



Wireless Access Point User's Guide *Model 3e-531AP*



3e Technologies International
700 King Farm Blvd., Rockville, MD 20850
(301) 670-6779 www.3eti.com

This page intentionally left blank.

3e Technologies International's Wireless Access Point

User's Guide

Model 3e-531AP

Safety Requirements

- If AC power will be used, the socket outlet shall be installed near the equipment and shall be easily accessible.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.
- External Power to Earth (PE) or ground connector must be connected first and shall always be connected if power is applied to the unit.

3e Technologies International
700 King Farm Blvd.
Rockville, MD 20850
(301) 670-6779 www.3eti.com

Copyright © 2004 3e Technologies International. 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. Palm and Palm OS are registered trademarks of Palm, Inc. PRISM is a registered trademark of Intersil Corporation. Samsung, CC&C and Senao are registered trademarks of their companies respectively.

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

Chapter 1: Introduction	1
Basic Features	2
Wireless Basics.....	3
802.11b	3
Network Configuration	4
Access Point Configurations	4
Possible AP Topologies.....	4
Gateway Configurations	5
Bridging Mode	6
Default Configuration.....	6
Data Encryption and Security	6
SSID	7
AES and 3DES.....	7
Dynamic Key Management	7
Authentication	7
DHCP Server and NAT.....	8
Operator Authentication and Management	8
Management	8
Chapter 2: Hardware Installation	9
Preparation for Use.....	9
Installation Instructions	10
Minimum System and Component Requirements	10
Cabling	11
Indicator Lights.....	12
Chapter 3: Access Point Configuration	13
Introduction	13
Preliminary Configuration Steps	14
Initial Setup using the “Local” Port	14
System Configuration.....	16
General	16
WAN	17
LAN	18
Operating Mode.....	18
Wireless Setup	19
General	19
Encryption	21
Dynamic Key Management	21
Static 3DES Key/Open System Authentication.....	21
Static AES Key/Open System Authentication	22
MAC Address Filtering	23
Bridging and Bridging Encryption	23
Rogue AP Detection	24
802.1x.....	24
Advanced.....	25
Services Settings	26
DHCP Server	26
Print Server	26
SNMP	27
User Management.....	28
List All Users	28
Add New User	28

Monitoring/Reports	29
System Status	29
Bridging Status.....	30
Wireless Clients.....	30
Rogue AP List.....	32
DHCP Client List	32
System Log	33
Web Access Log	33
Network Activites	34
System Administration	34
Firmware Upgrade	34
Self-Test	35
Factory Default	36
Remote Logging.....	36
Reboot	37
Utilities	37
Chapter 4: Gateway Configuration	39
Introduction	39
Configuring in Gateway Mode	41
System Configuration.....	43
General	43
WAN	43
LAN	44
Operating Mode.....	45
Wireless Configuration	45
General	45
Encryption	47
WEP (RC4) Data Encryption	47
Static 3DES Key/Open System Authentication.....	47
Static AES Key/Open System Authentication.....	48
Mac Address Filtering.....	49
Rogue AP Detection	50
802.1x.....	50
Advanced.....	51
Services Settings	52
DHCP Server	52
Print Server.....	53
SNMP Agent.....	53
Firewall.....	54
Content Filtering.....	54
IP Filtering	55
Port Filtering	55
Virtual Server	56
Demilitarized Zone (DMZ)	57
Block WAN ICMP.....	58
User Management.....	58
List All Users	58
Add New User	59
Monitoring/Reports	60
System Status	60
Wireless Clients.....	60
Rogue AP List.....	61
DHCP Client List	61
System Log	62

Web Access Log	62
Network Activites	63
System Administration	63
Firmware Upgrade	63
Factory Default	64
Remote Logging.....	64
Reboot	65
Utilities.....	65
Chapter 5: Bridge Configuration	67
Introduction	67
Preliminary Setup	67
General Bridge Setup	68
Bridging Type Configuration	71
Point-to-Point Bridge Configuration	71
Point-to-Point Bridging Setup Guide.....	72
Point-to-Multipoint Bridge Configuration	75
Point-to-Multipoint Bridging Setup Guide	76
Back-to-Back Bridge Configuration	76
Back-to-Back Bridging Setup Guide.....	77
Repeater Bridge Configuration	78
Repeater Bridging Setup Guide	78
Chapter 6: PC Card Installation on a Laptop	79
Chapter 7: The RF Manager Function	81
Introduction	81
How to Access the RF Manager Function	82
How to Program the RF Manager	83
Chapter 8: Network Printer Setup	87
Install Print Service for Unix (Windows 2000):	87
Printer Setup	88
Chapter 9: Technical Support.....	93
Manufacturer’s Statement	93
Radio Frequency Interference Requirements.....	93

3e-531AP Navigation Options		
Access Point		Gateway
Not FIPS 140-2	FIPS 140-2	Not FIPS 140-2
System Configuration	System Configuration	System Configuration
General	General	General
WAN	WAN	WAN
LAN	LAN	LAN
Operating Mode	Operating Mode	Operating Mode
Wireless configuration	Wireless configuration	Wireless configuration
General	General	General
Encryption	Encryption	Encryption
Bridging	Bridging	
MAC Address Filtering	MAC Address Filtering	MAC Address Filtering
Rogue AP detection	Rogue AP detection	Rogue AP detection
802.1x		802.1x
Advanced	Advanced	Advanced
Services Settings	Services Settings	Services Settings
DHCP Server	DHCP Server	DHCP Server
Print Server	Print Server	Print Server
SNMP agent		SNMP agent
Firewall	Firewall	Firewall
		Content Filtering
		IP Filtering
		Port Filtering
		Virtual Server
		DMZ
		Block WAN IP ICMP
User Management	User Management	User Management
List All Users	List All Users	List All Users
Add New User	Add New User	Add New User
Monitoring Reports	Monitoring Reports	Monitoring Reports
System Status	System Status	System Status
Bridging Status	Bridging Status	
Wireless clients	Wireless clients	Wireless clients
Rogue AP List	Rogue AP List	Rogue AP List
DHCP Client List	DHCP Client List	DHCP Client List
System Log	System Log	System Log
Web Access Log	Web Access Log	Web Access Log
Network Activities	Network Activities	Network Activities
System Administration	System Administration	System Administration
Firmware Upgrade	Firmware Upgrade	Firmware Upgrade
	Self-Test	
Factory Default	Factory Default	Factory Default
Remote Logging	Remote Logging	
Reboot	Reboot	Reboot
Utilities	Utilities	Utilities

Chapter 1: Introduction

This manual covers the installation and operation of the 3e Technologies International's 3e-531AP Wireless Access Point, which conforms to the requirements of FIPS PUB 140-2, Security Requirements for Cryptographic Modules. The 3e-531AP Wireless Access Point provides a connection between an Ethernet LAN and a wireless LAN (WLAN). The wireless LAN can include mobile devices such as handheld Personal Data Assistants (PDAs), mobile web pads, and wireless laptops as long as they 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-531AP incorporates Power over Ethernet (PoE), IEEE 802.3af, and the highest security functionality including the ability to manage RF centrally and to even shut off RF to wireless devices entirely, should that be necessary. The PoE solution eliminates the need for internal gateway power supply units (AC-DC converters) and 110-220V cabling installations for the gateway operation. In the 3e-531AP, however, the capability to switch to AC power has been provided as a backup in the event the Power over Ethernet hub is lost or unavailable. The device detects power failure and automatically switches to AC current with minimal wireless connection interruption using the power cord provided. (Note: a power cord does not have to be plugged in to the 3e-531AP during setup, but it is recommended that it be kept available for use in case of failure of the PoE Power Supply.)

The PoE interface on the 3e-531AP is compatible with commercial vendor "injected power" hub units (also known as Ethernet Power Supply or Power over Ethernet Hub) interfaces.

The 3e-531AP conforms to the FIPS 140-2 specification. It includes the following cryptographic modules: AES/3DES for wireless encryption; dynamic key exchange (Diffie-Hellman module 1024) for wireless communication; and HTTPS/TLS, for secure web communication. The 3e-531AP contains three cryptographic modules and ports: Ethernet WAN uplink interface for communication to the wired LAN backbone; Ethernet LAN local port for communication to a local wired LAN; and wireless LAN port for wireless communication to local clients. The authorized roles supported are Crypto Officer Role and Administrator Role. Cryptographic services provided include; AES and 3DES for wireless; SHA-1 for authentication; HMAC SHA-1 for keyed authenticated firmware upgrade;

Diffie-Hellman Key Exchange; and HTTPS/TLS for web services via a secure link. Operator Authentication is performed by assigning operator type: Administrator can view configurations and logs, can do non-cryptographic functions such as assigning hostname, domain name, system date/time, TX Pwr Mode/Level and the like; the Crypto Officer role has total access and control and can perform cryptographic initialization or management functions such as module initialization, input or output of cryptographic keys and CSPs, and audit functions.

The 3e-531AP is wall-mountable and physically sealed with special tape for physical security. Violation of the unit's integrity will cause the unit to fail and display an Error State alarm, requiring reboot.

Basic Features

The 3e-531AP 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.

It has the following features:

- Local Ethernet LAN
- Ethernet uplink WAN
- Wireless (802.11b) interface with operating range of 2000+ feet
- AES/3DES encryption
- HTTPS/TLS secure Web
- 802.1x/EAP-TLS
- Sealed cover with tamper-proof tape
- DHCP client/sever
- Firewall
- NAT
- Bridging Mode
- Repeater Mode
- Adjustable Radio Power
- MAC address filtering

The following cryptographic modules have been implemented in the 3e-531AP.

- AES for wireless (802.11b)
- 3DES for wireless (802.11b)
- 802.1x/EAP-TLS for authentication
- SHA-1
- HMAC SHA-1 for firmware upgrade

Wireless Basics

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

The 3e-531AP incorporates the 802.11b (Wi-Fi) 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), establishes a stable standard. A user with an 802.11b product can use any brand of gateway/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.

802.11b uses DSSS (direct-sequence spread spectrum) for radio communication. Direct-sequence systems communicate by continuously transmitting a redundant pattern of bits called a chipping sequence. The chipping sequence is combined with a transmitted data stream to produce the wireless output signal.

For wireless devices to communicate with the 3e-531AP, they must meet the following conditions:

- The signal strength must be sufficient;
- The wireless device and wireless gateway 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-531AP);
- Encryption and authentication capabilities and types enabled must conform;
- The wireless device and wireless gateway must have compatible data rate configurations; and
- If MAC filtering is used, the 3e-531AP must be configured to allow the wireless device's MAC address to associate (communicate) with the 3e-531AP wireless interface.

Network Configuration

The 3e-531AP is capable of various configurations. The three basic configurations are:

- Access point mode with wired infrastructure
- Gateway mode with wired infrastructure
- Wireless bridging with choice of:
 - Point-to-point setup
 - Point-to-multipoint setup
 - Repeater setup

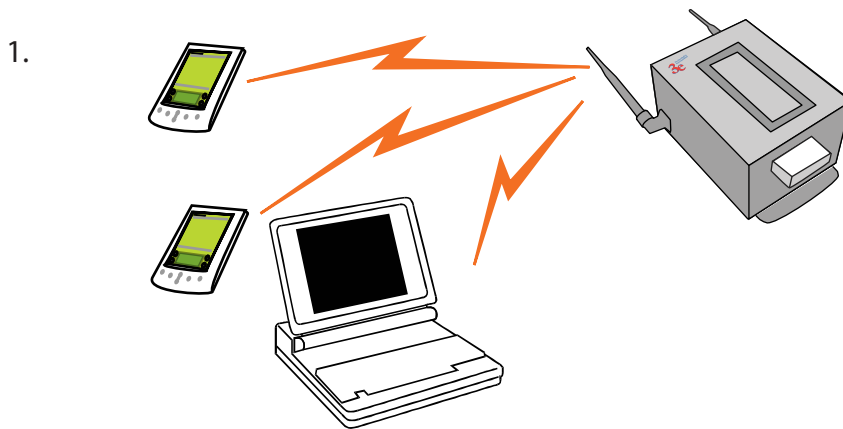
Bridging actually has more choices, but the above choices are popular and are discussed later in this user guide.

Access Point Configurations

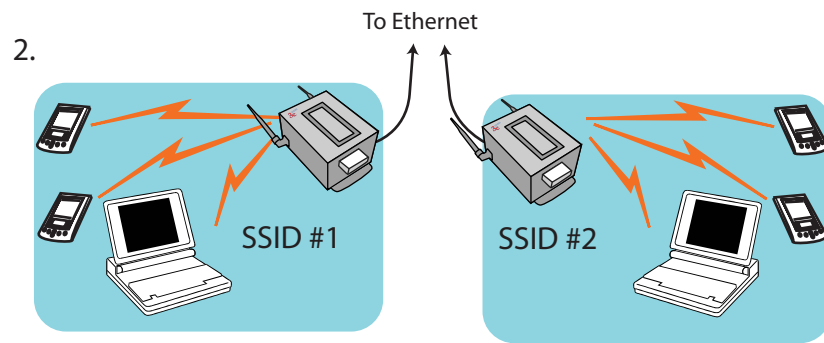
When a 3e-531AP is configured as an access point, IP addresses for wireless devices are typically assigned by the wired network's DHCP server. The wired LAN's DHCP server assigns addresses dynamically, and the AP virtually connects wireless users to the host wired network. All wireless devices connected to the AP are configured on the same sub-network as the attached wired network interface and can be accessed by devices on the wired network.

Possible AP Topologies

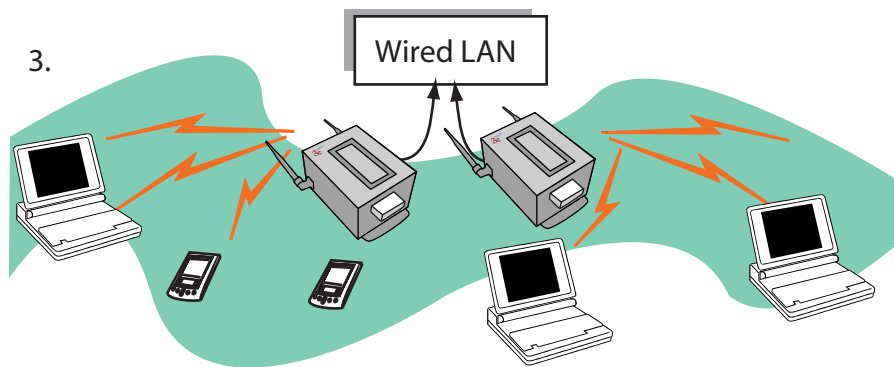
1. An access point can be used as a single AP without any connection to a wired network. In this configuration, it simply provides a stand-alone wireless network for a group of wireless devices.



2. The 3e-531AP 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).



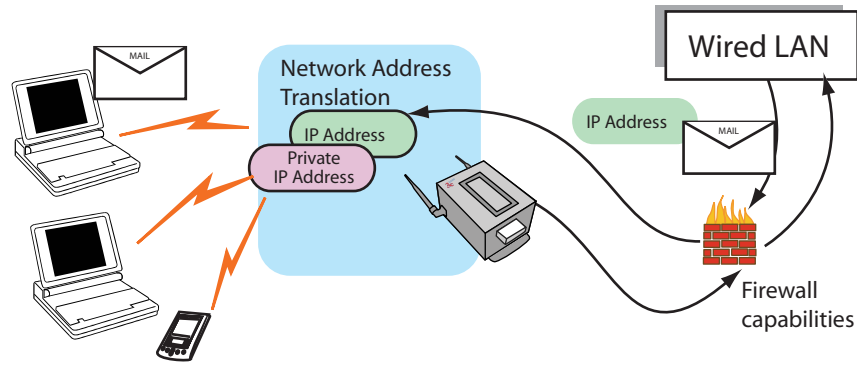
3. And lastly, multiple APs connected to a wired network and operating off that network's DHCP server can provide a wider coverage area for wireless devices, enabling the devices to "roam" freely about the entire site.



Gateway Configurations

In gateway mode, wireless users are provided additional firewall protection from the rest of the industrial or shipboard network or Internet using Network Address Translation (NAT) protocol features and firewall options.

Wireless users can still communicate with the wired network resources but communication must be initiated by the wireless devices. Using the NAT protocol, the only IP address visible to the wired network is that of the gateway itself, as assigned by the wired Ethernet DHCP server. The gateway provides firewall protection to its wireless users. It can dynamically assign private addresses to member devices using its own internal DHCP server. It acts as a router, not a bridge, and controls traffic flow and access control between the wired and wireless networks.



Alternately, if you wish, the network administrator can assign static addresses to the member wireless devices. In order to set static addresses, the system administrator will need to manually configure the TCP/IP configuration on each wireless device.

Bridging Mode

The wireless bridging function in the 3e-531AP allows setup as a bridge, in a number of alternate configurations, including the following popular configurations:

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

Default Configuration

By default, the 3e-531AP boots up in access point mode. See your network administrator or more advanced technical sections of this User's Guide for information if the device is to be configured in gateway mode or bridging mode.

Data Encryption and Security

The 3e-531AP Wireless Access Point includes advanced wireless security features, including Dynamic Key Management or Static key AES or 3DES encryption. AES or 3DES and MAC Address authentication are available in the 3e-531AP in all modes, and some level of encryption is recommended. In gateway mode, WEP encryption is an option.

The incorporation of AES and 3DES brings system security up to the most stringent standards. The functionality of these two enhancements, along with a more detailed discussion of the 3e-531AP security features, is further covered in the following paragraphs.

SSID

The Service Set ID (SSID) is a string used to define a common roaming domain among multiple wireless access points. Different SSIDs on gateways 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-531AP setup menus.

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 necessary. AES is incorporated into all current and future models of 3e Technologies International's series of wireless APs/gateways.

3DES is also incorporated on the 3e-531AP. 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.

Dynamic Key Management

Addition of Security Server software (3e-030, sold separately), which is configured to dynamically assign secure key access, raises the security capability to its highest level. The Security Server software operates from a remote point on the WLAN and is accessed by pointing to its IP Address in each of the 3e-531APs on the WLAN as part of the wireless encryption configuration process.

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-531AP gateways, if set up to use MC 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 gateways.

DHCP Server and NAT

In AP mode, the 3e-531AP has a DHCP (*Dynamic Host Configuration Protocol*) server function that is accessible to the LAN port. If the 3e-531AP is set up in gateway mode, this DHCP function is available, with many firewall functions in addition, to both the LAN and WLAN ports. DHCP is a protocol for assigning dynamic IP addresses.

When the 3e-531AP is in access point mode, the DHCP function is accessible only from the local LAN port. A local LAN can be established from the LAN port and can utilize the DHCP function.

If the 3e-531AP is reconfigured for gateway mode, and the DHCP function is enabled, the gateway Ethernet uplink interface becomes the only visible IP address to the Ethernet network. It uses Network Address Translation (NAT) to forward packets from wireless devices as if they were coming from the one visible IP address, managing a database of information in order to sort out and forward the replies to the correct client. NAT provides an additional layer of security by protecting information on the wireless LAN from direct access by the Ethernet LAN.

Operator Authentication and Management

Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.

There are two types of operators defined:

- **Crypto Officer:** The Crypto Officer user has total control of the gateway. The Crypto Officer can configure the encryption keys and upload firmware.
- **Administrator:** The Administrator can view configurations and logs, can do non-cryptographic functions such as assigning host-name, domain name, system date/time, TX Pwr Mode/Level and the like. This user can reboot the gateway if it is deemed necessary.

The Crypto Officer initially installs and configures the 3e-531AP after which the password should be changed from the default password. The enclosure itself must be physically secured.

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. For general maintenance, the Administrator logon should be sufficient.

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

Chapter 2: Hardware Installation

Preparation for Use

The 3e Technologies International's 3e-531AP Wireless Access Point requires physical mounting and installation on the site, following a prescribed placement design to ensure optimum operation and roaming. The 531AP must be professionally installed by an installer certified by the National Association of Radio and Telecommunications Engineers or equivalent institution.

If the 3e-531AP's Power over Ethernet (PoE) solution is being activated, it will, in addition, require the installation of a separate PoE-capable hub switch which "injects" DC current into the Cat5 cable. This injector device should have been specified and installed by a wireless LAN installation team.

To ensure that there is no possibility of danger from contact with the injected current should anyone open the 3e-531AP enclosure, each 3e-531AP device has been fitted with a safety interlock that functions as an internal circuit breaker to interrupt the flow of current when the device is opened.

The 3e-531AP package includes the following items:

- The FIPS-compliant 3e-531AP
- 2 attachable 5dBi omni-directional antennas
- Documentation as PDF files (on CD-ROM)
- Installable RF Manager utility (on CD-ROM)
- Registration card
- Warranty card

The following items are separately purchased in accordance with the exact dimensions of the network to be configured:

- Power cable with water-resistant circular connector
- Ethernet cable with special water-resistant circular connector



IMPORTANT NOTE: To comply with FCC RF expose compliance requirements, the antennas used with the 531AP 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-531AP is intended to be installed as part of a complete wireless design solution, and, as such, the design and architecture of that solution is unique to each location and is addressed in a separate document. Proper installation of the wireless system will ensure that users can “roam” freely throughout the serviced location, passing transparently from node to node with no loss of service but at the same time maintaining top security on the wireless LAN.

This manual deals only and specifically with the single 3e-531AP 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, four and five) only. A failed unit should be returned to the manufacturer for maintenance. Sites requiring emergency backup will maintain extra units of the device to interchange in case of failure.

Minimum System and Component Requirements

The 3e-531AP is designed to be attached to the wall or bulkhead at appropriate locations. To complete the configuration, you should have at least the following components:

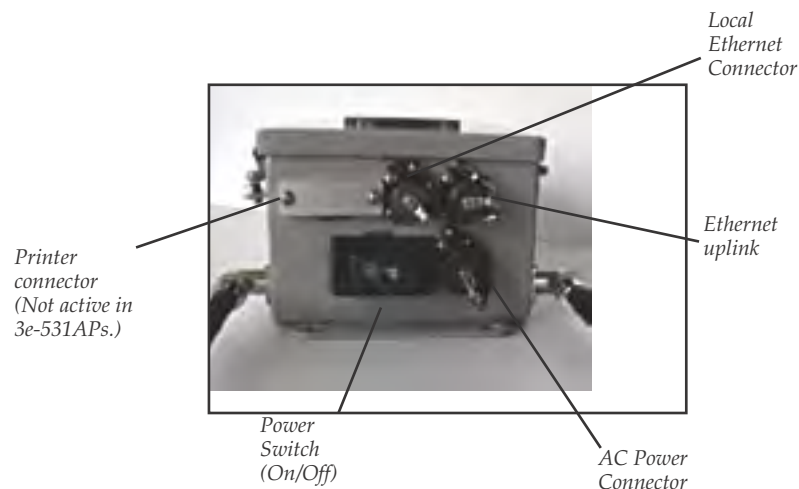
- PCs with one of the following operating systems installed: Windows NT 4.0, Windows 2000 or Windows XP;
- A compatible 802.11b PC Card or 802.11b device for each computer that you wish to wirelessly connect to your wireless network. (For wireless cards, select the 3e-110 PC Card with 3e-010F Crypto Client software (sold separately) or install the 3e-010F software with any compatible PC Card. (For maximum security and compatibility, we recommend the 3e Technologies International 3e-110 PC Card);

- 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. (The cable required will have a standard RJ-45 connector on one end and a circular connector on the other.)
- 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 Gateway.
- TCP/IP Protocol (usually comes installed on any Windows PC.)

Cabling

The 3e-531AP is well-protected in a metal enclosure which is generally bolted to the bulkhead. The front of the box is hinged but should not be opened, particularly if being employed as FIPS 140-2 compatible device.

The following illustration shows the external cabling on the 3e-531AP. However, even if the On-off switch is “on”, if the lid of the device is opened, power will cease to flow because of the safety interlock.



An AC Power Connector (not provided) can be plugged into an AC outlet. In some situations, the installation design may include elimination of the ability to plug the unit into an AC outlet. In such circumstances, the AC power is supplied (that is, hardwired) using the same AC Power Connector port. Usually, in the default configuration of the 3e-531AP, the AC Power Connector is not actively used. The socket outlet must be installed near the equipment and be easily accessible.

The Ethernet Uplink connector is used to connect the 3e-531AP to the shipboard LAN. When used as a PoE device, the Ethernet Uplink connector will have been routed from the unit to a PoE-capable hub switch which runs the power through the Ethernet cable to the unit. The Ethernet

cable is thus run from the 3e-531AP to the PoE-capable hub switch which is then connected to the wired LAN and to a power source.

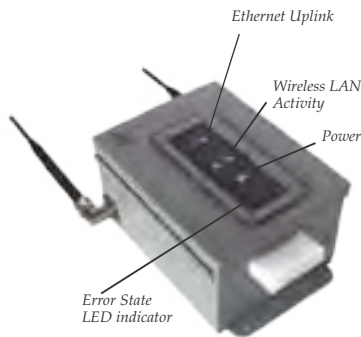
The 3e-531AP design includes an external Power Switch for the purpose of disabling power to the unit for servicing or removal.

Although a safety interlock is provided on the unit to disable power when the enclosure door is opened, AC and PoE power cables must be disconnected prior to servicing or removing the device. This is a precautionary measure.

An additional Ethernet connector labeled "Local" is designated for use during initial configuration. The installation team uses an RJ45 cable with Circular connector to connect the 3e-531AP to a laptop.

Indicator Lights

The top panel of the 3e-531AP contains a set of indicator lights (Light Emitting Diodes or LEDs) that help describe the state of various networking and connection operations.



This closeup shows the ground and one of the seals that are standard on the FIPS 140-2 compliant 3e-531AP. Note that the ground will be installed permanently on installation of the unit and should not be disturbed after that.

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. During firmware upgrades and resets, this light will blink
Ethernet Uplink	This light indicates the state of your connection to the shipboard 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 shipboard network.
Wireless LAN Activity	This light may be steady or blinking and indicates that information is passing through the connection.
Error State LED indicator	The Error State LED indicator will light to alert you if the device enters Error State. If the 3e-531AP enters an Error State, you must power down and up (using the On/Off switch), to allow it to invoke the power-up self tests.

Chapter 3: Access Point Configuration

Introduction

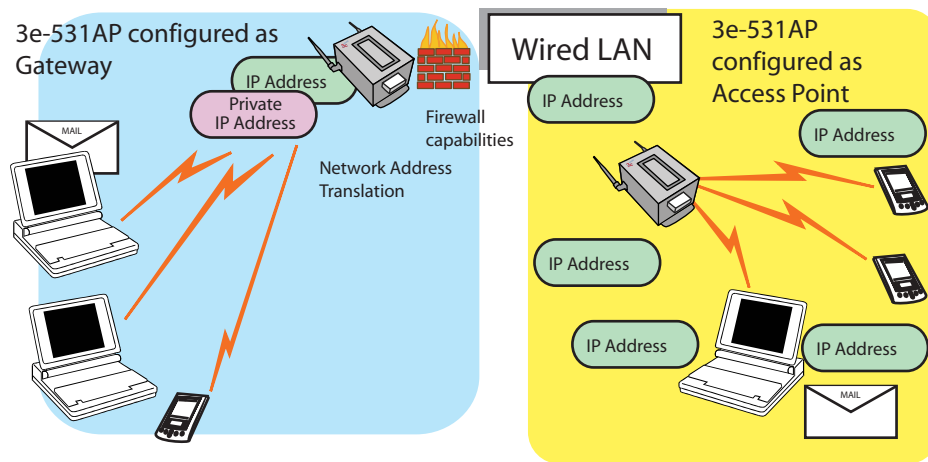
The 3e-531AP Gateway comes with the capability to be configured as either an access point, a gateway, or a bridge.

An “access point” is a device configured to allow one LAN to freely exchange data with another LAN without restriction. This is useful if you have an existing network and you want to extend it with a wireless network. For example, an existing wired LAN is extended by adding the 3e-531AP and thus bridging to the existing wired network resources configured to communicate with the wireless LAN.

The 3e-531AP default configuration is as an access point, allowing free roaming and data exchange with the existing LAN, bridging the wired and wireless networks.

In the event that certain areas of the network need greater security, the Administrator can alternatively, using the management software accessible through the WEB browser at the device’s assigned IP address, reconfigure it as a gateway.

This chapter follows the procedure for configuring the 3e-531AP as an access point. The procedure for configuring as a gateway is covered in Chapter 4. Bridging is addressed in Chapter 5.



Preliminary Configuration Steps

For preliminary installation the security officer (CryptoOfficer) should have the following information:

- IP address – a list of IP addresses that are assignable to be used for assignment to the APs
- Subnet Mask for the LAN
- Default IP address of the 3e-531AP
- 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-531AP network of access points (if MAC address filtering is to be enabled)
- Security Server IP Address, password, and Key type (if Dynamic Key Management will be used)
- The appropriate encryption key for Static 3DES or Static AES if static key management will be used.

Initial Setup using the “Local” Port

Initial setup of the 3e-531AP devices as a wireless LAN is accomplished by an installation team. The following information is provided for the CryptoOfficer for use if an additional 3e-531AP needs to be added to the configuration.

Plug one end of a separately purchased RJ-45 Crossover Ethernet cable with one circular connector to the LAN port of the 3e-531AP (see page 11) and the other end to an Ethernet port on your laptop. This LAN port in the 3e-531AP 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-531AP on the LAN port, you must be sure that the TCP/IP parameters on your laptop are 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 95/98 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.

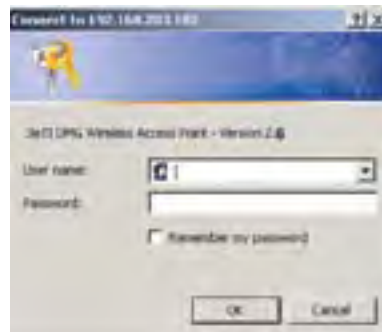
In Windows 95/98/Me, click **Start**, then **Run** and type **winipcfg** in the run instruction box. Then click **OK**. You will see the IP address of your laptop in the resulting window, along with the "default gateway" IP address. Verify that the IP address shown is 192.168.15.x

In Windows 2000, 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-531AP Local LAN in the address line. (<https://192.168.15.1>)



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

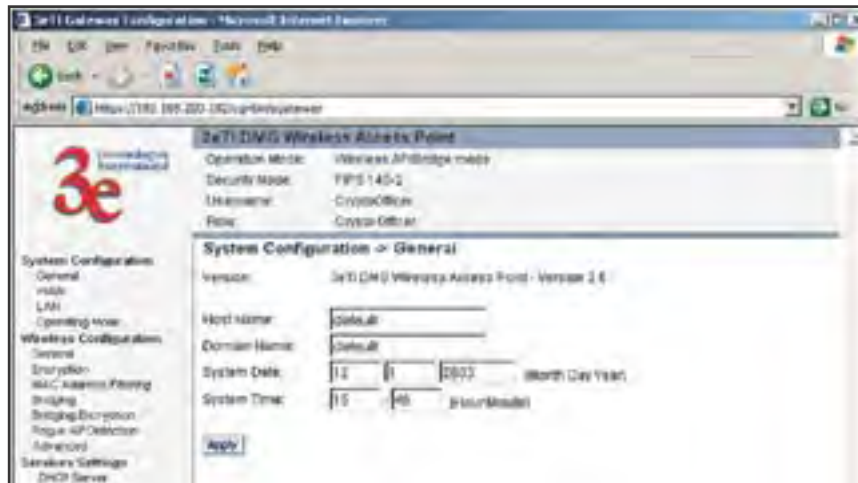


System Configuration

General

You will immediately be directed to the **System Configuration—General** page for the 3e-531AP access point.

This screen lists the firmware version number for your 3e-531AP 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**.

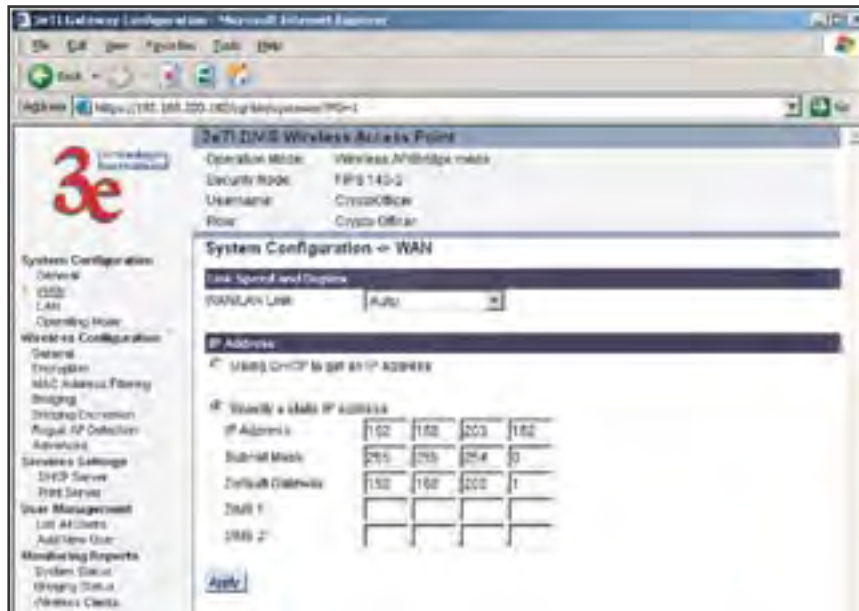


Go next to the **System Configuration—WAN** page.

WAN

Next, click the entry on the left hand navigation panel for **System Configuration -WAN**. You will be directed to the **System Configuration – WAN** page.

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-531AP 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.

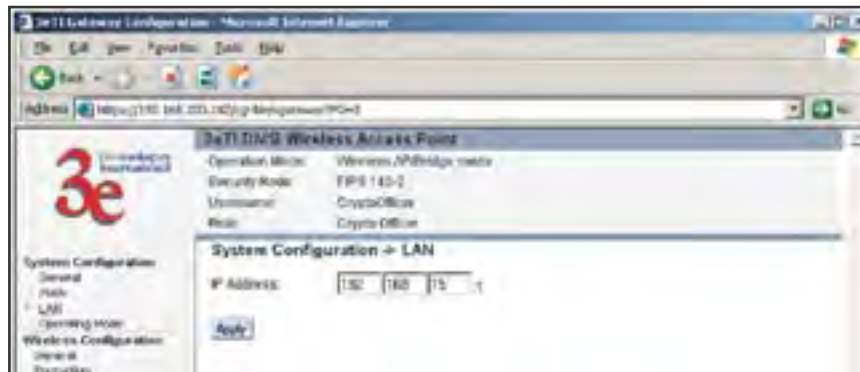


If not using DHCP to get an IP address, input the information that the access point requires in order to allow the wireless devices it controls access to the wired LAN. This will be the IP address, Subnet Mask, Default Gateway, and, where needed, DNS 1 and 2.

Click **Apply** to accept changes.

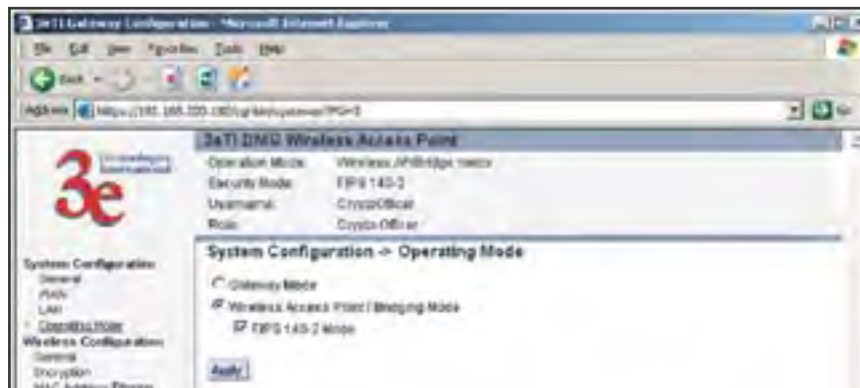
LAN

This sets up the default numbers for the first, second, or third octet for a possible private LAN function for the access point. The Local LAN port provides DHCP server functionality to automatically assign an IP address to a computer Ethernet port. It is not advisable to change the private LAN address while doing the initial setup as you are connected to that LAN.



Operating Mode

You need to visit this page only if you will be changing mode from Access Point or Bridge to Gateway or vice versa. The default setting is Access Point. Note that if you change mode, all previously entered information will be reset to factory settings. If in Access Point/ Bridging Mode, you can also select or deselect the FIPS 140-2 Mode. Selecting FIPS 140-2 Mode makes WEP, SNMP, and 802.1x unavailable as encryption options.



Wireless Setup

General

Wireless Setup allows your computer's PC card to talk to the Access Point.

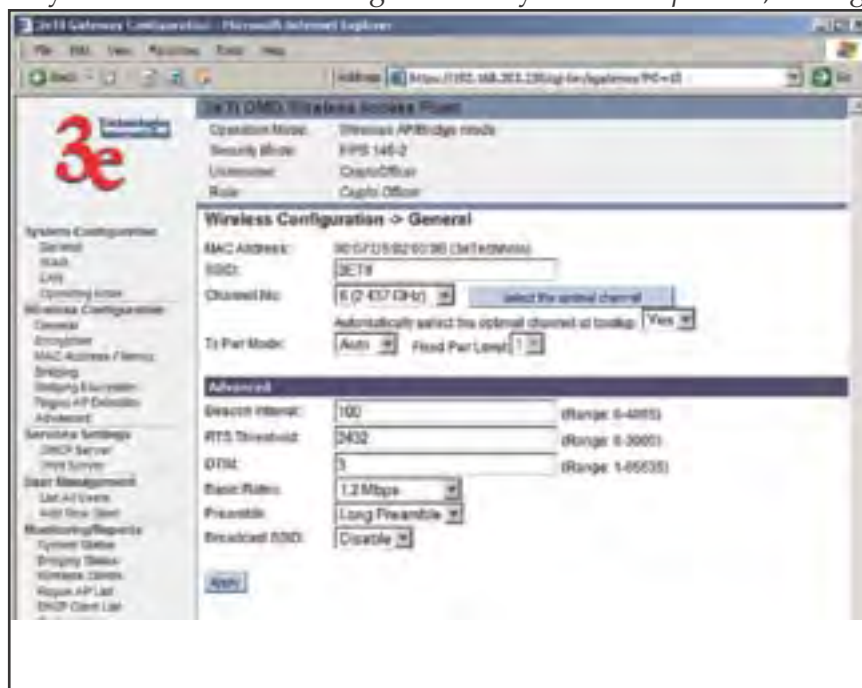
On the **Wireless Configuration — General** page, you must enter the SSID for the wireless LAN. This is also where you can assign a channel number to the AP (if necessary) and modify the Tx Pwr Mode.

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

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. You can assign channels manually or automatically, using the **Automatically select the optimal channel at bootup** function. If assigning manually, 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 wish to assign automatically, set the auto function to **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**.

If you have the 3e AP configured in any mode *except* FIPS, setting TX



Pwr Mode to **Off** will only shut off the power on that one AP.

If you have the 3e AP configured in FIPS mode and you have deployed the 3e-010F Crypto Client software v 2.6 or higher, however, you can use this management screen to turn off TX power to this particular AP and *all client devices associated with it*.

In FIPS Wireless AP mode, once you have given the command to turn off TX power, The screen called **Monitoring/Reports -> Wireless Clients** will contain a column called **EMCON** which shows the results of the command on any wireless device associated with the AP. This is more fully explained in **Chapter 7, The RF Manager Function**.

The 3e Access Point Installation CD contains the RF Manager Installation program. If you install this program, which is explained in Chapter 7, you can control the TX power level and TX power shutoff from a central location.

If you turn off TX power, whether from the **Wireless Configuration — General** page on each AP or using the RF Manager, turning it back on re-establishes it only in the AP or APs contacted. The wireless devices that are associated with those APs will need to re-establish power either by powering down and then powering up or by removing and reinserting the PC Card.

Use of the RF Manager allows a Crypto Officer or Administrator to manage TX Power level for a group of APs.

In the last section of the **Wireless Configuration — General** page, there are a number of advanced options which are described in the following chart:

Beacon interval	0-4095	The frequency in milliseconds in which the 802.11 beacon is transmitted by the AP.
RTS Threshold	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.
DTIM	1-65535	The number of beacon intervals between successive Delivery Traffic Identification Maps (DTIMs). This feature is used for Power Save Mode.
Basic Rates	- 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.
Preamble	Short/Long Preamble	Specifies whether frames are transmitted with the Short or Long Preamble.
Broadcast SSID	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-531AP is no encryption. It is

recommended that you set encryption as soon as possible. If your mode setting includes FIPS 140-2 mode, WEP encryption is not an option. WEP will appear as an option in AP mode if not using the ultra-secure FIPS 140.2 encryption settings.

Dynamic Key Management

Dynamic key management requires the installation of the 3e-030 Security Server software which resides on a self-contained workstation connected to the 3e-531AP over the Ethernet Uplink 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.

Static 3DES Key/Open System Authentication

If you do not have a Security Server installed, the 3e-531AP can accommodate static encryption using either AES or 3DES.

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

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.

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.

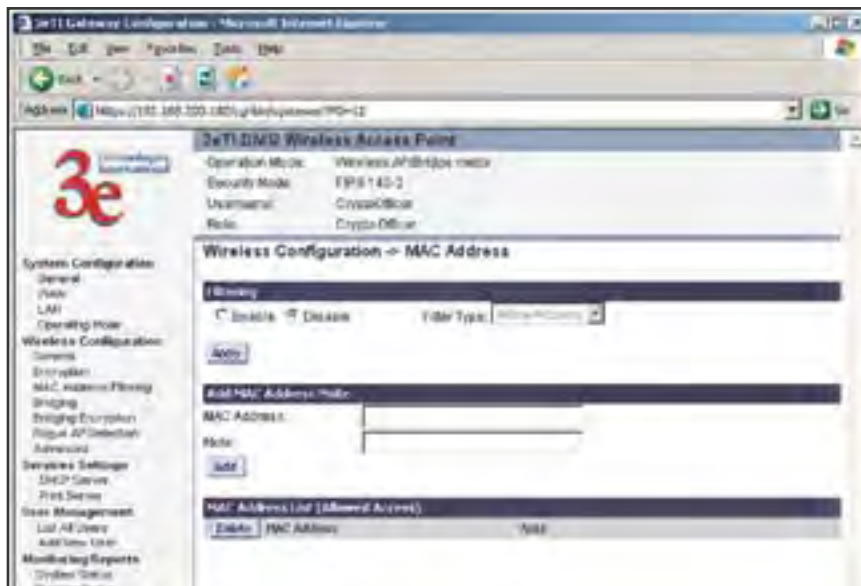


MAC Address Filtering

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

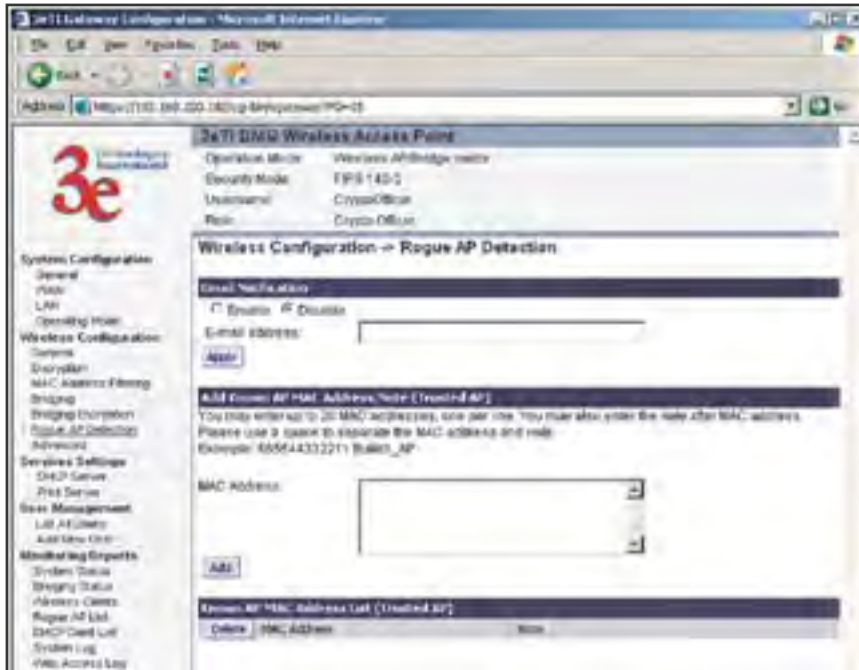
Bridging is covered in chapter five. If you will be deploying this 3e-531AP as a bridge, follow the instructions in chapter five.

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-531AP is located on the **Setup—General** page.

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

802.1x



802.1x is not available if you are using the FIPS 140-2 secure setup mode. 802.1x is a means of making a WEP encrypted system more secure.

Enabling 802.1x requires that you have at least one remote Radius server (preferably also a backup Radius server) but it will allow the use of the legacy WEP encryption key system with greater resultant security.

IEEE 802.1X offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1X ties a protocol called EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication.

If using 802.1x, you must know and input the IP address, Port Number and Shared Secret for the primary and backup Radius server and the key type selected on your Wireless Encryption page. Then set the accepted lifetime for the encryption key.

Advanced

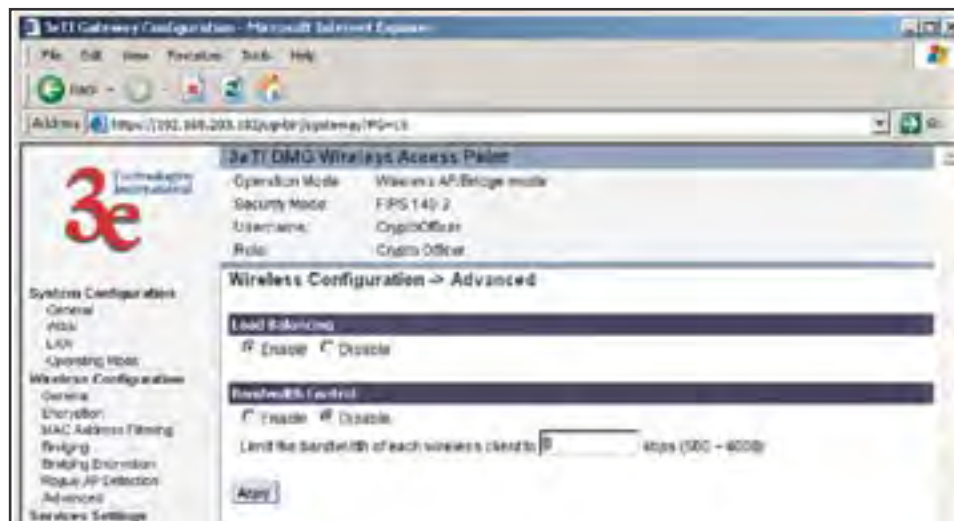
The Advanced page allows you to enable or disable load balancing

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 1 client is on the network, a maximum of 0.5 Mbps will be allowed that client. 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 it 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, on the other hand, 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.

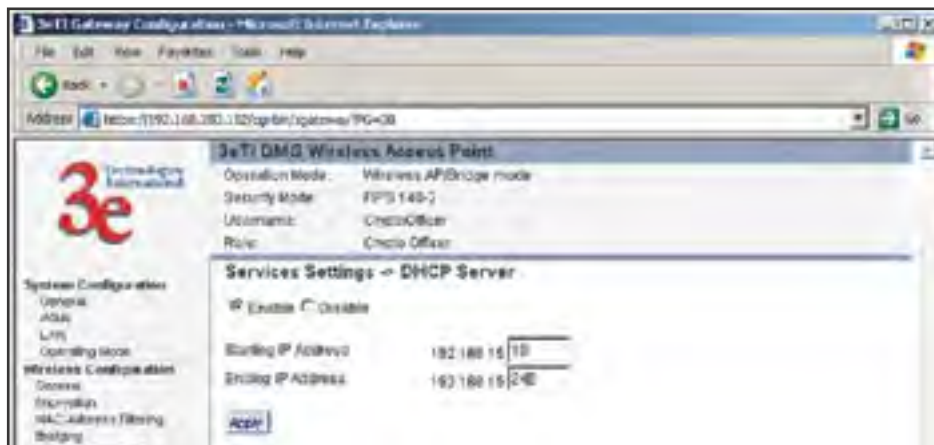
Once you have made any changes, click **Apply** to save.



Services Settings

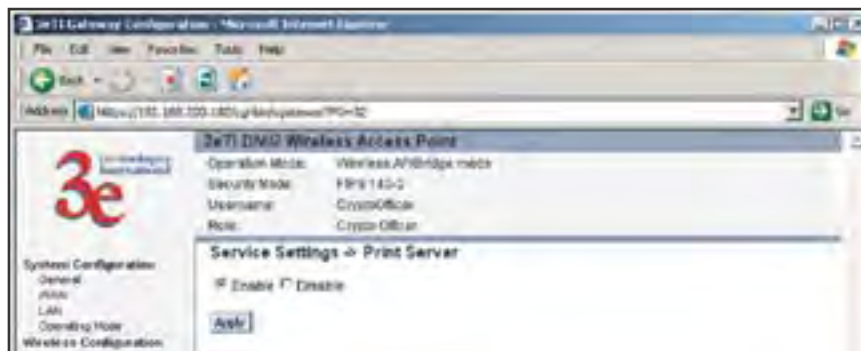
DHCP Server

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.



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 and leave the metal plate on the printer port. The metal plate is provided to protect that port from water.



SNMP

The SNMP (simple network management protocol) Agent is not available if you are using the FIPS 140-2 setup. SNMP is available in access point mode if FIPS 140-2 is left unchecked.

The SNMP 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-531AP'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

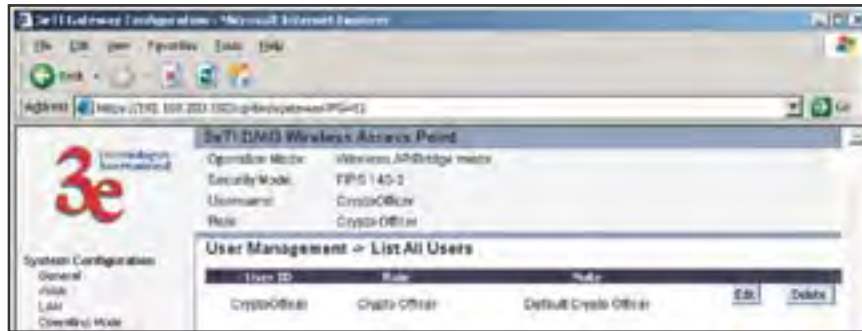
The SNMP configuration consists of several fields, which are explained below:

- **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.

User Management

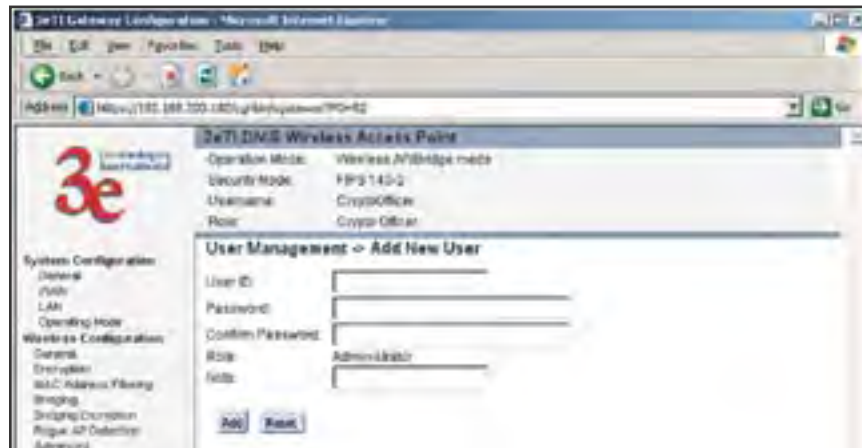
List All Users

The **List All Users** page simply lists all Crypto Officers and Administrators assigned.



Add New User

The Add New User screen allows you to add new Administrator users, assigning and confirming passwords. Only the Crypto Officer role is allowed to add a new Administrator to the 3e-531AP. 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.



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-531AP device and network interface details and the Routing Table.

The screenshot shows the web interface of a 3e-531AP Wireless Access Point. The browser address bar shows `http://192.168.255.254/cgi-bin/gateway/PGW2`. The page title is "3e-531AP Wireless Access Point".

Device Information:

- Operation Mode: Wireless AP/Bridge mode
- Security Mode: FIPS 140-2
- Manufacturer: Cisco/Orion
- Model: Cisco 0808

Monitoring/Reports -> System Status

Device Status

- Security Mode: FIPS 140-2 Level 2
- Current Encryption Mode: BYPASS MODE
- Bringing Encryption Mode: BYPASS MODE
- System Uptime: 1:25:48
- Total Usable Memory Size: 29518872 bytes
- Free Memory: 15470880 bytes
- Current Processor: T8

Other Information: [CPU](#) [NCP](#) [Statistics](#) [Processes](#) [Data Paths](#)

Network Interface Status

- VLAN Eth0/0 MAC address: 62:31:83:01:27:88
- LAN Ethernet MAC address: 62:31:83:01:25:38
- Primary VLAN MAC address (802.1P): 62:31:83:01:27:88

Routing Table

Dest. LAN IP	Subnet Mask	Default Gateway	Hop Count	Interface
192.168.255.0	255.255.255.0	-	0	eth0
192.168.252.0	255.255.252.0	-	0	br0
Default	0.0.0.0	192.168.252.1	0	br0

Copyright © 2002-10, Cisco Systems, Inc. All rights reserved.

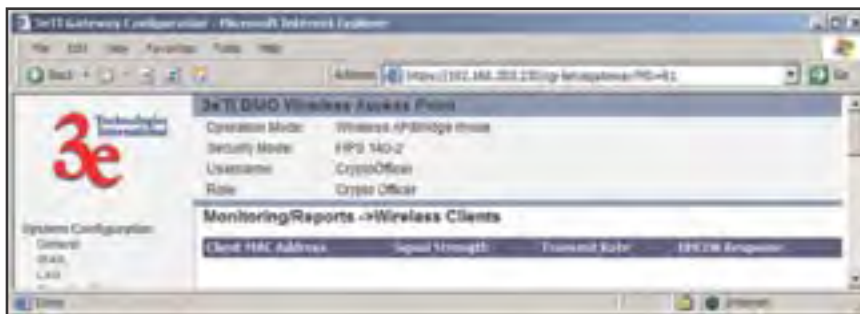
Bridging Status

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



Wireless Clients

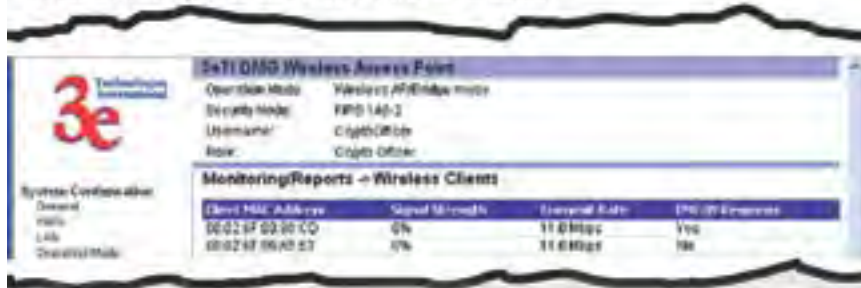
The Wireless Clients report screen displays the MAC Address of all wireless clients and their signal strength and transmit rate.



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.

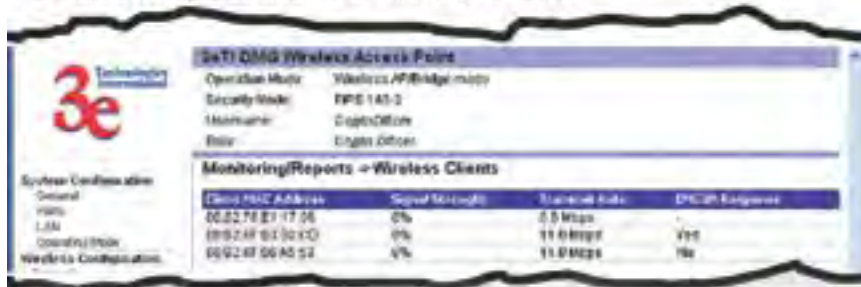
1. EMCON response when TX Power is disabled



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

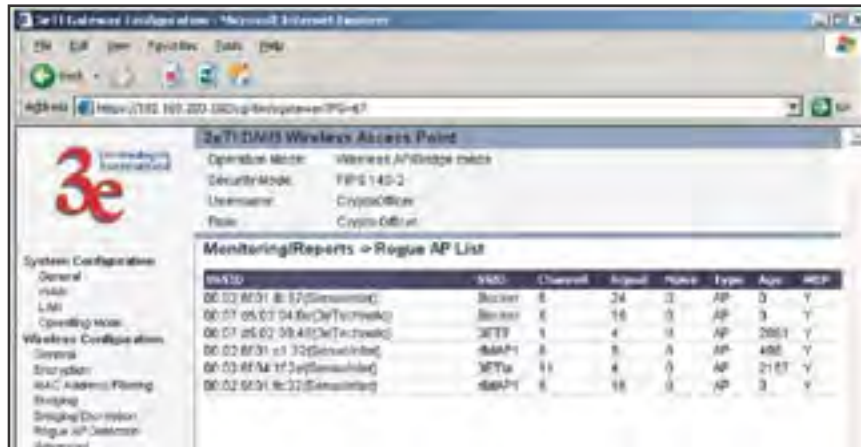
Once the transmit power is re-enabled and clients re-associate to the AP, EMCON information is maintained for them. If a new client that wasn't associated previously associates with the AP after the EMCON mode, its EMCON status appears as "-", which indicates the status record is not applicable.

2. EMCON response when TX Power is re-enabled



Rogue AP List

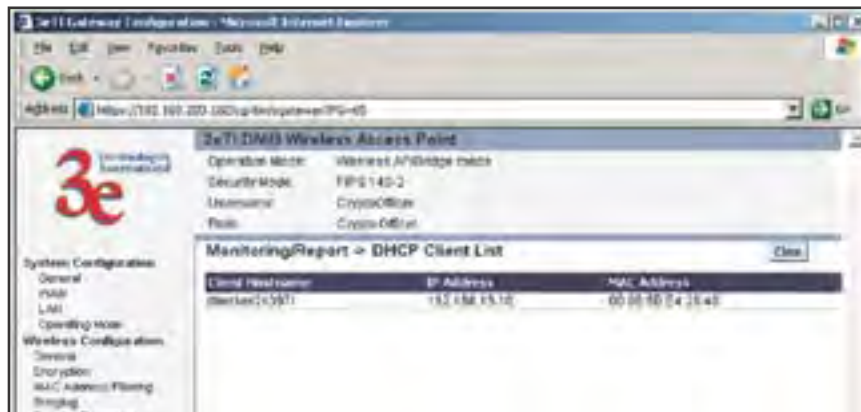
The rogue AP list shows all the APs on the network which are not seen by the subject AP as trusted clients.



DHCP Client List

The DHCP client list displays all clients currently connected to the 3e-531AP via DHCP server, including their hostnames, IP addresses, and MAC Addresses.

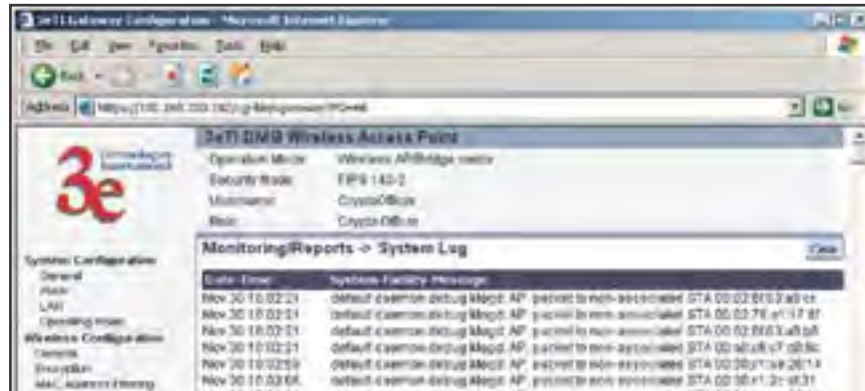
The DHCP client list will continue to accumulate listings unless you periodically clear it using the **Clear** button.



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.

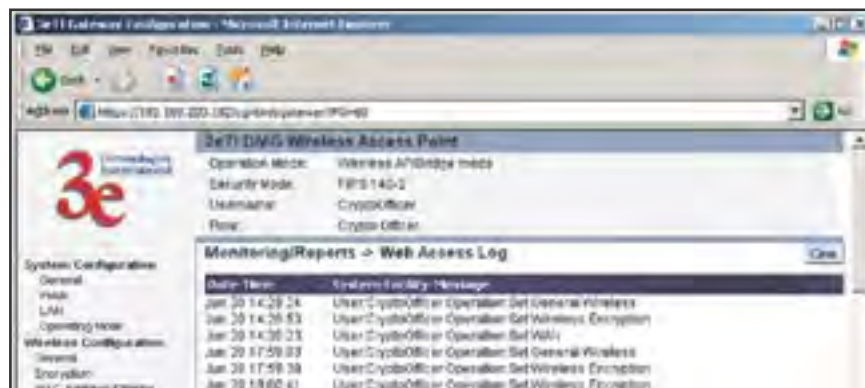
The System log will continue to accumulate listings unless you periodically clear it using the **Clear** button.



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.

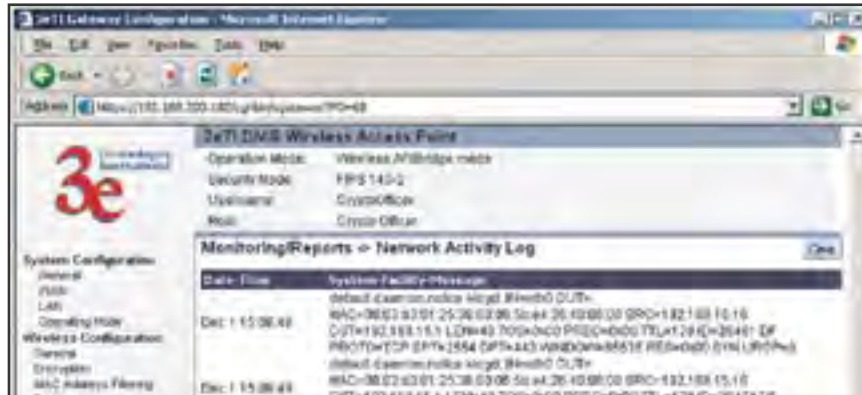
The Web access log will continue to accumulate listings unless you periodically clear it using the **Clear** button.



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.

The Network Activities Log will continue to accumulate listings unless you periodically clear it using the **Clear** button.



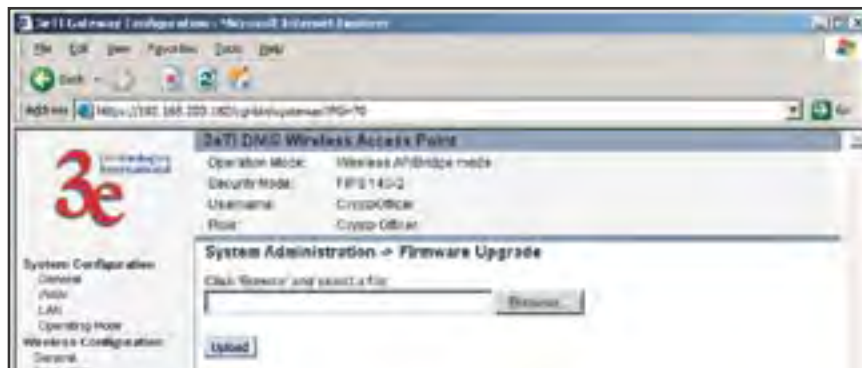
System Administration

The System administration screens contain administrative functions, some of which can only be performed 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-531AP 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-531AP from this page.

Only the Crypto Officer role can access this function.



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-531AP self-test suite includes: AES, 3DES, SHA-1 Algorithms, Random Number Generation, Diffie-Hellman for Dynamic Key Exchange, RSA, and HMAC SHA1 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-531AP 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 power cable (or POE cable).

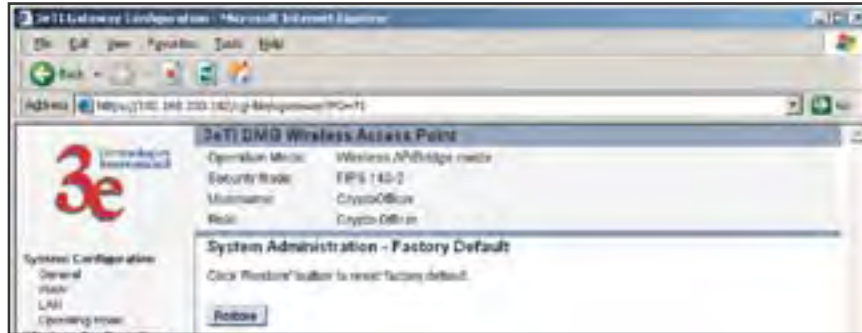
The 3e-531AP will then perform normal power up tests. If the Error State fails to clear, you must replace the device and return it to the manufacturer for servicing.



Factory Default

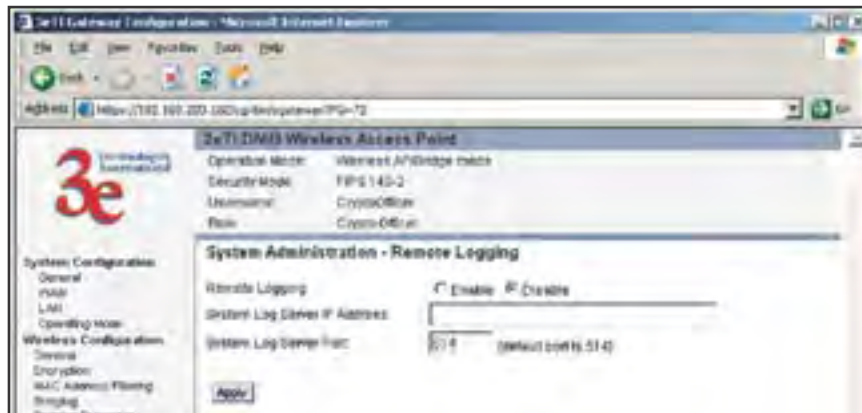
The "Restore" button is a fallback troubleshooting function that should only be used to reset to original settings.

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



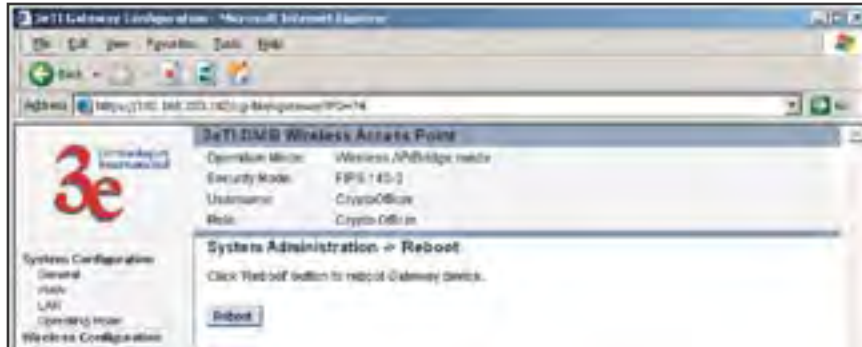
Remote Logging

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



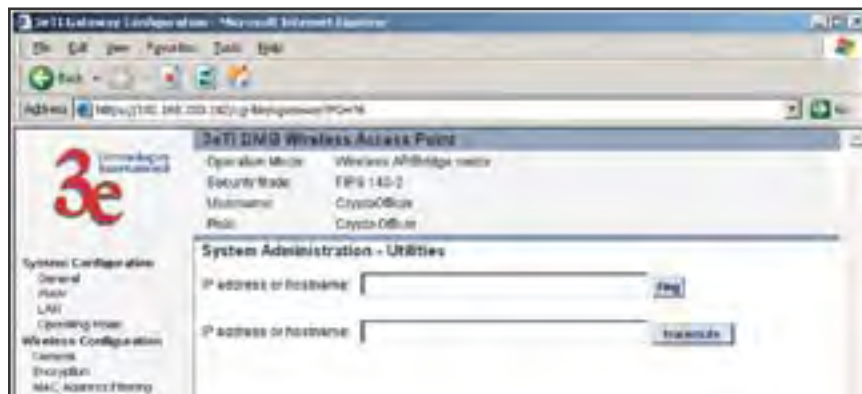
Reboot

The Reboot utility allows you to reboot the 3e-531AP 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.



This page intentionally left blank.

Chapter 4: Gateway Configuration

Introduction

Chapter 3 covered the default configuration of the 3e-531AP Wireless Access Point as an access point, for use as part of a host wired network. This chapter covers configuration as a gateway.

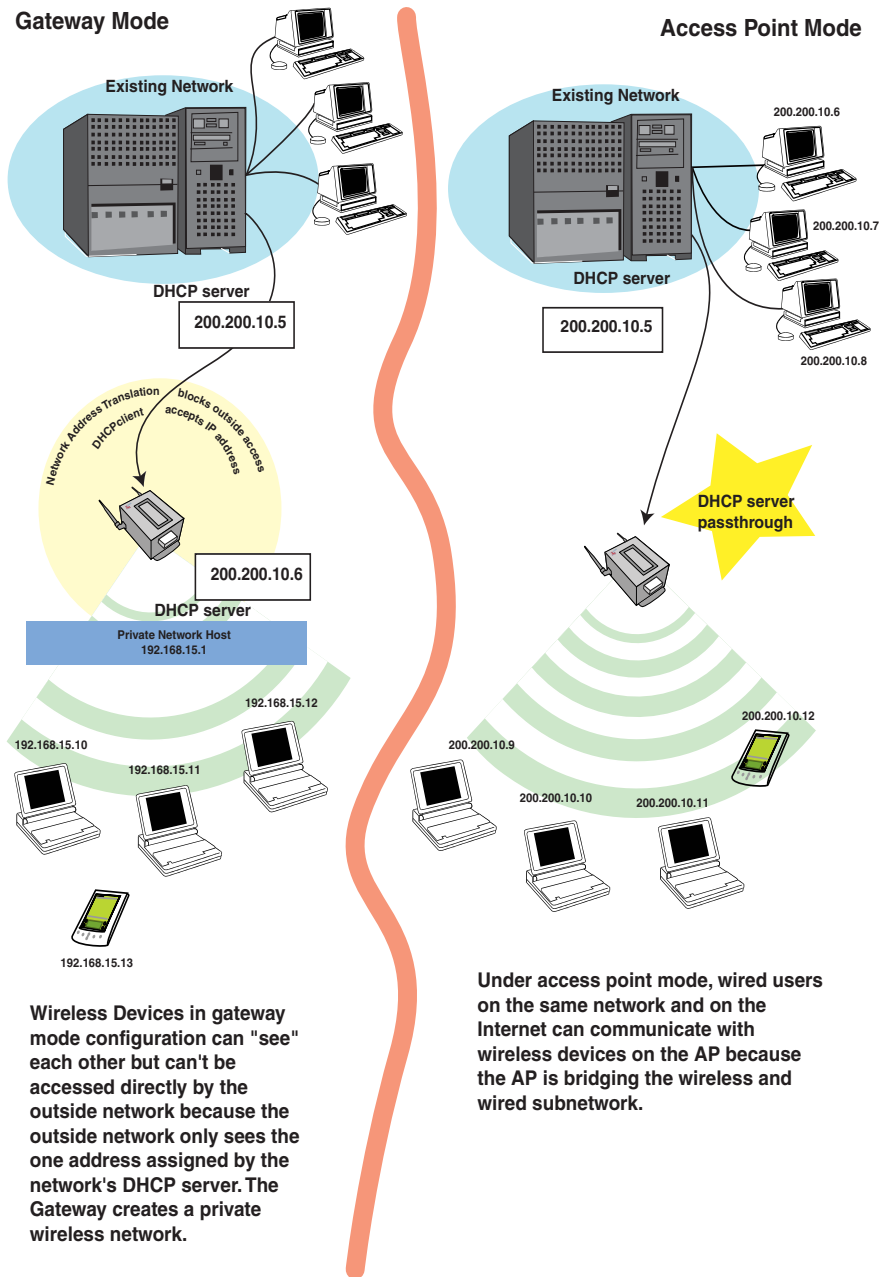
If additional security for the wireless network is desired (differentiating it from the wired network to which it is connected), set it up in gateway mode. Gateway mode takes advantage of some built-in “router” functions, such as the gateway’s ability to do Network Address Translation (NAT), providing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

A 3e-531AP 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-531AP 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-531AP 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.

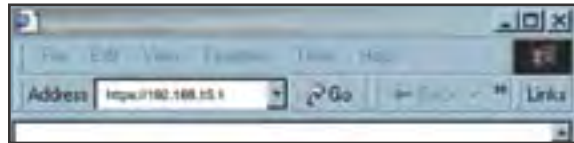
A comparison of gateway and access point setup for the 3e-531AP



Configuring in Gateway Mode

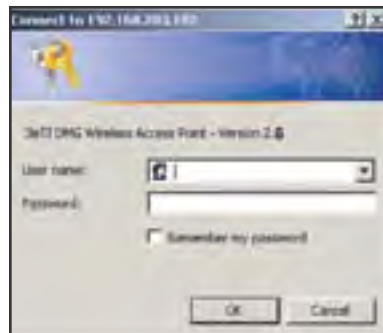
To configure the 3e-531AP in gateway mode, complete the following steps.

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-531 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`”.

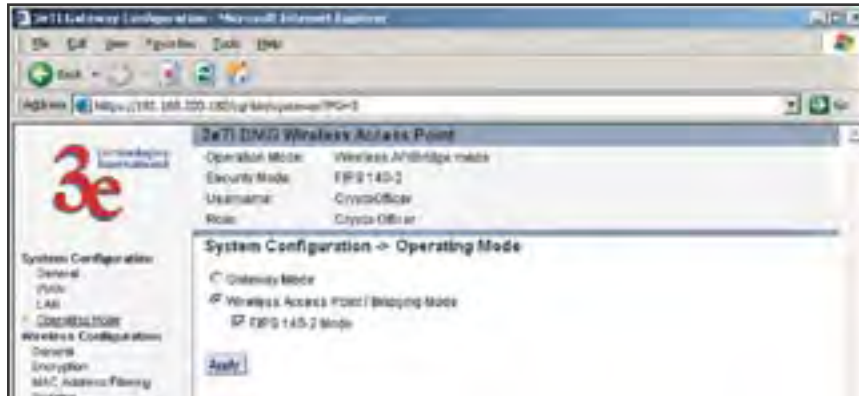


Then click **Go** on the Web browser.

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-531AP will reboot in gateway mode and reset all prior settings to factory default state.



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.

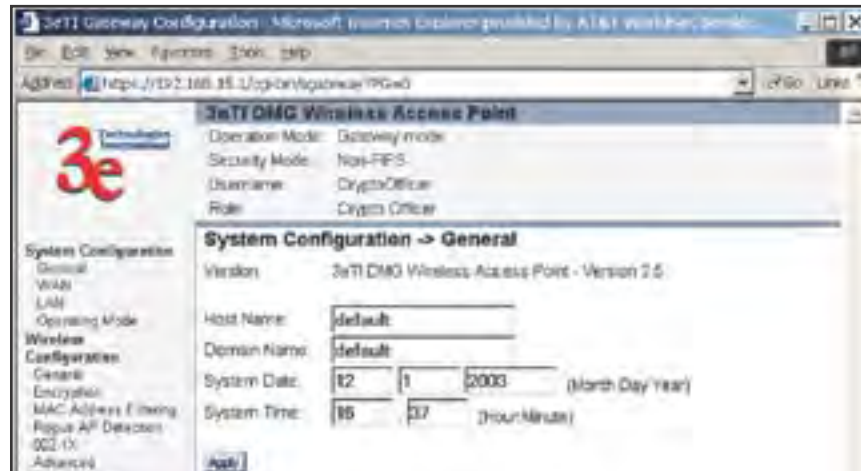
Note that you can't deploy the 3e-531AP as a bridge in Gateway mode, nor is it FIPS 140-2 compliant.

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-531AP gateway lists the firmware Version for your 3e-531AP 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-531AP 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.

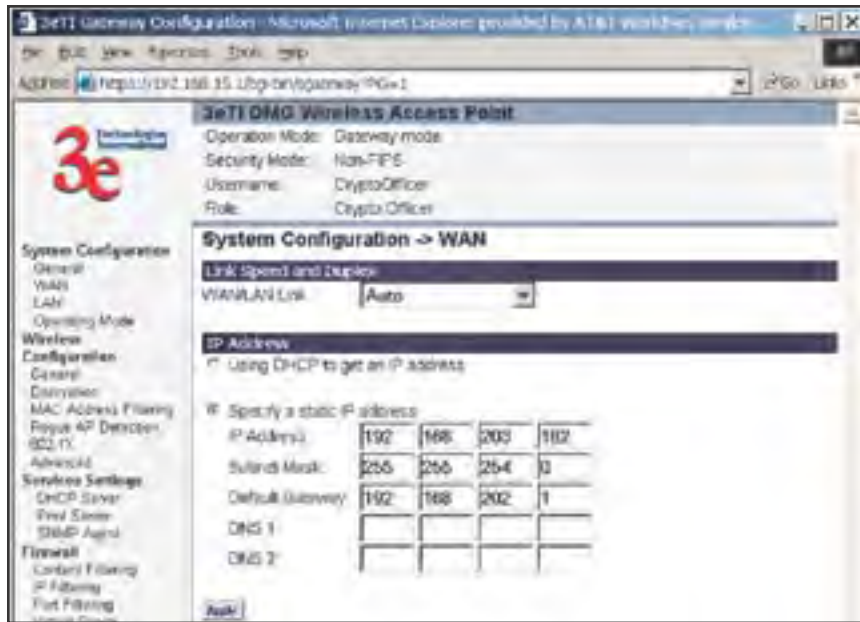
You also set information for how the IP address will be obtained.

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:

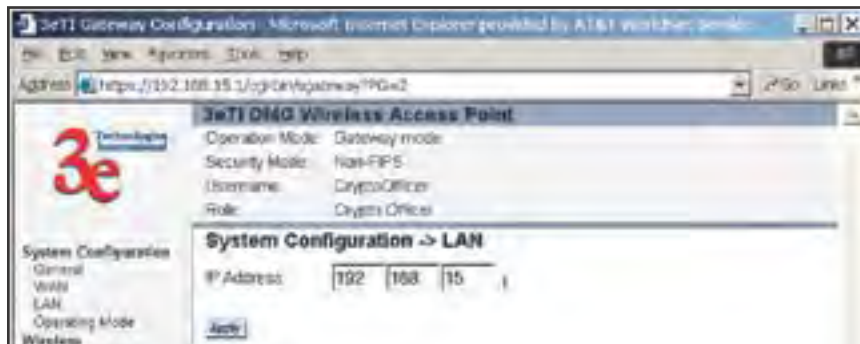
Obtain an IP address Automatically – This configuration allows the Ethernet network to use the DHCP server on the wired network to dynamically assign the WAN IP address to the DHCP client in the gateway.

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.



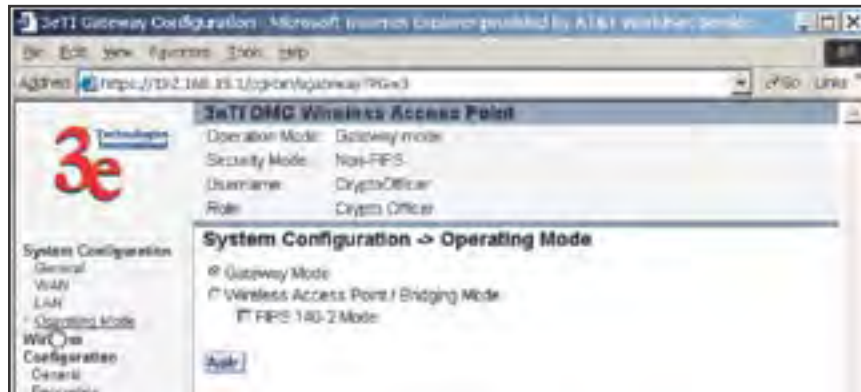
LAN

This sets up the default numbers for the first, second or third octet for a possible private LAN function for the access point. 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 or Bridge. Note that if you change mode, all previously entered information will be reset to factory settings.

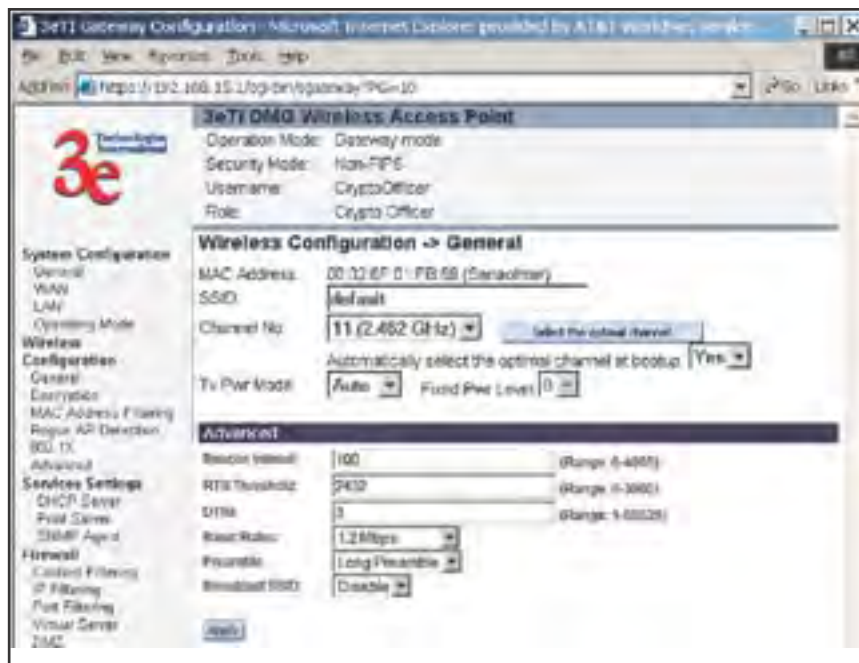


Wireless Configuration

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-531AP, 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.)

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 this page are described in the chart on the following page:

Beacon interval	0-4095	The frequency in milliseconds in which the 802.11 beacon is transmitted by the AP.
RTS Threshold	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.
DTIM	1-65535	The number of beacon intervals between successive Delivery Traffic Identification Maps (DTIMs). This feature is used for Power Save Mode.
Basic Rates	- 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.
Preamble	Short/Long Preamble	Specifies whether frames are transmitted with the Short or Long Preamble
Broadcast SSID	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-531AP is no encryption. It is recommended that you set encryption as soon as possible.

WEP (RC4) Data Encryption

Using the 3e-531AP in gateway mode allows you to employ s the WEP (RC4) encryption standard if you wish. WEP is not available in AP or Bridge mode for security reasons.

If using WEP, authentication type can be set to either Open System or Shared Key. Open System is probably adequate if you are using a remote authentication server (e.g. RADIUS) with 802.1x.

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 or home 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.

Static 3DES Key/Open System Authentication

The 3e-531AP 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.

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**.

The screenshot shows the configuration page for a 3eTDMO Wireless Access Point. The page is titled "3eTDMO Wireless Access Point" and displays the following information:

- Operation Mode: Gateway mode
- Security Mode: Non-PPS
- Username: CryptoOfficer
- Role: Crypto Officer

The "Wireless Configuration -> Encryption" section is active, showing the following options:

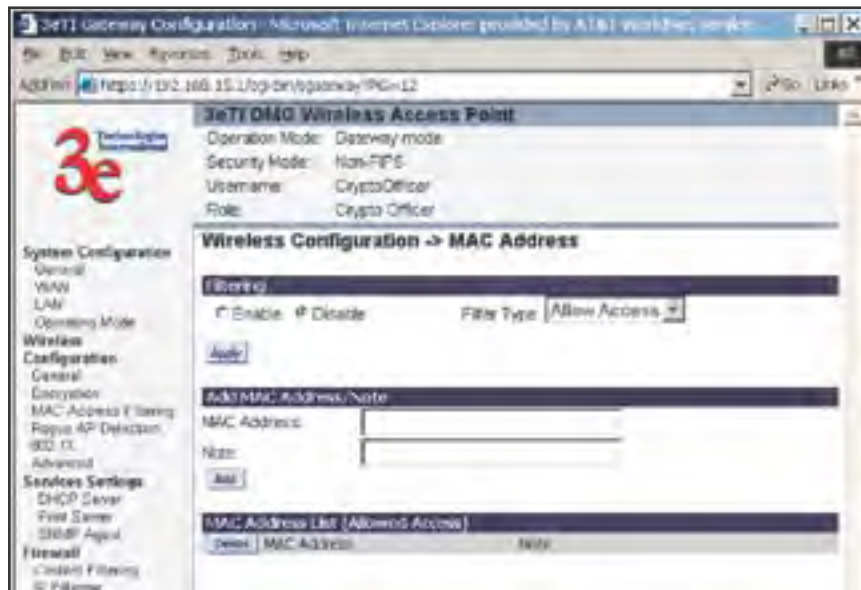
- WEP (RC4) Data Encryption
- WEP (RC4) Data Encryption
- Authentication Type:
- 64-bit Encryption
 - Default WEP Key:
 - (Enter 64-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F))
 - WEP Key 1:
 - WEP Key 2:
 - WEP Key 3:
 - WEP Key 4:
- 128-bit Encryption
 - (Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F))
 - WEP Key:
- Static RC4S Key / Open System Authentication
 - (Enter 192-bit keys as 48 hexadecimal digits (0-9, a-f, or A-F))
 - Key:
 - Again:
- Static AES Key / Open System Authentication:
 - 128-bit Encryption (Enter 128-bit keys as 32 hexadecimal digits (0-9, a-f, or A-F))
 - Key:
 - Again:
 - 192-bit Encryption (Enter 192-bit keys as 48 hexadecimal digits (0-9, a-f, or A-F))
 - Key:
 - Again:
 - 256-bit Encryption (Enter 256-bit keys as 64 hexadecimal digits (0-9, a-f, or A-F))
 - Key:
 - Again:

The "Apply" button is visible at the bottom left of the configuration area.

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.

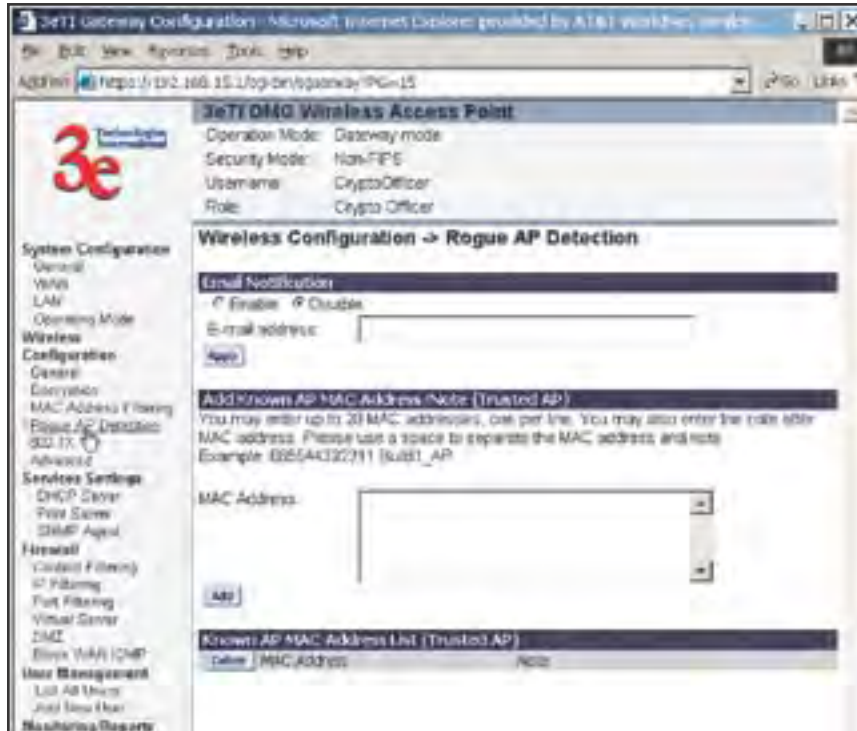
Input the MAC addresses of all the PC cards that will be authorized to access this device. The MAC address is engraved or written on the PC (PCMCIA) Card. The MAC Addresses you have input and any identifying note will appear in the lower window once you click the **Add** button. You delete MAC Addresses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



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.



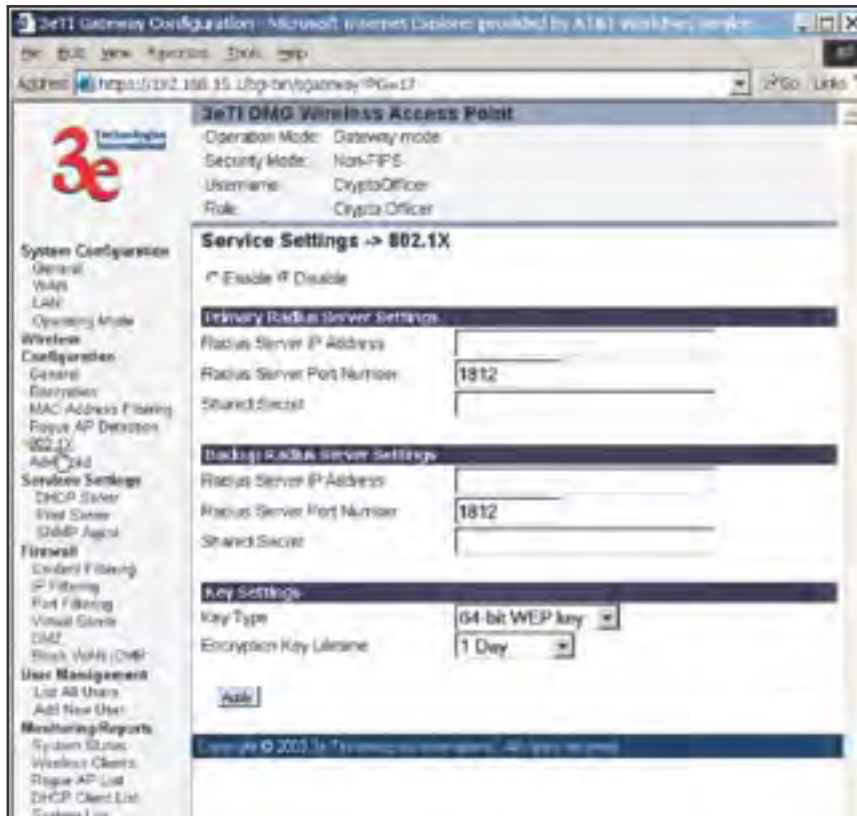
802.1x

Enabling 802.1x requires that you have at least one remote Radius server (preferably also a backup Radius server) but it will allow the use of the legacy WEP encryption key system with greater resultant security.

IEEE 802.1X offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1X ties a protocol called EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication.

If using 802.1x, you must know and input the IP address, Port Number and Shared Secret for the primary and backup Radius server and the key type selected on your Wireless Encryption page. Then set the accepted lifetime for the encryption key.

This is shown on the next page.



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.

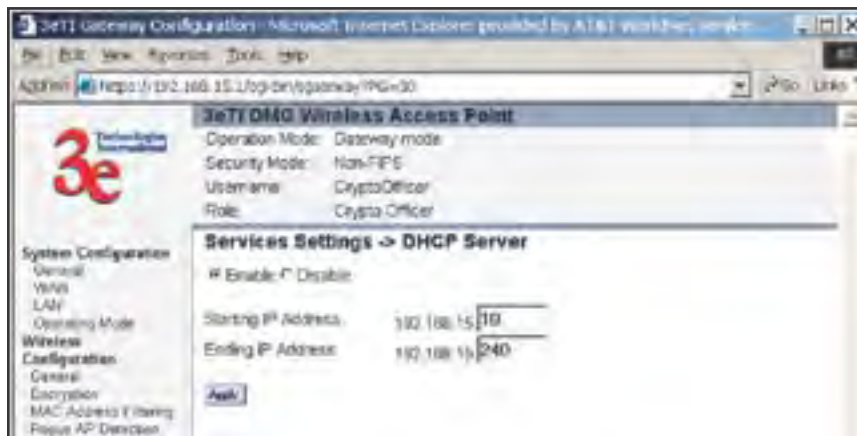
Once you have made any changes, click **Apply** to save.



Services Settings

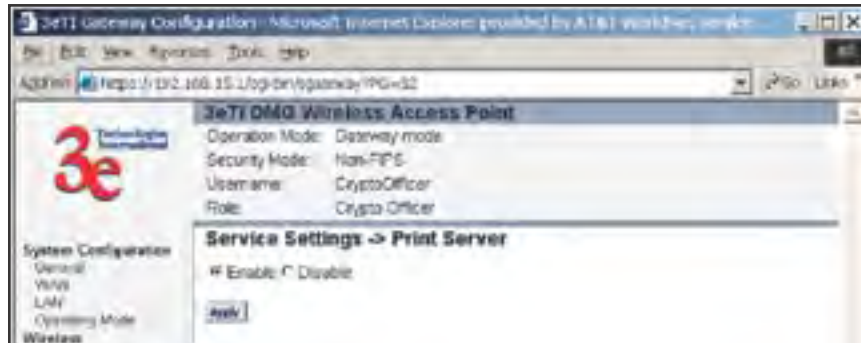
DHCP Server

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.



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** and leave the metal plate on the printer port. The metal plate is provided to protect that port from water.



SNMP Agent

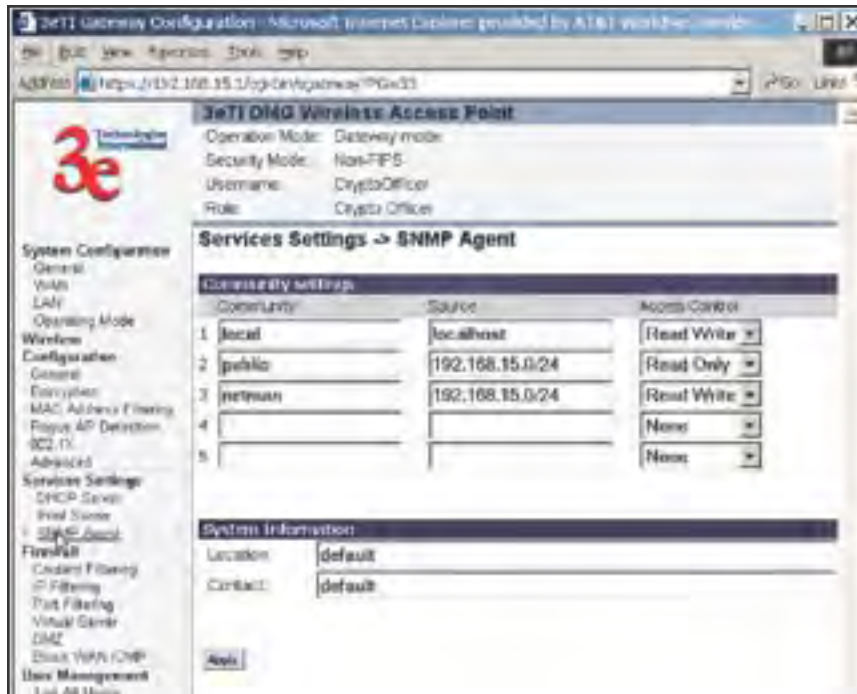
The SNMP (simple network management protocol) Agent setup page allows you to set up an SNMP Agent. The agent is a software module that collects and stores management information for use in a network management system. The 3e-531AP's integrated SNMP agent software module translates the device's management 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.



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**. Be aware, however, that the Content Filtering function does not exclude multihomed websites. Multihomed websites are those having two or more associated network addresses.



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 spe-

cific IP Address.



Port Filtering

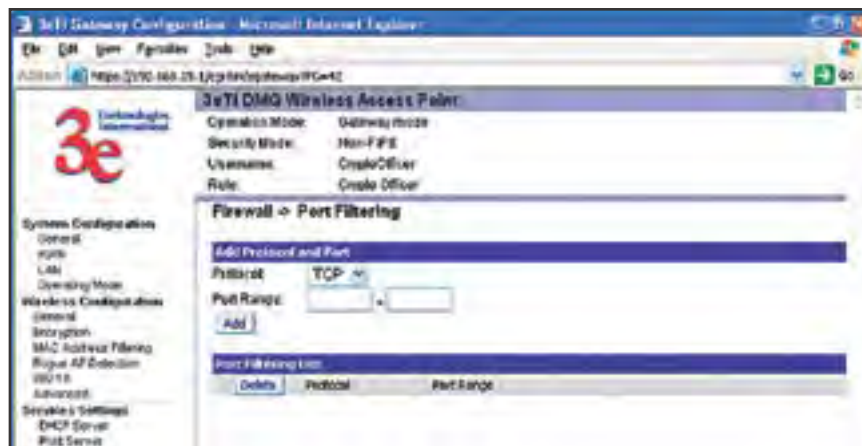
Port filtering permits you to configure the Gateway to block outbound traffic on specific ports. It can be used to block the wireless network from using specific protocols on the network.

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 Private 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.



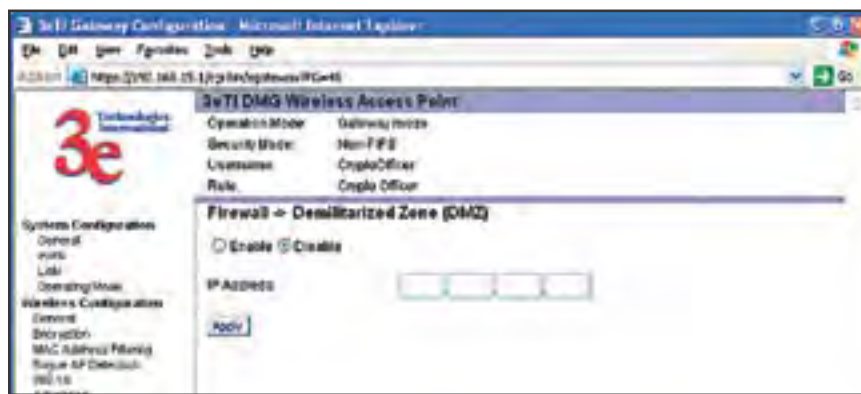
Protocol – Selection of either **UDP**, **TCP**, or **Both** (TCP and UDP) allows these specified network protocols to pass through during the TCP port communication with each virtual server IP address.

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-conferencing, where multiple TCP port

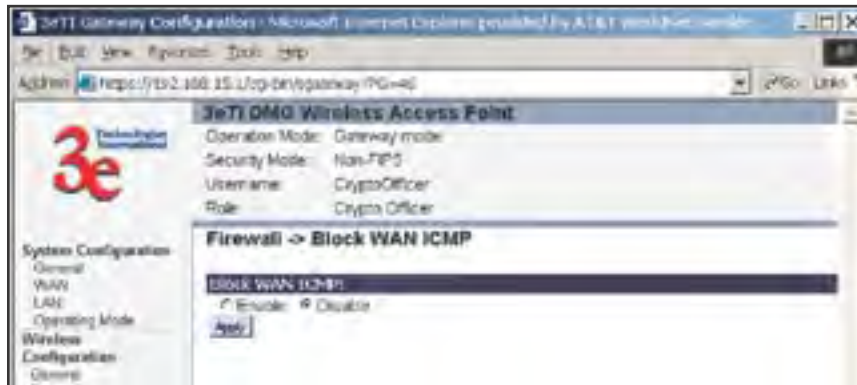
assignments are required for communication. To assign a PC the DMZ host status, fill in the Private IP address which is identified as the exposed host and click the **Apply** button. However, any Internet user who knows the WAN IP address of the gateway can connect to the DMZ host since the firewall 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.



Block WAN ICMP

If you enable ICMP (Internet Control Message Protocol) Blocking, a device outside the WLAN will not get a response to a ping or traceroute request. The default is disabled which will allow response to ping or traceroute for connectivity testing.



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.



Monitoring/Reports

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

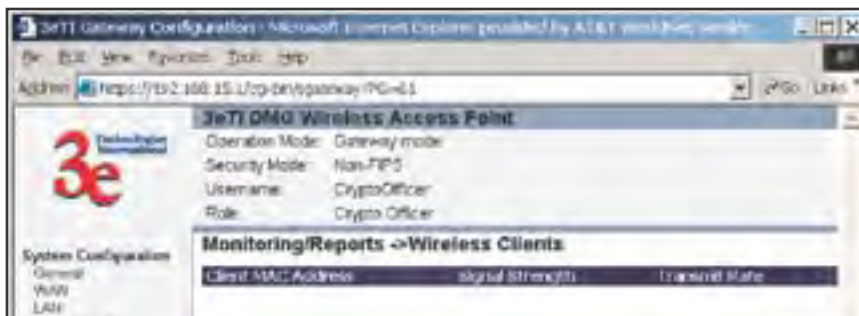
System Status

This screen displays the status of the 3e-531AP device and network interface details.



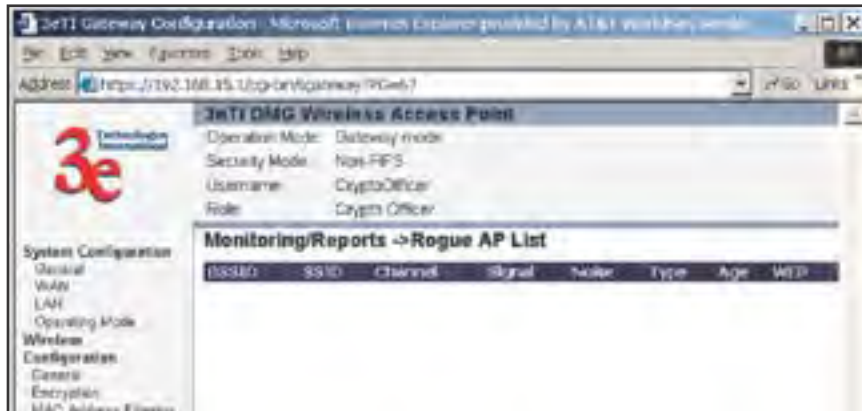
Wireless Clients

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



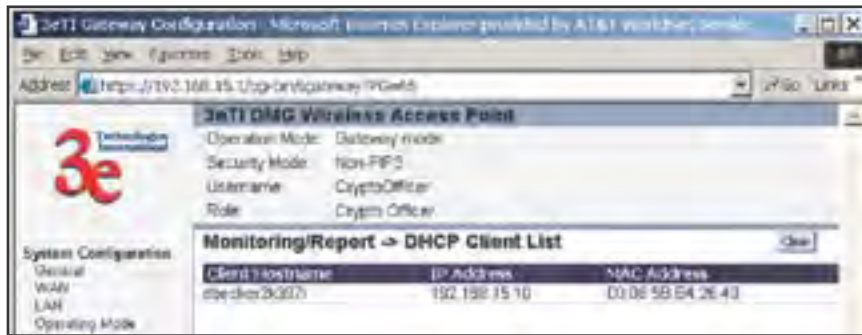
Rogue AP List

The rogue AP list shows all the APs on the network which are not seen by the subject AP as trusted clients.



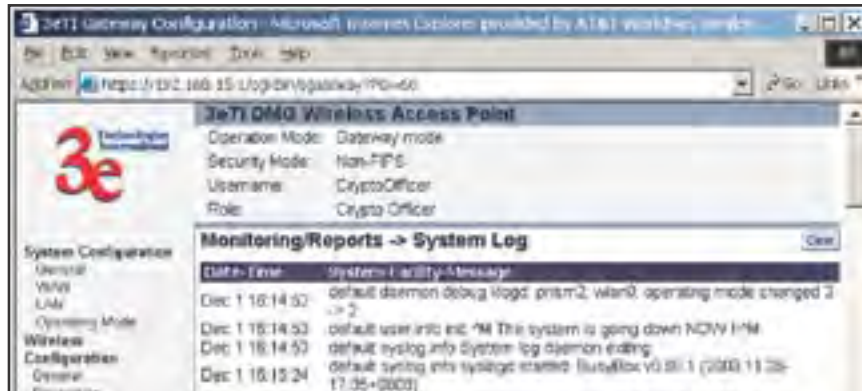
DHCP Client List

The DHCP client list displays all clients currently connected to the 3e-531AP via DHCP server, including their hostnames, IP addresses, and MAC Addresses.



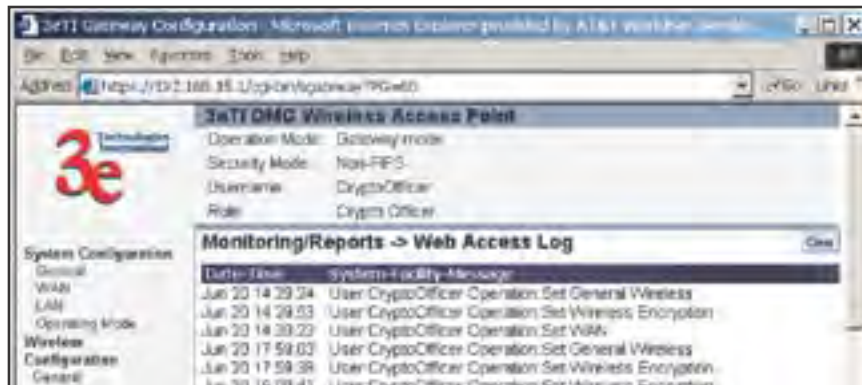
System Log

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.



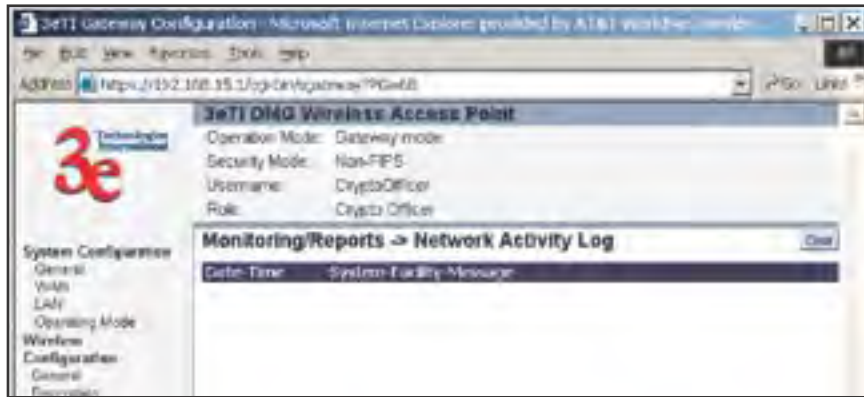
Web Access Log

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.



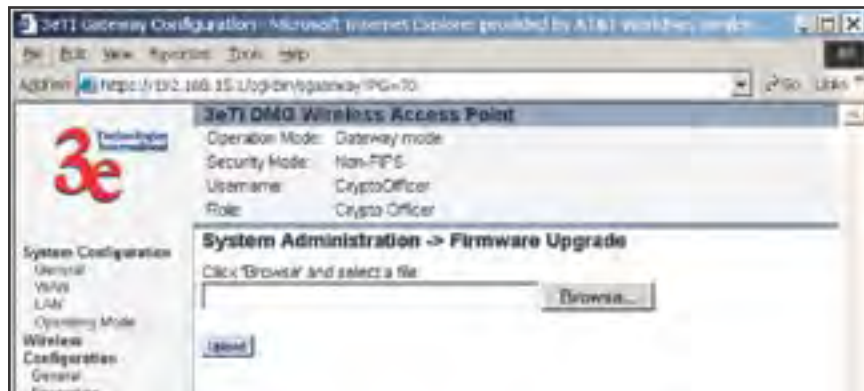
System Administration

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

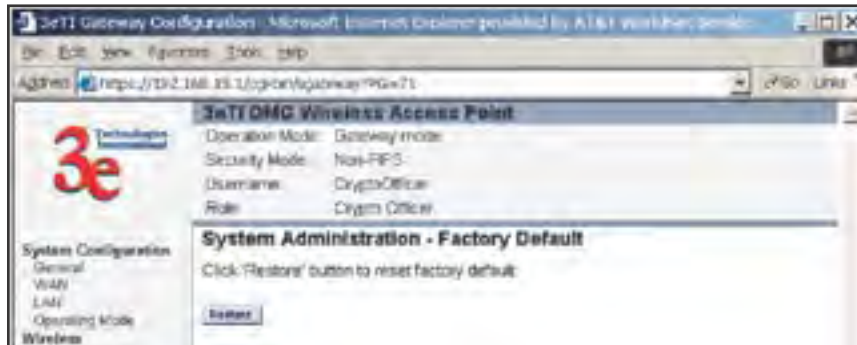
The **System Upgrade** utility is a functionality built into the 3e-531AP Series for updates to the device's firmware as they become available. When a new upgrade file becomes available, find it and upload it to the 3e-531AP from this page.

Only the Crypto Officer role can access this function.



Factory Default

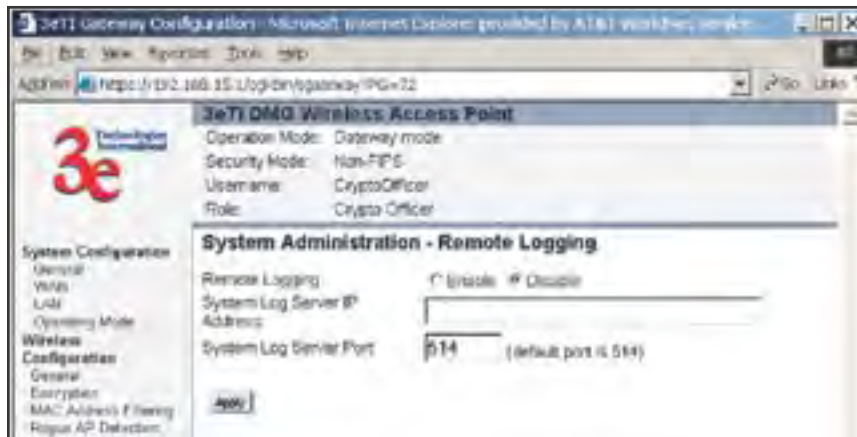
The Factory Default or "Restore" button is a fallback troubleshooting function that should only be used to reset to original settings.



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

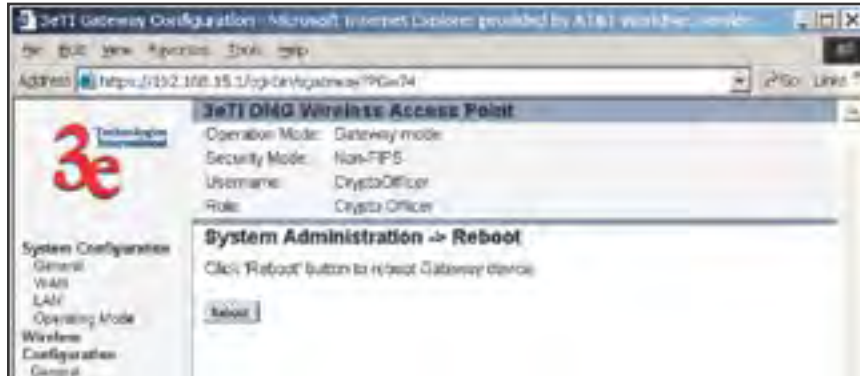
Remote Logging

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



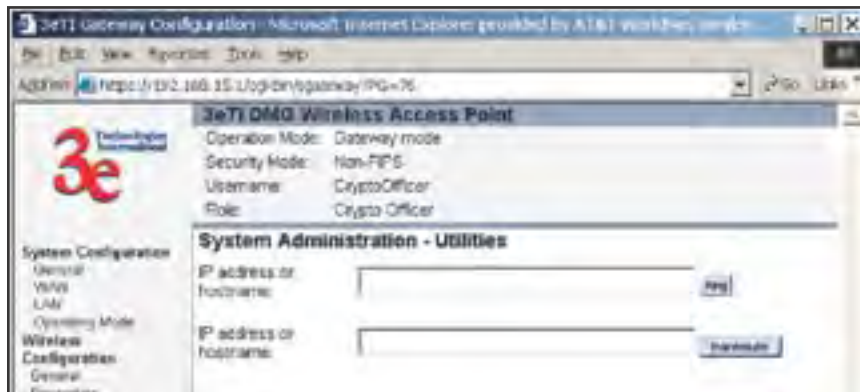
Reboot

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.



This page intentionally left blank.

Chapter 5: Bridge Configuration

Introduction

The wireless bridging function in the 3e-531AP allows setup as a bridge, in a number of alternate configurations. We discuss some of the most popular settings in this chapter:

1. Point-to-point bridging of 2 Ethernet Links;
2. Point-to-multipoint bridging of several Ethernet links;
3. Back-to-back bridging mode (with point-to-point bridging) to deliver mobile wireless connectivity; and
4. Repeater mode

Preliminary Setup

Your 3e-531AP Wireless Access Point must be configured in access point mode to utilize it as a bridge. If not already in Access Point mode, open the management module and navigate to the **System Configuration — Operating Mode** screen.



Select the radio button for **Wireless Access Point/Bridging Mode** and click **Apply**. If you wish to use Advanced Encryption, check the FIPS 140-2 Mode option. The unit will reboot. You do not need to log back on. After reboot, an instructional page will appear and you can then navigate back to the Management Module main screen.


General Bridge Setup

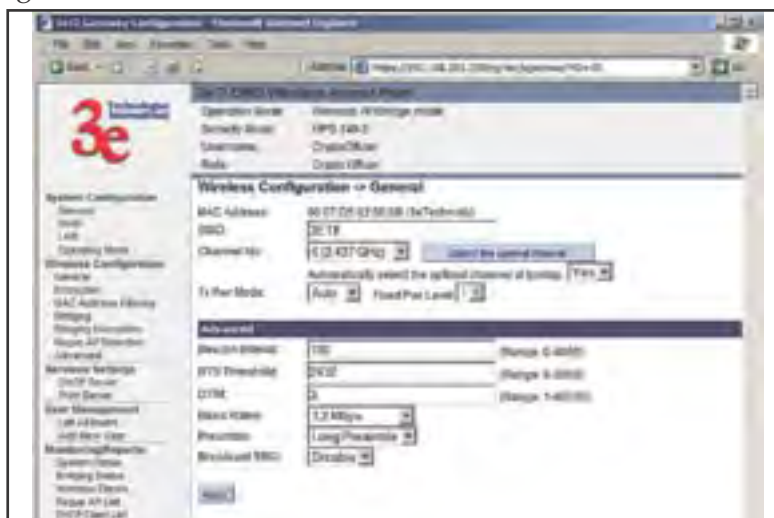
Once the unit is in access point mode, the navigation bar on the left side of the management module will include some screens that relate specifically to bridging. The screens that you may need to modify, regardless of what type of bridging mode you choose, will be in the **Wireless Configuration** section. These include:

- **Wireless Configuration — General**
- **Wireless Configuration — Encryption**
- **Wireless Configuration — MAC Address Filtering**
- **Wireless Configuration — Bridging**
- **Wireless Configuration — Bridging Encryption.**

The **Wireless Configuration — Encryption** and the **Wireless Configuration — MAC Address Filtering** are only needed if you are going to set up the bridge as a repeater. However, we have included a picture of them in this section for reference purposes.

The **Wireless Configuration — General** screen is used to set the SSID and Channel Number and is also the location where you can find the device MAC Address, which you will need. If you are setting up the 3e-531AP 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 the MAC Address, which is shown on this page. It is a good idea to write down the MAC Address before leaving the page. 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. Generally, channels 1, 6, and 11 are the best from which to choose, since these are the channels with optimum frequency spread. TX Pwr Mode can be left in its default of Auto. If you find later that the broadcast range can be decreased, this is where you will set it.

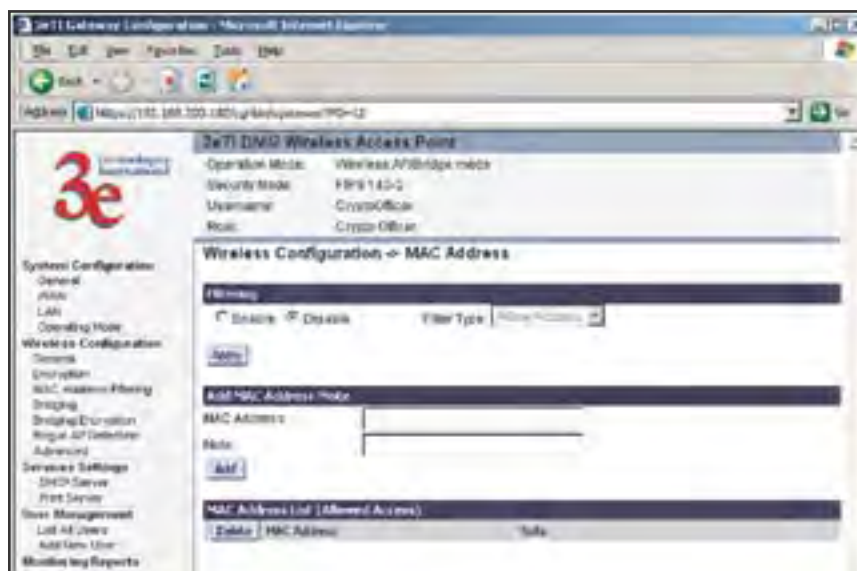
 **IMPORTANT NOTE:** It is vital that you not use the function, **Automatically select the optimal channel at bootup**, when you are configuring the 3e AP as a Bridge. Set the function to **NO**. In bridging mode, all APs must be on the same RF Channel.



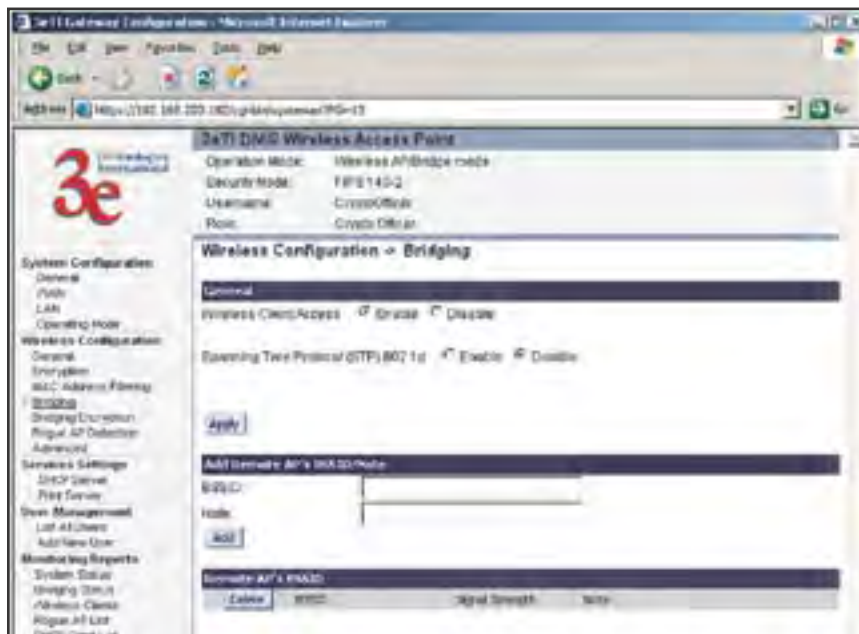
The **Wireless Configuration — Encryption** screen sets the encryption type and level for the WLAN. This page is only needed for repeater setup.



The **Wireless Configuration — MAC Address Filtering** screen would be used if the wireless LAN is using MAC Filtering. This page is only needed for repeater setup.

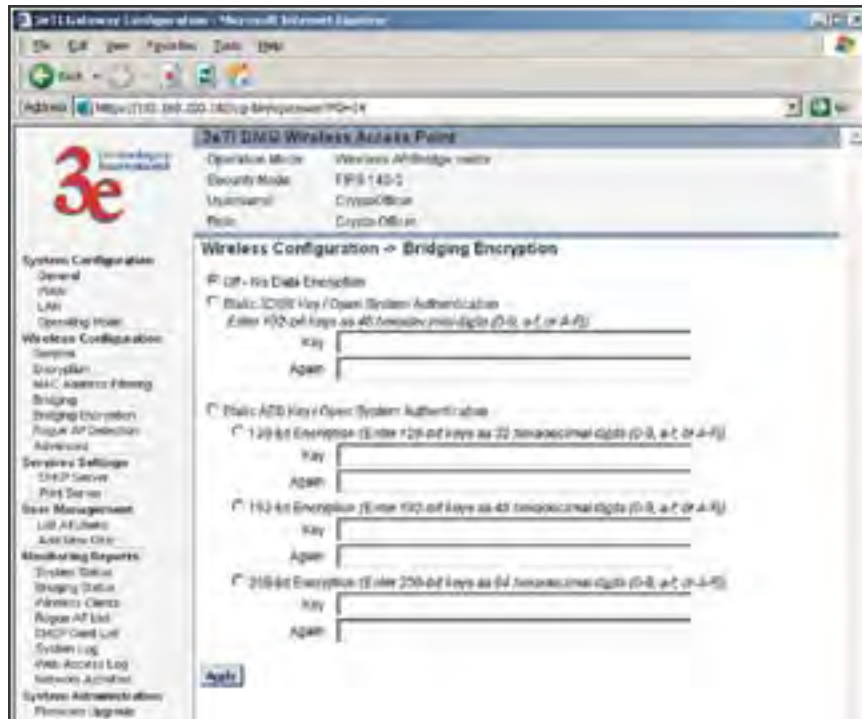


The **Wireless Configuration — Bridging** screen is used to enable/disable Wireless Client Access and Spanning Tree Protocol and to configure the BSSID of the peer bridges. This page is important in setting up your bridge configuration. We recommend that you disable Wireless Client Access for all bridge setups except repeater. 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.

NOTE: You can also select to leave encryption **OFF**, but this is not recommended.

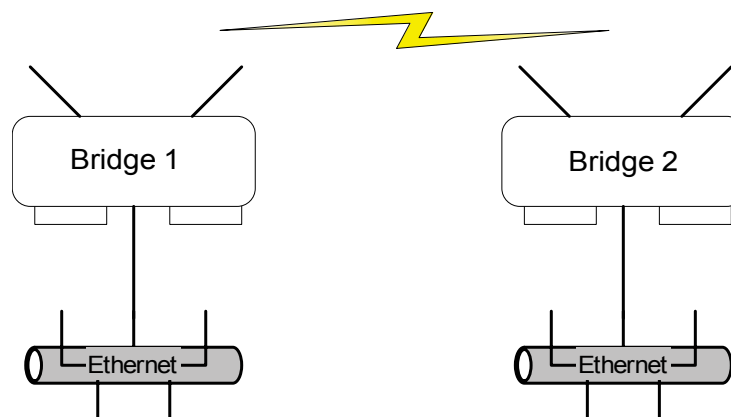


The following sections describe the setup for four types of bridging configuration: point-to-point, point-to-multipoint, back-to-back or, lastly, repeater.

Bridging Type Configuration

Point-to-Point Bridge Configuration

A point-to-point link is a direct connection between two, and only two, locations or nodes.



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

For instance, the bridges must have the same channel number. Both must be set for bridging with Wireless Client Access set to Disable. 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 must contain the other's BSSID. (The BSSID of each is equivalent to the MAC address. 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 the preferred settings.

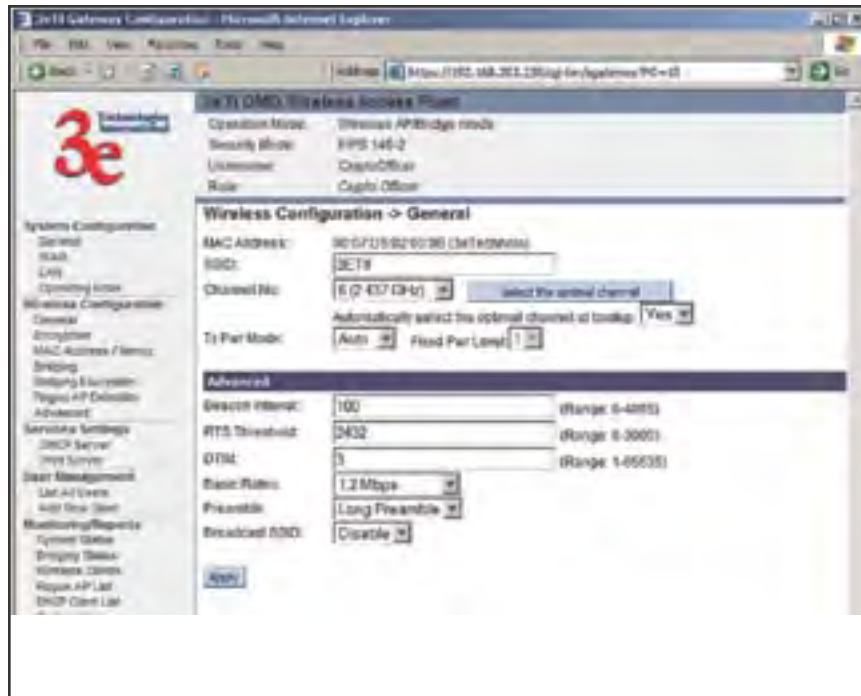
Point-to-Point Bridging Setup Guide

Direction	Bridge 1	Bridge 2
Mode	Bridging	Bridging
Wireless Configuration – General		
SSID	default	default
Channel	11	11
Tx Power	Auto	Auto
Wireless Configuration – Encryption	N/A	N/A
Wireless Configuration – Bridging		
Wireless Client Access	Disable	Disable
Spanning Tree Protocol	Enable (or Disable if no bridging loop possible)	Enable (or Disable if no bridging loop possible)
BSSID (the MAC Address, from the Wireless Configuration — General screen.)	Add Bridge 2 BSSID	Add Bridge 1 BSSID
Wireless Configuration – Bridging Encryption	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 steps 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.

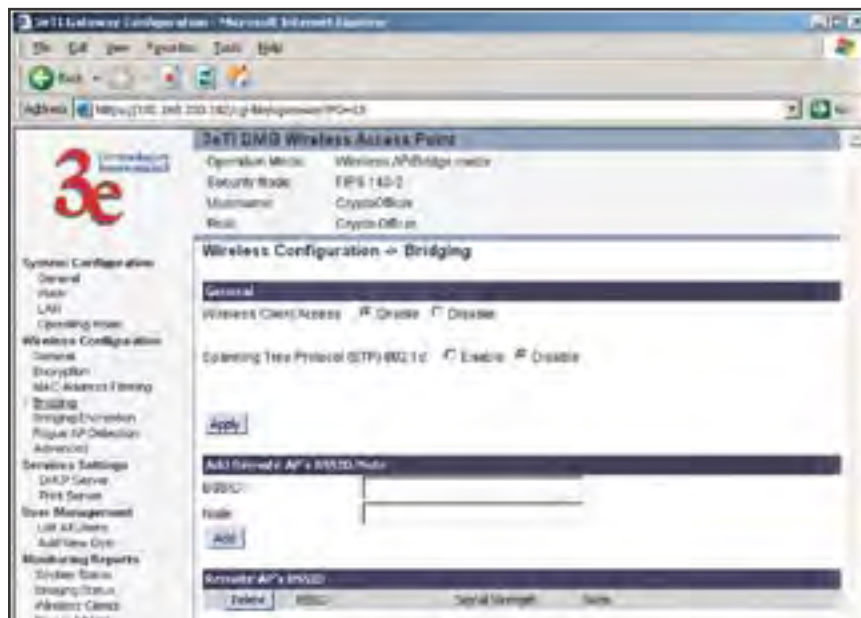
First, ensure that bridge 1 is in Bridging Mode by selecting that option on the **System Configuration — Operating Mode** screen and clicking **Apply** to reboot.

Navigate to the **Wireless Configuration — General** screen and set the Channel number. Leave the TX Pwr Mode in AUTO position at this time.



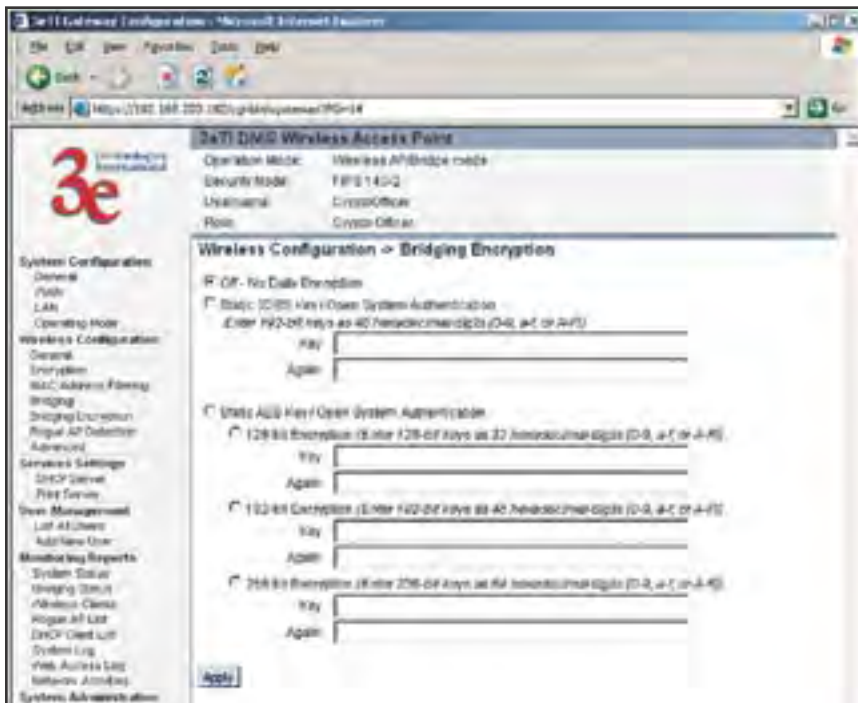
Navigate to the **Wireless Configuration — Bridging** screen.

In the first section: **General**, set **Wireless Client Access** to **Disable** and set **Spanning Tree Protocol (STP) BQ1.0** to **Enable**. 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.



You must complete the configuration of your Bridge 1 by visiting the other screens included in the navigation bar and 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.

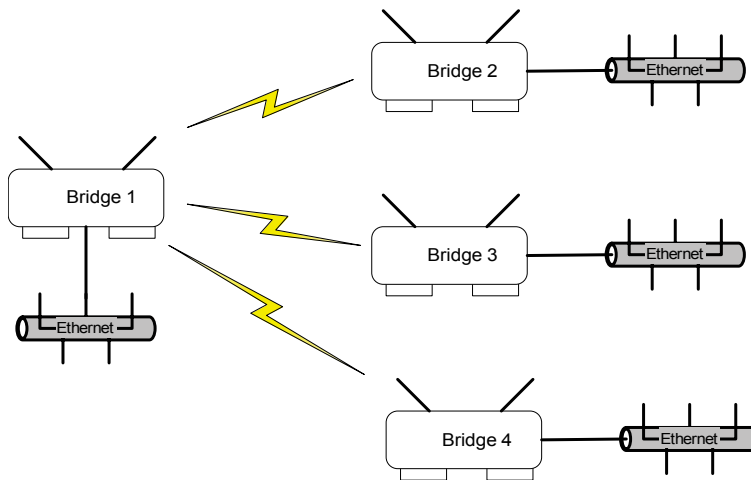
Point-to-Multipoint Bridge Configuration

A point-to-multipoint configuration allows you to set up three or more 3e-531AP 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. All must be set for bridging with Wireless Client Access set to Disable and Spanning Tree Protocol usually set to Enable. If configured as in the diagram below, 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. 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.

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 below describes the basic attributes.

Point-to-Multipoint Bridging Setup Guide

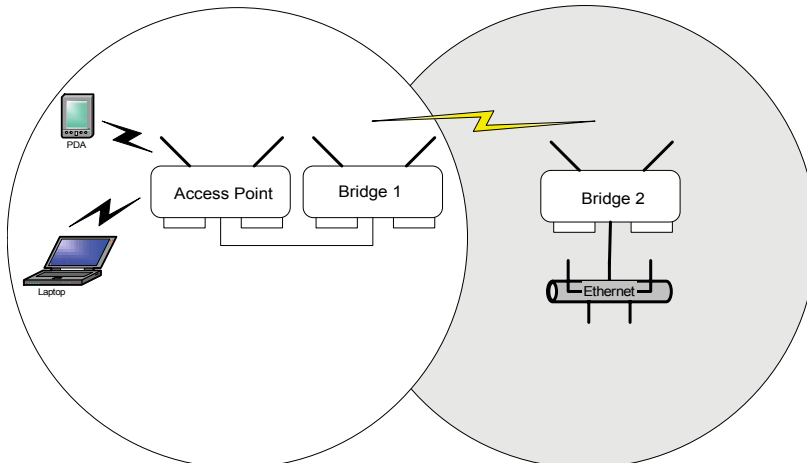
Direction	Bridge 1	Bridge 2 ~ n
Mode	Bridging	Bridging
Wireless Configuration – General		
SSID	default	default
Channel	6	6
Wireless Configuration – Encryption		
Wireless Configuration – Bridging		
Wireless Client Access	Disable	Disable
Spanning Tree Protocol	Enable (or Disable if no bridging loop possible)	Enable (or Disable if no bridging loop possible)
BSSID (the MAC Address, from the Wireless Configuration — General screen.)	Add Bridge 2 ~ n BSSIDs	Add Bridge 1 BSSID
Wireless Configuration – Bridging Encryption	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.

Back-to-Back Bridge Configuration

A back-to-back configuration could be of use when it is desirable to have a mobile unit able to communicate with an Ethernet LAN. As shown in the following diagram, this does require the use of an additional AP for managing local wireless communications at the mobile site, but may be desired for emergency or security reasons.



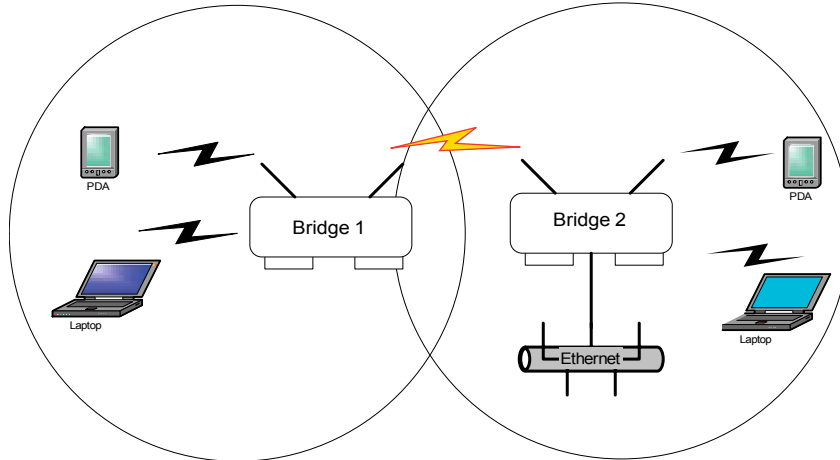
The following chart maps the basic procedure to be followed in configuring the three units as shown above. Essentially, you can follow the procedure as laid out in the section on point-to-point bridging. It is the BSSID and the Bridging Encryption that allows the two bridges to communicate. Needless to say, the configuration of the access point determines the functioning of the dependent WLAN.

Back-to-Back Bridging Setup Guide

Direction	Access Point	Bridge 1	Bridge 2
Mode	Access Point	Bridging	Bridging
Wireless Configuration – General			
SSID	SSID to be used for the local WLAN	Different from AP (can be left in Default)	Different from AP (can be left in Default)
Channel	11	1	1
Wireless Configuration – Encryption	Configure Dynamic Key Fields with your server's IP address and password	N/A	N/A
Wireless Configuration – Bridging			
Wireless Client Access	N/A	Disable	Disable
Spanning Tree Protocol	N/A	Enable	Enable
BSSID (the MAC Address, from the Wireless Configuration — General screen.)	N/A	Add Bridge 2 BSSID	Add Bridge 1 BSSID
Wireless Configuration – Bridging Encryption	N/A	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.

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

Direction	Bridge 1	Bridge 2
System Configuration – Operating Mode	Bridge	Bridge
Wireless Configuration – General		
SSID	Same as Bridge 2	Same as Bridge 1
Channel	6	6
Wireless Configuration – Encryption	Configure Dynamic Key Management fields with your server's IP address and password. (Alternately, use a static key.)	Configure Dynamic Key Management fields with your server's IP address and password. (Alternately, use a static key.)
Wireless Configuration – Bridging		
Wireless Client Access	Enable	Enable
Spanning Tree Protocol	Enable	Enable
BSSID (the MAC Address, from the Wireless Configuration — General screen.)	Add Bridge 2's BSSID	Add Bridge 1's BSSID
Wireless Configuration – Bridging Encryption	Select appropriate key type/length and enter key value. Must be the same as that on Bridge 2.	Select appropriate key type/length and enter key value. Must be the same as that on Bridge 1.

With this configuration, each bridge can control a wireless LAN. All wireless clients must have the same SSID as the bridges. All clients can roam between the two bridges.

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

Chapter 6: PC Card Installation on a Laptop

If you are setting up the 3e-531AP as part of a secure wireless LAN using AES or 3DES encryption options, you need to purchase and install an IEEE 802.11b PC Card on each laptop that will be a client on the network. The laptop must have a PCMCIA Card Type II or Type III slot. You will need to install the 3e-010 Crypto Client Software (separately sold with the 3e-110 Wireless PC Card).

3e Technologies International's 3e-010F Crypto Client Software is compatible with the 3e-110 Wireless PC Card and with other wireless cards based on INTERSIL PRISM 2 and 2.5 chipsets. It will install in a Windows 2000, Windows NT 4.0 or Windows XP operating system environment.

If you will be using the 3e-531AP with WEP encryption only, you can use any compatible PC Card.

Follow the manufacturer's instructions to complete installing the PC Card.

Once the PC Card is installed, you must now configure the encryption utility to allow the user access to the WLAN. Until the utility has been configured to allow access to the 3e-531AP, you will not be able to access the WLAN from the particular wireless device you are configuring.

If you are using the 3e-110 PC Card with secure 3e-010F AES or 3DES encryption software, there are two types of roles on the secure system: CryptoOfficer and Administrator. The following chart shows the different permissions in respect to the Crypto Client Utility.

Activity	CryptoOfficer	Administrator
Identifier (factory setting)	CryptoOfficer CryptoFIPS	Admin AdminFIPS
Ability to set Passwords	✓ (all)	✓ (only self)
Configures Crypto Client Utility	✓	✗
Configures encryption settings	✓	✗

Performs Site Survey	✓	✘
Resets to factory default	✓	✘
Changes power level on Client device (laptop)	✓	✓
Can turn Radio On/Off on laptop	✓	✓
Performs Rescan	✓	✓
Performs Self-test	✓	✓

You may need some or all of the following information handy as you install the FIPS secure drivers on your wireless device's PC Card interface:

- The driver configuration utility login. The factory default is Username equal to "CryptoOfficer," and Userid equal to "CryptoFIPS;"
- Type of encryption used by your WLAN (AES, 3DES, and whether you will be using Dynamic Key Exchange);
- Your security certificate, key and Certificate Authority (CA), if using DKE;
- Your Wireless SSID;
- Your user name and password to access your network account on the wireless device;

and, if addresses are to be statically assigned:

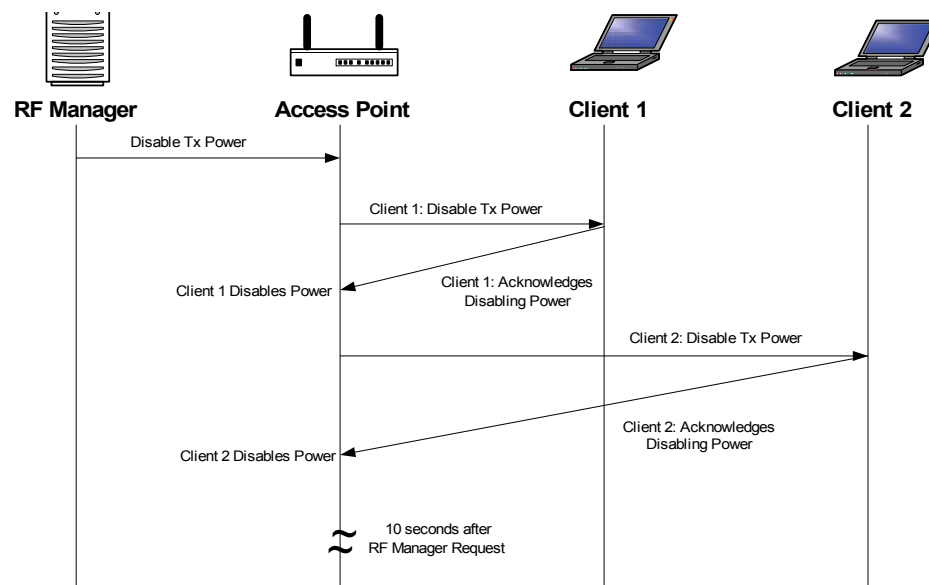
- Your IP address;
- Your Gateway address;
- Your Subnet Mask.

Follow the instructions that came with your PC Card to complete the installation. Once the configuration is complete, you should be able to access the WLAN.

Chapter 7: The RF Manager Function

Introduction

This chapter addresses a function of the 3e AP which facilitates remote management and programming of the Radio Frequency function for multiple 3e APs 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.

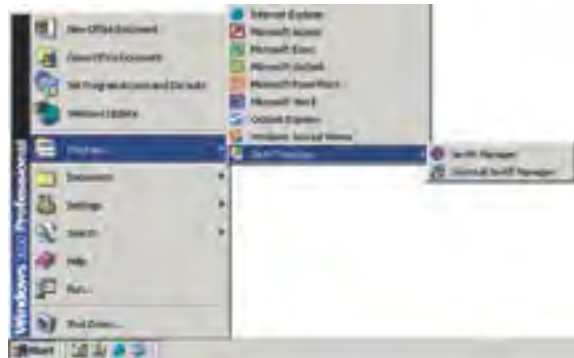
How to Access the RF Manager Function

The RF Manager can be installed from the CD that came with the 3e-531AP Install Kit to the desktop of anyone who needs to manage the wireless LAN.

Click on RF Manager on the CD main menu to start the autoinstall. If, for any reason, the autoinstall doesn't initiate, open a window from the **My Computer** icon to your CD drive and double-click the autoinstall 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.



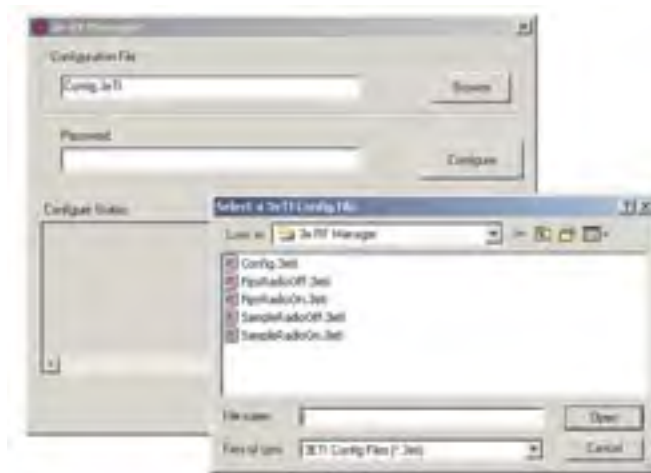
The main RF Manager screen will appear on your desktop.



How to Program the RF Manager

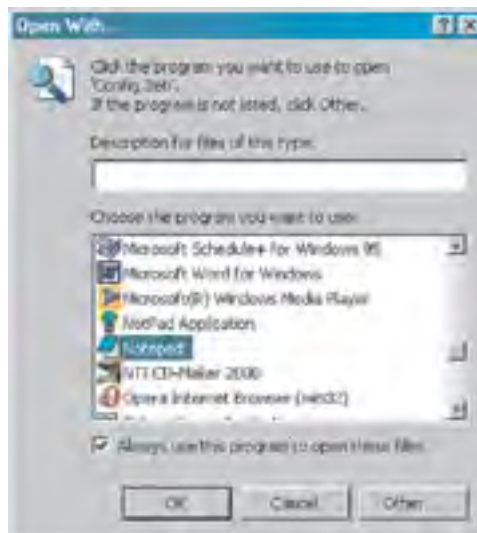
Before you are able to remotely manage access points, you need to program the RF Manager by putting the static IP Address of APs you want to manage in a configuration file.

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.



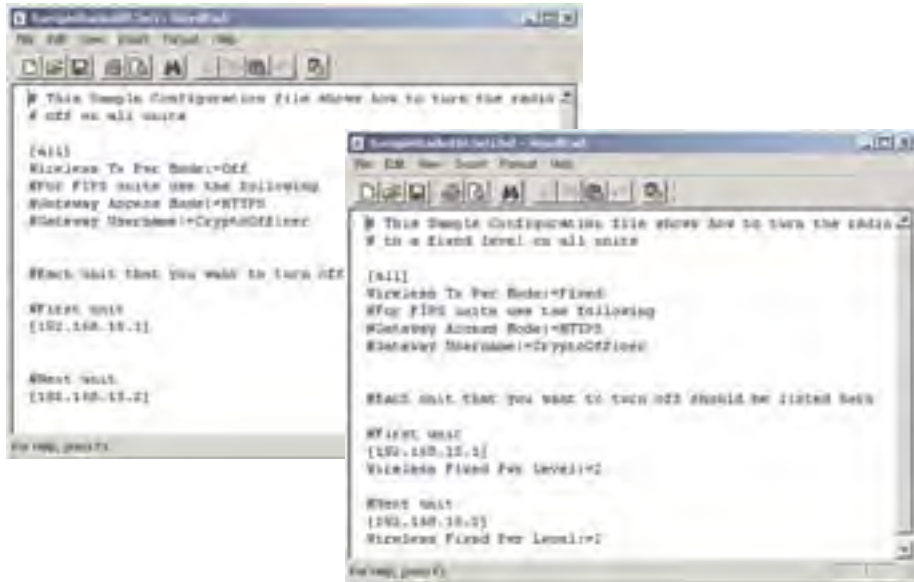
To see the contents of one of these files, simply right click the file name and select **Open** from the dropdown menu.

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 following screen. 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-531APs 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.)



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

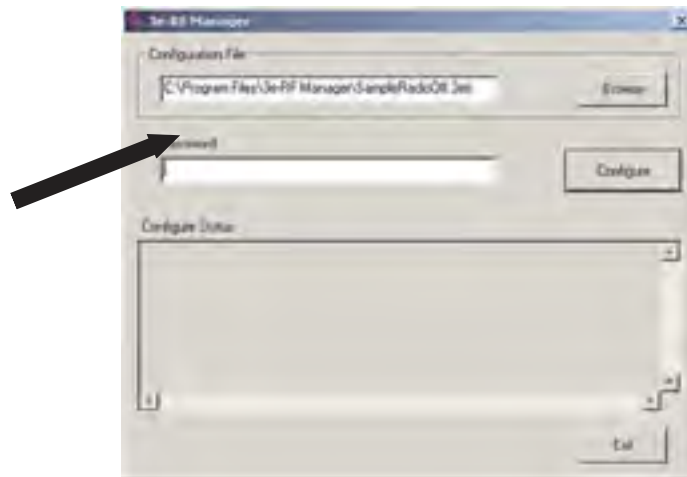
#Next unit
[192.168.15.2]
Wireless Fixed Pwr Level:=2
```

Important: you must remove the pound sign (#) from in front of any line that you want to be "read" by the program.

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.

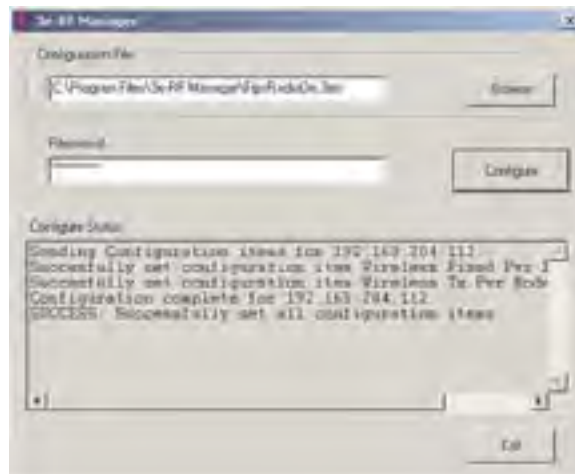
Now enter the Password for that group of APs.



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.



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 8: Network Printer Setup

If you want to have the 3e AP 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. (See the **Troubleshooting** chapter if you have Windows 95/98. Windows XP is similar to Windows 2000.)

Install Print Service for Unix (Windows 2000):

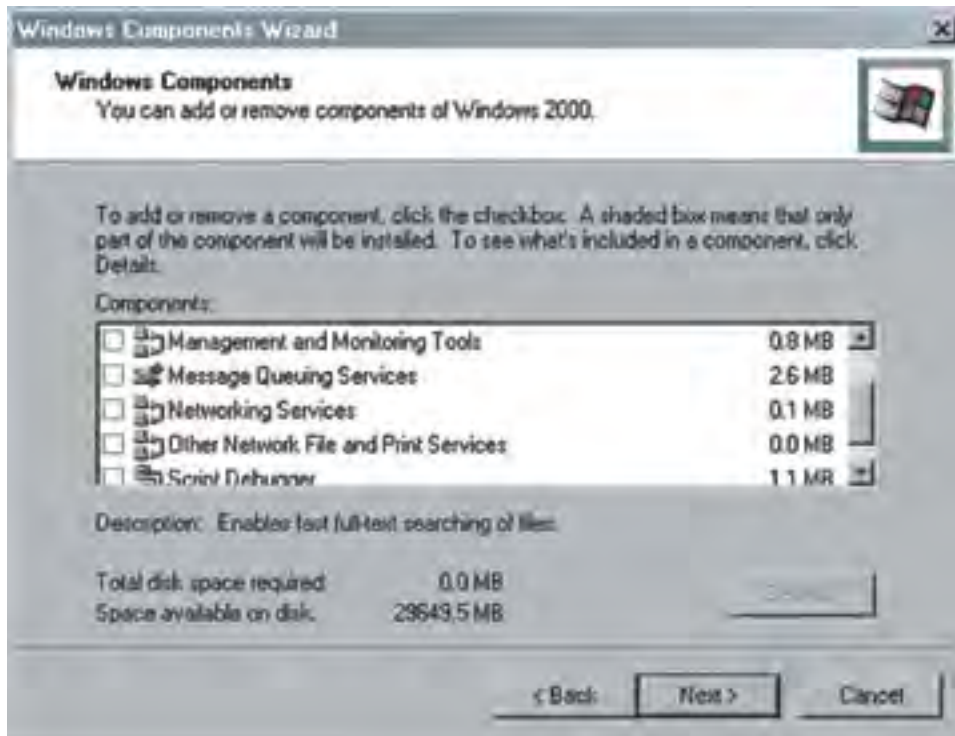
1. Open the Control Panel and select **Add/Remove Programs**



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.

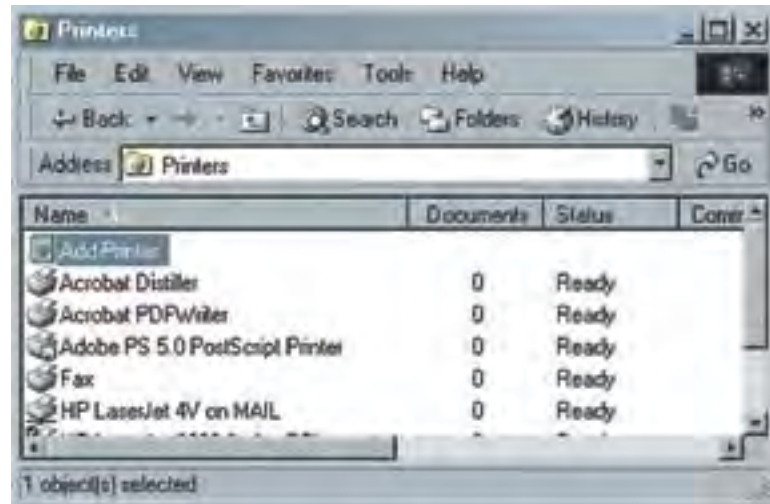
Printer Setup

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

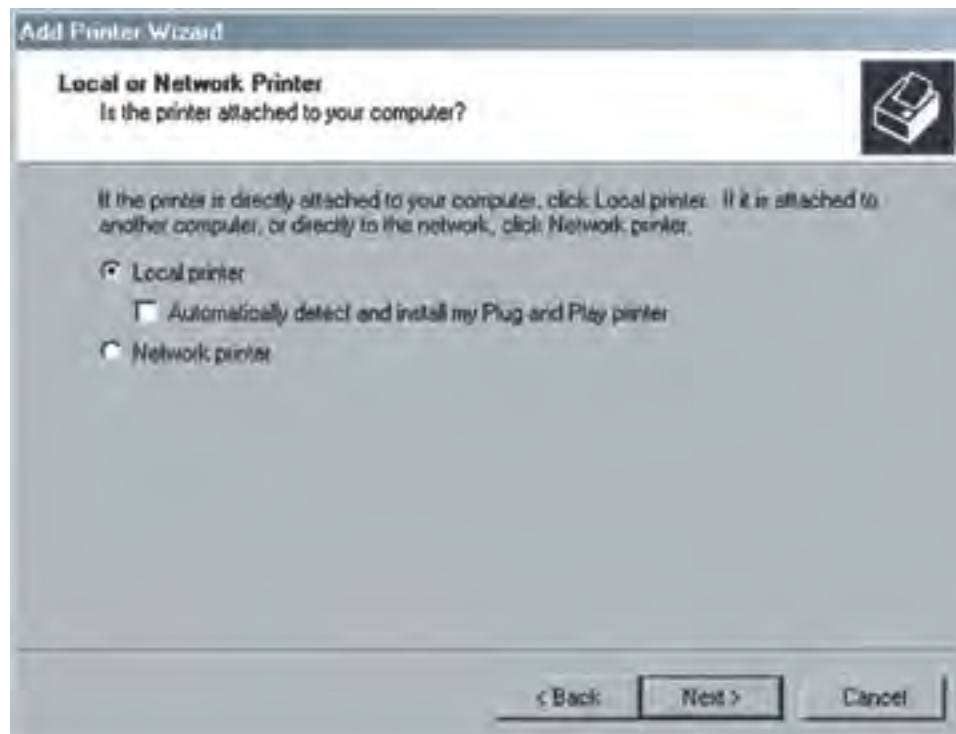
1. Access the **Control Panel** and select the **Printers** icon as shown on the following picture.



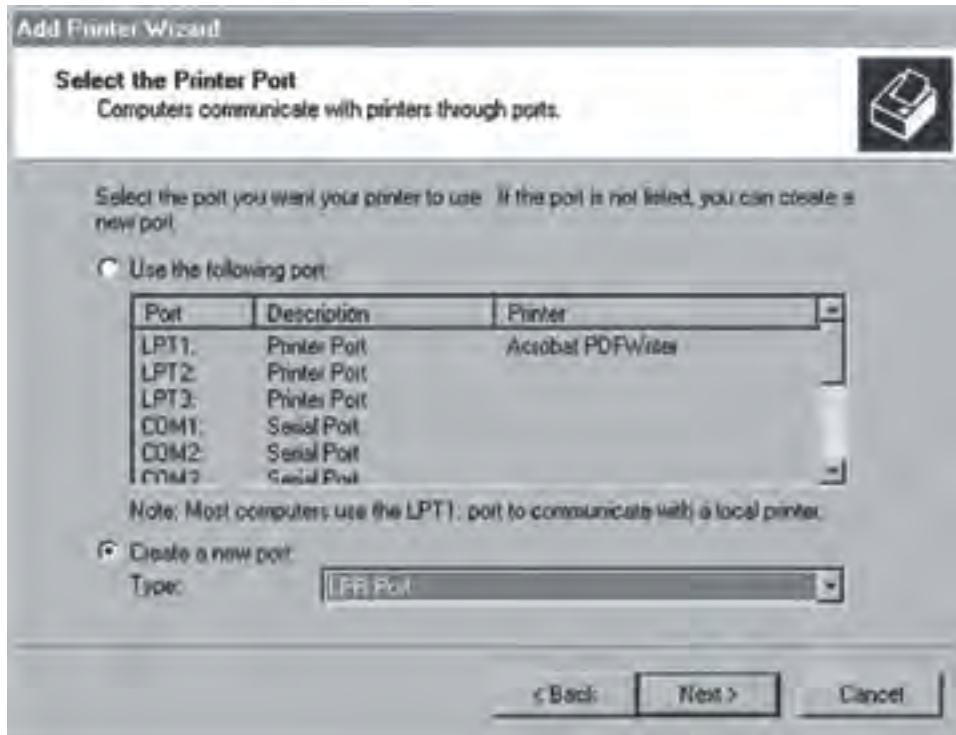
- From the **Printers** window, select **Add Printer**.



- The **Add Printer Wizard** starts. Click **Next**.
- 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-520 Gateway LAN. In the field for **Name of printer or print queue on the server:** type **lp**. 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 9: Technical Support

Manufacturer's Statement

The 3e-531AP 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.

This page intentionally left blank.

Glossary

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 Wi-Fi)

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.

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.

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.

Certification Authority

An entity responsible for establishing and vouching for the authenticity of public keys belonging to users (end entities) or other authorities. Activities of a certification authority can include binding public keys to distinguished names through signed certificates, managing certificate serial numbers, and certificate revocation.

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.

DMA

An abbreviation of Direct Memory Access, DMA is a technique for transferring data from main memory to a device without passing it through the CPU. Computers that have DMA channels can transfer data to and from devices much more quickly than computers without a DMA channel can. This is useful for making quick backups and for real-time applications.

DMZ

A DMZ (Demilitarized Zone) is used by a company that hosts its own Internet services. It sits between the Internet and the internal network. It is a combination of firewalls and bas-

tion hosts. Typically, the DMZ contains web servers, FTP servers, SMTP (email) servers, and DNS servers.

NAT (Network Address Translation)

an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.

NMS (Network Management Station)

Includes such management software as HP Openview and IBM Netview.

PCMCIA

Short for Personal Computer Memory Card International Association, and pronounced as separate letters, PCMCIA is an organization consisting of some 500 companies that has developed a standard for small, credit card-sized devices, called PC Cards. Originally designed for adding memory to portable computers, the PCMCIA standard has been expanded several times and is now suitable for many types of devices.

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.

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.