

Rhein Tech Laboratories, Inc.  
360 Herndon Parkway  
Suite 1400  
Herndon, VA 20170  
<http://www.rheintech.com>

Client: 3e Technologies International Inc.  
Model: 3e-525A  
Standards FCC 15.247  
FCC ID: QVT-525A  
Report #: 2004121

## **APPENDIX I: MANUAL**

Please refer to the following pages.



## Wireless Access Point User's Guide *Model 3e-525A*



**3e Technologies International**  
700 King Farm Blvd., Suite 600  
Rockville, MD 20850  
(301) 670-6779 [www.3eti.com](http://www.3eti.com)

29000132-001 A

publ. 7/09/04

This page intentionally left blank.

# **3e Technologies International's Wireless Access Point User's Guide**

*Model 3e-525A*

## **Safety Requirements**

- If AC power will be used, the socket outlet shall be installed near the equipment and shall be easily accessible.
- CAUTION: If this device contains a battery, there is risk of exposure if the battery is replaced by an incorrect type. Dispose of any used batteries according to the instructions on the battery.

Copyright © 2004 3e Technologies International, Inc. All rights reserved. No part of this documentation may be reproduced in any form or by any means or to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3e Technologies International.

3e Technologies International reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3e Technologies International to provide notification of such revision or change.

3e Technologies International provides this documentation without warranty, term or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms, or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3e Technologies International may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software or removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the printed documentation, or on the removable media in a readable file such as license.txt or the like. If you are unable to locate a copy of the license, contact 3e Technologies International and a copy will be provided to you.

---

#### UNITED STATES GOVERNMENT LEGEND

If you are a United States Government agency, then this documentation and the product described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3e Technologies International's standard commercial license for the software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

---

3e Technologies International and the 3e Technologies International logo are registered trademarks.

Windows is a registered trademark of Microsoft Corporation. Any other company and product name mentioned herein is a trademark of the respective company with which they are associated.

#### EXPORT RESTRICTIONS

This 3e Technologies International product contains encryption and may require U.S. and/or local government authorization prior to export to another country.

# Table of Contents

<b>Chapter 1: Introduction</b> .....	<b>1</b>
Basic Features .....	2
Wireless Basics.....	2
802.11b .....	3
802.11g.....	3
Network Configuration.....	3
Access Point Configurations.....	4
Possible AP Topologies.....	4
Bridging .....	5
Default Configuration.....	5
Data Encryption and Security.....	5
SSID .....	6
WEP .....	6
WPA with TKIP/ AES-CCMP.....	6
AES and 3DES.....	6
Authentication .....	7
DHCP Server .....	7
Operator Authentication and Management .....	7
Management .....	7
3e-525A Navigation Options .....	8
<b>Chapter 2: Hardware installation</b> .....	<b>9</b>
Preparation for Use.....	9
Installation Instructions .....	10
Minimum System and Component Requirements .....	10
Ensure the Cabling is Correctly Installed.....	10
The Indicator Lights.....	12
<b>Chapter 3: Access Point Configuration</b> .....	<b>13</b>
Introduction .....	13
Preliminary Configuration Steps.....	13
Initial Setup using the “Local” Port .....	14
System Configuration.....	15
General.....	15
WAN.....	16
LAN.....	17
Operating Mode.....	17
Submodes .....	18
Wireless Configuration .....	19
General.....	19
Security .....	22
No Encryption .....	22
Static AES Key .....	23
Static 3DES Key .....	23
Dynamic Key Exchange .....	24
No Encryption (non-FIPS) .....	24
Static WEP Encryption (non-FIPS) .....	25
WPA (non-FIPS).....	26
MAC Address Filtering .....	27
Bridging and Bridging Encryption .....	28
Rogue AP Detection .....	28
Advanced.....	29
Services Settings .....	30

DHCP Server .....	30
SNMP Agent.....	31
Misc Services .....	32
Print Server .....	32
User Management.....	33
List All Users .....	33
Add New User .....	33
Password Policy (FIPS Mode Only).....	34
Monitoring/Reports .....	34
System Status .....	34
Bridging Status.....	35
Wireless Clients.....	36
Adjacent AP List .....	38
DHCP Client List .....	38
System Log .....	39
Web Access Log .....	39
Network Activity .....	40
System Administration .....	41
Firmware Upgrade .....	41
Self-Test .....	41
Factory Default .....	42
Remote Logging.....	42
Reboot .....	43
Utilities .....	43
<b>Chapter 4: Gateway Configuration .....</b>	<b>45</b>
Introduction .....	45
Configuring in Gateway Mode .....	47
System Configuration.....	48
General .....	48
WAN .....	49
LAN .....	50
Operating Mode.....	51
Wireless Configuration .....	51
General .....	51
Advanced Options: .....	53
Encryption .....	54
No Encryption .....	54
Static WEP Encryption .....	54
WPA (non-FIPS) .....	55
Static AES Key/Open System Authentication .....	57
Static 3DES Key/Open System Authentication.....	57
Mac Address Filtering.....	58
Bridging .....	58
Rogue AP Detection .....	59
Advanced.....	59
Services Settings .....	60
DHCP Server .....	60
SNMP Agent.....	61
Misc Service.....	62
Firewall.....	62
Content Filtering.....	62
IP Filtering .....	63
Port Filtering .....	63
Virtual Server .....	64

Demilitarized Zone (DMZ) .....	66
Advanced Firewall .....	66
User Management.....	67
List All Users .....	67
Add New User .....	67
Monitoring/Reports .....	68
System Status .....	68
Bridging Status.....	69
Wireless Clients.....	69
Adjacent AP List .....	70
DHCP Client List .....	70
System Log .....	70
Web Access Log .....	71
Network Activites .....	71
System Administration .....	72
Firmware Upgrade .....	73
Factory Default .....	73
Remote Logging.....	73
Reboot .....	74
Utilities .....	74
<b>Chapter 5: Bridge Configuration .....</b>	<b>75</b>
Introduction .....	75
General Bridge Setup .....	75
Setting Up Bridging Type .....	78
Point-to-Point Bridge Configuration .....	78
Point-to-Point Bridging Setup Guide .....	79
Point-to-Multipoint Bridge Configuration .....	82
Point-to-Multipoint Bridging Setup Guide .....	83
Repeater Bridge Configuration .....	83
Repeater Bridging Setup Guide .....	83
<b>Chapter 6: The RF Manager Function .....</b>	<b>85</b>
Introduction .....	85
How to Access the RF Manager Function .....	86
How to Program the RF Manager .....	87
<b>Chapter 7: Network Printer Setup .....</b>	<b>91</b>
Install Print Service for Unix (Windows 2000): .....	91
Set Up the Printer.....	92
<b>Chapter 8: Technical Support.....</b>	<b>97</b>
Manufacturer's Statement .....	97
Radio Frequency Interference Requirements.....	97
Channel Separation and WLAN Cards .....	98
<b>Glossary .....</b>	<b>G-a</b>



This page intentionally left blank.

## Chapter 1: Introduction

This manual covers the installation and operation of the 3e Technologies International's 3e-525A Wireless Access Point. The 3e-525A is a ruggedized access point/gateway/bridge which is intended for use in industrial and external environments. It accommodates both 802.11b WLAN and 802.11g WLAN access and uses Power over Ethernet (PoE) access to the Ethernet WAN to eliminate the need for internal access point power supply units (AC-DC converters) and 110-220V cabling installations. The wireless LANs can include mobile devices such as handheld Personal Data Assistants (PDAs), mobile web pads, and wireless laptops.

If encryption is desired for the WLAN, you can employ different encryption depending on the mode you are in. If you are using FIPS 140-2 mode (highly secure) you can set encryption for None, Static AES, Static 3DES or Dynamic Key Exchange. If you are using the 3e-525A as an access point but not using FIPS 140-2 mode, you can select None, or Static 3DES, or Static AES, Static WEP, or WPA. WPA uses TKIP or AES-CCMP so you can employ legacy client WEP cards and still secure the wireless band.

If it is desired that the access point employ state-of-the-art AES or 3DES encryption, wireless devices must have the 3e-010F Crypto Client software installed. (The 3e-010F Crypto Client software is sold with the 3e-110 long range PC Card or sold separately for use with other compatible PC Cards.)

The 3e-525A incorporates IEEE 802.3af (Power over Ethernet) and the capability for the highest security functionality (AES) as well as long-range RF capability. The PoE interface on the 3e-525A is compatible with commercial vendor "injected power" hub units (also known as Ethernet Power Supply or Power over Ethernet Hubs).

The 3e-525A includes AES/3DES cryptographic modules for wireless encryption and HTTPS/TLS, for secure web communication. In addition, it contains the capability to use the traditional WEP algorithm, either as static WEP or managed under WPA. The 3e-525A has an Ethernet WAN interface for communication to the wired LAN backbone, Ethernet LAN local port for purposes of initial setup and configuration, and two wireless LAN antennas for communicating on the 802.11b or 802.11g frequency. Further, it has the capability for use of an external (remote) antenna (purchased separately), for bridging, using the 802.11b or 802.11g frequency. The 802.11g frequency is very suitable for use when configuring the unit to be used as a bridge.

## Basic Features

The 3e-525A is housed in a sturdy case which is not meant to be opened except by an authorized technician for maintenance or repair. The unit should work without fail. If you wish to reset to factory settings, use the reset function available through the web-screen management module.

The 3e-525A is wall-mountable.

It has the following features:

- Ethernet uplink WAN port
- Local Ethernet LAN port (for configuration only)
- USB port
- Wireless (802.11b) interface with operating range of 2000+ feet
- Wireless (802.11g) interface
- Power over Ethernet (PoE)
- Above average temperature range for extreme environments (with TEC option)
- AES, 3DES, WEP encryption or WPA with TKIP, depending on setup
- HTTPS/TLS secure Web
- 802.1x
- DHCP client
- Access Point or Gateway with Bridging also available in either mode
- Bandwidth control
- Adjustable Radio Power
- MAC address filtering
- Load Balancing
- Rogue AP Detection

The following cryptographic modules have been implemented in the 3e-525A .

- AES for wireless (128/192/256 bit)
- 3DES for wireless (192 bit)
- WEP
- WPA
- 802.1x/EAP-TLS for authentication
- MAC-based authentication
- Rogue AP detection

## Wireless Basics

Wireless networking uses electromagnetic radio frequency waves to transmit and receive data. Communication occurs by establishing radio links between the wireless access point and devices configured to be part of the WLAN.

The 3e-525A incorporates the 802.11b (WiFi) standard, the 802.11g standard and the most state of the art encryption for a very powerful and secure wireless environment.

## 802.11b

The IEEE 802.11b standard, developed by the Wireless Ethernet Compatibility Alliance (WECA) and ratified by IEEE, establishes a stable standard for compatibility. A user with an 802.11b product can use any brand of access point with any other brand of client hardware that is built to the 802.11b standard for basic interconnection. 802.11b devices provide 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps depending on signal strength) in the 2.4 GHz band.

For wireless devices to communicate with the 3e-525A, they must meet the following conditions:

- The wireless device and wireless access point must have been configured to recognize each other using the SSID (a unique ID assigned in setup so that the wireless device is seen to be part of the network by the 3e-525A);
- Encryption and authentication capabilities and types enabled must conform; and
- If MAC filtering is used, the 3e-525A must be configured to allow the wireless device's MAC address to associate (communicate) with the 3e-525A wireless interface.

## 802.11g

Because 802.11g is backwards-compatible with 802.11b, it is a popular component in LAN construction. 802.11g broadens 802.11b's data rates to 54 Mbps within the 2.4 GHz band using OFDM (orthogonal frequency division multiplexing) technology. The dual functionality of 802.11b and 802.11g is preferable to use of 802.11b with 802.11a, as this would require that you replace existing NICs with 802.11a/b NICs to ensure interoperability. These are some of the considerations that were taken into account in designing the 3e-525A.

## Network Configuration

The 3e-525A is an access point with bridging setup capability:

- Access point/Gateway plus:
- Wireless bridging with choice of:
  - Point-to-point setup
  - Point-to-multipoint setup
  - Repeater setup

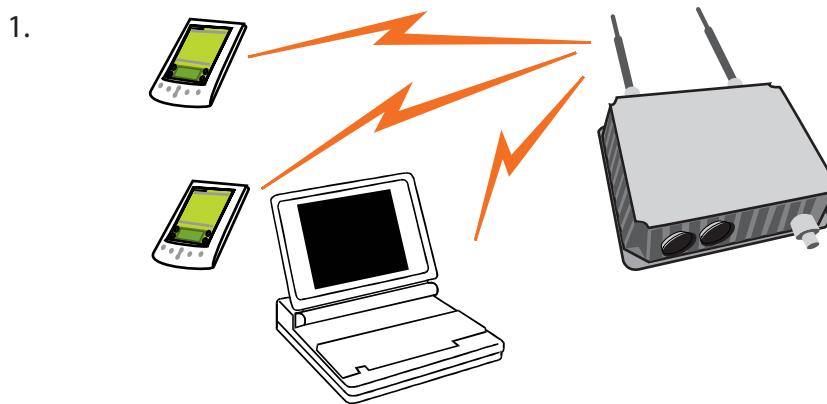
Bridging actually has more choices, but the above choices are popular and are discussed later in this user guide (Chapter 4).

## Access Point Configurations

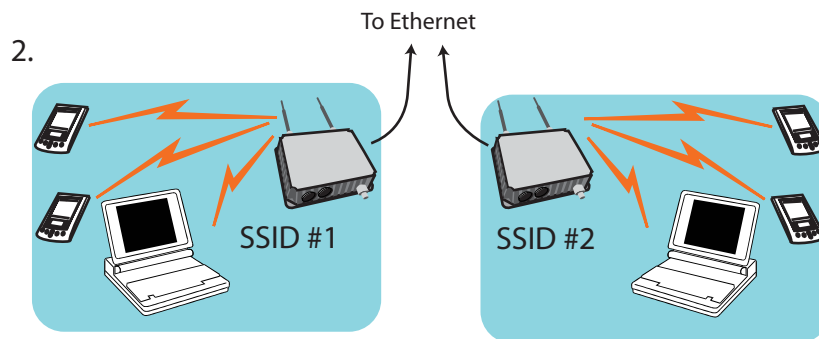
When a 3e-525A is used as an access point, IP addresses for wireless devices are typically assigned by the wired network's DHCP server. The wired LAN's DHCP server assigns addresses dynamically, and the AP virtually connects wireless users to the host wired network. All wireless devices connected to the AP are configured on the same subnet as the wired network interface and can be accessed by devices on the wired network.

### Possible AP Topologies

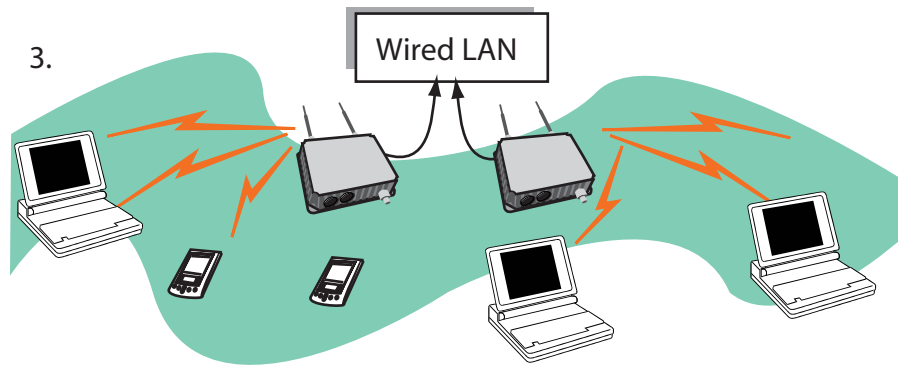
1. An access point can be used as a single AP without any connection to a wired network. In this configuration, it simply provides a stand-alone wireless network for a group of wireless devices.



2. The 3e-525A can be used as one of a number of APs connected to an existing Ethernet network to bridge between the wired and wireless environments. Each AP can operate independently of the other APs on the LAN. Multiple APs can coexist as separate individual networks at the same site without interference if each AP is set with a different network ID (SSID).



3. The last and most prevalent use is multiple APs connected to a wired network and operating off that network's DHCP server to provide a wider coverage area for wireless devices, enabling the devices to "roam" freely about the entire site. This is the topology of choice today.



## Bridging

The wireless bridging function in the 3e-525A allows use as a bridge, in a number of alternate configurations, including the following popular configurations:

- Point-to-point bridging of 2 Ethernet Links;
- Point-to-multipoint bridging of several Ethernet links;
- Repeater mode (wireless client to wireless bridge.)

## Default Configuration

The 3e-525A boots up in Access Point/Bridge mode.

## Data Encryption and Security

The 3e-525A Wireless Access Point includes advanced wireless security features. Over the AP band, you have a choice of no security, Static WEP, WPA, AES/3DES, depending on your mode of operation. Some level of security is suggested. Static WEP gives you a choice of 64-bit, 128-bit or 152-bit encryption. WPA includes the option of using a WPA pre-shared key or, for the enterprise that has a Radius Server installed, configuration to use the Radius Server for key management with either TKIP or AES-CCMP. Bridging encryption is established between 3e-525A's and includes use of AES-ECB or 3DES encryption (approved by the National Institute of Standards and Technology (NIST) for U.S. Government and DoD agencies). (As a side note, NIST is currently reviewing the AES-CCMP adopted by the WiFi Alliance and is expected to eventually ratify that standard for U.S. Government use.)

## **SSID**

The Service Set ID (SSID) is a string used to define a common roaming domain among multiple wireless access points. Different SSIDs on access points can enable overlapping wireless networks. The SSID can act as a basic password without which the client cannot connect to the network. However, this is easily overridden by allowing the wireless AP to broadcast the SSID, which means any client can associate with the AP. SSID broadcasting can be disabled in the 3e-525A setup menus if you're configuring to use WEP encryption. AES and 3DES always broadcast but are so secure that 'shared key' is not necessary.

## **WEP**

WEP is an older encryption standard but is preferable to no encryption. When using WEP, 802.1x can be used to increase security. If the 3e-525A is configured with WEP encryption, it is compatible with any 802.11b PC Card configured for WEP.

## **WPA with TKIP/ AES-CCMP**

WPA, an interim standard developed by the WiFi Alliance, combines several technologies that address known 802.11x security vulnerabilities. It provides an affordable, scalable solution for protecting existing corporate WLANs without the additional expense of VPN/firewall technology. It includes the use of the 802.1x standard and the Extensible Authentication Protocol (EAP). In addition, it uses, for encryption, the Temporal Key Integrity Protocol (TKIP) and WEP 128-bit encryption keys. Finally, a message integrity check (MIC) is used to prevent an attacker from capturing and altering or forging data packets. In addition, it can employ a form of AES called AES-CCMP. The WAB-1000 allows the user to configure Encryption type to allow either TKIP clients, AES-CCMP clients, or a mix of both.

WPA is a subset of the draft 802.11i standard and is expected to maintain forward compatibility.

## **AES and 3DES**

The Advanced Encryption Standard (AES) was selected by National Institute of Standards and Technology (NIST) in October 2000 as an upgrade from the previous DES standard. AES uses a 128-bit block cipher algorithm and encryption technique for protecting computerized information. It has the ability to use even larger 192-bit and 256-bit keys, if desired.

3DES is also incorporated on the 3e-525A . 3DES is modeled on the older DES standard but encrypts data three times over. Triple-DES uses more CPU resources than AES because of the triple encryption.

If you intend to use AES or 3DES, you must enable use by purchasing the 3eTI advanced Crypto Client software (3e-010F) for each client that

will be included in the WLAN. We sell this software with the 3e-110 PC Card.

The 3e-525A uses AES-CCMP in WPA mode and AES-ECB (or 3DES) for FIPS 140-2 mode and for the bridging channel.

## **Authentication**

The MAC address, short for *Media Access Control address*, is a hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the Data Link Control (DLC) layer of the OSI Reference Model is divided into two sub-layers: the *Logical Link Control (LLC) layer* and the *Media Access Control (MAC) layer*. The MAC layer interfaces directly with the network media. Consequently, each type of network media requires a unique MAC address.

Authentication is the process of proving a client identity. The 3e-525A access points, if set up to use MAC address filtering, detect an attempt to connect by a client and compare the client's MAC address to those on a predefined MAC address filter list. Only client addresses found on the list are allowed to associate. MAC addresses are assigned and registered to each of the wireless cards used by the portable computing devices during initial setup and after physical installation of the access points.

## **DHCP Server**

The DHCP function is accessible only from the local LAN port to be used for initial configuration.

## **Operator Authentication and Management**

Authentication mechanisms are used to authenticate an operator accessing the device and to verify that the operator is authorized to assume the requested role and perform services within that role.

Access to the management screens for the 3e-525A requires knowledge of the assigned operator ID and Password. The Factory defaults are:

- ID: CryptoOfficer
- Password: CryptoFIPS

The Crypto Officer initially installs and configures the 3e-525A after which the password should be changed from the default password. The ID and Password are case sensitive.

## **Management**

After initial setup, maintenance of the system and programming of security functions are performed by personnel trained in the procedure using the embedded web-based management screens.

The next chapter covers the basic procedure for setting up the hardware.



<b>3e-525A Navigation Options</b>		
<b>Access Point</b>		<b>Gateway</b>
Not FIPS 140-2	FIPS 140-2	Not FIPS 140-2
<b>System Configuration</b>	<b>System Configuration</b>	<b>System Configuration</b>
General	General	General
WAN	WAN	WAN
LAN	LAN	LAN
Operating Mode	Operating Mode	Operating Mode
<b>Wireless configuration</b>	<b>Wireless configuration</b>	<b>Wireless configuration</b>
General	General	General
Security	Security	Security
<ul style="list-style-type: none"> <li>• None</li> <li>• Static WEP</li> <li>• WPA <ul style="list-style-type: none"> <li>Preshared Key</li> <li>802.1x/Radius</li> <li>TKIP</li> <li>AES-CCMP</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• None</li> <li>• Static AES</li> <li>• Static 3DES</li> </ul>	<ul style="list-style-type: none"> <li>• None</li> <li>• Static WEP</li> <li>• WPA <ul style="list-style-type: none"> <li>Preshared Key</li> <li>802.1x/Radius</li> <li>TKIP</li> <li>AES-CCMP</li> </ul> </li> </ul>
	<ul style="list-style-type: none"> <li>• Dynamic Key Exchange</li> </ul>	<ul style="list-style-type: none"> <li>Static AES</li> <li>Static 3DES</li> </ul>
MAC Address Filtering	MAC Address Filtering	MAC Address Filtering
Bridging	Bridging	Bridging
Bridging Encryption	Bridging Encryption	Bridging Encryption
Rogue AP detection	Rogue AP detection	Rogue AP detection
Advanced	Advanced	Advanced
<b>Services Settings</b>	<b>Services Settings</b>	<b>Services Settings</b>
DHCP Server	DHCP Server	DHCP Server
SNMP agent	SNMP agent	SNMP agent
Misc Service	Misc Service	Misc Service
<b>Firewall</b>	<b>Firewall</b>	<b>Firewall</b>
		Content Filtering
		IP Filtering
		Port Filtering
		Virtual Server
		DMZ
		Advanced
<b>User Management</b>	<b>User Management</b>	<b>User Management</b>
List All Users	List All Users	List All Users
Add New User	Add New User	Add New User
	User Password Policy	
<b>Monitoring Reports</b>	<b>Monitoring Reports</b>	<b>Monitoring Reports</b>
System Status	System Status	System Status
Bridging Status	Bridging Status	Bridging Status
Wireless clients	Wireless clients	Wireless clients
Adjacent AP List	Adjacent AP List	Adjacent AP List
DHCP Client List	DHCP Client List	DHCP Client List
System Log	System Log	System Log

## Chapter 2: Hardware installation

### Preparation for Use

The 3e Technologies International's 3e-525A Wireless Access Point requires physical mounting and installation on the site, following a prescribed placement design to ensure optimum operation and roaming.

The 3e-525A operates with Power over Ethernet (PoE) which requires the installation of a separate Power injector which “injects” DC current into the Cat5 cable.

The 3e-525A package includes the following items:

- The 3e-525A Wireless Access Point
- 3 attachable 5dBi omni-directional antennas with reverse polarity type N connectors
- 1 15 Meter Ethernet cable
- 1 Power injector
- 1 mounting kit for unit
- 1 Ground wire
- Documentation as PDF files (on CD-ROM)
- Registration card
- Warranty card

The 802.11g antenna port is used when configuring the unit to be used as a bridge. The 802.11g port uses an omni-directional antenna.

The 3e-525A can be mounted outdoors on a high post to achieve the best bridge result. It has a lightning protection option to prevent lightning damage.



The antennas used with the 525A must be installed with a minimum separation distance of 20 cm from all persons, and must not be co-located or operated in conjunction with any other antenna or transmitter. Installation should be accomplished using the authorized cables and/or connectors provided with the device or available from the manufacturer/distributor for use with this device. Changes or modifications not expressly approved by the manufacturer or party responsible for this FCC compliance could void the user's authority to operate the equipment.

## Installation Instructions

The 3e-525A is intended to be installed as part of a complete wireless design solution.

This manual deals only and specifically with the single 3e-525A device as a unit. The purpose of this chapter is the description of the device and its identifiable parts so that the user is sufficiently familiar to interact with the physical unit. Preliminary setup information provided below is intended for information and instruction of the wireless LAN system administration personnel.

It is intended, and is the philosophy of 3e Technologies International, that the user not be required to open the individual unit. Any maintenance required is limited to the external enclosure surface, cable connections, and to the management software (as described in chapter three through five) only. A failed unit should be returned to the manufacturer for maintenance. Sites requiring emergency backup should maintain extra units of the device to interchange in case of failure.

## Minimum System and Component Requirements

The 3e-525A is designed to be attached to the wall at appropriate locations. To complete the configuration, you should have at least the following components:

- PCs with one of the following operating systems installed: Windows NT 4.0, Windows 2000 or Windows XP;
- A compatible 802.11b or 802.11g PC Card or 802.11b or 802.11g device for each computer that you wish to wirelessly connect to your wireless network. (For wireless cards, and particularly if you will be using secure FIPS mode with AES, we recommend that you select the 3e-110 PC Card with 3e-010F Crypto Client software (sold separately) or install the 3e-010F software with any compatible PC Card. (If you will be using WEP, the 3e-010F software is not required);
- Access to at least one laptop or PC with an Ethernet card and cable that can be used to complete the initial configuration of the unit.
- A Web browser program (such as Microsoft Internet Explorer 5.5 or later, or Netscape 6.2 or later) installed on the PC or laptop you will be using to configure the Access Point.
- TCP/IP Protocol (usually comes installed on any Windows PC.)

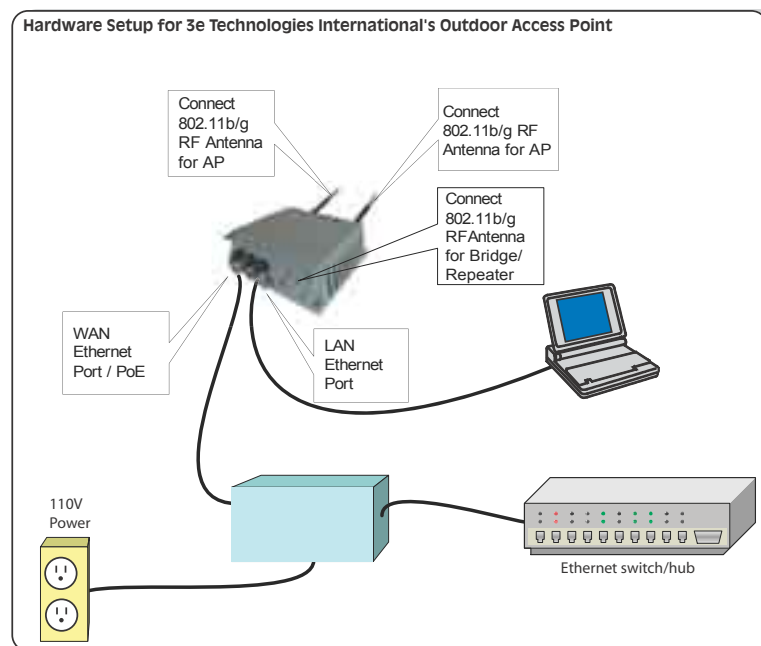
## Ensure the Cabling is Correctly Installed

The 3e-525A is well-protected in a metal enclosure which is generally bolted to a surface. The device should not be opened.

The following illustration shows the external cable connectors on the 3e-525A.



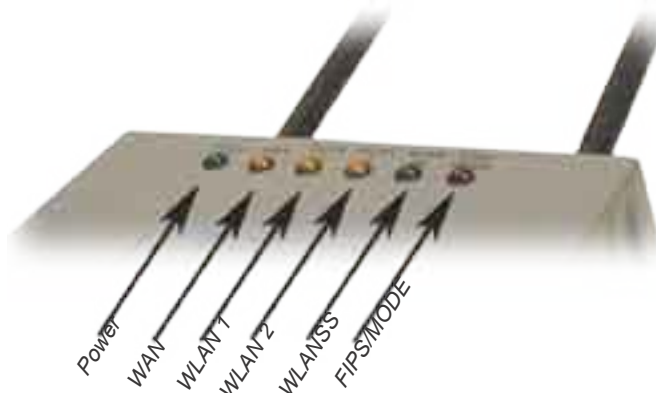
The WAN connector is used to connect the 3e-525A to the organization's LAN. The WAN connector is routed from the unit to the power injector which runs AC power through the Ethernet cable to the unit. The Ethernet cable is thus run from the 3e-525A to the power injector which is then connected to a power source and the wired LAN. A second (LAN Port) Ethernet connector is designed for use during initial configuration only. This uses an RJ45 cable to connect the 3e-525A to a laptop. The following diagram demonstrates the setup.



### The Indicator Lights

### 3e-525A Wireless Access Point

The top panel of the 3e-525A contains a set of indicator lights (Light Emitting Diodes or LEDs) that help describe the state of various networking and connection operations.



Detail of LEDs on the face of the 3e-525A

LED	Description
Power	The Power indicator LED informs you when the gateway is on or off. If this light is on, the gateway is on; if it is not on, the gateway is off.
WAN	This light indicates the state of your connection to the organization's Ethernet LAN network. When on, the WAN light indicates that the gateway is connected to the network. When the WAN light is off, the gateway does not have an active connection to the network.
WLAN1 Activity	This light may be steady or blinking and indicates that information is passing through the connection.
WLAN2 Activity	This light may be steady or blinking and indicates that information is passing through the connection.
WLAN Signal Strength	The Strength LED indicator indicates the strength of the connection. <ul style="list-style-type: none"> <li>1. LED Off: means on connection on the bridge side, or the signal is very weak</li> <li>2. LED blinks slowly (every 1 second): means there is a connection, and the signal quality is poor</li> <li>3. LED blinks fast: means there is a connection, and the signal quality is good</li> <li>4. LED steady on: means there is a connection, and the signal quality is excellent</li> </ul>
FIPS/MODE	The FIPS led is only lit when the software discovers a problem with the encryption algorithm or the system configuration file doesn't pass the integrity check. This is true no matter what mode of operation you are using, (AP -FIPS, AP-non-FIPS, or Gateway.)

## Chapter 3: Access Point Configuration

### Introduction

The 3e-525A comes with the capability to be configured as an access point. As it incorporates two separate 802.11 wireless cards, one for configuring a local WLAN and one for use in bridging, it can also be configured for bridging, either with access point or gateway configuration on the WLAN side. Configuration as a gateway is discussed in Chapter 4 and configuration for bridging is discussed in Chapter 5.

If configured as an access point, it can be further configured for use in FIPS 140-2 secure mode. In this example of configuration, we have chosen to present all the screens in the FIPS 140-2 mode. There are a few differences in non-FIPS mode which are described in the Navigation chart on page 8.

### Preliminary Configuration Steps

For preliminary installation the 3e-525A network administrator may need the following information:

- IP address – a list of IP addresses available on the organization's LAN that are available to be used for assignment to the AP(s)
- Subnet Mask for the LAN
- Default IP address of the 3e-525A
- DNS IP address
- SSID – an ID number/letter string that you want to use in the configuration process to identify all members of the wireless LAN.
- The MAC addresses of all the wireless cards that will be used to access the 3e-525A network of access points (if MAC address filtering is to be enabled)
- The appropriate encryption key for Static 3DES or Static AES if state-of-the-art key management will be used. Alternately, the appropriate WEP key.

## Initial Setup using the “Local” Port

Plug one end of an RJ-45 Ethernet cable to the LAN port of the 3e-525A (see page 11) and the other end to an Ethernet port on your laptop. This LAN port in the 3e-525A connects you to the device’s internal DHCP server which will dynamically assign an IP address to your laptop so you can access the device for reconfiguration. In order to connect properly to the 3e-525A on the LAN port, the TCP/IP parameters on your laptop must be set to “obtain IP address automatically.” (If you are unfamiliar with this procedure, use the following instructions for determining or changing your TCP/IP settings.)

In Windows 98/Me click **Start** → **Settings** → **Control Panel**. Find and double click the **Network** icon. In the **Network** window, highlight the TCP/IP protocol for your LAN and click the **Properties** button. Make sure that the radio button for **Obtain an IP address automatically** is checked.

In Windows 2000/XP, follow the path **Start** → **Settings** → **Network and Dialup Connections** → **Local Area Connection** and select the **Properties** button. In the **Properties** window, highlight the TCP/IP protocol and click **properties**. Make sure that the radio button for **Obtain an IP address automatically** is checked.

Once the DHCP server has recognized your laptop and has assigned a dynamic IP address, you will need to find that IP address. Again, the procedure is similar for Windows 95/98/Me machines and slightly different for Windows 2000/XP machines.

In Windows 98/Me, click **Start**, then **Run** and type **winipcfg** in the run instruction box. Then click **OK**. You will see the IP address of your laptop in the resulting window, along with the “default gateway” IP address. Verify that the IP address shown is 192.168.15.x

In Windows 2000/XP, click **Start**, then **Run** and type **cmd** in the run instruction box. Then click **OK**. This will bring up a window. In this window, type **ipconfig /all | more**. This will list information assigned to your laptop, including the IP address assigned. Verify that the IP address shown is 192.168.15.x

On your computer, pull up a browser window and put the default URL for the 3e-525A Local LAN in the address line. (<https://192.168.15.1>)



NOTE: be sure that you use the **https** prefix, not http.

You will be asked for your User Name and Password. The default is "CryptoOfficer" with the password "CryptoFIPS" to give full access for setup configuration. (This password is case-sensitive.)



## System Configuration

### General

You will immediately be directed to the **System Configuration—General** page for the 3e-525A access point.

This screen lists the firmware version number for your 3e-525A and allows you to set the Host Name and Domain Name as well as establish system date and time. (Host and Domain Names are both set at the factory for "default" but can optionally be assigned a unique name for each.) When you are satisfied with your changes, click **Apply**.

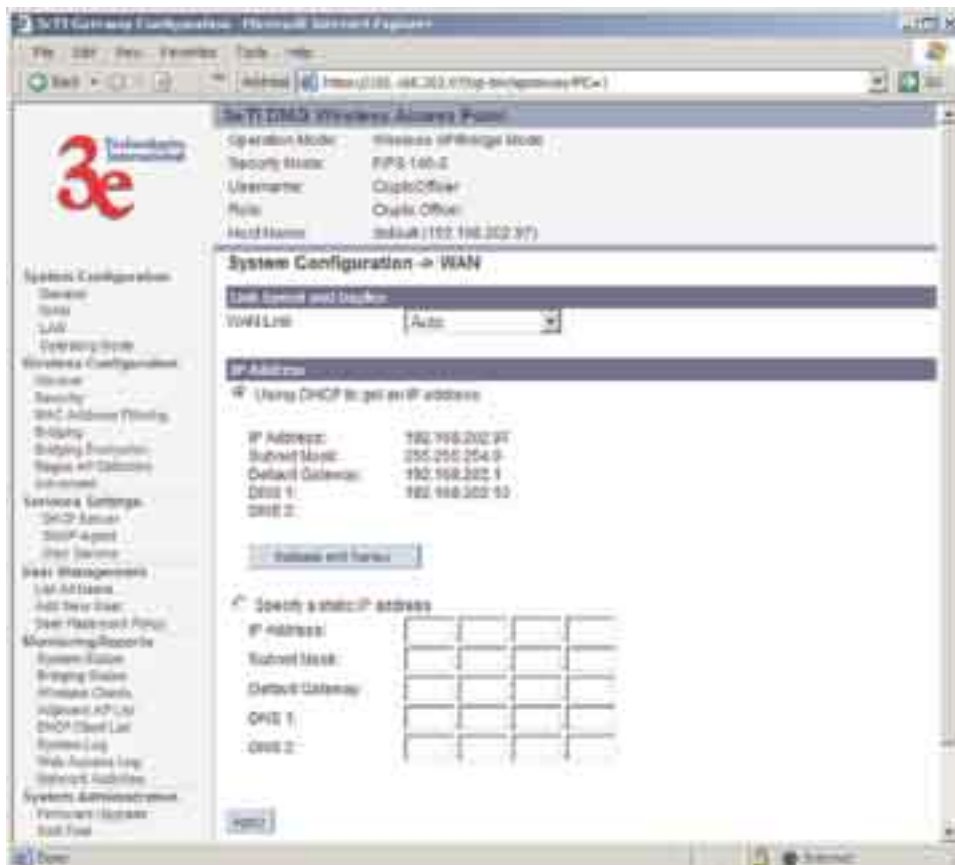




Go next to the **System Configuration—WAN** page.

## WAN

Click the entry on the left hand navigation panel for **System Configuration -WAN**. This directs you to the **System Configuration – WAN** page.



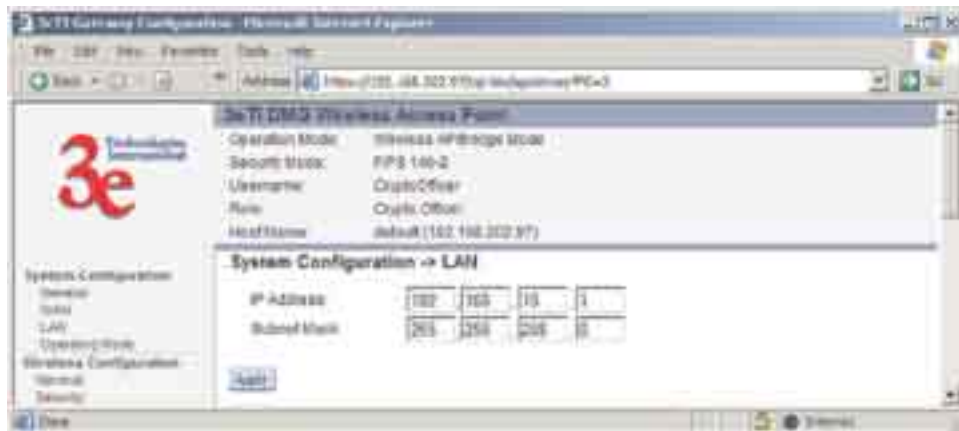
If not using DHCP to get an IP address, input the information that the

access point requires in order to allow the wireless devices it controls access to the wired LAN. This will be the IP address, Subnet Mask, Default Gateway, and, where needed, DNS 1 and 2.

Click **Apply** to accept changes.

## LAN

This sets up the default numbers for the four octets for a possible private LAN function for the access point. It also allows changing the default numbers for the LAN Subnet Mask. The Local LAN port provides local access for configuration. It is not advisable to change the private LAN address while doing the initial setup as you are connected to that LAN.



## Operating Mode

This screen allows you to set the operating mode to either Wireless Access Point/Bridging or Gateway mode. You only need to visit this page if you will be changing from Access Point to Gateway, or if you want to change your submode.

Note that if you change modes, all previously entered information will be reset to factory settings.

## Submodes

There are two options under Submodes:

- FIPS 140-2 Mode

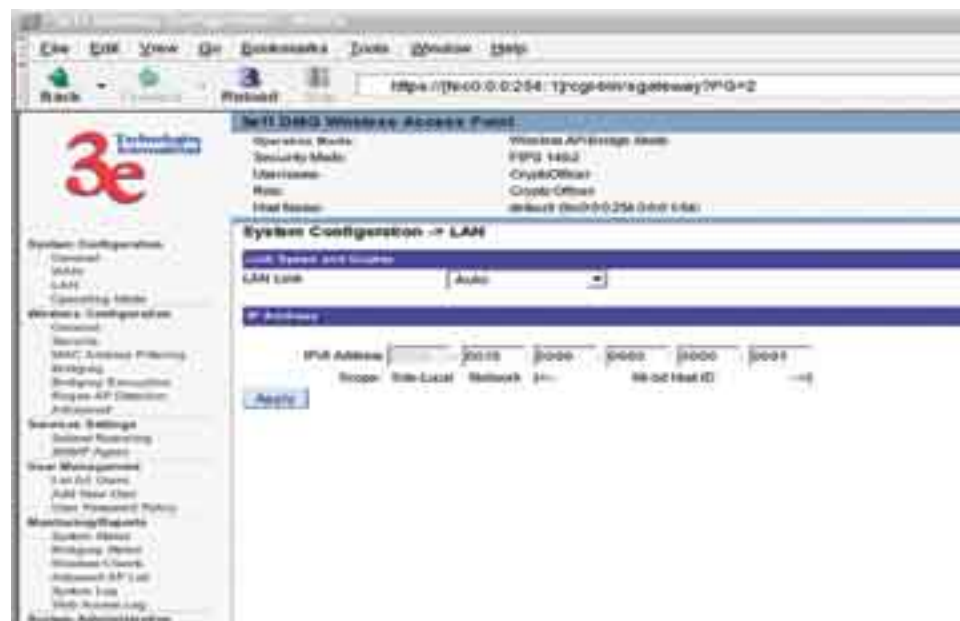
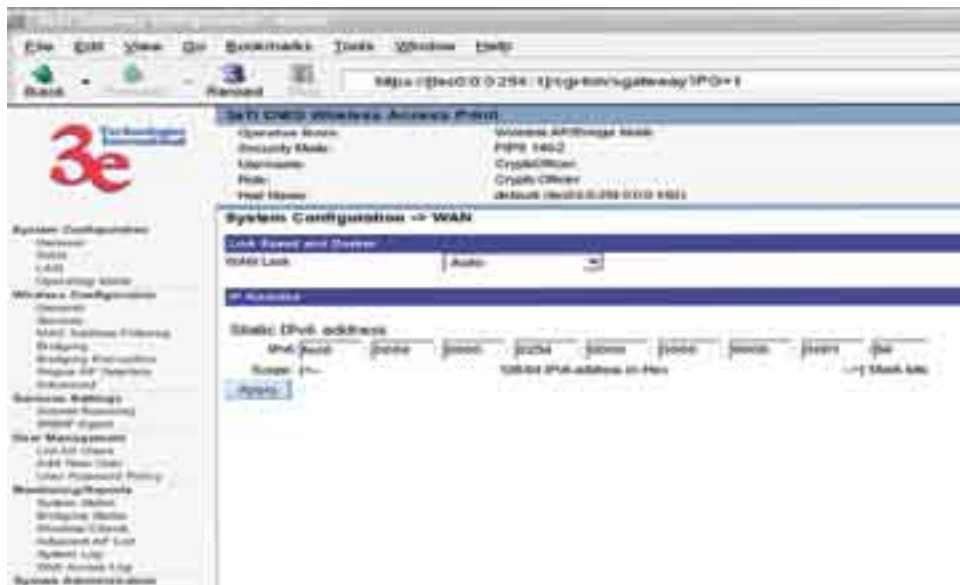


3e-525A Outdoor Access Point

- Use IPv6 Mode

If you can select the Use IPv6 Mode, the AP will be configured to support IPv6 addresses on the WAN and LAN ports. In IPv6 mode, the AP can be managed and pass traffic using IPv6 addresses. Since IPv6 is relatively new in the industry, some networking functions that cannot support IPv6 are disabled such as DHCP server and WPA-802.1x

If Use IPv6 mode is selected as a submode then you will need to enter a IPv6 address under System Configuration—WAN and LAN screens.



## Wireless Configuration

### General

Wireless Setup allows your computer's PC Card to talk to the access point. Once you have completed wireless configuration, you can complete the rest of the configuration wirelessly unless you will be employing the FIPS 140-2 secure mode, assuming that you have installed and configured a wireless PC card on your computer. (If you have not done so, you will have to do that to establish communications. Follow the manufacturer's instructions to set up the PC Card on each wireless device that will be part of the WLAN.)

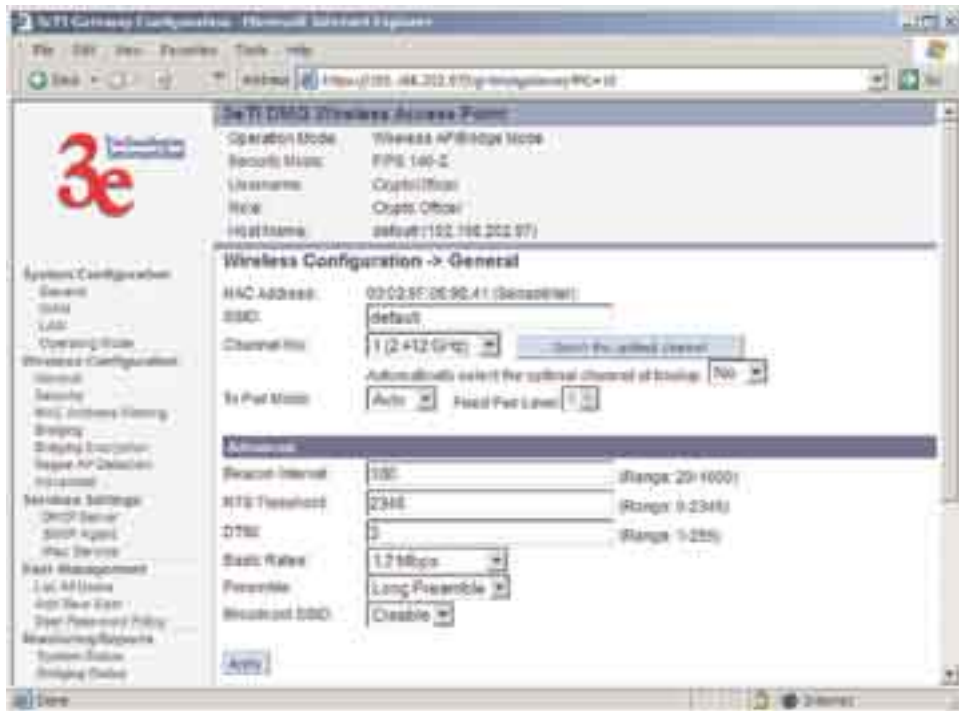


**WARNING:** If you are configuring this 3e-525A in FIPS 140-2 secure mode, your initial configuration will have to be accomplished through the LAN port due to the secure nature of the access point.

The **Wireless Configuration — General** page lists the MAC Address of the 3e-525A device. This is not the MAC Address that will be used for the BSSID for bridging setup, however. That is found on the Bridging page.

If you will be using an **SSID** for a wireless LAN, enter it here and in the setup of each wireless client. This nomenclature has to be set on the access point and each wireless device in order for them to communicate.

The Wireless Mode menu allows you to specify whether you want your AP to operate solely in the 802.11b band or in the 802.11g band or in a combination of the two. The 802.11b band will accommodate legacy systems. The 802.11g improves the wireless power but limits use to those WLANs that have only 802.11g clients. The 802.11 b/g mixed allows you to use both 802.11b and 802.11g clients but limits power to that of the 802.11b band.



You can assign a channel number to the AP (if necessary) and modify the Tx Pwr Mode.

The **Channel Number** is a means of assigning frequencies to a series of access points, when many are used in the same WLAN, to minimize interference. There are 11 channel numbers that may be assigned. If you assign channel number 1 to the first in a series, then channel 6, then channel 11, and then continue with 1, 6, 11, you will have the optimum frequency spread to decrease “noise.”

If you are using the WAB-1000 as both an AP and bridge, the channel number set for the AP board and the channel number set for the bridge should be sufficiently different to avoid interference. Generally, it has been found that selecting Channel 4 for Bridging and Channel 11 for AP gives a good spread.

If you click on the button **Select the optimal channel**, a popup screen will display the choices. This action does not select the channel for you but shows you what will most probably be the channel selected if you leave the following dropdown menu at **Yes**.

**Tx Pwr Mode and Fixed Pwr Level:** The Tx Power Mode defaults to Auto, giving the largest range of radio transmission available under normal conditions. As an option, the AP's broadcast range can be limited by setting the Tx Power Mode to Fixed and choosing from 1-8 for Fixed Pwr Level (1 being the shortest distance.) Finally, if you want to prevent any radio frequency transmission, set Tx Pwr Mode to **Off**.

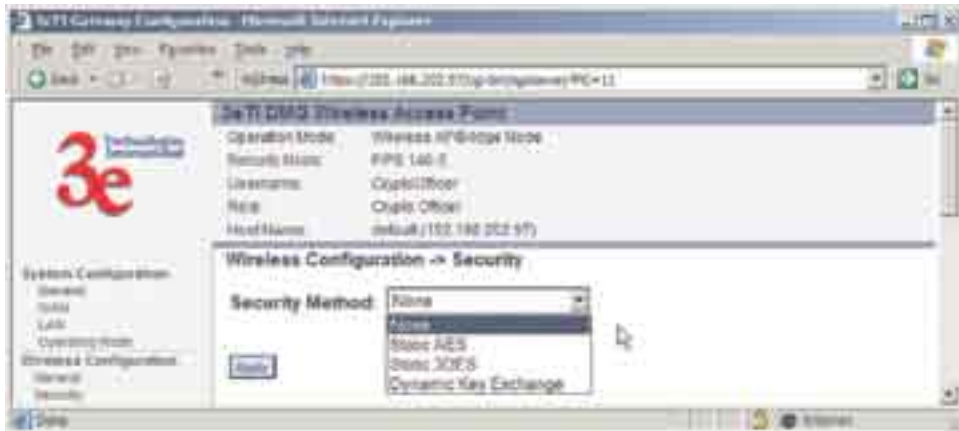
There are a number of advanced options included on this page as described in the following chart:

<b>Advanced Options</b>		
<b>Beacon interval</b>	0-4095	The frequency in milliseconds in which the 802.11 beacon is transmitted by the AP.
<b>RTS Threshold</b>	0-3000	The number of bytes used for the RTS/CTS handshake boundary. When a packet size is greater than the RTS threshold, the RTS/CTS handshaking is performed.
<b>Fragmentation</b>	256-2346 even only	Fragmentation boundary in bytes.
<b>DTIM</b>	1-65535	The number of beacon intervals between successive Delivery Traffic Identification Maps (DTIMs). This feature is used for Power Save Mode.
<b>Basic Rates</b>	<b>Basic Rates for 802.11b</b>	
	- 1 and 2 Mbps - 1, 2, 5.5 and 11 Mbps	The basic rates used and reported by the AP. The highest rate specified is the rate that the AP uses when transmitting broadcast/multicast and management frames.
	<b>Basic Rates for 802.11g or 802.11b/g mixed</b>	
	- 1 and 2 Mbps - 1, 2, 5.5, 11, 12, and 24 Mbps	The basic rates used and reported by the AP. The highest rate specified is the rate that the AP uses when transmitting broadcast/multicast and management frames.
<b>Supported Rates</b>	<b>Supported Rates for 802.11b</b>	
	All Rates 1 Mbps 2 Mbps 5.5 Mbps 11 Mbps	The rate at which all data frames will be transmitted
	<b>Supported Rates for 802.11g or 802.11b/g mixed</b>	
	All Rates 1 Mbps 2 Mbps 5.5 Mbps 11 Mbps 12 Mbps 18 Mbps 24 Mbps 36 Mbps 48 Mbps 54 Mbps	The rate at which all data frames will be transmitted
<b>Preamble</b>	Short/Long Preamble	Specifies whether frames are transmitted with the Short or Long Preamble
<b>Broadcast SSID</b>	Enabled/disabled	When disabled, the AP hides the SSID in outgoing beacon frames and stations cannot obtain the SSID through passive scanning. Also, when it is disabled, the AP doesn't send probe responses to probe requests with unspecified SSIDs.

## Security

The 3e-525A will display a default factory setting of no encryption, but for security reasons will not communicate to any clients unless the encryption is set by the administrator. There will be different encryption options for the AP in FIPS Mode and the non-FIPS Mode. The following chart shows the differences:

Encryption Options on the 3e-525A	
In FIPS 140-2 Mode	In non-FIPS AP Mode
None	None
Static AES (AES-ECB)	Static WEP
Static 3DES	WPA (Preshared Key or 802.1x using Radius Server, and TKIP or AES-CCMP)
Dynamic Key Exchange (with 3e-030 Security Server, purchased separately)	



In the following explanations, the FIPS Mode security options are discussed first.

### **No Encryption**

In order to the 3e-525A with no encryption, you must actively select **None** and click **Apply**. A screen will appear, asking if you really want to operate in Bypass mode. If you answer **Yes**, no encryption will be applied.

### Static AES Key

The Advanced Encryption Standard (AES) was selected by National Institute of Standards and Technology (NIST) in October 2000 as an upgrade from the previous DES standard. AES uses a 128-bit block cipher algorithm and encryption technique for protecting computerized information. With the ability to use even larger 192-bit and 256-bit keys, if desired, it offers higher security against brute-force attack than the old 56-bit DES keys. The specific AES algorithm authorized for use in FIPS 140-2 mode is AES-ECB.



### Static 3DES Key

To use 3DES, enter a 192-bit key as 48 hexadecimal digit (0-9, a-f, or A-F).

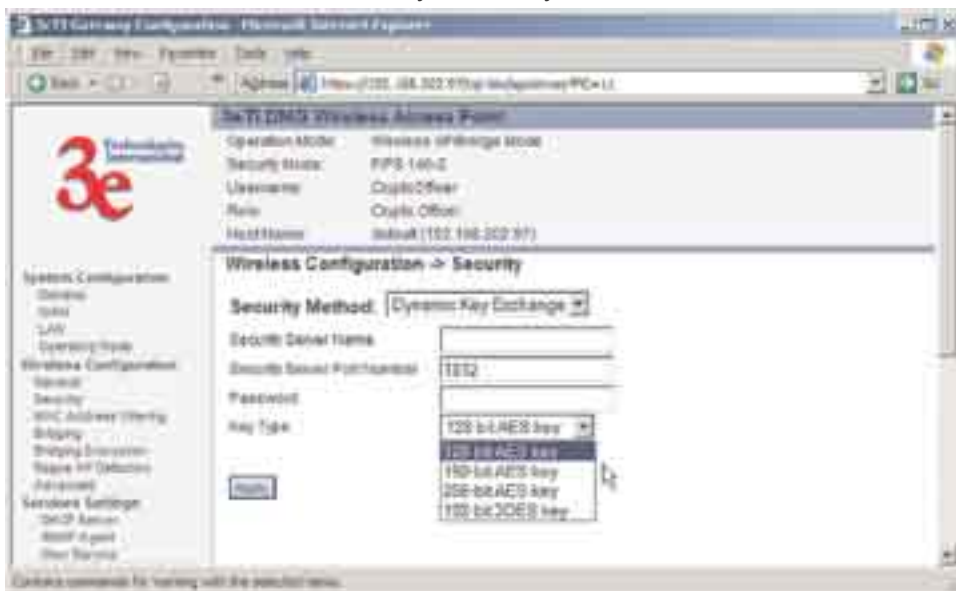


### Dynamic Key Exchange



Dynamic key management requires the installation of the 3e-030 Security Server software which resides on a self-contained workstation connected to the 3e-525A over the WAN port. The Security Server software configuration includes: obtaining a root certificate from a Certificate Authority (CA) like Microsoft; obtaining user certificates based on the CA which will be used by the clients; and configuring the 3e Technologies International's Security Server software with the appropriate root certificate. The Security Server software application is discussed in a separate manual.

If you have installed the Security Server software, Dynamic Key Management is the preferred security setup. Get the IP Address and password of the Security Server and the Key type. Key type will be either 3DES (192-bit), or AES (128-bit, 192-bit or 256-bit). Thereafter, the Security Server handles authentication dynamically.



Once you have selected the options you will use, click **Apply**.

If you have the 3e-525A configured in non-FIPS mode, the security screens will look a bit different.

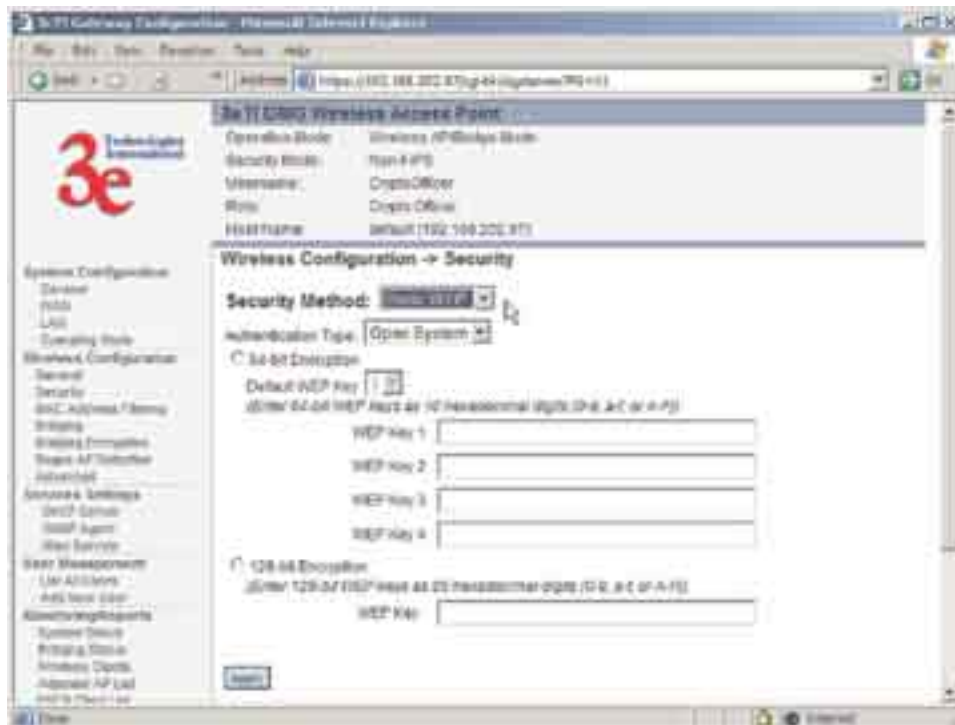
### ***No Encryption (non-FIPS)***

In order to the 3e-525A with no encryption, you must actively select **None** and click **Apply**. A screen will appear, asking if you really want to operate in Bypass mode. If you answer **Yes**, no encryption will be applied.



### **Static WEP Encryption (non-FIPS)**

If you choose to use WEP encryption, you can also select whether it will be Open System or Shared Key authentication. For greater security, set authentication type to "shared key." WEP Data encryption can be set to 40-bit or 128-bit encryption.



WEP (Wired Equivalent Privacy) Encryption is a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP was originally designed to provide the same level of security for wireless LANs as that of a wired LAN but has come under attack for its defaults and is not now state of the art. WEP relies on the use of identical static keys deployed on client stations and access points. But the use of

WEP encryption provides some measure of security.

Utilities exist for scanning for networks and logging all the networks it runs into—including the real SSIDs, the access point's MAC address, the best signal-to-noise ratio encountered, and the time the user crossed into the network's space. These utilities can be used to determine whether your network is unsecured. Note that, if WEP is enabled, that same WEP key must also be set on each wireless device that is to become part of the wireless network, and, if "shared key" is accepted, then each wireless device must also be coded for "shared key". To use WEP encryption, identify the level of encryption, the Default WEP key and designate the WEP keys as shown on the screen.

### WPA (non-FIPS)

Wi-Fi Protected Access or WPA was designed to enable use of wireless legacy systems employing WEP while improving security. WPA uses improved data encryption through the temporal key integrity protocol (TKIP) which scrambles keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. In addition, user authentication is enabled using the extensible authentication protocol (EAP).



WPA is an interim standard that will be replaced with the IEEE's 802.11i standard upon its completion. However, it is expected to remain

compatible. For those organizations already making the transition to the new AES algorithm, WPA uses a form of AES (AES-CCMP) agreed-upon by the WiFi Alliance 802.11i working team.

If you wish to use WPA on the 3e-525A, enable either WPA Pre-shared Key Settings or WPA 802.1x Settings.

If you are a SOHO user, selecting pre-shared key means that you don't have the expense of installing a Radius Server. Simply input up to 63 character / numeric / hexadecimals in the Passphrase field. If your clients use WPA-TKIP, select TKIP as encryption type. If your clients use WPA-AES, select AES-CCMP. If a combination, select AUTO.

For highest security, select the lowest re-keying interval.

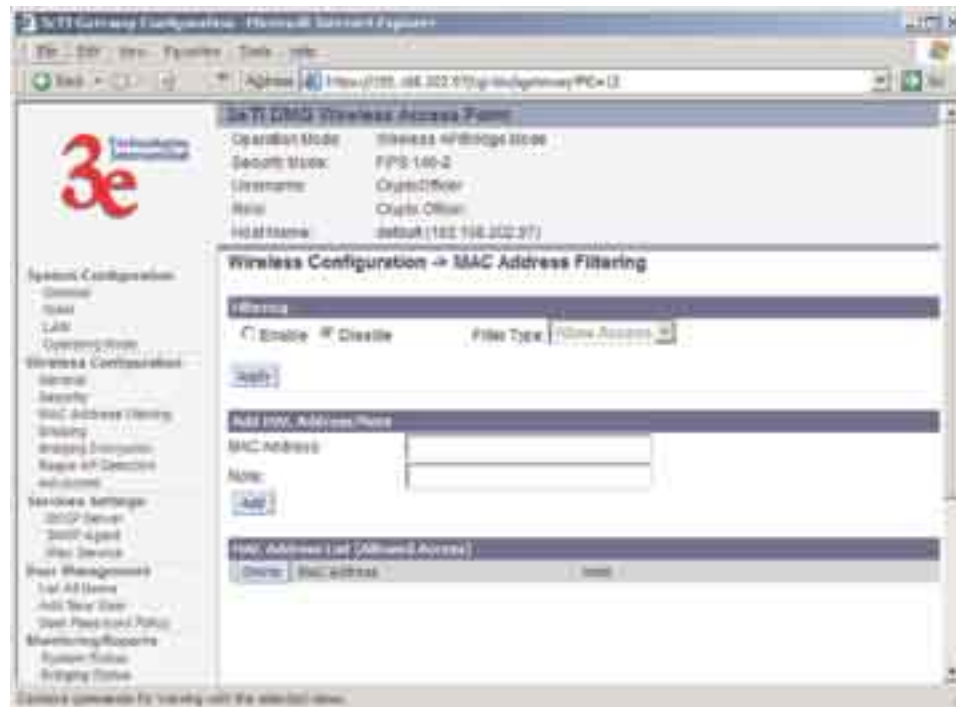
As an alternative, for business applications who have installed Radius Servers, select WPA 802.1x and input the Primary and Backup Radius Server settings. Use of Radius Server for key management and authentication requires that you have installed a separate certification system and each client must have been issued an authentication certificate.

Once you have selected the options you will use, click **Apply**.

If you will be using MAC Address filtering, navigate next to the MAC Address Filtering page.

### MAC Address Filtering

The factory default for MAC Address filtering is **Disabled**. If you enable MAC Address filtering, you should also set the toggle for **Filter Type**.



This works as follows:

- If **Filtering** is enabled and **Filter Type** is **Allow Access**, only those devices equipped with the authorized MAC addresses will be able

to communicate with the access point. In this case, input the MAC addresses of all the PC cards that will be authorized to access this access point. The MAC address is engraved or written on the PC (PCMCIA) Card.

- If **Filtering** is enabled and **Filter Type** is **Disallow Access**, those devices with a MAC address which has been entered in the MAC Address listing will NOT be able to communicate with the access point. In this case, navigate to the report: **Wireless Clients** and copy the MAC address of any Wireless Client that you want to exclude from communication with the access point and input those MAC Addresses to the MAC Address list.

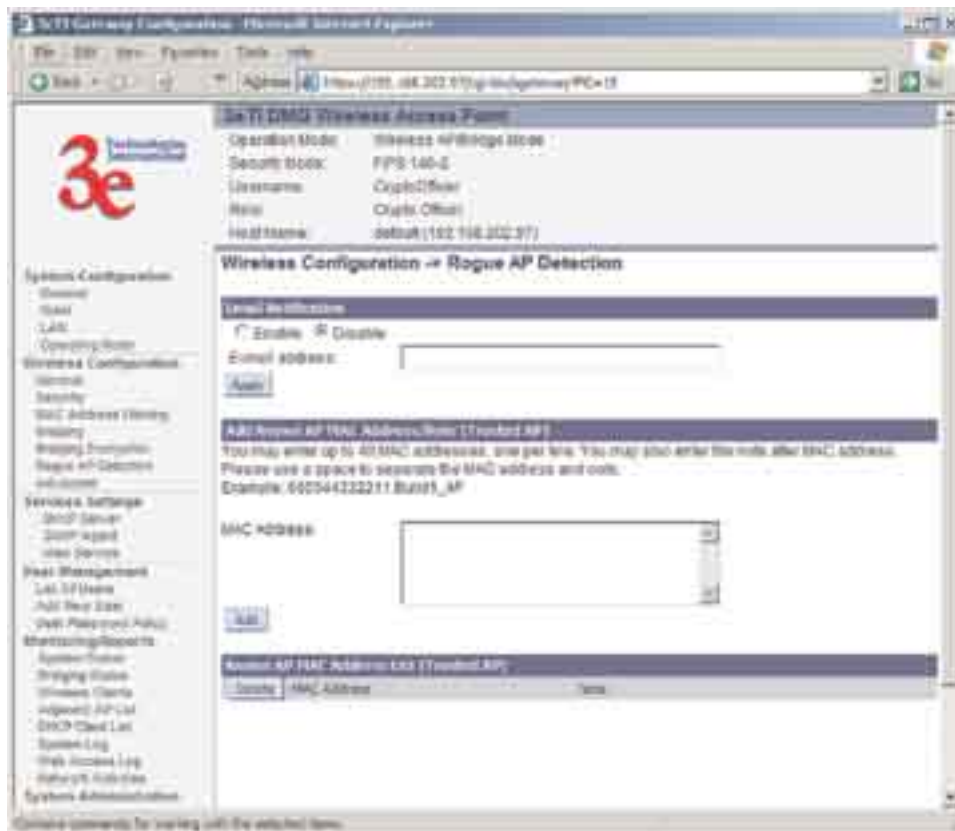
### Bridging and Bridging Encryption

Bridging is covered in chapter five. If you will be deploying this 3e-525A as a bridge, follow the instructions in chapter five.

### Rogue AP Detection

The Rogue AP Detection page allows the network administrator to set up rogue AP detection. If you enable rogue AP detection, also enter the MAC Address of each AP in the network that you want the AP being configured to accept as a trusted AP. (You may add up to 20 APs.) Enter an email address for notification of any rogue or non-trusted APs. (The MAC Address for the 3e-525A is located on the **Setup—General** page.

The **Rogue AP list**, under **Monitoring Reports** on the navigation menu, will detail any marauding APs.



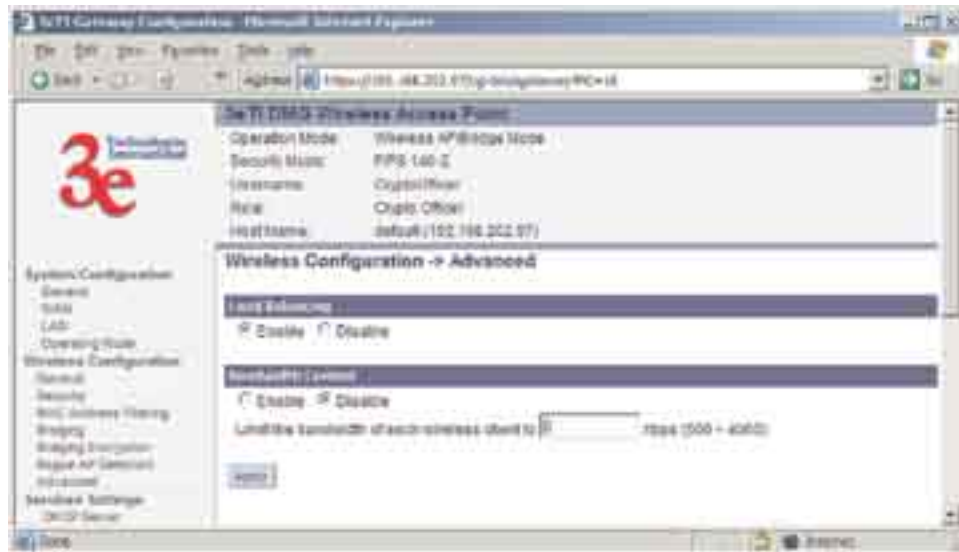
## Advanced

The Advanced page allows you to enable or disable load balancing and to control bandwidth.

Load balancing is enabled by default. Load balancing distributes traffic efficiently among network servers so that no individual server is overburdened. For example, the load balancing feature balances the wireless clients between APs. If two APs with similar settings are in a conference room, depending on the location of the APs, all wireless clients could potentially associate with the same AP, leaving the other AP unused. Load balancing attempts to evenly distribute the wireless clients on both APs.

If enabled, the Bandwidth Control function works by limiting the maximum bandwidth a single client is allowed to have. For example, if the total BW for the AP/WLAN is 4 Mbps and BW control is set to 500 kbps or 0.5 Mbps, the network can only serve a maximum of 0.5 mbps per client. Even if only one client is on the network, a maximum of 0.5 Mbps will be allowed. If, on the other hand, the BW Control is set to a higher number (say 3 Mbps), a single client can take up to 3 Mbps of bandwidth when it requires while the other clients will share the remaining bandwidth. The decision as to who gets the 3 Mbps and who gets the remainder depends on the requirement and when the requirement is acknowledged. This function can be disabled and the available bandwidth will be portioned out as required. If total bandwidth required exceeds the available bandwidth, the client last in line will get only the remaining bandwidth available.

Once you have made any changes, click **Apply** to save.



## Services Settings

### DHCP Server

This page allows configuration of the DHCP server function accessible from the Local LAN port. The default factory setting for the DHCP server function is enabled. You can disable the DHCP server function, if you

wish. You can also set the range of addresses to be assigned. The Lease period (after which the dynamic address can be reassigned) can also be varied.



The DHCP server function, accessible only from the LAN port, is used for initial configuration of the management functions.

## SNMP Agent

The SNMP Agent setup page (shown on the previous page) allows you to set up an SNMP Agent. The agent is a software module that collects and stores management information for use in a network management system. The 3e-525A's integrated SNMP agent software module translates the device's management information into a common form for interpretation by the SNMP Manager, which usually resides on a network administrator's computer.

The SNMP Manager function interacts with the SNMP Agent to execute applications to control and manage object variables (interface features and devices) in the gateway. Common forms of managed information include number of packets received on an interface, port status, dropped packets, and so forth. SNMP is a simple request and response protocol, allowing the manager to interact with the agent to either

- **Get** - Allows the manager to **Read** information about an object variable
- **Set** - Allows the manager to **Write** values for object variables within an agent's control, or
- **Trap** - Allows the manager to **Capture** information and send an alert about some pre-selected event to a specific destination

The SNMP configuration consists of several fields, which are explained below:

- **Community** –The Community field for Get (Read Only), Set



(Read & Write), and Trap is simply the SNMP terminology for “password” for those functions.

- **Source** –The IP address or name where the information is obtained.
- **Access Control** –Defines the level of management interaction permitted.

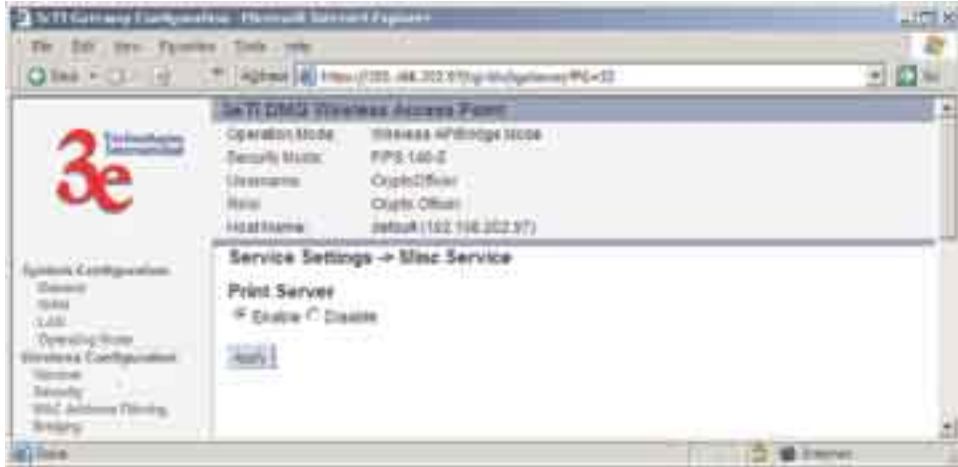
## Misc Services

### *Print Server*

The print server function can be enabled or disabled. It is enabled by default. If you do not plan to set up the print server function, you can click disable.



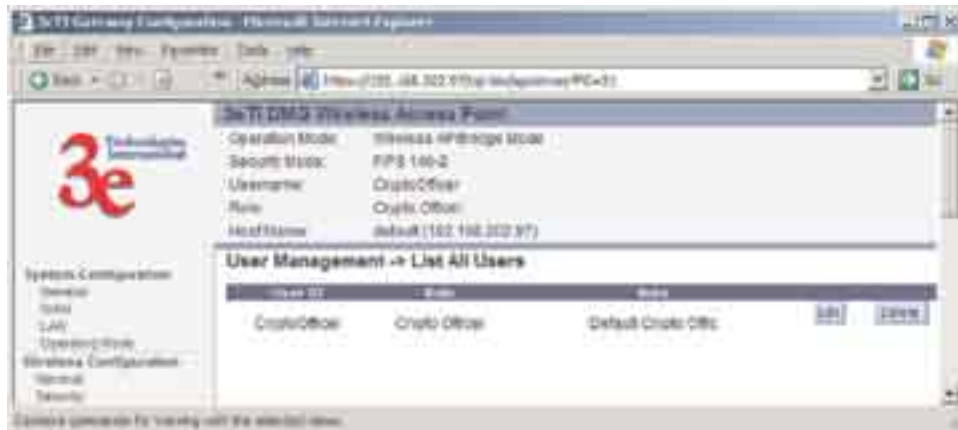
3e-525A Outdoor Access Point



## User Management

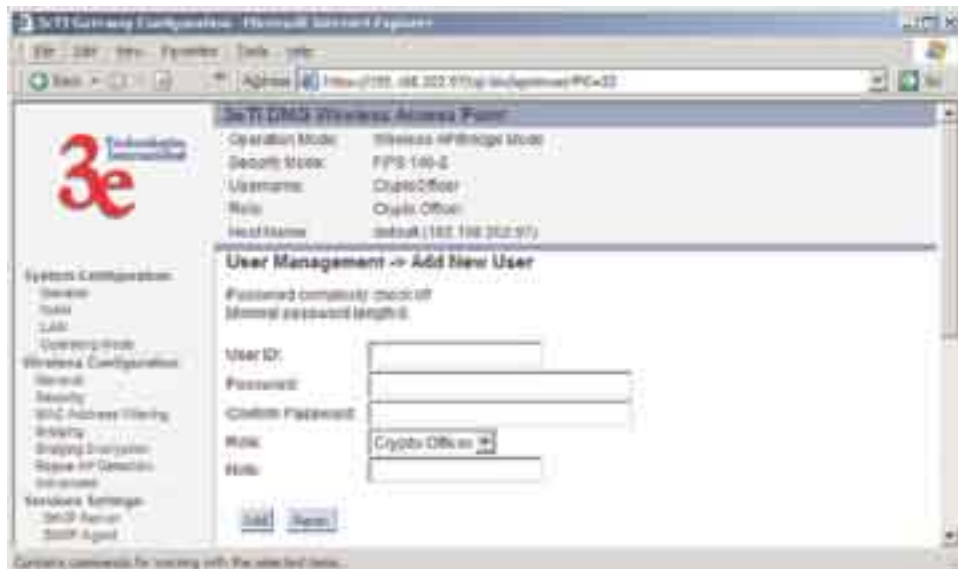
### List All Users

The **List All Users** page simply lists the Crypto Officer and all administrator accounts configured for the unit.



### Add New User

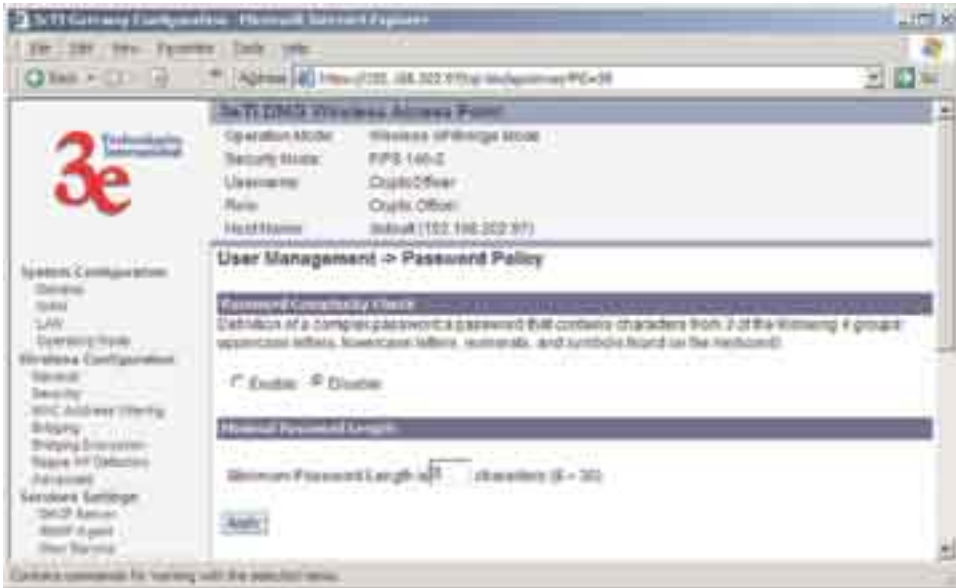
The **Add New User** screen allows you to add new Administrators, assigning and confirming the password for the administrator



The screen shown above is the screen as it will appear in FIPS 140-2 mode. The **Password complexity check off** and the **Minimal Password length** are established on the **User Management — Password Policy** page.

### Password Policy (FIPS Mode Only)

The Password Policy screen allows you to enable a Password Complexity Check when you are in FIPS 140-2 mode. The definition of a complex password is a password that contains characters from 3 of the following 4 groups: uppercase letters, lowercase letters, numerals, and symbols. If enabled, you must also select minimum password length. Click **Apply** to save your selection.

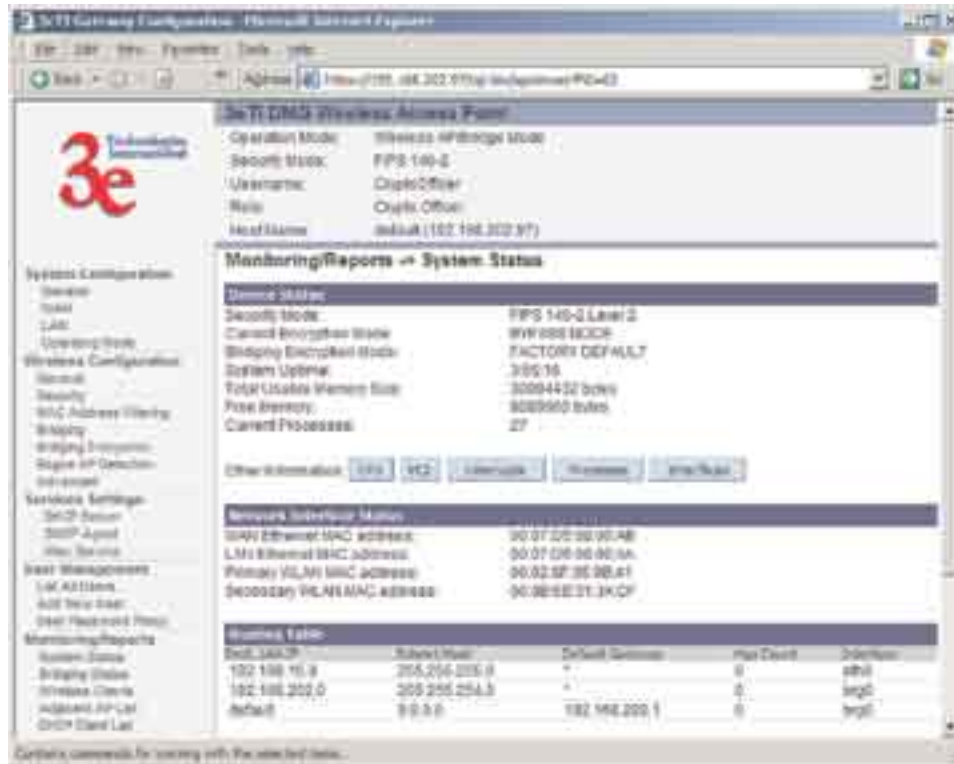


### Monitoring/Reports

This section gives you a variety of lists and status reports. Most of these are self-explanatory.

#### System Status

This screen displays the status of the 3e-525A Device and Network Interface Details and the Routing Table.



There are some pop-up informational menus that give detailed information about **CPU, PCI, Interrupts, Process, and Interfaces**.

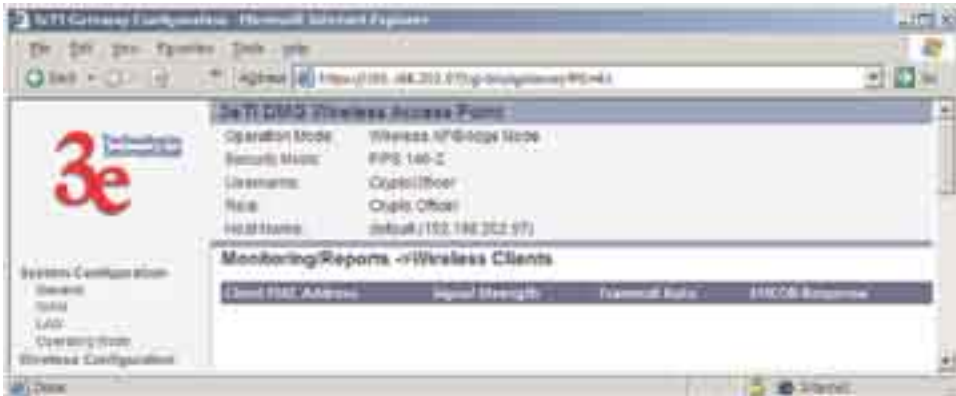
### **Bridging Status**

This screen displays the Ethernet Port STP Status, Wireless Port STP Status, and Wireless Bridging Information.



### Wireless Clients

The Wireless Clients report screen displays the MAC Address of all wireless clients and their signal strength and transmit rate. The screen shown here emulates the FIPS 140-2 setup and contains a column for EM-CON response. The non-FIPS mode doesn't display this column.



If Transmit power is disabled, either by setting TX Pwr Mode to Off on the management screen or by using the RF Manager (Chapter 7), the Wireless Clients page will show the results from each associated client in the EMCON Response column. If the client responds to the "disable" command, a **Yes** is displayed. If the column contains a **No**, this can mean either:

- the client didn't receive the command, or
- the client is no longer in the areas, or
- the client software doesn't support the RF management feature.

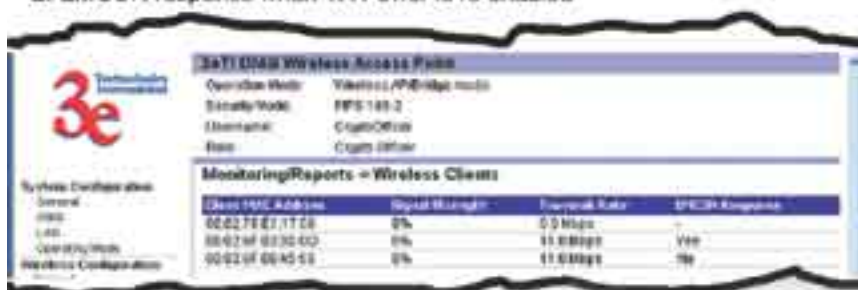
1. EMCON response when TX Power is disabled



This status information remains active for 5 minutes after the clients are disabled.

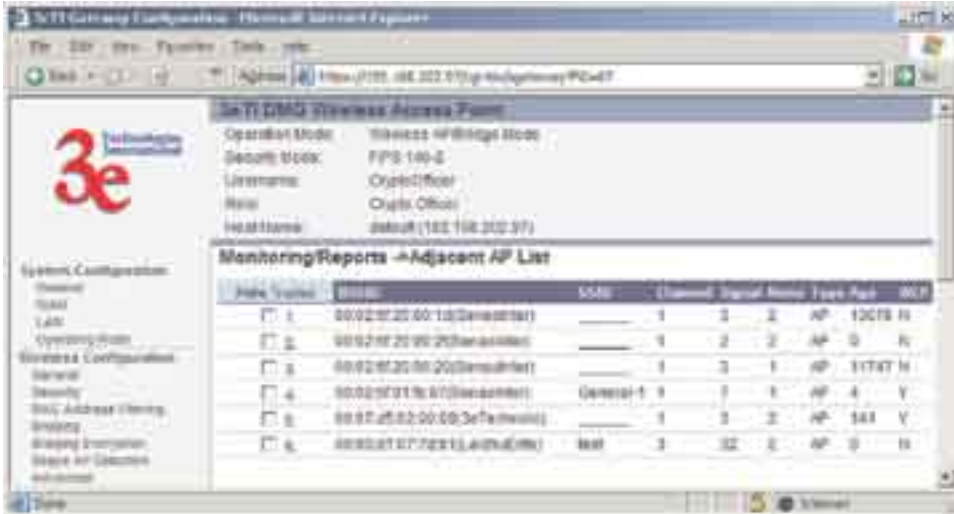
Once the transmit power is re-enabled and clients re-associate to the AP, EMCON information is maintained for them. If a new client that wasn't associated previously associates with the AP after the EMCON mode, its EMCON status appears as "-", which indicates the status record is not applicable.

2. EMCON response when TX Power is re-enabled



## Adjacent AP List

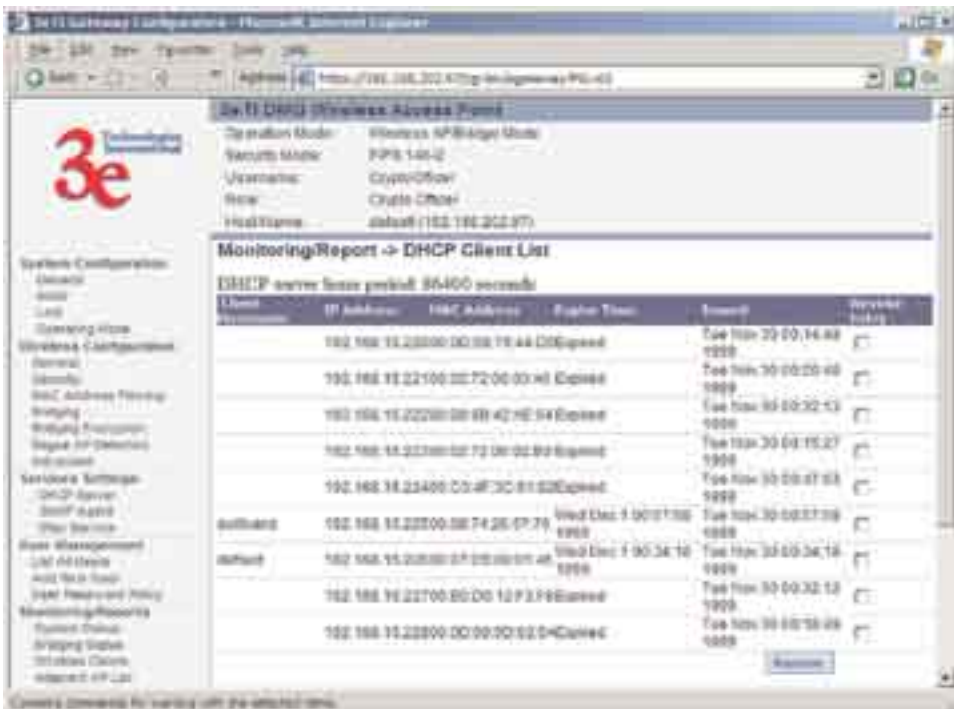
The **Adjacent AP** list shows all the APs on the network which are not seen by the subject AP as trusted clients. If you select the check box next to any AP shown and click the **Make Trusted** button, the AP will thereafter be accepted by the 3e-525A as a trusted AP.



## DHCP Client List

The DHCP client list displays all clients currently connected to the 3e-525A via DHCP server, including their hostnames, IP addresses, and MAC Addresses.

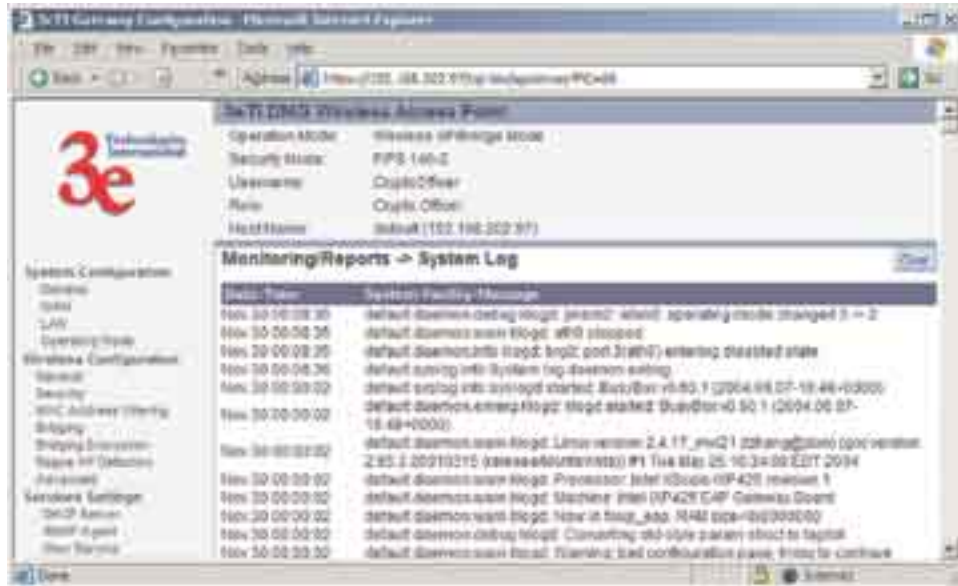
The DHCP Client list will continue to collect entries. To remove entries from the list, check mark the **Revoke Entry** selection and click **Remove** to confirm the action.



## System Log

The system log displays system facility messages with date and time stamp. These are messages documenting functions performed internal to the system, based on the system's functionality. Generally, the Administrator would only use this information if trained as or working with a field engineer or as information provided to technical support.

The System log will continue to accumulate listings. If you wish to clear listings manually, use the **Clear** button.

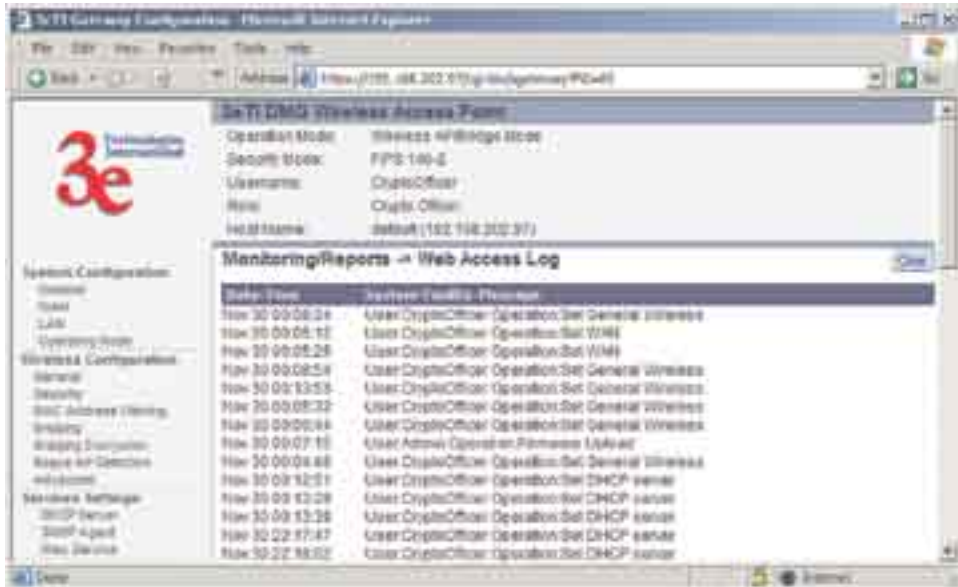


## Web Access Log

The Web Access Log displays system facility messages with date and time stamp for any actions involving web access. For example, this log records when you set encryption mode, change operating mode, etc., using the web browser. It establishes a running record regarding what actions were performed and by whom.

The Web access log will continue to accumulate listings. If you wish to clear listings manually, use the **Clear** button.

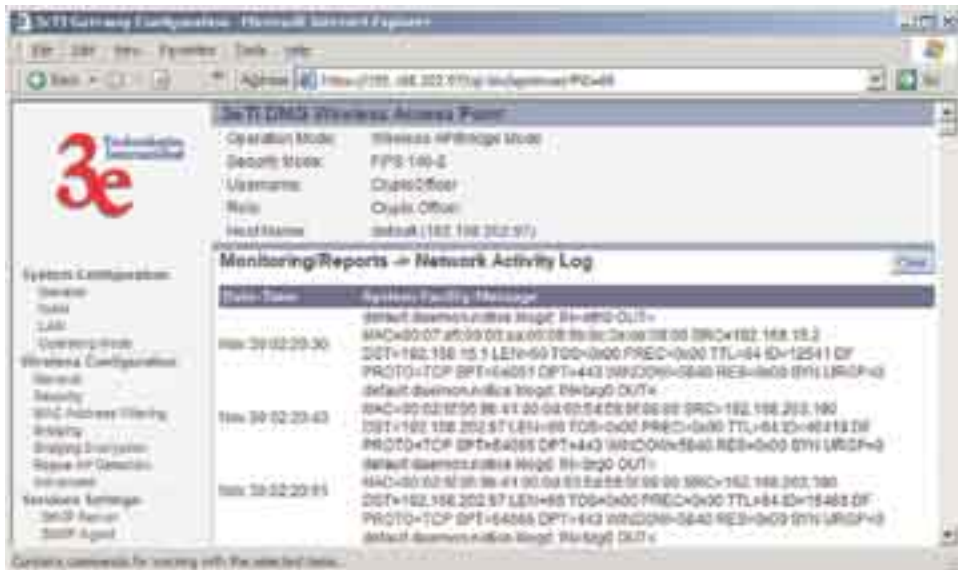




### Network Activity

The Network Activity Log keeps a detailed log of all activities on the network which can be useful to the network administration staff.

The Network Activities log will continue to accumulate listings. If you wish to clear listings manually, use the **Clear** button.

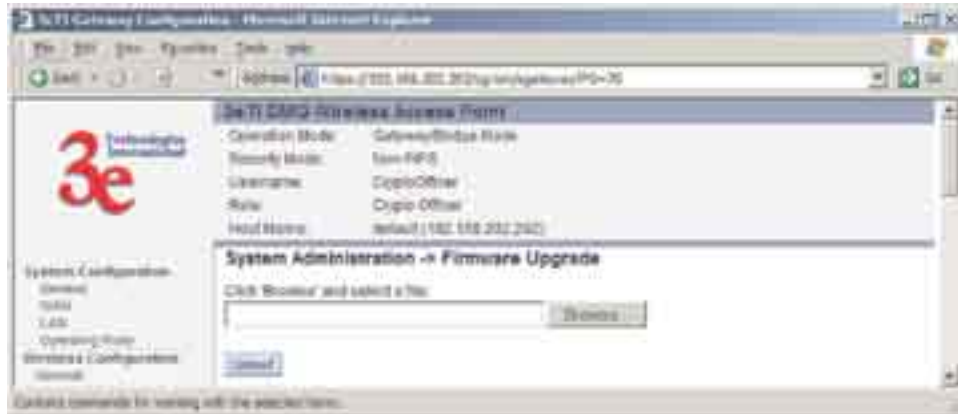


## System Administration

The System administration screens contain administrative functions. The screens and functions are detailed in the following section.

### Firmware Upgrade

The System Upgrade utility is a functionality built into the 3e-525A for updates to the device's firmware as they become available. When a new upgrade file becomes available, find it and upload it to the 3e-525A from this page.



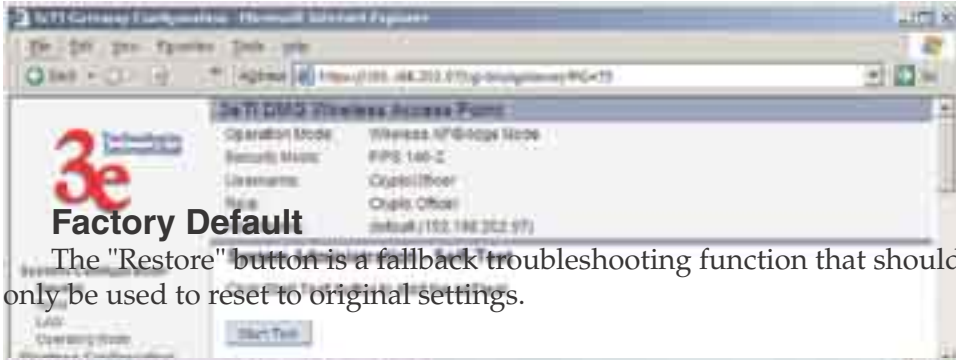
### Self-Test

Both Crypto Officer and Administrator functions can access the self-test functions. Self-tests are mandated by FIPS 140-2 and should be employed if you are operating in FIPS 140-2 mode. These include both power-up tests (such as cryptographic algorithm tests, software/firmware integrity tests, and critical function tests) and conditional tests. The 3e-525A self-test suite includes: AES, 3DES, SHA-1 Algorithms, Random Number Generation, Diffie-Hellman for Dynamic Key Exchange, RSA, and HMAC SHA-1 Algorithm for firmware verification.

If you want to perform a self-test, click on the **start test** button. A warning message will appear, stating "If self test fails, the system will halt. Proceed?" Click **OK**. If there are no errors, the browser will display the message: "Self test completed successfully. Hit **Back**."

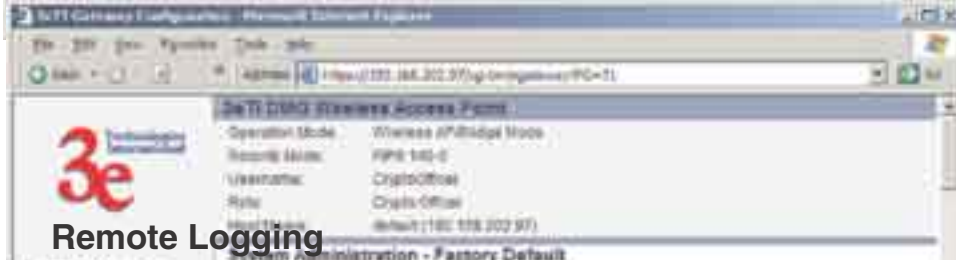
If there are errors, the 3e-525A will cease functioning. The device will emit a low-frequency beep for about 1 second. To exit the **Error State**, you must power down and power up by disconnecting the PoE cable.

The 3e-525A will then perform normal power up tests. If the **Error State** fails to clear, you must replace the device and return it to the manufacturer for servicing.



### Factory Default

The "Restore" button is a fallback troubleshooting function that should only be used to reset to original settings.



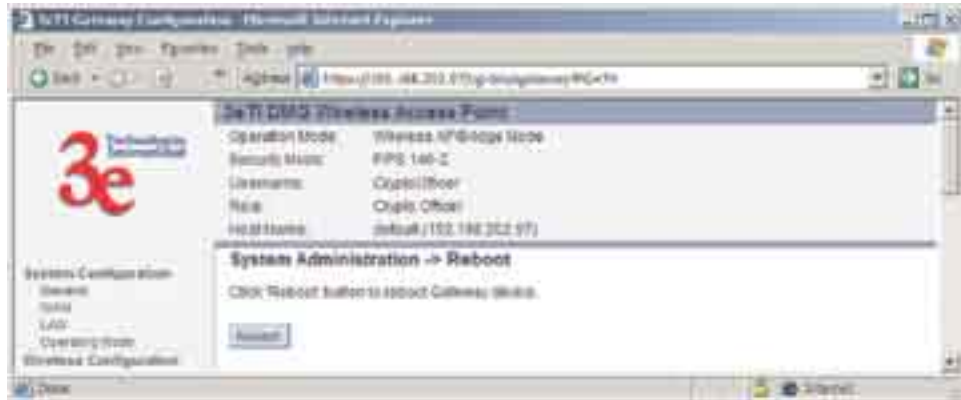
### Remote Logging

Remote logging allows you to forward the syslog data from each machine to a central remote logging server. In the 3e-525A, this function uses the `syslogd` daemon. You can find more information about `syslogd` by searching for "syslogd" in an Internet search engine (such as Google®) to find a version compatible with your operating system. If you enable Remote Logging, input a System Log Server IP Address and System Log Server Port. Click **Apply** to accept these values.



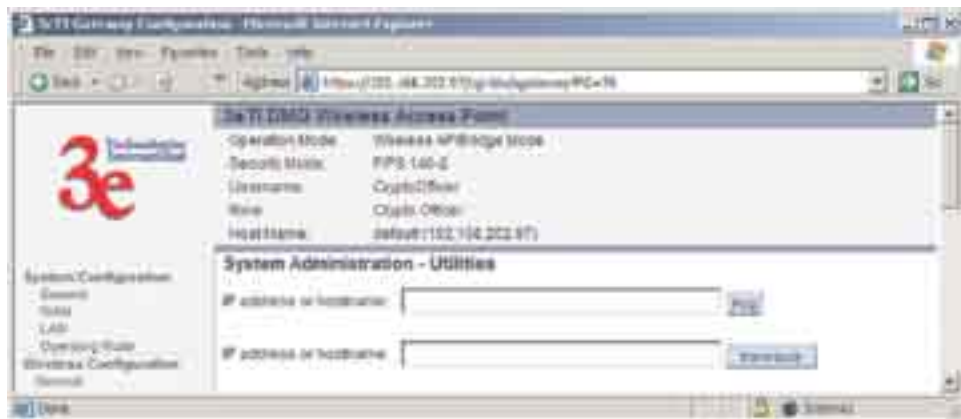
## Reboot

The Reboot utility allows you to reboot the 3e-525A without changing any preset functionality.



## Utilities

This screen gives you ready access to two useful utilities: Ping and Traceroute. Simply enter the IP Address or hostname you wish to ping or traceroute and click either the **Ping** or **Traceroute** button, as appropriate.



This page intentionality left blank.

## Chapter 4: Gateway Configuration

### Introduction

Chapter 3 covered the default configuration of the 3e-525A Wireless Access Point as an access point, for use as part of a host wired network. This chapter covers configuration as a gateway.

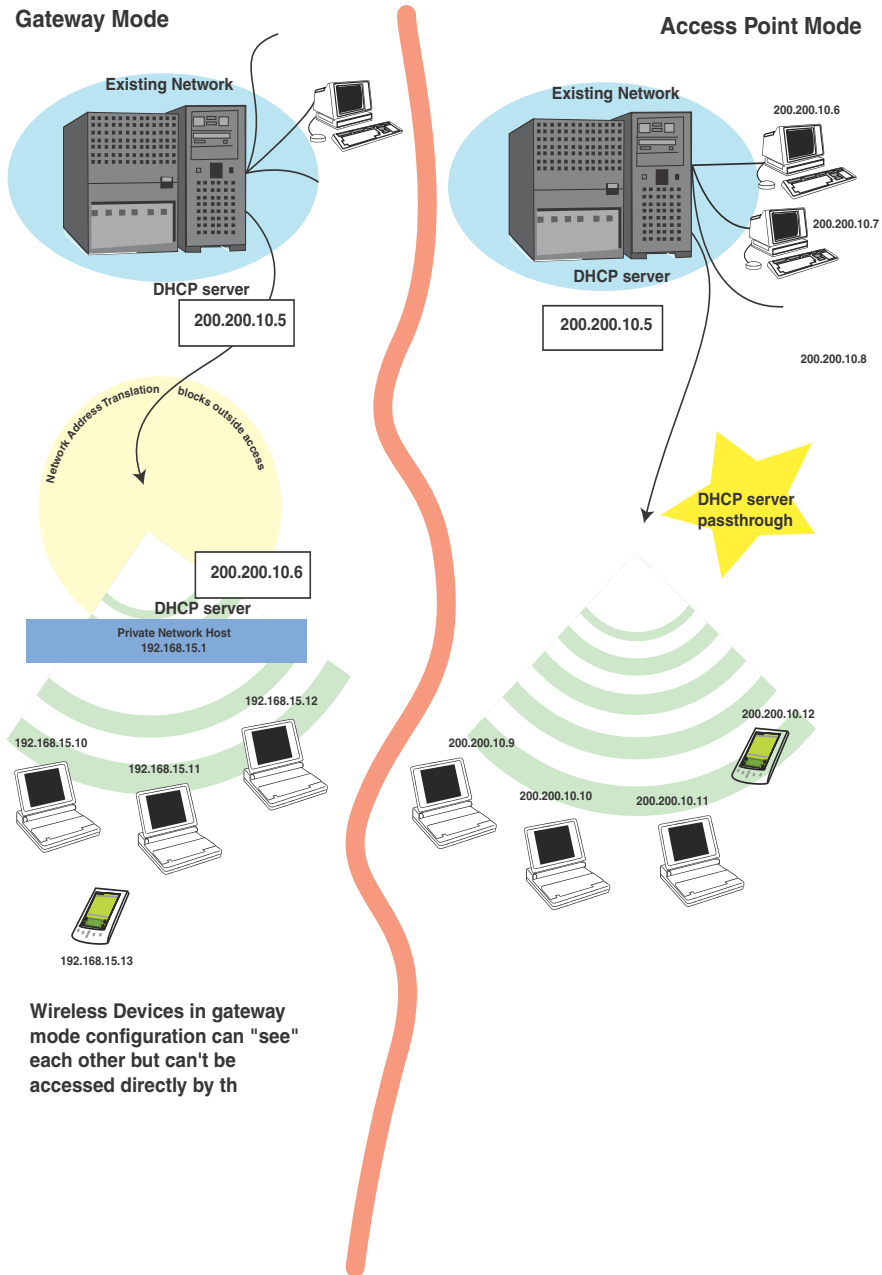
If additional security for the wireless network is desired (differentiating it from the wired network to which it is connected), set it up in gateway mode. Gateway mode takes advantage of some built-in “router” functions, such as the gateway’s ability to do Network Address Translation (NAT), providing private IP addresses for the wireless clients.

A 3e-525A AP set up in gateway mode can initiate wireless communications to the wired network but the wired network can’t initiate communications to the wireless network unless a specific network address has been assigned and the user on the wired network knows that address.

The illustration on the following page diagrams the difference.

**Caution:** If you have previously set up your WLAN using the 3e-525A AP devices as access points and you decide to change the configuration to gateway mode, you will need to convert the MAC addresses on each wireless device that has been set up so they can be seen by the reconfigured system. This is accomplished by the following procedure, done on each device that was configured to use the 3e-525A AP when the system was set up as an access point system. Pull up a System Prompt (“c:\” prompt, also called an MSDOS prompt) on the wireless device’s desktop. type: arp -d and hit return. This reconfigures the MAC address in the wireless device’s PC card so that it is now visible to the gateway.

### A comparison of gateway and access point setup for the 3e-525A AP



## Configuring in Gateway Mode

To configure the 3e-525A AP in gateway mode, complete the following steps.

Open a web browser on your monitor (using Netscape Navigator 3.0 or better or Internet Explorer 4.0 or better) and type in the default IP address of the gateway on its WAN port (for example, https://192.168.254.254). If you have changed the LAN address of the 3e-525A AP, then you will need to enter the LAN network address with a station address of .1. For example if the LAN address was changed to 10.0.0, then you would enter "https://10.0.0.1".



Then click **Go** on the Web browser.

You will be asked for your user name and password. You will need to have the ID and password for the Crypto Officer role to change the mode from access point to gateway. If that has not yet been changed, use the default "CryptoOfficer" with the password "CryptoFIPS" to allow full access. Click on **OK** and you will be directed to the **System Configuration – General** page.



Using the navigation bar to the left, navigate to the **System Configuration — Operating Mode** page, select the **Gateway Mode** radio button, and click **Apply**. The 3e-525A AP will reboot in gateway mode and reset all prior settings to factory default state.



## 3e-525A Wireless Access Point



You can then proceed to change the management screens as necessary to reconfigure the device as a gateway. Configuration in gateway mode allows you to set firewall parameters. This is the main difference between the screens you will see in gateway mode and those covered in access point setup as discussed in Chapter 3.

Note that the 3e-525A AP is not FIPS 140-2 compliant in gateway mode.

The following sections cover the functions and screens in gateway mode. Much of the information is similar to the access point mode but is presented here for your convenience.

## System Configuration

### General

The **System Configuration—General** page for the 3e-525A AP gateway lists the firmware version for your 3e-525A AP and allows you to set the Host Name and Domain Name as well as establish system date and time. (Host and Domain Names are both set at the factory for “default” but can optionally be assigned a unique name for each.) When you are satisfied with your changes, click **Apply**.



Go next to the **System Configuration—WAN** page.

## WAN

This screen allows you to set Link Speed and Duplex of the WAN port. If you select a choice other than Auto (the default), the 3e-525A AP will use only the selected link speed (10 Mbits/sec or 100 Mbits/sec) and Duplex (Half Duplex transfers or Full Duplex transfers) that you select in the WAN/LAN Link dropdown menu.

You also set information for how the IP address will be obtained.

The WAN IP address is the Public IP address required to link the private WLAN users to the external enterprise or shipboard network, which is to be outside the “protected” wireless LAN. Normally, you will be provided with the IP address, Subnet Mask, Default Gateway and DNS to assign by the Network Administrator for the Ethernet Network.

There are two ways to configure the WAN IP address:

1. **Obtain an IP address Automatically** – This configuration allows the Ethernet network to use the DHCP server on the wired network to dynamically assign the WAN IP address to the DHCP client in the gateway.
2. **Specify an IP address** – This configuration allows the user to manually type in a static IP address, default gateway, and Domain Name Server (DNS) if these are provided by the Ethernet network administrator.

### 3e-525A Wireless Access Point



### LAN

This sets up the default numbers for the four octets for a possible private LAN function for the access point. You can also change the default subnet mask. The Local LAN port provides DHCP server functionality to automatically assign an IP address to a computer Ethernet port.



## Operating Mode

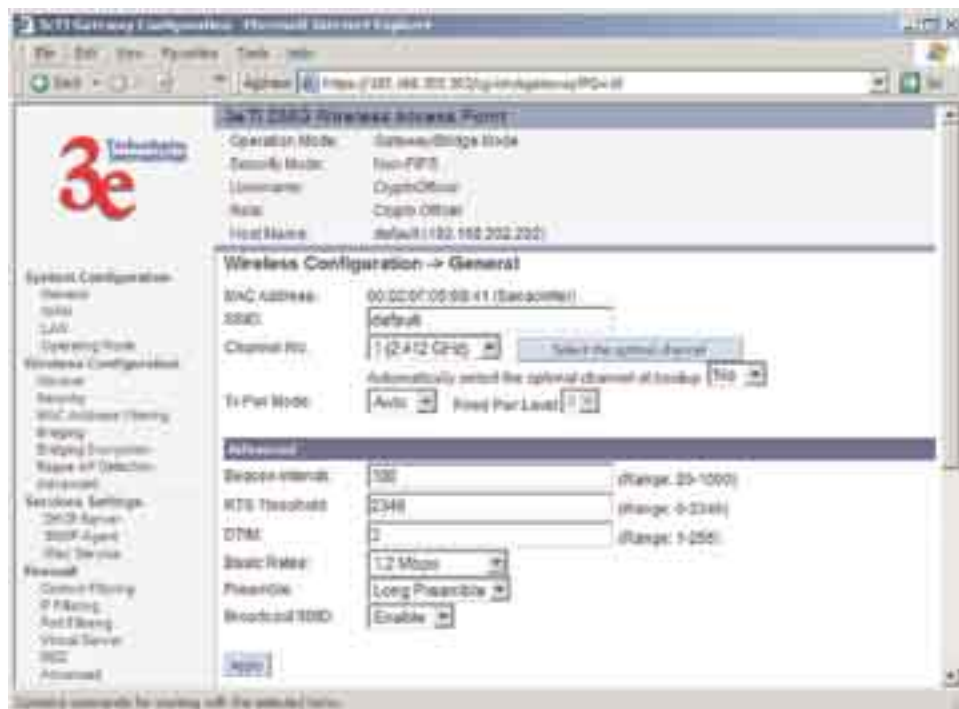
This is the page you accessed to change mode. You need to visit this page only if you will be changing mode from Gateway to Access Point. Note that if you change mode, all previously entered information will be reset to factory settings.



## Wireless Configuration

### General

Wireless configuration allows your computer's wireless PC Card to talk to the access point. Once you have completed wireless configuration of the 3e-525A AP, you can set up the rest of the configuration wirelessly if you wish. (This assumes that you have installed and configured the secure wireless card on your computer. If you have not done so, you will have to do that to establish communications.)



### 3e-525A Wireless Access Point

On the **Wireless Configuration — General** page, you must enter the SSID for the wireless LAN. This is also where you can assign a channel number to the AP (if necessary) and modify the Tx Pwr Mode. There are some advanced options which are detailed in the chart below.

The **SSID** can be any set of letters and numbers assigned by the network administrator. This nomenclature has to be set on the gateway and each wireless device in order for them to communicate.

The **Channel Number** is a means of assigning frequencies to access points, when many are used in the same WLAN, to minimize interference. There are 11 channel numbers that may be assigned.

**Tx Pwr Mode and Fixed Pwr Level:** The Tx Power Mode defaults to Auto, giving the largest range of radio transmission available under ambient conditions. As an option, the AP's broadcast range can be limited by setting the Tx Power Mode to Fixed and choosing from 1-8 for Fixed Pwr Level (1 being the shortest distance.) Finally, if you want to prevent any radio frequency transmission from the gateway, set Tx Pwr Mode to **Off**. This will not turn off RF transmission from any associated wireless devices, but they will not be able to communicate with the Gateway when the TX power mode is off.

**Advanced Options:**

The advanced options included on the second section of the above screen are described on the following chart:

Advanced Options		
<b>Beacon interval</b>	0-4095	The frequency in milliseconds in which the 802.11 beacon is transmitted by the AP.
<b>RTS Threshold</b>	0-3000	The number of bytes used for the RTS/CTS handshake boundary. When a packet size is greater than the RTS threshold, the RTS/CTS handshaking is performed.
<b>Fragmentation</b>	256-2346 even only	Fragmentation boundary in bytes.
<b>DTIM</b>	1-65535	The number of beacon intervals between successive Delivery Traffic Identification Maps (DTIMs). This feature is used for Power Save Mode.
<b>Basic Rates</b>	<b>Basic Rates for 802.11b</b>	
	- 1 and 2 Mbps - 1, 2, 5.5 and 11 Mbps	The basic rates used and reported by the AP. The highest rate specified is the rate that the AP uses when transmitting broadcast/multicast and management frames.
	<b>Basic Rates for 802.11g or 802.11b/g mixed</b>	
	- 1 and 2 Mbps - 1, 2, 5.5, 11, 12, and 24 Mbps	The basic rates used and reported by the AP. The highest rate specified is the rate that the AP uses when transmitting broadcast/multicast and management frames.
<b>Supported Rates</b>	<b>Supported Rates for 802.11b</b>	
	All Rates 1 Mbps 2 Mbps 5.5 Mbps 11 Mbps	The rate at which all data frames will be transmitted
	<b>Supported Rates for 802.11g or 802.11b/g mixed</b>	
	All Rates 1 Mbps 2 Mbps 5.5 Mbps 11 Mbps 12 Mbps 18 Mbps 24 Mbps 36 Mbps 48 Mbps 54 Mbps	The rate at which all data frames will be transmitted
<b>Preamble</b>	Short/Long Preamble	Specifies whether frames are transmitted with the Short or Long Preamble

### 3e-525A Wireless Access Point

<b>Broadcast SSID</b>	Enabled/ disabled	When disabled, the AP hides the SSID in outgoing beacon frames and stations cannot obtain the SSID through passive scanning.  Also, when it is disabled, the AP doesn't send probe responses to probe requests with unspecified SSIDs.
-----------------------	----------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Encryption

The default factory setting for the 3e-525A AP in gateway mode is no encryption but for security reasons it will not communicate to any clients unless the encryption is set by the administrator. It is recommended that you set encryption as soon as possible.

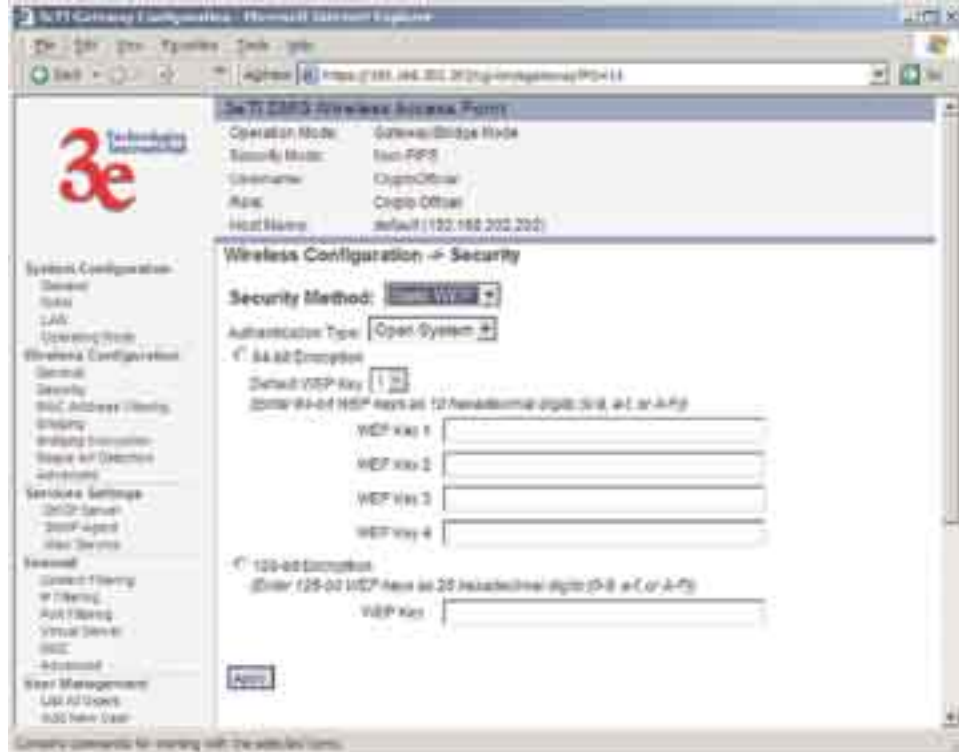


### **No Encryption**

In order to use the 3e-525A with no encryption, you must actively select **None** and click **Apply**. A screen will appear, asking if you really want to operate in Bypass mode. If you answer **Yes**, no encryption will be applied.

### **Static WEP Encryption**

Using the 3e-525A AP in gateway mode allows you to employ the WEP (RC4) encryption standard if you wish. If using WEP, authentication type can be set to Open System, Shared Key or a combination of Open/Shared.



WEP is designed to provide the same level of security for wireless LANs as that of a wired LAN. To use WEP encryption, identify the level of encryption (64 or 128). If using 64-bit WEP, you will need to program the Default WEP key on the AP and each wireless device and designate the four alternate 64-bit WEP keys. The four WEP keys thus programmed have to be input to the setup utility on each wireless device that will be part of the WLAN.

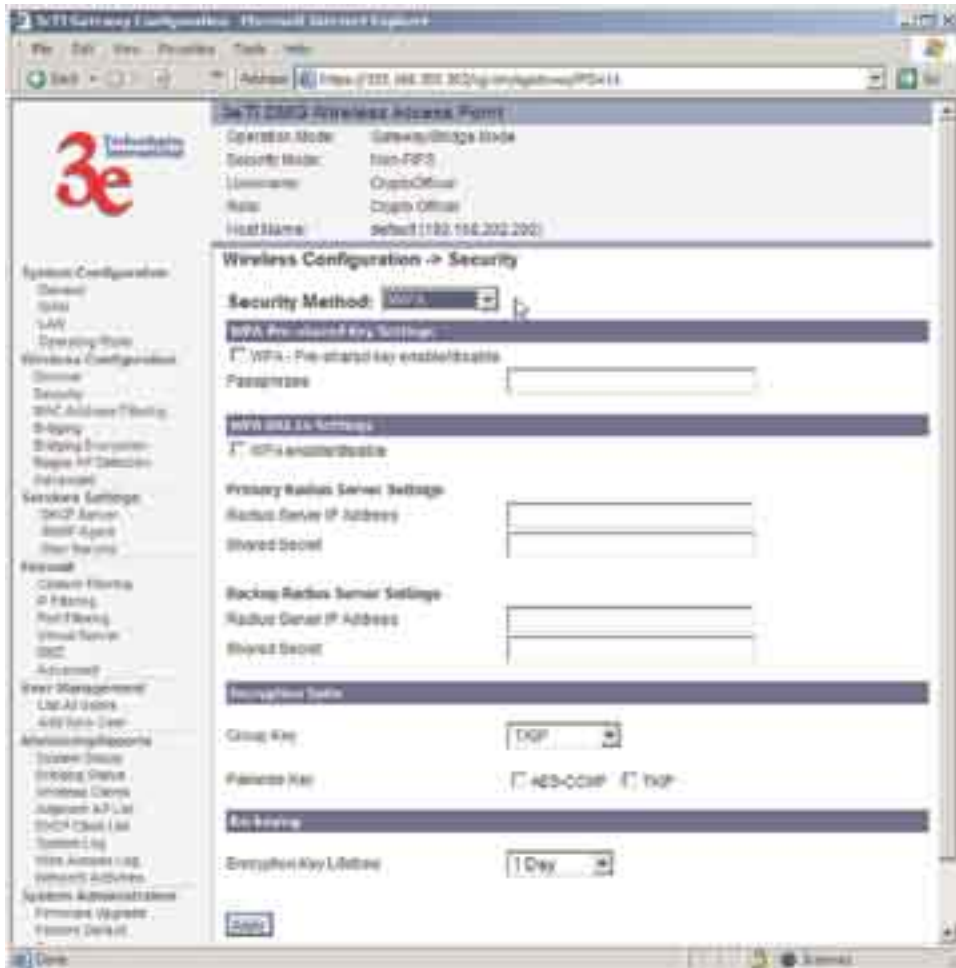
If using 128-bit WEP, simply designate the 48 hexadecimal digits on the AP and program the same number on each wireless device.

Key management becomes increasingly difficult as the number of clients increases, but the use of WEP encryption on small office wireless networks provides some measure of security. WEP was never intended to be a complete security solution but rather provides protection equivalent to that of wired networks.

### WPA (non-FIPS)

Wi-Fi Protected Access or WPA was designed to enable use of wireless legacy systems employing WEP while improving security. WPA uses improved data encryption through the temporal key integrity protocol (TKIP) which scrambles keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. In addition, user authentication is enabled using the extensible authentication protocol (EAP).





WPA is an interim standard that will be replaced with the IEEE's 802.11i standard upon its completion. However, it is expected to remain compatible. For those organizations already making the transition to the new AES algorithm, WPA uses a form of AES (AES-CCMP) agreed-upon by the WiFi Alliance 802.11i working team.

If you wish to use WPA on the 3e-525A, enable either WPA Pre-shared Key Settings or WPA 802.1x Settings.

If you are a SOHO user, selecting pre-shared key means that you don't have the expense of installing a Radius Server. Simply input up to 63 character / numeric / hexadecimals in the Passphrase field. If your clients use WPA-TKIP, select TKIP as encryption type. If your clients use WPA-AES, select AES-CCMP. If a combination, select AUTO.

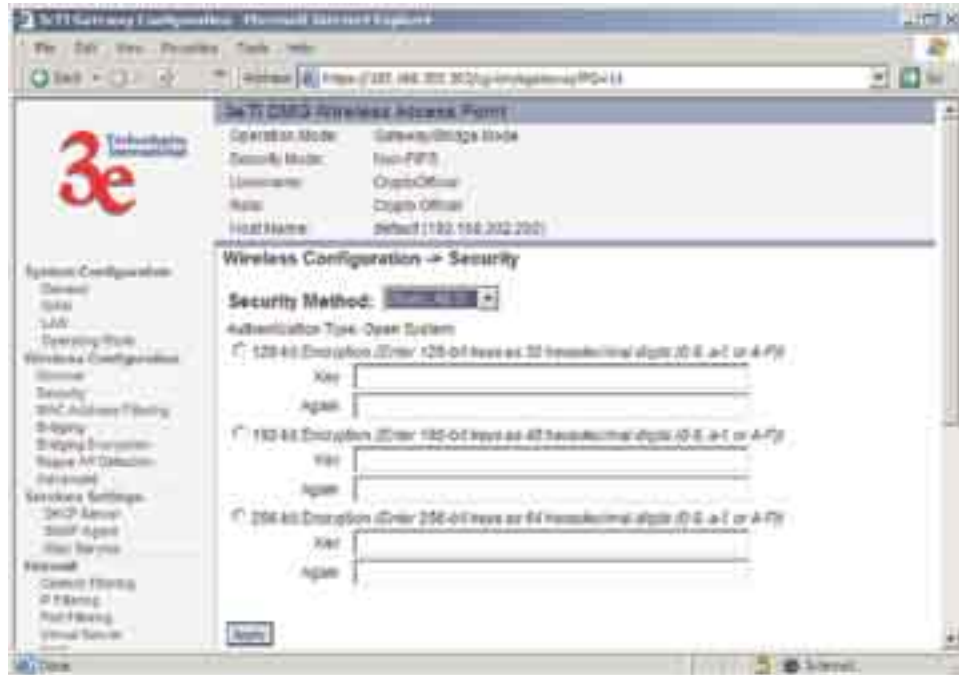
For highest security, select the lowest re-keying interval.

As an alternative, for business applications who have installed Radius Servers, select WPA 802.1x and input the Primary and Backup Radius Server settings. Use of Radius Server for key management and authentication requires that you have installed a separate certification system and each client must have been issued an authentication certificate.

Once you have selected the options you will use, click **Apply**.

### **Static AES Key/Open System Authentication**

The Advanced Encryption Standard (AES) was selected by National Institute of Standards and Technology (NIST) in October 2000 as an upgrade from the previous DES standard. AES uses a 128-bit block cipher algorithm and encryption technique for protecting computerized information. With the ability to use even larger 192-bit and 256-bit keys, if necessary, it offers higher security against brute-force attack than the old 56-bit DES keys. For even greater security, you can select a 192-bit or 256-bit key.



Once you have selected the options you will use, click **Apply**.

### **Static 3DES Key/Open System Authentication**

The 3e-525A AP in gateway mode can accommodate advanced static encryption using either AES or 3DES.

3DES is modeled on the older DES standard but encrypts data three times over.

To use 3DES, enter a 192-bit key as 48 hexadecimal digit (0-9, a-f, or A-F). Enter the key twice for verification.

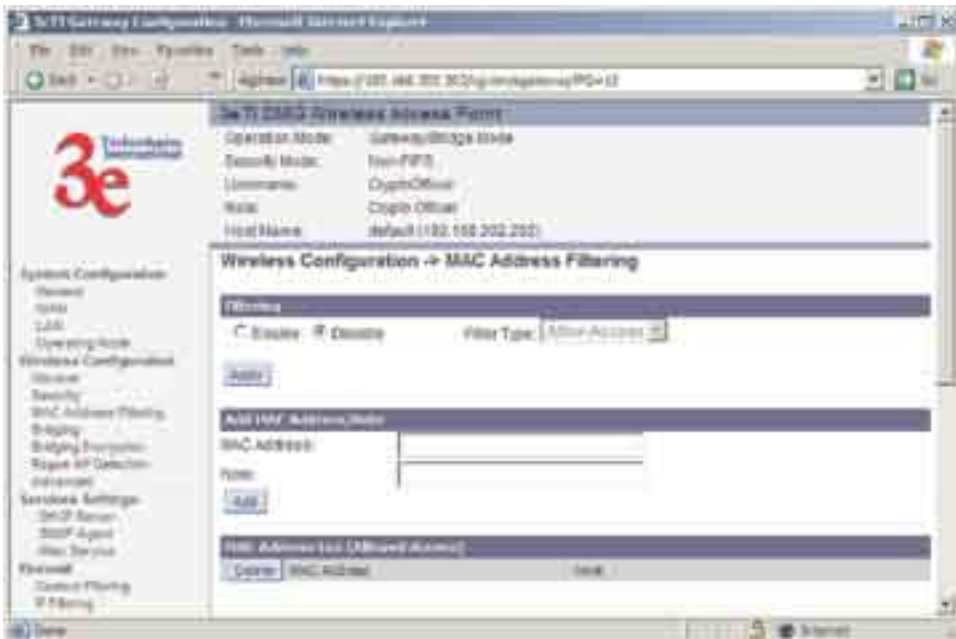


If you will be using MAC Address filtering, navigate next to the MAC Address Filtering page.

### Mac Address Filtering

The factory default for MAC Address filtering is Disabled. If you enable MAC Address filtering, only those devices equipped with the authorized MAC addresses will be able to communicate with the access point.

Input the MAC addresses of all the PC cards that will be authorized to access this device. The MAC address is engraved or written on the PC (PCMCIA) Card. The MAC Addresses you have input and any identifying note will appear in the lower window once you click the **Add** button. You delete MAC Addresses by simply clicking the Delete button next to the MAC Address you no longer want to include in the **WLAN**.



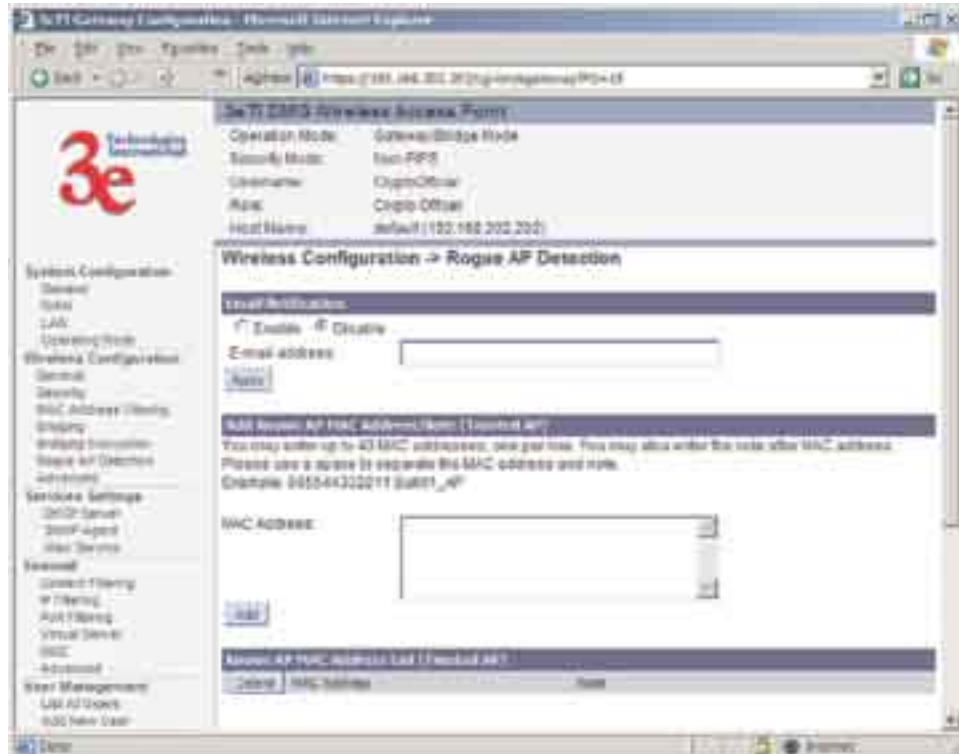
### Bridging

Bridging and bridging encryption are fully discussed in Chapter 5.

## Rogue AP Detection

The Rogue AP Detection page allows the network administrator to set up rogue AP detection. If you enable rogue AP detection, also enter the MAC Address of each AP in the network that you want the AP being configured to accept as a trusted AP. (You may add up to 20 APs.) Enter an email address for notification of any rogue or non-trusted APs.

The **Rogue AP list**, under **Monitoring Reports** on the navigation menu, will detail any marauding APs.



## Advanced

The Advanced page allows you to enable or disable load balancing and to control bandwidth.

Load balancing is enabled by default. Load balancing distributes traffic efficiently among network servers so that no individual server is overburdened. For example, the load balancing feature balances the wireless clients between APs. If two APs with similar settings are in a conference room, depending on the location of the APs, all wireless clients could potentially associate with the same AP, leaving the other AP unused. Load balancing attempts to evenly distribute the wireless clients on both APs.

If enabled, the Bandwidth Control function specifies the maximum bandwidth given to each wireless client.

Once you have made any changes, click **Apply** to save.

## 3e-525A Wireless Access Point



## Services Settings

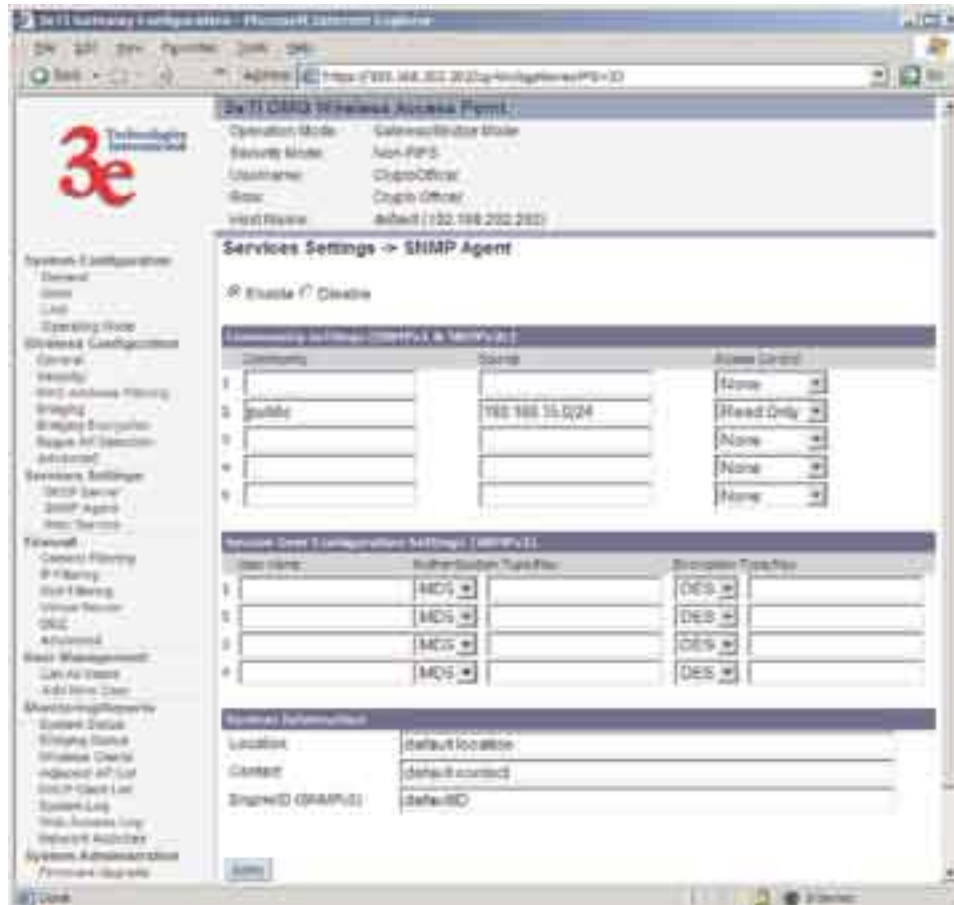
### DHCP Server

This page allows configuration of the DHCP server function accessible from the LAN port. The default factory setting for the DHCP server function is **enabled**. You can disable the DHCP server function, if you wish. You can also set the range of addresses to be assigned.



## SNMP Agent

The SNMP (simple network management protocol) Agent setup page allows you to set up an SNMP Agent. The agent is a software module that collects and stores management information for use in a network management system. The 3e-525A AP's integrated SNMP agent software module translates the device's management information into a common form for interpretation by the SNMP Manager, which usually resides on a network administrator's computer.



The SNMP Manager function interacts with the SNMP Agent to execute applications to control and manage object variables (interface features and devices) in the gateway. Common forms of managed information include number of packets received on an interface, port status, dropped packets, and so forth. SNMP is a simple request and response protocol, allowing the manager to interact with the agent to either:

- **Get** - Allows the manager to **Read** information about an object variable;
- **Set** - Allows the manager to **Write** values for object variables within an agent's control; or
- **Trap** - Allows the manager to **Capture** information and send an alert about some pre-selected event to a specific destination.

The SNMP configuration consists of several fields, which are ex-

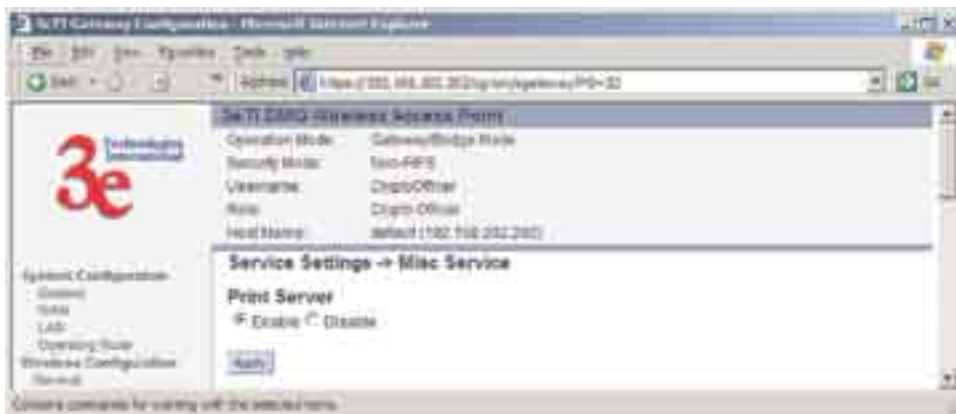
## 3e-525A Wireless Access Point

plained below:

- **Community** –The Community field for Get (Read Only), Set (Read & Write), and Trap is simply the SNMP terminology for “password” for those functions.
- **Source** –The IP address or name where the information is obtained.
- **Access Control** –Defines the level of management interaction permitted.

### Misc Service

The print server function can be enabled or disabled. It is enabled by default. If you do not plan to set up the print server function, you can click **Disable**.



## Firewall

### Content Filtering

The **Content Filtering** page allows the system administrator to identify particular hosts or IPs that will be blocked from access by the gateway. Simply input the IP address and click **Add**.



## IP Filtering

The **IP Filtering** page will block certain IPs on the Private LAN from accessing your Internet connection. It restricts clients to those with a specific IP Address.



## Port Filtering

Port filtering permits you to configure the Gateway to block outbound traffic on specific ports. It can be used to block the wireless network from using specific protocols on the network.

Following is a list of well known TCP and UDP ports.

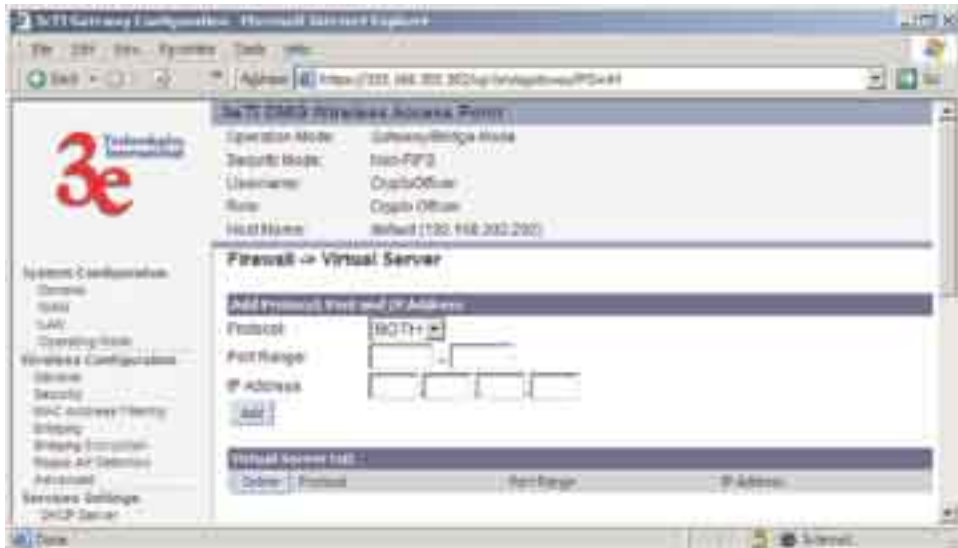
Port Range	Protocol
20-21	FTP
23	Telnet
25	SMTP (Simple Mail Transfer for email sending)
80	HTTP (World Wide Web)
110	POP3 (Post Office Protocol for email receiving.)





### Virtual Server

In order to protect the Private Network, the built-in NAT firewall filters out traffic to the private network. Since all clients on the Private Network are normally not visible to outside users, the virtual server function allows some clients on the Private Network to be accessed by outside users by configuring the application mapping function offered on this page. Certain well known applications use specific TCP ports, such as Telnet (port 23), FTP (port 21), and Web server (port 80). Client computers on the Private LAN can host these applications, and allow users from the Internet to access these applications hosted on the virtual servers.



This is done by mapping virtual servers to private IP addresses, according to the specific TCP port application. As the planning table below shows, we have identified a Telnet (port 23) virtual server for private IP 192.168.15.56, a SMTP Mail (port 25) virtual server for private IP 192.168.15.33, and a Web (port 80) virtual server for private IP 192.168.15.64. For example, all Internet requests to the gateway for SMTP Mail services (port 25) to the WAN IP address will be redirected to the Pri-

vate Network computer specified by the server IP 192.168.15.33.

Service Port	Server IP
23	192.168.15.56
25	192.168.15.33
80	192.168.15.64

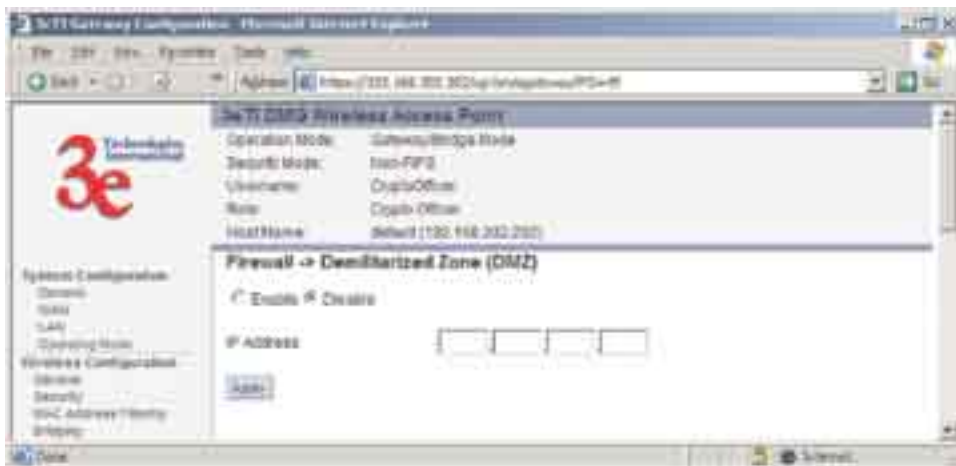
We recommend that IP addresses of virtual server computers hosted on the Private Network be manually (statically) assigned to coincide with a static server mapping to that specific IP address. Virtual servers should not rely on the dynamic IP assignment of the DHCP server function which could create unmapped IP address assignments.

**Protocol** – Selection of either **UDP**, **TCP**, or **Both** (TCP and UDP) allows these specified network protocols to pass through during the TCP port communication with each virtual server IP address.

## Demilitarized Zone (DMZ)

The Demilitarized Zone (DMZ) host allows one computer on the Private Network to be totally exposed to the wired network or Internet for unrestricted two-way communication. This configuration is typically used when a computer is operating a proprietary client software or 2-way communication such as video-teleconferencing, where multiple TCP port assignments are required for communication. To assign a PC the DMZ host status, fill in the Private IP address which is identified as the exposed host and click the **Apply** button. However, any Internet user who knows the WAN IP address of the gateway can connect to the DMZ host since the firewall feature is disabled for this device, causing a potential security risk to data residing on that host.

Again, it is recommended that IP addresses of DMZ host computers on the Private Network be manually (statically) assigned to coincide with a static DMZ host mapping to that specific IP address. DMZ hosts should not rely on the dynamic IP assignment of DHCP server function which could create incorrectly mapped IP address assignments to non-DMZ hosts.

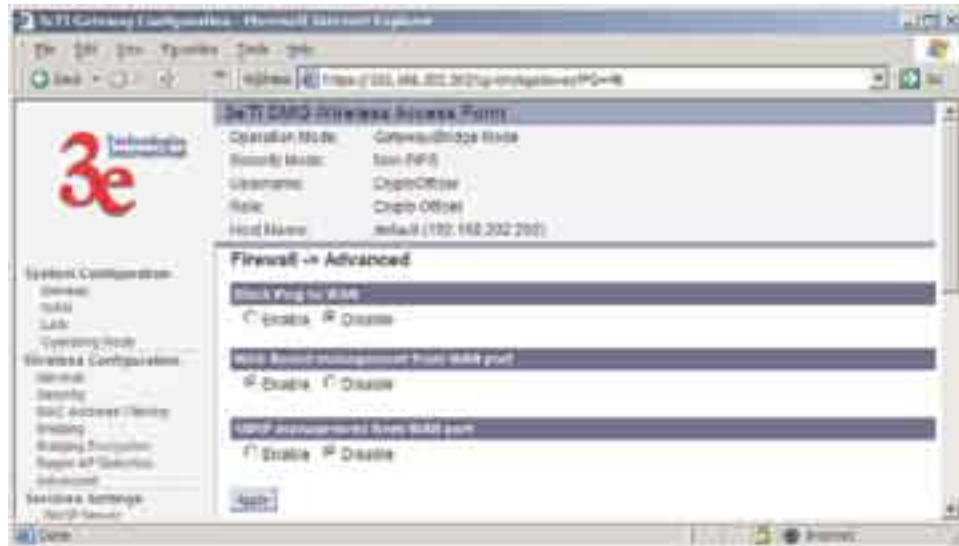


## Advanced Firewall

As advanced firewall functions, you can enable/disable

- Block Ping to WAN
- Web-based management from WAN port
- SNMP management from WAN port

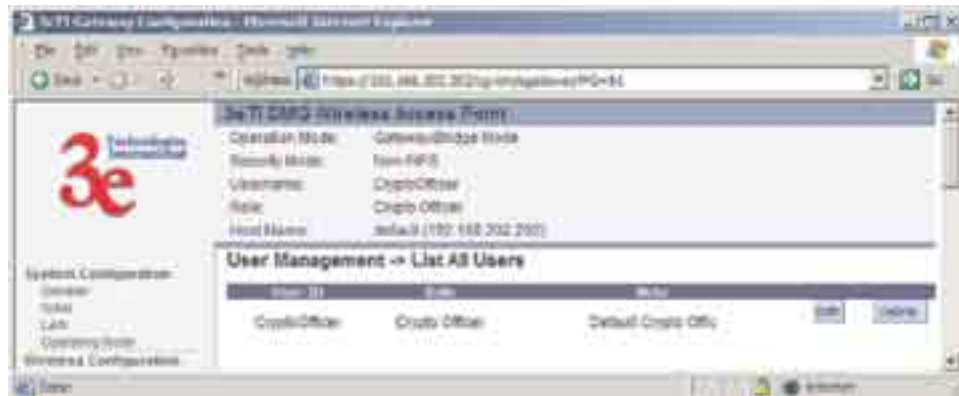
These options allow you more control over your environment.



## User Management

### List All Users

This List All User page simply lists all Crypto Officers and Administrators assigned.



### Add New User

The **Add New User** screen allows the Crypto Officer to add new Administrator users, assigning and confirming passwords. The Administrator role performs general security services, including cryptographic operations and other approved security functions. The Administrator role does not, however, perform cryptographic initialization or management functions such as module initialization, input or output of cryptographic keys and CSPs, and audit functions.

### 3e-525A Wireless Access Point

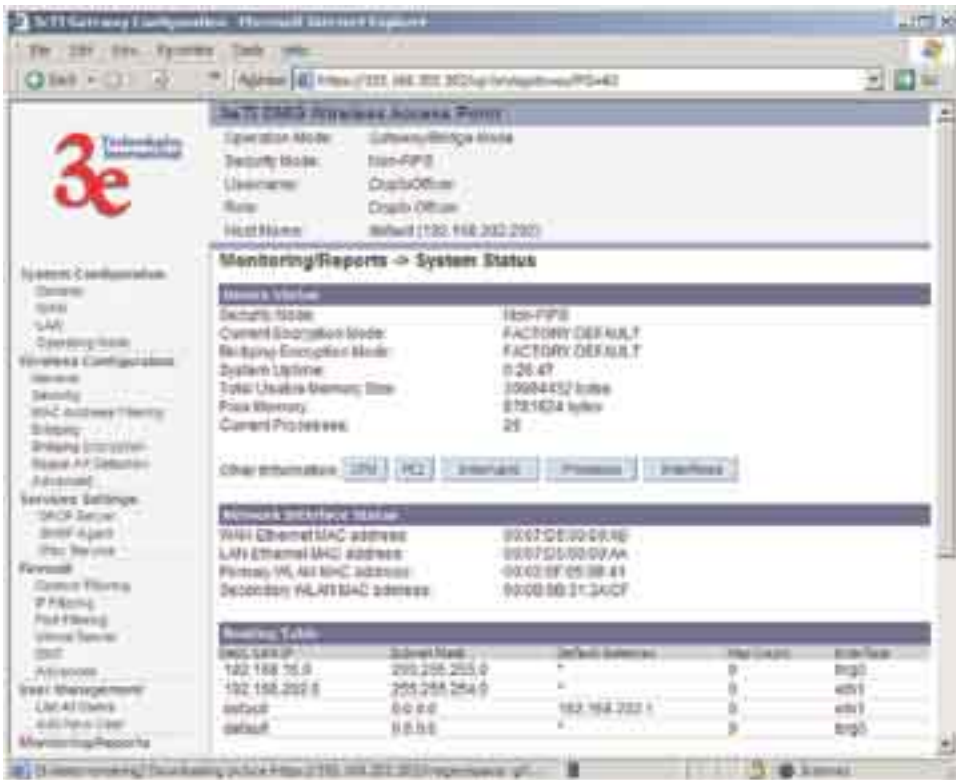


## Monitoring/Reports

This section gives you a variety of lists and status reports. Most of these are self-explanatory.

### System Status

This screen displays the status of the 3e-525A AP device and network interface details.



## Bridging Status

This screen displays the Ethernet Port STP Status, Wireless Port STP Status, and Wireless Bridging Information.

The screenshot shows the 3e Gateway Configuration web interface. The main content area is titled "Monitoring/Reports -> Bridging Status". It contains three sections:

- Ethernet Port STP Status:**
  - Port Priority: 8000
  - Path Cost: 80
  - State: forwarding
  - Designated Bridge: 8000.0000.0000.0000
- Wireless Port STP Status:**
  - Port Priority: 8000
  - Path Cost: 100
  - State: forwarding
  - Designated Bridge: 8000.0000.0000.0000
- Wireless Bridging Information:**
  - Bridge Priority: 8000
  - Bridge Hello Time: 2:00 sec
  - Bridge Forward Delay: 3:00 sec
  - Bridge Max Age: 20:30 sec
  - Bridge ID: 8000.0000.0000.0000
  - Designated Root: 8000.0000.0000.0000
  - Root Path: 0
  - Path Cost: 0
  - Hello Time: 2:00 sec
  - Forward Delay: 3:00 sec
  - Max Age: 20:30 sec
  - MAC Aging Time: 300.00 sec
  - MAC Aging Interval: 4:00 sec
  - Flags:

## Wireless Clients

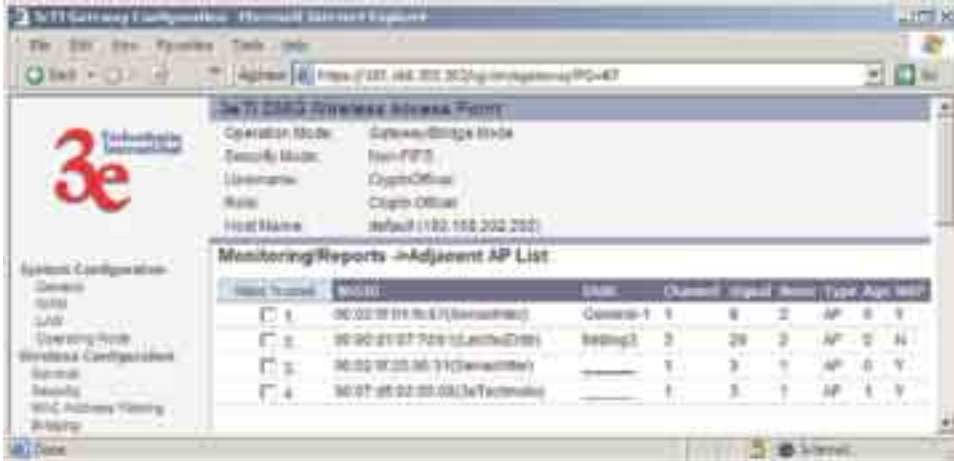
The Wireless Clients report screen displays the MAC Address of all wireless clients and their signal strength and transmit rate.

The screenshot shows the 3e Gateway Configuration web interface. The main content area is titled "Monitoring/Reports -> Wireless Clients". It displays a table with the following columns:

- Client MAC Address
- Signal Strength
- Transmit Rate

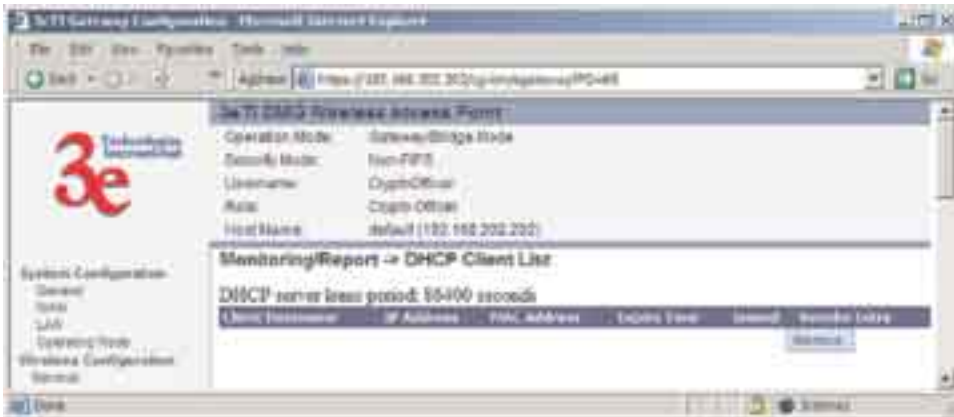
### Adjacent AP List

The Adjacent AP list shows all the APs on the network which are not seen by the subject AP as trusted clients. To make any AP shown a trusted client, simply click on the Make Trusted box for that AP.



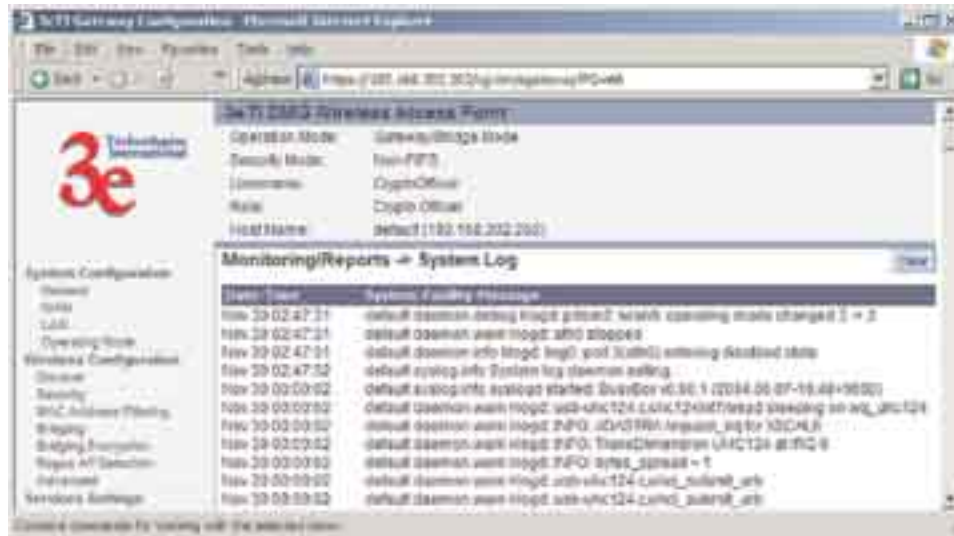
### DHCP Client List

The DHCP client list displays all clients currently connected to the 3e-525A AP via DHCP server, including their hostnames, IP addresses, and MAC Addresses.



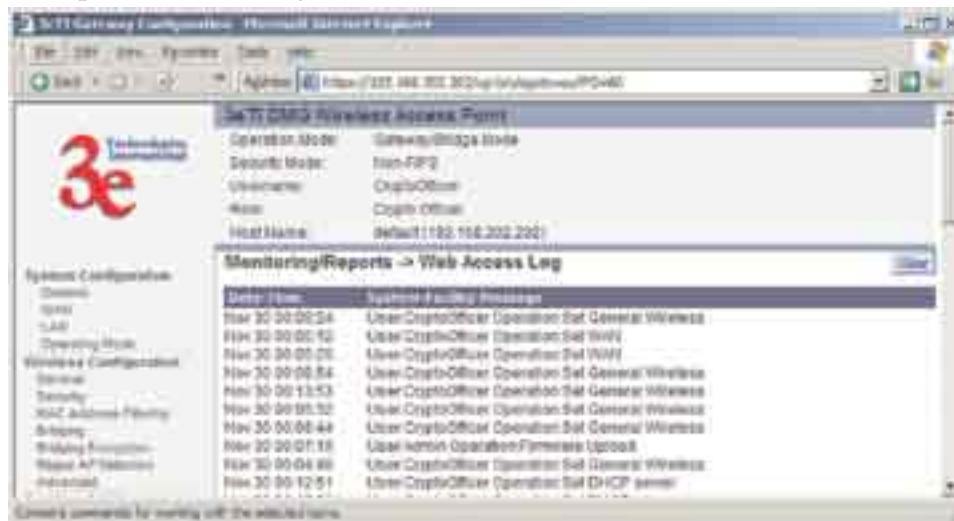
### System Log

The system log displays system-facility-messages with date and time stamp. These are messages documenting functions performed internal to the system, based on the system’s functionality. Generally, the Administrator would only use this information if trained as or working with a field engineer or as information provided to technical support.



### Web Access Log

The web access log displays system-facility-messages with date and time stamp for any actions involving web access. For example, this log records when you set encryption mode, change operating mode, etc., using the web browser. It establishes a running record regarding what actions were performed and by whom.

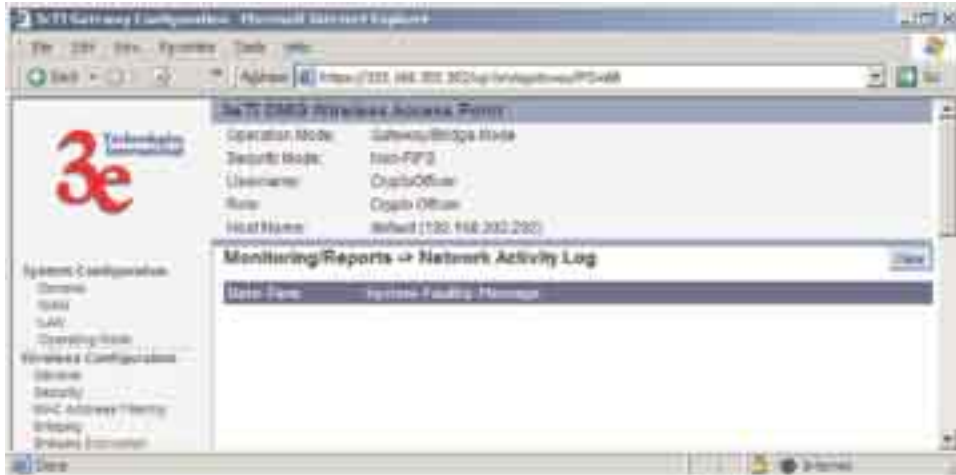


### Network Activities

The Network Activities Log keeps a detailed log of all activities on the network which can be useful to the network administration staff.



## 3e-525A Wireless Access Point



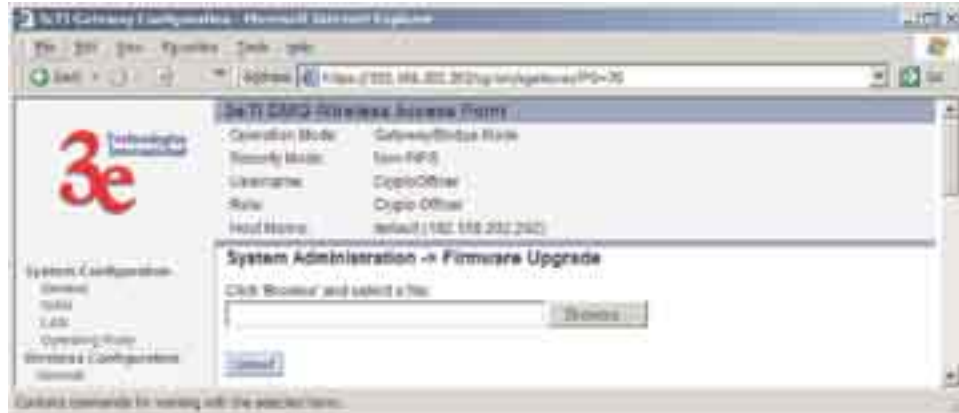
## System Administration

The System administration functions contain administrative functions, some of which can be performed only if the user is logged on as a Crypto Officer. The screens and functions are detailed in the following section.

## Firmware Upgrade

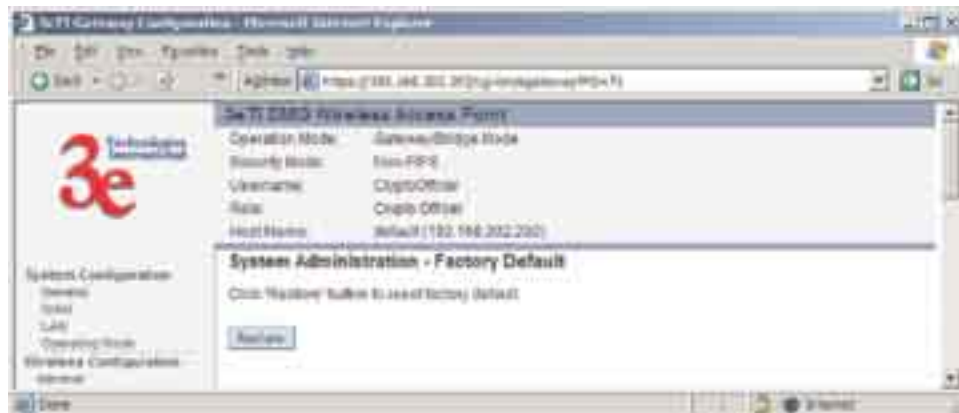
The **System Upgrade** utility is a functionality built into the 3e-525A AP for updates to the device's firmware as they become available. When a new upgrade file becomes available, find it and upload it to the 3e-525A AP from this page.

Only the Crypto Officer role can access this function.



## Factory Default

The Factory Default or "Restore" button is a fallback troubleshooting function that should only be used to reset to original settings.



Only the Crypto Officer role has access to the **Restore** button.

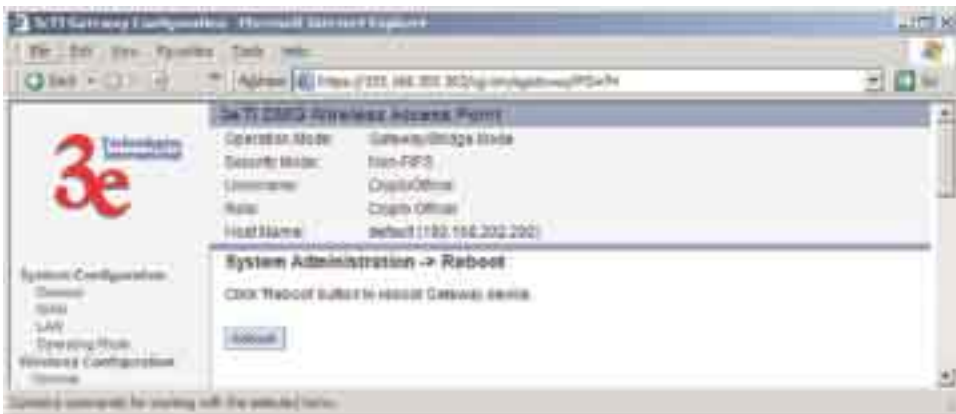
## Remote Logging

If enabled, input a System Log Server IP Address and System Log Server Port. Click **Apply** to accept these values.



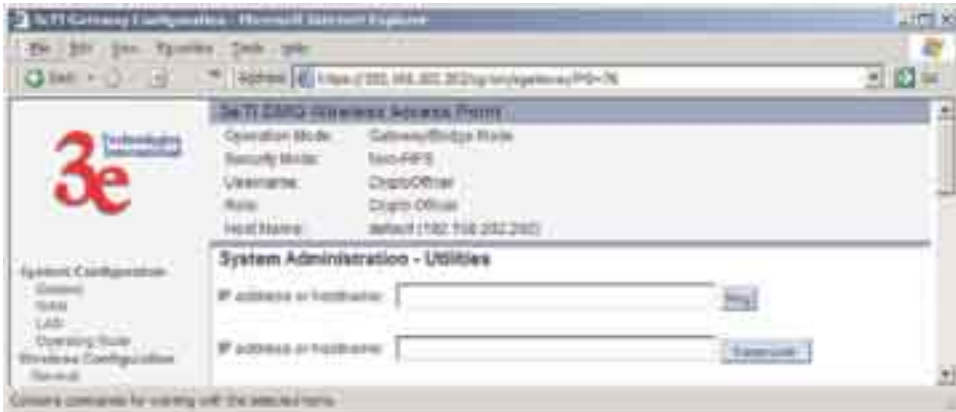
## Reboot

The Reboot utility allows you to reboot the Gateway without changing any preset functionality. Both Crypto Officer and Administrator functions have access to this function.



## Utilities

This screen gives you ready access to two useful utilities: Ping and Traceroute. Simply enter the IP Address or hostname you wish to ping or traceroute and click either the **Ping** or **Traceroute** button, as appropriate.



## Chapter 5: Bridge Configuration

### Introduction

In the 3e-525A, wireless bridging uses a second WLAN card to set up an independent wireless bridge connection. Since wireless bridging provides a mechanism for APs to collaborate, it is possible to extend the basic service set (BSS) of a standalone AP and to connect two separate LANs without installing any cabling.

The wireless bridging function in the 3e-525A allows you to set a number of alternate bridging configurations. We discuss some of the most popular settings in this chapter:

- **Point-to-point bridging of 2 Ethernet Links**
- **Point-to-multipoint bridging of several Ethernet links**
- **Repeater mode**

The wireless bridging screens are the same whether you are in access point or gateway mode.

### General Bridge Setup

Bridging is a function that is set up in addition to basic access point setup. If you will be using the 3e-525A solely as a bridge, some of the settings you may have selected for access point/gateway use will not be necessary.

If setting up as a bridge during initial setup, you can either use the LAN Port directly wired by Ethernet cable to a laptop to set the appropriate settings, or, once you have configured wireless settings, use a laptop with a correctly configured PC Card to complete the setup using the 3e-525A's management screens. The management screens that you may need to modify, regardless of what type of bridging mode you choose, will be in the **Wireless Configuration** section of the navigation bar. These include:

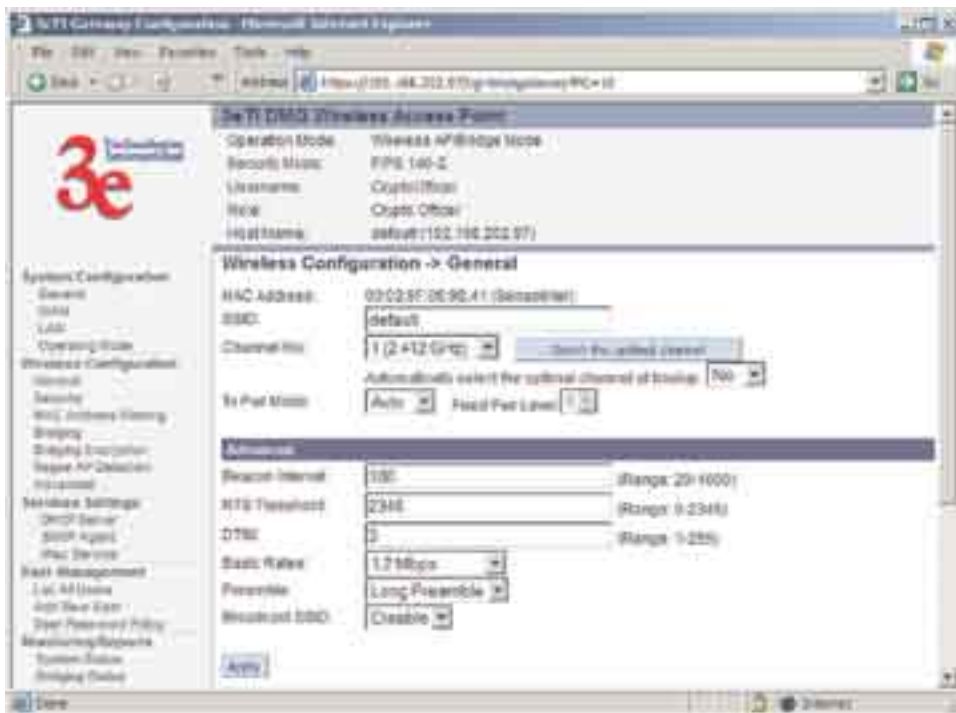
**Wireless Configuration — General**

**Wireless Configuration — Encryption**

**Wireless Configuration — MAC Address Filtering**

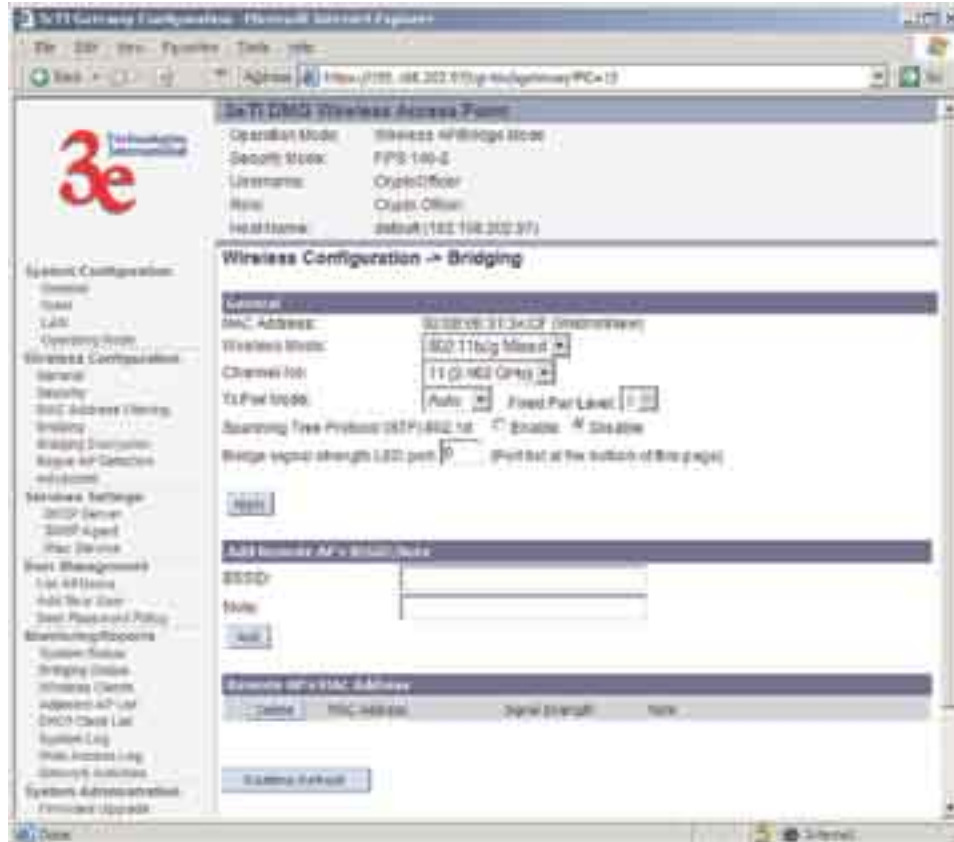
## Wireless Configuration — Bridging

### Wireless Configuration — Bridging Encryption

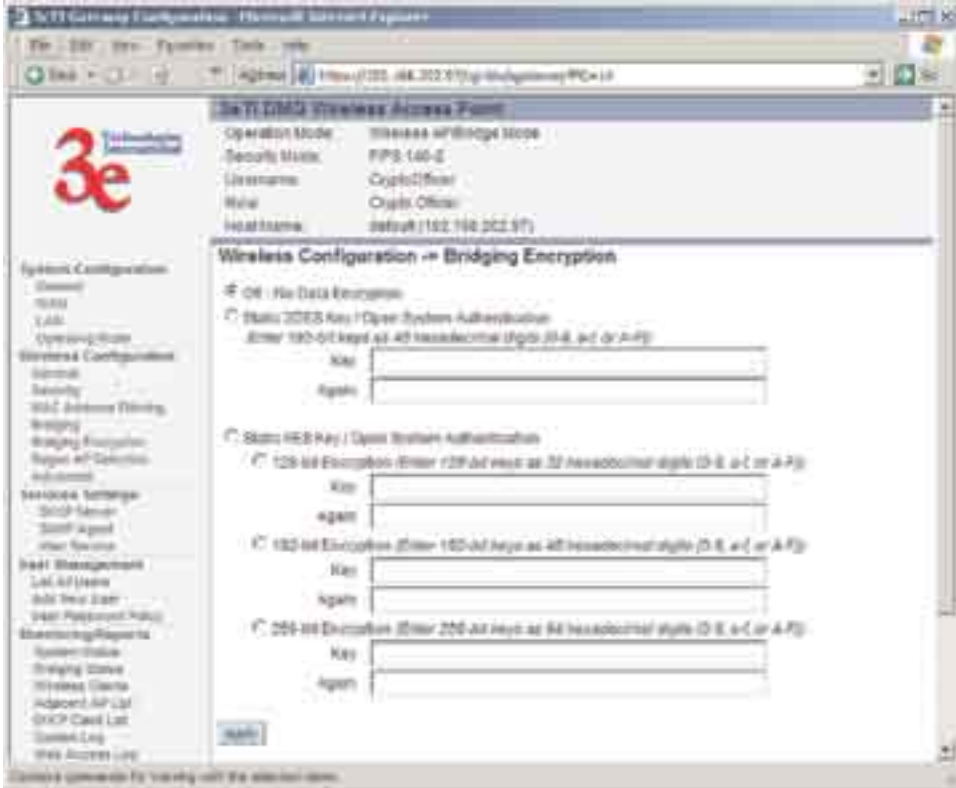


In the **Wireless Configuration — General** screen, if you are setting up the 3e-525A only as a bridge, the SSID can remain in its default setting, since the bridge uses the BSSID for purposes of establishing contact. The BSSID is shown on the **Wireless Configuration — Bridging** page (see page 77.) It is the MAC Address for the bridge WLAN card. Channel number is a means of assigning frequencies to access points used in proximity or series to minimize interference or "noise." There are 11 channel numbers that can be assigned. TX Pwr Mode can be left in its default of Auto.

The **Wireless Configuration — Bridging** screen contains wireless bridging information including the channel number, Tx power, spanning tree protocol (802.1d) enable/disable, and remote OAP BSSID. This page is important in setting up your bridge configuration. Spanning Tree Protocol should be enabled if there is any possibility that a bridging loop could occur. If you are certain that there is no possibility that a bridging loop will occur, you should disable Spanning Tree Protocol, because the bridge will be more efficient (faster) without it. However, if not sure, the safest solution is to enable Spanning Tree Protocol.



The **Wireless Configuration — Bridging Encryption** page is used to configure static encryption keys for the wireless bridge. This is an important page to set up to ensure that your bridge is working correctly. The encryption key that you use on this screen must be the same for any bridge connected to your bridging network in order for communication to occur. And on this screen you can only select either a static 192 bit 3DES key or an AES key of either 128-bit, 192-bit, or 256-bit.

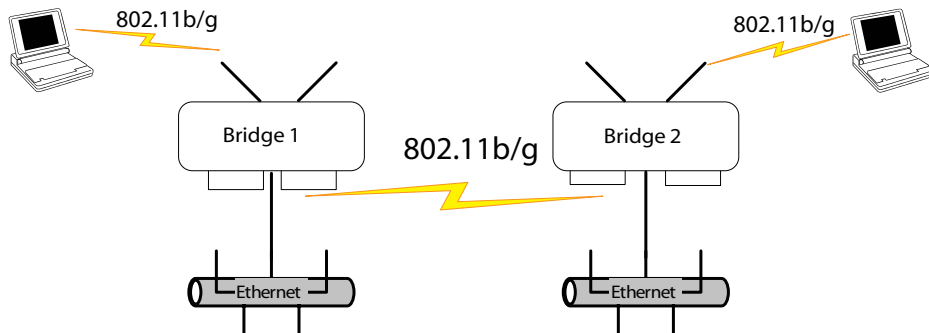


The following sections describe the setup for three types of bridging configuration: point-to-point, point-to-multipoint, or, lastly, repeater.

## Setting Up Bridging Type

### Point-to-Point Bridge Configuration

A point-to-point link is a direct connection between two, and only two, locations or nodes. Because the bridge function uses a separate WLAN card for bridging, you can also set up WLANs on the separate AP WLAN card.



For the two bridges that are to be linked to communicate properly, they must be set up with compatible commands in the setup screens.

For instance, the bridges must have the same channel number. Because there is a separate WLAN card for bridging, there can be a separate WLAN on the AP WLAN card with no loss efficiency, as long as you set the channel numbers so there's no conflict or noise with the channel as-

signed to the bridge. Spanning Tree Protocol may be set to Enable, if there is any possibility of a bridging loop, or to Disable (which is more efficient) if there's no possibility of a bridging loop. Each bridge must contain the other's BSSID. (The BSSID of each is equivalent to the MAC address contained on the **Wireless Configuration — Bridging** setup page. Enter only hexadecimal numbers, no colons. Data entry is not case sensitive.) Finally, the wireless bridging encryption must be set to the appropriate type and key length and must be identical on each bridge.

The following chart shows sample settings.

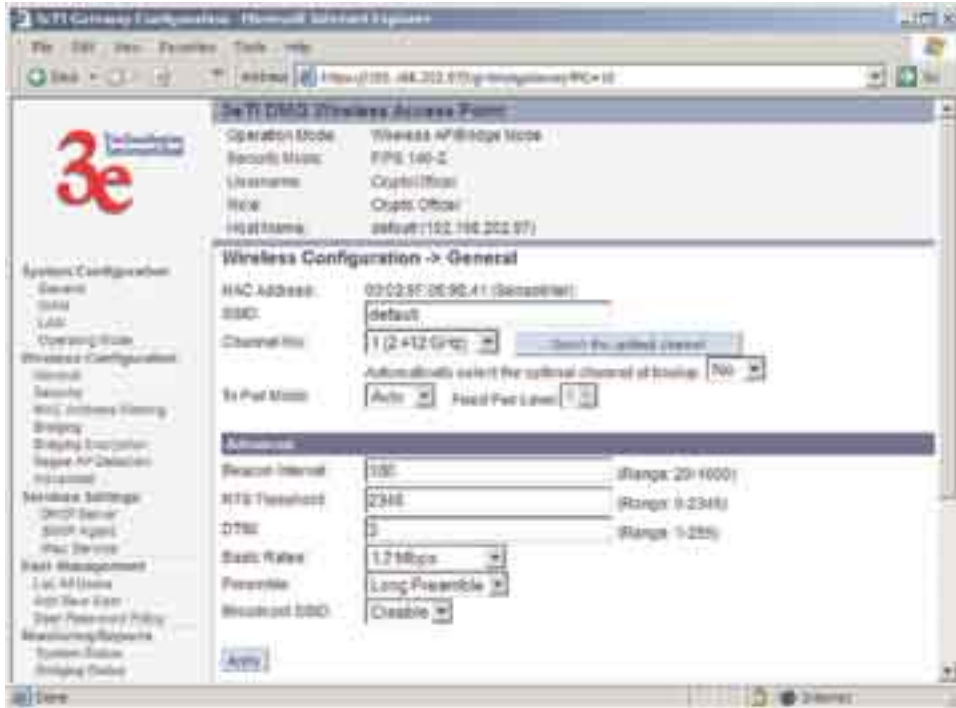
### ***Point-to-Point Bridging Setup Guide***

Direction	Bridge 1	Bridge 2
<b>Wireless Configuration – General</b>		
SSID	default (or set for 802.11b/g WLAN)	default (or set for 802.11b/g WLAN)
Channel	11	11
<b>Wireless Configuration – Encryption</b>	Set for 802.11b/g WLAN	Set for 802.11b/g WLAN
<b>Wireless Configuration – Bridging</b>		
Channel	4	4
Tx Power	Auto	Auto
Wireless Client Access	Enable	Enable
Spanning Tree Protocol	Enable (or Disable if no bridging loop possible)	Enable (or Disable if no bridging loop possible)
BSSID	Add Bridge 2 BSSID	Add Bridge 1 BSSID
<b>Wireless Configuration – Bridging Encryption</b>	Select appropriate key type/length and value. Must be the same key as Bridge 2.	Select appropriate key type/length and value. Must be the same key as Bridge 1.

The following sequence walks you through the setup of bridge 1. Bridge 2 would duplicate this procedure, with the BSSID of bridge 2 being the MAC address of bridge 1 and vice versa.

First, navigate to the **Wireless Configuration — General** screen and set the Channel number of the WLAN AP card so that it doesn't conflict with the channel number you will be using for the bridge. Leave the TX Pwr Mode in AUTO position at this time. If there is a wireless LAN on the AP WLAN card, information would be set as discussed in Chapter 3.





Navigate to the **Wireless Configuration — Bridging** screen.

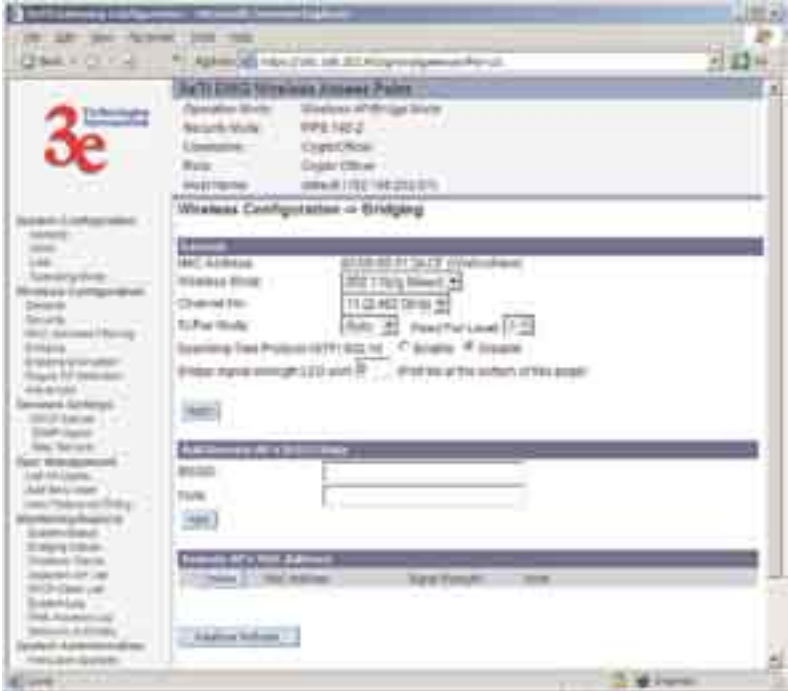
In the first section: **General**, you will see the MAC Address of the bridging card. This is used as the BSSID on other 3e-525As that will be communicating with this one.

**Wireless Mode** can be set to 802.11g for best rate, to 802.11b (if necessary) or to mixed 802.11b/g. Set Basic and Supported Rates. **Channel Number** must be set the same for each bridge to communicate. **TX Pwr Mode** can be left on **Auto** unless the power needs to be regulated. Set **Spanning Tree Protocol** to **Enable** unless you are sure that there is no chance of a loop.

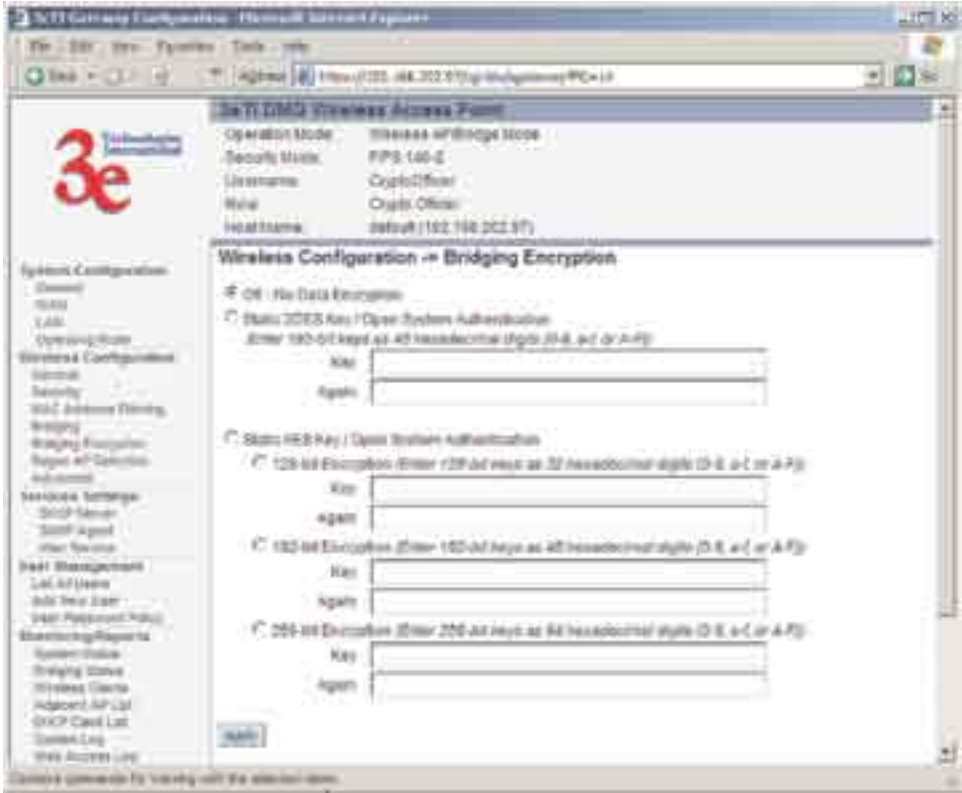
**Bridge signal strength LED port** allows you to set the number of one of the Remote APs which will be listed in section 3 at the bottom of the screen once the system is operational as the guiding port that you wish to have display in the WLANSS LED on the front of the 3e-525A as a signal. If you don't wish to display any connection signal, simply leave this set at 0.

Click **Apply** to accept your changes but remain on that screen.

In the second section on the **Wireless Configuration — Bridging** screen, add the BSSID of the remote bridge. The BSSID corresponds to that bridge's MAC address. In entering the BSSID, enter only hexadecimal numbers, no colons. Data entry is not case sensitive. You may also enter a note that defines the location of the remote bridge. Then click **Add** to accept. The remote bridge's BSSID will now appear in the third section of the page. If, at some time you wish to delete the entry, simply click the check box next to it and confirm by clicking **Delete**.



Next, navigate to **Wireless Configuration — Bridging Encryption**. Select the appropriate key type and length and the key value. The encryption key value and type for Bridge 1 must be the same as for Bridge 2. For wireless bridging, only AES and 3DES are available for encryption.



You must complete the configuration of your Bridge 1 by following the general instructions in Chapter 3 of this guide to establish any other required configuration options such as General, WAN and LAN settings.

Configure the second of your two point-to-point bridges following the instructions given for Bridge 1 above.

### Point-to-Multipoint Bridge Configuration

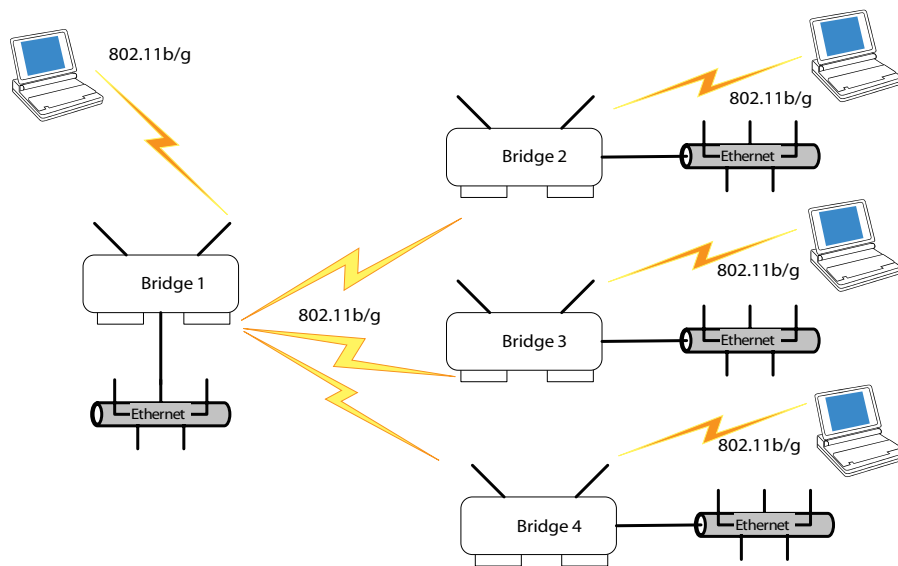
A point-to-multipoint configuration allows you to set up three or more 3e-525A access points in bridging mode and accomplish bridging between 3 or more locations wirelessly.

For the three bridges that are to be linked to communicate properly, they have to be set up with compatible commands in their setup screens.

For instance, all bridges must have the same channel number. Spanning Tree Protocol will usually be set to Enable. If configured as in the diagram following, Bridge 1 must contain all of the others' BSSIDs, while Bridge 2 ~ n must only contain Bridge 1's BSSID. (The BSSID of each is equivalent to the MAC address found on the **Wireless Configuration — Bridging** page. Enter only hexadecimal numbers, no colons. Data entry is not case sensitive.) Finally, the wireless bridging encryption of each must be set to the appropriate type and key length and must be the same on all.

Because the 3e-525A has two separate WLAN cards, one for the AP and one for the Bridge, each bridge can have a WLAN on the 802.11b/g protocol with no loss of efficiency in bridging if you wish.

The following diagram pictures a point-to-multipoint setup, which might be of use where a company's network spans several buildings within a campus-like setting.



Follow the steps of the procedure outlined in the point-to-point bridge section. The chart following describes the basic attributes.

### ***Point-to-Multipoint Bridging Setup Guide***

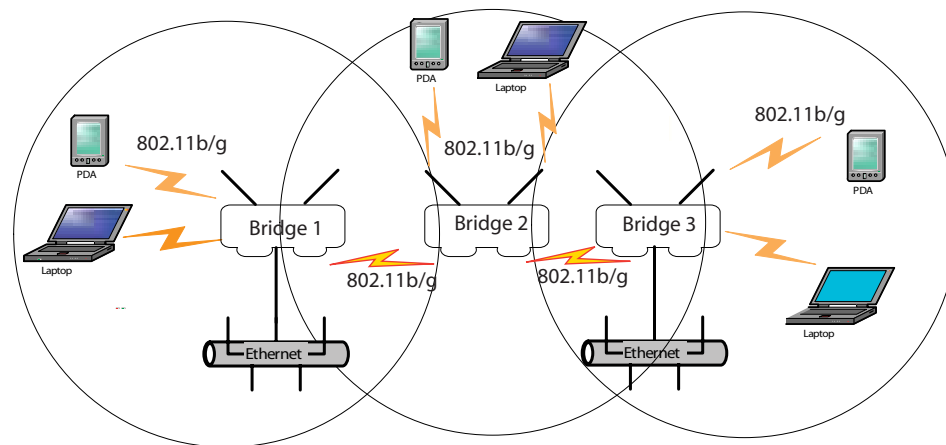
Direction	Bridge 1	Bridge 2 ~ n
<b>Wireless Configuration – General</b>		
SSID	default (or set for 802.11b/g WLAN)	default (or set for 802.11b/g WLAN)
Channel	11	11
<b>Wireless Configuration – Encryption</b>	Set for 802.11b/g WLAN	Set for 802.11b/g WLAN
<b>Wireless Configuration – Bridging</b>		
Channel	4	4
Wireless Client Access	Enable	Enable
Spanning Tree Protocol	Enable (or Disable if no bridging loop possible)	Enable (or Disable if no bridging loop possible)
BSSID	Add Bridge 2 ~ n BSSIDs	Add Bridge 1 BSSID
<b>Wireless Configuration – Bridging Encryption</b>	Select appropriate key type/length and value. Must be the same key as Bridge 2~n.	Select appropriate key type/length and value. Must be the same key as Bridge 1.

The above recommended setup requires only Bridge 1 to be set in point-to-multipoint mode. It is possible to set all bridges in point-to-multipoint mode, in which case, each bridge would have to contain the BSSID for each of the other bridges and Spanning Tree Protocol must be Enabled.

As stated previously, complete any other setup screens following general instructions in Chapter 3.

### **Repeater Bridge Configuration**

A repeater setup can be used to extend the wireless signal from one bridge connected to an Ethernet LAN wirelessly so that another bridge can control a wireless LAN at a distance.



### ***Repeater Bridging Setup Guide***

### 3e-525A Wireless Access Point

Direction	Bridge 1	Bridge 2	Bridge 3
<b>Wireless Configuration – General</b>			
<b>SSID</b>	default (or set for 802.11b/g WLAN)	default (or set for 802.11b/g WLAN)	default (or set for 802.11b/g WLAN)
<b>Channel</b>	11	11	11
<b>Wireless Configuration – Encryption</b>	Select appropriate key type and length and enter key value	Select appropriate key type and length and enter key value	Select appropriate key type and length and enter key value
<b>Wireless Configuration – Bridging</b>			
<b>Channel</b>	4	4	4
<b>Tx Power Mode</b>	Auto	Auto	Auto
<b>BSSID</b>	Add Bridge 2's BSSID	Add Bridge 1's and Bridge 3's BSSID	Add Bridge 2's BSSID
<b>Wireless Configuration – Bridging Encryption</b>	Select appropriate key type/length and enter key value. Must be the same as that on the other 2 Bridges.	Select appropriate key type/length and enter key value. Must be the same as that on the other 2 Bridges.	Select appropriate key type/length and enter key value. Must be the same as that on the other 2 Bridges.

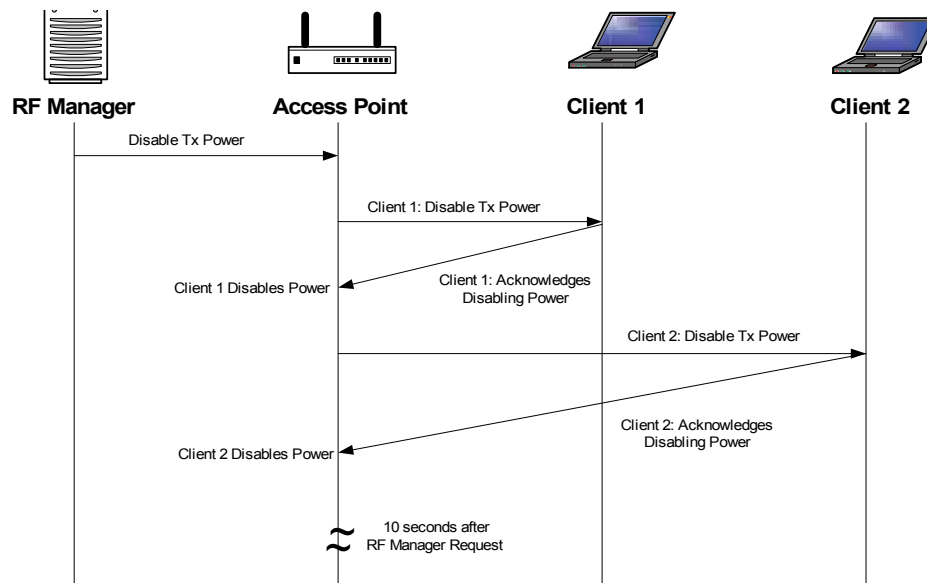
With this configuration, each bridge can control a wireless LAN. All wireless clients must have the same SSID as the bridges on the AP card channel. All clients can roam between the three bridges.


All other setup screens should be completed following the guidelines in Chapter 3.

## Chapter 6: The RF Manager Function

### Introduction

This chapter addresses a function of the 3e-525A which facilitates remote management and programming of the Radio Frequency function for multiple 3e-525As located on a common network. This function allows you to remotely manage the Radio Frequency Power levels. For each AP selected, the RF Manager can remotely disable the AP's transmit power and, in turn, the transmit power of each client that is associated with it. The basic architecture is shown in the chart below.



 **CAUTION:** You can not use this utility if you are using dynamic IP address assignment on your wireless network. We recommend that you have your LAN Administrator set a range of static IP Addresses and that you change the WAN IP Address on each gateway to one of this range of IP Addresses as part of your setup process.

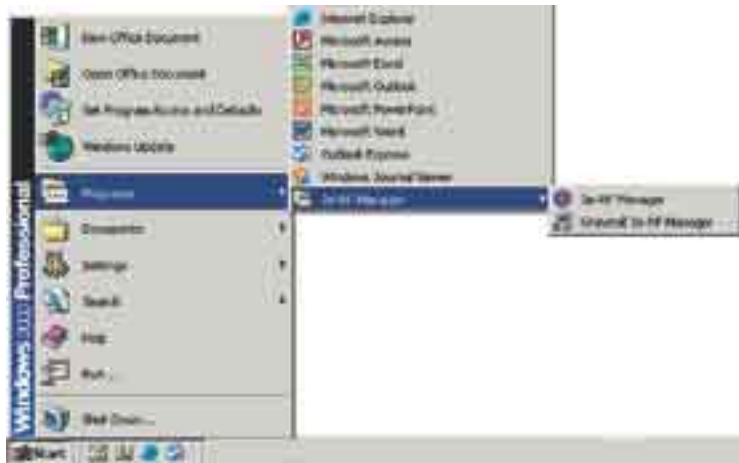
## How to Access the RF Manager Function

The RF Manager can be installed from the CD that came with the 3e-525A Install Kit to the desktop of anyone who needs to manage the wireless LAN.

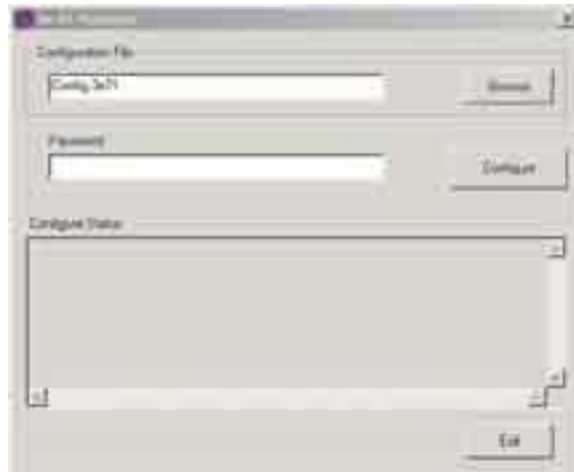
Click on **RF Manager** on the Installation CD main menu to start the autoinstall. If, for any reason, the autoinstall function doesn't initiate, open a window from the **My Computer** icon on your desktop to your CD drive and double-click the 3E-RFMGR.EXE icon in the RF Manager folder on the CD.



Once the RF Manager is installed, use the path **Start -> Programs -> 3e-RF Manager** and click on 3e-RF Manager.



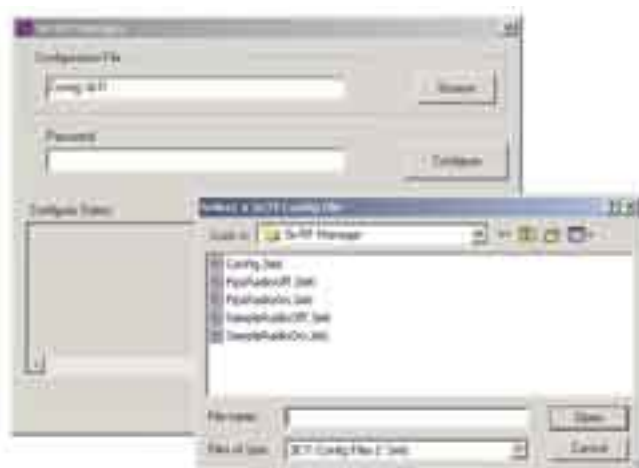
The main RF Manager screen will appear on your desktop.



## How to Program the RF Manager

Before you are able to remotely manage access points, you need to program the RF Manager by putting the static IP Address of APs you want to manage in a configuration file.

Click on the **Browse** button. This will open a window with some sample files that you can edit. You should edit the contents of SampleRadioOn.3eti and SampleRadioOff.3eti.



To see the contents of one of these files, simply right click the file name and select **Open** from the dropdown menu.

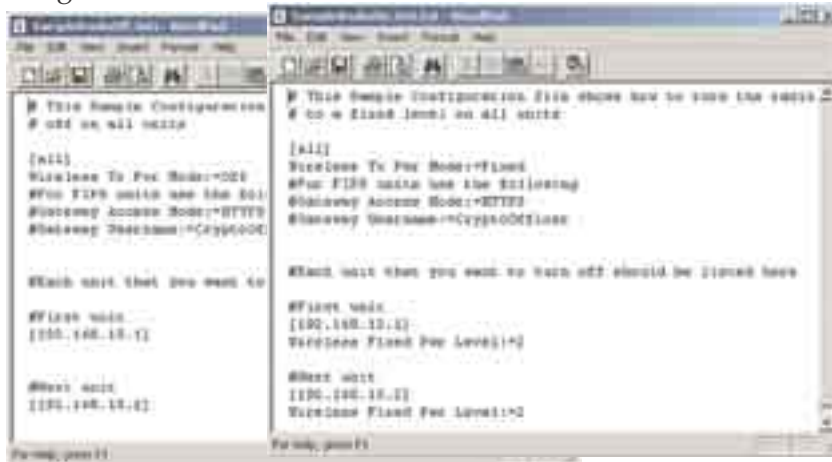
Because the file has an extension (.3eti) which Windows is not yet familiar with, the very first time you attempt to open it, Windows will ask you what program you want to open it with, as shown in the screen on the following page. Choose a text editor that you are comfortable with, such as Wordpad. In future, Windows will open all files with the extension of .3eti with the text editor you have chosen. You will be able to edit the file and save it without changing the file properties.





You can now edit the file by adding the IP addresses of the 3e-525As that you want to manage, each in a pair of brackets [ ].

The two files SampleRadioOn.3eti and SampleRadioOff.3eti must be edited as a minimum. This will permit you to turn all the APs on or off at will. You can save them to another file name if you wish (maintaining the same file extension.) Note, if you turn all APs off and then re-enable transmit power, be aware that the clients, which have also been turned off, will have to be individually re-engaged, either by rebooting or by re-inserting the PC Card.



You can customize files to control only certain APs or groups of APs. Each AP that you group into a configuration file must have the same Admin Password.

The following gives you a sample of the code that you can use from the SampleRadioOn.3eti file.

### Sample of coding in SampleRadioOn.3eti file

```
# This Sample Configuration file shows how to turn the radio
# to a fixed level on all units

[all]
Wireless Tx Pwr Mode:=Fixed
#For FIPS units use the following
#Gateway Access Mode:=HTTPS
#Gateway Username:=CryptoOfficer

#Each unit that you want to turn on should be listed here

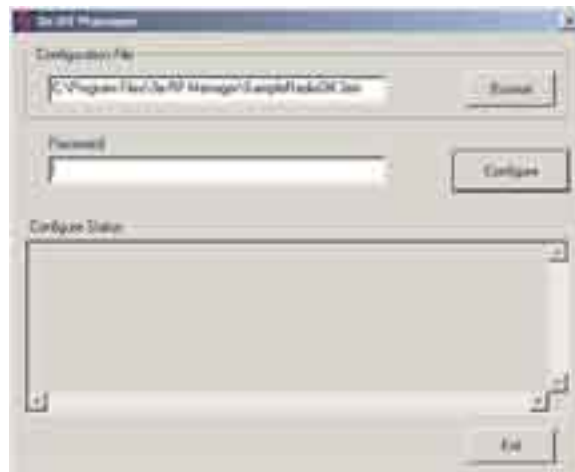
#First unit
[192.168.15.1]
Wireless Fixed Pwr Level:=2

#Next unit
[192.168.15.2]
Wireless Fixed Pwr Level:=2
```

Once you have edited the file, save it. You can now update the APs you have included in your configuration files from an Ethernet connection on your network.

To test out the files you have edited, on the main RF Manager screen, browse to and select the file that you want to use to manage your APs. That file name should now appear in the Configuration File window.

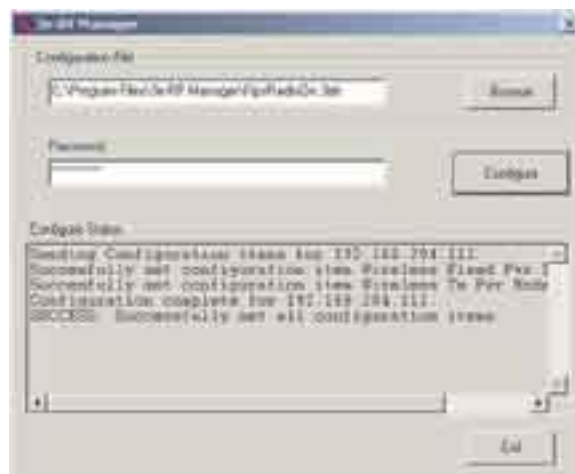
Now enter the Password for that group of APs.



Finally, hit the **Configure** button.

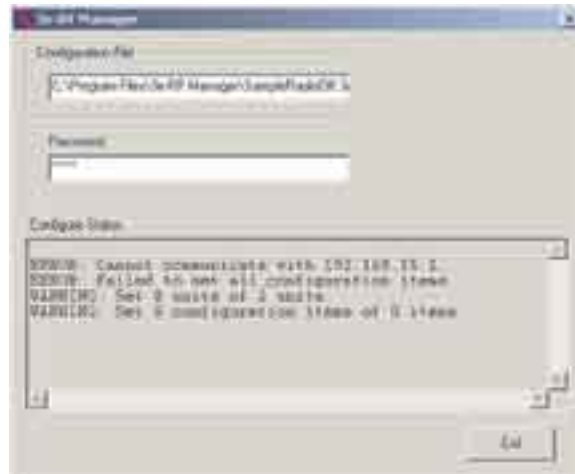
The Configure Status window will keep you informed of the progress of the update.

If your update has been successful, you should see a message that indicates you have successfully set all configuration items.



### 3e-525A Wireless Access Point

If any part of your update has failed, the Configure Status window will show you that it has failed in part or in whole and direct you to the area of the configuration file that you need to fix.



## Chapter 7: Network Printer Setup

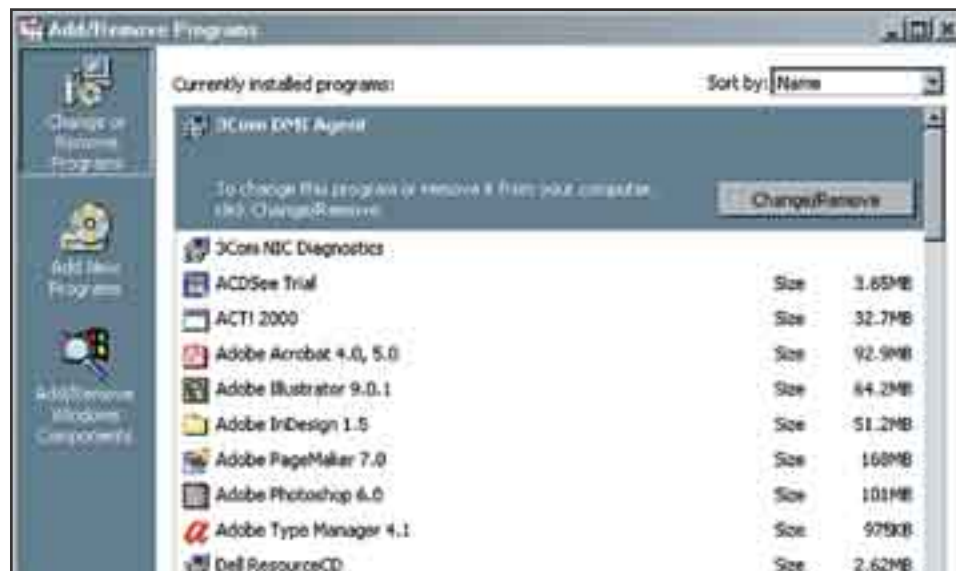
If you want to have the 3e-525A operate as a printer server, connect a printer to the wireless gateway now. The following instructions cover how to set it up using Windows 2000 as your operating system. (Windows XP is similar to Windows 2000.)

### Install Print Service for Unix (Windows 2000):

1. Open the Control Panel and select **Add/Remove Programs**



2. In the **Add/Remove Programs** window, on the left navigation bar, select **Add/Remove Windows Components**.



3. In the Add/Remove Windows Components wizard, select Other Network File and Print Services.



4. Click **Next** and the wizard will install this component. You may need your windows install CD.
5. Windows informs you that the action is complete. Click **Finish** and close the prior screen.

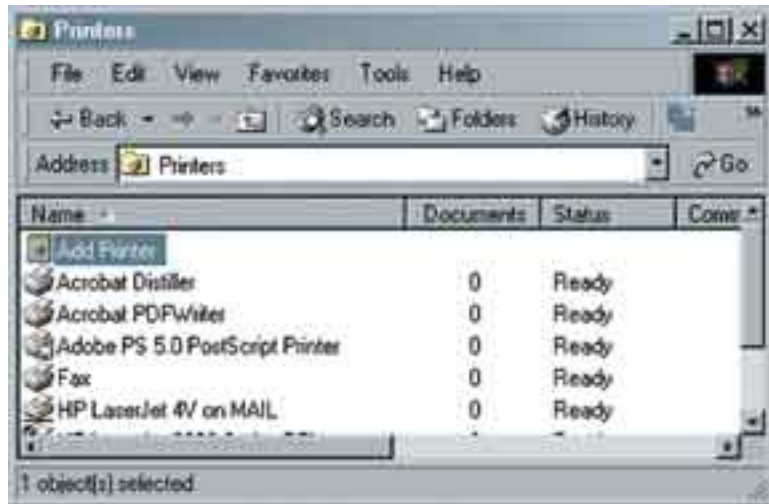
## Set Up the Printer

Now you are prepared to set up your new printer resource. Follow this procedure:

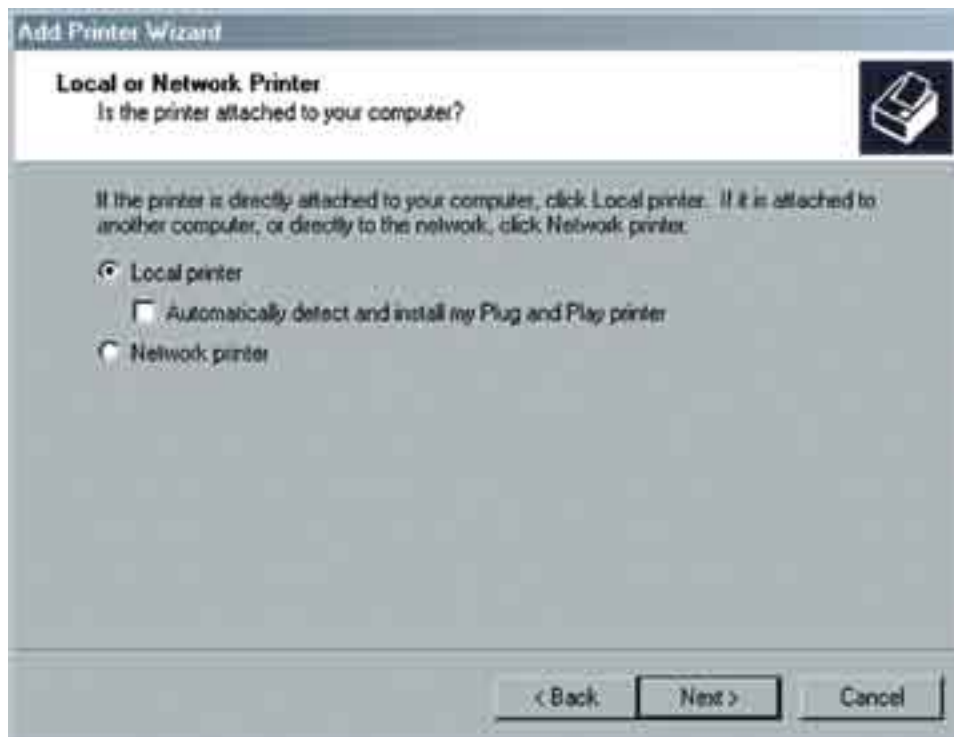
1. Access the **Control Panel** and select the **Printers** icon as shown on the following picture.



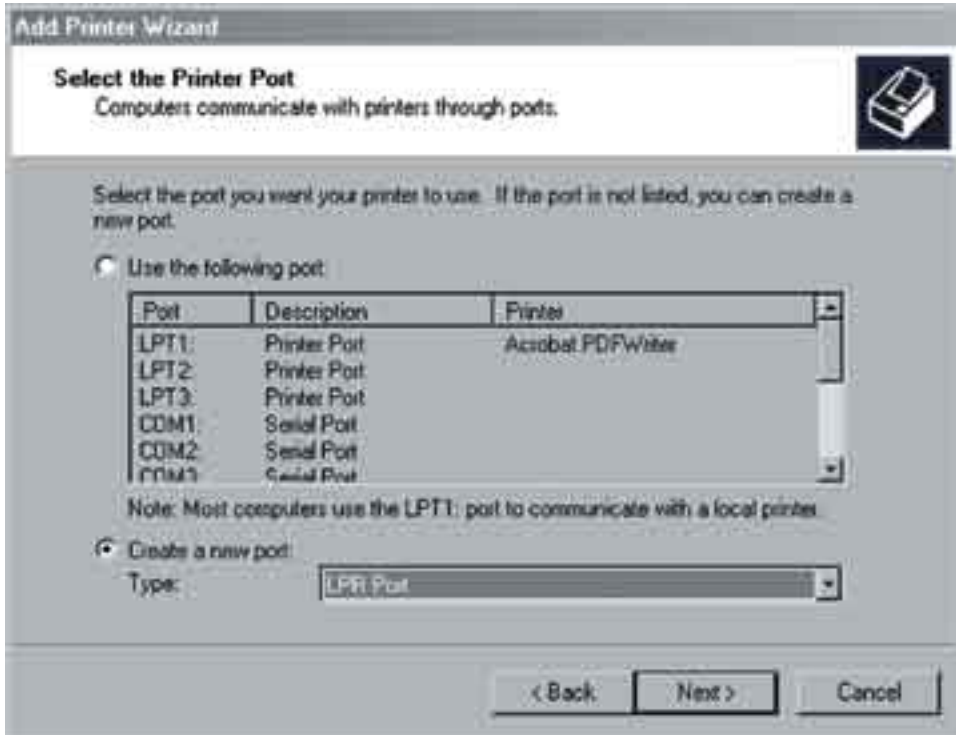
2. From the **Printers** window, select **Add Printer**.



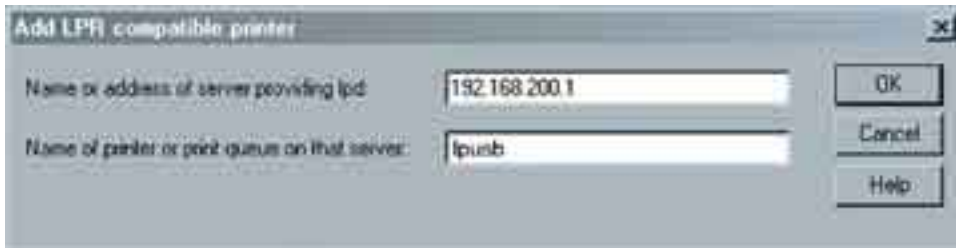
3. The Add Printer Wizard starts. Click Next.
4. From the following screen, select **Local Printer** and uncheck the selection: **Automatically detect and install my Plug and Play printer**. Then click Next.



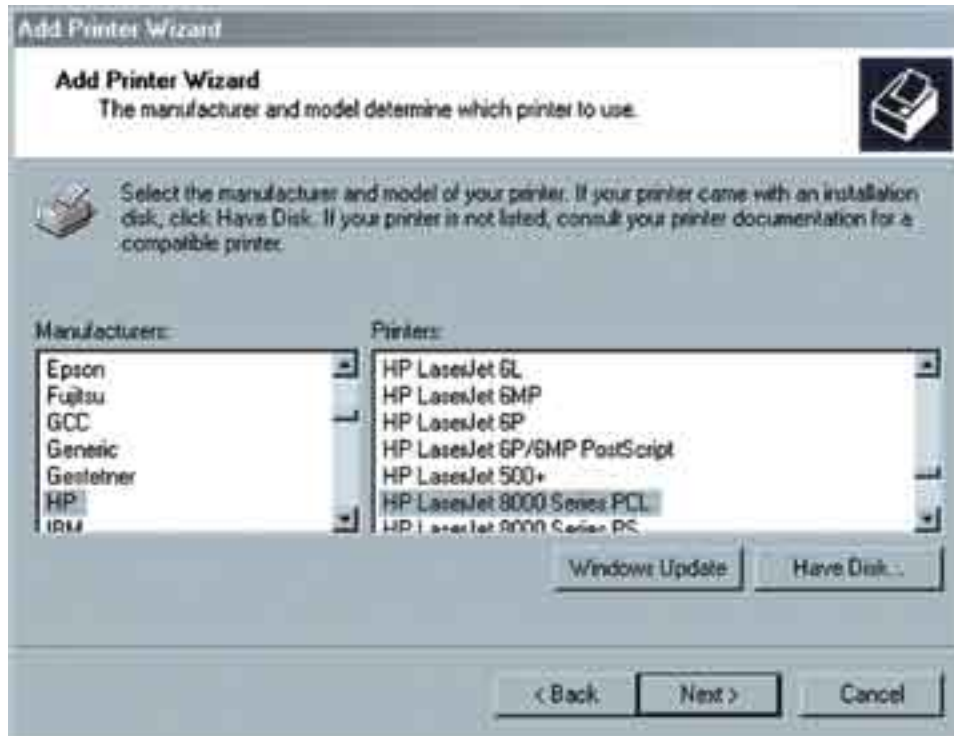
5. Select **Create a new port** and use the arrow to find and highlight **LPR Port**. Then click **Next**.



6. Next, in the field for Name or address of the server providing lpd: type the IP address assigned to the 3e-525A LAN. In the field for Name of printer or print queue on the server: type **lp** or **lpusb**. Then click **OK**.



7. In the next screen, locate first the manufacturer for the printer you are using, then the specific model of printer you are using. Then click **Next**.



8. You will be asked to provide additional information. Continue through the wizard screens until you reach the last. Then click **Finish**.



**Important Note:** On the **Printer Sharing** screen, do not select to "share" the printer. The Access Point does the sharing, not the printer.

It is a good idea to print a test page to confirm that the setup has been successful. After you complete the printer's setup, you will also need to ensure that each device that needs to access the printer on the network is properly configured by performing the procedure detailed above.

The above procedure applies to Windows 2000. Windows XP is similar. If you have another version of Windows, there are Microsoft sites that will provide directions.



This page intentionally left blank.

## **Chapter 8: Technical Support**

### **Manufacturer's Statement**

The 3e-525A is provided with warranty. It is not desired or expected that the user open the device. If malfunction is experienced and all external causes are eliminated, the user should return the unit to the manufacturer and replace it with a functioning unit.

If you are experiencing trouble with this unit, the point of contact is:

support@3eti.com

or visit our website at

www.3eti.com

### **Radio Frequency Interference Requirements**

This device has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission's Rules and Regulations. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Installation should be accomplished using the authorized cables and/or connectors provided with the device or available from the manufacturer/distributor for use with this device. Changes or modifications not expressly approved by the manufacturer or party responsible for this FCC compliance could void the user's authority to operate the equipment.

## **Channel Separation and WLAN Cards**

There are two WLAN cards in this access point. One is used for the Access Point function; the other is used for the Bridge. Channel Separation is required to reduce interference between the AP and Bridge WLAN cards. We have found that assigning 11 to the AP WLAN card channel and 4 to the Bridge WLAN card has given the optimum channel separation in test installations.

## Glossary

### **3DES**

Also referred to as Triple DES, a mode of the DES encryption algorithm that encrypts data three times.

### **802.11**

802.11 refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997.

### **802.11b (also referred to as 802.11 High Rate or WiFi)**

802.11b is an extension to 802.11 that applies to wireless LANs and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.

### **802.11g**

802.11g applies to wireless LANs and provides 20-54 Mbps in the 2.4 GHz band. Because 802.11g is backwards-compatible with 802.11b, it is a popular component in WLAN construction. 802.11g uses OFDM (orthogonal frequency division multiplexing) technology.

### **Access Point**

An access point is a gateway set up to allow a group of LAN users access to another group or a main group. The access point doesn't use the DHCP server function and therefore accepts IP address assignment from the controlling network.

### **AES**

Short for Advanced Encryption Standard, a symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously.

### **Bridge**

A device that connects two local-area networks (LANs), or two segments of the same LAN that use the same protocol, such as Ethernet or Token-Ring.

### **DHCP**

Short for Dynamic Host Configuration Protocol, DHCP is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address. Many ISPs use dynamic IP addressing for dial-up users.

### **NMS (Network Management Station)**

Includes such management software as HP Openview and IBM Netview.

**PC Card**

A computer device packaged in a small card about the size of a credit card and conforming to the PCMCIA standard.

**PDA (Personal Digital Assistant)**

A handheld device.

**SNMP**

Simple Network Management Protocol

**SSID**

A Network ID unique to a network. Only clients and access points that share the same SSID are able to communicate with each other. This string is case-sensitive. Wireless LANs offer several security options, but increasing the security also means increasing the time spent managing the system. Encryption is the key. The biggest threat is from intruders coming into the LAN. You set a seven-digit alphanumeric security code, called an SSID, in each wireless device and they thereafter operate as a group.

**TKIP**

Temporal Key Integrity Protocol. TKIP is a protocol used in WPA. It scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

**VPN (Virtual Private Network)**

A VPN uses encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

**WLAN (Wireless Local Area Network)**

A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.

**WPA**

WPA stands for WiFi Protected Access. It's an interim standard developed by the WiFi Alliance pending full ratification of the 802.11i standard, to protect the wired band and improve upon the old WEP encryption standard.