cell size. The default is Autofallback.
DTIM Period	Deferred Traffic Indicator Map (DTIM) is used with clients that use power management. DTIM should be left at the default value. Range is 1-65535.
RTS/CTS Medium Reservation	This value affects message flow control, and should not be changed under normal circumstances. When set to a value between 0 and 2347, the card uses the RTS/CTS mechanism for packets that are the specified size or greater. Range is 0 to 2347; default is 2347 (off).

802.11b Wireless Interface Card

Figure 2-14: 802.11b Wireless Interface Options



Field	Description
Network Name	Enter a Network Name for each PC Card. This is the same name used on client machines to connect using the client configuration software. • Range is 1 - 31 characters. • **Default** is “My Wireless Network A” for card in Slot A and “My Wireless Network B” for card in Slot B.
Enable Auto Channel Select (ACS)	By **default** this feature is enabled. The AP-3 device • scans the area for other AP-3 devices and • selects a free or relatively unused communication channel. This helps prevent interference problems and increases network performance. If you are setting up a Wireless Distribution System (WDS), it must be disabled. See Auto Channel Select (ACS) for additional information on this feature.

Field	Description
Frequency Channel	If Auto Channel Select is disabled, use the pull-down menu to select the desired card frequency. Ensure nearby devices do not use the same frequency. The Frequency Channels available will depend on the following: • card type, and • country of use. Refer to Radio Specifications for details.
Distance Between APs	Set to **Large**, **Medium**, **Small**, **Microcell,** or **Minicell** depending on the site survey for your system. The distance value is related to the **Multicast Rate** (described next). In general, larger systems operate at a slower average rate. This feature is only available for 802.11b wireless cards. **Default** is large.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Multicast Rate</td><td>Set the rate at which Multicast messages may be sent. This value is related to the Distance Between APs parameter.This feature is only available for 802.11b wireless cards. Default is 2 Mbits/sec.

<table>
<tr><th>Distance between APs</th><th>Multicast Rate</th></tr>
<tr><td>Large</td><td>1 and 2 Mbits/sec</td></tr>
<tr><td>Medium</td><td>1, 2, and 5.5 Mbits/sec</td></tr>
<tr><td>Small</td><td>1, 2, 5.5 and 11 Mbits/sec</td></tr>
<tr><td>Minicell</td><td>1, 2, 5.5 and 11 Mbits/sec</td></tr>
<tr><td>Microcell</td><td>1, 2, 5.5 and 11 Mbits/sec</td></tr>
</table>
</td></tr>
<tr><td>DTIM Period</td><td>Deferred Traffic Indicator Map (DTIM) is used with clients that use power management. DTIM should be left at the default value. Range is 1-65535.</td></tr>
</table>

Field	Description
RTS/CTS Medium Reservation	This value affects message flow control, and should **not be changed** under normal circumstances. When set to a value between 0 and 2347, the card uses the RTS/CTS mechanism for packets that are the specified size or greater. Range is 0 to 2347. **Default** is 2347 (off).
Enable Interference Robustness	Enable this option if other electrical devices in the 2.4 GHz range may be interfering with the wireless signal. This feature is only available for 802.11b wireless cards. **Default** is enable.
Enable Closed System	Check this box (enable) to allow only clients configured with your specific Network Names to access the AP-3. When the box is unchecked (disable), a client configured with the Network Name “ANY” can connect to the AP-3. This feature is only available for 802.11b wireless cards. **Default** is disable.

Field	Description
Enable Load Balancing	Enable this option so clients can evaluate which access point to associate with, based on current AP loads, to more evenly balance the load between APs. This feature is only available for systems using two 802.11b wireless cards. **Default** is enable.
Enable Medium Density Distribution	Enable this option to automatically notify client stations of roaming thresholds for the nearby APs. This feature is only available for 802.11b wireless cards. **Default** is enable.

Auto Channel Select (ACS)

When Auto Channel Select is enabled, an AP-3 selects its own frequency channel based on

- interference situation,
- bandwidth usage, and
- adjacent channel use.

This is beneficial when deploying AP-3 units in a new environment or adding an AP-3 unit in an existing environment.

The first AP-3 turned on within an area assigns itself the default channel (which differs based on card type and regulatory region). When a second AP-3 unit is turned on in the vicinity of the first AP-3 device, the Auto Channel Select feature changes the frequency channel of the second unit so there is no interference between the two units. Multiple AP-3 units can be turned on simultaneously to establish proper channel selection. In addition, you may override Auto Channel Select and manually configure the AP-3 device to use a specific Channel.

Note: If you plan to use ACS, you should be aware of the following:

- The range of available channels varies based upon the regulatory domain of your wireless cards. Some regulatory agencies allow more channels than others.
- ACS is enabled by default.
- You must disable ACS and manually configure the AP-3's channel if you intend to create a Wireless Distribution System (see Wireless Distribution System (WDS) in Advanced Features).
- The ability to enable or disable ACS is not available for 802.11a products sold in Europe. See Dynamic Frequency Selection (DFS) for details.

Disabling ACS

1. From the Web interface, select **Configuration** then click the **Interfaces** tab.
2. Deselect the check box next to **Enable Auto Channel Select**.
3. Select a frequency channel from the drop-down menu. The clients automatically sense the channel and will configure themselves to reassociate on the new channel.
4. On changing the status you must reboot your AP-3, which will disconnect all clients from the AP-3.

Enabling ACS

1. From the Web interface, select **Configuration** then click the **Interfaces** tab.
2. Select the check box to **Enable Auto Channel Select**.

CAUTION: On changing the status you must reboot your AP-3, which will disconnect all clients from the AP-3.

Dynamic Frequency Selection (DFS)

Dynamic Frequency Selection (DFS) is a technique used in 802.11a cards sold in Europe (for example, cards whose regulatory domain is set to the European Telecommunications Standard Institute (ETSI). DFS automatically selects an operating channel. ETSI requires that 802.11a devices use DFS to prevent interference with radar systems and other devices that already occupy the 5 GHz band.

802.11a cards sold in Europe use a technique called Dynamic Frequency Selection (DFS) to automatically select an operating channel. During boot-up, the AP-3

- scans the available frequency and
- selects a channel that is free of interference. If the AP-3 subsequently detects interference on its channel, it automatically reboots and selects another channel that is free of interference.

If you are using 802.11a cards in Europe, keep in mind the following:

- DFS is not a configurable parameter. It is always enabled and cannot be disabled.
- You cannot manually select an operating channel for 802.11a cards; you must let DFS select the channel.
- You cannot configure the **Enable Auto Channel Select** option. Within the HTTP interface, this option will always appear enabled.
- 802.11b cards (and 802.11a cards outside of Europe) use ACS (which can be enabled or disabled, see Auto Channel Select (ACS) for details).

Distance Between APs

Note: This feature is only applicable to 2.4 GHz (802.11b) cards.

Cells

Distance Between APs defines how far apart (physically) your AP-3 devices are located, which in turn determines the size of your cell. Cells of different sizes have different capacities and therefore suit different applications. For instance, a typical office has many stations requiring high bandwidth and transmit rates for complex, high-speed data processing. In contrast, a typical warehouse has a few forklifts requiring low bandwidth and transmit rates for simple transactions.

Cell capacities are compared in the following table, which shows small cells suit most offices, while large cells suit most warehouses:

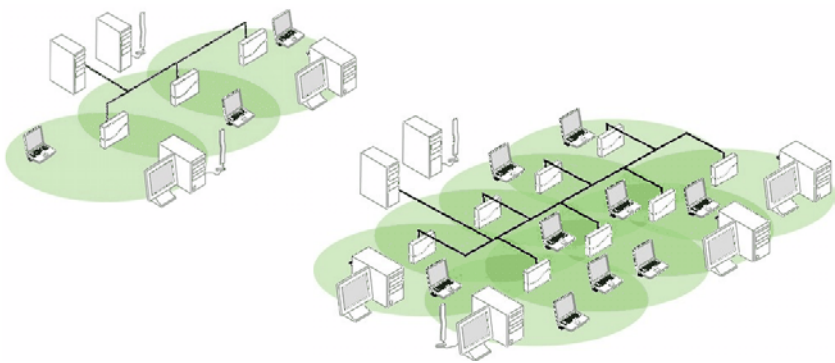
Small Cell	Large Cell
Physically accommodates few stations	Physically accommodates many stations
High cell bandwidth per station	Lower cell bandwidth per station
High transmit rate	Lower transmit rate

Coverage

The number of access point units in a set area determines the network coverage for that area. A great number of access point units covering a small area would be a high-density cell. Few access point units, or even a single unit covering the same small area would result in a low-density cell, even though in both cases the actual area did not change; only the number of access points covering the area changed.

In a typical office, smalls cells may have a 3 meter (10 ft.) diameter and an AP-3 device every 6 m (20 ft.), which would be considered high density. In contrast, large cells in a typical warehouse may have a 27.5 meter (90 ft.) diameter and an AP-3 unit every 60 m (200 ft.), considered low density.

Figure 2-15: Low Density vs. Ultra High Density Network



Set the Distance Between APs

1. From the Web interface, click the **Configure** button, and select the **Network** tab.
2. Select the **Interfaces** sub-tab.
3. Select the **Wireless Slot** tab that corresponds to an 802.11b card.
4. Use the drop-down menu to set the Distance Between APs for the appropriate card. The AP-3 recognizes the following five values for the Distance Between APs parameter (configurable for each Wireless NIC): Large, Medium, Small, Minicell, and Microcell.

CAUTION: The distance between APs should not be approximated. It is calculated by means of a manual Site Survey, in which an AP-3 unit is set up and clients are tested throughout the area to determine signal strength and coverage, and local limits such as physical interference are investigated.

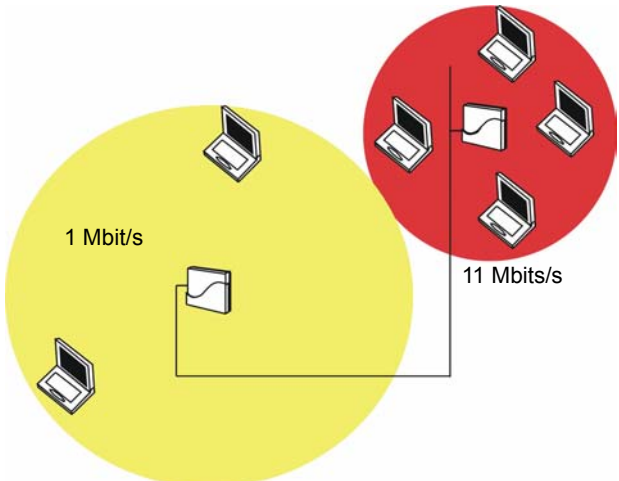
From these measurements the appropriate cell size and density is determined, and the optimum distance between APs is calculated to suit your particular business requirements.

Multicast Rate

The multicast rate measures how quickly information is transmitted across your network. This rate is approximated for a cell, since physical proximity to the AP increases throughput. Stations closer to an AP actually have higher multicast rates than stations in the same cell that are located farther from the AP. In addition, a small cell with several stations located close to the AP-3 unit can actually transmit information faster than a larger cell with only a few stations located farther from the AP-3 device.

Note: This feature is only applicable to 2.4 GHz (802.11b) cards.

Figure 2-16: 1 Mbits/s and 11 Mbits/s Multicast Rates



Note: There is an inter-dependent relationship between the Distance between APs and the Multicast Rate. In general, larger systems operate at a lower average transmit rate.The variation between Multicast Rate and Distance Between APs is presented in the following table:

	1.0 Mbit/s	2.0 Mbits/s	5.5 Mbits/s	11 Mbits/s
Large	yes	yes		
Medium	yes	yes	yes	
Small	yes	yes	yes	yes
Minicell	yes	yes	yes	yes
Microcell	yes	yes	yes	yes

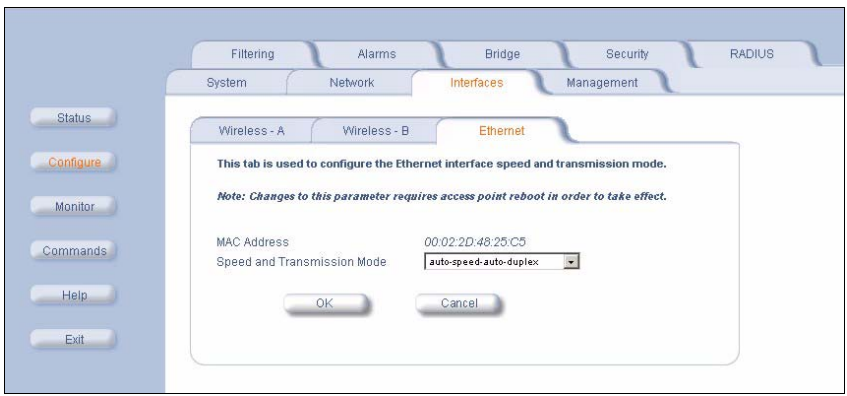
Set the Multicast Rate

1. From the Web interface, click the **Configure** button, and select the **Network** tab.
2. Select the **Interfaces** sub-tab.
3. Select the **Wireless Slot** tab that corresponds to an 802.11b card.
4. Use the drop down menu to select a **Multicast rate**.
5. The Distance Between APs **must be set before** the Multicast Rate, because when you select the Distance Between APs, the appropriate range of Multicast values automatically populates the drop down menu.

Step 6: Ethernet Settings

Set Ethernet Speed and Transmission Mode

Figure 2-17: Ethernet Interface



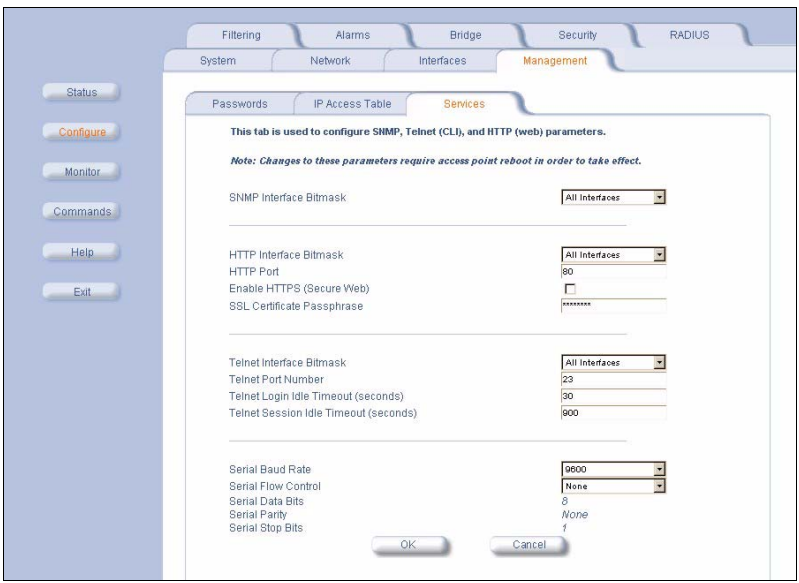
Select the desired speed and transmission mode from the pull down menu. Half-duplex means that only one side can broadcast at a time, full-duplex allows both sides to transmit, while auto-duplex selects the best transmission mode for the given configuration. The recommended setting is **auto-speed-auto-duplex**. Choose between:

- 10 Mbit/s - half duplex, full duplex, or auto duplex
- 100 Mbit/s - half duplex, full duplex, or auto duplex
- auto speed - half duplex, auto duplex

Step 7: Configure your Management Interfaces

Select which interfaces will be available through the Wireless, Ethernet, and Serial Port interfaces of the AP-3 unit.

Figure 2-18: Management Interface Settings



Set HTTP Interface Management Services

1. In the Web Interface, click the **Configure** button and select the **Management** tab.
2. Choose the **Services** sub-tab.
3. For each service, there is a list of associated settings. From the drop-down menu, select which physical interface(s) can be used to manage the AP-3 device using the Web interface. For example, to allow Web configuration via the Ethernet network only, set **HTTP Interface Bitmask** to **Ethernet**. The available configuration options are:
   - Disabled (all interfaces)
   - Ethernet only enabled
   - Wireless A only enabled
   - Wireless B only enabled
   - All Interfaces enabled
4. Enter the HTTP communication port number. Default is 80.

Note: See Configuring Management Service Interfaces for information on the SNMP, Telnet, and other HTTP parameters that can be configured from the Services page.

Configure Serial Port Interface Settings

The serial port interface on the AP-3 device is enabled at all times. You can set the following parameters as needed:

- **Baud Rate**. Select the serial port speed (bits per second). Choose between 2400, 4800, 9600, 19200, 38400, or 57600; the default Baud Rate is **9600**.
- **Flow Control**. Select either **None** (default) or **Xon/Xoff** (software controlled) data flow control.

Note: It is recommended that you leave the setting for Flow Control to its default value (none) unless you are sure what this setting should be.

Step 8: Other Security Configuration Settings

Control access to the AP-3 device using

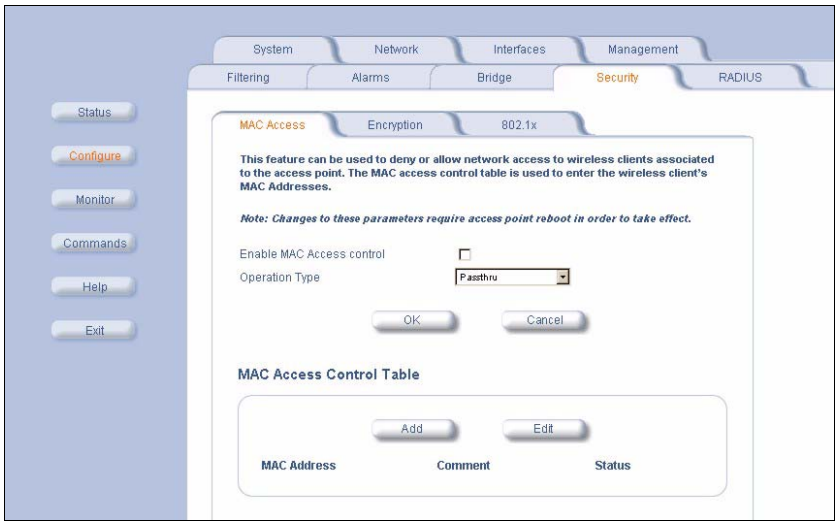
- MAC Address authentication,
- WEP encryption, or
- 802.1x security settings.

Configure your MAC (Address) Access Control Table

The MAC Authentication tab allows you to build a list of stations, identified by their MAC addresses, authorized to access the AP-3 device within your network. The list is stored inside each AP-3 within your network.

- **Enable MAC Access Control**. Check this box to enable the Control Table.
- **Operation Type**. Choose between **Passthru** and **Block**. This determines how the stations identified in the MAC Access Control Table are filtered.

Figure 2-19: Security Configuration Page - MAC Authentication



Add an Entry to the MAC Access Control Table

1. Click the **Add** button in the **MAC Access Control Table**.
2. Enter the MAC address of the client station authorized to manage this AP-3 device.
3. Add a comment as needed. Entries are automatically enabled.

Disable or Delete an Entry in the MAC Access Control Table

1. Click the **Edit** button in the MAC Access Control Table.
2. Select the MAC Address you want to disable or delete.
3. Click **OK**.

Note: For larger networks that include multiple AP-3 devices, you may prefer to maintain this list on a centralized location using the RADIUS Authentication Settings.

RADIUS Authentication Settings

The AP-3 provides two methods for authenticating wireless clients using a RADIUS Server: MAC Access Control Via RADIUS and IEEE 802.1x Security Mode.

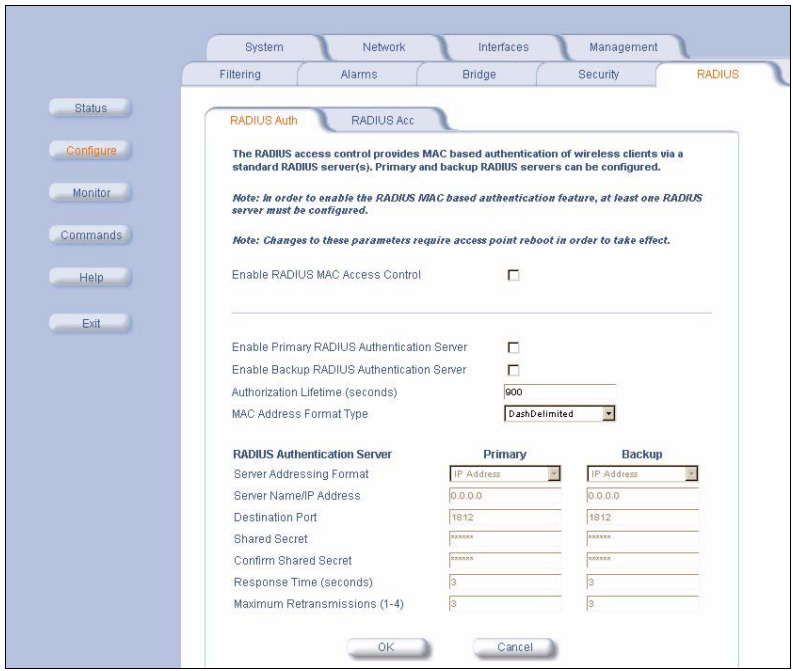
Note: The AP-3 supports additional RADIUS features. See Advanced RADIUS Features for details.

MAC Access Control Via RADIUS

If you want to control wireless access to the network and if your network includes a RADIUS Server, you can store the list of MAC addresses on the RADIUS server rather than configure each AP-3 individually. From the RADIUS Authentication tab, you can define the IP Address of the server that contains a central list of MAC Address values that identify the authorized stations that may access the wireless network. You must specify information for at least the Primary RADIUS server. The Backup RADIUS server is optional.

Note: Problems with RADIUS Server configuration or RADIUS Authentication should be referred to the RADIUS Server developer.

Figure 2-21: Security Configuration Page - RADIUS Authentication



Field	Description
Enable RADIUS MAC Access Control	Click inside the check box to provide authentication by the RADIUS server. Deselect the check box to prevent use of the RADIUS server.
Enable the Primary or Backup RADIUS Server	Click in the desired check box to enable the RADIUS Server. You must specify information for at least the Primary RADIUS server. The Backup RADIUS server is optional.
Authorization Lifetime (seconds)	Enter the time, in seconds, each client session may be active before being automatically re-authenticated. Range is 60 - 43200 seconds (in 1 sec increments). **Default** is 900 sec.

Field	Description
MAC Address Format Type	Enter the format in which the 12-digit MAC addresses are listed within the RADIUS server. Options include • dash delimited (dash between each pair of digits: xx-yy-zz-aa-bb-cc), • colon delimited (colon between each pair of digits: xx:yy:zz:aa:bb:cc), • single dash delimited (dash between the sixth and seventh digits: xxyyzz-aabbcc), and • no delimiters between pairs of hexadecimal digits (xxyyzzaabbcc).
Server Addressing Format	Select either server name or IP address. Use a server name only if you have enabled the DNS Client functionality. See RADIUS DNS Host Name Support.
Server Name/IP Address	Enter the server's IP address or name (depending on the Server Addressing Format setting) in the field provided.
Destination Port	Enter the RADIUS Authentication port. The **default** value is 1812.

Field	Description
Shared Secret	The password for the user on the RADIUS Server must be the same as the Shared Secret.
Response time (seconds)	Enter the maximum time, in seconds, to wait for RADIUS to respond with authentication status.
Maximum Retransmissions	Enter the maximum number of times an authentication may be retransmitted.

IEEE 802.1x Security Mode

IEEE 802.1x is a standard that provides a means to authenticate and authorize network devices attached to a LAN port. A port in the context of IEEE 802.1x is a point of attachment to the LAN, either a physical Ethernet connection or a wireless link to an Access Point.

802.1x uses the Extensible Authentication Protocol (EAP) as a standards-based authentication framework, and supports automatic key distribution for enhanced security. The EAP-based authentication framework can easily be upgraded to keep pace with future EAP types.

Popular EAP types include:

- **EAPoL (EAP over LAN):** Transport protocol used to negotiate the WLAN user's secure connection to the network. EAP messages are encapsulated in 802.1X messages.
- **EAP-Message Digest 5 (MD5):** Username/Password-based authentication; does not support automatic key distribution
- **EAP-Transport Layer Security (TLS):** Certificate-based authentication (a certificate is required on the server and each client); supports automatic key distribution
- **EAP-Tunneled Transport Layer Security (TTLS):** Certificate-based authentication (a certificate is required on the server; a client's username/password is tunneled to the server over a secure connection); supports automatic key distribution
- **PEAP - Protected EAP with MS-CHAP v2:** Secure username/password-based authentication; supports automatic key distribution

Different servers support different EAP types and each EAP type provides different features. Refer to the documentation that came with your RADIUS server to determine which EAP types it supports.

Note: The AP-3 supports the following EAP types:

- When 802.1x Security Mode is set to 802.1x, EAP-TLS, PEAP, and EAP-TTLS are supported.
- When 802.1x Security Mode is set to Mixed, EAP-TLS, PEAP, EAP-TLLS, and EAP-MD5 (MD5 does not support automatic key distribution; therefore, if you choose this method you need to manually configure each client with the network's encryption key) are supported.

Authentication Process

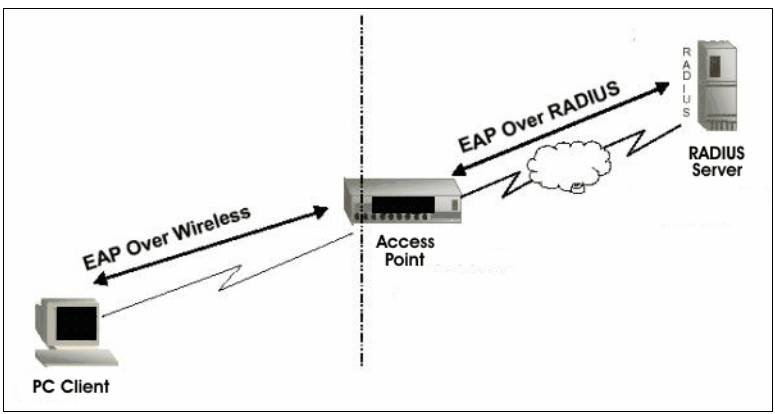
There are three main components in the authentication process. The standard refers to them as:

1. supplicant (client PC)
2. authenticator (Access Point)
3. authentication server (RADIUS server)

When using 802.1x Security Mode or Mixed mode (802.1x and WEP), you need to configure your RADIUS server for authentication purposes.

Prior to successful authentication, an unauthenticated client PC cannot send any data traffic through the AP-3 device to other systems on the LAN. The AP-3 device inhibits all data traffic from a particular client PC until the client PC is authenticated. Regardless of its authentication status, a client PC can always exchange 802.1x messages in the clear with the AP-3 unit (the client begins encrypting data after it has been authenticated).

Figure 2-22: RADIUS Authentication Illustrated



The AP-3 device acts as a pass-through device to facilitate communications between the client PC and the RADIUS server. The AP-3 unit and the client PC exchange 802.1x messages using an EAPOL (EAP Over LAN) protocol. Messages sent from the client station are encapsulated by the AP-3 device and transmitted to the RADIUS server using EAP extensions.

Upon receiving a reply EAP packet from the RADIUS, the message is typically forwarded to the client PC, after translating it back to the EAPOL format. Negotiations take place between the client PC and the RADIUS server. After the client has been successfully authenticated, the client PC receives an encryption key from the AP-3 (if the EAP type supports automatic key distribution). The client uses this key to encrypt data after it has been authenticated. For 802.11a, each client receives its own unique encryption key; this is known as Per User Per Session Encryption keys. (This feature is only available when using 802.1x mode; it is not available when in Mixed mode or using WEP encryption only).

Configuring Security Settings

Click the 802.1x tab in the **Security Configuration** page to set the 802.1x security mode for the AP-3. (Note that the configuration settings for standard encryption (that does not use 802.1x) are located on the Encryption page.) The AP-3 software offers four security settings:

Security Setting	Description
No security or encryption	Set the 802.1x Security Mode to **none** on the 802.1x page and disable Encryption for both interface cards on the Encryption page.
WEP encryption only on one or both wireless interfaces	WEP encryption is the wireless equivalent of the security level available through a wired network. Select the 802.1x Security Mode to **none** on the 802.1x page. Click the **Encryption** tab and **enable** the Encryption status for one or both wireless PC Cards. The available Encryption Key Length varies based on the card type. See Set WEP Encryption for each Wireless Interface.

Security Setting	Description
802.1x security (requires RADIUS server authentication)	When you decide to use the 802.1x security mode, you must first configure the RADIUS server to receive an authentication response (see RADIUS Authentication Settings for information on the server settings). Your computer operating system must also be configured to receive and send authenticated packets. Then, set **802.1x Security Mode** to 802.1x. In addition, you must select an **Encryption Key Length** for each wireless interface (key size varies based on card type) and a Re-keying Interval. The rekey feature determines how often your encryption key is changed (the interval between changes) and can be set to any value between 60 - 65535 seconds. Rekeying frustrates hacking attempts without taxing system resources. Setting a fairly frequent rekey value (900 seconds=15 minutes) effectively protects against intrusion without disrupting network activities. For detailed configuration steps, see Setting Up the AP-3 using 802.1x Security Mode.

Security Setting	Description
Mixed mode with 802.1x and WEP encryption	Mixed mode supports both 802.1x and WEP encryption simultaneously. To use this option, set **802.1x Security Mode** to Mixed and configure the 802.1x settings (Encryption Key Length and Re-keying interval), Encryption settings (enable Encryption and enter key 1), and RADIUS server settings. For Encryption settings, enable Encryption on the required interfaces and enter key 1 (keys 2-4 are not required). **Note:** In Mixed mode, when entering **Encryption Key 1** on the Encryption page, you must use the same size key that you configured for **Encryption Key Length** on the 802.1x page.

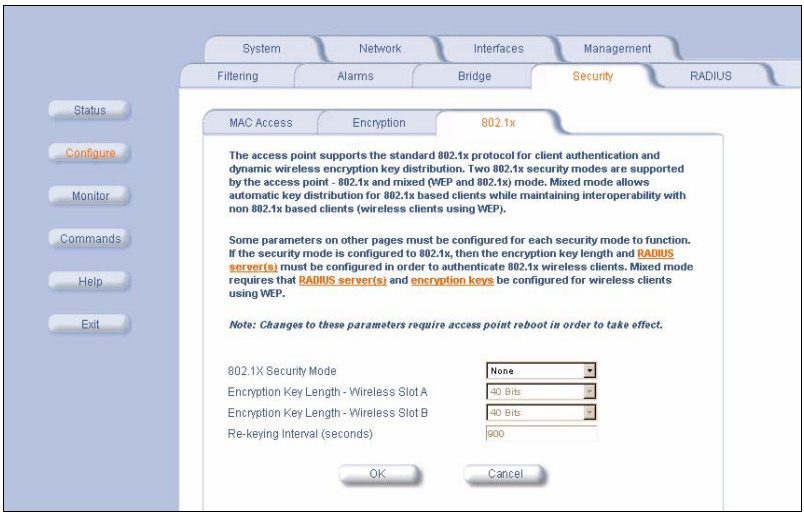
Setting Up the AP-3 using 802.1x Security Mode

1. In the Web Interface, click the **Configure** button and select the **Security** tab.
2. Select the **802.1x** tab. Set the **802.1x Security Mode** to **802.1x** or **Mixed** and click **OK**.

3. Ignore the reboot message - this can be done when the entire procedure is finished.
4. Select the **RADIUS** tab and the **Radius Auth** sub-tab.
5. Enable the Primary RADIUS server. (You must specify information for at least the Primary RADIUS server. The Backup RADIUS server is optional.)
6. Enter an **Authorization Lifetime** (the length of time, in seconds, that can elapse before a client session is automatically re-authenticated). Range is 60 - 43200 seconds (in 1 sec increments); default is 900 sec.
7. Select a **Server Addressing Format** (either name or IP address). Use a server name only if you have enabled the DNS Client functionality. See RADIUS DNS Host Name Support.
8. Enter the Server Name or IP Address for the Primary RADIUS server.
9. Enter the **Destination Port**. The default is 1812, however your RADIUS server provider may have another communication port defined.
10. Enter the RADIUS server password in the **Shared Secret** and **Confirm Shared Secret** fields.
11. Configure the **Response Time** (the maximum time, in seconds, to wait for the RADIUS server to respond to a request) and **Maximum Retransmission** (the maximum number of times a request may be retransmitted) values.

12. Reboot the AP-3 device for these changes to take effect.

Figure 2-23: Security Configuration Page - 802.1x Security Mode



802.1x Security and Wireless Distribution Systems (WDS)

Wireless distribution systems (WDS) are configured using specific ports on the AP-3 unit and frequency channels in the wireless interface cards. To use 802.1x with WDS, you need to set the 802.1x Security Mode to Mixed (WEP and 802.1x) and confirm that the AP-3 units communicating in the WDS share the same encryption key (Key 1). See Wireless Distribution System (WDS) for more information.

Note: WDS is only available for 802.11b cards.

If You Encounter Problems...

- Cannot Associate with a Network. When the client starts, it automatically looks for a network. If it cannot associate with a network, confirm that the case-sensitive Network Name (SSID) is properly configured on the client.

Note: Refer to the documentation that came with your wireless client for assistance with configuring its Network Name.

- If the Network Name is the same in both the client and the AP-3 device, then verify the settings in the Security Properties table, which includes encryption settings.
- Other Errors. Systematically double-check the AP-3 unit settings, especially the IP Addresses and the client IP Address Pool.

For more information, please refer to Troubleshooting in this guide.

AP-3 Device Management 3

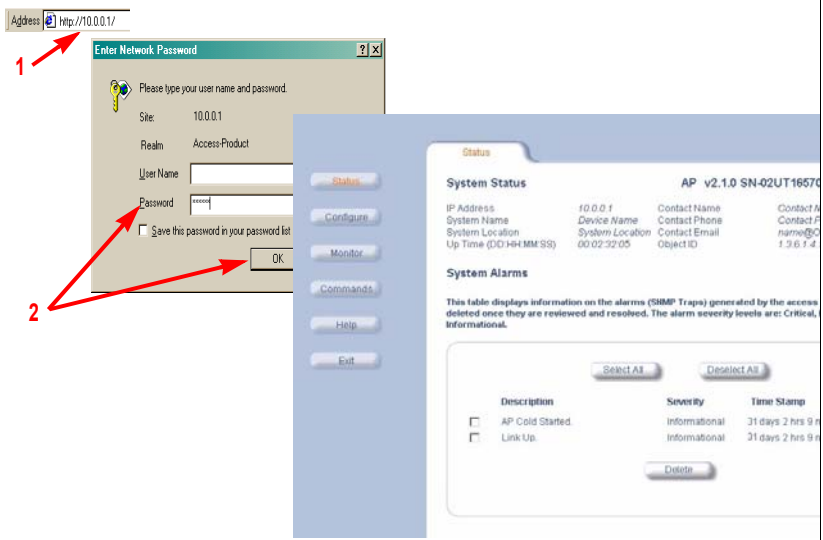
In This Chapter

Management Interface

Once you have a valid AP-3 IP Address and an Ethernet connection, you may use a web browser to issue commands and monitor network statistics.

The Command Line Interface (CLI) also provides a method for issuing commands and viewing network statistics using Telnet and Terminal clients. This section covers only use of the HTTP Interface. For more information about issuing commands and viewing network statistics with the CLI, refer to Using the Command Line Interface.

Figure 3-1: Login to HTTP Interface



1. Open your browser and enter the IP Address in the address bar. Press the **ENTER** key.

   Result: The AP-3 **Login** dialog appears.

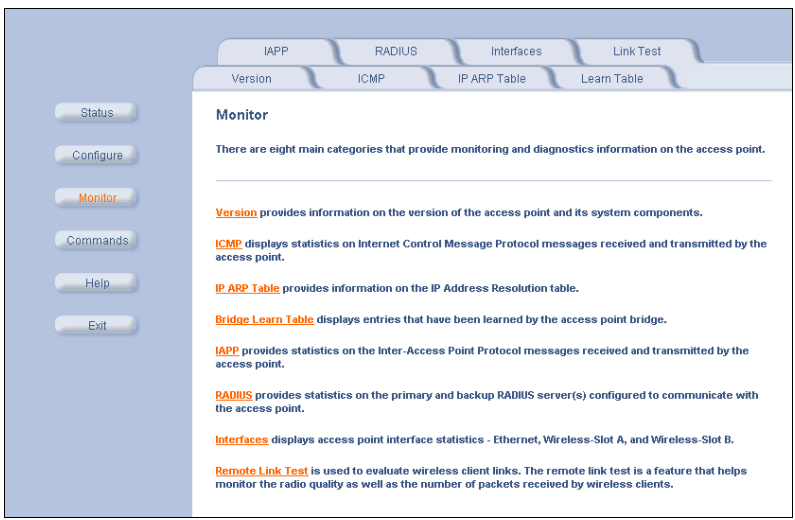
Note: Leave the **User Name** field empty.

2. Enter your password in the **Password** field (default is “public”).
3. The **System Status** page provides the following information.
   - **System Status**. This area provides system level information, including the AP-3 IP Address and contact information.
   - **System Traps**. System traps (if any) appear in this area. Each trap identifies a specific severity level.

Monitoring Network Statistics

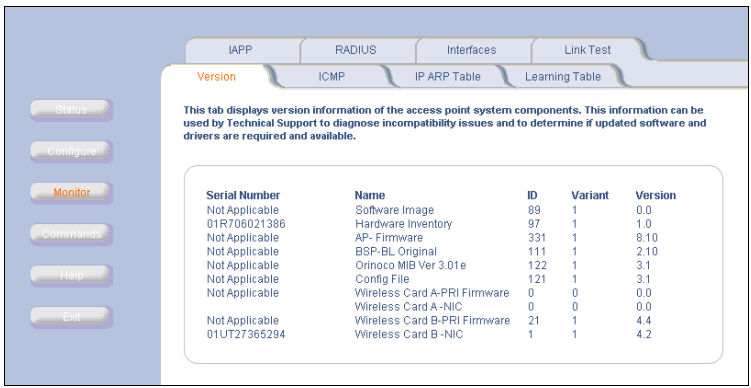
To observe the AP-3 network statistics, click the **Monitor** button. Result: The Monitor page appears. Each tab contains information for monitoring specific statistics.

Figure 3-2: Monitor Page



View Hardware/Software Component Information

Figure 3-3: Hardware/Software Component Information



From the HTTP interface:

1. Click the **Monitor** button
2. Select the **Version** tab.

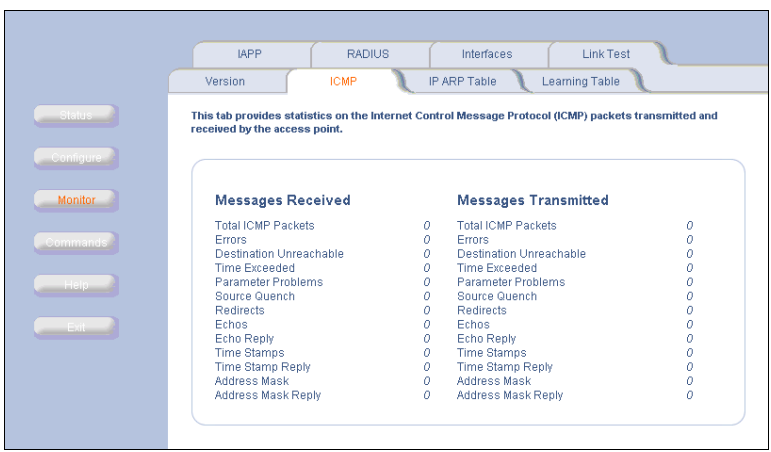
The list displayed provides you with information that may be pertinent when calling Technical Support. With this information, your Technical Support representative can

- verify compatibility issues and
- make sure the latest software and drivers are loaded.

Monitoring ICMP Statistics

This tab provides statistical information for both received and transmitted messages directed to the AP-3 device. Not all network traffic is counted in ICMP (Internet Control Message Protocol) statistics.

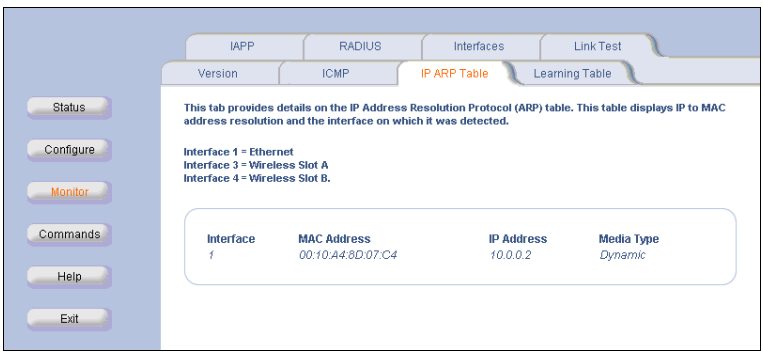
Figure: 3-4 ICMP Statistics Page



Monitoring IP/ARP Statistics

This tab provides information based on the Address Resolution Protocol (ARP), which relates MAC Address and IP Addresses.

Figure 3-5: IP/ARP Statistics Page



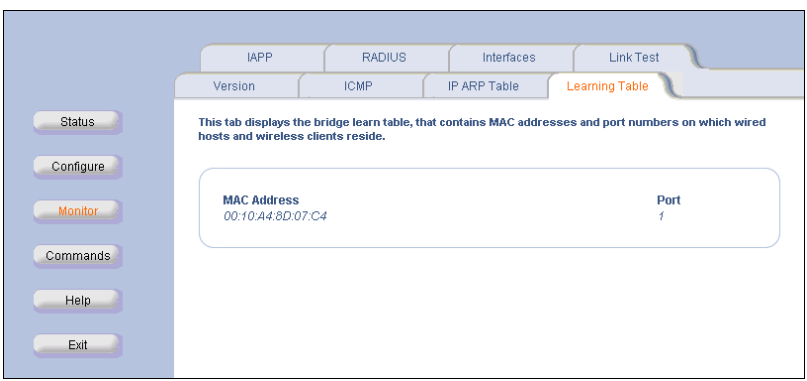
Monitoring Learn Table Statistics

This tab displays information relating to network bridging. It reports the

- MAC address for each node that the device has learned is on the network and
- interface on which the node was detected.

There can be up 10,000 entries in the Learn Table. The Learn Table displays both wireless and wired networks.

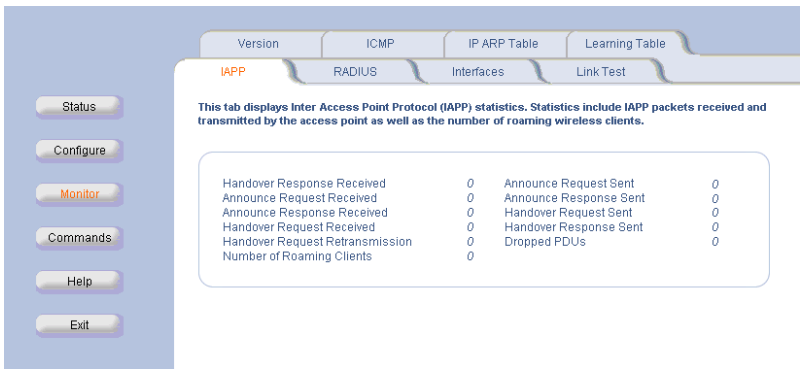
Figure 3-6: Learn Table Statistics Page



Monitoring IAPP Statistics

This tab displays statistics relating to client handovers and communications between Access Points.

Figure 3-7: IAPP Statistics Page

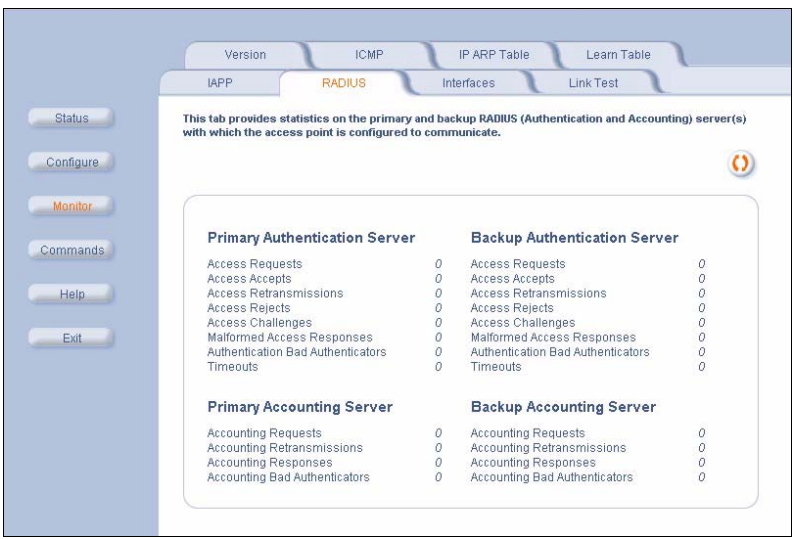


Monitoring RADIUS Server Statistics

This tab provides RADIUS authentication information for both the Primary and Backup RADIUS servers.

Note: RADIUS authentication must be enabled for this information to be valid.

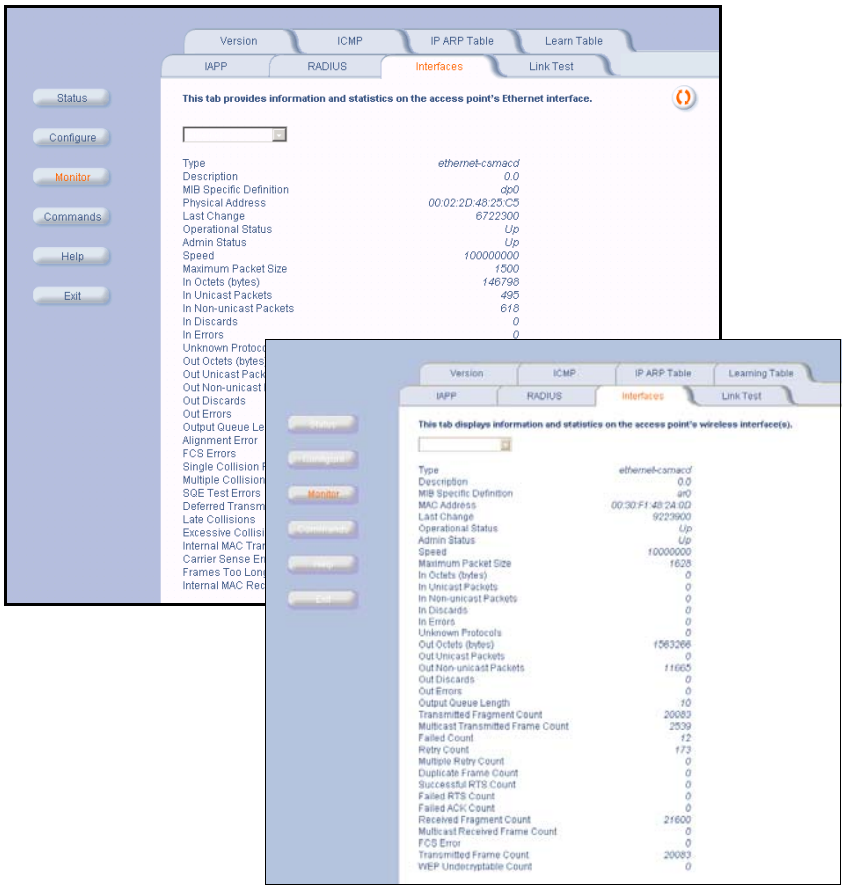
Figure 3-8: RADIUS Server Statistics Page



Monitoring Interfaces Statistics

This tab displays information for the Ethernet interface, as well as each PC Card interface. The Operational Status can be up, down, or testing.

Figure 3-9: Interface Statistics Page



Monitoring Remote Link Test Statistics

This tab displays information on the quality of the wireless link to clients and other AP-3 units in the Wireless Distribution System.

Note: The Remote Link Test feature is only available for 2.4 GHz (802.11b) clients.

Figure 3-10: Link Test Page

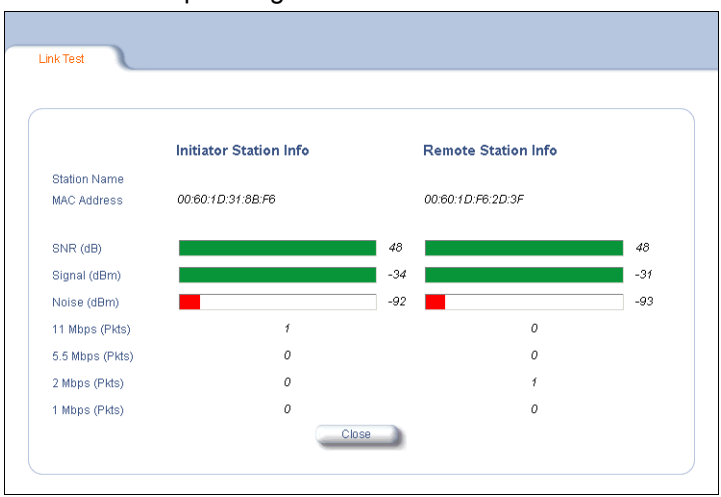
To find wireless clients connected to the AP-3 device,

1. Click **Explore**.
2. Click **Refresh**.

To test the link quality,

1. Select a station.
2. Cick **Link Test**. Quality is measured in terms of Signal strength, Noise strength, and the Signal to Noise Ratio (SNR).

Figure 3-11: SNR Report Page

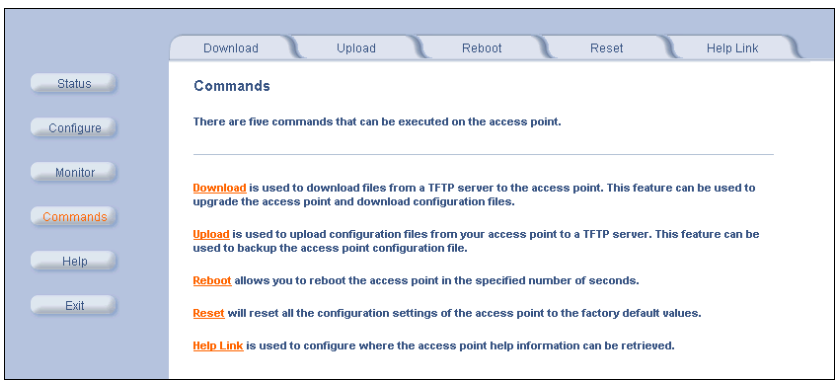


Issuing System Commands

To issue commands, click on the **Commands** operation button.

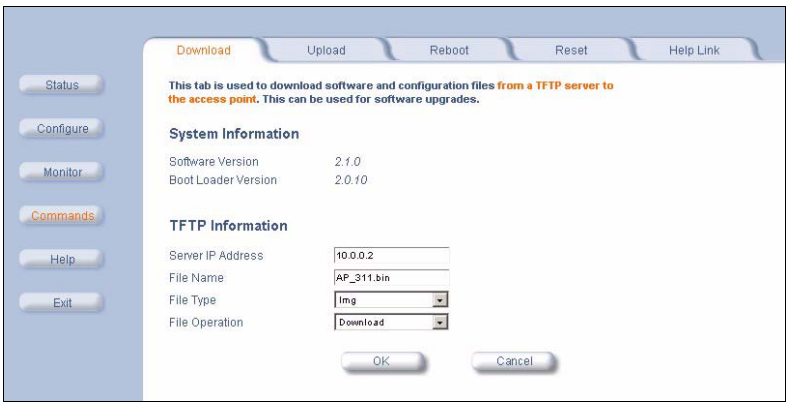
Result: The **Commands** page appears. Each tab allows a specific operation.

Figure 3-12: System Commands Page



Download

Figure 3-13: Commands Page - Download



Use the **Download** tab to download Configuration, AP Image, and Bootloader files to the AP-3. A TFTP server must be running and configured to point to the directory containing the file.

If you don't have a TFTP server installed on your system, install the TFTP server from the CD.

1. Select the "Xtras/SolarWinds" sub-directory
2. Double-click "OEM-TFTP-Server.exe".

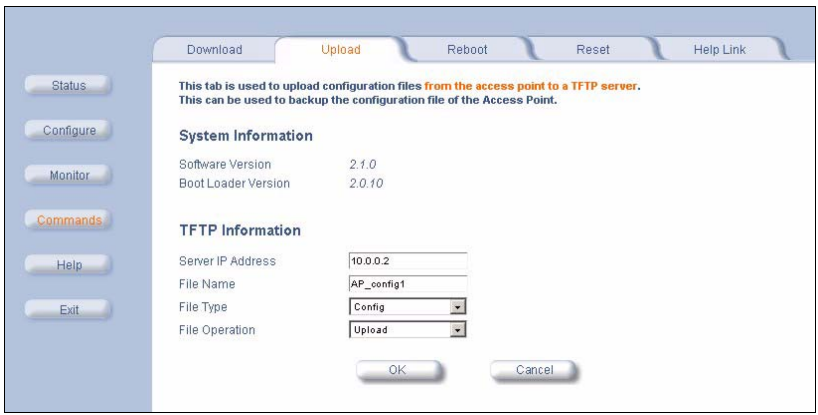
3. Follow the directions given to complete the installation.

The **Download** tab shows version information and allows you to enter TFTP information as described below.

- **Server IP Address**. Enter the TFTP server IP Address. Double-click the TFTP server icon on your desktop and locate the IP address assigned to the TFTP server. Note: This is the IP address that will be used to point the Access Point to the AP Image file.
- **File Name**. Enter the name of the file to be downloaded. Copy the updated AP Image file to the shared TFTP server folder. The default AP Image is located at C:/Program Files/ Avaya_Wireless/AP/.
- **File Type**. Select the proper file type. Choices include:
  - **Config** for configuration information, such as System Name, Contact Name, and so on.
  - **Img** for the AP Image (executable program).
  - **BspBl** for the Bootloader software.
- **File Operation**. Select either **Download**, or **Download & Reboot**. Downloaded Config, Image and Bootloader files are not active until the AP-3 has been rebooted. AP-3.

Upload

Figure 3-14: Command Pages - Upload



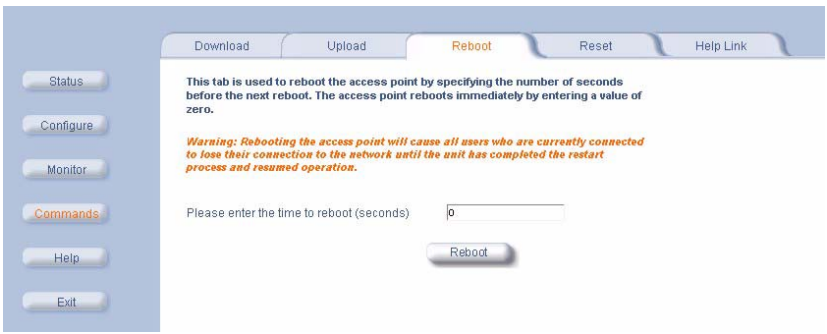
Use the **Upload** tab to upload Configuration files from the AP-3. The TFTP server must be running, and configured to point to the directory that is to contain the uploaded file. It is recommended that you assign the file a meaningful name, which may include version or location information.

If you don't have a TFTP server installed on your system, install the TFTP server from the CD. Select the "Xtras/SolarWinds" sub-directory, double-click "OEM-TFTP-Server.exe", and follow the directions given to complete the installation.

- **Server IP Address**. Enter the TFTP server IP Address. Double-click on the TFTP server icon on your desktop and locate the IP address assigned to the TFTP server. Note: This is the IP address that will be used to point the Access Point to the AP Image file.
- **File Name**. Enter the name of the file to be uploaded. Copy the updated AP Image file to the shared TFTP server folder. The default AP Image is located at C:/Program Files/ Avaya_Wireless/AP/.
- **File Type**. Select **Config**.
- **File Operation**. Select **Upload**.

Reboot

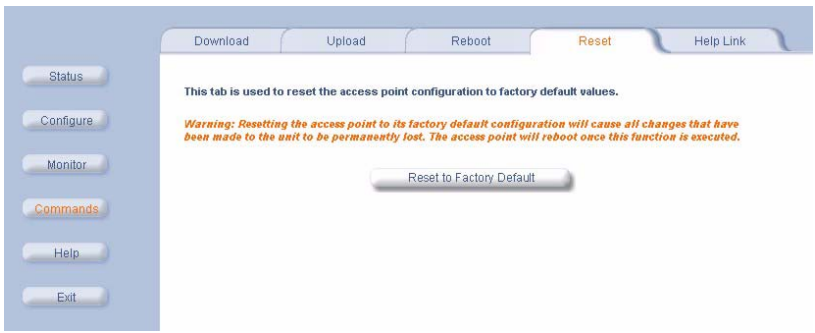
Figure 3-15: Command Pages - Reboot



Use the **Reboot** tab to save configuration changes (if any) and reset the AP-3. Entering a value of 0 (zero) seconds causes an immediate reboot.

Reset

Figure 3-16: Command Pages - Reset

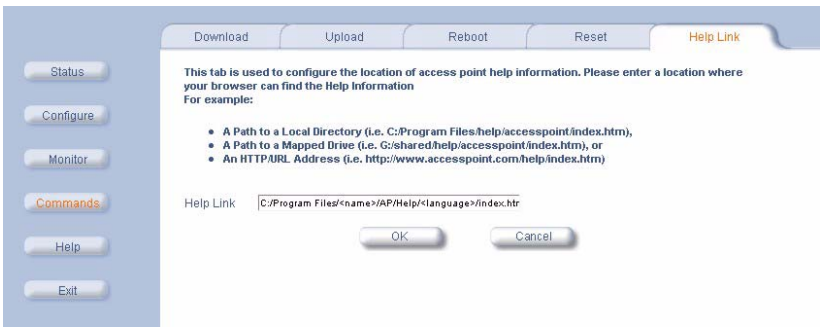


Use the **Reset** tab to restore the AP-3 to factory default conditions. The AP-3 may also be reset from the **RESET** button on indicator side of the unit. Since this will reset the current AP-3 IP Address, a new IP Address must be assigned. Also refer to Recovery Procedures.

Note: Reset, described next, does not save configuration changes.

Help Link

Figure 3-17: Command Pages - Help Link



To open **Help**, click the **Help** button on any display screen.

During initialization, the AP-3 on-line help files are downloaded to the default location:
C:\Program Files\Avaya_Wireless\AP\Help\<language>\. The Avaya Wireless AP-3 Help information is available in English, French, German, Italian, Spanish, and Japanese. Default language is English.

If you want to place these files on a shared drive, copy the Help Folder to the new location, and then specify the new path in the Help Link box.

Advanced Features 4

In This Chapter

Some of the more complex networking configurations are described in this chapter:

Network Settings • Advanced DHCP Server Configuration • DHCP IP Pool Table Settings • Link Integrity Settings	Set parameters for DHCP server including the IP Pool table. Configure Link Integrity settings and Target IP Address table.
VLAN Support • Typical VLAN Configurations • VLAN Workgroups and Traffic Management • Typical User VLAN Configurations • Typical VLAN Management ID Configuration Scenarios	Setup a VLAN network.

Management Settings • Managing IP Access • Configuring Management Service Interfaces	Configure system management settings such as passwords, management IP Access table, and service parameters (SNMP, Telnet, HTTP, Serial).
Setting Filters • Setting the Ethernet Protocol Filter • Advanced Filtering • TCP/UDP Port Filtering	Set AP-3 device filters including Ethernet filters, Static MAC address filters, and other advanced filters.
Alarms (SNMP Traps) • Alarm (Trap) Groups • Alarm Host Table • Syslog	Set alarms (SNMP Traps) including enabling alarm groups and the alarm host table. Also, configure the Syslog settings.
Bridge Configuration Settings • Static MAC Address Filter • Spanning Tree Protocol • Broadcast Storms and Storm Thresholds • Intra BSS Subscriber Blocking • Packet Forwarding	Setup the AP-3 device as a simple bridge or a wireless repeater, setup loop avoidance through the Spanning Tree protocol and Storm Threshold protection. Also, allows you to filter packets based on MAC addresses, prevent wireless clients associated with the same AP-3 from communicating with each other, and forward all wireless traffic to a specified network node.

Wireless Distribution System (WDS) • WDS Setup Procedure • Wireless Port Mapping • Configuring the AP-3 Unit as a Wireless Repeater	Establish point-to-point connections with other access points (the wireless backbone).
Advanced RADIUS Features • Fallback to Primary RADIUS Server • RADIUS Start/Stop Accounting • RADIUS DNS Host Name Support	Configure RADIUS server settings to implement advanced features, including RADIUS Accounting and DNS client functionality to support RADIUS server host names.

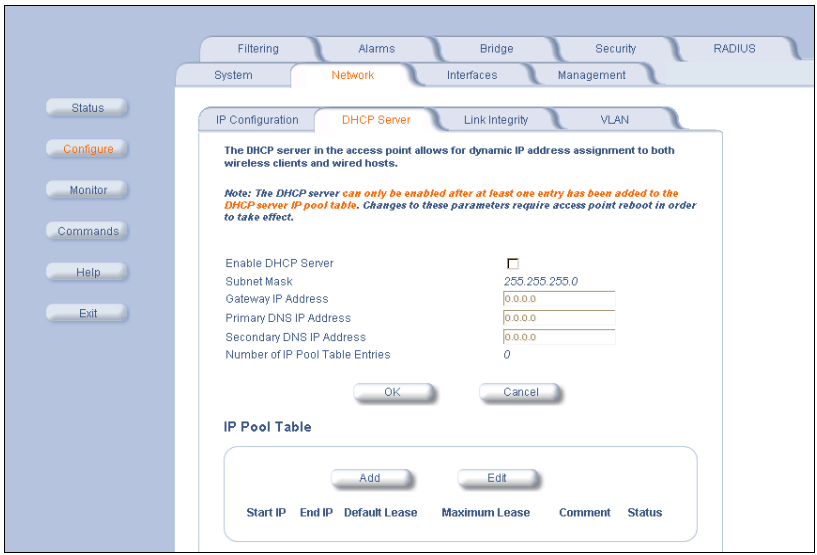
Network Settings

Advanced DHCP Server Configuration

Configure DHCP to provide dynamic client IP Addresses from one or more IP Pool Tables. Create IP Pool Tables by specifying a Start IP Address and an End IP Address.

CAUTION: Before enabling this feature, confirm that the IP address pools you have configured are valid addresses on the network. Do not overlap the addresses assigned by any other DHCP server on the network. Enabling this feature with incorrect address pools will cause problems on your network.

Figure 4-1: DHCP Server Configuration Page



- **Enable DHCP Server**. Place a check mark in the box provided to allow the AP-3 to assign clients IP Addresses from IP Pool Tables. Uncheck the box to prevent client IP Address assignment from the AP-3.

Note: You should have at least one entry in the DHCP Server IP Address Pool table before you enable the DHCP Server feature.

- **Subnet Mask**. Read-only value of the AP-3 mask.
- **Gateway IP Address**. Enter the default Gateway IP Address.
- **Primary DNS IP Address**. Enter the Domain Name Server IP Address.
- **Secondary DNS IP Address**. Enter the Domain Name Server IP Address.

DHCP IP Pool Table Settings

To add an entry, click **Add**, and then specify the start and end IP Address.

- **Start IP Address**. Enter the starting IP Address for this IP Pool Table.
- **End IP Address**. Enter the ending IP Address for this IP Pool Table.
- **Comment**. Enter related information.
- **Default Lease Time (optional)** - The default time value for clients to retain the assigned IP Address. DHCP automatically renews IP Addresses without client notification. Default is 86400 seconds. 86,400 seconds is equal to 24 hours (1 day).
- **Maximum Lease Time (optional)** -The maximum time value for clients to retain the assigned IP Address. DHCP automatically renews IP Addresses without client notification. Default is 86400 seconds.
- **Status**. Shows enabled/disabled status.

To edit or delete an entry:

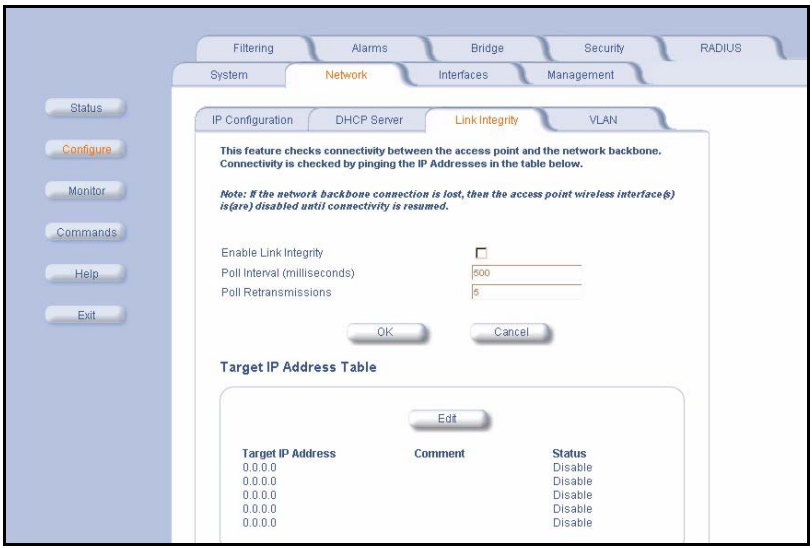
1. Click **Edit**.
2. Edit the information, or select **Enable**, **Disable**, or **Delete** from the **Status** pull-down menu.

Link Integrity Settings

This feature checks the link between the AP-3 and connected network server(s). If the link goes down then the client will connect to another AP-3 in your network that still communicates with the server.

If the wired link between the AP-3 and the backbone goes down, the AP-3 will automatically administratively shut down the wireless interfaces. When the link comes back up, the AP-3 will administratively bring up the wireless interfaces.

Figure 4-2: Link Integrity Configuration Page



- **Enable Link Integrity**. Place a check mark in the box provided to activate the Link Integrity feature.
- **Poll Interval**. Set the interval (minimum 500ms and in increments of 500ms) between polls.
- **Poll Retransmissions**. Set the number of times a poll should be retransmitted before the link is considered down.

Target IP Address Table Settings

To add an Target IP Address entry, click **Add**, and then specify the IP Address of the servers you want to check.

- **Target IP Address**. Enter the IP Address
- **Comments**. Enter related information.
- **Status**. Shows enabled/disabled status. A disabled status only means that the AP-3 is not checking the link, for example, when the network server is being serviced.

To edit or delete an entry:

1. Click **Edit**.
2. Edit the information, or select **Enable**, **Disable**, or **Delete** from the **Status** pull-down menu.

VLAN Support

Virtual Local Area Networks (VLANs) are logical groupings of network resources. VLAN resources simplify traffic flow between clients and their frequently-used or restricted resources.

VLANs now extend as far as the access point signal reaches; clients can connect from anywhere in the broadcast area. The broadcast area is defined by the network name configured for the wireless card on the access point device.

AP-3 devices are fully VLAN-ready; however, by **default** VLAN support is disabled. Before enabling VLAN support, certain network settings should be configured, and network resources such as a VLAN-aware switch, a RADIUS server, and possibly a DHCP server should be available.

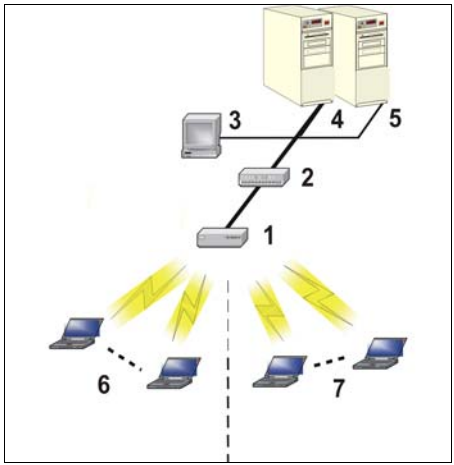
Once enabled, VLANs are used to more conveniently, efficiently, and easily manage your network.

- Manage adds, moves, and changes from a single point of contact
- Define and monitor groups
- Reduce broadcast and multicast traffic to unnecessary destinations
- Improve network performance and reduce latency
- Increase security
  - Secure network restricts members to resources on their own workgroup
  - Allows clients to roam without compromising security

Typical VLAN Configurations

VLANs collect and distribute data through wireless AP-3 network interface cards (NIC). An Ethernet port on the access point typically connects a wireless cell to a wired backbone. They communicate across a VLAN-capable switch that reviews packet headers and directs traffic to the appropriate ports. On the wired network, a RADIUS server authenticates traffic and a DHCP server manages IP addresses. Resources like servers and printers may be present, and a hub may include multiple APs, extending the network over a larger area.

Figure 4-3: Components of a typical VLAN



In this figure, the numbered items correspond to the following components:

1 VLAN-enabled access point

2 VLAN-aware switch (IEEE 802.1Q uplink)

3 AP-3 management via wired host (SNMP, Web interface or CLI)

4 DHCP Server

5 RADIUS Server

6 VLAN 1 (Wireless Card A)

7 VLAN 2 (Wireless Card B)

VLAN Workgroups and Traffic Management

Traditional, dual-slot access point devices that are not VLAN-capable typically transmit broadcast and multicast traffic to all wireless Network Interface Cards (NICs). This process

- wastes wireless bandwidth and
- degrades throughput performance.

In comparison, the dual-slot, VLAN-capable AP-3 device is designed to efficiently manage delivery of broadcast, multicast, and unicast traffic to wireless clients.

The AP-3 device assigns clients to one of two VLANs designated by a network name. First, each one of the wireless NICs in the AP-3 device is configured with a unique network name and an 802.1Q-compliant VLAN identifier. Each NIC represents a VLAN.

Each network client is then assigned one of the two wireless NIC network names. The AP-3 device matches packets transmitted or received to a network name with the associated VLAN. Traffic received by a VLAN is only sent on the wireless NIC associated with that same VLAN. This eliminates unnecessary traffic on the wireless LAN, conserving bandwidth and maximizing throughput.

Traffic Management

In addition to enhancing wireless traffic management, the VLAN-capable AP-3 device supports easy assignment of wireless users to workgroups. In a typical scenario, each user VLAN represents a workgroup. For example, one VLAN could be used for an EMPLOYEE workgroup and the other, for a GUEST workgroup.

In this scenario, the AP-3 device would assign every packet it accepted to a VLAN. Each packet would then be identified as EMPLOYEE or GUEST, depending on which wireless NIC received it. The AP-3 device would insert VLAN headers or “tags” with identifiers into the packets transmitted on the wired backbone to a network switch.

Finally, the switch would be configured to route packets from the EMPLOYEE workgroup to the appropriate corporate resources such as printers and servers. Packets from the GUEST workgroup transmitted on the same network as packets from the EMPLOYEE workgroup, could, in contrast, be restricted to a gateway that allowed access to only the Internet. A member of the GUEST workgroup could send and receive e-mail and access the Internet, but would be prevented from accessing servers or hosts on the local corporate network.

Typical User VLAN Configurations

VLANs segment network traffic into workgroups, which enable you to limit broadcast and multicast traffic. Workgroups enable clients from different VLANs to access different resources using the same network infrastructure. Clients using the same physical network are limited to those resources available to their workgroup. The three primary scenarios for use of the VLAN support feature are detailed as follows.

- **Scenario 1:** Setting Up Independent VLAN Workgroups (“Tagged” User VLANs)
- **Scenario 2:** Setting Up Independent VLAN Workgroups (Tagged & Untagged User VLANs)
- **Scenario 3:** Setting Up One VLAN Workgroup (One Tagged VLAN)

Setting Up Independent VLAN Workgroups (Tagged)

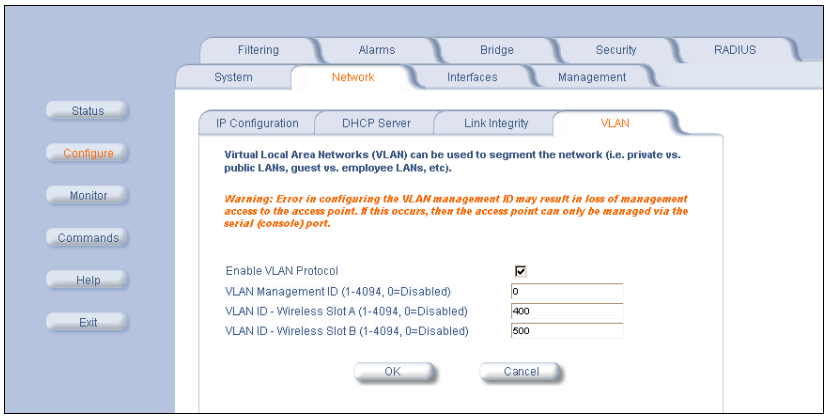
The AP-3 tags all traffic received from wireless clients transmitted on either the wired or the wireless backbone (see description of Wireless Distribution System (WDS) feature) with a header identifying each packet as belonging to one VLAN workgroup or another.

To configure this scenario, set up two different workgroups with separate VLAN Identifiers (IDs).

- VLAN ID for Wireless NIC in Slot A = a number between 1 and 4094 (per the IEEE 802.1Q standard)
- VLAN ID for Wireless NIC in Slot B = a number between 1 and 4094

Note: The number configured for the wireless NIC in Slot A must be different than the number configured for the wireless NIC in Slot B.

Figure 4-4: VLAN Configuration Page (Wireless A and Wireless Tagged with Different VLAN IDs)



1. In the Web Interface, click the **Configure** button and select the **Interfaces** tab.
2. Enter a ***unique* Network Name** (SSID) for each wireless network interface card (NIC).
3. Select the **Network** tab and select the **VLAN** sub-tab.
4. Set a ***unique*** VLAN User ID for each wireless NIC (enter a value between 1 and 4094).
5. Place a checkmark in the Enable VLAN Protocol box.

6. Configure the wireless client with one of the two **Network Names** based on VLAN membership.

Setting Up Independent VLAN Workgroups (Tagged & Untagged)

The VLAN-capable AP-3 supports configuration of both “tagged” and “untagged” user VLANs.

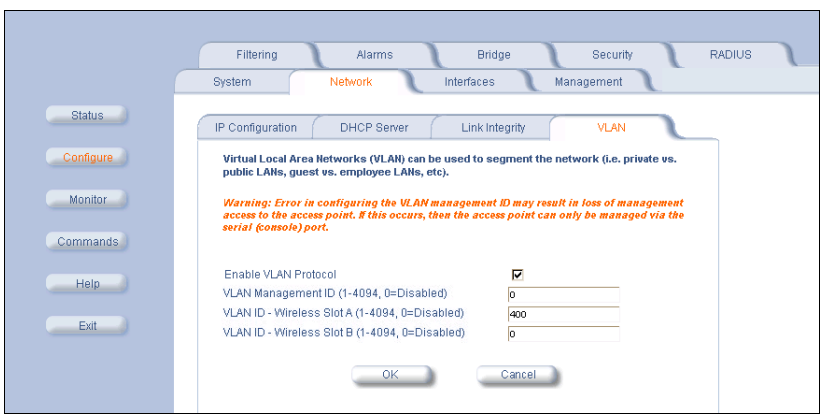
- A “**tagged**” user VLAN is created when a VLAN ID between 1 and 4094 (per the 802.1Q standard) is configured for one of the wireless NICs and VLAN is enabled. The AP-3 applies a VLAN header to tag traffic from wireless clients (members of a “tagged” VLAN) and transmits the traffic as appropriate, on either the wired or wireless backbone.
- An “**untagged**” User VLAN is created when a VLAN ID of 0 is configured for one of the wireless NICs and VLAN is enabled. Traffic received from wireless clients (members of an “untagged” VLAN) is transmitted as appropriate, on either the wired or wireless backbone. “Untagged” User VLANs enable VLANs to coexist on networks with non-VLAN capable devices such as legacy servers.

To configure this scenario, set up only one workgroup by configuring one tagged interface and one untagged interface:

- VLAN ID for Wireless NIC in Slot A = 0 or a number between 1 and 4094
- VLAN ID for Wireless NIC in Slot B = 0 or a number between 1 and 4094

Note: Either the wireless NIC in Slot A or the wireless NIC in Slot B must be set to 0.

Figure 4-5: VLAN Configuration Page (Wireless A Tagged Only)



1. In the Web Interface, click the **Configure** button and select the **Interfaces** tab
2. Enter a ***unique*** **Network Name** (SSID) for each NIC.
3. Select the **Network** tab and select the **VLAN** sub-tab.
4. Set the **VLAN UserID** for one NIC to 0.
5. Set the **VLAN User ID** for the other NIC to a value between 1 and 4094.
6. Place a checkmark in the Enable VLAN Protocol box.
7. Configure the wireless client with one of the two **Network Names** based on VLAN membership.

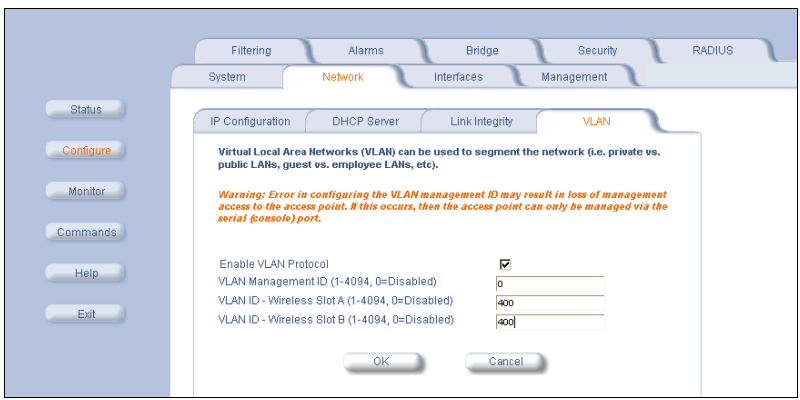
Setting Up a Single VLAN Workgroup

The VLAN feature enables all wireless clients that access the network through the same AP-3 to be configured as members of the same VLAN. In this scenario, each wireless NIC is configured with the same VLAN ID. The same VLAN header or tag is then applied to all traffic received from wireless clients and transmitted on the wired or wireless backbone. All wireless clients become members of the same VLAN.

To configure this scenario, set up one, large workgroup:

- VLAN ID for Wireless NIC in Slot A = 0 or a number between 1 and 4094
- VLAN ID for Wireless NIC in Slot B = 0 or a number between 1 and 4094

Figure 4-6: VLAN Configuration Page (Wireless A and Wireless B Use Same VLAN ID)



1. In the Web Interface, click the **Configure** button and select the **Interfaces** tab.

2. Enter a ***unique*** Network Name (SSID) for each wireless network interface card (NIC).
3. Select the **Network** tab and select the **VLAN** sub-tab.
4. Set the **VLAN UserID** for the NIC in Slot A to a value between 1 and 4094.
5. Set the **VLAN UserID** for the NIC in Slot B to the same value configured for the NIC in Slot A.
6. Place a checkmark in the Enable VLAN Protocol box.
7. Configure the wireless client with one of the two **Network Names** based on VLAN membership.

Typical VLAN Management ID Configuration Scenarios

Making the AP-3 a VLAN Member to Control Management Access

Management access to the AP-3 can easily be secured by making management stations or hosts and the AP-3 device itself members of a common VLAN. Simply configure a non-zero management VLAN ID and enable VLAN to restrict management of the AP-3 device to members of the same VLAN.

1. In the Web Interface, click the **Configure** button and select the **Network** tab.

2. Select the **VLAN** sub-tab.
3. Set the **VLAN Management ID** to a value between1 and 4094 (a value of 0 disables VLAN management).
4. Place a checkmark in the Enable VLAN Protocol box.

Note: If a non-zero management VLAN ID is configured then management access to the AP-3 is restricted to wired or wireless hosts that are members of the same VLAN. Ensure your management platform or host is a member of the same VLAN before attempting to manage the AP-3 device.

Managing the AP-3 from a Wireless Host

The VLAN feature enables wireless clients to manage the AP-3. If the VLAN Management ID matches a VLAN User ID, then those wireless clients who are members of both VLANs will have AP-3 management access.

1. In the Web Interface, click the **Configure** button and select the **Interfaces** tab.
2. Enter a ***unique*** **Network Name** (SSID) for each wireless NIC.
3. Select the **Network** tab and the **VLAN** sub-tab.
4. Set the **VLAN User ID** for the wireless NICs in Slot A and Slot B to values between 1 and 4094.

5. Set the **VLAN Management ID** to a value equivalent to one of the VLAN User IDs.

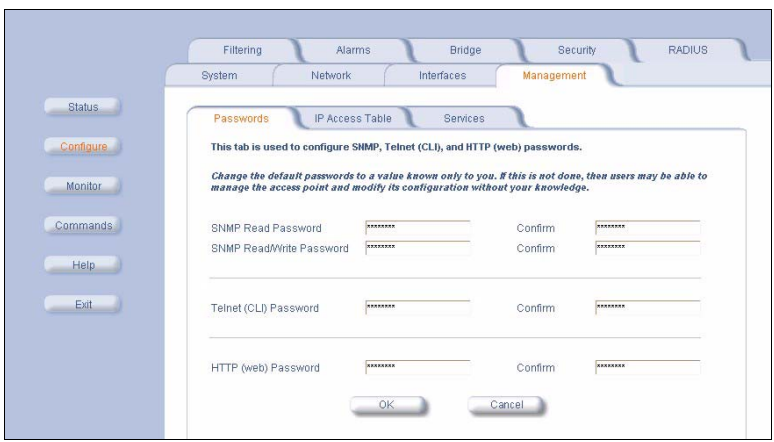
6. Place a checkmark in the Enable VLAN Protocol box.

CAUTION: Once a VLAN Management ID is configured and is equivalent to one of the VLAN User IDs on the AP-3, all members of the User VLAN will have management access to the AP-3. Be careful to restrict VLAN membership to those with legitimate access to the AP-3 device.

Management Settings

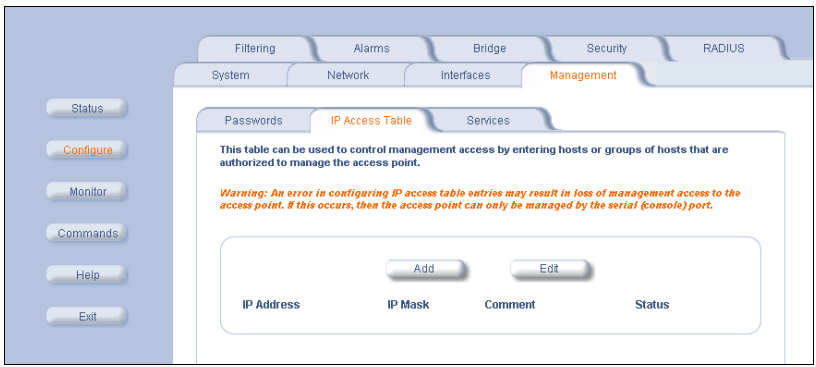
Configure system management settings, including interface access passwords, destination port numbers, and service timeouts. Select new passwords during initial configuration.

Figure 4-7: Management Configuration Page



Managing IP Access

Figure 4-8: IP Access Table Configuration Page



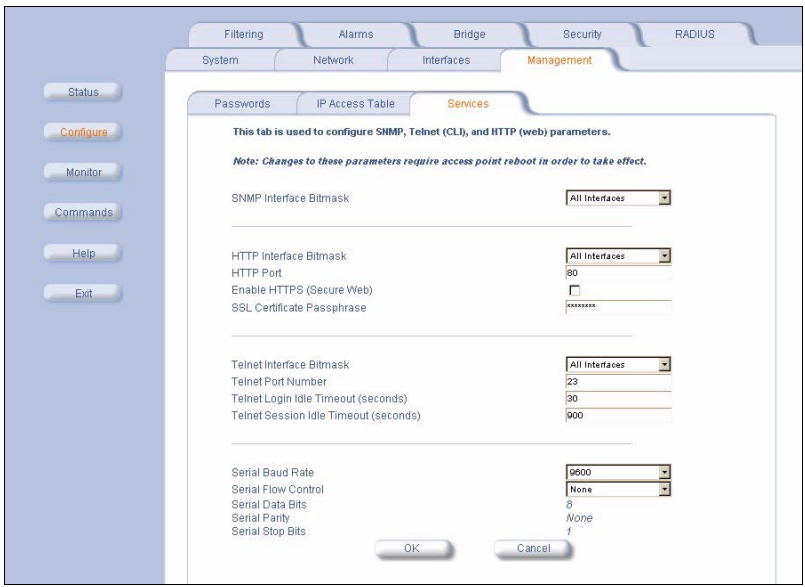
The Management IP Access table is used to specify a station or stations that are authorized to manage the AP-3 device through available management services (SNMP, HTTP [Web], and Telnet [CLI]). To configure this table, click **Add** and set the following parameters:

- **IP Address**. Enter the IP Address for the management station.
- **IP Mask**. Enter a mask that will act as a filter to limit access to a range of IP Addresses.
- **Comment**. Enter an optional comment such as the station name.

Note: The IP mask 255.255.255.255 would authorize the single station defined by the IP Address to configure the Access Point device. The Access Point device would ignore commands from any other IP address. In contrast, the IP mask 255.255.255.0 would authorize **anyone on the subnet shared by the IP Address** to configure the Access Point device. To edit or delete an entry, click **Edit**. Edit the information, or select **Enable**, **Disable**, or **Delete** from the ***Status*** pull-down menu.

Configuring Management Service Interfaces

Figure 4-9: Management Services Configuration Page



SNMP-Based Management Interface Bitmask

Configure the interface or interfaces (Ethernet, Wireless-A, Wireless-B, All Interfaces) from which you will manage the AP-3 device via SNMP. You can also select Disabled to prevent a user from accessing the AP-3 device via SNMP. Reboot the AP-3 for this setting to take effect.

HTTP Access

Several configuration options are available that restrict access to the Web interface. Reboot the AP-3 for any changes to take effect.

- **HTTP Interface Bitmap.** Configure the interface or interfaces (Ethernet, Wireless-A, Wireless-B, All Interfaces) from which you will manage the AP-3 device via the Web interface. You can also select Disabled to prevent a user from accessing the AP-3 device from the Web interface.
- **HTTP Port.** Configure the HTTP port from which you will manage the AP-3 device via the Web interface. By **default,** the HTTP port is 80.

Telnet Configuration Settings

Use the Services tab to set the Telnet port, timeout, and session parameters.

Field	Description
Telnet Interface Bitmask	Select the interface(s) (Disabled, Ethernet, Wireless A, Wireless B, All Interfaces) from which you can manage the AP-3 device via telnet. This parameter can also be used to Disable telnet management. You need to reboot the AP-3 for this setting to take effect.
Telnet Port	Enter the Telnet Port. The default port number is 23.
Login Idle Timeout (seconds)	Enter the number of seconds the system will wait for a login attempt. The AP-3 terminates the session when it times out.
Session Idle Timeout (seconds)	Enter the number of seconds the system will wait during a session while there is no activity. The AP-3 will terminate the session on timeout.

Note: See Configure Serial Port Interface Settings for information on the serial port parameters.

Setting Filters

Setting protocol filters through the Ethernet Protocol Filter, TCP/UDP Port Filter, and the Advanced Filtering interface can impact the performance of your network by limiting the amount of unnecessary traffic received from unsupported protocols. In addition, you can set up various filters through the Static MAC Address Table to control the following:

- Interaction between network devices.
- Types of protocol packets distributed by your network.

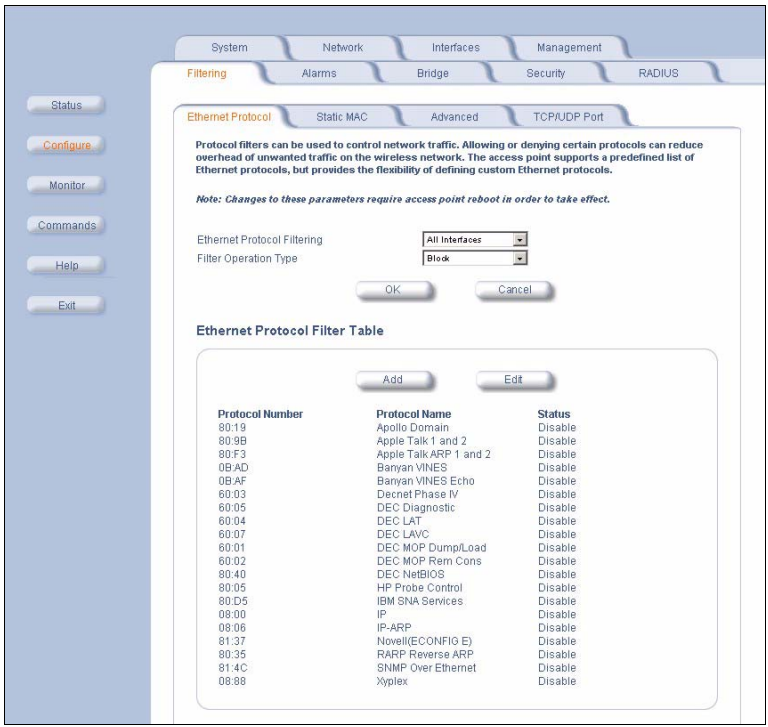
This section describes the Ethernet Protocol, Advanced, and TCP/UDP Port filtering options. See Static MAC Address Filter for information on the Static MAC address filter.

Setting the Ethernet Protocol Filter

Use the Ethernet Protocol tab to set filters.

- **Enable Ethernet Filter Status.** Place a checkmark in the box provided to enable filtering. If disabled, then the AP-3 will not filter any of the Ethernet protocols listed in the Filter Table. **Filter Operation Type.** If set to **Passthru**, only the enabled Ethernet Protocols listed in the Filter Table will pass through the bridge. If set to **Block**, the bridge will block enabled Ethernet Protocols listed in the Filter Table.

Figure 4-10: Ethernet Filter Configuration Page



Ethernet Protocol Filter Table

This table is pre-populated with existing Ethernet Protocol Filters, however, you may enter additional filters by specifying the appropriate parameters.

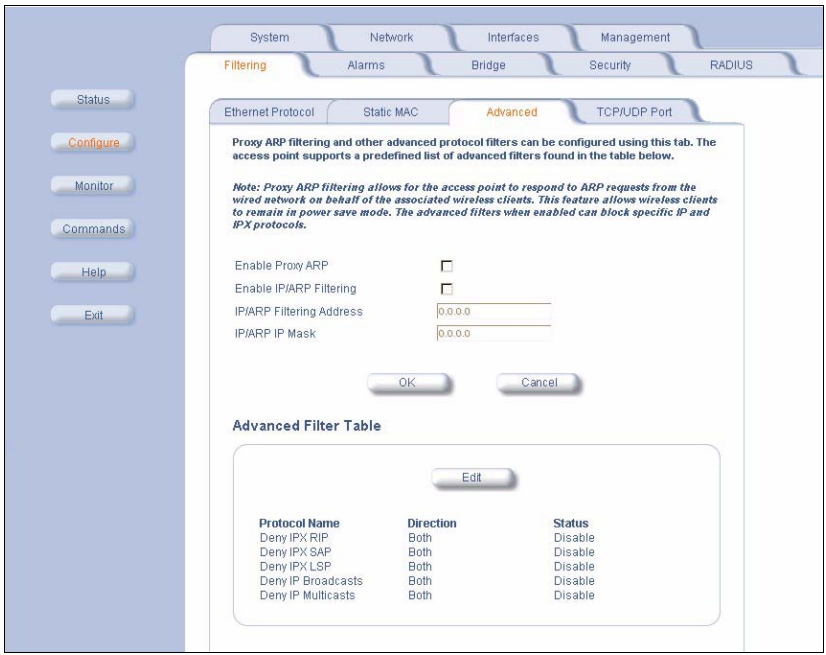
To add an entry:

1. Click **Add**,
2. Specify the **Protocol Number** and a **Protocol Name**.
   - **Protocol Number**. Enter the protocol number. See http://www.iana.org/assignments/ethernet-numbers for a list of protocol numbers.
   - **Protocol Name**. Enter related information, typically the protocol name.

To edit or delete an entry, click **Edit** and change the information, or select **Enable**, **Disable**, or **Delete** from the **Status** pull-down menu.

Advanced Filtering

Figure 4-11: Advanced Filtering Configuration Page



Field	Description
Enable Proxy ARP	Place a checkmark in the box provided to allow the Access Point to respond to Address Resolution Protocol (ARP) requests for wireless clients. Proxy ARP answers ARP requests for wireless stations without actually forwarding the (broadcast) ARP request to the wireless network. If disabled, the Access Point will bridge ARP requests for wireless clients to the wireless LAN.
Enable IP/ARP Filtering	Place a checkmark in the box provided to allow IP/ARP filtering based on the IP/ ARP Filtering Address and IP Mask. Leave the box unchecked to prevent filtering.
IP/ARP Filtering Address	Enter the Network filtering IP Address.
IP/ARP IP Mask	Enter the Network Mask IP Address.

The following advanced filtering protocols can filter in the wireless-to-Ethernet direction, the Ethernet-to-wireless direction, or in both directions. Click Edit and use the **Status** field to Enable or Disable the filter.

- Deny IPX RIP
- Deny IPX SAP
- Deny IPX LSP
- Deny IP Broadcasts
- Deny IP Multicasts

TCP/UDP Port Filtering

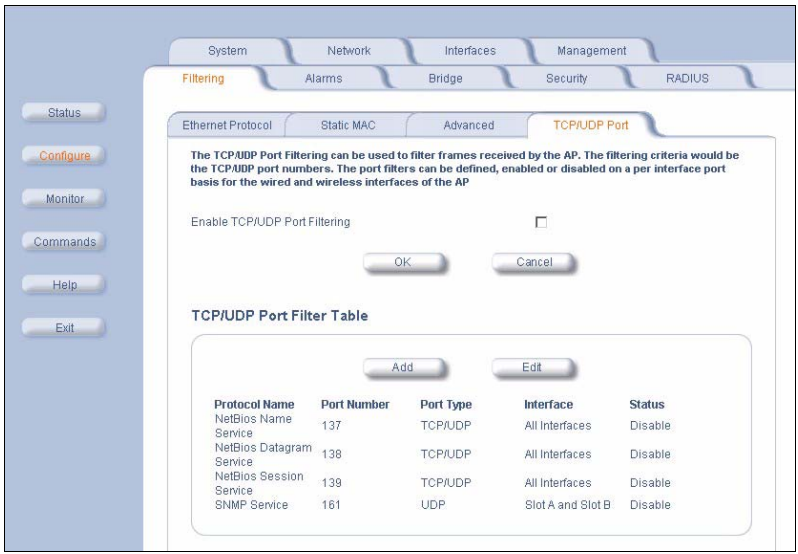
Port-based filtering enables you to control wireless user access to network services by selectively blocking TCP/UDP protocols through the AP-3. A user specifies the following in order to block access to services, such as Telnet and FTP, and traffic, such as NETBIOS and HTTP.

- Protocol Name,
- Port Number,
- Port Type (TCP, UDP, or TCP/UDP), and
- Filtering interfaces (all interfaces, no interfaces, or any combination of Wireless Slot A, Wireless Slot B, and Ethernet).

For example, an AP-3 with the following configuration would discard frames received on Wireless Slot A with a UDP destination port number of 137, effectively blocking NETBIOS Name Service packets.

Protocol Type (TCP/UDP)	Destination Port Number	Protocol Name	Interface	Status (Enable/ Disable)
UDP	137	NETBIOS Name Service	Wireless port A	Enable

Figure 4-12: TCP/UDP Port Filtering Configuration Page

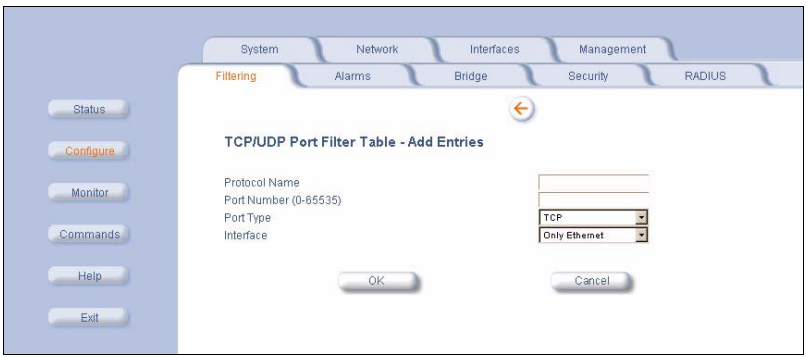


Adding TCP/UDP port filters

1. In the Web Interface, click the **Configure** button and select the **Filtering** tab.
2. Select the **TCP/UDP Port** sub-tab.
3. Click the box to **Enable TCP/UDP Port Filtering.**

4. Under the heading, **TCP/UDP Port Filter Table**, click **Add**.

Figure 4-13: Adding a Port to the TCP/UDP Port Filter Table



14. In the **TCP/UDP Port Filter Table,** enter the Protocol Names to filter.
15. Set the destination Port Number (a value between 0 and 65535) to filter. See the IANA Web site at http://www.iana.org/assignments/port-numbers for a list of assigned port numbers and their descriptions.
16. Set the Port Type for the protocol: TCP, UDP, or both (TCP/UDP).
17. Set the **Interface** to filter (any combination of the following):
    - Wireless Slot A

- Wireless Slot B
- Ethernet

18. Click **OK**.

Note: Filters are enabled by default. Frames that the AP-3 receives on the specified interface(s) with the specified TCP/UDP destination port, are discarded.

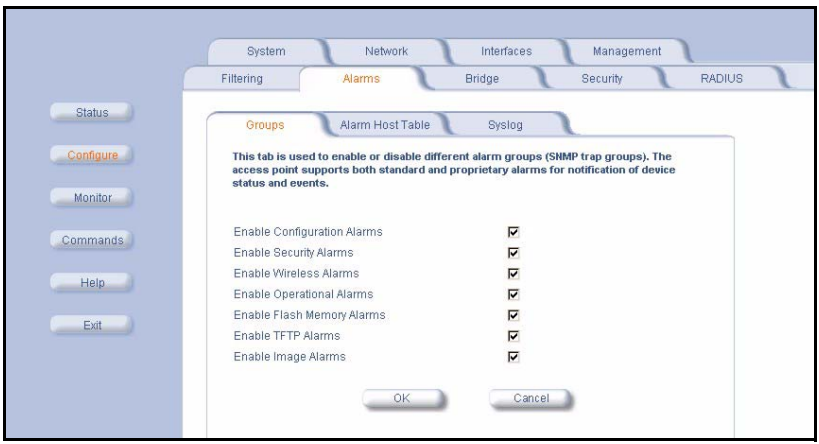
Editing TCP/UDP port filters

1. In the Web Interface, click the **Configure** button and select the **Filtering** tab.
2. Select the **TCP/UDP Port** sub-tab.
3. Under the heading, **TCP/UDP Port Filter Table**, click the button marked **Edit.**
4. Make any changes to the Protocol Name or Port Number for a specific entry, if necessary.
5. In the row that defines the port, set the **Status** to **enable**, **disable**, or **delete** as appropriate.
6. Select **OK.**

Alarms (SNMP Traps)

Alarm (Trap) Groups

Figure 4-14: Alarm Groups Configuration Page



There are seven alarm groups that can be enabled or disabled:

- **Enable Configuration Alarms**.
- **Enable Security Alarms**.
- **Enable Wireless Alarms**.
- **Enable Operational Alarms**.
- **Enable Flash Memory Alarms**.
- **Enable TFTP Alarms**.
- **Enable Image Alarms.**

Enable Image Alarms. Place a checkmark in the box provided to enable a specific group. Remove the checkmark from the box to disable the alarms.

See System Alarms (Traps) for the list of alarms contained in each group.

Alarm Host Table

To add an entry and enable the AP-3 to send SNMP trap messages to a Trap Host:

1. Click **Add**.

2. Specify the IP Address and Password for the Trap Host.
   - **IP Address**. Enter the Trap Host IP Address.
   - **Password, Confirm**. Enter the password in the **Password** field and the **Confirm** field.
   - **Comment**. Enter an optional comment, such as the alarm (trap) host station name.

To edit or delete an entry:

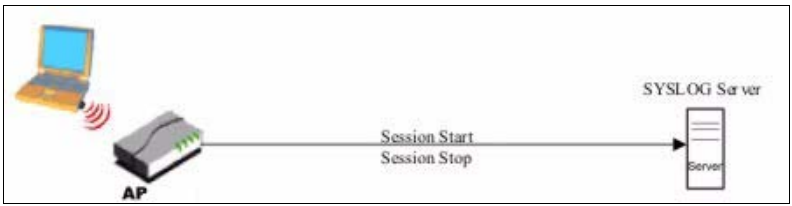
1. Click **Edit**.
2. Edit the information, or select **Enable, Disable**, or **Delete** from the **Status** pull-down menu.

Syslog

The Syslog messaging system enables the AP-3 to transmit event messages to a central server for monitoring and troubleshooting. The access point logs “Session Start (Log-in)” and “Session Stop (Log-out)” events for each wireless client as an alternative to RADIUS accounting.

See RFCs 3164 at http://www.rfc-editor.org/ for more information on the Syslog standard.

Figure 4-15: Syslog Interaction with the Access Point 3



Setting Syslog Event Notifications

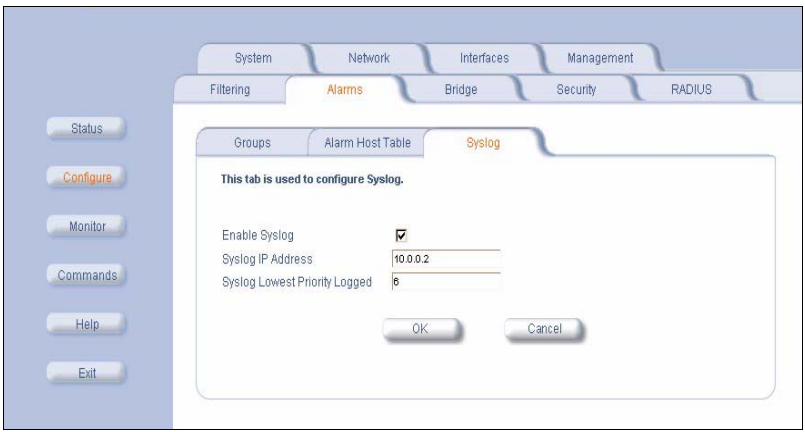
Syslog Events are logged according to the level of detail specified by the administrator. Logging only urgent system messages will create a far smaller, more easily read log then a log of every event the system encounters. Determine which events to log by selecting a priority defined by the following scale:

EventPriorityDescription

LOG_EMERG	0	system is unusable
LOG_ALERT	1	action must be taken immediately
LOG_CRIT	2	critical conditions
LOG_ERR	3	error conditions
LOG_WARNING	4	warning conditions
LOG_NOTICE	5	normal but significant condition
LOG_INFO	6	informational
LOG_DEBUG	7	debug-level messages

Enabling Syslog Event Notifications

Figure 4-16: Syslog Configuration Page



1. In the Web Interface, click the **Configure** button and select the **Alarms** tab.
2. Select the **Syslog** sub-tab.
3. Place a checkmark in the box provided to **Enable Syslog.**
4. Enter the IP address of the Syslog server.

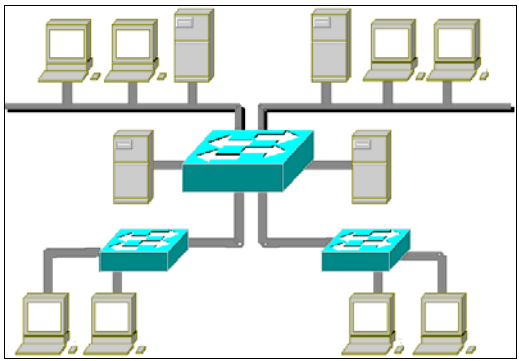
5. Enter the **Syslog Lowest Priority Logged.** The AP-3 will send event messages to the Syslog server that correspond to the selected priority and below. For example, if set to 6, the AP-3 will transmit event messages labeled priority 0 to 6 to the Syslog server.
6. Click **OK**.

Bridge Configuration Settings

The AP-3 device can be set up as a simple bridge between your wired and wireless network devices. As a bridge, the functions performed by the AP-3 device include:

- MAC address learning
- Forward and filtering decision making
- Spanning Tree protocol used for loop avoidance

Figure 4-17: Simple Bridge SetupMAC Address Learning



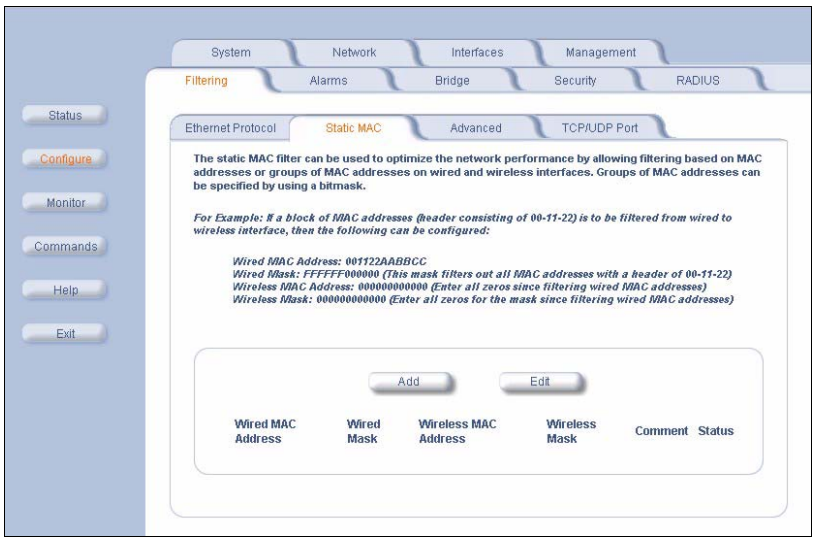
Once the AP-3 unit is connected to your network, it learns which devices are connected to it by recording the MAC addresses of each device to which it sends packets during the course of a normal session. To view the Learn Table:

1. Click on the **Monitor** button in the web interface.
2. Select the **Learn Table** tab. The table can hold up to 10,000 entries.

Static MAC Address Filter

The Static MAC Address filter optimizes the performance of a wireless (and wired) network. The filter is an advanced Bridge setup parameter for AP-3 devices that enables you to deny data traffic between two specific devices via the wireless interface(s) of the AP-3 bridge.

Figure 4-18: Static MAC Filter Configuration Page



For example, to prevent redundant traffic from being transmitted over the wireless network, you could deny traffic between two particular servers, identified by their MAC Address and their location as perceived by the AP-3 (on the ‘wired’ or wireless’ port of the bridge). In most situations, however, it is easier to control redundant traffic via other filtering options, such as Protocol Filtering.

Field	Description
Wired MAC Address	Enter the device MAC Address.
Wired Mask	Enter the Wired Mask value.
Wireless MAC Address	Enter the device MAC Address.
Wireless Mask	Enter the Wireless Mask value.
Comment	Enter related information.

Information Masks

The MAC Address combines with the Bit Mask to create a filter. Wired MAC Addresses and their associated masks, and wireless MAC Addresses and their associated masks are known generically as "information masks" and are written in the following format:

MAC Address:00 02 10 12 34 56

Bit Mask:FF FF FF FF 00 00

In this example, all MAC Addresses starting with 00 02 10 12 are filtered.

Spanning Tree Protocol

A Spanning Tree is used to avoid redundant communication loops in networks with multiple bridging devices. Bridges do not have any inherent mechanism to avoid loops, because having redundant systems is a necessity in certain networks. However, redundant systems can cause Broadcast Storms, multiple frame copies, and MAC address table instability problems.

Complex network structures can create multiple loops within a network. The Spanning Tree configuration blocks certain ports on AP-3 devices to control the path of communication within the network, avoiding loops and following a spanning tree structure.

Note: For more information on Spanning Tree protocol, please see Section 8.0 of the IEEE 802.1d standard.

Broadcast Storms and Storm Thresholds

Storm Threshold is an advanced Bridge setup option that you can use to protect the network against data overload by:

- Specifying a maximum number of frames per second as received from a single network device (identified by its MAC address).
- Specifying an absolute maximum number of messages per port.

The ‘Storm Threshold’ parameters allow you to specify a set of thresholds for each port of the AP-3, identifying separate values for the number of broadcast messages/second and Multicast messages/second.

When the number of frames for a port or identified station exceeds the maximum value per second, the AP-3 will ignore all subsequent messages issued by the particular network device, or ignore all messages of that type.

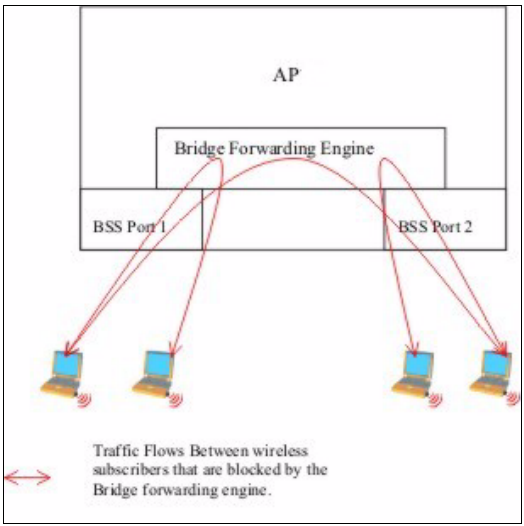
Field	Description
Address Threshold	Enter the maximum allowed number of packets per second.
Ethernet Threshold	Enter the maximum allowed number of packets per second.
Wireless-Slot A Threshold	Enter the maximum allowed number of packets per second.
Wireless-Slot B Threshold	Enter the maximum allowed number of packets per second.

Intra BSS Subscriber Blocking

The wireless clients (or *subscribers*) that associate with a certain AP-3 form the Basic Service Set (BSS) of a network infrastructure. By default, wireless subscribers in the same BSS can communicate with each other. However, some administrators (such as wireless public spaces) may wish to block traffic between wireless subscribers that are associated with the same AP-3 to prevent unauthorized communication and to conserve bandwidth. This feature enables you to prevent wireless subscribers within a BSS from exchanging traffic.

Although this feature is generally enabled in public access environments, Enterprise LAN administrators use it to conserve wireless bandwidth by limiting communication between wireless clients. For example, this feature prevents peer-to-peer file sharing or gaming over the wireless network.

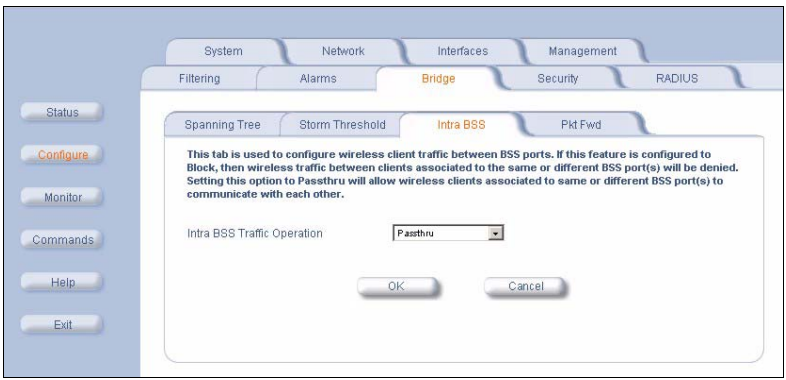
Figure 4-19: Intra BSS Traffic Blocking



Blocking Intra BSS Traffic

1. In the Web Interface, click the **Configure** button and select the **Bridge** tab.
2. Select the **Intra BSS** sub-tab.
3. Select **Block** from the **Intra BSS Traffic Operation** drop-down menu.
4. Click **OK.**

Figure 4-20: Intra BSS Configuration Page



Enabling Intra BSS Traffic

1. In the Web Interface, click on the **Configure** button and Select the **Bridge** tab
2. Select the **Intra BSS** sub-tab
3. Select **Passthru** from the **Intra BSS Traffic Operation** drop-down menu
4. Click **OK**

Packet Forwarding

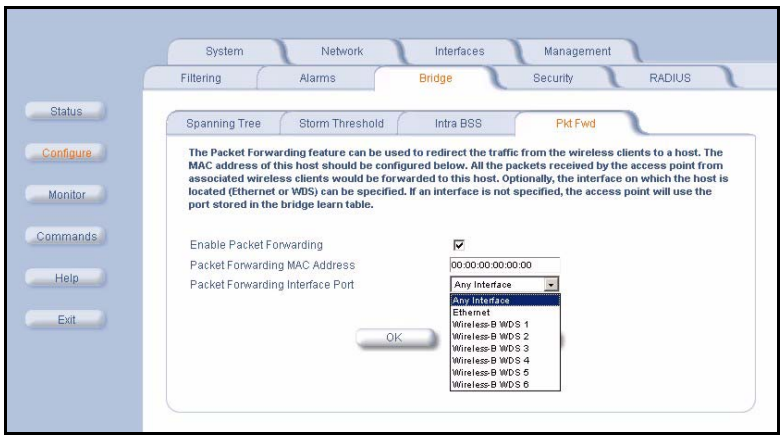
The Packet Forwarding feature enables you to redirect traffic generated by wireless clients that are all associated to the same AP-3 to a single MAC address. This filters wireless traffic without burdening the AP-3 and provides additional security by

- limiting potential destinations or
- by routing the traffic directly to a firewall.

You can redirect a specific port (Ethernet or WDS) or allow the bridge's learning process (and the forwarding table entry for the selected MAC address) to determine the optimal port.

Note: The gateway to which traffic will be redirected should be node on the Ethernet network. It should not be a wireless client.

Figure 4-21: Packet Forwarding Configuration Page



Configuring Interfaces for Packet Forwarding

Configure your AP-3 to forward packets by specifying interface port(s) though which packets are redirected and a destination MAC address.

1. In the Web Interface, click the **Configure** button and select the **Bridge** tab.
2. Select the **Pkt Forwarding** sub-tab.

3. Specify a destination **Packet Forwarding MAC Address**. The AP-3 will redirect all unicast, multicast, and broadcast packets received from wireless clients to the address you specify.
4. Click the down arrow to activate the menu and select a **Packet Forwarding Interface**. You can redirect traffic to:
   - Ethernet
   - A WDS connection (see Wireless Distribution System (WDS) for details)
   - Any (traffic is redirected to a port based on the bridge learning process)
5. Check the box to **Enable Packet Forwarding**.
6. Click **OK** to save your changes.

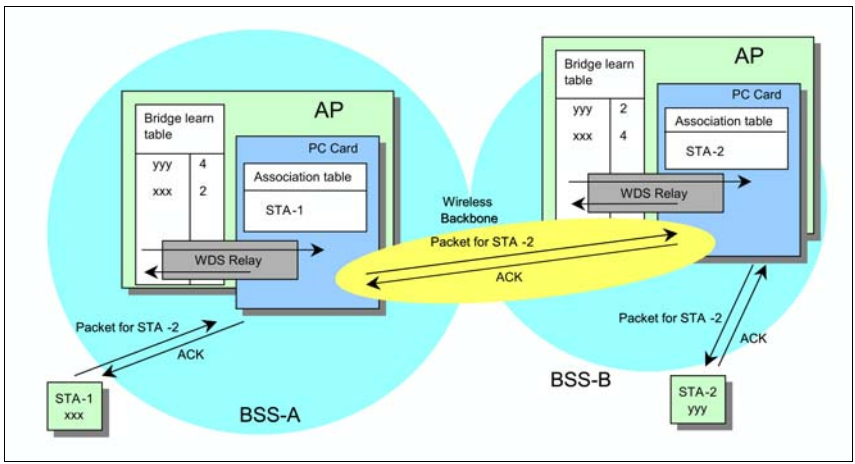
Note: Only those wireless interfaces corresponding to cards currently inserted and available in the AP-3 will be visible on the configuration menu.

Wireless Distribution System (WDS)

Wireless Distribution System (WDS) is a wireless method of configuring a network backbone between AP-3 devices. WDS functions much like Ethernet. Using wireless cards, WDS allows you to configure up to six (6) point-to-point links between Access Point devices.

Note: This feature is only applicable to 2.4 GHz (802.11b) cards. It cannot be implemented on 802.11a.

Figure 4-22: Traffic flow between AP-3 devices with WDS



Bridging WDS

Each wireless card can support up to six WDS links, and each link is mapped to a logical port on the AP-3 (WDS ports). WDS ports behave like Ethernet ports on the AP-3 but BSS ports are handled differently: the AP-3 learns by association on BSS ports and from frames on WDS/ Ethernet ports.

AP-3 Ports
1. Ethernet Port
2. BSS Port (Wireless Card A)
3-8. WDS ports for Wireless Card A
9. BSS Port (Wireless Card B)
10-15. WDS Ports for Wireless Card B

Note: The above assumes that the AP-3 has two 802.11b cards installed.

Configuring WDS

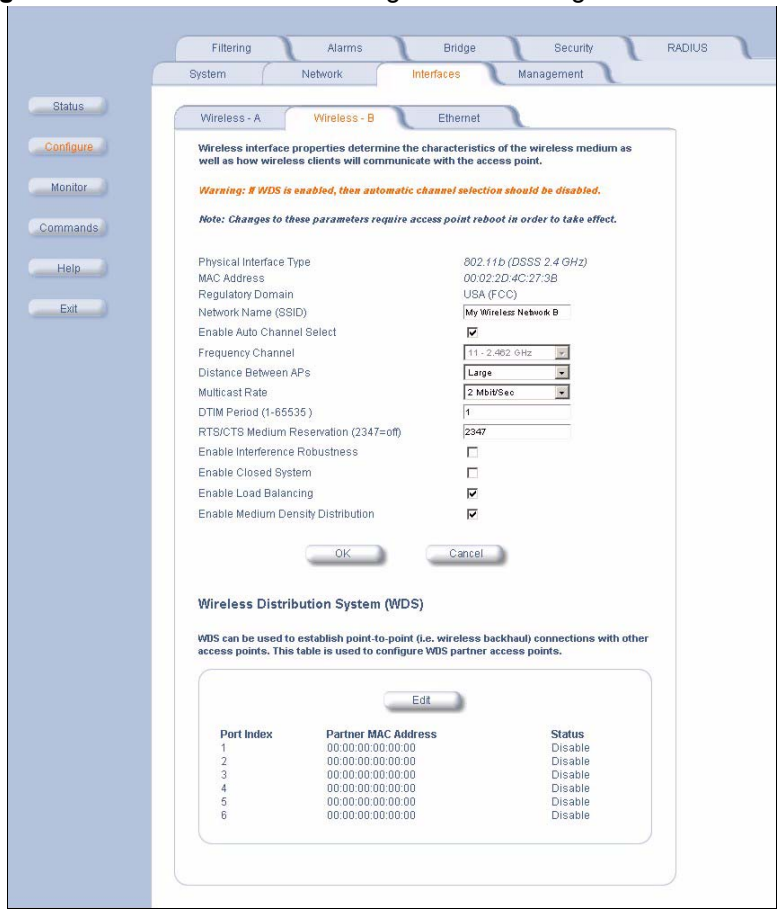
- The state of each WDS port in the bridge/spanning tree can be controlled from two places:
  - 802.11 MIB WDS table
  - Bridge MIB port table
- If you are only using one card, always place it in Slot A.
- Spanning tree determines the port states if WDS configurations are correct.
- If there is no partner MAC address configured in the WDS table, the WDS port remains disabled.
- No two partner MAC addresses should be the same for WDS ports on the same card.
- Channel settings on the cards should be the same.

WDS Setup Procedure

Note: WDS and ACS cannot be Enabled at the same time on the same card.

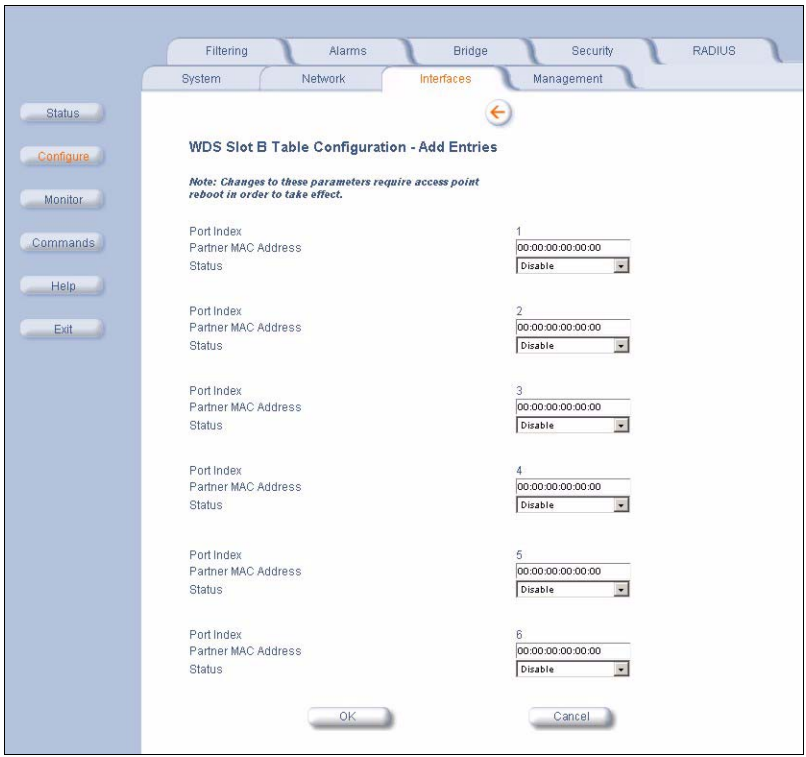
To setup a wireless backbone follow the steps below for each AP-3 that you wish to include in the wireless distribution system. Since WDS and ACS cannot be Enabled at the same time on the same card, the first step must be to ensure ACS is disabled. Follow the process described in Disabling ACS in Prerequisites.

Figure 4-23: Wireless Interface Page - WDS Configuration



1. Write down the MAC Address of the Avaya Wireless PC Card inside the wireless slot of the AP-3 that you wish to include in the wireless distribution system (this value is printed on a label on the back of the PC Card).
2. In the Web Interface, click the **Configure** button and select **Interfaces**.
3. Select the **Wireless** sub-tab that corresponds to the card's location (slot A or B).
4. Click the **Edit** button to update the Wireless Distribution System (WDS) Table.

Figure 4-24: WDS Table Configuration Page



1. Enter the MAC Address that you registered in Step 2 in the **Partner MAC Address** field of the Wireless Distribution Setup window.
2. Set the **Status** of the device to **Enable**.
3. Select **OK.**

Setup the WDS 802.1x Security Mode

To set up a Wireless Distribution System (WDS) with 802.1x security mode, set the AP-3 unit in mixed mode and give each AP-3 unit in the WDS the same encryption key 1:

1. In the Web Interface, click the **Configure** button and select the **Security** tab.
2. In the **802.1x Security Mode** field, select **Mixed (802.1x and WEP)** from the pull-down menu.
3. Select a key length from the pull-down menu.

Note: A **64-bit card** (also sometimes referred to as 40-bit encryption) has a key length of 5 alphanumeric characters or 10 hexadecimal digits, while a **128-bit card** (also sometimes referred to as 104-bit encryption) has a key length of 13 characters or 26 hexadecimal digits. Key length varies based on the card type. 802.11a cards do not support WDS.

4. Click the **Encryption** and enter a value for **Encryption Key 1**. This must be the same length as what you choose for the key length in the 802.1x page.

Note: Make sure that each AP-3 unit that is a member of the WDS has the same value for Encryption Key 1.

5. Click **OK**.

6. The AP-3 unit will need to be rebooted for the changes to take affect.

Wireless Port Mapping

When using Spanning Tree to configure WDS links, you must first configure the MAC address of the card to which the wireless link will be established. Data transmitted on the WDS port goes directly, via point-to-point link, to the MAC address of the wireless card you configure.

Note: Since six (6) WDS ports can be configured for each card, you need to map paths from WDS ports to mutually exclusive wireless port designations for Spanning Tree.

Configuring the AP-3 Unit as a Wireless Repeater

This configuration requires two or three AP-3 devices. If you have three devices, a dedicated wireless AP-3 unit should be configured with Slot A and Slot B of the AP-3 device wireless distribution link. This AP-3 unit should not be connected to a wired interface. Please note: A slot may repeat up to six wired links. Also, the other two wired AP-3 units should be configured so that one slot partners with the Wireless WDS partner.

If you have two devices, form a WDS link between them by configuring one wireless card in each AP-3 as a dedicated WDS port.

Additional Information: The AP-3 unit should only allow client associations on those channels and network names that are configured for a WDS link.

Result: The wireless AP-3 unit functions as a repeater.

Advanced RADIUS Features

This section contains additional information about the AP-3's interaction with your network's RADIUS servers.

Fallback to Primary RADIUS Server

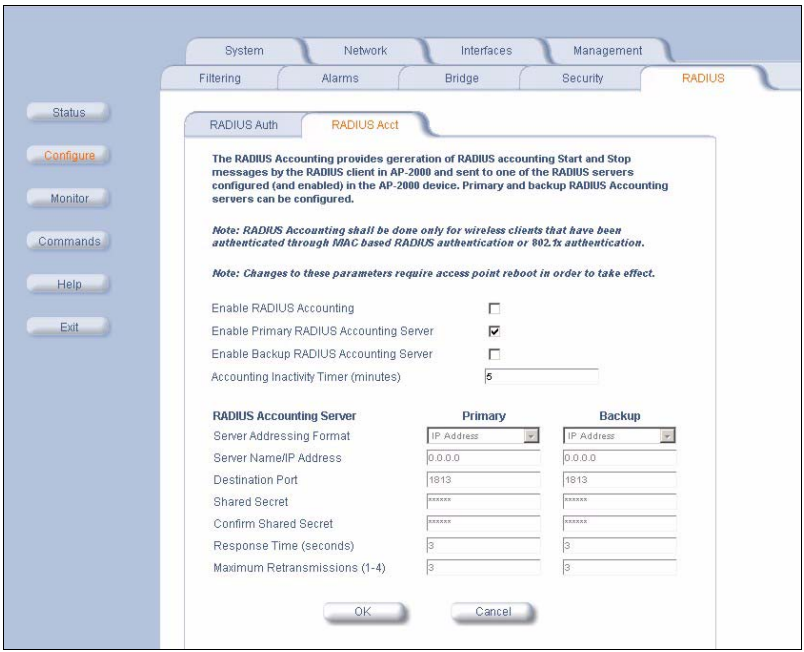
This automatic feature ensures the primary RADIUS server is used to authenticate your network when it is available. If you have configured the AP-3 with a primary and a backup RADIUS server, the following process occurs:

1. The AP-3 will switch to the backup server if the primary server fails for any reason.
2. After the unit has switched to the backup server, it will periodically check the status of the primary RADIUS server every five (5) minutes.
3. Once the primary RADIUS server is again online, the AP-3 automatically reverts from the backup RADIUS server back to the primary RADIUS server.
4. All subsequent requests are sent to the primary RADIUS server.

RADIUS Start/Stop Accounting

Using an external RADIUS server, the AP-3 can track and record the length of client sessions on the access point by sending RADIUS accounting messages per RFC2866. When a wireless client is successfully authenticated, RADIUS accounting is initiated by sending an “Accounting Start” request to the RADIUS server. When the wireless client session ends, an “Accounting Stop” request is sent to the RADIUS server.

Figure 4-25: RADIUS Accounting Configuration Page



Session Length

Sessions continue when a client reauthenticates to the same AP-3. Sessions are terminated when a client:

- disassociates.
- does not transmit any data to the AP-3 for a fixed amount of time.
- is detected on a different interface.

If the client roams from one AP-3 to another, one session is terminated and a new session is begun.

Note: This feature requires RADIUS authentication using MAC Access Control or 802.1x. Wireless clients configured in the AP-3's static MAC Access Control list are not tracked.

Configuring RADIUS Accounting

Follow these steps to enable RADIUS accounting on the AP-3:

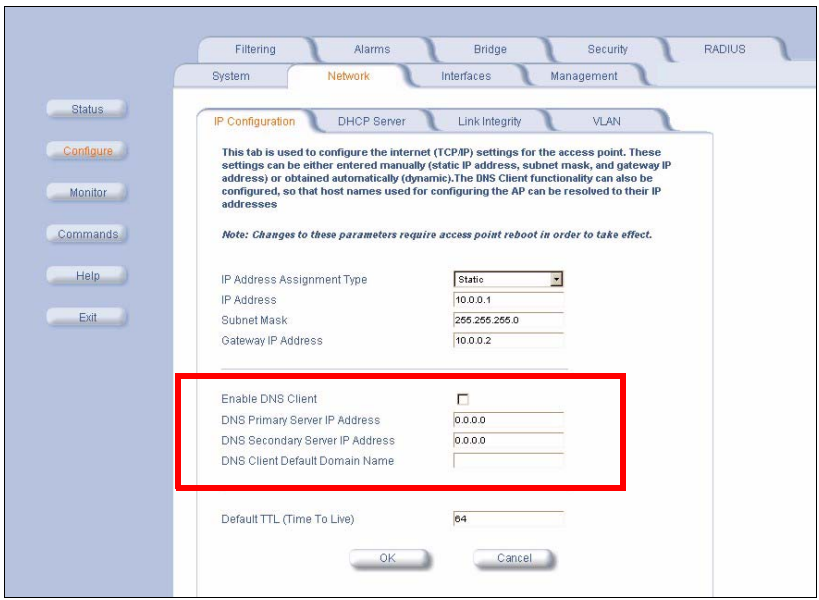
1. In the Web Interface, click the **Configure** button and select **RADIUS**.
2. Select the **RADIUS Acct** sub-tab.
3. Place a checkmark in the **Enable RADIUS Accounting** box to turn on this feature.

4. Place a checkmark in the appropriate box or boxes to enable the primary and backup RADIUS Accounting servers. You must specify information for at least the Primary RADIUS server. The Backup RADIUS server is optional.
5. Enter the session timeout interval in minutes within the **Accounting Inactivity Timer** field. An accounting session automatically ends for a client that is idle for the period of time specified.
6. Select the **Server Addressing Format** (either IP address or server name). Use a server name only if you have enabled the DNS Client functionality. See RADIUS DNS Host Name Support.
7. Enter the server's IP address or name (depending on the Server Addressing Format setting) in the field provided.
8. Enter the **Destination Port**. The default is 1813, however your RADIUS server provider may have another communication port defined.
9. Enter the RADIUS server password in the **Shared Secret** and **Confirm Shared Secret** fields.
10. Configure the **Response Time** (the maximum time, in seconds, to wait for the RADIUS server to respond to a request) and **Maximum Retransmission** (the maximum number of times a request may be retransmitted) values.
11. Click **OK** to save your changes and reboot the AP-3.

RADIUS DNS Host Name Support

DNS Names are familiar names used to identify network hosts instead of IP addresses. For your convenience, the AP-3 can be configured as a DNS client to recognize the DNS host name of your RADIUS server (so you can specify a RADIUS Server's name rather than its IP address in the RADIUS server configuration pages).

Figure 4-26: IP Configuration Page - Configuring the AP-3 as a DNS Client



Using DNS Host Names

1. In the Web Interface, click the **Configure** button and select the **Network** tab.
2. Select the **IP Configuration** sub-tab.
3. Once you have configured the IP information for your AP-3, select the check box to **Enable DNS Client**.
4. In the **DNS Primary Server IP Address** field, enter the IP Address of the Primary DNS server which will resolve the RADIUS Server Host name to an IP address.
5. In the **DNS Secondary Server IP Address** field, enter the IP Address of the Secondary DNS server which will resolve the RADIUS Server Host name to an IP address, if applicable.
6. Enter the DNS host name, also called the **DNS Client Default Domain Name**.
7. Select **OK** to save your changes and reboot the AP-3.

Troubleshooting 5

In This Chapter

Note: This section helps you locate problems related to the AP-3 device setup. For details about RADIUS, TFTP, Serial communications program (such as HyperTerminal), Telnet applications or web browsers, please refer to their respective documentation.

Troubleshooting Concepts

The following list identifies important troubleshooting concepts and topics. The most common initialization and installation problems relate to IP Addressing. For example, you must have valid IP Addresses for both the AP-3 device and the TFTP server before you can transfer files over Ethernet.

- **IP Address management is fundamental**. Refer to Record Configuration Settings
- **Factory default units are set for "Dynamic" (DHCP) IP Address assignment**. The default IP Address for the AP-3 is 10.0.0.1. If you connect the AP-3 unit to a network with an active DHCP server, then use ScanTool to locate the IP Address of your unit. If a DHCP server is not active on your subnet, then the ScanTool can be used to configure your AP-3.
- **The Trivial File Transfer Protocol (TFTP) provides a means to download and upload files**. These files include the AP-3 Image (executable program) and configuration files.

- **If the** AP-3 **password is lost or forgotten, you will need to reset to default values**. The Reset to Factory Default Procedure resets configuration, but does not change the current AP Image.
- **If all else fails**… Use the Forced Reload Procedure to erase the current AP-3 Image and then download a new image. Once the new image is loaded, use the Reset to Factory Default Procedure to set the unit to factory default values and reconfigure the unit.
- AP-3 **supports a Command Line Interface (CLI)**. If you are having trouble locating your AP-3 on the network, connect to the unit directly using the serial interface and refer to Using the Command Line Interface for CLI command syntax and parameter names.

Symptoms and Solutions

Connectivity Issues

Connectivity issues include any issues that prevent you from powering up or connecting to the AP-3 device.

AP-3 Unit Will Not Boot - No LED Activity

1. Make sure your power source is operating.
2. Make sure all cables are connected to the AP-3 unit correctly.
3. With Active Ethernet, make sure you are using a Category 5, foiled, twisted pair cable to power the AP-3 unit.

Serial Link Does Not Work

1. Make sure you are using the proper serial port cable.
2. Double-check the physical network connections.

3. Make sure your PC terminal program (such as HyperTerminal) is active and configured to the following values:
   - Com Port: (COM1, COM2, etc. depending on your computer);
   - Baud rate: 9600; Data bits: 8; Stop bits: 1; Flow Control: None; Parity: None;
   - Line Feeds with Carriage Returns
     (In HyperTerminal select:
     File -> Properties -> Settings -> ASCII Setup -> Send Line Ends with Line Feeds.)

Ethernet Link Does Not Work

1. Double-check the physical network connections. Use a known-good unit to make sure the network connection is present. Once you have the AP-3 IP Address, you can use the “Ping” command over Ethernet to test the IP Address. If the AP-3 responds to the Ping, then the Ethernet Interface is working properly.
2. Perform network infrastructure troubleshooting (check switches, routers, etc.).

Basic Software Setup and Configuration Problems

Lost AP-3, Telnet, or SNMP Password

1. Perform the Reset to Factory Default Procedure in this guide. This procedure resets system and network parameters, but does not affect the AP-3 Image.

Important: The default AP-3 password is “public”, and the default Telnet password is also “public”.

2. Document your password(s) in the form provided in Record Configuration Settings.

Client Computer Cannot Connect

1. Each wireless PC Card in the AP-3 unit should have a unique Network Name. This Network Name must match the active Network Name on client machines.

Note: For example the Avaya Wireless client software allows you to store Network Names in configuration profiles, then you can select a profile to fit your location.

2. Network Names should be allocated and maintained by the Network Administrator.

3. Refer to the documentation that came with your client card for additional troubleshooting suggestions.

AP-3 Has Incorrect IP Address

1. Default IP Address Assignment mode is dynamic (DHCP). If you do not have a DHCP server on your network, the default IP Address is **10.0.0.1**.
2. If the DHCP server in your network is not available for some reason while the AP-3 unit reboots, the device will retain the last IP Address it had. Reboot the AP-3 device once your DHCP server is on-line again or use the ScanTool to find the current IP Address of the AP-3 unit in question.
3. To find the current IP Address using DHCP, check the IP Client Table in the DHCP Server to find the current AP-3 IP Address, match to the AP-3 MAC Address in the table to the one on your unit.
4. **Or use ScanTool to locate the current** AP-3 **IP Address.** Once you have the current IP Address, use the HTTP or CLI Interface to either set the unit to DHCP mode or assign a static IP Address.
5. If you use static IP Address assignments, and cannot access the unit over Ethernet, use the Initializing the IP Address using Normal CLI procedure. Once the IP Address is set, you can use the Ethernet Interface to complete configuration.
6. Perform the Reset to Factory Default Procedure in this guide. This will reset the unit to “DHCP” mode. If there is a DHCP Server on the same subnet, the DHCP Server will assign an IP Address to the AP-3.

HTTP (browser) or Telnet Interface Does Not Work

1. Make sure you are using a compatible browser: Microsoft Internet Explorer 5.0 or better (preferred), or Netscape 6 or higher.
2. Make sure you have the proper IP Address. Enter your AP-3 IP Address in the browser address bar, similar to this example:

   http://192.168.1.100

   When the AP-3 **Login** window appears, leave *the User Name* field empty and enter **public** in the *Password* field.
3. Use the CLI over the serial port to check the SNMP Table, which can be restricting access to Telnet and HTTP.

HTML Help Files Do Not Appear

1. Verify that the HTML Help files are installed in the default directory:
   C:\Program Files\Avaya_Wireless\AP\Help\<language>
2. If the Help files are not located in this folder, contact your network administrator to find out where the Help files are located on your server.

3. Perform the following steps to verify or enter the pathname for the Help files:

   a. Click the **Help** button in the Web Interface.

   b. Select the Help Link tab located at the top of the screen.

   c. Enter the pathname where the Help files are located.

   d. Click **OK** when finished.

Telnet CLI Does Not Work

1. Make sure you have the proper IP Address. Enter your AP-3 IP Address in the Telnet connection dialog, from a DOS prompt, type:

   C:\> telnet <AP-3 **IP Address>**

2. Use the CLI over the serial port to check the SNMP Table, which can be restricting access to Telnet and HTTP.

TFTP Server Does Not Work

1. Make sure the TFTP Server has been started.
2. Verify the IP Address of the TFTP Server. The server may be local or remote, so long as it has a valid IP Address.
3. Configure the TFTP Server to “point” to the folder containing the file to be downloaded (or to the folder in which the file is to be uploaded).
4. Verify that you have the proper AP-3 Image file name and directory path.

Client Connection Problems

Client Software Finds No Connection

- Make sure you have configured your client software with the proper Network Name(s).
- Network Names are typically allocated and maintained by your network administrator.

Client PC Card Does Not Work

1. Make sure you are using the latest PC Card driver software.
2. Download and install the latest Avaya Wireless client software.

Intermittent Loss of Connection

1. Make sure you are within range of an active AP-3 device.
2. You can check the signal strength using the signal strength gauge on your Avaya Wireless client software.

Client Does Not Receive an IP Address - Cannot Connect to Internet

1. If the AP-3 device is configured as a DHCP server, open the Web-browser Interface and select the **Configure** button and then the **Network** tab to make sure the proper DHCP settings are being used.
2. If you are not using the DHCP feature on the AP-3 unit, then make sure that your local DHCP server is operating on the same subnet as your AP-3 device.
3. From the client computer, use the “ping” network command to test the connection with the AP-3 unit. If the AP-3 device responds, but you still cannot connect to the Internet, there may be a physical network configuration problem (contact your network support staff).
4. For units with Active Ethernet, make sure you are not using a crossover type Ethernet cable between the AP-3 unit and the hub.

VLAN Operation Issues

Verifying Proper Operation of the VLAN Feature

The correct VLAN configuration can be verified by “pinging” both wired and wireless hosts from both sides of the AP-3 device and the network switch. Traffic can be “sniffed” on both the wired (Ethernet) and wireless (WDS) backbones (if configured). Bridge frames generated by wireless clients and viewed on one of the backbones should contain IEEE 802.1Q compliant VLAN headers or tags. The VLAN ID in the headers should correspond to one of the VLAN User IDs configured for the AP-3 device.

VLAN Workgroups

The correct VLAN assignment can be verified by doing the following.

- pinging the AP-3 to ensure connectivity,
- pinging the switch to ensure VLAN properties, and
- pinging hosts past the switch to confirm the switch is functional.

Ultimately, traffic can be “sniffed” on the Ethernet or WDS interfaces (if configured) using third-party packages. Most problems can be avoided by ensuring that 802.1Q compliant VLAN tags containing the proper VLAN ID have been inserted in the bridged frames. The VLAN ID in the header should correspond to the user’s assigned network name.

What if network traffic is being directed to a nonexistent host?

- All sessions are disconnected, traffic is lost, and a manual override is necessary
- Workaround: you can configure the switch to mimic the nonexistent host

I have just configured the Management ID and now I can't manage the AP?

- Check to ensure your password is correct. If your password is incorrect or all inbound packets do NOT have the correct tag, then a manual override is necessary.

CAUTION: The manual override process disconnects all users and resets all values to factory defaults.

Active Ethernet

The AP-3 Unit Does Not Work

1. Verify that you are using a standard UTP Cat. 5 cable, including all 8 wires (4 pairs).
2. Try to move the same load into a different port on the same AE hub – if it works, there is probably a faulty port or bad RJ-45 port connection.
3. If possible, try to connect the load device into a different AE hub.

4. Try using a different Ethernet cable – if it works, there is probably a faulty connection over the long cable, or a bad RJ45 connection.
5. Check power plug and hub.
6. If Ethernet link goes down, check cable, cable type, switch, and hub.

There Is No Data Link

1. Verify that the indicator for the port is “on.”
2. Verify that the AE is connected to the Ethernet network with a good connection.
3. Verify that the Ethernet cable is Category 5 or better, and is less than 100 meters (approx. 3.25 ft.) in length from the Ethernet source to the AP-3.
4. Try to connect a different device over the same port – if it works and link is established, there is probably a faulty data link in the load.
5. Try to re-connect the load into a different output port (remember to move the input port accordingly) – if it works, there is probably a faulty output or input port in the AE or a bad RJ-45 connection.

“Overload” Indications

1. Verify that you are not using any cross-over cable between the AE output port to the AP-3 device.
2. Verify that there is no short over any of the twisted pair cable or the RJ-45 connector.
3. Move the device into a different output port – if it works, there is probably a faulty port or bad RJ-45 connection.

Recovery Procedures

The most common installation problems relate to IP Addressing. For example, without the TFTP server IP Address, you will not be able to download the AP Image to the AP-3. IP Address management is fundamental. It is recommended that you create a chart to document and validate the IP addresses for your system. You can also use the form provided in Record Configuration Settings.

If the password is lost or forgotten, you will need to reset the AP-3 to default values. The Reset to Factory Default Procedure resets configuration settings, but does not change the current AP Image.

If the AP-3 has a corrupted software image, follow the Forced Reload Procedure to erase the current AP Image and download a new image.

Reset to Factory Default Procedure

Use this procedure to reset the network configuration values, including the AP-3 IP Address, IP Mask, and so on. The current AP Image is not deleted. This procedure may be required if the AP-3 password is forgotten.

1. Press and hold the **RELOAD** button for about 10 seconds. Result: The AP-3 reboots, and the factory default network values are restored.
2. If not using DHCP, use the ScanTool or normal CLI to set the AP-3 IP Address, IP Mask, and so on. Please refer to Using the Command Line Interface for CLI information.

Forced Reload Procedure

Use this procedure to erase the current AP image and download a new AP Image. This procedure may be required when the current AP Image is missing or corrupted. Note that this does not delete the AP-3's configuration (in other words, the Forced Reload Procedure does not reset to device to factory defaults).

In this procedure, use the Bootloader CLI over the serial port to set the IP Address and download a new AP Image.

1. While the AP Image is running, press the **RESET** button. Result: The AP-3 reboots and the indicators begin to flash.

Note: By completing Step 2, the firmware in the AP-3 will be erased. A serial cable, a cross-over Ethernet cable, and a TFTP server will be required to reload firmware.

2. Press and hold the **RELOAD** button for about 20 seconds until the **POWER LED** turns amber. Result: The AP-3 deletes the current AP Image. The Bootloader CLI becomes active. The following procedure describes how to use the Bootloader CLI to assign an IP Address and download a new AP Image.

Initialize the AP-3 using the Bootloader CLI

In some cases, specifically when a bad AP Image prevents successful booting, you may need to use the Bootloader CLI to download a new executable AP Image. If you need to force the AP-3 to factory default state after loading a new AP image, use the Reset to Factory Default Procedure above.

To download the AP Image, you will need an Ethernet connection to the computer on which the TFTP server resides. This can be any computer on the LAN, or connected to the AP-3 with a “crossover” Ethernet cable.

You must also connect the AP-3 to a computer with a standard serial cable and use a terminal client, such as HyperTerminal. From the terminal, enter CLI Commands to set the IP Address and download an AP Image.

Preparing to Download the AP Image

Before starting, you need to know the AP-3 IP Address, IP Mask, the TFTP Server IP Address, and the AP Image file name. Make sure the TFTP sever is running and configured to point to the folder containing the image to be downloaded.

Download Procedure

1. Connect the computer serial cable to the AP-3 serial port.
2. Start TFTP Server, and make sure the new AP Image file is in the TFTP directory. In this procedure, TFTP downloads an AP Image to the AP-3.
3. Open your terminal emulator, set the following connection properties, and then connect.
   - Com Port: <COM1, COM2, etc., depending on your computer>
   - Baud rate: 9600
   - Data Bits: 8
   - Stop bits: 1
   - Flow Control: None
   - Parity: None
4. Enable the “ASCII Setup” settings by selecting “Send line ends with line feeds”. Result: HyperTerminal sends a line return at the end of each line of code.

5. Press the **RESET** button on the AP-3. Result: The terminal display shows Power On Self Tests (POST) activity. After approximately 30 seconds, a message indicates: **Sending Traps to SNMP manager periodically**. After this message appears, press the **ENTER** key repeatedly until the following prompt appears.

```
[Device name]>
```

6. Enter only the following statements.

```
[Device name]> set ipaddr <Access Point IP Address>
[Device name]> set ipsubmask <IP Mask>
[Device name]> set ipaddrtype static
[Device name]> set tftpipaddr <TFTP Server IP Address>
[Device name]> set tftpfilename <AP Image File Name>
[Device name]> set ipgw <Gateway IP Address>
[Device name]> reboot 0
```

Example:

```
[Device name]> set ipaddr 10.0.0.12
[Device name]> set ipsubmask 255.255.255.0
[Device name]> set ipaddrtype static
[Device name]> set tftpipaddr 10.0.0.20
[Device name]> set tftpfilename MyImage[Device name]> set
ipgw 10.0.0.30
[Device name]> reboot 0
```

Result: The AP-3 will reboot and then download the image file. Observe the **TFTP** display and you should see downloading activity begin after a few seconds. When downloading has stopped,

the AP-3 is ready for configuration, providing the AP-3 IP Address is correct.

7. Once the AP-3 image is downloaded and you have a valid AP-3 IP Address, configure the AP-3 as described in Prerequisites.

Setting IP Address using Serial Port and Normal CLI

Use the following procedure to set an IP Address over the serial port using the normal CLI. The network administrator typically provides the AP-3 IP Address.

Hardware and Software Requirements

- Standard serial data (RS-232) cable with a female DB-9 connector at each end or a standard serial cable and the Mini-DIN8 to DB-9 adapter included in your kit.
- ASCII Terminal software, such as HyperTerminal.

Attaching the Serial Port Cable

1. Remove power from the AP-3 and your computer.
2. Connect the serial port cable to the back of the AP-3 unit and to your computer.
3. Restart the computer and power up the Access Point device.

Initializing the IP Address using Normal CLI

After installing the serial port cable, you may use the CLI to communicate with the AP-3 using most generic terminal programs, such as HyperTerminal. Once the IP Address has been assigned, use the HTTP Interface or the CLI to complete configuration. Many web sites offer shareware or commercial terminal programs you can download.

Use the following procedure to initialize the AP-3 IP Address.

1. Open your terminal emulator, and then set the following connection properties:
   - Com Port: <COM1, COM2, etc., depending on your computer>
   - Baud rate: 9600
   - Data Bits: 8
   - Stop bits: 1
   - Flow Control: None
   - Parity: None
2. Enable the “ASCII Setup” settings by selecting “Send line ends with line feeds”. Result: HyperTerminal sends a line return at the end of each line of code.
3. Press the **RESET** button on the AP-3 (located on the LED Indicator side of the unit). Result: The terminal display shows Power On Self Tests (POST) activity, and then displays a CLI prompt, similar to the example below. This process may take up to 90 seconds.

```
[Device name]> Please enter password:
```

4. Enter the password (default is "public"). Result: The terminal displays a welcome message and then the CLI Prompt:

```
[Device name]>
```

5. Enter **show ip**. Result: Network parameters appear:

```
[Device name]> show ip
```

Figure 5-1: Result of “show ip” bootloader CLI command

```
[Device Name]> show ip
IP/Network Group Parameters
===========================

ipaddr          :       10.0.0.1
ipsubmask       :       255.0.0.0
ipgw            :       10.0.0.1
ipttl           :       64
ipaddrtype      :       static


[Device Name]> _
```

2. Change the IP Address and other network values using **set** and **reboot** CLI commands, similar to the example dialog below (use your own IP Address and IP Mask). Result: After each entry the CLI reminds you to reboot; however wait to reboot until all commands have been entered.

```
[Device name]> set ipaddrtype static
[Device name]> set ipaddr <IP Address>
[Device name]> set ipsubmask <IP Mask>
[Device name]> set ipgw <Default Gateway IP
```

```
Address>
[Device name]> reboot 0
```

3. After the AP-3 reboots, verify the new IP Address by reconnecting, and then entering a **show ip** CLI statement (as in Step 5). Alternatively, you can use the **ping** network command from networked computers to test the new IP Address.
4. When the proper IP Address is set, use CLI or the HTTP Interface over the LAN to complete configuration and manage operations.

System Alarms (Traps)

Security Alarms

oriTrapAuthenticationFailure	A client has failed to authenticate using one of the following authentication methods: MAC Access Control Table, RADIUS MAC Authentication, or 802.1x Authentication (for 802.1x, EAP type is specified)
oriTrapUnauthorizedManagerDetected	An unauthorized manager has attempted to view and/or modify parameters

Wireless Interface Card Alarms

oriTrapWLCNotPresent	Wireless Card (A and/or B) not present
oriTrapWLCFailure	Wireless Card (A and/or B) general failure
riTrapWLCRemoval	Wireless Card (A and/or B) removal
oriTrapWLCIncompatibleFirmware	Wireless Card (A and/or B) incompatible firmware detected
oriTrapWLCVoltageDiscrepancy	Wireless Card (A and/or B) voltage discrepancy detected
oriTrapWLCIncompatibleVendor	Wireless Card (A and/or B) incompatible vendor detected
oriTrapWLCFirmwareDownloadFailure	Wireless Card (A and/or B) firmware download failure detected

Operational Alarms

oriTrapWatchDogTimerExpired	Watch Dog Timer has expired
oriTrapRADIUSServerNotResponding	RADIUS Server is not responding or error communicating with RADIUS Server
oriTrapModuleNotInitialized	Module has not been initialized

oriTrapDeviceRebooting	Device is rebooting
oriTrapTaskSuspended	Task suspension has been detected
oriTrapBootPFailed	BootP failure detected (no response from BootP Server)
oriTrapDHCPFailed	DHCP Client failure detected (no response from DHCP server)

FLASH Memory Alarms

oriTrapFlashMemoryEmpty	Flash memory card detected empty
oriTrapFlashMemoryCorrupted	Flash memory data corrupted

TFTP Alarms

oriTrapTFTPFailedOperation	FTP (upload or download) failure detected
oriTrapTFTPOperationInitiated	TFTP (upload or download) operation initiated
oriTrapTFTPOperationCompleted	TFTP (upload or download) operation completed

Image Alarms

oriTrapZeroSizeImage	Zero size image has been downloaded to device
oriTrapInvalidImage	Invalid image has been downloaded to device
oriTrapImageTooLarge	Image downloaded to device is too big
oriTrapIncompatibleImage	Incompatible image has been downloaded to device

Standard MIB-II (RFC 1213) Alarms

coldStart	Device has been cold started
warmStart	Device has been warm started
linkUp	Device Link is up (Ethernet interface is up)
linkDown	Device Link is down (Ethernet interface is down)

Bridge MIB (RFC 1493) Alarms

newRoot	New root has been added to Bridge
topologyChange	Network Topology change has been detected

Related Applications

RADIUS Authentication Server

If the RADIUS authentication server is selected for authentication during configuration, make sure RADIUS is configured and running. Otherwise, clients will not be able to log in. There are several reasons the authentication server services might be unavailable, here are two typical things to check:

- Make sure you have the proper RADIUS authentication server information setup configured in the AP-3. Check the RADIUS Authentication Server's Shared Secret and Destination Port number (default is 1812; for RADIUS Accounting, the default is 1813).
- Make sure the RADIUS authentication server RAS setup matches the AP-3.

TFTP Server

The “Trivial File Transfer Protocol” (TFTP) server allows you to transfer files across a network. You can upload files from the AP-3 for backup or copying, and you can download the files for configuration and AP Image upgrades. The TFTP software is located on the Avaya Wireless AP-3 Installation CD-ROM.

If a TFTP server is not configured and running, you will not be able to download and upload images and configuration files to/from the AP-3. Remember that the TFTP server does not have to be local, so long as you have a valid TFTP IP Address. TFTP does not have to be running for AP-3 operations that do not transfer files.

After the TFTP server is installed:

- Check to see that TFTP is configured to point to the directory containing the AP Image.
- Make sure you have the proper TFTP server IP Address, the proper AP Image file name, and that the TFTP server is connected.
- Make sure the TFTP server is configured to both send and receive, with no time-out.

LED Indicators

POWER	ETHERNET	PC CARD A	PC CARD B	INDICATION
Green	Green flash with data activity	Green flash with data activity	Green flash with data activity	Normal Operation
Amber	n/a (not applicable)	Amber	Amber	Rebooting
Amber	n/a	n/a	n/a	Missing or bad AP Image if amber after reboot
Red	Red	n/a	n/a	Power On Self Test (POST) running
n/a	n/a	Red	Red	PC Card incompatible on indicated interface
n/a	n/a	Red	Red	PC Card failure on indicated interface
Green	n/a	Amber	Amber	Indicated interface in Administrative State
n/a	n/a	Off	Off	PC Card not present

Using the Command Line Interface 6

In This Chapter

This section provides details for the Command Line (CLI) Interface used to manage an Avaya Wireless AP-3 device. CLI commands can be used to initialize, configure, and manage network operation of the Access Point.

- CLI commands may be entered in real time through a keyboard or submitted with CLI scripts.
- The CLI is available through both the Serial Port Interface and the Ethernet Interface.

Note: All CLI commands and parameters are case-sensitive.

Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts, network access infrastructures, and client-server relationships. In addition, you should be familiar with software setup procedures for typical network operating systems and servers.

Notation Conventions

- Computer prompts are shown as constant width type. For example: `[Device name]>`
- Information that you input as shown is displayed in bold constant width type. For example: `[Device name]>` **`set ipaddr 10.0.0.12`**
- The names of keyboard keys, software buttons, and field names are displayed in bold type. For example: Click the **Configure** button
- Screen names are displayed in bold italics. For example, the ***System Status*** screen.

Important Terminology

- Configuration Files - Database files containing the current Access Point configuration. Configuration items include the IP Address and other network-specific values. Config files may be downloaded to the Access Point or uploaded for backup or troubleshooting.
- Download Vs. Upload - Downloads transfer files to the Access Point. Uploads transfer files from the Access Point. The TFTP server performs file transfers in both directions.
- Group - A logical collection of network parameter information. For example, the System Group is composed of several related parameters. Groups can also contain Tables. All items for a given Group can be displayed with a “show” <Group> CLI Command.
- Image File - The Access Point software executed from RAM. To update an Access Point you typically download a new Image File.

This file is often referred to as the "AP Image".

- Parameter - A fundamental network value that can be displayed and may be changeable. For example, the Access Point must have a unique IP Address and the Radio PC Cards must know which channel to use. Change parameters with the CLI set Command, and view them with the CLI show Command
- Table - Tables hold parameters for several related items. For example, you can add several potential managers to the SNMP Table. All items for a given Table can be displayed with a show <Table> CLI Command.
- TFTP - Refers to the TFTP Server, used for file transfers.

Navigation and Special Keys

This CLI supports the following navigation and special key functions to move the cursor along the prompt line.

Key Combination	Operation
Delete or Backspace	Delete previous character
Ctrl-A	Move cursor to beginning of line
Ctrl-E	Move cursor to end of line
Ctrl-F	Move cursor forward one character
Ctrl-B	Move cursor back one character
Ctrl-D	Delete the character the cursor is on

Key Combination	Operation
Ctrl-U	Delete all text to left of cursor
Ctrl-P	Go to the previous line in the history buffer
Ctrl-N	Go to the next line in the history buffer
Tab	Complete the command line
?	List available commands

CLI Error Messages

The following table describes the error messages associated with improper inputs or expected CLI behavior.

Error Message	Description
Syntax error	Invalid syntax entered at the command prompt.
Invalid command	A non-existent command has been entered at the command prompt.
Invalid parameter name	An invalid parameter name has been entered at the command prompt.
Invalid parameter value	An invalid parameter value has been entered at the command prompt.
Invalid table index	An invalid table index has been entered at the command prompt.
Invalid table parameter	An invalid table parameter has been entered at the command prompt.
Invalid table parameter value	An invalid table parameter value has been entered at the command prompt.
Read only parameter	User is attempting to configure a read-only parameter.
Incorrect password	An incorrect password has been entered in the CLI login prompt.
Download unsuccessful	The download operation has failed due to incorrect TFTP server IP Address or file name.

Error Message	Description
Upload unsuccessful	The upload operation has failed due to incorrect TFTP server IP Address or file name.

Command Line Interface (CLI) Variations

Administrators use the CLI to control Access Point operation and monitor network statistics. The AP-3 supports two types of CLI: the Bootloader CLI and the normal CLI. The Bootloader CLI provides a limited command set, and is used when the current AP Image is bad or missing. The Bootloader CLI allows you to assign an IP Address and download a new image. Once the image is downloaded and running, the Access Point uses the normal CLI. This guide covers the normal CLI unless otherwise specified.

Bootloader CLI

The Bootloader CLI is a minimal subset of the normal CLI used to perform initial configuration of the AP-3 device. This interface is only be accessible via the serial interface if the AP-3 unit does not contain an image (binary) or the TFTP operation has failed as result of the download command for an image.

The Bootloader CLI provides you with the ability to configure the initial setup parameters as well as download an image (binary) to the device.

The functions that shall be supported by the Bootloader CLI are:

- configuration of initial device parameters using the **`set`** command
- **`show`** command to view the device's configuration parameters
- **`help`** command to provide additional information on all commands supported by the Bootloader CLI
- **`reboot`** command to reboot the device.

The parameters supported by the Bootloader CLI (for viewing and modifying) are:

- System Name
- IP Address Assignment Type
- IP Address
- IP Mask
- Gateway IP Address
- TFTP Server IP Address
- Image (binary) File Name

The following lists display the results of using the **help** and **show** commands in the Bootloader CLI:

```
[DeviceName]>help<CR>
```

Figure 6-1: Results of “help” bootloader CLI command

```
[Device name]> help

Command List        Description
============        ===========
set                 Set system parameters
show                Show running system information
help                Description of commands, command usage and parameters
reboot              reboot the target

Command Usage
=============
set <parameter name> <parameter value> <cr>
show <cr>
help <cr>
reboot <cr>

Parameter List      Description
==============      ===========
sysname             System Name
ipaddr              System IP Address
ipsubmask           System Subnet Mask
ipgw                System Default Gateway IP Address
tftpipaddr          TFTP Server IP Address
tftpfilename        Image or Binary File name
ipaddrtype          System IP Address Type - STATIC or DYNAMIC

[Device name]>
```

CLI Command Types

This guide divides CLI Commands into two categories: Operational and Parameter Control.

Operational CLI Commands

This type affects Access Point behavior, such as downloading, rebooting, and so on. After entering commands (and parameters, if any) press the Enter key to execute the Command Line.

Operational commands include:

- ? - (Question Mark) Lists CLI Commands or parameters, depending on usage
- done, exit, quit - Terminates the CLI session
- download - Uses TFTP server to download “image”, “config”, or “bootloader upgrade” files to Access Point
- help - Displays general CLI help information or command help information, such as command usage and syntax
- history - Remembers commands to help avoid re-entering complex statements
- passwd - Sets the Access Point CLI password
- reboot - Reboots the Access Point in specified time
- search - Lists the parameters in a specified Table

- upload - Uses TFTP server to upload “config” files from Access Point to TFTP default directory or specified path

? (List Commands)

This command has varied uses to display commands and parameters, depending on the operation in which it is used.

The following table lists each operation and provides a basic example. Following the table are detailed examples and display results for each operation.

Operation	Basic Example
Display the Command List (Example 1)	`[Device Name]>?`
Display commands that start with specified letters (Example 2)	`[Device Name]>s?`
Display parameters for set and show Commands (Examples 3a and 3b)	`[Device Name]>set ?` `[Device Name]>show ipa?`
Prompt to enter successive parameters for Commands (Example 4)	`[Device Name]>download ?`

Example 1. Display Command list

To display the Command List, enter "?"

```
[Device Name]>?<CR>
```

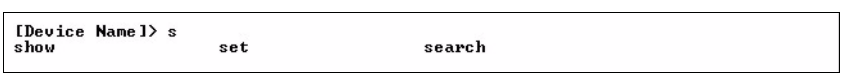
Figure 6-2: Result of "?" CLI command

Example 2. Display specific Commands

To show all commands that start with specified letters, enter one or more letters, then "?" with no space between letters and "?".

```
[Device Name]>s?<CR>
```

Figure 6-3: Result of "s?" CLI command



Example 3. Display parameters for set and show

Example 3a allows you to see every possible parameter for the set (or show) commands. Notice from example 3a that the list is very long. Example 3b shows how to display a subset of the parameters based on initial parameter letters.

Example 3a. Display every parameter that can be changed

```
[Device Name]>set ?<CR>
```

Figure 6-4: Result of “set ?” CLI command

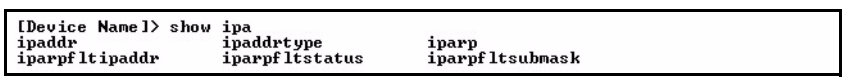
```
[Device Name]> set
Command Description:
The set command modifies the value of a given scalar parameter or table entry.

Command Usage:
set <parameter> <parameter value> <CR>
set <table> <index> <arg1> <value1> ..... <argN> <valueN> <CR>

Example:
set sysname "My Wireless Device" <CR>
set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask 255.255.0.0 cmt "Test WorkStation"
 <CR>

[Device Name]> set
broadcastflttbl
dhcpgw
dhcpippooltbl
dhcppridnsipaddr
dhcpsecdnsipaddr
dhcpstatus
dnsdomainname
dnsprisvripaddr
dnssecsvripaddr
dnsstatus
etherfltifbitmask
.
.
.
.
telsessiontout
tftpfilename
tftpfiletype
tftpipaddr
vlanidtbl
vlanmgmtid
vlanstatus
wdstbl
wif
wifsec
[Device Name]> set _
```

Example 3b. Display parameters based on letter sequence

This example shows entries for parameters that start with the letter "i". The more letters you enter, the fewer the results returned. Notice that there is no space between the letters and the question mark.

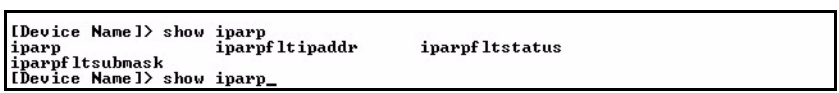
```
[Device Name]> show ipa?<CR>
```

Figure 6-5: Result of “show ipa?” CLI command




```
[Device Name]> show iparp?<CR>
```

Figure 6-6: Result of “show iparpf?” CLI command



Example 4. Display Prompts for Successive Parameters

Enter the command, a space, and then "?". Then, when the parameter prompt appears, enter the parameter value. Result: The parameter is changed and a new CLI line is echoed with the new value (in the first part of the following example, the value is the IP Address of the TFTP server).

After entering one parameter, you may add another "?" to the new CLI line see the next parameter prompt, and so on until you enter all parameters. The following example shows how this is used for the "download" Command. The last part of the example shows the completed download Command ready for execution.

```
[Device Name]> download ?<CR>
               <TFTP IP Address>
[Device Name]> download 10.0.0.2 ?<CR>
               <File Name>
[Device Name]> download 10.0.0.2 apimage ?<CR>
               <file type (config/bin/bspbl)>
[Device Name]> download 10.0.0.2 apimage bin
```

done, exit, quit

Each command disconnects the CLI Session.

```
[Device Name]> done
[Device Name]> exit
[Device Name]> quit
```

download

Downloads the specified file from TFTP server to the Access Point. Executing 'download' in combination with the asterisks character, "*", will make use of the previously set TFTP parameters. Executing download without parameters will display command help and usage information.

1. Syntax to download a file:

```
[Device Name]>download <tftp server address> <path and
              filename> <file type>
```

Example:

```
[Device Name]>download 192.168.1.100 APImage2 bin
```

2. Syntax to display help and usage information:

```
[Device Name]>download
```

3. Syntax to execute the download Command using previously set (stored) TFTP Parameters:

```
[Device Name]>download *
```

help

Displays instructions on using control-key sequences for navigating a Command Line, and displays command information and examples.

1. Using help as the only argument:

```
[Device Name]>help<space>
```

Figure 6-7: Results of “help<space>” CLI command

```
[Device Name]> help
Type ? at the command prompt for a command list.

Complete command description and command usage can be provided by:
help <command name> <CR>
<command name> help <CR>

Special keys supported:
Arrow Keys
DEL, BS .... delete previous character
Ctrl-A  .... go to beginning of line
Ctrl-E  .... go to end of line
Ctrl-F  .... go forward one character
Ctrl-B  .... go backward one character
Ctrl-D  .... delete current character
Ctrl-U, X .. delete to beginning of line
Ctrl-K  .... delete to end of line
Ctrl-W ..... delete previous word
Ctrl-T ..... transpose previous character
Ctrl-P  .... go to previous line in history buffer
Ctrl-N  .... go to next line in history buffer

Tab     .... will attempt command completion
# .... Comment Character
?       .... will provide command listing

Examples:
 '?'            list all the supported commands
'sh?'           list all commands that start with sh
'show ?'        list all arguments to the show command
'sh<TAB>'       complete the 'show' command

[Device Name]>
```

8. Complete command description and command usage can be provided by:

```
[Device Name]>help <command name>
[Device Name]><command name> help
```

history

Shows content of Command History Buffer. The Command History Buffer stores command statements entered in the current session. To avoid re-entering long command statements, use the keyboard “up arrow” (Ctrl-P) and “down arrow” (Ctrl-N) keys to recall previous statements from the Command History Buffer. When the desired statement reappears, press the “Enter” key to execute, or you may edit the statement before executing it.

```
[Device Name]> history
```

passwd

Changes the CLI Password.

```
[Device Name]> passwd oldpassword newpassword newpassword
```

reboot

Reboots Access Point after specified number of seconds. Specify a value of 0 (zero) for immediate reboot.

```
[Device Name]> reboot 0
[Device Name]> reboot 30
```

search

Lists the members of the specified table. This list corresponds to the table information displayed in the HTTP Interface. In this example, the CLI returns the same IP Management table items displayed in the HTTP Interface.

Figure 6-8: Results of “search” and “search mgmtipaccesstbl” CLI command

```
[Device Name]> search
```

```
[Device Name]> search
broadcastflttbl
dhcpippooltbl
etherflttbl
linkinttbl
macacltbl
mgmtipaccesstbl
portflttbl
radiustbl
radacctbl
secenckeylentbl
snmptraphosttbl
staticmactbl
stmthrestbl
stptbl
sysloghosttbl
vlanidtbl
wdstbl
wif
wifsec
```

```
[Device Name]> search mgmtipaccesstbl
```

```
[Device Name]> search mgmtipaccesstbl
The supported elements are:
index
ipaddr
ipmask
cmt
status
```

upload

Uploads the specified file from AP-3 to TFTP Server directory. Executing ‘upload” with the asterisks, “*”, character will make use of the previously set/stored TFTP parameters. Executing 'upload' without parameters will display command help and usage information.

1. Syntax to upload a file:

```
[Device Name]>upload <tftp server address> <path and
              filename> <filetype>
```

Example:

```
[Device Name]>upload 192.168.1.100 APImage2 bin
```

2. Syntax to display help and usage information:

```
[Device Name]>help upload
```

3. Syntax to execute the upload command using previously set (stored) TFTP Parameters:

```
[Device Name]>upload *
```

Parameter Control Commands

The following sections cover each CLI Command, and include several tables showing parameter properties. The two Parameter Control Commands are show and set. These allow you to view (show) all parameters and statistics and to change (set) parameters.

- show - To see any Parameter or Statistic values, you specify a single parameter, a Group, or a Table.
- set - Use this CLI Command to change parameter values. You can use a single CLI Statement to modify Tables, or modify each parameter separately.

"set" and "show" Command Examples

In general, you will use the CLI "show" Command to view current parameter values, and use the CLI "set" Command to change parameter values. As shown in the following six examples, parameters may be set individually, and all parameters for a given table can be set with a single statement.

Example 1 - Set the Access Point IP Address Parameter

```
Syntax:
[Device Name]>set <parameter name> <parameter value>

Example:
[Device Name]> set ipaddr 10.0.0.12
```

Result: IP Address will be changed when you reboot the Access Point. The CLI reminds you when rebooting is required for a change to take effect. To reboot immediately, enter **`reboot 0`** (zero) at the CLI prompt.

Example 2 - Create a table entry or row

Use 0 (zero) as the index to the table when creating an entry. When creating a table row, only the mandatory table elements are required (comment is usually an optional table element). There are other optional table elements, which, if not entered, the default value applies.

Syntax:

```
[Device Name]>set <table name> <table index> <element 1>
              <value 1> … <element n> <value n>
```

Example:

```
[Device Name]> set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask
               255.255.0.0
```

Result: A new table entry is created that for IP address 10.0.0.10 with a 255.255.0.0 subnet mask.

Example 3 - Modify a table entry or row

Use the index to be modified and the table elements you would like to modify. For example, suppose the IP Access table has one entry and you wanted to modify the IP Address:

```
[Device Name]>set mgmtipaccesstbl 1 ipaddr 10.0.0.11
```

You can also modify several elements in the table entry. Enter the index number and specific table elements you would like to modify. Hint: Use the search Command to see the elements that belong to the table.

```
[Device Name]>set mgmtipaccesstbl 1 ipaddr 10.0.0.12 ipmask
              255.255.255.248 cmt "First Row"
```

Example 4 - Enable, Disable, or Delete a table entry or row

In this example you would like to manage the second table row/entry.

Syntax:

```
[Device Name]>set <Table> index status <enable, disable,
              delete>
[Device Name]>set <Table> index status <1=enable, 2=disable,
              3=delete>
```

Example:

```
[Device Name]>set mgmtipaccesstbl 2 status enable
[Device Name]>set mgmtipaccesstbl 2 status disable
```

```
[Device Name]>set mgmtipaccesstbl 2 status delete
[Device Name]>set mgmtipaccesstbl 2 status 2
```

Note: You may need to enable a disabled table entry before you can change the entry's elements.

Example 5 - Show the Group Parameters

In this example you can view all elements of a group or table.

Syntax:

```
[Device Name]> show <group name>
```

Example:

```
[Device Name]>show network
```

Result: The CLI displays network group parameters. Note **`show network`** and **`show ip`** return the same data.

Figure 6-9: Results of “show network” and “show ip” CLI Commands

```
[Device Name]> show network
IP/Network Group Parameters
===========================

ipaddr          :       10.0.0.1
ipsubmask       :       255.0.0.0
ipgw            :       10.0.0.1
ipttl           :       64
ipaddrtype      :       static


[Device Name]> show ip
IP/Network Group Parameters
===========================

ipaddr          :       10.0.0.1
ipsubmask       :       255.0.0.0
ipgw            :       10.0.0.1
ipttl           :       64
ipaddrtype      :       static


[Device Name]> _
```

Example 6 - Show Individual and Table Parameters

1. View a single parameter.

Syntax:

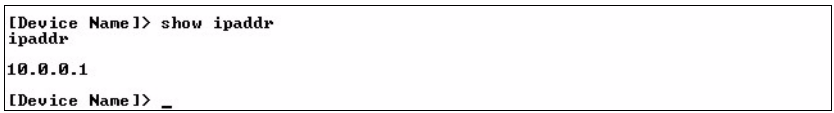
```
[Device Name]>show <parameter name>
```

Example:

```
[Device Name]> show ipaddr
```

Result: Displays the Access Point IP Address.

Figure 6-10: Result of “show ipaddr” CLI Command



2. View all parameters in a table.

Syntax:

```
[Device Name]> show <table name>
```

Example:

```
[Device Name]> show mgmtipaccesstbl
```

Result: Displays the Access Point IP Access Table and its entries.

Using Tables & User Strings

Working with Tables

Each member of the table must be specified, as in the example below.

```
[Device Name]>set mgmtipaccesstbl 0 ipaddr 10.0.0.10 ipmask
              255.255.0.0
```

Below are the rules for creating, modifying, enabling/disabling, and deleting table entries.

- Creation
  - The table name is required.
  - The table index is required – for table entry/instance creation the index is always zero (0).
  - The order in which the table arguments or objects are entered in not important.
  - Parameters that are not required can be omitted, in which case they will be assigned the default value as specified in the MIB or product functional specification document.
- Modification
  - The table name is required.
  - The table index is required – to modify the table, “index” must be the index of the entry to be modified.

- Only the table objects that are to be modified need to be specified. Not all the table objects are required.
- If multiple table objects are to be modified the order in which they are entered is not important.
- If the entire table entry is to be modified, all the table objects have to be specified.

- Enabling/Disabling
  - The table name is required.
  - The table index is required – for table enabling/disabling the index should be the index of the entry to be enabled/disabled.
  - The reserved word enable or disable are required.
- Deletion
  - The table name is required.
  - The table index is required – for table deletion the index should be the index of the entry to be deleted.
  - The reserved word delete is required.

Using Strings

Since there are several string objects supported by the AP-3 device, a string delimiter is required for the strings to be interpreted correctly by the command line parser. For this CLI implementation, the single quote or double quote character can be used at the beginning and at the end of the string.

For example:

```
[Device Name]> set sysname Lobby - Does not need quote marks
[Device Name]> set sysname "Front Lobby" - Requires quote
marks.
```

The scenarios supported by this CLI are:

“My Desk in Nieuwegein”	Double Quotes
‘My Desk in Nieuwegein’	Single Quotes
“My ‘Desk’ in Nieuwegein”	Single Quotes within Double Quotes
‘My “Desk” in Nieuwegein’	Double Quotes within Single Quotes
“Daniel’s Desk in Nieuwegein”	One Single Quote within Double Quotes
‘Daniel”s Desk in Nieuwegein’	One Double Quote within Single Quotes

The string delimiter does not have to be used for every string object. The single quote or double quote only has to be used for string objects that contain blank space characters. If the string object being used does not contain blank spaces, then the string delimiters, single or double quotes, mentioned in this section are not required.

Configuring Objects that Require Reboot

Certain objects supported by Avaya Wireless devices require the device to be rebooted in order for the changes to take effect. In order to inform the end-user of this behavior, the CLI shall provide informational messages when the user has configured an object or object(s) that requires the device to be rebooted. The following message shall be displayed as a result of the configuring such object or objects.

Example 1: Configuring objects that require the device to be rebooted

The following message is displayed every time the user has configured an object that requires the device to be rebooted.

```
[Device Name]>set ipaddr 135.114.73.10
In order for this change to take effect, the device is required to
be rebooted.
```

Example 2: Executing the exit, quit, or done commands when an object that requires reboot has been configured

In addition to the above informational message, the CLI also provides a message as a result of the exit, quit, or done command if changes have been made to objects that require reboot. If you make changes to objects that require reboot and execute the exit command the following message is displayed:

```
[Device Name]>exit<CR> OR quit<CR> OR done<CR>

Modifications have been made to parameters that require the device
to be rebooted. These changes will only take effect after the next
reboot.
```

"set" CLI Command

Sets (modifies) the value of given parameter. To see a definition and syntax example, type only set and then press the Enter key. To see a list of available parameters, enter a space, then a question mark (?) after set (example: set?).

Syntax:

```
[Device Name]>set <parameter> <value>
[Device Name]>set <table> <index> <argument 1> <value 1> ...
                <argument N> <value N>
```

Example:

```
[Device Name]>set sysloc "Main Lobby"
[Device Name]>set mgmtipaccesstbl 0 ipaddr 10.0.0.10 submask
                255.255.0.0
```

"show" CLI Command

Displays the value of specified parameter, or displays all parameter values of a specified group (parameter table). Groups contain Parameters and Tables. Tables contain parameters for a series of similar entities.

To see a definition and syntax example, type only show and then press the Enter key. To see a list of available parameters, enter a question mark (?) after show (example: **show ?**).

Syntax:

```
[Device Name]>show <parameter>
[Device Name]>show <group>
[Device Name]>show <table>
```

Examples:

```
[Device Name]>show ipaddr
[Device Name]>show network
[Device Name]>show mgmtipaccesstbl
```

Configuring the AP-3 Unit using CLI commands

Log Into the AP-3 Unit using HyperTerminal

1. Launch HyperTerminal from the **Start > Programs** menu. Open an existing connection or create a new one with the following settings:
   - Com Port: <COM1, COM2, etc., depending on your computer>
   - Baud rate: 9600
   - Data Bits: 8
   - Stop bits: 1
   - Flow Control: None
   - Parity: None
2. Enable the "ASCII Setup" settings by selecting "**Send line ends with line feeds**".
   (Result: HyperTerminal sends a line return at the end of each line of code.)
3. Enter the CLI password (default is **`public`**).
4. We recommend changing your default passwords immediately. To perform this operation using CLI commands, refer to Change Passwords.

Log Into the AP-3 Unit using Telnet

The CLI commands can be used to access, configure, and manage your AP-3 device using Telnet or a terminal emulation application, such as HyperTerminal. Log into the AP-3 unit using Telnet:

1. Go to the DOS command prompt on your computer.
2. Type in **`telnet <IP Address of the unit>`**.
3. Enter the CLI password (default is **`public`**).

Note: It is recommended that you change your default passwords immediately. To perform this operation using CLI commands, refer to Change Passwords.

Set Basic Configuration Parameters using CLI Commands

There are a few basic configuration parameters that you will want to setup right away when you receive the AP-3 unit. For example:

- Set System Name, Location and Contact Information
- Set Static IP Address for the AP-3 device
- Set Network Names for each Wireless Interface
- Set WEP Encryption for each Wireless Interface
- Change Passwords
- Download an AP-3 Configuration File from your TFTP Server
- Backup your AP-3 Configuration File

Set System Name, Location and Contact Information

```
[Device Name]>set sysname <system name> sysloc <Unit Location>
[Device Name]>set sysctname <Contact Name (person responsible
              for system)>
[Device Name]>set sysctphone <Contact Phone Number> sysctemail
              <Contact E-mail address>
[Device Name]>show system <CR>
```

Figure 6-11: Result of "show system" CLI Command

```
[Device Name]> show system
System Parameters
=================

sysname                    :       Device Name
sysloc                     :       System Location
sysctname                  :       Contact Name
sysctemail                 :       name@Organization.com
sysctphone                 :       Contact Phone Number
sysuptime (DD:HH:MM:SS)    :        0:11: 6:40
sysoid                     :       1.3.6.1.4.1.11898.2.4.6
sysdescr                   :        AP v2.1.0  SN-02UT16570004 v2.0.10
sysservices                :       2
sysflashupdate             :       0
sysflashbckint             :       120
sysresettodefaults         :       0


[Device Name]> _
```

Set Static IP Address for the AP-3 device

Note: The IP Mask of the AP-3 unit must match your network IP Mask. If you are setting up the AP-3 device from a client station, check the IP mask of your computer before proceeding.

```
[Device Name]>set ipaddrtype static
[Device Name]>set ipaddr <fixed IP address of unit>
[Device Name]>set ipsubmask <IP Mask (default = 255.0.0.0)>
[Device Name]>set ipgw <gateway IP address (default =
               10.0.0.1)>
[Device Name]>show network<CR>
```

Set Network Names for each Wireless Interface

- 3 = wireless card in Slot A4 = wireless card in Slot B

```
[Device Name]>set wif 3 netname <Network Name (SSID) for
              wireless card in Slot A>
[Device Name]>set wif 4 netname <Network Name (SSID) for
              wireless card in Slot B>
[Device Name]>show wif<CR>
```

Figure 6-12: Results of “show wif” CLI command

```
[Device Name]> show wif
Wireless Interface Table
========================
Index                          :       3
Network Name                   :       My Wireless Network A
Distance Between APs           :       large
Interference Robustness        :       disable
DTIM Period                    :       1
Automatic Channel Selection    :       enable
Frequency Channel              :       56
RTS/CTS Medium Reservation     :       2347
Multicast Rate                 :       2 MBps
Closed System                  :       Not Supported
Load Balancing                 :       Not Supported
Medium Density Distribution    :       Not Supported
MAC Address                    :       00:30:F1:5B:11:0A
Supported Data Rates           :       6 9 12 18 24 36 48 54
Supported Frequency Channels   :       52 56 60 64 36 40 44 48
Physical Layer Type            :       OFDM
Regulatory Domain List         :       USA (FCC)
Transmit Rate                  :       0
TurboMode                      :       disable


Index                          :       4
Network Name                   :       My Wireless Network B
Distance Between APs           :       large
Interference Robustness        :       disable
DTIM Period                    :       1
Automatic Channel Selection    :       enable
Frequency Channel              :       11
RTS/CTS Medium Reservation     :       2347
Multicast Rate                 :       2 MBps
Closed System                  :       disable
Load Balancing                 :       enable
Medium Density Distribution    :       enable
MAC Address                    :       00:02:2D:4C:27:3B
Supported Data Rates           :       1 2 5.5 11
Supported Frequency Channels   :       1 2 3 4 5 6 7 8 9 10 11
Physical Layer Type            :       DSSS
Regulatory Domain List         :       USA (FCC)
Transmit Rate                  :       0
TurboMode                      :       disable
```

Set WEP Encryption for each Wireless Interface

- 3 = wireless card in Slot A4 = wireless card in Slot B

CAUTION: Client stations must have the same encryption key to be able to communicate with the AP-3 device. Each Wireless Interface can only support one Key Length (so each of the configured keys must have the same length). The available key sizes vary based on card type. See Set WEP Encryption for each Wireless Interface for more information.

For the wireless card in Slot A

You can set up to four encryption keys. This example describes setting encryption Key 1 on the wireless card in Slot A.

```
[Device Name]>set wifsec 3 encryptstatus enable encryptkey1
              <WEP key (number of characters vary
              depending on card type)> encryptkeytx 1
[Device Name]>show wifsec<CR>
```

For the wireless card in Slot B

You can set up to four encryption keys. This example describes setting encryption Key 2 on the wireless card in Slot B.

```
[Device Name]>set wifsec 4 encryptstatus enable encryptkey2
              <WEP key (number of characters vary
              depending on card type)> encryptkeytx 1
[Device Name]>show wifsec<CR>
```

Figure 6-13: Result of “show wifsec” CLI Command

```
[Device Name]> show wifsec
Wireless Security table
==============
Index                    :              3
EnableEncryption         :        disable
EncryptionKey1           :       ********
EncryptionKey2           :       ********
EncryptionKey3           :       ********
EncryptionKey4           :       ********
Encryption Key in Use    :           key1
Deny Non Encrypted Data  :         enable

Index                    :              4
EnableEncryption         :        disable
EncryptionKey1           :       ********
EncryptionKey2           :       ********
EncryptionKey3           :       ********
EncryptionKey4           :       ********
Encryption Key in Use    :           key1
Deny Non Encrypted Data  :         enable
```

Change Passwords

[Device Name]>**passwd <Old Password> <New Password> <Confirm Password>**

(CLI password)

[Device Name]>**set httppasswd <New Password>**

[Device Name]>**set snmprpasswd <New Password> (SNMP read password)**

[Device Name]>**set snmprwpasswd <New Password> (SNMP read/write)**

[Device Name]>**reboot 0**

CAUTION: It is strongly recommended that you change the default passwords to restrict access to your network devices to authorized personnel. It is also recommended that you document your AP-3 configuration using the work sheets

provided for you in the chapter, Record Configuration Settings. If you lose or forget your password settings, you can always perform the Reset to Factory Default Procedure.

Download an AP-3 Configuration File from your TFTP Server

Begin by starting your TFTP program. It must be running and configured to transmit and receive.

```
[Device Name]>set tftpfilename <file name> tftpfiletype
              config tftpipaddr <IP address of your TFTP
              server>
[Device Name]>show tftp (ensure the filename, file type,
and the IP address are correct)
[Device Name]>download *
[Device Name]>reboot 0
```

After following the complete process (above) once, you can download a file of the same name (so long as all the other parameters are the same), with the following command:

```
[Device Name]>download *
```

Backup your AP-3 Configuration File

Begin by starting your TFTP program. It must be running and configured to transmit and receive.

```
[Device Name]>upload <TFTP Server IP address> <tftpfilename
              (such as "config.sys")> config
[Device Name]>show tftp (ensure the filename, file type,
              and the IP address are correct)
```

After setting the TFTP parameters, you can backup your current file (so long as all the other parameters are the same), with the following command:

```
[Device Name]>upload *
```

Other Network Settings

There are other configuration settings that you may want to set for your AP-3 unit. Some of them are listed below.

- Configure your AP-3 device as a DHCP Server
- Maintain 802.11b Client Connections using Link Integrity
- Disable VLAN Management
- Change your Wireless Interface Settings
- Configure MAC Access Control
- Set RADIUS Parameters

Note: Refer to Advanced Features for more complex network settings.

Configure your AP-3 device as a DHCP Server

Note: You must have at least one entry in the DHCP Server client IP Address assignment table before you can enable the DHCP Server Status feature.

```
[Device Name]>set dhcpstatus disable
[Device Name]>set dhcpippooltbl 0 startipaddr <start ip
              address> endipaddr <end ip address>
[Device Name]>set dhcpgw <gateway ip address>
[Device Name]>set dhcppridnsipaddr <primary dns ip address>
[Device Name]>set dhcpsecdnsipaddr <secondary dns ip
              address>
[Device Name]>set dhcpstatus enable
[Device Name]>reboot 0
```

CAUTION: Before enabling this feature, confirm that the IP address pools you have configured are valid addresses on the network and do not overlap the addresses assigned by any other DHCP server on the network. Enabling this feature with incorrect address pools will cause problems on your network.

Maintain 802.11b Client Connections using Link Integrity

Note: This feature is only applicable to 2.4 GHz (802.11b) cards.

```
[Device Name]>show linkinttbl (this shows the current
              links)
[Device Name]>set linkinttbl <1-5 (depending on what row in
              the table you wish to address)>ipaddr <ip
              address of the host computer you want to
              check>
[Device Name]>set linkintpollint <the interval between link
              integrity checks>
[Device Name]>set linkintpollretx <number of times to
              retransmit before considering the link
              down>
[Device Name]>set linkintstatus enable
[Device Name]>reboot 0
```

Disable VLAN Management

```
[Device Name]>set vlanmgmtid <1-4094, 0 = disable>
[Device Name]>set vlanstatus disable
[Device Name]>reboot 0
```

Change your Wireless Interface Settings

Enable/Disable Interference Robustness

3 = wireless card in Slot A4 = wireless card in Slot B

```
[Device Name]>set wif <3 or 4> interrobust <enable/disable>
```

This feature is only available for 802.11b wireless cards.

Enable/Disable Closed System

3 = wireless card in Slot A4 = wireless card in Slot B

```
[Device Name]>set wif <3 or 4> closedsys <enable/disable>
```

Note: When disabled, a client configured with the Network Name "ANY" can connect to the AP-3. This feature is only available for 802.11b wireless cards.

Enable/Disable Load Balancing

3 = wireless card in Slot A4 = wireless card in Slot B

```
[Device Name]>set wif <3 or 4> ldbalance <enable/disable>
```

This feature is only available for 802.11b wireless cards.

Enable/Disable Medium Density Distribution

3 = wireless card in Slot A4 = wireless card in Slot B

```
[Device Name]>set wif <3 or 4> meddendistrib <enable/
              disable>
```

This feature is only available for 802.11b wireless cards.

Autochannel Select (ACS)

ACS is enabled by default. In order to disable ACS, disable the cards in slots A and B and reboot.

3 = wireless card in Slot A4 = wireless card in Slot B

```
[Device Name]>set wif <3 or 4> autochannel disable
[Device Name]>reboot 0
```

Re-enable ACS

3 = wireless card in Slot A 4 = wireless card in Slot B

```
[Device Name]>set wif <3 or 4> autochannel enable
[Device Name]>reboot 0
```

Set the Distance Between APs

```
[Device Name]>set wif <3 or 4> distaps <large, medium,
               small, minicell, microcell>
[Device Name]>reboot 0
```

This feature is only available for 802.11b wireless cards.

Note: The distance between APs should not be approximated. It is calculated by means of a manual Site Survey. The site survey is done by setting up an AP-3 unit and by testing the client throughout the area to determine signal strength and coverage, and local limits such as physical interference. From these measurements the appropriate cell size and density is determined, and the optimum distance between APs is calculated to suit your particular business requirements. The Site Survey is contained on the Installation CD included in your kit.

Set the Multicast Rate

```
[Device Name]>set wif <3 or 4> multrate <1,2,5.5,11 (Mbps)>
```

This feature is only available for 802.11b wireless cards.

Note: The Distance Between APs **must be set before** the Multicast Rate.

Set Ethernet Speed and Transmission Mode

```
[Device Name]>set etherspeed <value (see below)>
[Device Name]>reboot 0
```

Ethernet Speed and Transmission Mode	Value
10 Mbit/s - half duplex	10halfduplex
10 Mbit/s - full duplex	10fullduplex
10 Mbit/s - auto duplex	10autoduplex
100 Mbit/s - half duplex	100halfduplex
100 Mbit/s - full duplex	100fullduplex
Auto Speed - half duplex	autohalfduplex
Auto Speed - auto duplex	autoautoduplex (recommended)

Set Interface Management Services

Set Communication Ports

```
[Device Name]>set httpport <HTTP port number
              (default is 80)>
[Device Name]>set telport <Telnet port number
              (default is 23)>
```

Set Telnet Session Timeouts

```
[Device Name]>set tellogintout <time in seconds>
[Device Name]>set telsessiontout <time in seconds>
```

Configure Management Ports

```
[Device Name]>set snmpifbitmask <0, 1, 4, 8, 15
              (default is 15 see below)>
[Device Name]>set httpifbitmask <0, 1, 4, 8, 15
              (default is 15 see below)>
[Device Name]>set telifbitmask <0, 1, 4, 8, 15
              (default is 15 see below)>
```

Choose from the following values:

Interface bitmask	Description
0 = disable (all interfaces)	All management channels disabled
1 = ethernet if	Ethernet only enabled
4 = pcCardA if	Wireless A only enabled
8 = pcCardB if	Wireless B only enabled
15 = allInterfaces	All management channels enabled

Edit Management IP Access Table

```
[Device Name]>set mgmtipaccesstbl <index> ipaddr
              <IP address> ipmask <subnet mask>
```

Configure Serial Port Interface

Note: To avoid unexpected AP-3 performance, leave Flow Control value at default (none) unless you are sure what this setting should be.

```
[Device Name]>set serbaudrate <2400, 4800, 9600, 19200,
              38400, 57600>
[Device Name]>set serflowctrl <none, xon/xoff>
[Device Name]>show serial
```

Figure 6-14: Result of “show serial” CLI Command

```
[Device Name]> show serial
Serial Interface Group Parameters
=================================

serbaudrate              :       9600
serdatabits              :       8
serparity                :       none
serstopbits              :       1
serflowctrl              :       none
```

Configure MAC Access Control

Setup MAC (Address) Access Control Table

```
[Device Name]>set macaclstatus enable
[Device Name]>set macacloptype <passthru, block>
[Device Name]>reboot 0
```

Add an Entry to the MAC Access Control Table

```
[Device Name]>set macacltbl <index> macaddr <MAC Address,
              such as 00:12:34:56:78:ab>status enable
[Device Name]>show macacltbl
```

Disable or Delete an Entry in the MAC Access Control Table

```
[Device Name]>set macacltbl <index> status <disable/delete>
[Device Name]>show macacltbl
```

Note: For larger networks that include multiple AP-3 devices, you may prefer to maintain this list on a centralized location using the RADIUS parameters (see Set RADIUS Parameters).

Set RADIUS Parameters

Configure RADIUS Authentication server

```
[Device Name]>set radiustbl <index> status enable
              seraddrfmt <ipaddr or name>ipaddr <RADIUS
              IP address or name> port <user defined>
              ssecret <user defined> responsetm <1 to 4
              seconds> maxretx <1 to 10 times>
[Device Name]>show radiustbl
```

Figure 6-15: Results of “show radiustbl” CLI command

```
[Device Name]> show radiustbl
RADIUS Authentication Group Table
=========================
Index                    :              1
RADIUS Auth Server Status:       disable
IP Address/Host Name     :       0.0.0.0
Authentication Port      :          1812
Response Time            :             3
Shared Secret            :       ******
Server Addressing Format:          ipaddr
Maximum Retransmission   :             3

Index                    :              2
RADIUS Auth Server Status:       disable
IP Address/Host Name     :       0.0.0.0
Authentication Port      :          1812
Response Time            :             3
Shared Secret            :       ******
Server Addressing Format:          ipaddr
Maximum Retransmission   :             3
```

Enable RADIUS MAC Access Control

```
[Device Name]>set radmacaccctrl enable
[Device Name]>reboot 0
```

Set MAC Address Format Type

```
[Device Name]>set radmacaddrformat <dashdelimited,
              colondelimited, singledashdelimited,
              nodelimiter>
```

Set Authentication Lifetime

```
[Device Name]>set radauthlifetm <60-43200 seconds (in 60
              sec increments)>
```

Enable RADIUS Accounting

```
[Device Name]>set radaccstatus enable
[Device Name]>set radaccinactivetmr <inactivity timer in
              minutes>
[Device Name]>show radius
```

Figure 6-16: Result of “show radius” CLI Command

```
[Device Name]> show radius
RADIUS Group

RADIUS Authentication
====================
radcliinvsvraddr                :       0
radmacaccctrl                   :       disable
radauthlifetm                   :       900
radmacaddrformat                :       dashdelimited

RADIUS Accounting
=================
radaccstatus                    :       disable
radaccinactivetmr               :       5
```

Configure RADIUS Accounting server

```
[Device Name]>set radacctbl <index> status enable seraddrfmt
              <ipaddr or name> ipaddr <RADIUS IP address or
              name> port <user defined> ssecret <user
              defined> responsetm <1 to 4 seconds> maxretx <1
              to 10 times>
[Device Name]>show radacctbl
```

Figure 6-17: Results of “show radacctbl” CLI command

```
[Device Name]> show radacctbl
RADIUS Accounting Group Table

=======================
Index                    :              1
RADIUS Acc Server Status :        disable
IP Address/Host Name     :        0.0.0.0
Accounting Port          :           1813
Response Time            :              3
Shared Secret            :         ******
Server Addressing Format :         ipaddr
Maximum Retransmission   :              3

Index                    :              2
RADIUS Acc Server Status :        disable
IP Address/Host Name     :        0.0.0.0
Accounting Port          :           1813
Response Time            :              3
Shared Secret            :         ******
Server Addressing Format :         ipaddr
Maximum Retransmission   :              3
```

Configure the DNS Client

```
[Device Name]>set dnsstatus enable
[Device Name]>set dnsprisvripaddr <IP address of primary
              DNS server>
[Device Name]>set dnssecsvripaddr <IP address of secondary
              DNS server>
[Device Name]>set dnsdomainname <default domain name>
[Device Name]>show dns
```

Figure 6-18: Results of “show dns” CLI command

```
[Device Name]> show dns
DNS Client Group
================

dnsstatus       :       disable
dnsprisvripaddr :       0.0.0.0
dnssecsvripaddr :       0.0.0.0
dnsdomainname   :
```

Parameter Tables

Objects contain groups that contain both parameters and parameter tables.

Use the following Tables to configure the Access Point. Columns used on the tables include:

- Name - Parameter, Group, or Table Name
- Type - Data type
- Values - Value range, and default value, if any
- Access = access type, R = Read Only (show), RW = Read-Write (can be “set”), W = Write Only
- CLI Parameter - Parameter name as used in the Access Point

Access Point network objects are associated with Groups. The network objects are listed below and associated parameters are described in the following Parameter Tables:

- System Parameters - Access Point system information
  - Inventory Management Information - Hardware, firmware, and software version information
- Network Parameters - IP and Ethernet information
  - DHCP Server Parameters - Enable or disable dynamic host configuration
  - VLAN Parameters - Enable, disable, and configure VLAN

(Virtual LAN) settings

- Ethernet Interface Parameters - Set the speed and duplex of the Ethernet port

- Wireless Interface Parameters - Wireless card Information
- Wireless Distribution System (WDS) Parameters - Configure the WDS partnerships
- Security Parameters - Access Point security settings
  - Wireless Interface Security Parameters - Configure WEP encryption settings
  - Primary and Backup RADIUS Server Table Parameters - RADIUS Authentication and Accounting information
  - MAC Access Control Parameter - Control wireless access based on MAC address
- Management Parameters - Control access to the AP-3's management interfaces
  - SNMP Parameters - Set read and read/write passwords
  - IP Access Table Parameters - Configure range of IP addresses that can access the AP-3
  - SNMP Table Host Table Parameters - Enter the list of IP addresses that will receive alarms from the AP-3
  - Telnet Parameters - Telnet Port setup
  - Serial Port Parameters - Serial Port setup
  - TFTP Server Parameters - Set up for file transfers; specify IP Address, file name, and file type

- HTTP (web browser) Parameters - Set up the graphical web browser interface

- Advanced Parameters
  - Link Integrity Group - Monitor link status
  - Proxy ARP Parameters - Enable or disable proxy ARP for wireless clients
  - Ethernet Protocol Filtering Parameters - Control network traffic based on protocol type
  - Broadcast Filtering Table - Enable or disable proxy ARP for wireless clients
  - IP ARP Filtering Parameters - Control which ARP messages are sent to wireless clients based on IP settings
  - TCP/UDP Port Filtering - Filter IP packets based on TCP/UDP port
  - Syslog Parameters - Configure the AP-3 to send Syslog information to network servers
  - IAPP Parameters - Enable or disable the Inter-Access Point Protocol
  - SpectraLink VoIP Parameters - Enable or disable SpectraLink Voice over IP feature
- Bridging Parameters
  - Static MAC Address Filter Table - Enable and disable specific addresses
  - Spanning Tree Parameters - Used to help prevent network loops

- Storm Threshold Parameters - Set threshold for number of broadcast packets
- Intra BSS Subscriber Blocking - Enable or disable peer to peer traffic on the same AP
- Packet Forwarding Parameters - Redirect traffic from wireless clients to a specified MAC address

- CLI Monitoring Parameters - View AP-3 statistics

System Parameters

Name	Type	Values	Access	CLI Parameter
System	Group	N/A	R	system
Name	DisplayString	User Defined	RW	sysname
Location	DisplayString	User Defined	RW	sysloc
Contact Name	DisplayString	User Defined	RW	sysctname
Contact E-mail	DisplayString	User Defined	RW	sysctemail
Contact Phone	DisplayString	User Defined max 254 characters	RW	sysctphone
FLASH Backup Interval	Integer	0 - 65535 seconds	RW	sysflashbckint
Flash Update		0 1	RW	sysflashupdate
System OID	DisplayString	N/A	R	sysoid
Descriptor	DisplayString	System Name, flash version, S/N, bootloader version	R	sysdescr
Up Time	Integer	dd:hh:mm:ss dd – days hh – hours mm – minutes ss – seconds	R	sysuptime
Emergency Restore to defaults		Resets all parameters to default factory values	RW	sysresettodefaults Note: You must enter the following command twice to reset to defaults: **set sysresettodefaults 1**

Inventory Management Information

Name	Type	Values	Access	CLI Parameter
System Inventory Management	Subgroup	N/A	R	sysinvmgmt
Component Table	Subgroup	N/A	R	sysinvmgmtcmptbl
Component Interface Table	Subgroup	N/A	R	sysinvmgmtcmpiftbl

Note: The inventory management commands display advanced information about the AP-3's installed components. You may be asked to report this information to a technical representative if you contact customer support.

Network Parameters

Name	Type	Values	Access	CLI Parameter
Network	Group	N/A	R	network
IP Configuration	Group	N/A	R	ip (Note: The **network** and **ip** parameters display the same information)
IP Address	IpAddress	User Defined	RW	ipaddr
IP Mask	IpAddress	User Defined	RW	ipmask
Default Router IP Address	IpAddress	User Defined	RW	ipgw
Default TTL	Integer	User Defined 64 (default)	RW	ipttl
Address Type	Integer	static dynamic (default)	RW	ipaddrtype

Note: The IP Address Assignment Type (ipaddrtype) must be set to static before the IP Address (ipaddr), IP Mask (ipmask) or Default Gateway IP Address (ipgw) values can be entered.

DHCP Server Parameters

Name	Type	Values	Access	CLI Parameter
DHCP Server	Group	N/A	R	dhcp
DHCP Server Status	Integer	enable (1) (default) disable (2) delete (3)	RW	dhcpstatus
Gateway IP Address	IpAddress	User Defined	RW	dhcpgw
Primary DNS IP Address	IpAddress	User Defined	RW	dhcppridnsipaddr
Secondary DNS IP Address	IpAddress	User Defined	RW	dhcpsecdnsipaddr
Number of IP Pool Table Entries	Integer32	N/A	R	dhcpippooltblent

Note: The DHCP Server (dhcpstatus) can only be enabled after a DHCP IP Pool table entry has been created.

DHCP Server table for IP pools

Name	Type	Values	Access	CLI Parameter
DHCP Server IP Address Pool Table	Table	N/A	R	dhcpippooltbl
Table Index	Integer	User Defined	N/A	index
Start IP Address	IpAddress	User Defined	RW	startipaddr
End IP Address	IpAddress	User Defined	RW	endipaddr
Width	Integer	User Defined	RW	width
Default Lease Time (optional)	Integer32	> 0 86400 sec (default)	RW	defleasetm
Maximum Lease Time (optional)	Integer32	> 0 86400 sec (default)	RW	maxleasetm
Comment (optional)	DisplayString	User Defined	RW	cmt
Status (optional)	Integer	enable (1) disable (2) delete (3)	RW	status

Note: Set either End IP Address or Width (but not both) when creating an IP address pool.

VLAN Parameters

Name	Type	Values	Access	CLI Parameter
VLAN	Group	N/A	R	vlan
Status	Integer	enable disable (default)	RW	vlanstatus
Management ID	VlanId	0 (disable) or 1 – 4094	RW	vlanmgmtid

VLAN ID Table

Name	Type	Values	Access	CLI Parameter
VLAN ID Table	Table	N/A	R	vlanidtbl
Index	Integer32	1 (Wireless A) 2 (Wireless B)	R	index
Identifier (ID)	VlanId	0 (disable) or 1 – 4094	RW	id

Ethernet Interface Parameters

Name	Type	Values	Access	CLI Parameter
Ethernet Interface	Group	N/A	R	ethernet
Speed	Integer	10halfduplex 10fullduplex 10autoduplex 100halfduplex 100fullduplex autohalfduplex autoautoduplex (default)	RW	etherspeed
MAC Address	PhyAddress	N/A	R	ethermacaddr

Wireless Interface Parameters

Since the AP-3 devices support two PC Card slots, we differentiate the two cards by using the table index:

- Slot A = index 3
- Slot B = index 4

The wireless interface group parameter is **wif**, which displays the objects associated with both PC Cards A and B.

Wireless 802.11b Parameters

Name	Type	Values	Access	CLI Parameter
Wireless Interfaces	Group	N/A	R	wif
Network Name	DisplayString	1 – 31 characters My Wireless Network A (default) My Wireless Network B (default)	RW	netname
Distance between APs	Integer	large (default) medium small minicell microcell	RW	distaps
Auto Channel Select (ACS)	Integer	enable (default) disable	RW	autochannel
Interference Robustness	Integer	enable (default) disable	RW	interrobust
DTIM Period	Integer	1 – 65535 1 = default	RW	dtimperiod
Operating Frequency Channel	Integer	1 - 11 (FCC) (3 = default) 1 - 13 (ETSI) (3 = default) 1 - 14 (JP) (3 = default) 10 - 13 (FR) (10 = default)	RW	channel
RTS/CTS Medium Reservation	Integer	0 – 2347 Default is 2347 (off)	RW	medres
Multicast Rate	Integer	1 Mbit/sec (1) 2 Mbit/sec (2) (default) 5.5 Mbit/sec (3) 11 Mbit/sec (4)	RW	multrate

Name	Type	Values	Access	CLI Parameter
Closed Wireless System	Integer	enable disable (default)	RW	closedsys
Load Balancing	Integer	enable (default) disable	RW	ldbalance
Medium Distribution	Integer	enable (default) disable	RW	meddendistrib
MAC Address	PhyAddress	12 hex digits	R	macaddr
Supported Data Rates	Octet String	Reported in 500 Kb/ sec intervals: 2 (1 Mbit/sec) 4 (2 Mbit/sec) (default) 11 (5.5 Mbit/sec) 22 (11 Mbit/sec)	R	suppdatarates
Transmit Rate	Integer32	Reported in 500 Kb/ sec intervals: 0 (auto fallback) 2 (1 Mbit/sec) 4 (2 Mbit/sec) (default) 11 (5.5 Mbit/sec) 22 (11 Mbit/sec)	RW	txrate
Supported Frequency Channels	Octet String	Depends on Regulatory Domain	R	suppchannels
Physical Layer Type	Integer	dsss (direct sequence spread spectrum) for 802.11b	R	phytype
Regulatory Domain List	DisplayString	USA (FCC) Canada (DOC) Europe (ETSI) Spain (SP) France (FR) Japan (MKK)	R	regdomain

Note: There is an inter-dependent relationship between the Distance between APs and the Multicast Rate. In general, larger systems operate a lower average transmit rates.

Distance between APs	Multicast Rate
Large	1 and 2 Mbits/sec
Medium	1, 2, and 5.5 Mbits/sec
Small	1, 2, 5.5 and 11 Mbits/sec
Minicell	1, 2, 5.5 and 11 Mbits/sec
Microcell	1, 2, 5.5 and 11 Mbits/sec

Wireless 802.11a Parameters

Name	Type	Values	Access	CLI Parameter
Wireless Interfaces	Group	N/A	R	wif
Network Name	DisplayString	2 – 31 characters My Wireless Network A (default) My Wireless Network B (default)	RW	netname
Auto Channel Select (ACS)	Integer	enable (default) disable	RW	autochannel
DTIM Period	Integer	1 – 65535 (1 = default)	RW	dtimperiod

Name	Type	Values	Access	CLI Parameter
Operating Frequency Channel	Integer	36 - 5.180 GHz 40 - 5.200 GHz 44 - 5.220 GHz 48 - 5.240 GHz 52 - 5.260 GHz (default FCC) 56 - 5.280 GHz 60 - 5.300 GHz 64 - 5.320 GHz Channels 36-64 are valid for the FCC and ETSI regulatory domains. For Turbo mode (not available in all countries), the following channels are available: 42 - 5.21 GHz 50 - 5.25 GHz 58 - 5.29 GHz The following channels are available in Japan: 34 - 5.170 GHz (default) 38 - 5.190 GHz 42 - 5.210 GHz 46 - 5.230 GHz	RW	channel
RTS/CTS Medium Reservation	Integer	0 – 2347 Default is 2347 (off)	RW	medres
MAC Address	PhyAddress	12 hex digits	R	macaddr
Turbo Mode (not available in all countries)	Integer	enable disable (default)	RW	turbo
Supported Data Rates	Octet String	See “Transmit Rate”	R	suppdatarates

Name	Type	Values	Access	CLI Parameter
Transmit Rate	Integer32	Reported in 500 Kb/ sec intervals: 0 - Auto Fallback (default) 12 (6 Mbit/sec) 18 (9 Mbits/sec) 24 (12 Mbits/sec) 36 (18 Mbits/sec) 48 (24 Mbits/sec) 72 (36 Mbits/sec) 96 (48 Mbits/sec) 108 (54 Mbits/sec) For Turbo mode (not available in all countries): 0 - Auto Fallback (default) 24 (12 Mbit/sec) 38 (18 Mbits/sec) 48 (24 Mbits/sec) 72 (36 Mbits/sec) 96 (48 Mbits/sec) 144 (72 Mbits/sec) 192 (96 Mbits/sec) 216 (108 Mbits/sec)	RW	txrate
Supported Frequency Channels	Octet String	See Operating Frequency Channel	R	suppchannels
Physical Layer Type	Integer	ofdm (orthogonal frequency division multiplexing) for 802.11a	R	phytype
Regulatory Domain List	DisplayString	USA (FCC) Canada (DOC) Europe (ETSI) Spain (SP) France (FR) Japan (MKK)	R	regdomain

Note: For 802.11a cards in Europe, Auto Channel Select is a read-only parameter; it is always enabled.

Wireless Distribution System (WDS) Parameters

Note: These parameters only apply to 802.11b radios.

Name	Type	Values	Access	CLI Parameter
WDS Table	Table	N/A	R	wdstbl
Port Index	Integer	3.1 - 3.6 (Wireless A) 4.1 - 4.6 (Wireless B)	R	portindex
Status	Integer	enable (1) disable (2) (default)	RW	status
Partner MAC Address	PhysAddress	User Defined	RW	partnermacaddr

Security Parameters

Name	Type	Values	Access	CLI Parameter
Security	Group	N/A	R	security
Configuration Mode	Integer	none 802.1x mixed	RW	secconfig
Re-keying Interval	Integer	60 – 65535 seconds default is 900 sec	RW	secrekeyint

Wireless Interface Security Parameters

The following table details the WEP encryption parameters for the AP-3. This information applies to both the 802.11a and the 802.11b wireless interfaces.

Name	Type	Values	Access	CLI Parameter
Wireless Interfaces Security	Group		R	wifsec
Encryption Status	Integer	enable disable	RW	encryptstatus
Index	Integer	3 = PC Card A 4 = PC Card B	N/A	N/A
Encryption Key 1	DisplayString	User Defined	W	encryptkey1
Encryption Key 2	DisplayString	User Defined	W	encryptkey2
Encryption Key 3	DisplayString	User Defined	W	encryptkey3
Encryption Key 4	DisplayString	User Defined	W	encryptkey4
Deny non-encrypted Data	Integer	enable (default) disable	RW	encryptdeny

Data Transmission Encryption Key	Integer	1 (default) 2 3 4	RW	encryptkeytx

Security Encryption Key Length Table

The following table details how to set the Encryption Key Length for the wireless interfaces.

Name	Type	Values	Access	CLI Parameter
Security Encryption Key Length Table	Table	N/A	R	secenckeylentbl
Index	Integer	3 = PC Card A 4 = PC Card B	N/A	index
Encryption Key Length	Integer	64 bit 128 bit 152 bit	RW	enckeylen

Note: The available Encryption Key Lengths vary based on card type. Depending on the model, 802.11b cards support 64 (also referred to as 40) bits or 128 (also referred to as 104) bits. 802.11a cards support 64 (also referred to as 40), 128 (also referred to as 104), or 152 (also referred to as 128) bits.

Primary and Backup RADIUS Server Table Parameters

Avaya Wireless devices that use RADIUS authentication and/or accounting support both primary and backup RADIUS servers. The configuration parameters and statistics are the same for both primary and backup servers. The CLI differentiates the primary and backup RADIUS parameters by using the table index.

General RADIUS Parameters

Name	Type	Values	Access	CLI Parameter
RADIUS	Group	N/A	R	radius
MAC Access Control Status	Integer	enable disable (disable)	R	radmacacctrl
Authorization Lifetime	Integer32	60 – 43200 seconds (in 60 sec increments) 900 sec. (default)	RW	radauthlifetm
MAC Address Format	Integer	dashdelimited (default) colondelimited singledashdelimited no delimiter	RW	radmacaddrformat
RADIUS Accounting Status	Integer	enable disable	RW	radaccstatus
Accounting Inactivity Timer	Integer32	0 – 2147483647 minutes; default is 5 min.	RW	radaccinactivetmr

RADIUS Authentication

Name	Type	Values	Access	CLI Parameter
RADIUS Authentication	Table	N/A	R	radiustbl
Primary RADIUS	N/A	N/A	R	(index) 1
Backup RADIUS	N/A	N/A	R	(index) 2
RADIUS Server Status	Integer	enable disable (default)	RW	status
Server Addressing Format (see note)	Integer	ipaddr (default) name	RW	seraddrfmt
Server IP Address or Name	IpAddress DisplayString	User Defined (enter an IP address if seraddrfmt is ipaddr or a name if set to name)	RW	ipaddr
Port (optional)	Integer	User Defined 1812 (default)	RW	port
Shared Secret	DisplayString	User Defined max 63 characters	W	ssecret
Response Time (sec)	Integer	1 – 4 seconds 3 sec (default)	RW	responsetm
Maximum Retransmissions (optional)	Integer	1 – 10 3 (default)	RW	maxretx

Note: Use a server name only if you have enabled the DNS Client functionality. See RADIUS DNS Host Name Support.

RADIUS Accounting

Name	Type	Values	Access	CLI Parameter
RADIUS Accounting	Table	N/A	R	radacctbl
Primary RADIUS	N/A	N/A	R	(index) 1
Backup RADIUS	N/A	N/A	R	(index) 2
RADIUS Server Status	Integer	enable disable (default)	RW	status
Server Addressing Format (see note)	Integer	ipaddr (default) name	RW	seraddrfmt
Server IP Address or Name	IpAddress Display String	User Defined (enter an IP address if seraddrfmt is ipaddr or a name if set to name)	RW	ipaddr
Port (optional)	Integer	User Defined 1813 (default)	RW	port
Shared Secret	DisplayString	User Defined max 63 characters	W	ssecret
Response Time (sec)	Integer	1 – 4 seconds 3 sec (default)	RW	responsetm
Maximum Retransmissions (optional)	Integer	1 – 10 3 (default)	RW	maxretx

Note: Use a server name only if you have enabled the DNS Client functionality. See RADIUS DNS Host Name Support.

DNS Client for RADIUS Name Resolution

Name	Type	Values	Access	CLI Parameter
DNS Client	Group	N/A	R	dns
DNS Client status	Integer	enable disable (default)	RW	dnsstatus
Primary DNS Server IP Address	IpAddress	User Defined	RW	dnspridnsipaddr
Secondary DNS Server IP Address	IpAddress	User Defined	RW	dnssecdnsipaddr
Default Domain Name	Integer32	User Defined	RW	dnsdomainname

MAC Access Control Parameter

Name	Type	Values	Access	CLI Parameter
MAC Address Control	Group	N/A	R	macacl
Status	Integer	enable disable	RW	macaclstatus
Operation Type	Integer	passthru block	RW	macacloptype

MAC Access Control Table

Name	Type	Values	Access	CLI Parameter
MAC Address Control Table	Table	N/A	R	macacltbl
Table Index	N/A	N/A	R	index
MAC Address	PhysAddress	User Defined	RW	macaddr
Comment (optional)	DisplayString	User Defined max 254 characters	RW	cmt
Status (optional)	Integer	enable (default) disable	RW	status

Management Parameters

SNMP Parameters

Name	Type	Values	Access	CLI Parameter
SNMP	Group	N/A	R	snmp
SNMP Management Interface Bitmask	Interface Bitmask	0 - no interfaces (disable) 1 - Ethernet 4 - Wireless A 8- Wireless B 15 - all interfaces	RW	snmpifbitmask
Read Password	DisplayString	User Defined public (default) max 63 characters	W	snmprpasswd
Read/Write Password	DisplayString	User Defined public (default) max 63 characters	W	snmprwpasswd
SNMP Trap Host Table	N/A	N/A	R	snmptraphosttbl

IP Access Table Parameters

When creating table entries, you may either specify the argument name followed by argument value or simply entering the argument value. When only the argument value is specified, then enter the values in the order depicted by the following table. CLI applies default values to the omitted arguments. Due to the nature of the information, the only argument that can be omitted is the “comment” argument.

Name	Type	Values	Access	CLI Parameter
IP Access Table	Table	N/A	R	mgmtipaccesstbl
Table Index	Integer	User Defined	N/A	index
IP Address	IpAddress	User Defined	RW	ipaddr
IP Mask	IpAddress	User Defined	RW	ipmask
Comment (optional)	DisplayString	User Defined	RW	cmt
Status (optional)	Integer	enable disable delete	RW	status

SNMP Table Host Table Parameters

When creating table entries, you may either specifying the argument name followed by argument value. CLI applies default values to the omitted arguments. Due to the nature of the information, the only argument that can be omitted is the “comment” argument.

Name	Type	Values	Access	CLI Parameter
SNMP Trap Host Table	Table	N/A	R	snmptraphosttbl
Table Index	Integer	User Defined	N/A	index
IP Address	IpAddress	User Defined	RW	ipaddr
Password	DisplayString	User Defined	W	passwd
Comment (optional)	DisplayString	User Defined	RW	cmt
Status (optional)	Integer	enable disable delete	RW	status

Telnet Parameters

Name	Type	Values	Access	CLI Parameter
Telnet	Group	N/A	R	telnet
Telnet Management Interface Bitmask	Interface Bitmask	0 - no interfaces (disable) 1 - Ethernet 4 - Wireless A 8- Wireless B 15 - all interfaces	RW	telifbitmask
Telnet Port	Integer	User Defined 23 (default)	RW	telport
Telnet Login Inactivity Time-out	Integer	1 – 60 seconds 30 sec (default)	RW	tellogintout
Telnet Session Idle Time-out	Integer	1 - 900 seconds 900 sec (default)	RW	telsessiontout

Serial Port Parameters

Name	Type	Values	Access	CLI Parameter
Serial	Group	N/A	R	serial
Baud Rate	Integer	2400, 4800, 9600 (default), 19200, 38400, 57600	RW	serbaudrate
Data Bits	Integer	8	R	serdatabits
Parity	Integer	none	R	serparity
Stop Bits	Integer	1	R	serstopbits
Flow Control	Value	none (default) xon/xoff	RW	serflowctrl

TFTP Server Parameters

These parameters relate to upload and download commands.

When a user executes an upload and/or download Command, the specified arguments are stored in TFTP parameters for future use. If nothing is specified in the command line when issuing subsequent upload and/or download commands, the stored arguments are used.

Name	Type	Values	Access	CLI Parameter
TFTP	Group	N/A	R	tftp
TFTP Server IP Address	IpAddress	User Defined	RW	tftpipaddr
TFTP File Name	DisplayString	User Defined	RW	tftpfilename
TFTP File Type	Integer	img config bootloader	RW	tftpfiletype

HTTP (web browser) Parameters

Name	Type	Values	Access	CLI Parameter
HTTP	Group	N/A	R	http
HTTP Management Interface Bitmask	Interface Bitmask	0 - no interfaces (disable) 1 - Ethernet 4 - Wireless A 8- Wireless B 15 - all interfaces	RW	httpifbitmask
HTTP Password	DisplayString	User Defined max 64 characters	W	httppasswd

HTTP Port	Integer	User Defined Default = 80	RW	httpport
Help Link	DisplayString	User Defined	RW	httphelplink

Advanced Parameters

Link Integrity Group

Name	Type	Values	Access	CLI Parameter
Link Integrity	Group	N/A	R	linkint
Link Integrity Status	Integer	enable (default) disable	RW	linkintstatus
Link Integrity Poll Interval	Integer	500 - 15000 ms (in increments of 500ms) 500 ms (default)	RW	linkintpollint
Link Integrity Poll Retransmissions	Integer	0 - 65535 5 (default)	RW	linkintpollretx
Link Integrity IP Target Table	N/A	N/A	R	linkinttbl

Link Integrity IP Target Table

Name	Type	Values	Access	CLI Parameter
Link Integrity IP Target Table	Table	N/A	R	linkinttbl
Table Index	Integer	User Defined	N/A	index
Target IP Address	IpAddress	User Defined	RW	ipaddr
Comment (optional)	DisplayString	User Defined	RW	cmt
Status (optional)	Integer	enable disable delete	RW	status

Proxy ARP Parameters

Name	Type	Values	Access	CLI Parameter
Proxy ARP	Group	N/A	R	parp
Status	Integer	enable disable	RW	parpstatus

Ethernet Protocol Filtering Parameters

Name	Type	Values	Access	CLI Parameter
Ethernet Filtering	Group	N/A	R	etherflt
Filtering Interface Bitmask	Interface Bitmask	0 - no interfaces (disable) 1 - Ethernet 4 - Wireless A 8- Wireless B 15 - all interfaces (default)	RW	etherfltifbitmask
Operation Type		passthru block	RW	etherfltoptype

Ethernet Filtering Table

Identify the different filters by using the table index.

Name	Type	Values	Access	CLI Parameter
Ethernet Filtering Table	Table	N/A	R	etherflttbl
Table Index	N/A	N/A	R	index
Protocol Number	Octet String	N/A	RW	protonumber
Protocol Name (optional)	DisplayString		RW	protoname
Filter Comment	DisplayString	2- 31 characters	RW	cmt
Status (optional)	Integer	enable (1) disable (2) delete (3)	RW	status

Note: The filter Operation Type (passthru or block) applies **only** to the protocol filters that are **enabled** in this table.

Broadcast Filtering Table

Name	Type	Values	Access	CLI Parameter
Broadcast Filtering Table	Table	N/A	R	broadcastflttbl
Index	Integer	N/A	N/A	index
Protocol Name	DisplayString	N/A	R	protoname
Direction	Integer	ethertowireless wirelesstoether both	RW	direction
Status	Integer	enable disable delete	RW	status

IP ARP Filtering Parameters

Name	Type	Values	Access	CLI Parameter
IP ARP Filtering	Group	N/A	R	iparp
Status	Integer	enable disable	RW	iparpfltstatus
IP Address	IpAddress	User Defined	RW	iparpfltipaddr
Subnet Mask	IpAddress	User Defined	RW	iparpfltsubmask

TCP/UDP Port Filtering

The following parameters are used to enable/disable the Port filter feature.

Name	Type	Values	Access	CLI
Port Filtering	Group	N/A	R	portflt
Port Filter Status	Integer	enable (default) disable	RW	portfltstatus

The following parameters are used to configure TCP/UDP Port filters.

Name	Type	Values	Access	CLI
Port Filtering Table	Table	N/A	R	portflttbl
Table Index	N/A	User Defined (there are also 4 pre-defined indices, see “Port Number” below for more information)	R	index
Port Type	Octet String	TCP UDP TCP/UDP	RW	porttype
Port Number	Octet String	User Defined (there are also 4 pre-defined protocols: NetBios Name Service – 137, NetBios Datagram Service – 138, NetBios Session Service – 139, SNMP Service – 161)	RW	portnum
Protocol Name	DisplayString	User Defined (there are also 4 pre-defined protocols, see ”Port Number” above)	RW	protoname

Interface Bitmask	Integer32	1 (Ethernet only) 4 (Slot A only) 5 (Slot A & Ether) 8 (Slot B only) 9 (Slot B & Ether) 12 (Slot A & B) 15 (All interfaces)	RW	ifbitmask
Status	Integer	enable (1) disable (2) delete (3)	RW	status

Syslog Parameters

The following parameters configure the Syslog settings.

Name	Type	Values	Access	CLI
Syslog	Group	N/A	R	syslog
Syslog Status	Integer	enable disable (default)	RW	syslogstatus
Syslog Port	Octet String	514	R	syslogport
Syslog Lowest Priority Logged	Integer	1 – 7 1 = LOG_ALERT 2 = LOG_CRIT 3 = LOG_ERR 4 = LOG_WARNING 5 = LOG_NOTICE 6 = LOG_INFO (default) 7 = LOG_DEBUG	RW	syslogpritolog
Heartbeat Status	Integer	enable (1) disable (2) (default)	RW	heartbeatstatus
Heartbeat Interval (seconds)	Integer	1 – 604800 seconds; 900 sec. (default)	RW	heartbeatinterval

Note: The Heartbeat parameters are advanced settings not available via the HTTP interface. When Heartbeat is enabled, the AP-3 periodically sends a message to the Syslog server to indicate that it is active. The frequency with which the heartbeat message is sent depends upon the setting of the Heartbeat Interval.

Syslog Host Table

The table described below configures the Syslog hosts that will receive message from the AP-3. You can configure up to ten Syslog hosts. Note that you can only configure one Syslog host via the HTTP interface (row 1, which defaults to 10.0.0.2).

Name	Type	Values	Access	CLI Parameter
Syslog Host Table	Table	N/A	R	sysloghosttbl
Table Index	Integer	1 – 10	N/A	index
IP Address	IpAddress	User Defined	RW	ipaddr
Comment (optional)	DisplayString	User Defined	RW	cmt
Status (optional)	Integer	enable disable delete	RW	status

IAPP Parameters

Name	Type	Values	Access	CLI Parameter
IAPP	Group	N/A	R	iapp
IAPP Status	Integer	enable (default) disable	RW	iappstatus

Periodic Announce Interval (seconds)	Integer	80 120 (default) 160 200	RW	iappannint
Announce Response Time	Integer	2 seconds	R	iappannresp
Handover Time-out	Integer	410 ms 512 ms (default) 614 ms 717 ms 819 ms	RW	iapphandtout
Max. Handover Retransmissions	Integer	1 - 10 (default 4)	RW	iapphandretx
Send Announce Request on Startup	Integer	enable (default) disable	RW	iappannreqstart

Note: These parameters configure the Inter Access Point Protocol (IAPP) for roaming. Leave these settings at their default value unless a technical representative asks you to change them.

SpectraLink VoIP Parameters

Name	Type	Values	Access	CLI Parameter
Spectralink VoIP	Group	N/A	R	spectralink
Spectralink VoIP Status	Integer	enable disable (default)	RW	speclinkstatus

Bridging Parameters

Static MAC Address Filter Table

Name	Type	Values	Access	CLI Parameter
Static MAC Address Filter Table	Table	N/A	R	staticmactbl
Table Index	N/A	N/A	R	index
Static MAC Address on Wired Network	PhysAddress	User Defined	RW	wiredmacaddr
Static MAC Address Mask on Wired Network	PhysAddress	User Defined	RW	wiredmask
Static MAC Address on Wireless Network	PhysAddress	User Defined	RW	wirelessmacaddr
Static MAC Address Mask on Wireless Network	PhysAddress	User Defined	RW	wirelessmask
Comment (optional)	DisplayString	max 255 characters	RW	cmt
Status (optional)	Integer	enable (default) disable delete	RW	status

Spanning Tree Parameters

Name	Type	Values	Access	CLI Parameter
Spanning Tree	Group	N/A	R	stp
Spanning Tree Status	Integer	enable disable (default)	RW	stpstatus
Bridge Priority	Integer	0 – 65535 32768 (default)	RW	stppriority

Maximum Age	Integer	600 – 4000 (in 0.01 sec intervals; i.e., 6 to 40 seconds) 2000 (default)	RW	stpmaxage
Hello Time	Integer	100 – 1000 (in 0.01 sec intervals; i.e., 1 to 10 seconds) 200 (default)	RW	stphellotime
Forward Delay	Integer	400 – 3000 (in 0.01 sec intervals; i.e., 4 to 30 seconds) 1500 (default)	RW	stpfwddelay

Spanning Tree Priority and Path Cost for Each Interface

Name	Type	Values	Access	CLI Parameter
Spanning Tree Table	Table	N/A	R	stpbl
Table Index (Port)	N/A	1 – 15	R	index
Priority	Integer	0 – 255 128 (default)	RW	priority
Path Cost	Integer	1 – 65535 100 (default)	RW	pathcost
State	Integer	disable blocking listening learning forwarding broken	R	state
Status	Integer	enable disable	RW	status

Storm Threshold Parameters

Name	Type	Values	Access	CLI Parameter
Storm Threshold	Group	N/A	N/A	stmthres
Broadcast Threshold	Integer	0 – 255 packets/sec	RW	stmbrdthres
Multicast Threshold	Integer	0 – 255 packets/sec	RW	stmmultithres

Storm Threshold Table

Name	Type	Values	Access	CLI Parameter
Storm Threshold Table	Table	N/A	R	stmthrestbl
Table Index	Integer	1 = Ethernet 2 = PC Card A 3 = PC Card B	R	index
Broadcast Threshold	Integer	0 – 255 packets/sec	RW	bcast
Multicast Threshold	Integer	0 – 255 packets/sec	RW	mcast

Intra BSS Subscriber Blocking

The following parameters control the Intra BSS traffic feature, which prevent wireless clients that are associated with the same AP-3 from communicating with each other:

Name	Type	Values	Access	CLI
Intra BSS Traffic	Group	N/A	R	intrabss
Intra BSS Traffic Operation	Integer	passthru block	RW	intrabssoptype

Packet Forwarding Parameters

The following parameters control the Packet Forwarding feature, which redirects wireless traffic to a specific MAC address:

Name	Type	Values	Access	CLI
Packet Forwarding MAC Address	Group	N/A	R	pktfwd
Packet Forwarding MAC Address	MacAddress	User Defined	RW	pktfwdmacaddr
Packet Forwarding Status	Integer	enable disable (default)	RW	pktfwdstatus
Packet Forwarding Interface Port	Integer	0 (any) 1 (Ethernet) 3 (Slot A WDS 1) 4 (A WDS 2) 5 (A WDS 3) 6 (A WDS 4) 7 (A WDS 5) 8 (A WDS 6) 10 (Slot B WDS 1) 11 (B WDS 2) 12 (B WDS 3) 13 (B WDS 4) 14 (B WDS 5) 15 (B WDS 6)	RW	pktfwdif

CLI Monitoring Parameters

Using the “show” command with the following table parameters will display operating statistics for the AP-3 (these are the same statistics that are described in Monitoring Network Statistics for the HTTP Web interface).

- **staticmp.** Displays the ICMP Statistics.
- **statarptbl.** Displays the IP ARP Table Statistics.
- **statbridgetbl.** Displays the Learn Table.
- **statiapp.** Displays the IAPP Statistics.
- **statradius.** Displays the RADIUS Authentication Statistics.
- **statif.** Displays information and statistics about the Ethernet and wireless interfaces.
- **stat802.11.** Displays additional statistics for the wireless interfaces.
- **statethernet.** Displays additional statistics for the Ethernet interface.

Record Configuration Settings

A

It is recommended that you keep a copy of the configuration settings for each of the AP-3 devices in your network. The information below is hard-coded in your system and can be viewed from the Web Interface pages by clicking the Configure button and viewing the System and Interfaces screens.

MAC Address of the AP-3 unit	
AP software image version	
BSP/Bootloader firmware version	
Hardware revision level	
MAC Address of the PC Card in Slot A	
Driver version of the PC Card in Slot A	
MAC Address of the PC Card in Slot B	
Driver version of the PC Card in Slot B	

In the web interface, click the **Monitor** button and select the **Version** tab. The table displays the Object ID and version numbers for each piece of hardware. For the **Hardware Inventory**, the following information may be useful when contacting Technical Support:

Type	Object ID
AP-3 with Mini-DIN8 serial port adapter	97
AP-3 converted to AS-I with Mini-DIN8 serial port adapter	96

Use the following pages to document your configuration. You can use this information to easily recover your network settings if necessary.

Configuration Settings

In the table below, record the configuration settings for each of your AP-3 units. The shaded cells indicate the location of the parameters within the HTTP web interface. The first column in the table indicates the parameter name, the second column indicates the default value of each parameter (when applicable). Use the third column to record your settings. The last column is an aide which indicates the CLI command syntax required to define the configuration parameters in case you need to re-enter data through the Command Line Interface.

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
System Parameters			> show system
Name	AP-3		> set sysname <System Name>
Location			> set sysloc “Unit Location”
Contact Name			> set sysctname “Contact Name”
Contact E-mail			> set sysctnemail “name@organization.com”
Contact Phone			> set sysctphone “Contact Phone Number”
Network Parameters - IP Configuration			> show network OR > show ip
IP Address Assignment Type	dynamic (DHCP)		> set ipaddrtype <static, dynamic> **NOTE:** If the IP Address Assignment type is set to dynamic, no other information is required. The AP-3 device will act as a DHCP client to the server in your network.
IP Address (static)	10.0.0.1		> set ipaddr <IP Address>
IP Mask	255.0.0.0		> set ipsubmask <IP Mask IP Address>

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
Default Router IP Address (Gateway IP Address)	10.0.0.1		> set ipgw <Default Gateway IP Address>
Default TTL (Time to Live)	64		> set ipttl <number of hops to destination>
Network Parameters - DHCP Server			> show dhcp
DHCP Server Status	disable (2)		> set dhcpstatus <enable, disable, delete>
Gateway IP Address			> set dhcpgw <Default Gateway IP Address>
Primary DNS IP Address			> set dhcppridnsipaddr <DNS Server IP Address>
Secondary DNS IP Address			> set dhcpsecdnsipaddr <DNS Server IP Address>
Network Parameters - DHCP Server - IP Pool Table			> show dhcpippooltbl
Start IP Address			> set dhcpippooltbl <index> startipaddr <Starting IP Address in the Range>
End IP Address			> set dhcpippooltbl <index> endipaddr <Ending IP Address in the Range>
Default Lease Time	86400	(sec)	> set dhcpippooltbl <index> defleasetm <Time in Seconds>
Maximum Lease Time	86400	(sec)	> set dhcpippooltbl <index> maxleasetm <Time in Seconds>
Comment (optional)			> set dhcpippooltbl <index> cmt "Optional Comment"
Status	disable (2)		> set dhcpippooltbl <index> status <enable, disable, delete>
Network Parameters - Link Intergrity			> show linkint
Link Integrity Status	disable (2)		> set linkintstatus <enable, disable>
Poll Interval	500	(sec)	> set linkintpollint <Time in Seconds>
Poll Retransmissions	5		> set linkintpollretx <Number of Times to Retransmit>

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
Network Parameters - Link Intergrity - Target IP Address Table			> show linkinttbl
Target IP Address	0.0.0.0		> set linkinttbl <index> addr
Comment (optional)			> set linkinttbl <index> cmt <Optional Comment>
Status	disable (2)		> set linkinttbl <index> status <enable, disable>
Network Parameters - VLAN			> show vlan
Status	disable		> set vlanstatus <enable, disable>
Management ID			> set vlanmgmtid <VLAN ID for AP-3 device 1 - 4094; 0=disabled>
Network Parameters - VLAN ID Table			> show vlanidtbl
VLAN ID (wireless interfaces)			> set <index> id <VLAN ID 1 - 4094; 0=disabled>
Interfaces Parameters - Wireless Slot A with 5 GHz (802.11a) card			> show wif
Physical Layer Type	OFDM		> show wif
Network Name	My Wireless Network A		> set wif 3 netname “Network Name for PC Card in Slot A”
Auto Channel Select	enable		>set wif 3 autoselect <enable, disable> (Not configurable in Europe)
Frequency Channel	US/CAN: 52 - 5260 MHz Japan: 34 - 5170 ETSI: varies	MHz	> show wif > set wif 3 channel <for FCC and ETSI regulatory domains: 36, 40, 44, 48, 52, 56, 60, 64 - in Japan: 34, 38, 42, 46 - in Turbo mode (not available in all countries): 42, 50, 58>
RTS/CTS Medium Reservation	2347 (off)		> set wif 3 medres <0 - 2347 (2347=off)>

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
DTIM Period	1		> set wif 3 dtimperiod <1 - 65355>
Transmit Rate	0 - Auto Fallback	(Mbits/s)	> show wif > set wif 3 txrate <0 (auto), 12, 18, 24, 36, 48, 72, 96, 108 or 0, 24, 36, 48, 72, 96, 144, 192, 216 in Turbo> (Reported in 500 Kb/sec increments so each value is twice the Mb/sec number)
Turbo Mode	disabled		> set turbo <enable, disable>
Interfaces Parameters - Wireless Slot A with 2.4 GHz (802.11b) card			> show wif
Physical Layer Type	DSSS		> show wif
Network Name	My Wireless Network A		> set wif 3 netname "Network Name for PC Card in Slot A"
Auto Channel Select	enable		>set wif 3 autoselect <enable, disable> **NOTE:** When setting up WDS, Auto Channel Select **must** be disabled.
Frequency Channel	3 - 2422 MHz 11 - 2462 MHz (France)	MHz	> show wif > set wif 3 channel <Frequency Channel> **NOTE:** When setting up WDS, Auto Channel Select **must** be disabled.
RTS/CTS Medium Reservation	2347 (off)		> set wif 3 medres <0 - 2347 (2347=off)>
Interference Robustness	enable		>set wif 3 interrobust <enable, disable>
DTIM Period	1		> set wif 3 dtimperiod <1 - 65355>
Closed System	disable		>set wif 3 closedsys <enable, disable>
Load Balancing	enable		> set wif 3 ldbalancing <enable, disable>

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
Distance Between APs	Large		> set wif 3 distaps <Large, Medium, Small, Minicell, Microcell> **NOTE:** The Distance between APs and the Multicast Rate are inter-dependent. As you increase the distance between APs, the Multicast rate drops.
Multicast Rate	2 Mbits/s	(Mbits/s)	> show wif > set wif 3 multrate <1, 2, 5.5, 11>
Interfaces Parameters - Wireless Slot A with 2.4 GHz (802.11b) card- Wireless Distribution System			> show wdstbl 3
			When setting up WDS, Auto Channel Select **must** be disabled. **NOTE:** The WDS table index uses two digits - the first represent the wireless interface card (3 = Slot A and 4 = Slot B), the second digit represents the channel numbers 1-6.
1.Partner MAC Address	00.00.00. 00.00.00		> set wdstbl 3.1 partnermacaddr <MAC Address>
Status	disable		> set wdstbl 3.1 status <1=enable, 2=disable> OR > set wdstbl 3.1 <enable, disable>
2.Partner MAC Address	00.00.00. 00.00.00		> set wdstbl 3.2 partnermacaddr <MAC Address>
Status	disable		> set wdstbl 3.2 status <1=enable, 2=disable> OR > set wdstbl 3.2 <enable, disable>
3.Partner MAC Address	00.00.00. 00.00.00		> set wdstbl 3.3 partnermacaddr <MAC Address>
Status	disable		> set wdstbl 3.3 status <1=enable, 2=disable> OR > set wdstbl 3.3 <enable, disable>

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
4.Partner MAC Address	00.00.00. 00.00.00		> set wdstbl 3.4 partnermacaddr <MAC Address>
Status	disable		> set wdstbl 3.4 status <1=enable, 2=disable> OR > set wdstbl 3.4 <enable, disable>
5.Partner MAC Address	0.0.0.0		> set wdstbl 3.5 partnermacaddr <MAC Address>
Status	disable		> set wdstbl 3.5 status <1=enable, 2=disable> OR > set wdstbl 3.5 <enable, disable>
6.Partner MAC Address	0.0.0.0		> set wdstbl 3.6 partnermacaddr <MAC Address>
Status	disable		> set wdstbl 3.6 status <1=enable, 2=disable> OR > set wdstbl 3.6 <enable, disable>
Interfaces Parameters - Wireless Slot B with 5 GHz (802.11a) card			> show wif
Physical Layer Type	OFDM		> show wif
Network Name	My Wireless Network A		> set wif 4 netname "Network Name for PC Card in Slot A"
Auto Channel Select	enable		>set wif 4 autochannel <enable, disable> (Not configurable in Europe)
Frequency Channel	52 - 5260 MHz	MHz	> show wif > set wif 4 channel <for FCC and ETSI regulatory domains: 36, 40, 44, 48, 52, 56, 60, 64 - in Japan: 34, 38, 42, 46 - in Turbo mode (not available in all countries): 42, 50, 58>
RTS/CTS Medium Reservation	2347 (off)		> set wif 4 medres <0 - 2347 (2347=off)>
DTIM Period	1		> set wif 4 dtimperiod <1 - 65355>

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
Transmit Rate	0 - Auto Fallback	(Mbits/s)	> show wif > set wif 4 txrate <0 (auto), 12, 18, 24, 36, 48, 72, 96, 108 or 0, 24, 36, 48, 72, 96, 144, 192, 216 in Turbo> (Reported in 500 Kb/sec increments so each value is twice the Mb/sec number)
Turbo Mode	disabled		> set wif <index> turbo <enable, disable>
Interfaces Parameters - Wireless Slot B with 2.4 GHz (802.11b) card			> show wif
Physical Layer Type	DSSS		> show wif
Network Name	My Wireless Network B		> set wif 4 netname "Network Name for PC Card in Slot A"
Auto Channel Select	enable		> set wif 4 autochannel <enable, disable> **NOTE:** When setting up WDS, Auto Channel Select **must** be disabled.
Frequency Channel	3 - 2422 MHz 11 - 2462 MHz (France)	MHz	> show wif > set wif 4 channel <Frequency Channel>
RTS/CTS Medium Reservation	2347 (off)		> set wif 4 medres <0 - 2347 (2347=off)>
Interference Robustness	enable		>set wif 4 interrobust <enable, disable)
DTIM Period	1		> set wif 4 dtimperiod <1 - 65535>
Closed System	disable		>set wif 4 closedsys <enable, disable>
Load Balancing	enable		> set wif 4 ldbalance <enable, disable>
Distance Between APs	Large		> set wif 4 distaps <large, medium, small, minicell, microcell> **NOTE:** The Distance between APs and the Multicast Rate are inter-dependent. As you increase the distance between APs, the Multicast rate drops.

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
Multicast Rate	2 Mbits/s	(Mbits/s)	> show wif > set wif 4 multrate <1, 2, 5.5, 11>
Interfaces Parameters - Wireless Slot B with 2.4 GHz (802.11b) card - Wireless Distribution System			> show wdstbl 4
			NOTE: When setting up WDS, Auto Channel Select **must** be disabled. The WDS table index uses two digits - the first represent the wireless interface card (3 = Slot A and 4 = Slot B), the second digit represents the channel numbers 1-6.
1.Partner MAC Address	00.00.00. 00.00.00		> set wdstbl 4.1 partnermacaddr <MAC Address>
Status	disable		> set wdstbl 4.1 status <1=enable, 2=disable> OR > set wdstbl 4.1 <enable, disable>
2.Partner MAC Address	00.00.00. 00.00.00		> set wdstbl 4.2 partnermacaddr <MAC Address>
Status	disable		> set wdstbl 4.2 status <1=enable, 2=disable> OR > set wdstbl 4.2 <enable, disable>
3.Partner MAC Address	00.00.00. 00.00.00		> set wdstbl 4.3 partnermacaddr <MAC Address>
Status	disable		> set wdstbl 4.3 status <1=enable, 2=disable> OR > set wdstbl 4.3 <enable, disable>
4.Partner MAC Address	00.00.00. 00.00.00		> set wdstbl 4.4 partnermacaddr <MAC Address>
Status	disable		> set wdstbl 4.4 status <1=enable, 2=disable> OR > set wdstbl 4.4 <enable, disable>

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
5.Partner MAC Address	00.00.00. 00.00.00		> set wdstbl 4.5 partnermacaddr <MAC Address>
Status	disable		> set wdstbl 4.5 status <1=enable, 2=disable> OR > set wdstbl 4.5 <enable, disable>
6.Partner MAC Address	00.00.00. 00.00.00		> set wdstbl 4.6 partnermacaddr <MAC Address>
Status	disable		> set wdstbl 4.6 status <1=enable, 2=disable> OR > set wdstbl 4.6 <enable, disable>
Interfaces Parameters - Ethernet (speed and transmission mode)			> show ethernet
Configuration	autoautos peed		> set etherspeed <10halfduplex, 10fullduplex, 10autoduplex, 100halfduplex, 100fullduplex, autohalfduplex, autoautospeed> **NOTE:** 10 and 100 indicate the transmission speed in Mbps.
Management Parameters - Passwords			
SNMP Read Password	public		> set snmprpasswd <New Password>
SNMP Read/Write Password	public		> set snmprwpasswd <New Password>
Telnet/CLI Password	public		> passwd <Old Password> <New Password> <Confirm Password>
HTTP (AP-3) Password	public		> set httppasswd <New Password>
Management Parameters - IP Access Table			> show mgmtipaccesstbl
Management IP Access Table Status	enable		> set mgmtipaccesstblstatus <enable, disable>
IP Address			> set mgmtipaccesstbl <index> ipaddr <IP Address>
IP Mask			> set mgmtipaccesstbl <index> submask <IP Address>
Interface (optional)	all		> set mgmtipaccesstbl <index> if <1=Ethernet, 3=SlotA, 4=SlotB, all>
Comment (optional)			> set mgmtipaccesstbl <index> cmt <Optional Comment>

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
Status (optional)	enabled with entry		> set mgmtipaccesstbl <index> status <enable, disable>
Management Parameters - Services			> show snmp OR show http OR show telnet OR show serial
SNMP Status	disable		> set snmpstatus <enable, disable>
HTTP Status	enable		> set httpstatus <enable, disable>
HTTP Port	80		> set httpport <0 - 65535>
Telnet Status	enable		> set telstatus <enable, disable>
Telnet Port Number	23		> set telport <0 - 65535>
Telnet Login Time-out	30	(sec)	> set tellogintout <0 - 300 >
Telnet Session Idle Time-out	450	(sec)	> set telsessiontout <0 - 36000>
Serial Baud Rate	9600		>set serbaudrate <2400, 4800, 9600, 19200, 38400, 57600>
Serial Flow Control	None		> set serflowctrl <xon/xoff, none> **NOTE:** It is recommended that you leave this setting at its default value.
Filtering Parameters - Ethernet Protocol Filter			> show etherflt
Status	enable		> set etherfltstatus <enable, disable>
Operation Type	block		> set etherfltoptype <passthru, block>
Filtering Parameters - Ethernet Protocol Filter Table			> show etherflttbl

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
1 - 80:19 Apollo Domain Status	disable		**NOTE:** The Ethernet Protocol Filter Table contains a list of common protocol filters. You can add filters to this table as needed. **The Filter Operation (passthru or block) applies only to the protocols enabled in this table.** To add a filter to the table: > set etherflttbl <index> protonumber <Protocol Number> protoname <(Optional) Protocol Name> status <(Optional) enable, disable, delete> cmt <Optional Comment> To enable or disable a protocol filter: > set etherflttbl <index> enable OR > set etherflttbl <index> protonumber <Protocol Number> status <enable, disable, delete>
2 - 80:09 Apple Talk 1 and 2	disable		
3 - 80:F3 Apple Talk ARP 1 and 2	disable		
4 - 0B:AD Banyan VINES	disable		
5 - 0B:AF Banyan VINES Echo	disable		
6 - 60:03 Decnet Phase IV	disable		
7 - 60:05 DEC Diagnostics	disable		
8 - 60:04 DEC LAT	disable		
9 - 60:07 DEC LAVC	disable		
10 - 60:01 DEC MOP Dump/Load	disable		
11 - 60:02 DEC MOP Rem Cons	disable		
12 - 80:40 DEC Netbios	disable		
13 - 80:05 HP Probe Control	disable		
14 - 80:D5 IBM SNA Services	disable		
15 - 08:00 IP	disable		
16 - 08:06 IP-ARP	disable		
17 - 81:37 Novell (ECONFIG E)	disable		
18 - 80:35 RARP Reverse ARP	disable		
19 - 81:4C SNMP Over Ethernet	disable		

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
Filtering Parameters - Static MAC Address Filter Table			
Refer to Filtering Parameters - Static MAC Address Table			

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
Filtering Parameters - Advanced Filtering			
Proxy ARP Status	disable		>show parp >setparp status <enable, disable>
IP/ARP Filtering Status	disable		>show iparp >set iparp status <enable, disable>
IP/ARP Filtering Address			>set iparpfltipaddr <Network filter IP Address>
IP/ARP IP Mask			>set iparpfltsubmask <Network Mask IP Address>
Filtering Parameters - TCP/UDP Filtering			
Port Filter Status	enable, disable		> set portfltstatus <enable, disable>
Port Type	TCP, UDP, TCP/UDP		> set porttype <TCP, UDP, TCP/UDP>
Port Number			> set portnum
Protocol Name			> set protoname
Interface Bitmask	Only Ethernet Only Slot A Only Slot B All interface Slot A and Ethernet Slot B and Ethernet Slot A and Slot B		> set ifbitmask <1 (Ethernet only), 4 (Slot A only), 5 (Slot A & Ethernet), 8 (Slot B only), 9 (Slot B & Ethernet), 12 (Slots A & B), 15 (All interfaces)>
Status		enable disable delete	> set portfltstatus
Alarms Parameters - Groups			
Configuration Trap Status	enable		

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
Security Trap Status	enable		
Wireless Interface Trap Status	enable		
Operational Trap Status	enable		
Flash Memory Trap Status	enable		
TFTP Trap Status	enable		
Image Trap Status	enable		
Alarms Parameters - Trap Host Table			> show snmptraphosttbl
IP Address			> set snmptraphosttbl <index> ipaddr <IP Address>
Password			> set snmptraphosttbl <index> passwd <New Password>
Comment (optional)			> set snmptraphosttbl <index> cmt <Optional Comment>
Status (optional)	enabled with entry		> set snmptraphosttbl <index> status <enable, disable>
Alarms Parameters - Syslog			> show syslog
Syslog Status	disable		> set syslogstatus <enable, disable>
Syslog Port	514	N/A	> show syslogport
Syslog Lowest Priority Logged	6		> set syslogpritolog <1 (LOG_ALERT), 2 (LOG_CRIT), 3 (LOG_ERR), 4 (LOG_WARNING), 5 (LOG)_NOTICE), 6 (LOG_INFO), 7 (LOG_DEBUG)>
Heartbeat Status	disable (2)		> set heartbeatstatus <enable, disable>
Heartbeat Interval (seconds)	900	(sec)	> set heartbeatinterval <60 – 604800 seconds>
Alarms Parameters - Syslog Host Table			> show sysloghosttbl
IP Address	10.0.0.2 for index 1		> set sysloghosttbl <index> ipaddr <IP Address>
Comment (optional)			> set sysloghosttbl <index> cmt <Optional Comment>
Status (optional)	enabled with entry		> set sysloghosttbl <index> status <enable, disable, delete>

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
Bridge Parameters - Spanning Tree			> show stp
Spanning Tree Status	enable		> set stpstatus <enable, disable>
Bridge Priority	32768		> set stppriority <0 - 65535>
Max Age	2000	(1/100 sec)	> set stpmaxage <0 - 65535>
Hello Time	200	(1/100 sec)	>set stpbridgehellotime <0 - 65535>
Forward Delay	1500	(1/100 sec)	> set stpfwddelay <0 - 65535>
Bridge Parameters - Spanning Tree - Priority and Path Cost Table			
Refer to Bridge Parameters - Spanning Tree - Bridge Parameters - Spanning Tree - Priority Path and Cost Table			
Bridge Parameters - Storm Threshold Table			>show stmthres
Broadcast Address Threshold	0	(packets/sec)	>set stmbrdthres <0 - 255>
Multicast Address Threshold	0	(packets/sec)	>set stmmultithres <0 - 255>
Broadcast Ethernet Threshold	0	(packets/sec)	>set stmthrestbl 1 bcast <0 - 9999>
Multicast Ethernet Threshold	0	(packets/sec)	>set stmthrestbl 1 mcast <0 - 9999>
Broadcast Wireless - Slot A Threshold	0	(packets/sec)	>set stmthrestbl 3 bcast <0 - 9999>
Multicast Wireless - Slot A Threshold	0	(packets/sec)	>set stmthrestbl 3 mcast <0 - 9999>
Broadcast Wireless - Slot B Threshold	0	(packets/sec)	>set stmthrestbl 4 bcast <0 - 9999>
Multicast Wireless - Slot B Threshold	0	(packets/sec)	>set stmthrestbl 4 mcast <0 - 9999>
Bridge Parameters - Intra BSS			
Intra BSS Client Blocking	Passthru		> set intrabssoptype <passthru, block>

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
Bridge Parameters - Pkt Forwarding			
Packet Forwarding MAC Address	N/A		> set pktfwdmacaddr <MAC Address>
Packet Forwarding Status			> set pktfwdstatus <enable, disable>
Packet Forwarding Interface Port			> set pktfwdif <0 (any), 1 (Ethernet), 3 (Slot A - WDS 1), 4 (Slot A - WDS 2), 5 (Slot A - WDS 3), 6 (Slot A - WDS 4), 7 (Slot A - WDS 5), 8 (Slot A - WDS 6), 10 (Slot B - WDS 1), 11 (Slot B - WDS 2), 12 (Slot B - WDS 3), 13 (Slot B - WDS 4), 14 (Slot B - WDS 5), 15 (Slot B - WDS 6)>
Security Parameters - MAC Access Control			> show macacl
MAC Access Control Status	disable		> set macaclstatus <enable, disable>
MAC Access Control Operation	block		> set macacloptype <passsthru, block>
Security Parameters - MAC Access Control Table			> show macacltbl
MAC Address			> set macacltbl <index> macaddr <MAC address>
Comment (optional)			> set macacltbl <index> cmt <Optional Comment>
Status (optional)	enable on entry		> set macacltbl <index> status <enable, disable, delete>
Security Parameters - RADIUS Authentication/ Accounting			> show radius
RADIUS MAC Access Control Status	disable		> set radmacaccctrl <enable, disable>
Authorization Lifetime	900 sec	(sec)	> set radauthlifetm <60 - 43200 (in 60 sec increments)>
MAC Address Format	Dash Delimiter		set radmacaddrformat <dashdelimited, colondelimited, singledashdelimited, no delimiter>
RADIUS Accounting Status	disable		set radaccstatus <enable, disable>
Accounting Inactivity Timer	5 minutes		set radaccinactivetmr <0 – 2147483647 (in minutes)>
Security Parameters - RADIUS Authentication/ Accounting - Primary RADIUS Server			> show radiustbl
Status	disable		> set radiustbl 1 status <enable, disable>

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
Server Address Format	IP address		> set seraddrfmt <name, ipaddr>
Server IP Address or Name			> set radiustbl 1 ipaddr <IP Address or server name>
Port (optional)	1812		> set radiustbl 1 port <Port Number>
Shared Secret	public		> set radiustbl 1 ssecret <Password>
Response Time (optional)	3	(sec)	> set radiustbl 1 responsetm <1 - 10>
Max. Retransmissions (optional)	3		> set radiustbl 1 maxretx <Number of Times to Retransmit 1 - 4>

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
Security Parameters - RADIUS Authentication/ Accounting - Backup RADIUS Server			> show radiustbl
Status	disable		> set radiustbl 2 status <enable, disable>
Server Address Format	IP address		> set seraddrfmt <name, ipaddr>
Server IP Address or Name			> set radiustbl 2 ipaddr <IP Address or server name>
Destination Port	1813		> set radiustbl 2 port <1 - 65535>
Response Time (optional)	3	(sec)	> set radiustbl 2 responsetm <1 - 10>
Max. Retransmissions (optional)	3		> set radiustbl 2 maxretx <Number of Times to Retransmit 1-4>
RADIUS - DNS Client			
DNS Client status	enable disable		> set dnsstatus <enable, disable>
Primary DNS Server IP Address			> set dnspridnsipaddr <IP address of primary DNS server>
Secondary DNS Server IP Address			> set dnssecdnsipaddr <IP address of secondary DNS server>
Default Domain Name			> set dnsdomainname <domain name>
Security Parameters - Encryption - None - Wireless Slot A			
802.1x Security Mode	none		> set secconfig none
Encryption Status (Wireless Slot A)	disable		> set wifsec 3 encryptstatus disable
Security Parameters - Encryption - None - Wireless Slot B			
802.1x Security Mode	none		> set secconfig none
Encryption Status (Wireless Slot B)	disable		> set wifsec 4 encryptstatus disable
Security Parameters - Encryption - WEP only - Slot A			
802.1x Security Mode	none		> set secconfig none

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
Encryption Status	enable		> set wifsec 3 encryptstatus enable
Key Length		(bits)	> set secenckeylentbl 3 enckeylen <64, 128, or 152 bits (depends on card type)>
Encryption Key 1			> set wifsec 3 encryptkey1 <Encryption Key>
Encryption Key 2			> set wifsec 3 encryptkey2 <Encryption Key>
Encryption Key 3			> set wifsec 3 encryptkey3 <Encryption Key>
Encryption Key 4			> set wifsec 3 encryptkey4 <Encryption Key>
Deny Non-Encrypted Data	enable		> set wifsec 3 encryptdeny <enable, disable>
Encrypt Data Transmissions Using	1		> set wifsec 3 encryptkeytx <Key Number 1-4>
Security Parameters - Encryption - WEP only - Slot B			
802.1x Security Mode		none	> set secconfig none
Encryption Status		enable	> set wifsec 4 encryptstatus enable
Key Length		(bits)	> set secenckeylentbl 3 enckeylen <64, 128, or 152 bits (depends on card type)>
Encryption Key 1			> set wifsec 4 encryptkey1 <Encryption Key>
Encryption Key 2			> set wifsec 4 encryptkey2 <Encryption Key>
Encryption Key 3			> set wifsec 4 encryptkey3 <Encryption Key>
Encryption Key 4			> set wifsec 4 encryptkey4 <Encryption Key>
Deny Non-Encrypted Data	enable		> set wifsec 4 encryptdeny <enable, disable>
Encrypt Data Transmissions Using	1		> set wifsec 4 encryptkeytx <Key Number 1-4>
Security Parameters - Encryption - 802.1x only			> show security
802.1x Security Mode		802.1x	> set secconfig 802.1x
Encryption Status (Wireless Slot A)	enable		> set wifsec 3 encryptstatus disable
Encryption Status (Wireless Slot B)	enable		> set wifsec 4 encryptstatus disable
Key Length (Wireless Slot A)		(bits)	> set secenckeylentbl 3 enckeylen <64, 128, or 152 bits (depends on card type)>

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
Key Length (Wireless Slot B)		(bits)	> set secenckeylentbl 4 enckeylen <64, 128, or 152 bits (depends on card type)>
Rekeying Interval	900 seconds	(sec)	> set secrekeyint <60 - 65535>
Security Parameters - Encryption - Mixed (WEP and 802.1x) - Slot A			
802.1x Security Mode		Mixed (WEP and 802.1x)	> set secconfig mixed
Encryption Status		enable	> set wifsec 3 encryptstatus enable
Key Length		(bits)	> set secenckeylentbl 3 enckeylen <64, 128, or 152 bits (depends on card type)>
Encryption Key 1	user defined		
Encryption Key 2	---	---	---
Encryption Key 3	---	---	---
Encryption Key 4	---	---	---
Deny Non-Encrypted Data	enable	---	---
Encrypt Date Transmissions Using	Key 1	Key 1	---
Rekeying Interval	900 seconds	(sec)	> set secrekeyint <60 - 65535>
Security Parameters - Encryption - Mixed (WEP and 802.1x) - Slot B			
802.1x Security Mode		Mixed (WEP and 802.1x)	> set secconfig mixed
Encryption Status		enable	> set wifsec 4 encryptstatus enable
Key Length		(bits)	> set secenckeylentbl <index> enckeylen <64, 128, or 152 bits (depends on card type)>
Encryption Key 1	generated automatically	---	---
Encryption Key 2	---	---	---
Encryption Key 3	---	---	---

Configurable Parameter	Factory Default Values	My System Values	CLI Parameter Syntax
Encryption Key 4	---	---	---
Deny Non-Encrypted Data	enable	---	---
Encrypt Date Transmissions Using	Key 1	Key 1	---
Rekeying Interval	900 seconds	(sec)	> set secrekeyint <60 - 65535>
Commands - Download - TFTP Server			> show tftp
Server IP Address	10.0.0.2		> set tftpipaddr <IP Address> > download <TFTP IP Address> <File Name> <config, bin, bspbl>
Commands - Upload - TFTP Server			> show tftp
Server IP Address	10.0.0.2		> set tftpipaddr <IP Address> > upload <TFTP IP Address> <File Name> config
Commands - Reset			
Reset to Factory Defaults	---	---	> set sysresettodefaults 1 **NOTE:** This command requires you to re-enter the command for confirmation. The following message will be displayed: **WARNING: This command will reset the device configuration parameters to factory default values. Please re-enter this command in order to proceed with execution.**

Filtering Parameters - Static MAC Address Table

Wired MAC Address	Wired Mask	Wireless MAC Address	Wireless Mask	Comment (optional)	Status (optional)

Use the following commands to enter information into the Static MAC Address Table:

```
> show staticmactbl
> set staticmactbl <index> wiredmacaddr <wired MAC address>
> set staticmactbl <index> wiredmask <wired mask MAC address>
> set staticmactbl <index> wirelessmacaddr <wireless MAC
  address>
> set staticmactbl <index> wirelessmask <wireless mask MAC
  address>
> set staticmactble <index> cmt <Optional Comment>
> set staticmactbl status <enable, disable (optional - enabled
  with entry in table)>
```

Result: the table is now configured. Use **`show staticmactbl`** to view the table.

Table 7-1 Bridge Parameters - Spanning Tree - Priority Path and Cost Table

Port	Priority	Path Cost	Status
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Use the following commands to enter information into the Priority Path and Cost Table:

```
> set stptbl <index 1 - 15> priority <0 - 255>
> set stptbl <index> pathcost <1 - 65535>
> set stptbl <index> status <enable, disable, delete>
```

Once you have entered information into the Priority Path and Cost Table, view the table to confirm your changes using the **`show stptbl`** command.

Specifications B

In This Chapter

Hardware Specifications

Physical Specifications

AP-3 Unit

Dimensions (H x W x L) = 6.5 x 18.5 x 26 cm (2.5 x 7.25 x 10.25 in.)
Weight = 1.75 Kg (3.5 lb.)

802.11a Antenna Adapter

Dimensions (H x W x L) = 11.3 x 2.10 x 26.2 cm (4.5 x 0.83 x 10.3in.)
Weight = 0.18kg (0.4lb)

Electrical Specifications

Without Active Ethernet Module

Voltage = 100 to 240 VAC (50-60 Hz)
Current = 0.2 amp
Power Consumption = 20 Watts

With Active Ethernet Module

Input Voltage = 42 to 60 VDC
Output Current = 200mA at 48V
Power Consumption = 9-10 Watts

Environmental Specifications

AP-3 Unit

Operating = 0° to 40°C (32° to 104 °F) @ 20 to 90% relative humidity
Transport = -40° to 60°C (-40° to 140°F) @ 15 to 95% relative humidity (no condensation allowed)
Storage = -10° to 60°C (14° to 140°F) @ 10 to 90% relative humidity (no condensation allowed)

802.11a Antenna Adapter

Operating = 0° to 70°C (32° to 158 °F) @ 20 to 90% relative humidity
Transport = -40° to 75°C (-40° to 167 °F) @ 15 to 95% relative humidity
Storage = -20° to 75°C (-4° to 167 °F) @ 10 to 95% relative humidity

Ethernet Interface

10/100 Base-T, RJ-45 female socket

PCMCIA Interface

PC Card Slot (A & B) = Standard PC Card slot for Avaya Wireless PC Card

Serial Port Interface

Connector Type = DB9, male

Serial Cable = Standard RS-232C serial data cable, with a female DB-9 connector at each end or a standard serial cable and the mini-DIN8 to DB-9 adapter included in your kit.

Active Ethernet Interface

Category 5, foiled, twisted pair cables must be used to ensure compliance with FCC Part 15, subpart B, Class B requirements

Standard 802.3af pin assignments

HTTP Interface

Microsoft Internet Explorer 5.5 or better (preferred), or Netscape 4.x or higher.

Radio Specifications

802.11a radio certification is not available in all countries. Contact your sales representative for details.

802.11b radio certification is available in the US/Canada (FCC), Japan (VCCI), Europe (ETSI), and France.

802.11b Channel Frequencies

The following table shows the channel allocations that vary from country to country. Values listed in bold font indicate default channels and frequencies.

Channel ID	FCC/World (MHz)	ETSI (MHz)	France (MHz)	Japan (MHz)
1	2412	2412	-	2412
2	2417	2417	-	2417
3 (default - most countries)	**2422**	**2422**	**-**	**2422**
4	2427	2427	-	2427
5	2432	2432	-	2432
6	2437	2437	-	2437
7	2442	2442	-	2442
8	2447	2447	-	2447
9	2452	2452	-	2452
10	2457	2457	2457	2457
11 (default-France)	2462	2462	**2462**	2462
12	-	2467	2467	2467

Channel ID	FCC/World (MHz)	ETSI (MHz)	France (MHz)	Japan (MHz)
13	-	2472	2472	2472
14				2484

802.11a Channel Frequencies

The following table shows the channel allocations that vary from country to country. Values listed in bold font indicate default channels and frequencies.

Note: 802.11a radios may not be available in all countries. Contact your sales representative for details.

Channel ID	FCC/World (MHz)	FCC Turbo mode (MHz)	ETSI (MHz)	Japan (MHz)
34	-	-	-	**5170**
36	5180	-	5180	-
38	-	-	-	5190
40	5200	-	5200	-
42	-	5210	-	5210
44	**5220**	**-**	**5220**	**-**
46	-	-	-	5230
48	5240	-	5240	-
50	**-**	5250	-	-
52	**5260**	-	5260	-
56	5280	-	5280	-
58	-	5290	-	-
60	5300	-	5300	-
64	5320	-	5320	-

Wireless Communication Range

The range of the wireless signal is related to the composition of objects in the radio wave path, and the transmit rate of the wireless communication. Communications at a lower transmit range may travel longer distances.

Note: The range values listed in the Communications Range Chart are typical distances as measured at the development laboratories. These values provide a rule of thumb and may vary according to the actual radio conditions at the location where the product is used.

The range of your wireless devices can be affected when the antennas are placed near metal surfaces and solid high-density materials. Ranges for outdoor antenna installations are related to type of outdoor antennas used, and length of antenna cables. Range is also impacted due to “obstacles” in the signal path of the radio that may either absorb or reflect the radio signal.

In Open Office environments, antennas can “see” each other (no physical obstructions between them). In Semi-open Office environments, workspace is divided by shoulder-height, hollow wall elements; antennas are at desktop level. In a Closed Office environment, solid walls and other obstructions may affect signal strength.

The following tables show typical range values for various environments.

The first table shows the 802.11b wireless communication ranges.

Range	**11 Mbs**	**5.5 Mbs**	**2 Mbs**	**1 Mbs**
Open Office	160 m (525 ft.)	270 m (885 ft.)	400 m (1300 ft.)	550 m (1750 ft.)
Semi-Open Office	50 m (165 ft.)	70 m (230 ft.)	90 m (300 ft.)	115 m (375 ft.)
Closed Office	25 m (80 ft.)	35 m (115 ft.)	40 m (130 ft.)	50 m (165 ft.)
Receiver Sensitivity	-82 dBm	-87 dBm	-91 dBm	-94 dBm
Delay Spread (at FER of <1%)	65 ns	225 ns	400 ns	500 ns

The second table shows the 802.11a wireless communication ranges.

Range	**54 Mbs**	**48 Mbs**	**36 Mbs**	**24 Mbs**	**18 Mbs**	**12 Mbs**	**9 Mbs**	**6 Mbs**
Open Office	19 m (62 ft.)	35 m (115 ft.)	74 m (243 ft.)	112 m (367 ft.)	153 m (502 ft.)	189 m (620 ft.)	232 m (761 ft.)	258 m (846 ft.)
Semi-Open Office	17 m (56 ft.)	29 m (95 ft.)	34 m (111 ft.)	49 m (161 ft.)	63 m (206 ft.)	76 m (249 ft.)	90 m (295 ft.)	99 m (325 ft.)
Closed Office	15 m (49 ft.)	24 m (79 ft.)	27 m (88 ft.)	36 m (118 ft.)	45 m (147 ft.)	52 m (170 ft.)	60 m (197 ft.)	64 m (210 ft.)
Receiver Sensitivity	-65 dBm	-69 dBm	-73 dBm	-77 dBm	-80 dBm	-82 dBm	-84 dBm	-85 dBm