



AirGuard™ Wireless Access Point User's Guide

Model 3e-525C-3



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

29000171-001 A

publ. 12/12/05

This page intentionally left blank.

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

Model 3e-525C-3

Copyright © 2005 3e Technologies International, Inc. All rights reserved. No part of this documentation may be reproduced in any form or by any means or to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3e Technologies International.

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

3e Technologies International provides this documentation without warranty, term or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms, or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3e Technologies International may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time. Certain features listed may have restricted availability and/or are subject to change without notice - please confirm material features when placing orders.

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. AirGuard™ is a trademark of 3e Technologies International, Inc.

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

EXPORT RESTRICTIONS

This product contains components, software, and/or firmware exported from the United States in accordance with U. S. export administration regulations. Diversion contrary to U.S. law is prohibited.

Table of Contents

Chapter 1: Introduction	1
Basic Features	2
Wireless Basics.....	2
802.11b	3
802.11g.....	3
802.11a	3
802.11b/g Mixed.....	3
802.11g Super and 802.11a Turbo	4
Network Configuration.....	4
Access Point Configurations.....	4
Possible AP Topologies.....	5
Bridging	6
Default Configuration.....	6
Data Encryption and Security.....	6
SSID	6
WEP	6
WPA/WPA2 with TKIP/ AES-CCMP.....	7
802.11i.....	7
Wireless VLAN	8
MAC Address Filtering	10
DHCP Server.....	10
Operator Authentication and Management	10
Management.....	11
3e-525C-3 Navigation Options	12
Chapter 2: Hardware installation	13
Preparation for Use.....	13
Installation Instructions	14
Minimum System and Component Requirements	14
Cabling	15
Bridge Transmit Distance.....	16
Bridge Antenna Location.....	16
Outdoor Protection Kit Installation.....	17
Earth Ground Connection	18
Lightning Arrestor Installation.....	18
Antenna Installation	20
Sealing Antenna Connections.....	20
Mounting Kit Setup	21
The Indicator Lights	21
Reset Button.....	22
Chapter 3: Access Point Configuration	23
Introduction	23
Preliminary Configuration Steps.....	23
Initial Setup using the “LAN” Port.....	24
System Configuration.....	26
General.....	26
Operating Mode.....	27
WAN.....	28
LAN.....	29
Wireless Access Point Configuration	30
General.....	30
Security	33

No Encryption	33
Static WEP Encryption	34
IEEE 802.11i and WPA	35
Wireless VLAN	37
MAC Address Filtering	38
Rogue AP Detection	39
Advanced.....	40
Wireless Bridge.....	40
Services Settings.....	41
SNMP Agent.....	41
Admin User Management	43
List All Users	43
Add New User	44
Monitoring/Reports.....	45
System Status	45
Bridging Status.....	46
Bridge Site Map	47
Wireless Clients.....	48
Adjacent AP List	48
DHCP Client List.....	49
Logs.....	49
System Log	49
Web Access Log	50
System Administration	51
System Upgrade	51
Firmware Upgrade.....	51
Local Configuration Upgrade	52
Remote Configuration Upgrade	53
Factory Default	55
Remote Logging.....	56
Reboot	56
Utilities	57
Chapter 4: Gateway Configuration	59
Introduction	59
Configuring in Gateway Mode	61
WAN.....	62
Main IP Setting	62
IP Aliasing	63
LAN	64
Security	65
Firewall.....	65
Content Filtering.....	65
IP Filtering	66
Port Filtering	66
Virtual Server	67
Demilitarized Zone (DMZ)	68
Advanced Firewall	69
Chapter 5: Wireless Bridge Configuration	71
Introduction	71
Wireless Bridge — General	72
Auto-forming Wireless Bridging	72
Manual Bridging	74
Monitoring	75
Wireless Bridge — Radio.....	75

Wireless Bridge — Encryption.....	78
Wireless Bridge — MAC Address Filtering.....	79
Setting Up Bridging Type	80
Point-to-Point Bridge Configuration	80
Point-to-Point Bridging Setup Guide - Manual Mode.....	81
Point-to-Point Bridging Setup Guide - Auto Mode	81
Point-to-Multipoint Bridge Configuration	85
Point-to-Multipoint Bridging Setup Guide - Manual Mode.....	86
Point-to-Multipoint Bridging Setup Guide - Auto Mode.....	86
Repeater Bridge Configuration	87
Repeater Bridging Setup Guide - Manual Mode.....	87
Repeater Bridging Setup Guide - Auto Mode.....	88
Chapter 6: Technical Support.....	89
Manufacturer's Statement	89
Radio Frequency Interference Requirements.....	89
Glossary	G-a

Chapter 1: Introduction

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

If encryption is desired for the WLAN, you can employ different encryption depending on the mode you are in. You can select None, Static WEP, WPA, or WPA2. WPA uses TKIP or AES-CCMP so you can employ legacy client WEP cards and still secure the wireless band.

The 3e-525C-3 incorporates Power over Ethernet. The PoE interface on the 3e-525C-3 is compatible with commercial vendor "injected power" hub units.

The 3e-525C-3 includes cryptographic modules for wireless encryption and HTTPS/TLS, for secure web communication. In addition, it contains the capability to use the traditional WEP algorithm, either as static WEP or managed under WPA. The 3e-525C-3 has an Ethernet WAN interface for communication to the wired LAN backbone, Ethernet LAN local port for purposes of initial setup and configuration, and two wireless AP antennas for communicating on the 802.11a/b/g frequencies. Further, it has the capability for use of an external (remote) antenna, for bridging, using the 802.11b/g Mixed, 802.11a, 802.11g Super, 802.11a Turbo frequencies.

Basic Features

The 3e-525C-3 is housed in a sturdy case which is not meant to be opened except by an authorized technician for maintenance or repair. If you wish to reset to factory settings, use the reset function available through the GUI-based management module.

The 3e-525C-3 is wall-mountable.

It has the following features:

- Ethernet uplink WAN port
- Local Ethernet LAN port (for configuration only)
- Wireless VLAN
- Wireless AP with operating range of 2000+ feet
- Wireless Bridge
- Power over Ethernet (PoE)
- Above average temperature range for extreme environments (with TEC option)
- WEP encryption or WPA/WPA2/AES-CCM with TKIP
- HTTPS/TLS secure Web
- DHCP client
- Adjustable Radio Power
- MAC address filtering
- Load Balancing
- Rogue AP Detection

The following security modules have been implemented in the 3e-525C-3 .

- WEP
- WPA/WPA2
- AES-CCM

Wireless Basics

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

802.11b

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

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

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

802.11g

Because 802.11g is backwards-compatible with 802.11b, it is a popular component in LAN construction. 802.11g broadens 802.11b's data rates to 54 Mbps within the 2.4 GHz band using OFDM (orthogonal frequency division multiplexing) technology.

802.11a

The IEEE 802.11a standard is an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.

802.11b/g Mixed

802.11b/g combines 802.11b and 802.11g data rates to offer a broader range.

802.11g Super and 802.11a Turbo

802.11g Super and 802.11a Turbo technologies provide speed and throughput of more than double standard wireless LAN technologies in networking products such as PCs, access points, routers and PC cards. It is very helpful to users who require additional bandwidth (over standard WLAN technologies) that results in higher throughput necessary for a variety of functions such as: streaming media (video, DVD, MPEG), VoIP, etc., or for providing multiple users on a single WLAN with optimal speeds despite network demand.

108 Mbps is the *maximum link speed* available and the typical MAXIMUM end-user throughput ranges from approximately 40 Mbps to 60+ Mbps, depending on application demand and network environment.

NOTE: Super G's channel bonding feature can significantly degrade the performance of neighboring 2.4GHz WLANs that don't use Super G, because there isn't enough room in the 2.4GHz wireless LAN spectrum for the increased spectrum used by channel bonding. Moreover, Super G doesn't check to see if 11b or 11g standards-compliant devices are in range before using its non-standard techniques.

Network Configuration

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

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

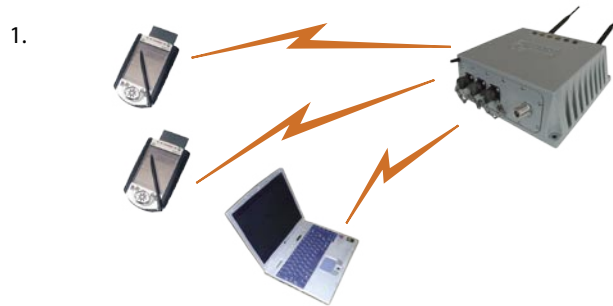
Bridging actually has more choices, but the above choices are popular and are discussed later in this user guide (Chapter 4).

Access Point Configurations

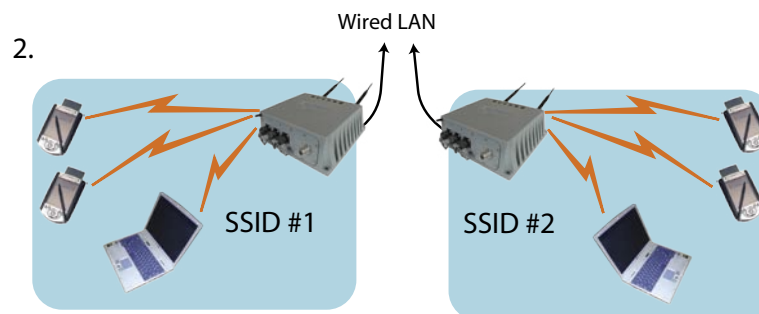
When a 3e-525C-3 is used as an access point, IP addresses for wireless devices are typically assigned by the wired network's DHCP server. The wired LAN's DHCP server assigns addresses dynamically, and the AP virtually connects wireless users to the host wired network. All wireless devices connected to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

Possible AP Topologies

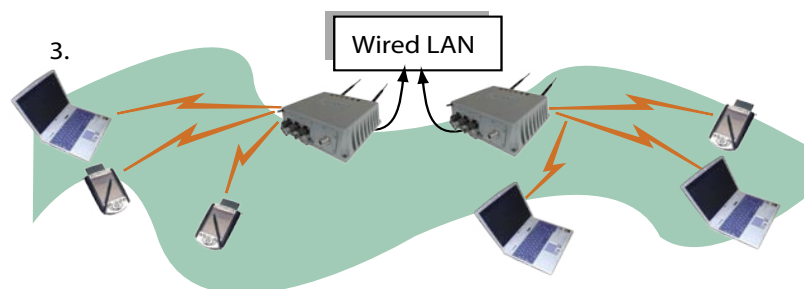
1. An access point can be used as a stand-alone AP without any connection to a wired network. In this configuration, it simply provides a stand-alone wireless network for a group of wireless devices.



2. There can be multiple 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 with a different network ID (SSID).



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



Bridging

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

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

Default Configuration

The 3e-525C-3's default configuration is an Access Point/Bridge.

Data Encryption and Security

The 3e-525C-3 Wireless Access Point includes advanced wireless security features. Over the AP band, you have a choice of no security, Static WEP, WPA, or AES-CCMP, depending on your mode of operation. Some level of security is suggested. Static WEP gives you a choice of 64-bit or 128-bit encryption. WPA includes the option of using a WPA pre-shared key or, for the enterprise that has a Radius Server installed, configuration to use the Radius Server for key management with either TKIP or AES-CCMP. Bridging encryption is established between 3e-525C-3's and includes use of AES-CCMP encryption.

SSID

The Service Set ID (SSID) is a string used to define a common roaming domain among multiple wireless access points. Different SSIDs on access points can enable overlapping wireless networks. The SSID can act as a basic password without which the client cannot connect to the network. However, this is easily overridden by allowing the wireless AP to broadcast the SSID, which means any client can associate with the AP. SSID broadcasting can be disabled in the 3e-525C-3 setup menus.

WEP

WEP is an older encryption standard but is preferable to no encryption. If the 3e-525C-3 is configured with WEP encryption, it is compatible with any 802.11b PC Card configured for WEP.

WPA/WPA2 with TKIP/ AES-CCMP

WPA, an interim standard developed by the WiFi Alliance, combines several technologies. It includes the use of the 802.1x standard and the Extensible Authentication Protocol (EAP). In addition, it uses, for encryption, the Temporal Key Integrity Protocol (TKIP) and WEP 128-bit encryption keys. Finally, a message integrity check (MIC) is used to prevent an attacker from capturing and altering or forging data packets. In addition, it can employ a form of AES called AES-CCMP.

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

802.11i

Four major categories or primary functions of 802.11i are invoked within 3eTI products, including the wireless client devices, wireless access points, and the security server. These primary functions of 802.11i include:

- EAP-TLS: Extensible Authentication Protocol Transport Layer Security, EAP-TLS was compulsory for WPA2 Enterprise products certified prior to April 15, 2005; for products certified after this date, EAP-TLS testing is compulsory if the product can support EAP-TLS. The only products that might not support EAP-TLS are tightly integrated systems that do not support software upgrades by a third party, such as some cell phones intended for, e.g., the 3G market. Non-tightly integrated products like most laptop and PDU adapters still must support EAP-TLS to receive WPA2 certification. 3eTI wireless client and wireless access point devices use standards-based EAP-TLS with no modifications, for complete interoperability with 802.11i and WPA2 certified equipment.
- IEEE 802.1X: also known as port based network access control, 802.1X provides an authentication framework within 802.11i. 802.11i depends upon 802.1X to control the flow of MSDUs between the DS and STAs by use of the IEEE 802.1X Controlled/Uncontrolled Port model. IEEE 802.1X authentication frames are transmitted in 802.11 Data frames and passed via the IEEE 802.1X Uncontrolled Port. The 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an 802.1X authentication procedure completes successfully over the 802.1X Uncontrolled Port. It is the responsibility of the authenticator (3eTI Access Point) to implement port blocking. 802.11 depends upon IEEE 802.1X and the EAPOL-Key 4-Way and Group Key Handshakes, to establish and change cryptographic keys. Keys are established after authentication has completed. Keys may change for a variety of reasons, including expiration of an IEEE 802.1X authentication timer, key compromise,

danger of compromise, or policy. 3eTI products implement standards-based 802.1X with absolutely no custom modifications, again ensuring interoperability with 802.11i and WPA2 certified equipment.

- 4-way handshake: The 4-way handshake defined in 802.11i achieves the following important goals within the security protocol:
 - it confirms the PMK between the supplicant (3e client) and authenticator (3e Access Point)
 - it establishes the temporal keys to be used by the data-confidentiality protocol
 - it authenticates the security parameters that were negotiated
 - it provides keying material to implement the group key handshake within 802.11i

3eTI implements the 4-way handshake within its wireless product line per the 802.11i specification, again with absolutely no custom modifications, in order to maximize interoperability with 3rd party 802.11i and WPA2 compliant equipment.

- AES CCMP: 802.11i and WPA2 employ AES CCM, which is a combination of AES Counter (CTR) mode per packet data encryption, combined with AES Cipher Block Chaining – Message Authentication Code (CBC-MAC) per packet data integrity / authentication of the entire packet including the MAC header. AES CCMP has been deemed to surpass the RC4 stream cipher, upon which the older WEP and WPA security protocols are based. 3eTI was the first company to take its AES algorithm through the NIST CCM algorithm certification process, thereby ensuring that 3eTI's AES CCMP is standards-based, non-proprietary, and ready for wide WPA2 interoperability usage.

Wireless VLAN

According to the IEEE, VLANs define broadcast domains in a Layer 2 network. VLANs have the same attributes as physical LANs with the additional capability to group end stations physically to the same LAN segment regardless of the end stations' geographical location

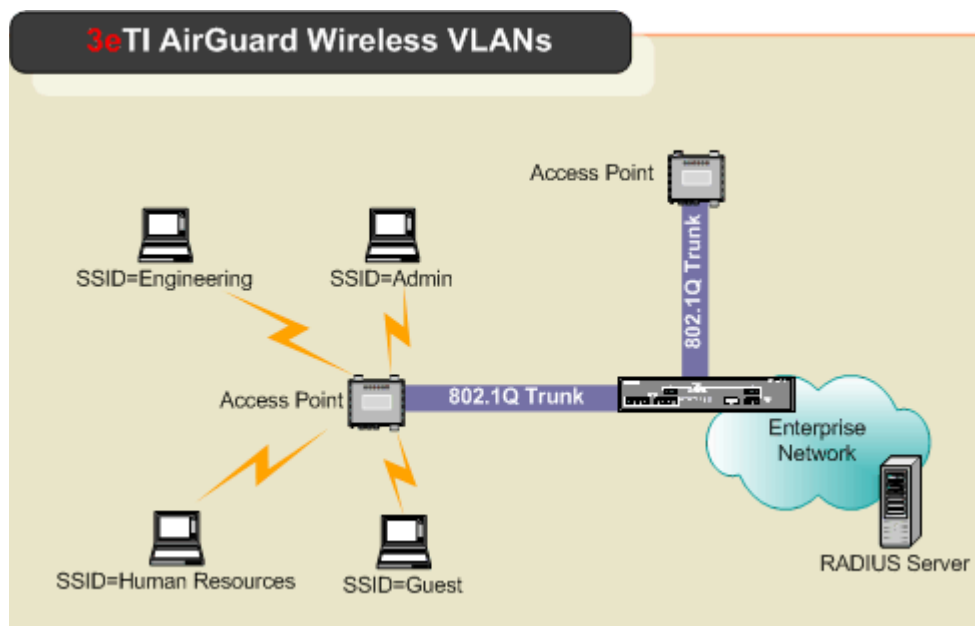
To interconnect two different VLANs, routers or Layer 3 switches are used. These routers or Layer 3 switches execute inter-VLAN routing or routing of traffic between VLANs. Broadcast traffic is then terminated and isolated by these Layer 3 devices (for example, a router or Layer 3 switch will not route broadcast traffic from one VLAN to another).

Wireless VLAN is an extension of Layer 2 wired VLANs in wireless LAN (WLAN) environment. As with wired VLANs, wireless VLANs segregate the WLAN network into disjointed sections, each of which can serve a different purpose or users, such as engineering, accounting or guest. To get the same network configuration, with VLAN incapable

APs, a set of APs need to be installed for each network section; but with a VLAN capable AP, like the 3e-525C-3, one AP can serve multiple sections with traffic segregated inside the AP, so that only one set of APs is needed.

When wireless VLAN is enabled, an AP can be configured to have multiple SSIDs, so that it supports multiple wireless networks. Each network, per configuration, belongs to a VLAN. A wireless client talks with the AP inside a wireless network defined by an SSID, so it does not know the wireless VLAN exists. The mapping between the wireless network and the wireless VLAN happens inside the AP. Each Wireless VLAN can set its own security level. For example, the VLAN for an enterprise network access may use 802.11i with EAP-TLS authentication, while the VLAN for guest internet access may simply use 802.11i with Pre-Shared Key.

3e-525C-3 supports up to 16 VLANs.



When VLAN is enabled, all data coming out of the WAN port is VLAN-tagged, which means an external network unit such as a router, switch, or a VLAN-enabled computer has to be used to terminate the VLAN traffic. Data originating from or targeting to a wireless network client is tagged with the VLAN ID corresponding to the SSID to which it is associated. Data generated by an Access Point itself is tagged with the management VLAN ID.

MAC Address Filtering

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-525C-3 access points, if set up to use MAC address filtering, detect an attempt to connect by a client and compare the client's MAC address to those on a predefined MAC address filter list. Only client addresses found on the list are allowed to associate. MAC addresses are pre-assigned by the manufacturer for each wireless card.

DHCP Server

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

Operator Authentication and Management

Authentication mechanisms are used to authenticate an operator accessing the device and to verify that the operator is authorized to assume the requested role and perform services within that role. The 3e-525C-3 provides authentication services for all users of the wireless network when they first attempt to connect. While the user must log in, basic non-user generated information is allowed to pass on the wireless network prior to authentication, including the authentication data to and from the authentication server and audit records passed from the client to the server. The user is not allowed to specifically send any traffic over the network until successful authentication. Once successfully authenticated, all actions taken by that user (such as accessing a connected printer) and by processes created or started by that user, will be associated with that user, binding the credentials from the user account to all subsequent user processes. This ensures that all processes and network traffic are authorized.

User accounts are defined with three basic attributes: username, role and authentication credentials (i.e. password). A user account can be defined as a normal user or as an administrator. Administrative users can access the TOE management interface in addition to being able to use the wireless network, while normal users can only access the wireless network.

The TOE authentication sequence includes a counter for unsuccessful attempts. When a user or administrator fails to enter the correct credentials after a specified number of attempts (the default is 3), the account will be locked. The account must then be unlocked by a Crypto Officer in the case of an administrator locking their account). This is active for access to the management website.

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

- ID: crypto
- Password: officer

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

Management

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

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

3e-525C-3 Navigation Options	
ACCESS POINT	GATEWAY
System Configuration	System Configuration
General	General
Operating Mode	Operating Mode
WAN	WAN
LAN	LAN
Wireless Access Point	Wireless Access Point
General	General
Security <ul style="list-style-type: none"> • None • Static WEP • 802.11i and WPA 	Security <ul style="list-style-type: none"> • None • Static WEP • 802.11i and WPA
Wireless VLAN	Wireless VLAN
MAC Address Filtering	MAC Address Filtering
Rogue AP Detection	Rogue AP Detection
Advanced	Advanced
Wireless Bridge	Wireless Bridge
General <ul style="list-style-type: none"> • Monitoring 	General <ul style="list-style-type: none"> • Monitoring
Radio	Radio
Encryption <ul style="list-style-type: none"> • AES-CCM 	Encryption <ul style="list-style-type: none"> • AES-CCM
MAC Address Filtering (Auto Bridge mode only)	MAC Address Filtering (Auto Bridge mode only)
Services Settings	Services Settings
SNMP Agent	SNMP Agent
Firewall	Firewall
	Content Filtering
	IP Filtering
	Port Filtering
	Virtual Server
	DMZ
	Advanced
Admin User Management	Admin User Management
List All Users <ul style="list-style-type: none"> • Edit/Delete 	List All Users <ul style="list-style-type: none"> • Edit/Delete
Add New User	Add New User
Monitoring Reports	Monitoring Reports
System Status	System Status
Bridging Status	Bridging Status
Bridging Site Map	Bridging Site Map
Wireless Clients	Wireless Clients
Adjacent AP List	Adjacent AP List
DHCP Client List	DHCP Client List
Logs	Logs
System Log	System Log
Web Access Log	Web Access Log
System Administration	System Administration
System Upgrade <ul style="list-style-type: none"> • Firmware Upgrade • Local Configuration Upgrade • Remote Configuration Upgrade 	System Upgrade <ul style="list-style-type: none"> • Firmware Upgrade • Local Configuration Upgrade • Remote Configuration Upgrade
Factory Default	Factory Default
Remot Logging	Remote Logging
Reboot	Reboot
Utilities	Utilities

Chapter 2: Hardware installation

Preparation for Use

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

FCC Regulations require that the 3e-525C-3 be professionally installed by an installer certified by the National Association of Radio and Telecommunications Engineers or equivalent institution.

The 3e-525C-3 operates with Power over Ethernet (PoE) which requires the installation of a separate Power injector which "injects" DC current into the Cat5 cable. There are two versions of the 3e-525C-3 available, the standard version with a temperature range of -5 degrees C to +50 degrees C, and there is the extended temperature range product with a range of -30 degrees C to +70 degrees C. The latter version of the product employs ThermoElectric Cooler (TEC) technology to extend the product into the higher temperature environment.

The TEC Technology comes with a price, it requires power to transfer the heat. Unfortunately, this raises the electric current requirement to 25 watts, beyond the 802.3af specification of 15.4 watts. To ensure that the 3e-525C-3 with TEC option is provided with the power it requires, an extended range PoE power injector is required such as the 3eTI Model 3e-POE-1 or Hyperlink Technologies Model BT-CAT5-P1.

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

- The 3e-525C-3 Wireless Access Point
- 3 attachable 5dBi omni-directional antennas
- 1 RED Ethernet/PoE cable
- 1 BLUE 4-wire Ethernet cable
- Documentation as PDF files (on CD-ROM)
- Registration and Warranty cards

The following items are accessories:

- Power Injector, POE, 50W (model 3e-POE-1, p/n 90000831-001)
- Power Cord, POE Injector, European version (p/n 90000832-001)
- Power Cord, POE Injector, UK version (p/n 90000833-001)
- 3 meter antenna extension cable
- 3e-OPK-3 outdoor protection kit

The 3e-525C-3 can be mounted outdoors on a high post to achieve the best bridge result. If mounted outdoors, the outdoor protection kit must be used to prevent lightning damage.



To comply with FCC RF exposure compliance requirements, the antennas used with the 3e-525C-3 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-525C-3 is intended to be installed as part of a complete wireless design solution.

This manual deals only with the 3e-525C-3 device and its accessories. 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 that the user not open the unit. Any maintenance required is limited to the external enclosure surface, cable connections, and to the management software (as described in chapter three through five) only. A failed unit should be returned to the manufacturer for maintenance.

Minimum System and Component Requirements

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

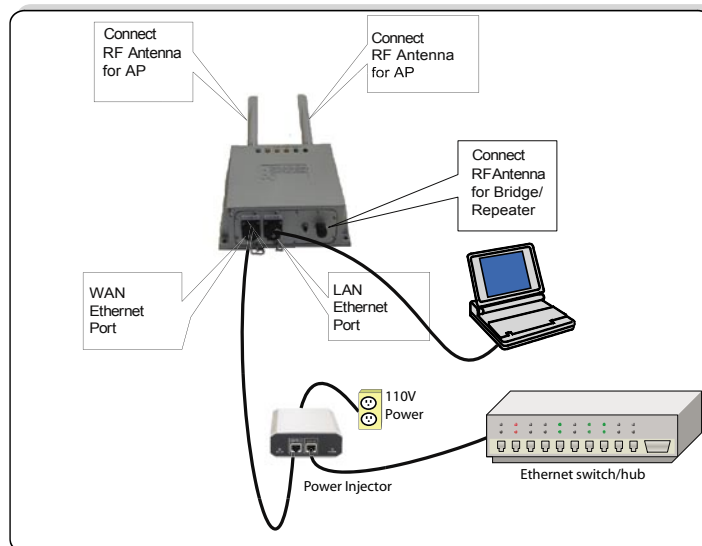
- PCs with one of the following operating systems installed: Windows NT 4.0, Windows 2000 or Windows XP;
- A Wi-Fi compatible 802.11a/b/g device for each computer that you wish to wirelessly connect to your wireless network.
- Access to at least one laptop or PC with an Ethernet card and cable that can be used to complete the initial configuration of the unit.
- A Web browser program (such as Microsoft Internet Explorer 5.5 or later, or Netscape 6.2 or later) installed on the PC or laptop you will be using to configure the Access Point.
- TCP/IP Protocol (usually comes installed on any Windows PC.)

Cabling

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



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



Bridge Transmit Distance

Normally, the bridge need transmit RF signal to another bridge device at long distance. You may need to calculate the RF link Budget as reference. The equation of RF link budget is:

Fade Margin = received signal – receiver threshold

Where

Received signal = Transmitter power – Transmitter cable loss + Transmitter antenna gain – free space path loss + Receiver antenna gain – Receiver cable loss

Received threshold = Received sensitivity

Free Space Path Loss

Using below Free Space Loss Formula to calculate free space path loss

$$L_p = 96.6 + 20\log_{10} F + 20\log_{10} D$$

Where

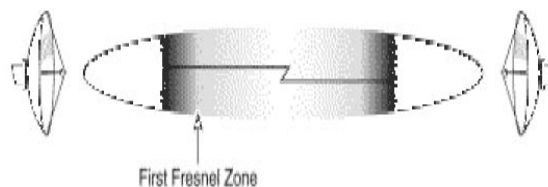
L_p = free space path loss between antennas

F = frequency in GHz

D = path length in miles

Bridge Antenna Location

When as bridge device, the 3e-525C-3 may need to be mounted outdoors on a high place to achieve the best bridge result. The Fresnel zone and Earth bulge dominate to decide how high that the unit's Antenna need be put. The total antenna height equals the width of Fresnel zone plus the height of earth bulge.



The Fresnel zone is the area around the visual line-of-sight that radio waves spread out into after they leave the antenna. This area must be clear or else signal strength will weaken. The rule of thumb is that 60% of the Fresnel zone must be clear of obstacles. Typically, 20% Fresnel Zone blockage introduces little signal loss to the link. Beyond 40% blockage, signal loss will become significant.

The equation of the width of Fresnel Zone is:

$$W = 43.3 \times \sqrt{\frac{D}{4F}}$$

Where

W = Width of the Fresnel Zone (in feet)

D = Distance between the antennas (in miles)

F = Frequency in GHz

When the transmit distance of RF signal is longer than seven miles, the curvature of the earth may be a factor and require the antenna put at higher location. The additional antenna height can be calculated by below formula:

$$H = \frac{D^2}{8}$$

Where

H = Height of earth bulge (in feet)

D = Distance between antennas (in miles)

Outdoor Protection Kit Installation

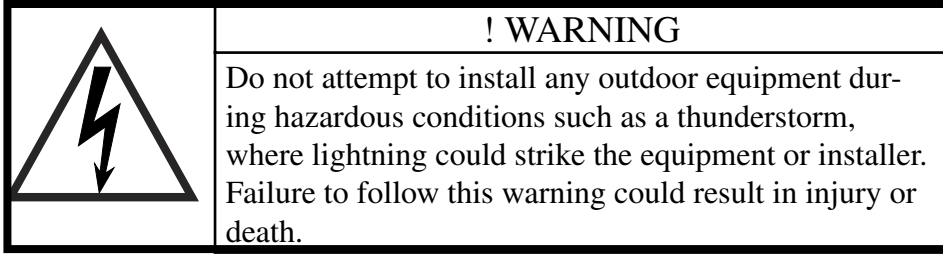
If any portion of this system (3e-525C-3 enclosure, antennas, cables etc.) is mounted outdoors, it is strongly recommended that the Outdoor Protection Kit (3e-OPK-3) for this product be used. This kit contains lightning arrestors and ground cables designed for this product.

If the system is mounted outdoors where CE Mark certification is required, use of the Outdoor Protection Kit (or equivalent) is **MANDATORY**. Failure to install this protection will void the warranty.

The Outdoor Protection Kit (3e-OPK-3) contains the following items:

- 10-inch, 10AWG wire with #8 ring terminal on one end and a #10 ring terminal on the other end
- 12-inch, 10 AWG wire with #8 ring terminal on one end and a #10 ring terminal on the other end
- 18-inch, 10 AWG wire with #8 ring terminal on one end and a #10 ring terminal on the other end
- Three lightning arrestors, Reverse N Polarity

NOTE: You (the user) are required to ensure that the connection to a proper earth ground is made by properly certified and authorized personnel and must conform to all applicable codes and regulations. The materials required to connect to a proper ground are defined by local conditions and must be procured locally to ensure the correct safety environment is achieved. The cable used to connect to a proper ground must be AWG 10 or heavier. This cable should be kept as short as possible.



Earth Ground Connection

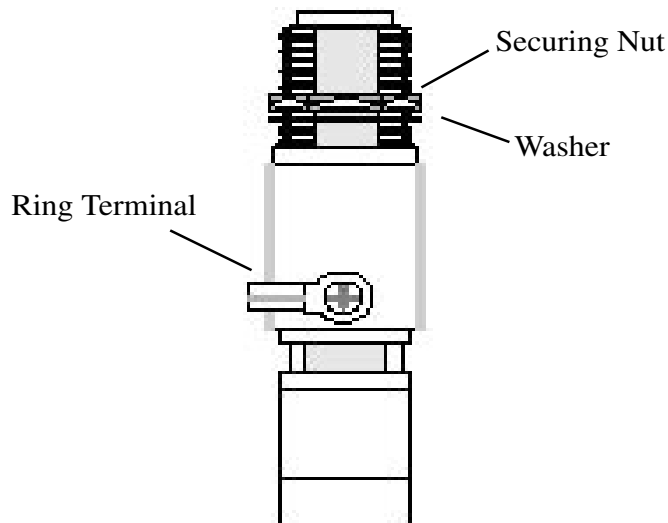
Attach the earth ground cable to the ring terminal attached to the 3e-525C-3's grounding stud. Make sure the ring terminal is against the unit's metal case. The earth ground ring terminal should be the first connection on the unit's grounding stud.

NOTE: The cable used to connect to a proper earth ground must be AWG 10 or heavier. This cable should be kept as short as possible.

Lightning Arrestor Installation

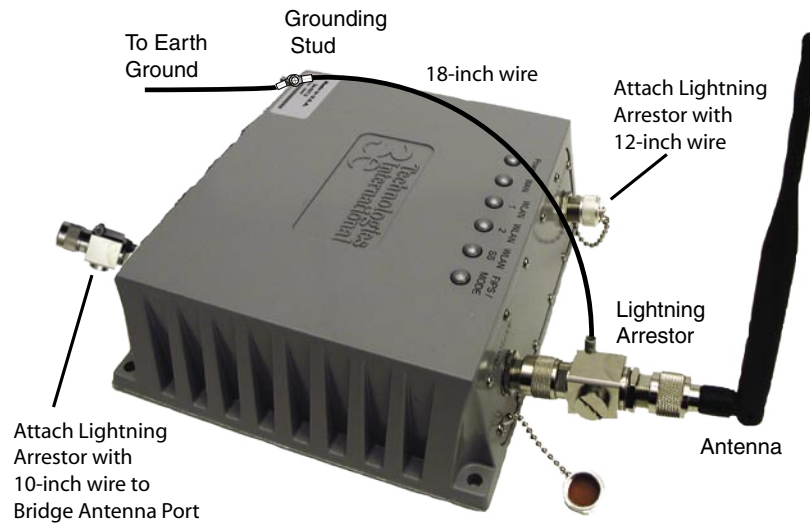
Examine the lightning arrestors and remove and discard the following items (if necessary). See figure below.

- Securing Nut
- Washer
- Ring Terminal (but retain the screw)



Attach the 10, 12, and 18-inch wires to the lightning arrestors ensuring that the smaller ring terminals and with identifying labels are used. Tighten the ring terminal securely using a screwdriver.

To install the lightning arrestors to the 3e-525C-3, attach one end of the lightning arrestor to the 3e-525C-3's N connector. Make sure that the lightning arrestor with the 12-inch wire is mounted closer to the ground stud (see figure). Tighten the two lightning arrestors to the N connector finger tight.



Attach the ring terminal from the Lightning Arrestors' ground cable to the grounding stud on the 3e-525C-3 unit. The lightning arrestor's ring terminal should be attached to the unit after the earth ground ring terminal is attached.

Perform this same procedure for every antenna installed on the unit.

It is recommended that this Outdoor Protection Kit be replaced every three years. If the unit is operated in an area subject to intense lightning activity, it is recommended that the Outdoor Protection Kit be replaced every year.

Antenna Installation

The 3e-525C-3 ships with two 5dBi omni-directional antennas. These antennas should be connected to the AP antenna connectors located on the rear of the unit.

NOTE: Make sure a lightning arrestor is installed between the unit and the antenna if any part of this assembly is located outdoors. See the previous section.



If you are not using the access point function then you do not need the AP antennas. Make sure during your configuration set up that you go to the **Wireless Access Point—General** screen and set the Tx Pwr Mode to Off (see Chapter 3).

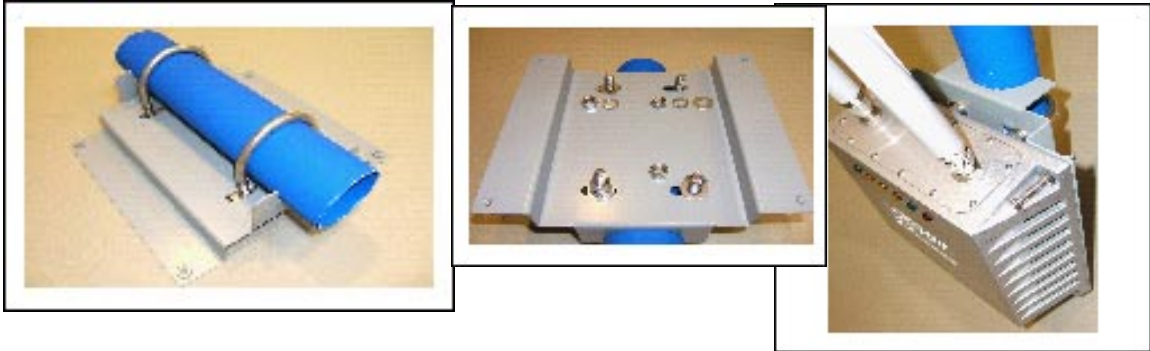
Sealing Antenna Connections

Once all antennas have been installed, the connections should be sealed to protect them from the exterior harsh environment. Use a self amalgamating polyisobutylene tape which, over a period of hours, adheres to itself and forms a single amalgamated rubber molding conforming to the shape of the item it is covering. Once the tape is in place for several hours, it forms a shaped rubber molding that is resistant to water and most solvents. It remains stable over a wide temperature range and degrades very slowly in sunlight. If you need to remove the tape after it has sealed for 30 minutes or more, cut it away with a sharp knife.

The bridge antenna port is located on the front of the 3e-525C-3. To obtain the best performance, the bridge antenna should be placed away from the AP antennas. Use a 1.5 meter low loss antenna cable to connect a directional antenna to the 3e-525C-3. The maximum gain for the directional antenna should be 14 dBi.

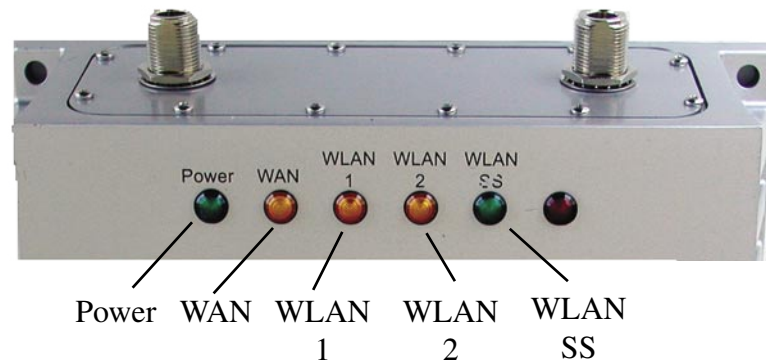
Mounting Kit Setup

To mount the 3e-525C-3 outdoors, you should choose a suitable post to mount the unit high in the air. Use the U-ring, screws and nuts to attach the mounting plate to the post. Next attach the 3e-525C-3 to the mounting plate with screws.



The Indicator Lights

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



LED	Description
Power	The Power indicator LED informs you when the gateway is on or off. If this light is on, the gateway is on; if it is not on, the gateway is off.
WAN	This light indicates the state of your connection to the organization's Ethernet LAN network. When on, the WAN light indicates that the unit is connected to the network. When the WAN light is off, the gateway does not have an active connection to the network.
WLAN1 Activity (AP)	This light may be steady or blinking and indicates that information is passing through the AP connection.
WLAN2 Activity (Bridge)	This light may be steady or blinking and indicates that information is passing through the Bridge connection.
WLAN Signal Strength (Bridge)	The Strength LED indicator indicates the strength of the Bridge connection (WLAN2). <ol style="list-style-type: none"> 1. LED Off: means no connection on the bridge side, or the signal is very weak. 2. LED blinks slowly (every 1 second): means there is a connection, and the signal quality is poor. 3. LED blinks fast: means there is a connection, and the signal quality is good. 4. LED steady on: means there is a connection, and the signal quality is excellent.

Note: When the WLAN1 and WLAN2 LEDs blink simultaneously then the system is halted. The software has discovered a problem with the encryption algorithm or the system configuration does not pass the integrity check.

Reset Button

You can reboot the 3e-525C-3 by pressing and holding the reset button on the front of the unit for five seconds. Input is acknowledged by the LWLANSS LED turning on.

To reset the 3e-525C-3 to its factory default press and hold the reset button located on the front of the unit for 10 seconds. Input is acknowledged by the WLANNSS LED turning on and then turning off after 10 seconds.

Chapter 3: Access Point Configuration

Introduction

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

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

Preliminary Configuration Steps

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

- IP address – a list of IP addresses available on the organization's LAN that are available to be used for assignment to the AP(s)
- Subnet Mask for the LAN
- Default IP address of the 3e-525C-3
- 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-525C-3 network of access points (if MAC address filtering is to be enabled)
- The appropriate encryption key for wireless communication.

Initial Setup using the “LAN” Port

Plug one end of an RJ-45 Ethernet cable to the LAN port of the 3e-525C-3 (see page 15) and the other end to an Ethernet port on your laptop. This LAN port in the 3e-525C-3 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 configuration. In order to connect properly to the 3e-525C-3 on the LAN port, the TCP/IP parameters on your laptop must be set to “obtain IP address automatically.” (If you are unfamiliar with this procedure, use the following instructions for determining or changing your TCP/IP settings.)

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

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

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

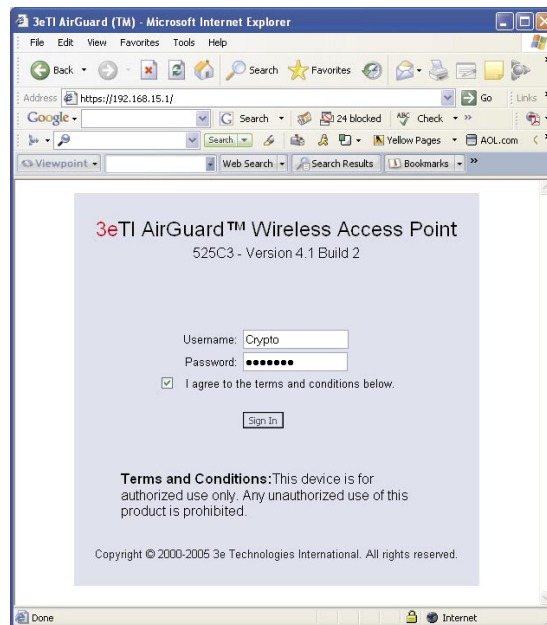
In Windows 98/Me, click **Start**, then **Run** and type **winipcfg** in the run instruction box. Then click **OK**. You will see the IP address of your laptop in the resulting window, along with the “default gateway” IP address. Verify that the IP address shown is 192.168.15.x

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

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



You will be asked for your User Name and Password. The default is "crypto" with the password "officer" to give full access for setup configuration. (This password is case-sensitive.) Please read the terms and conditions and check the checkbox then click **Sign In** to continue configuration.



System Configuration

General

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

This screen lists the firmware version number for your 3e-525C-3 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.) You can also enter a description of the physical location of the unit in the Description field. This is useful when deploying units to remote locations.

To set the date and time, you can do it manually or set it based on the NTP server.

Also, you can modify the terms and conditions login banner on the login screen. The default is "This device is for authorized use only. Any unauthorized use of this product is prohibited."

When you are satisfied with your changes, click **Apply**.

3eTI AirGuard™ Wireless Access Point

Operation Mode: Wireless AP/Bridge Mode

Username: CryptoOfficer Host Name: default (192.168.254.254)

Role: Crypto Officer

System Configuration -> General

Version: 525C3 - Version 4.1 Build 2

Description: default location

Host Name: default

Domain Name: default

System Time: Date: 01/01/2005 Time: 20:54

Manual

New Date: / / (Month / Day / Year)

New Time: : : (Hour:Minute)

From NTP Server

Time Zone: (GMT-05:00) Eastern Time (US & Canada)

Time Server 1:

Time Server 2:

NIST servers: time-a.nist.gov, time-b.nist.gov, time.nist.gov

Login Banner:

Maximum 500 characters. If shorter than 5 characters, the system default banner will be displayed.

Current number of characters: 0

Apply

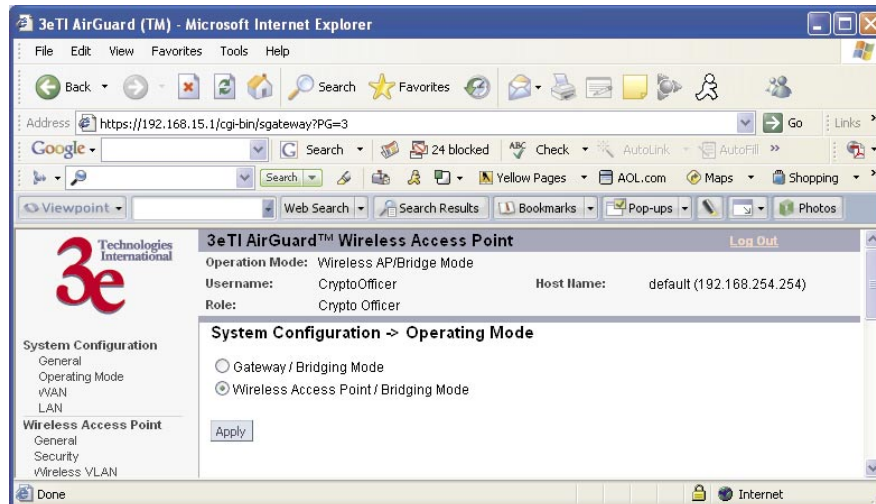
© 2000-2005 3e Technologies International. All rights reserved.

Go next to the **System Configuration — Operating Mode** page.

Operating Mode

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

Note that if you change modes from AP to Gateway, your configuration is not lost.



WAN

Click the entry on the left hand navigation panel for **System Configuration — WAN**. This directs you to the **System Configuration — WAN** screen.

If not using DHCP to get an IP address, input the static IP information that the access point requires in order to be managed from 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.

The screenshot shows the configuration page for a 3eTI AirGuard Wireless Access Point. The browser window title is "3eTI AirGuard (TM) - Microsoft Internet Explorer". The address bar shows "https://192.168.15.1/cgi-bin/sgateway?PG=1". The page content includes a navigation menu on the left and a main configuration area. The main area is titled "3eTI AirGuard™ Wireless Access Point" and shows the following information:

- Operation Mode: Wireless AP/Bridge Mode
- Username: CryptoOfficer
- Role: Crypto Officer
- Host Name: default (192.168.254.254)

The "System Configuration -> WAN" section is active, showing the following settings:

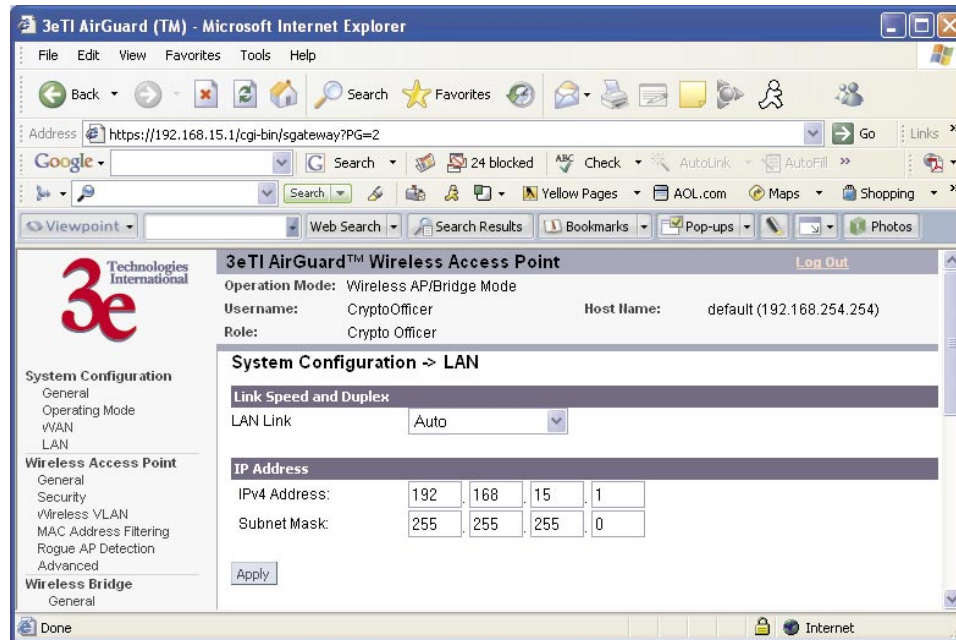
- Link Speed and Duplex:** WAN Link is set to "Auto".
- IP Address:**
 - Using DHCP to get an IP address
 - Specify a static IP address
- IP Address:** 192 . 168 . 254 . 254
- Subnet Mask:** 255 . 255 . 255 . 0
- Default Gateway:** 192 . 168 . 254 . 1
- DNS 1:** [] . [] . [] . []
- DNS 2:** [] . [] . [] . []

An "Apply" button is located at the bottom of the configuration section.

LAN

Click the entry on the left hand navigation panel for **System Configuration — LAN**. This directs you to the **System Configuration — LAN** screen.

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



Wireless Access Point Configuration

General

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

The **Wireless Access Point — General** screen lists the MAC Address of the AP card. This is not the MAC Address that will be used for the BS-SID for bridging setup, however. That is found on the **Wireless Bridge — General** screen.

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

The screenshot displays the configuration interface for a 3eTI AirGuard Wireless Access Point. The browser window shows the URL `https://192.168.15.1/cgi-bin/sgateway?PG=10`. The page title is "3eTI AirGuard™ Wireless Access Point". The user is logged in as "CryptoOfficer" with the role of "Crypto Officer". The host name is "default (192.168.254.254)".

The configuration is set to "Wireless AP/Bridge Mode". The "General" tab is selected, showing the following settings:

- MAC Address: 00:0B:6B:35:2E:D8 (WistronNew)
- SSID: default
- Wireless Mode: 802.11b
- Channel No.: 1 (2.412 GHz)
- Automatically select the optimal channel at bootup: No
- Tx Pwr Mode: Auto
- Fixed Power Level: 1

The "Advanced" section includes:

- Beacon Interval: 100 (Range: 20-1000)
- RTS Threshold: 2346 (Range: 1-2346)
- DTIM: 1 (Range: 1-255)
- Basic Rates: 1, 2 Mbps
- Preamble: Long Preamble
- Broadcast SSID: Enable

An "Apply" button is located at the bottom of the configuration area.

Select the wireless mode from the drop-down list. You can choose from the following options:

- 802.11b
- 802.11g
- 802.11g Super
- 802.11b/g Mixed
- 802.11a
- 802.11a Turbo

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

The **Channel Number** is a means of assigning frequencies to a series of access points, when many are used in the same WLAN, to minimize noise. 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 click on the button **Select the optimal channel**, a popup screen will display the choices. It will select the optimal channel for you. You can also set it up to automatically select the optimal channel at boot up.

CHANNEL NO. OPTIONS	
Wireless Mode	Channel No.
802.11b 802.11g 802.11b/g Mixed	1 (2.412 GHz) 2 (2.417 GHz) 3 (2.422 GHz) 4 (2.427 GHz) 5 (2.432 GHz) 6 (2.437 GHz) 7 (2.442 GHz) 8 (2.447 GHz) 9 (2.452 GHz) 10 (2.457 GHz) 11 (2.462 GHz)
802.11g Super	6 (2.437 GHz)
802.11a	52 (5.26 GHz) 56 (5.28 GHz) 60 (5.30 GHz) 64 (5.32 GHz) 149 (5.745 GHz) 153 (5.765 GHz) 157 (5.785 GHz) 161 (5.805 GHz) 165 (5.825 GHz)
802.11a Turbo	50 (5.25 GHz) Turbo Mode 58 (5.29 GHz) Turbo Mode 152 (5.76 GHz) Turbo Mode 160 (5.80 GHz) Turbo Mode

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 1-5 for Fixed Pwr Level (1 being the shortest distance.) Finally, if you want to prevent any radio frequency transmission, set Tx Pwr Mode to **Off**.

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

ADVANCED OPTIONS		
Beacon interval	20-1000	The time interval in milliseconds in which the 802.11 beacon is transmitted by the AP.
RTS Threshold	1-2346	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	1-255	The number of beacon intervals that broadcast and multicast traffic is buffered for a client in power save mode.
Basic Rates	Basic Rates for 802.11b	
	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.
	Basis Rates for 802.11g	
	1, 2, 5.5, 11, 6, 12, 24 Mbps 1, 2, 5.5, 11 Mbps	
	Basic Rates for 802.11g Super	
	1, 2, 5.5, 11, 6, 12, 24 Mbps 1, 2, 5.5, 11 Mbps	
	Basic Rates for 802.11b/g Mixed	
	1, 2 Mbps 1, 2, 5.5, 11 Mbps	
	Basic Rates for 802.11a	
	6, 12, 24 Mbps	
Basic Rates for 802.11a Turbo		
6, 12, 24 Mbps		
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.

Security

The **Wireless Access Point — Security** screen displays a default factory setting of no encryption, but for security reasons it will not communicate to any clients unless the encryption is set by the CryptoOfficer. There are different encryption options for the AP. The following chart shows the differences:

Encryption Options
None
802.11i and WPA (Preshared Key or 802.1x using Radius Server, and TKIP or AES-CCMP)
Static WEP

No Encryption

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

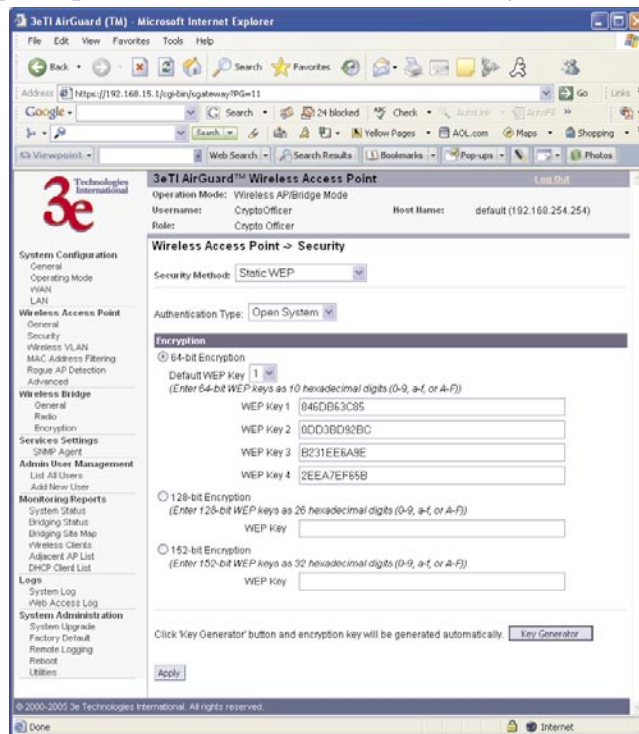


Static WEP Encryption

If you choose to use WEP encryption, you can also select whether it will be Open System or Shared Key authentication. For greater security, set authentication type to “shared key.” WEP Data encryption can be set to 64-bit or 128-bit encryption.

The Key Generator button automatically generates a randomized key of the appropriate length. This key is initially shown in plain text so the user has the opportunity to copy the key. Once the key is applied, the key is no longer displayed in plain text.

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



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

IEEE 802.11i and WPA

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

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

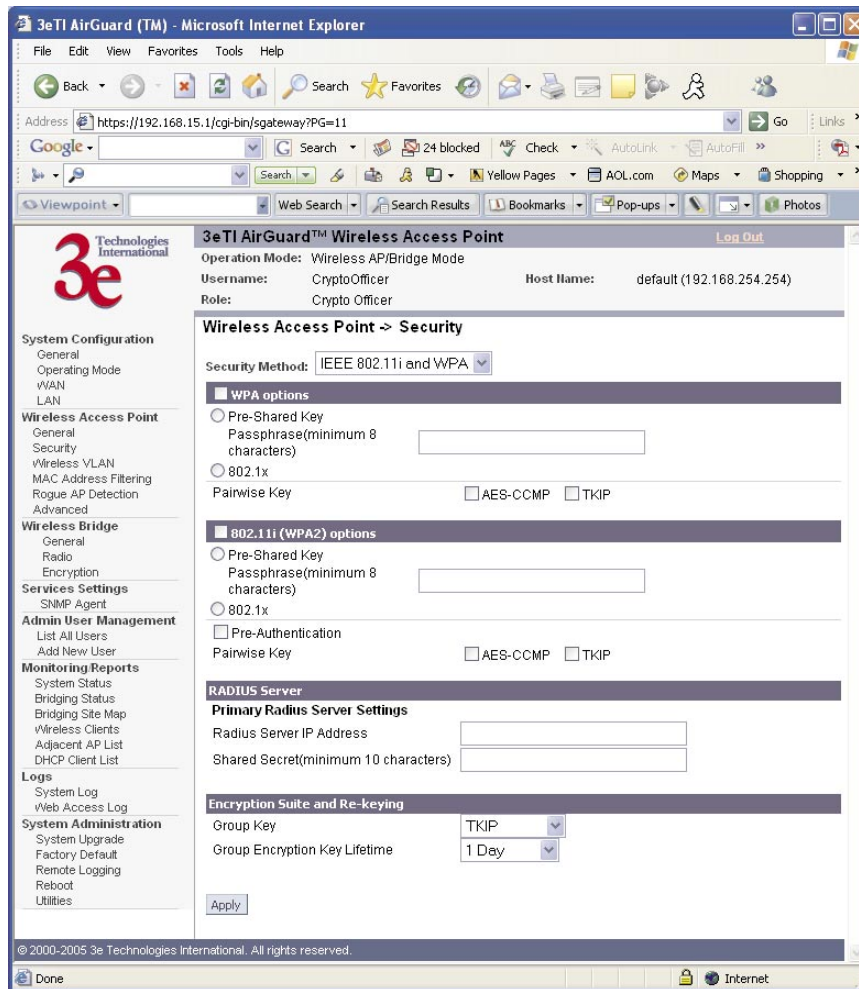
If you are a SOHO user, selecting pre-shared key means that you don't have the expense of installing a Radius Server. Simply input up to 63 character / numeric / hexadecimals in the Passphrase field. If your clients use WPA-TKIP, select TKIP as encryption type. If your clients use WPA-AES, select AES-CCMP.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

Enable pre-authentication to allow a client to authenticate in advance with the AP before the client is associated with it. Allowing the AP to pre-authenticate a client decreases the transition time when a client roams between APs.

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

Re-keying time is the frequency in which new encryption keys are generated and distributed to the client. The more frequent re-keying, the better the security. For highest security, select the lowest re-keying interval.

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

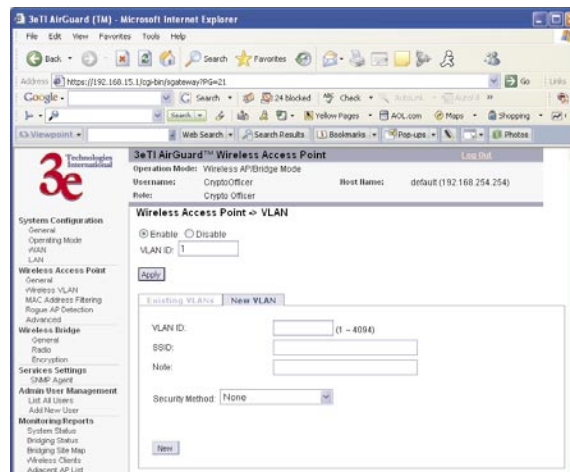


If you will be using MAC Address filtering, navigate next to the MAC Address Filtering screen.

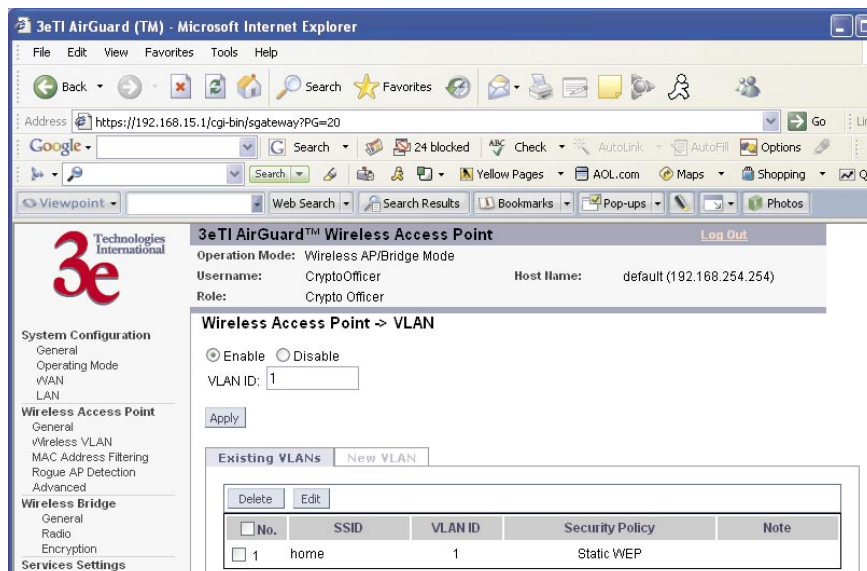
Wireless VLAN

When VLAN is enabled, all data coming out of the WAN port is VLAN-tagged, which means an external network unit such as a router, switch, or a VLAN-enabled computer has to be used to terminate the VLAN traffic. Data originating from or targeting to a wireless network client is tagged with the VLAN ID corresponding to an SSID it is associated with. Data generated by an Access Point itself is tagged with the management VLAN ID.

To create a new VLAN, enter a VLAN ID (range from 1 to 4094) and an SSID. Set the security to None, Static WEP, or IEEE 802.11i and WPA.

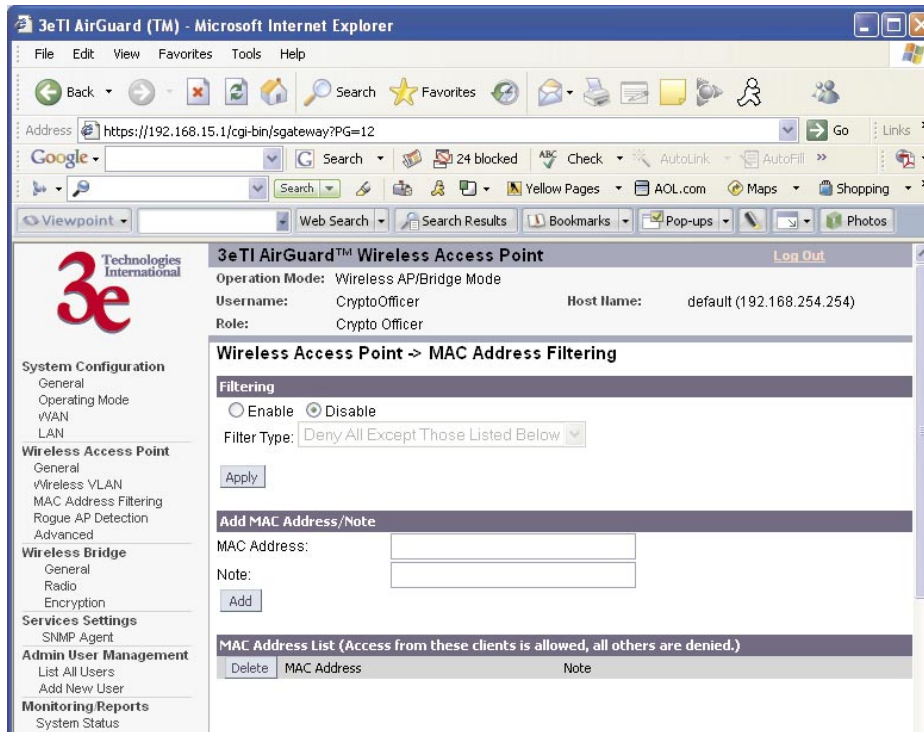


After you create a VLAN you can modify it by selecting the VLAN from the existing VLAN list.



MAC Address Filtering

The **Wireless Access Point — MAC Address Filtering** screen is used to set up MAC address filtering for the 3e-525C-3 device. 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 **Deny All Except Those Listed Below**, 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 **Allow All Except Those Listed Below**, 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.

Rogue AP Detection

The **Wireless Access Point — Rogue AP Detection** screen allows the network administrator to set up rogue AP detection. Enable rogue AP detection and 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-525C-3 is located on the **System Configuration — General** screen. You can also select the following filter options.

- **SSID Filter:** Check the SSID option to only send rogue APs that match the AP's SSID or wireless bridge's SSID.
- **Channel Filter:** Check the channel filter option to only send rogue APs that match the AP's channel or the wireless bridge's channel.
- If both options are checked, only APs that match both the SSID and channel are sent.

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

The screenshot displays the configuration page for a 3eTI AirGuard™ Wireless Access Point. The browser window title is "3eTI AirGuard (TM) - Microsoft Internet Explorer". The address bar shows "https://192.168.15.1/cgi-bin/sgateway?PG=15". The page header includes the 3e logo and the text "3eTI AirGuard™ Wireless Access Point" with a "Log Out" link. Below the header, the current configuration is shown: Operation Mode: Wireless AP/Bridge Mode, Username: CryptoOfficer, Host Name: default (192.168.254.254), and Role: Crypto Officer.

The main content area is titled "Wireless Access Point -> Rogue AP Detection". It features an "Email Notification" section with radio buttons for "Enable" and "Disable" (selected). Below this is a "To:" field and "Filter Options" with checkboxes for "SSID Filter" and "Channel Filter". An "Apply" button is located below the filter options.

Below the filter options is a section titled "Add Known AP MAC Address/Note (Trusted AP)". It contains the text: "You may enter up to 128 MAC addresses, one per line. You may also enter the note after MAC address. Please use a space to separate the MAC address and note. Example: 665544332211 Build1_AP". There is a "MAC Address:" label and a text input field with a vertical scrollbar. An "Add" button is positioned below the input field.

At the bottom of the page is a table titled "Known AP MAC Address List (Trusted AP)". The table has three columns: "Delete", "MAC Address", and "Note". The table is currently empty.

The left sidebar contains a navigation menu with the following categories and items:

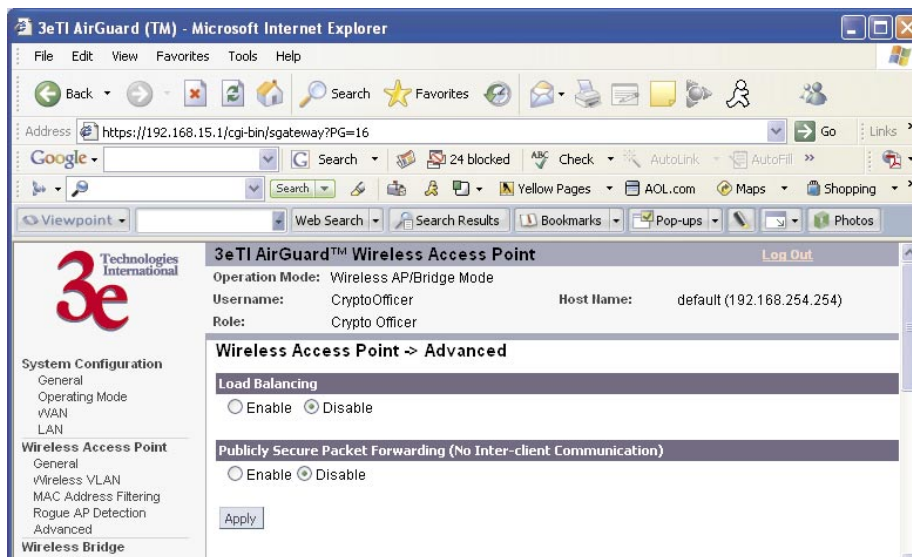
- System Configuration
 - General
 - Operating Mode
 - WAN
 - LAN
- Wireless Access Point
 - General
 - Wireless VLAN
 - MAC Address Filtering
 - Rogue AP Detection
 - Advanced
- Wireless Bridge
 - General
 - Radio
 - Encryption
- Services Settings
 - SNMP Agent
- Admin User Management
 - List All Users
 - Add New User
- Monitoring Reports
 - System Status
 - Bridging Status
 - Bridging Site Map
 - Wireless Clients
 - Adjacent AP List
 - DHCP Client List
- Logs
 - System Log
 - Web Access Log
- System Administration
 - System Upgrade

Advanced

The **Wireless Access Point — Advanced** screen allows you to enable or disable load balancing and to control layer 2 isolation.

Load balancing is enabled by default. 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.

Layer 2 isolation prevents wireless clients that associate with the same AP from communicating with each other.



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

Wireless Bridge

The Wireless Bridge screens are described in Chapter 5.

Services Settings

SNMP Agent

The **Service Settings — SNMP Agent** screen 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-525C-3'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

The screenshot shows the configuration page for the 3eTI AirGuard Wireless Access Point. The browser address bar shows the URL: https://192.168.15.1/cgi-bin/sgateway?PG=33. The page title is "3eTI AirGuard™ Wireless Access Point".

System Configuration:

- General
- Operating Mode
- WAN
- LAN

Wireless Access Point:

- General
- Wireless VLAN
- MAC Address Filtering
- Rogue AP Detection
- Advanced

Wireless Bridge:

- General
- Radio
- Encryption

Services Settings:

- SNMP Agent

Admin User Management:

- List All Users
- Add New User

Monitoring Reports:

- System Status
- Bridging Status
- Bridging Site Map
- Wireless Clients
- Adjacent AP List
- DHCP Client List

Logs:

- System Log
- Web Access Log

System Administration:

- System Upgrade
- Factory Default
- Remote Logging
- Reboot
- Utilities

3eTI AirGuard™ Wireless Access Point

Operation Mode: Wireless AP/Bridge Mode

Username: CryptoOfficer Host Name: default (192.168.254.254)

Role: CryptoOfficer

Services Settings -> SNMP Agent

Enable Disable

Community settings (SNMPv1 & SNMPv2c)

Community	Source	Access Control
1		None
2		None
3		None
4		None
5		None

Secure User Configuration Settings (SNMPv3)

User name	Authentication Type/Password	Encryption Type/Password
1	MD5	DES
2	MD5	DES
3	MD5	DES
4	MD5	DES

System Information

Location: default location

Contact: default contact

EngineID (SNMPv3): defaultID

Apply

© 2000-2005 3e Technologies International. All rights reserved.

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

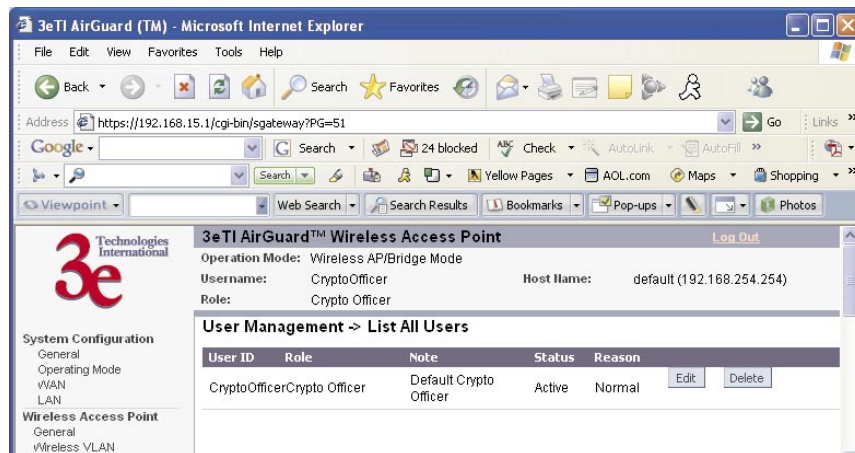
- **Community** –The Community field for Get (Read Only), Set (Read & Write), and Trap is simply the SNMP terminology for “password” for those functions.
- **Source** –The IP address or name where the information is obtained.
- **Access Control** –Defines the level of management interaction permitted.

If using SNMPv3, enter a username (minimum of eight characters), authentication type with key and data encryption type with a key. This configuration information will also need to be entered in your MIB manager setup.

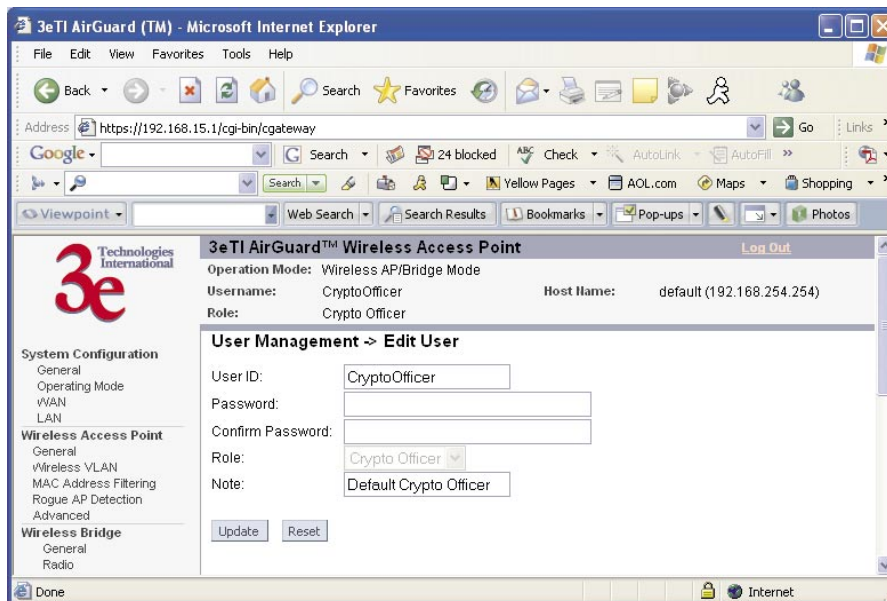
Admin User Management

List All Users

The **Admin User Management — List All Users** screen lists the Crypto Officer and administrator accounts configured for the unit. You can edit or delete users from this screen.

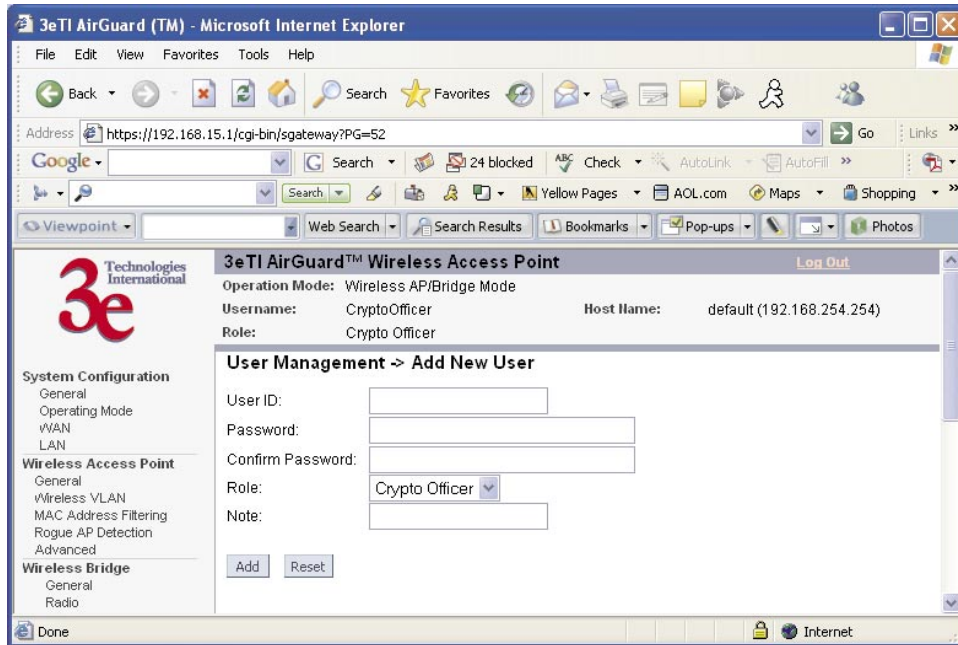


If you click on Edit, the **Admin User Management — Edit User** screen appears. On this screen you can edit the user ID, password, role, and note fields.



Add New User

The **Admin User Management — Add New User** screen allows you to add new Administrators and CryptoOfficers, assigning and confirming the password.

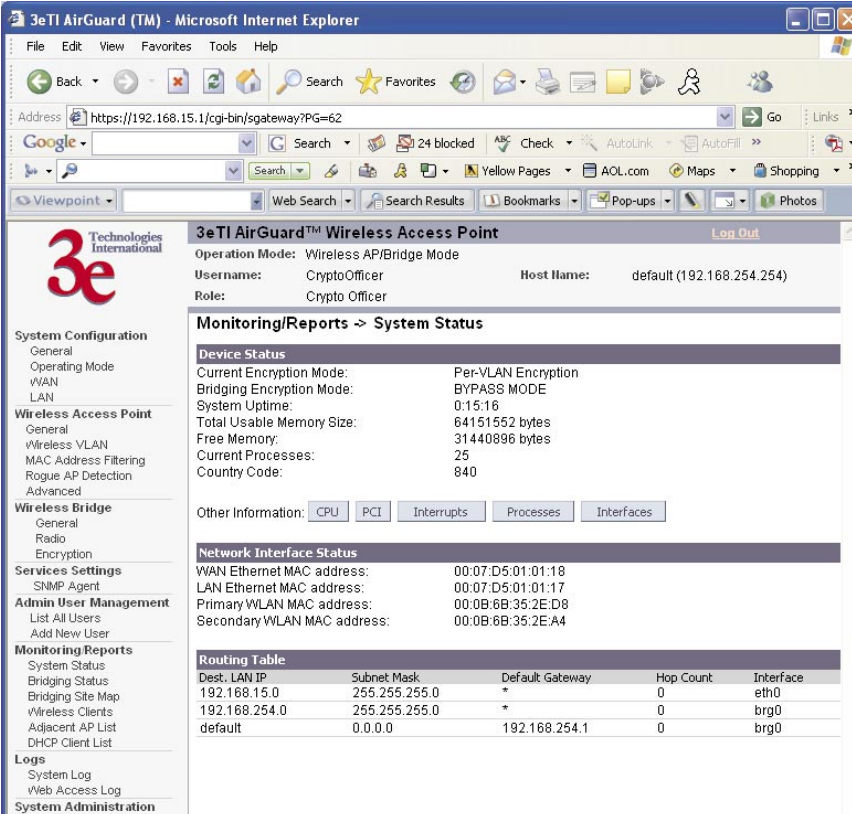


Monitoring/Reports

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

System Status

The **Monitoring/Report — System Status** screen displays the status of the 3e-525C-3 device, the network interface, and the routing table.



The screenshot shows the 3eTI AirGuard (TM) Web Management Interface in Microsoft Internet Explorer. The browser address bar shows the URL: `https://192.168.15.1/cgi-bin/sgateway?PG=62`. The page title is "3eTI AirGuard™ Wireless Access Point".

At the top, the page displays the following information:

- Operation Mode: Wireless AP/Bridge Mode
- Username: CryptoOfficer
- Host Name: default (192.168.254.254)
- Role: Crypto Officer

The main content area is titled "Monitoring/Reports -> System Status". It contains three sections:

Device Status

Current Encryption Mode:	Per-VLAN Encryption
Bridging Encryption Mode:	BYPASS MODE
System Uptime:	0:15:16
Total Usable Memory Size:	64151552 bytes
Free Memory:	31440896 bytes
Current Processes:	25
Country Code:	840

Other Information: [CPU](#) [PCI](#) [Interrupts](#) [Processes](#) [Interfaces](#)

Network Interface Status

WAN Ethernet MAC address:	00:07:D5:01:01:18
LAN Ethernet MAC address:	00:07:D5:01:01:17
Primary WLAN MAC address:	00:0B:6B:35:2E:D8
Secondary WLAN MAC address:	00:0B:6B:35:2E:A4

Routing Table

Dest. LAN IP	Subnet Mask	Default Gateway	Hop Count	Interface
192.168.15.0	255.255.255.0	*	0	eth0
192.168.254.0	255.255.255.0	*	0	brg0
default	0.0.0.0	192.168.254.1	0	brg0

The left sidebar contains a navigation menu with the following categories:

- System Configuration
 - General
 - Operating Mode
 - WAN
 - LAN
- Wireless Access Point
 - General
 - Wireless VLAN
 - MAC Address Filtering
 - Rogue AP Detection
 - Advanced
- Wireless Bridge
 - General
 - Radio
 - Encryption
- Services Settings
 - SNMP Agent
- Admin User Management
 - List All Users
 - Add New User
- Monitoring Reports
 - System Status
 - Bridging Status
 - Bridging Site Map
 - Wireless Clients
 - Adjacent AP List
 - DHCP Client List
- Logs
 - System Log
 - Web Access Log
- System Administration

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

Bridging Status

The **Monitoring/Report — Bridging Status** screen displays the Ethernet Port STP status, Ethernet DSL Port STP status, Wireless Port STP status, and Wireless Bridging information.

The screenshot shows the 3eTI AirGuard™ Wireless Access Point web interface in Microsoft Internet Explorer. The browser address bar shows `https://192.168.15.1/cgi-bin/sgateway?PG=64`. The page title is "3eTI AirGuard™ Wireless Access Point" and includes a "Log Out" link. The user is logged in as "CryptoOfficer" with the role "Crypto Officer".

The main content area is titled "Monitoring/Reports -> Bridging Status" and contains three sections:

- Ethernet Port STP Status**

Port Priority (hex):	50
Path Cost:	80
State:	forwarding
Designated Bridge:	0128.0007d5010118
- Wireless Port 0 STP Status**

Port Priority (hex):	50
Path Cost:	100
State:	forwarding
Designated Bridge:	0128.0007d5010118
- Wireless Bridging Information**

Bridge Priority(hex):	128
Bridge Hello Time:	2.00 sec
Bridge Forward Delay:	3.00 sec
Bridge Max Age:	20.00 sec
Bridge ID:	0128.0007d5010118
Designated Root:	0128.0007d5010118
Root Port:	0
Path Cost:	0
Hello Time:	2.00 sec
Forward Delay:	3.00 sec
Max Age:	20.00 sec
MAC Ageing Time:	300.00 sec
MAC Ageing Interval:	4.00 sec
Flags:	

The left sidebar contains a navigation menu with categories: System Configuration, Wireless Access Point, Wireless Bridge, Services Settings, Admin User Management, Monitoring Reports, Logs, and System Administration. The footer of the page reads: © 2000-2005 3e Technologies International. All rights reserved.

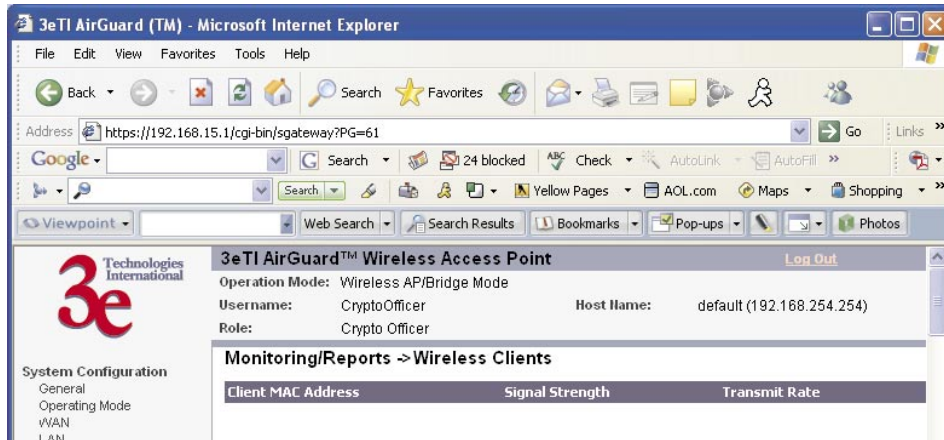
Bridge Site Map

The Bridge Site Map shows the spanning tree network topology of both wired and wireless nodes connected to the network. The root STP node is always on top and the nodes of the hierarchy are displayed below it. Wired links are double dotted lines and wireless links are single dotted lines. This map does not update dynamically. You must press the Update button to refresh the map.

The screenshot displays the web interface for a 3eTI AirGuard™ Wireless Access Point. The browser window title is "3eTI AirGuard (TM) - Microsoft Internet Explorer". The address bar shows "https://192.168.15.1/cgi-bin/sgateway?PG=691". The page title is "3eTI AirGuard™ Wireless Access Point" with a "Log Out" link. The main content area is titled "Monitoring/Reports -> Bridging Site Map" and includes an "Update" button and a legend: "Legend: Wired Link <==(interface)== Wireless Link <--(signal strength)--". A node information box shows: "BRG: 00:07:D5:01:01:18", "IP: 192.168.254.254", "Radio : 00:0B:6B:35:2E:A4", and "Desc: default location". Below this, it states "Last Update: Sat Jan 1 21:07:22 2005" and "Current Time: Sat Jan 1 21:07:26 2005". A warning message reads: "1 possible nodes in the network, missing nodes are shown in red. Duplicate IP nodes are shown in red." At the bottom, it says "To retrieve the missing nodes information Please click 'Retrieve' button" with a "Retrieve" button, and "Missing nodes information may be cached here" with a "Cached Nodes Info" button. The left sidebar contains a navigation menu with categories: System Configuration, Wireless Access Point, Wireless Bridge, Services Settings, Admin User Management, Monitoring Reports, and Logs.

Wireless Clients

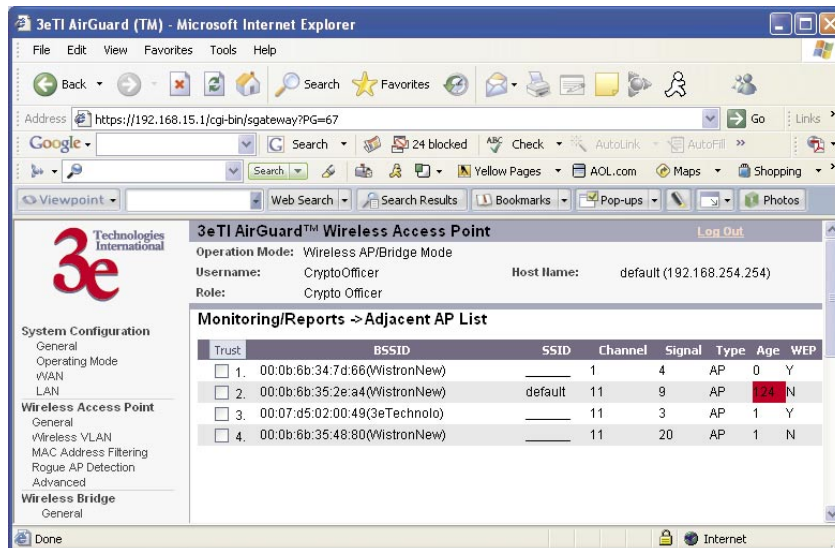
The **Monitoring/Report — Wireless Clients** screen displays the MAC Address of all wireless clients and their signal strength and transmit rate.



Adjacent AP List

The **Monitoring/Report — Adjacent AP List** screen shows all the APs on the network. If you select the check box next to any AP shown, the AP will thereafter be accepted by the 3e-525C-3 as a trusted AP.

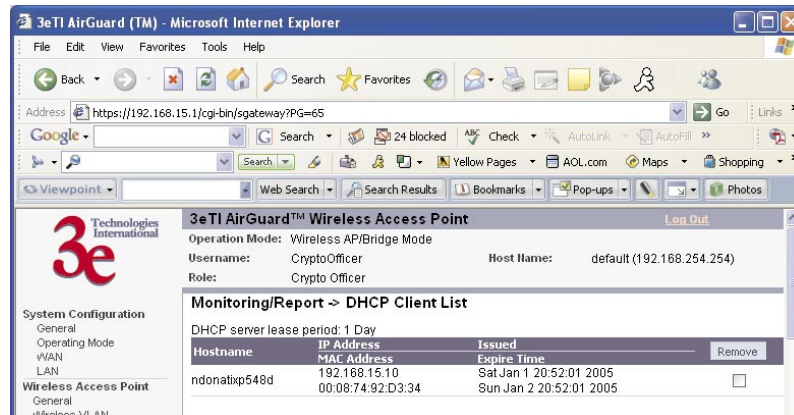
These APs are detected by the AP's wireless card and the wireless bridge's wireless card. The list of APs are only within the band that can be seen from a particular channel. For example, if the AP is on channel 1, it will display APs on channels 1-3.



DHCP Client List

The **Monitoring/Report — DHCP Client List** screen displays all clients currently connected to the 3e-525C-3 via DHCP server, including their hostnames, IP addresses, and MAC Addresses.

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



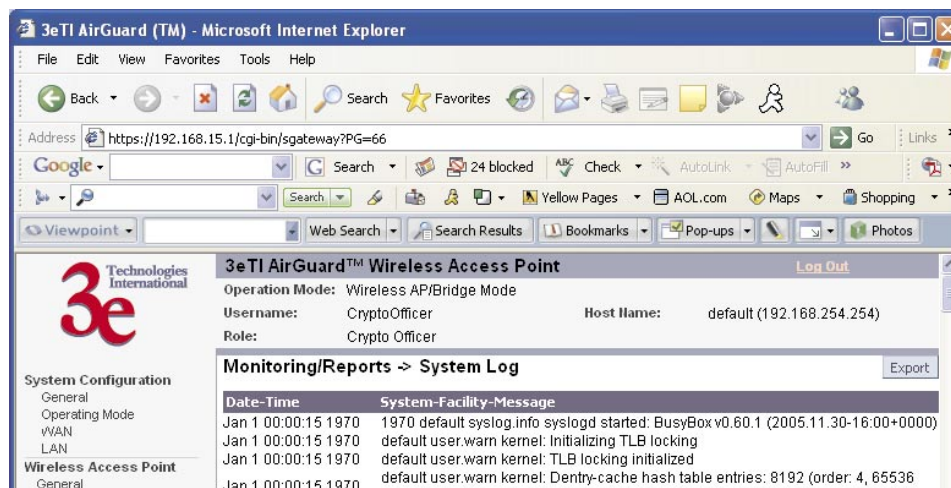
Logs

There are two logs available for viewing and exporting.

System Log

The **Logs — System Log** screen 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.

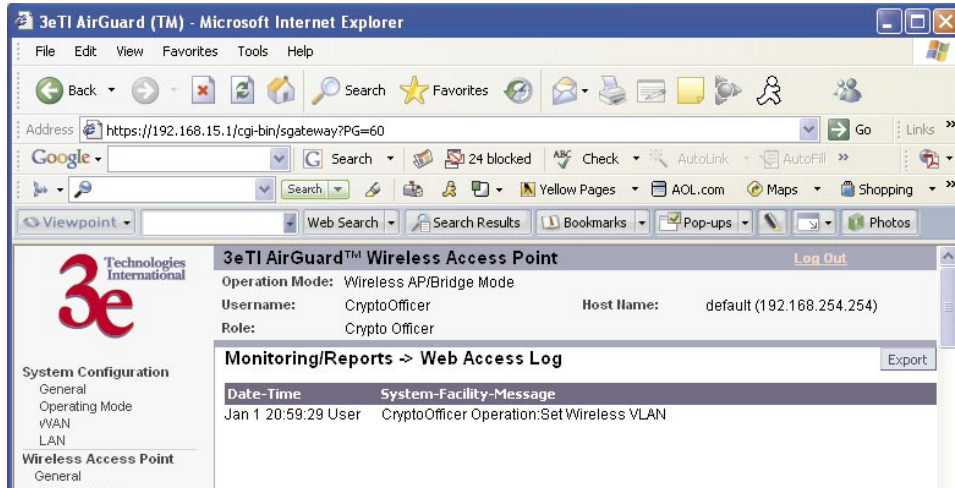
The System log continues to accumulate listings. If you wish you can export the log and save it as a file on your PC. Click on **Export**.



Web Access Log

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

The Web access log will continue to accumulate listings. If you wish you can export the log and save it as a file on your PC. Click on **Export**.



System Administration

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

System Upgrade

The **System Administration — System Upgrade** screen gives you the ability to upload updates to the 3e-525C-3 device's firmware as they become available. When a new upgrade file becomes available, you can do a firmware upgrade from the **Firmware Upgrade** window.

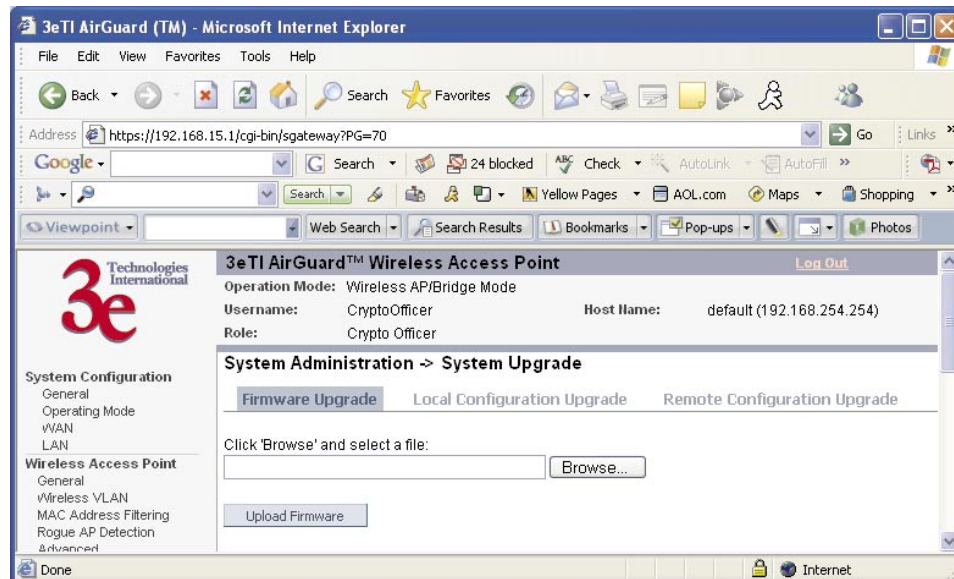
There is also a configuration file transfer option which allows the system configuration file from one AP to be transferred to another AP, in order to minimize the administration of the APs. Only configuration parameters that can be shared between APs are downloaded in the configuration file. WAN IP address and hostname are not transferred in the configuration file. Click on the **Local Configuration Upgrade** and **Remote Configuration Upgrade** tabs to perform file transfers.

Only the Crypto Officer role can access this function.

Firmware Upgrade

On the **System Administration — System Upgrade** screen, the Firmware Upgrade tab is the default view.

Click browse and select the firmware file to be uploaded. Click on the Upload Firmware button.

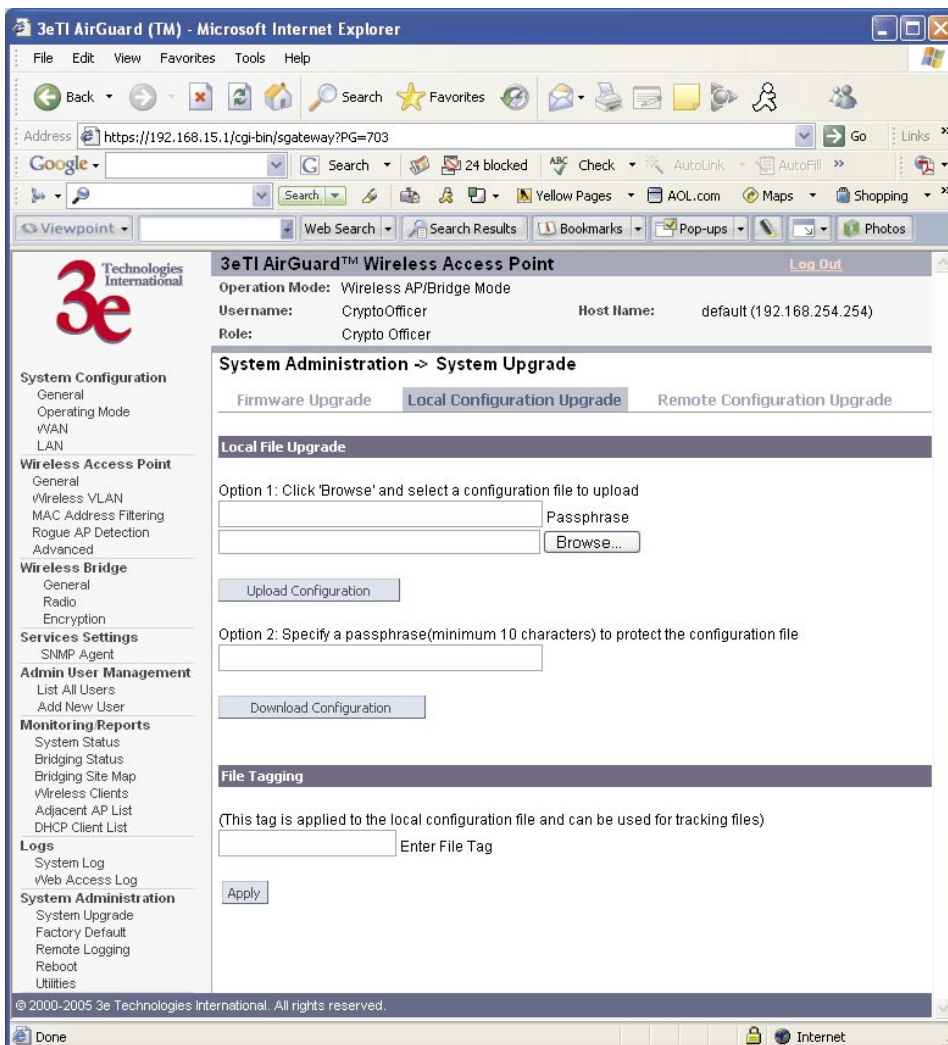


Local Configuration Upgrade

On the **System Administration — System Upgrade** screen, click on the **Local Configuration Upgrade** tab to upload and download configuration files to access points connected to the network.

To upload a configuration file, select the file using the browse button and enter the passphrase for that file. The passphrase protects the file from unauthorized users. It prevents unauthorized users from applying the system configuration file to an unauthorized AP to gain access to the network. Before downloading the system configuration file to a local computer, the user must enter a passphrase to protect the file. Before the system configuration file can be uploaded onto another AP, the passphrase must be entered on the remote AP.

The configuration file can be tagged with a 12 character tag to keep track of the configuration file as it is transferred to other APs.



Remote Configuration Upgrade

On the **System Administration — System Upgrade** screen, click on the **Remote Configuration Upgrade** tab to upload and download configuration files to access points in remote locations which are not configured.

This remote configuration upgrade feature allows you to selectively transfer a configuration file to other APs. Once the file is transferred, the remote AP will be rebooted. Once the remote units are rebooted, the site map can be updated and the File Tag will show the status of the units. If the tag matches the local tag, the unit was updated successfully.

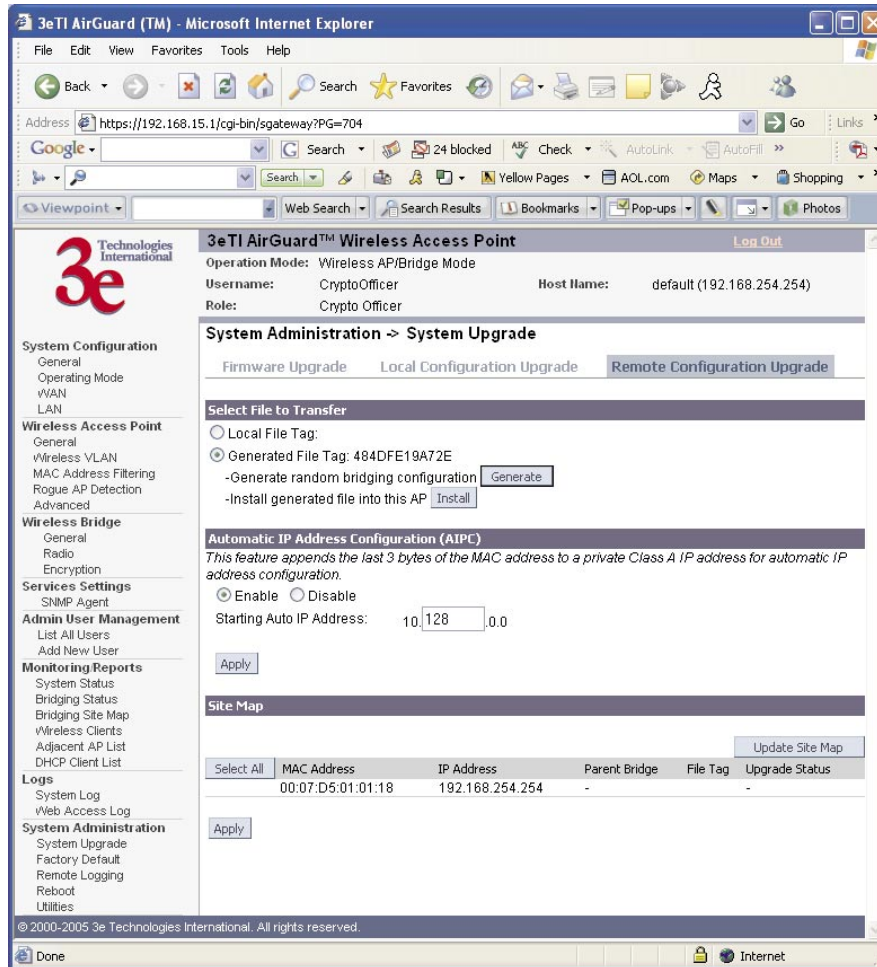
The screenshot shows the web interface of a 3eTI AirGuard™ Wireless Access Point. The browser window is titled "3eTI AirGuard (TM) - Microsoft Internet Explorer" and the address bar shows "https://192.168.15.1/cgi-bin/gateway?PG=704". The page title is "3eTI AirGuard™ Wireless Access Point" with a "Log Out" link. The main content area is titled "System Administration -> System Upgrade" and has three tabs: "Firmware Upgrade", "Local Configuration Upgrade", and "Remote Configuration Upgrade". The "Remote Configuration Upgrade" tab is active. Under "Select File to Transfer", there are radio buttons for "Local File Tag" (selected) and "Generated File: Not Available". Below this is a "Generate" button. The "Automatic IP Address Configuration (AIPC)" section is also visible, with "Enable" selected and a "Starting Auto IP Address" of 10.128.0.0. At the bottom, there is a "Site Map" table with columns for "Select All", "MAC Address", "IP Address", "Parent Bridge", "File Tag", and "Upgrade Status". The table contains one row with the following data:

Select All	MAC Address	IP Address	Parent Bridge	File Tag	Upgrade Status
	00:07:D5:01:01:18	192.168.254.254	-	-	-

The footer of the page shows "© 2000-2005 3e Technologies International. All rights reserved."

The random configuration file is used to update the bridging SSID and bridging encryption on other devices using the existing bridging link. If the bridging key or the bridging SSID is changed on the normal configuration screen, then the bridging link to the other devices will be terminated, and the configuration can not be updated.

To create a randomly generated bridging configuration file, click **Generate**. A new configuration is created in a temporary file and an **Install** button appears. In order to transfer this file, select the **Generated File** radio button, check the desired recipients in the Site Map section, and click **Apply**. After the file has been successfully transferred to the recipients (check the status field in the lower section), click **Install** to apply the randomly generated configuration file to the AP. Once applied, the unit will reboot and start using the new configuration file.



The automatic IP address configuration feature can be used to assign a remote device an IP address. This feature minimizes the effort to configure IP addresses in a wireless network. The IP addresses are assigned on the private class A IP address range (10.0.0.0). By default, this feature is enabled, so if you want to assign your own IP addresses you need to disable this feature.

You have the option to configure the second byte of the IP address to limit the range in which the IP addresses are distributed. For example, if your network already uses the 10.0.0.0 network address for other devices, you can limit the auto configuration to an upper range of 10.128.0.0 and the IP addresses will start from that number.

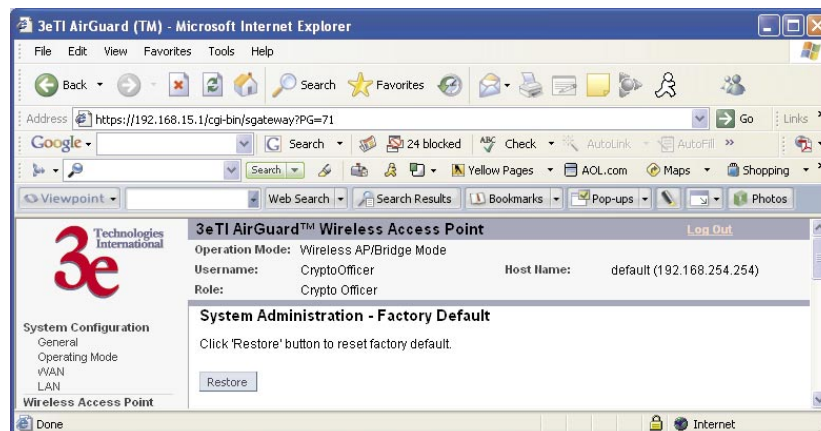
The automatic IP address configuration feature uses the last three bytes of the WAN MAC address for the last three bytes of the IP address. For example, the WAN MAC address of 00:07:D5:01:02:03 will translate to an IP address of 10.1.2.3. If the starting range of the automatic IP address configuration is set to 10.128.0.0 and the WAN MAC address is 00:07:D5:01:02:03, then the IP address is pushed to the upper range and becomes 10.129.2.3 (basically the second byte adds 128+1). The MAC addresses on the WAN port are from the 3eTI's address pool of 16 million addresses. There is a small chance for duplicate MACs. However, if a duplicate IP address is detected, the bridge site map will show this device with a red IP address. The distributed default gateway is the first IP address in the valid range. For example: for 10.128.0.0, the default gateway is 10.128.0.1. The distributed netmask is 255.0.0.0.

Factory Default

The **System Administration — Factory Default** screen is used to reset the AP to its factory settings.

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

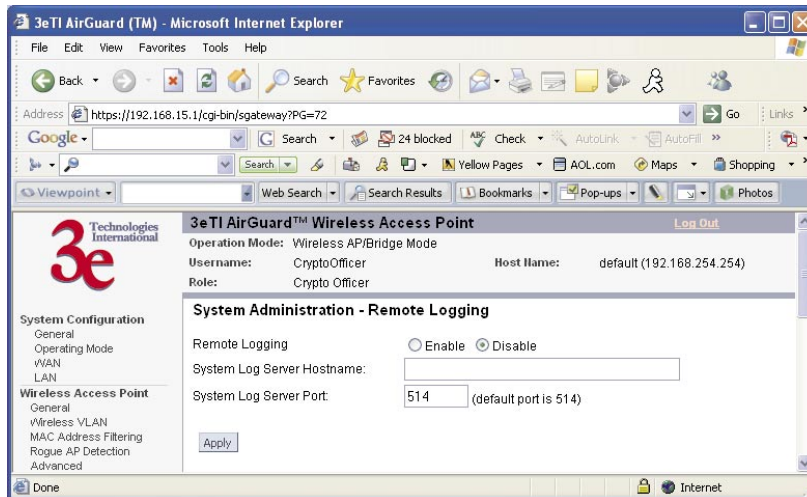
Only the Crypto Officer role has access to the **Restore** button.



You can also reset the 3e-525C-3 to its factory default by pressing and holding the reset button located on the front of the unit for 10 seconds. Input is acknowledged by the WLANNSS LED turning on and then turning off after 10 seconds.

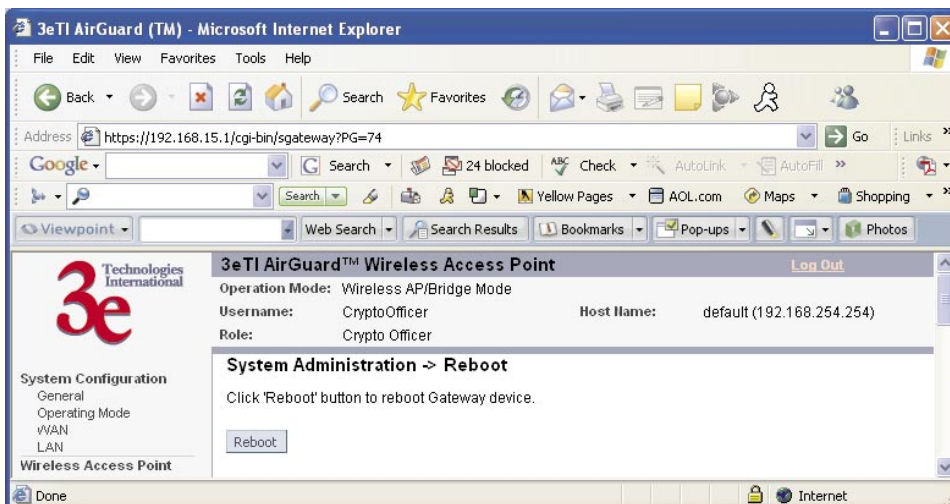
Remote Logging

The **System Administration — Remote Logging** screen allows you to forward the syslog data from each machine to a central remote logging server. In the 3e-525C-3, this function uses the **syslogd** daemon. If you enable Remote Logging, input a System Log Server IP Address and System Log Server Port. Click **Apply** to accept these values.



Reboot

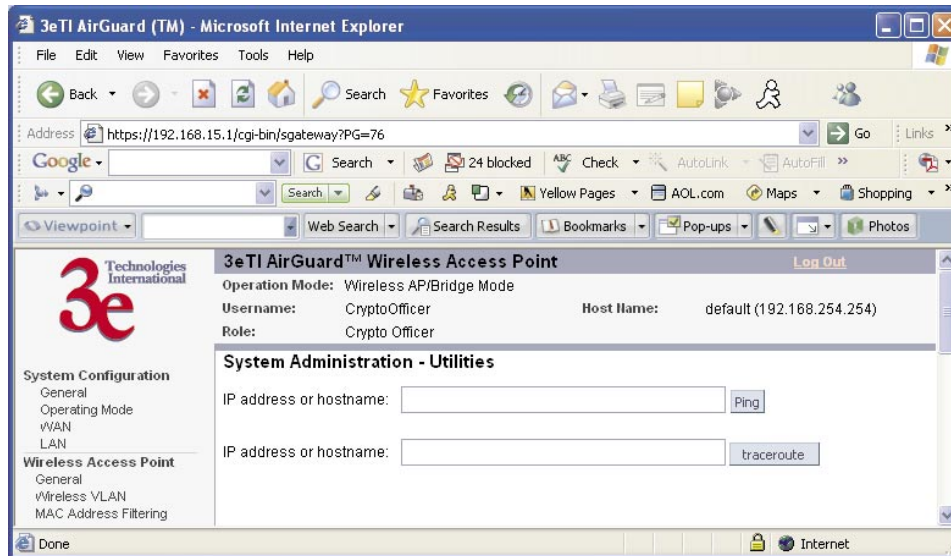
The **System Administration — Reboot** screen allows you to reboot the 3e-525C-3 without changing any preset functionality. Both Crypto Officer and Administrator functions have access to this function.



You can also reboot the 3e-525C-3 by pressing and holding the reset button on the front of the unit for five seconds. Input is acknowledged by the LWLANSS LED turning on.

Utilities

The **System Administration — Utilities** 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

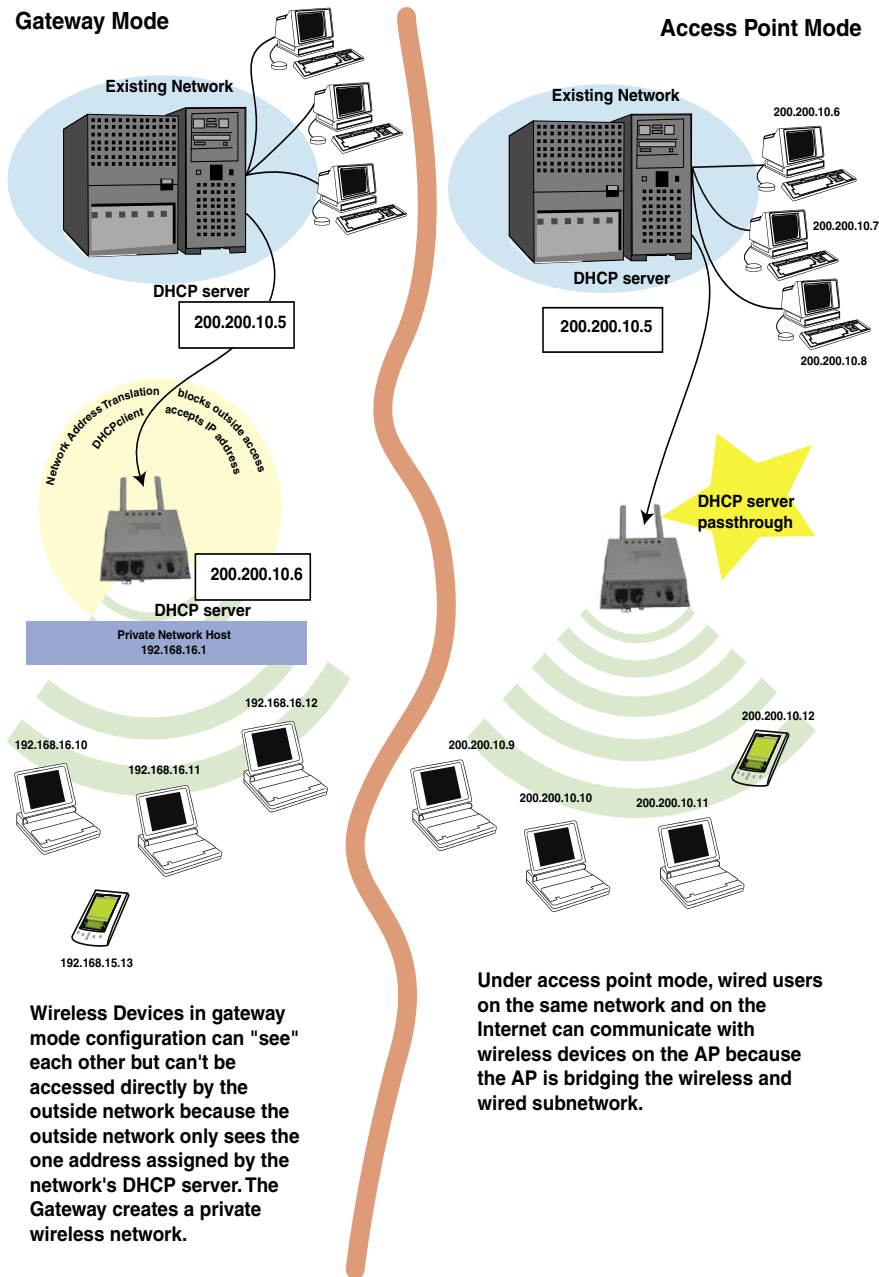
Chapter 3 covered the default configuration of the 3e-525C-3 Wireless Access Point as an access point, for use as part of a host wired network. This chapter covers configuration as a gateway.

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.

The illustration on the following page shows the difference between AP mode and Gateway mode.

Caution: If you have previously set up your WLAN using the 3e-525C-3 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-525C-3 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-525C-3



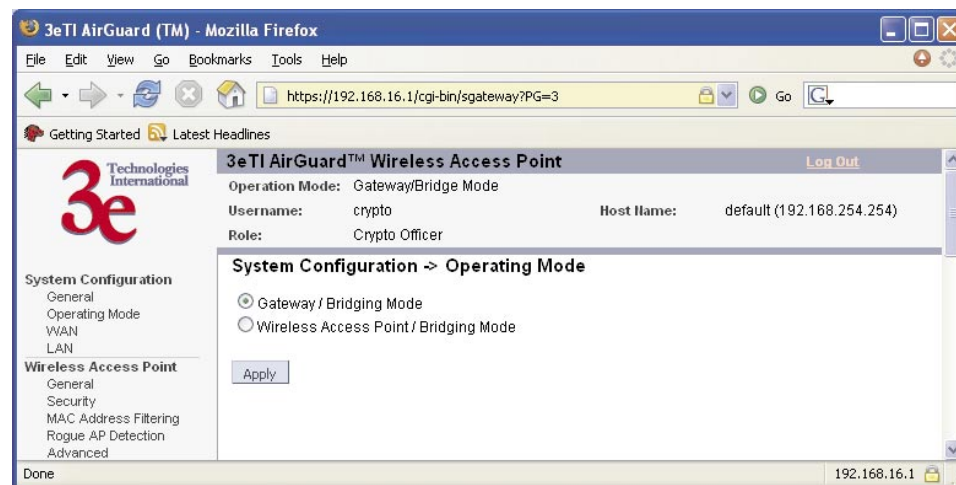
Configuring in Gateway Mode

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

1. Log in to the 3e-525C-3 (see Chapter 3, page 25).
2. Using the navigation bar to the left, navigate to the **System Configuration — Operating Mode** screen, select the **Gateway/Bridging Mode** radio button, and click **Apply**. The 3e-525C-3 AP will reboot in gateway mode.

NOTE: After the unit reboots, you will need to enter the default subnet of the IP LAN address, **https://192.168.16.1**. Now you can log on to the 3e-525C-3 in gateway mode.

Also note that if you change modes from AP to Gateway, your configuration is not lost. However, if you switch from FIPS 140-2 submode to non-FIPS, all previously entered information will be reset to factory settings.



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.

This chapter only covers the functions and screens that are unique to gateway mode. All the screens that are common to both the AP and Gateway modes are covered in Chapter 3.

WAN

In Gateway mode, the System Configuration–WAN screen has two tabs: Main IP Setting and IP Aliasing.

Main IP Setting

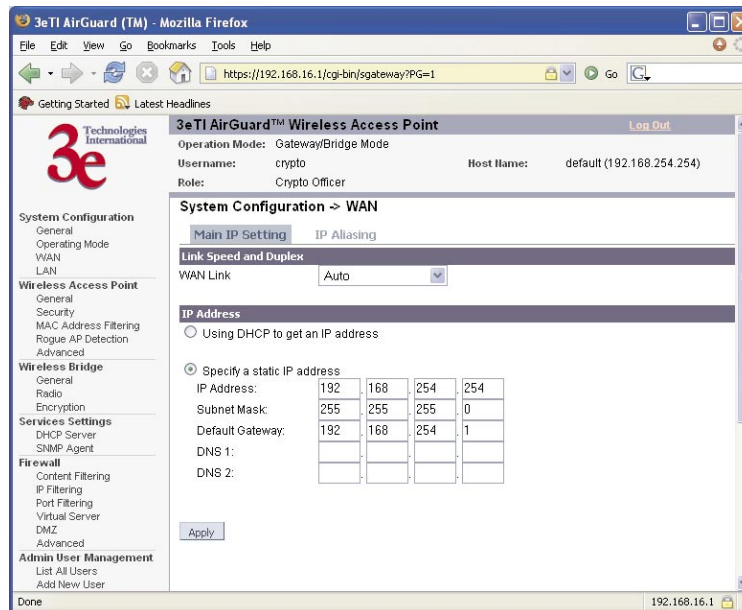
The Main IP Setting screen allows you to set Link Speed and Duplex of the WAN port. If you select a choice other than Auto (the default), the 3e-525C-3 will use only the selected link speed (10 Mbits/sec or 100 Mbits/sec) and Duplex (Half Duplex transfers or Full Duplex transfers) that you select in the WAN/LAN Link drop-down 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 network, which is to be outside the “protected” wireless LAN. Normally, you will be provided with the IP address, Subnet Mask, Default Gateway and DNS to assign by the Network Administrator for the Ethernet Network.

There are two ways to configure the WAN IP address:

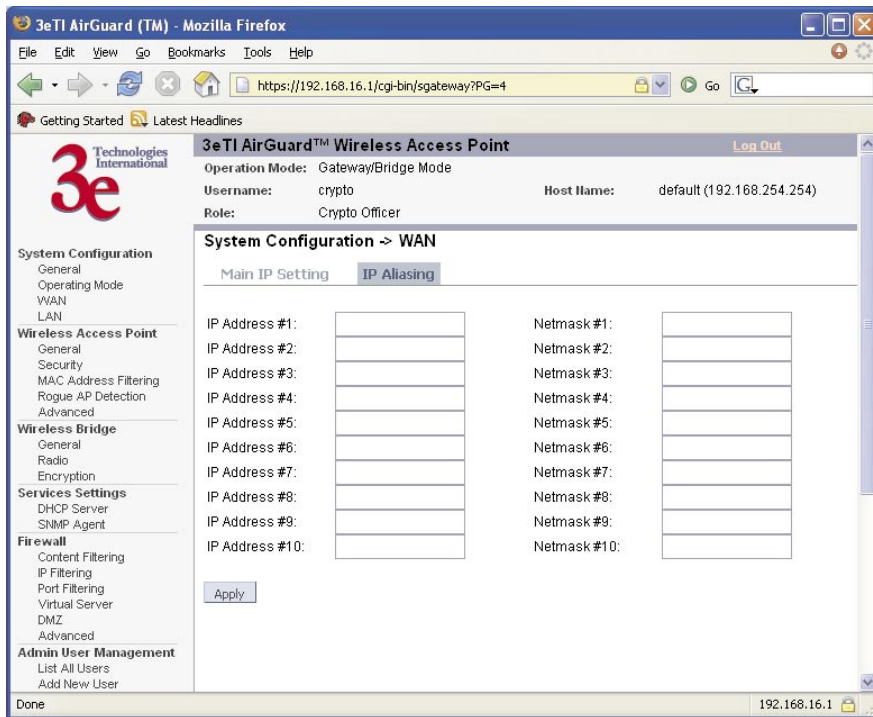
1. **Obtain an IP address Automatically** – This configuration allows the Ethernet network to use the DHCP server on the wired network to dynamically assign the WAN IP address to the DHCP client in the gateway.
2. **Specify an IP address** – This configuration allows the user to manually type in a static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



IP Aliasing

You can add up to ten additional IP aliases on the WAN port.

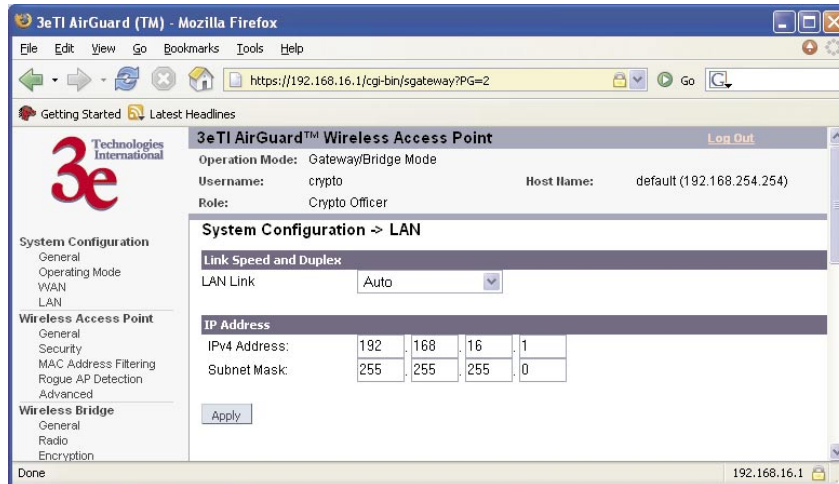
The IP aliasing entries can be used by the virtual server to map a public IP address to a private IP address. If the virtual server needs to map multiple public IP addresses to multiple private IP addresses, the IP aliasing entries can be used to create additional public IP addresses. These entries are always static entries and can not use DHCP.



LAN

Click the entry on the left-hand navigation panel for **System Configuration—LAN**. This directs you to the **System Configuration—LAN** screen.

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



Security

Click the entry on the left hand navigation panel for **Wireless Access Point — Security**. This directs you to the **Wireless Access Point — Security** screen.

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

Gateway mode has the same encryption options as the AP mode.

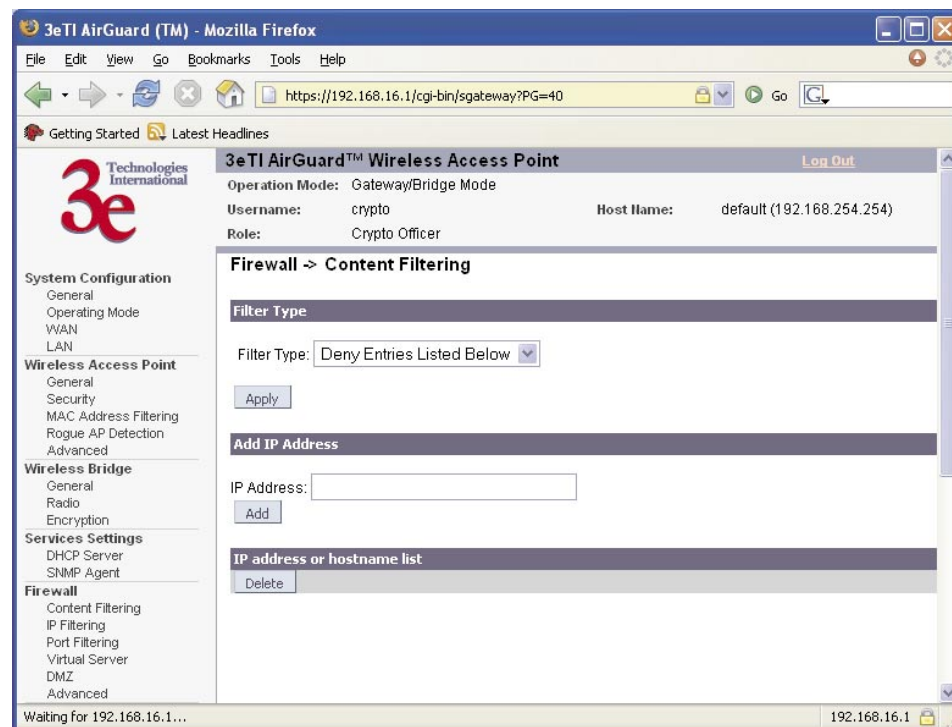
Firewall

Content Filtering

Click the entry on the left hand navigation panel for **Firewall — Content Filtering**. The **Content Filtering** screen 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**.

Entries can be added as:

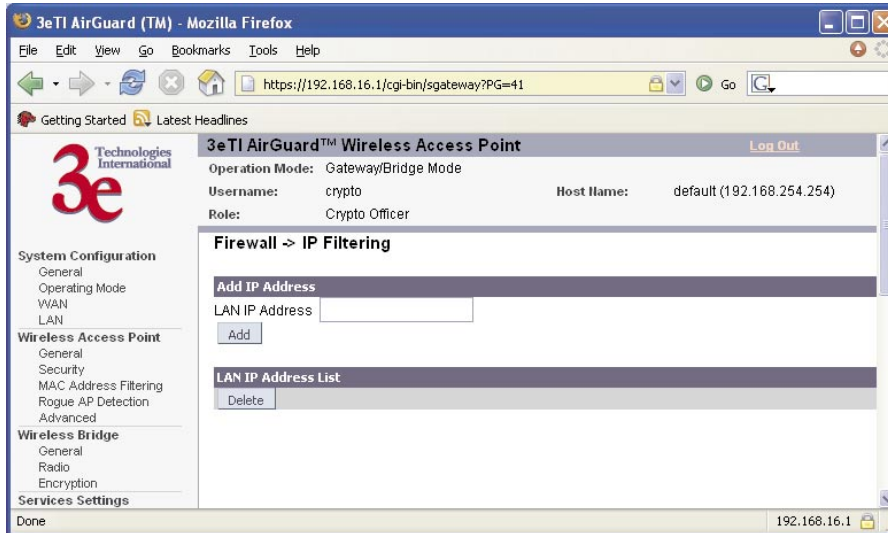
- Individual IP addresses (192.168.204.10)
- IP address range (192.168.204.0/24)
- Exact URL (www.yahoo.com)
- Wildcard URL (*.gov)



IP Filtering

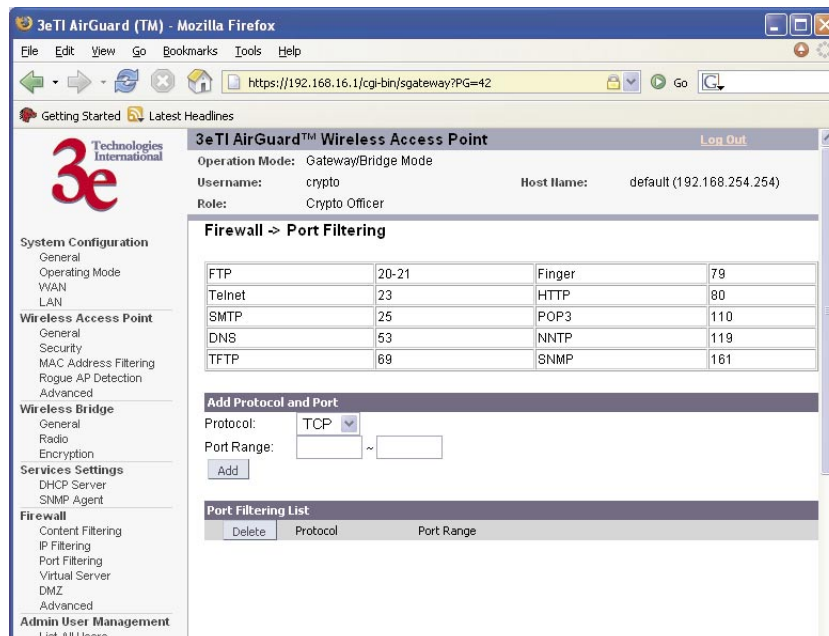
Click the entry on the left hand navigation panel for **Firewall — IP Filtering**.

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



Port Filtering

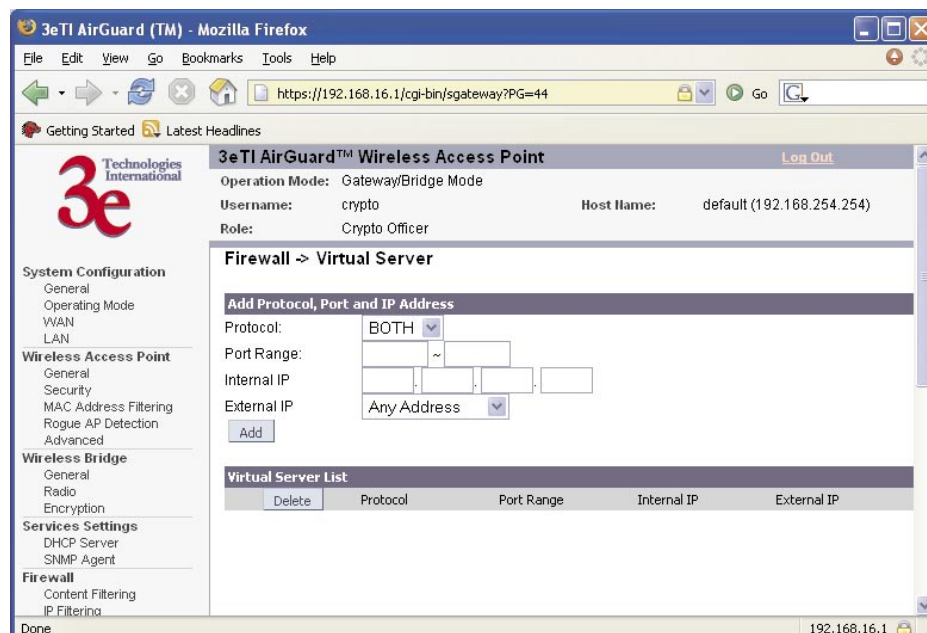
Click the entry on the left hand navigation panel for **Firewall — Port Filtering**. Port filtering permits you to configure the Gateway to block outbound traffic on specific ports. It can be used to block the wireless network from using specific protocols on the network.



Virtual Server

Click the entry on the left hand navigation panel for **Firewall — 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

It is 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.

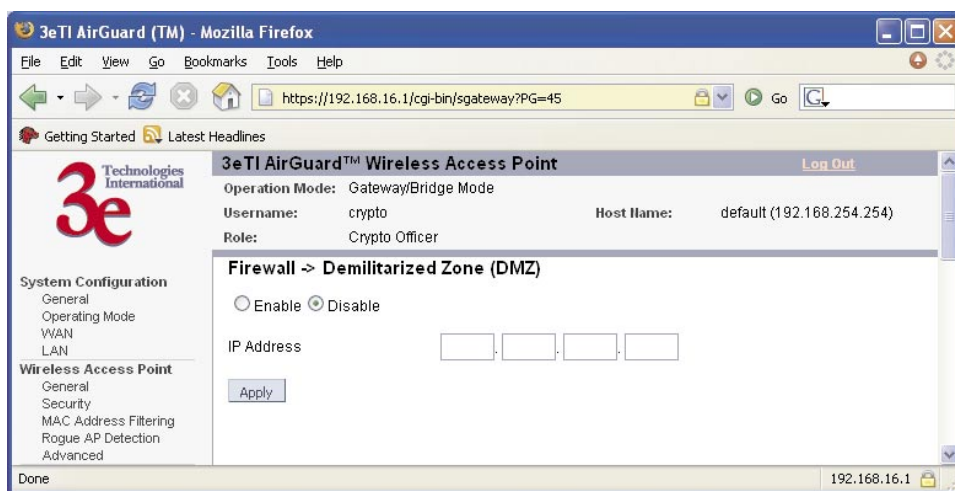
Protocol – Selection of either **UDP**, **TCP**, or **Both** (TCP and UDP) allows these specified network protocols to pass through during the TCP port communication with each virtual server IP address.

Demilitarized Zone (DMZ)

Click the entry on the left hand navigation panel for **Firewall** — **DMZ**.

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

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



Advanced Firewall

As advanced firewall functions, you can enable/disable

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

These options allow you more control over your environment.



This page intentionally left blank.

Chapter 5: Wireless Bridge Configuration

Introduction

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

The wireless bridging function in the 3e-525C-3 supports a number of bridging configurations. Some of the most popular settings are discussed in this chapter:

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

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

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

If setting up as a bridge during initial setup, you can either use the LAN Port directly wired by Ethernet cable to a laptop to set the appropriate settings. The management screens that you may need to modify, regardless of what type of bridging mode you choose, will be in the **Wireless Bridge** section of the navigation bar. These include:

- **Wireless Bridge — General**
- **Wireless Bridge — Radio**
- **Wireless Bridge — Encryption**

Wireless Bridge — General

The **Wireless Bridge — General** screen contains wireless bridging information. This page is important in setting up your bridge configuration. Wireless bridging supports two modes of operation:

- Manual wireless bridging
- Auto-forming wireless bridging (AWB) - with a maximum number of allowable bridges (the default is 40)

Auto-forming Wireless Bridging

When the wireless bridge is in auto-forming mode, the wireless bridge sniffs for beacons from other wireless bridges and identifies APs that match a policy such as SSID and channel.

Instead of simply adding the APs with the same SSID/channel to the network, a three-way association handshake is performed in order to control network access.

To make a unit the root (leaf) STP node, set the bridge priority lower than any other node in the network.

3eTI AirGuard™ Wireless Access Point

Operation Mode: Wireless AP/Bridge Mode
 Username: CryptoOfficer Host Name: default (192.168.254.254)
 Role: Crypto Officer

Wireless Bridge -> General Monitoring

Bridging Mode: Manual Bridging Auto Bridging

SSID:

Max Auto Bridges: (1-40)

Bridge Priority: (1-40)

Signal Strength Threshold:

Broadcast SSID:

Signal Strength MAC:

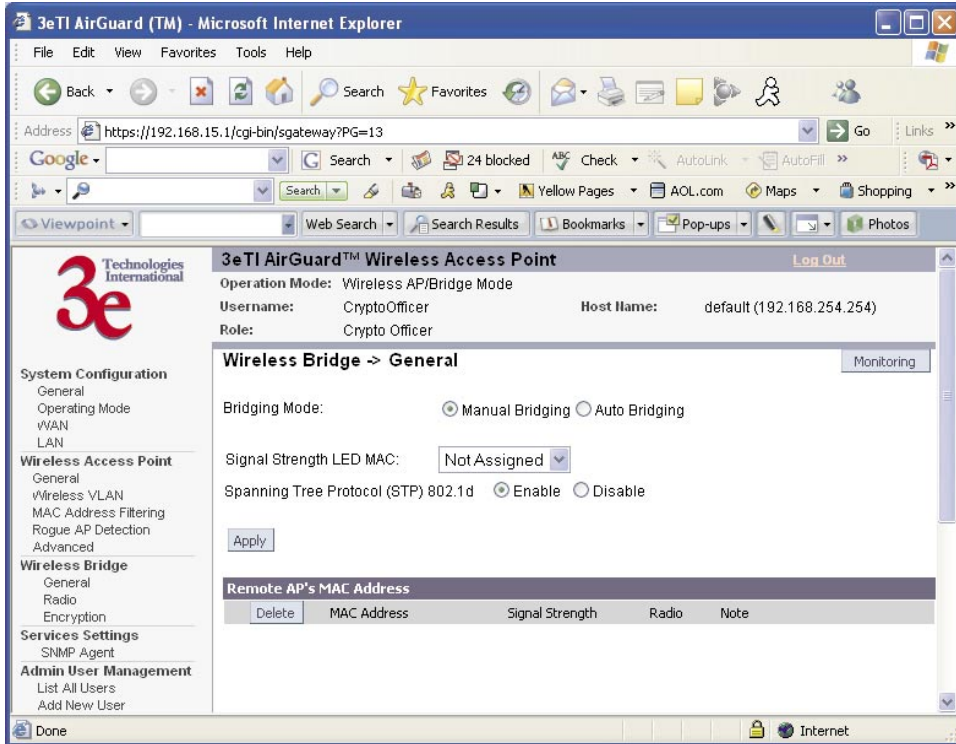
Remote AP's MAC Address

Index	BSSID	Signal Strength	Link Status	Description

AUTO BRIDGING GENERAL SETTINGS OPTIONS		
Bridging Mode	Auto Bridging	auto bridging selected
SSID	numbers or letters	Can be any set of letters and numbers assigned by the network administrator. This nomenclature has to be set on the wireless bridge and each wireless device in order for them to communicate.
Max Auto Bridges	1-40	Maximum number of auto bridges allowed.
Bridge Priority	1-40	Determines the root (leaf) STP node. The lowest bridge priority in the network will become the STP root.
Signal Strength Threshold	27% 21% 15% 9%	Prevents the node under the threshold from associating and joining the network.
Broadcast SSID	Diabile/Enable	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 bridge doesn't send probe responses to probe requests with unspecified SSIDs.
Signal Strength MAC		The signal strength of this wireless bridge will be indicated on the Signal Strength LED located on the front of the case.

Manual Bridging

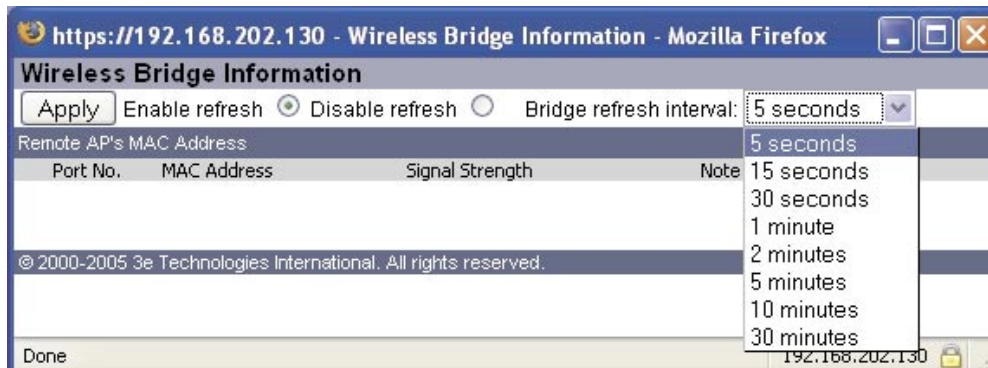
When the wireless bridge is in manual bridging mode, you can manually select a signal strength LED MAC and enable or disable spanning tree protocol. You can also delete remote AP's MAC addresses.



MANUAL BRIDGING GENERAL SETTINGS OPTIONS		
Bridging Mode	Manual Bridging	manual bridging selected
Signal Strength LED MAC	Not Assigned	Allows you to set the number of one of the Remote APs which will be listed at the bottom of the screen once the system is operational This wireless bridge becomes the guiding port that is displayed in the WLANNSS LED on the front of the 3e-525C-3 as a signal.
Spanning Tree Protocol (STP)	Enable/Disable	Enable STP is 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, then disable STP. The bridge will be more efficient (faster) without it. If you are not sure, the safest solution is to enable STP.

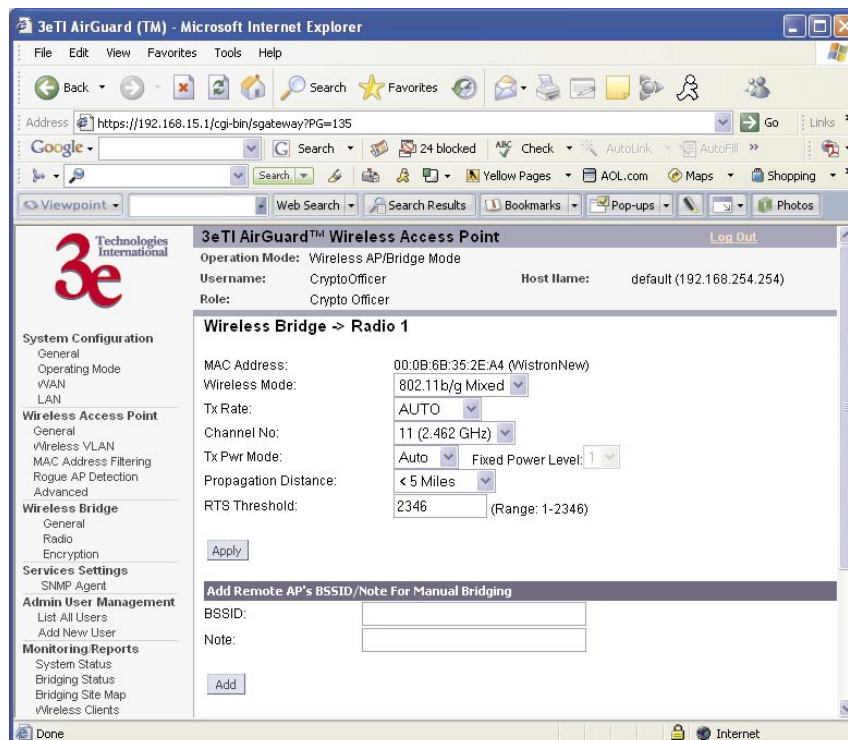
Monitoring

In the upper right-hand corner of the **Wireless Bridge — General** screen there is a button called Monitoring. If you click on this button, a pop-up window will appear (Wireless Bridge Information). If you select Enable refresh, you can set the bridge refresh interval from 5 seconds to 30 minutes. Refreshing the screen allows you to see the effect of aiming the antenna to improve signal strength.



Wireless Bridge — Radio

The **Wireless Bridge — Radio** screen contains wireless bridging information including the channel number, Tx rate, Tx power, spanning tree protocol (802.1d) enable/disable, and remote AP's BSSID. This page is important in setting up your bridge configuration.

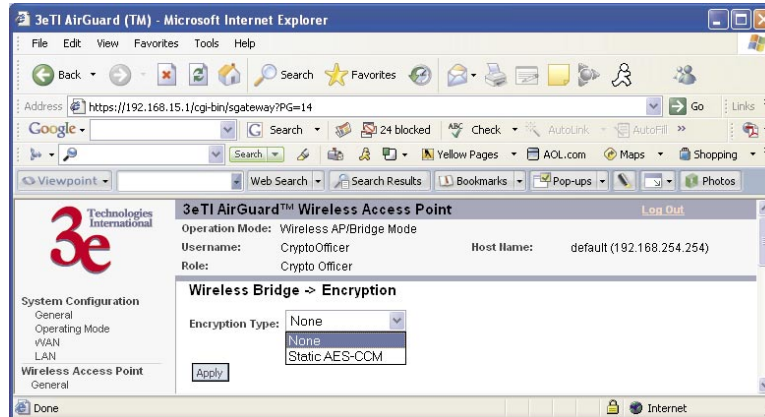


Radio Settings		
Wireless Mode	802.11b/g Mixed 802.11g Super 802.11a 802.11a Turbo	Sets the wireless mode for the wireless bridge.
Tx Rate	802.11b/g Mixed	
	AUTO, 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54 Mbps	When set to AUTO, the card attempts to select the optimal rate for the channel. If a fixed rate is used, the card will only transmit at that rate.
	802.11g Super	
	AUTO	The card attempts to select the optimal rate for the channel.
	802.11a	
	AUTO, 6, 9, 12, 18, 24, 36, 48, 54 Mbps	When set to AUTO, the card attempts to select the optimal rate for the channel. If a fixed rate is used, the card will only transmit at that rate.
	802.11a Turbo	
AUTO	The card attempts to select the optimal rate for the channel.	
Channel No.	802.11b/g Mixed	
	1 (2.412 GHz) 2 (2.417 GHz) 3 (2.422 GHz) 4 (2.427 GHz) 5 (2.432 GHz) 6 (2.437 GHz) 7 (2.442 GHz) 8 (2.447 GHz) 9 (2.452 GHz) 10 (2.457 GHz) 11 (2.462 GHz)	Sets the channel frequency for the wireless bridge.
	802.11g Super	
	6 (2.437 GHz)	Sets the channel frequency for the wireless bridge.
	802.11a	
	52 (5.26 GHz) 56 (5.28 GHz) 60 (5.30 GHz) 64 (5.32 GHz) 149 (5.745 GHz) 153 (5.765 GHz) 157 (5.785 GHz) 161 (5.805 GHz) 165 (5.825 GHz)	Sets the channel frequency for the wireless bridge.
	802.11a Turbo	
50 (5.25 GHz) Turbo Mode 58 (5.29 GHz) Turbo Mode 152 (5.76 GHz) Turbo Mode 160 (5.80 GHz) Turbo Mode	Sets the channel frequency for the wireless bridge.	

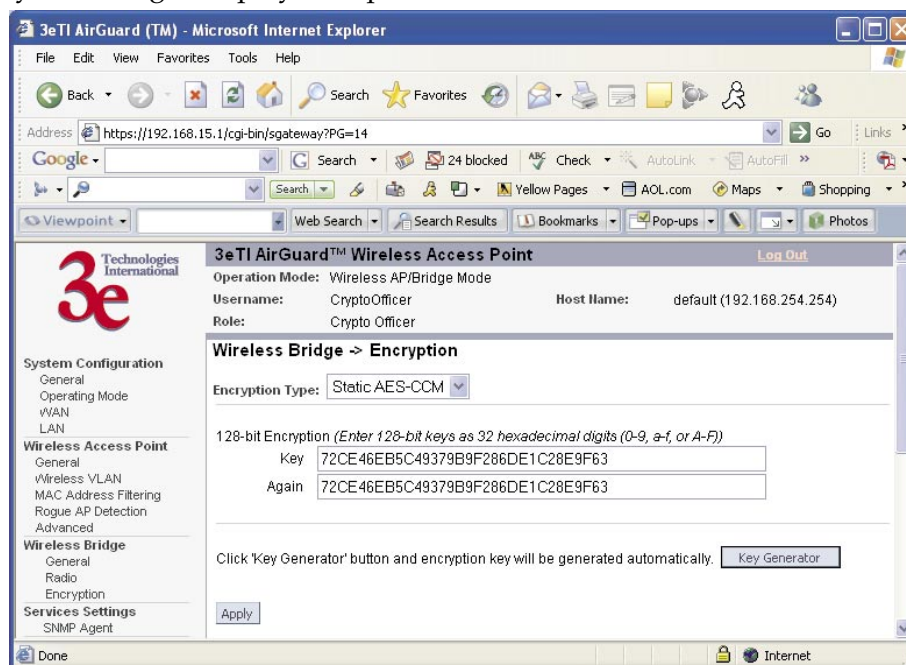
Tx Pwr Mode	OFF FIXED, AUTO	The Tx Pwr Mode defaults to AUTO, giving the largest range of radio transmission available under ambient conditions. The wireless bridge's broadcast range can be limited by setting the Tx Pwr Mode to Fixed and choosing from 1-5 for Fixed Pwr Level. If you want to prevent any radio frequency transmission from the wireless bridge, set the Tx Pwr Mode to OFF. This will not turn off RF transmissions from any associated wireless devices, but they will not be able to communicate with the wireless bridge when the Tx Pwr Mode is off.
Fixed Pwr Level	1, 2, 3, 4, 5	Select a range when Rx Pwr Mode is set to FIXED. Level 1 is the shortest distance (Level 1=7dBm) and Level 5 is the longest (Level 5=15dBm)
Propagation Distance	< 5 Miles 5-10 Miles 11-15 Miles 16-20 Miles 21-25 Miles 26-30 Miles > 30 Miles	Set the distance based on the distance between this bridge and furthest bridge that is connected to it.
RTS Threshold	Range 1-2346	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.
BSSID	Enter hexadecimal numbers	Add the MAC address of the remote bridge. The remote bridge's MAC address will appear at the bottom of the screen.
Note		You can enter a note that defines the location of the remote bridge.

Wireless Bridge — Encryption

The **Wireless Bridge — Encryption** screen 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. On this screen you can select None or AES-CCM.

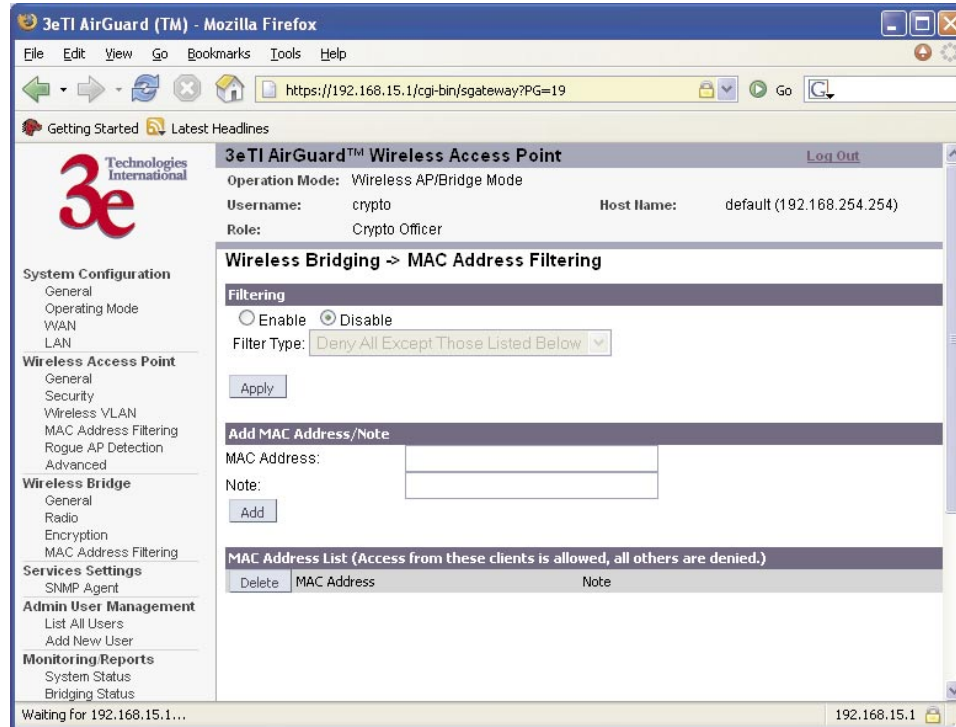


If you select AES-CCM, enter a 128-bit key as 32 hexadecimal digits or use the Key Generator button to automatically generate a randomized key of the appropriate length. This key is initially shown in plain text so you have the opportunity to copy the key. Once the key is applied, the key is no longer displayed in plain text.



Wireless Bridge — MAC Address Filtering

The **Wireless Bridge — MAC Address Filtering** screen functions just like the AP MAC Address Filter (see page 38) but it is only used in auto bridging mode and only controls access to the wireless bridge network.

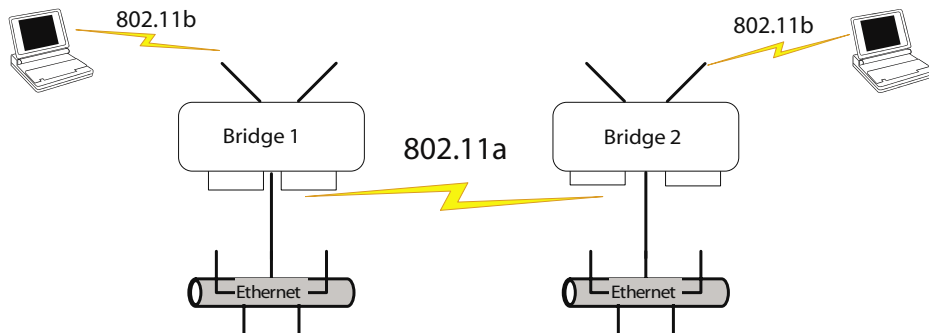


The following sections describe the setup for three types of bridging configuration: point-to-point, point-to-multipoint, or, lastly, repeater.

Setting Up Bridging Type

Point-to-Point Bridge Configuration

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



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

For instance, the bridges must have the same channel number. Because there is a separate WLAN card for bridging, there can be a separate WLAN on the AP WLAN card with no loss efficiency, as long as you set the channel numbers so there's no conflict or noise with the channel assigned to the bridge. Spanning Tree Protocol may be set to Enable, if there is any possibility of a bridging loop, or to Disable (which is more efficient) if there's no possibility of a bridging loop. Each bridge must contain the other's BSSID. (The BSSID of each is equivalent to the MAC address contained on the **Wireless Bridge — Radio** setup page. Enter only hexadecimal numbers, no colons. Data entry is not case sensitive.) Finally, the wireless bridging encryption must be set to the appropriate type and key length and must be identical on each bridge.

The following charts show sample settings for manual bridging and auto bridging modes.

Point-to-Point Bridging Setup Guide - Manual Mode

Direction	Bridge 1	Bridge 2
Wireless Bridge — General (Manual Bridging Mode)		
Bridging Mode	manual bridging selected	manual bridging selected
Signal Strength LED MAC	Not Assigned (select from drop-down list)	Not Assigned (select from drop-down list)
Spanning Tree Protocol (STP)	Enable (or Disable if no bridging loop possible)	Enable (or Disable if no bridging loop possible)
Wireless Bridge — Radio		
Wireless Mode	802.11a	802.11a
Tx Rate	AUTO	AUTO
Channel No.	Must be the same as Bridge 2	Must be the same as Bridge 1
Tx Power Mode	Auto	Auto
Propagation Distance	< 5 Miles	< 5 Miles
RTS Threshold	2346	2346
BSSID	Add Bridge 2 MAC	Add Bridge 1 MAC
Wireless Bridge — Encryption		
Bridging encryption options	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.

Point-to-Point Bridging Setup Guide - Auto Mode

Direction	Bridge 1	Bridge 2
Wireless Bridge — General (Auto Bridging Mode)		
Bridging Mode	Auto bridging selected	Auto bridging selected
SSID	Must be the same as Bridge 2	Must be the same as Bridge 1
Max Auto Bridges	40 (range 1-40)	40 (range 1-40)
Bridge Priority	40 (range 1-40)	40 (range 1-40)
Signal Strength Threshold	9%	9%
BroadcastSSID	Disable	Disable
Signal Strength MAC	Enter from list at the bottom of the screen	Enter from list at the bottom of the screen
Wireless Bridge — Radio		
Wireless Mode	802.11a	802.11a
Tx Rate	AUTO	AUTO
Channel No.	Must be the same as Bridge 2	Must be the same as Bridge 1
Tx Power Mode	Auto	Auto
Propagation Distance	< 5 Miles	< 5 Miles
RTS Threshold	2346	2346
Wireless Bridge — Encryption		
Bridging encryption options	Select appropriate key type/length and value. Must be same as Bridge 2.	Select appropriate key type/length and value. Must be same as Bridge 1.
Wireless Bridge — MAC Address Filtering		
Filtering	Enable/Disable	Enable/Disable
Filter Type	Deny All/Allow All	Deny All/Allow All
MAC Address	Add MAC address of bridges	Add MAC address of bridges

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

Navigate to the **Wireless Bridge — Radio** screen.

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

Select the **Wireless Mode** to be used for bridging. Set the **Tx Rate** to a fixed transmit rate or select AUTO if you want the card to attempt to select the optimal rate for the channel. If the Tx rate is set to a fixed rate, then the card will only transmit at that rate.

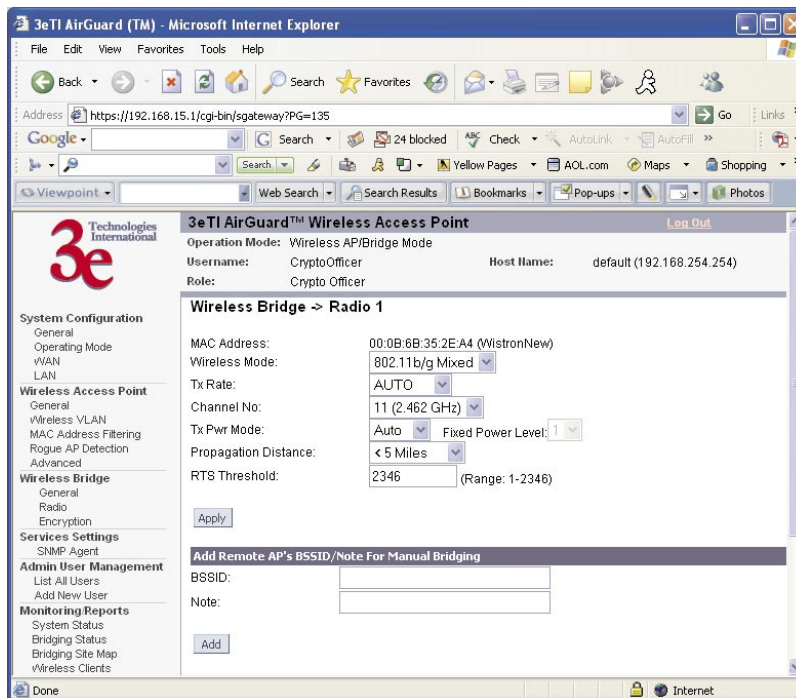
Next select the **Channel Number**. The **Channel Number** must be set to the same frequency in order for each bridge to communicate. **TX Pwr Mode** can be left on **Auto** unless the power needs to be regulated.

Select the **Propagation Distance** which is based on the distance between a bridge and the furthest bridge that is connected to it.

Set the **RTS Threshold** which is 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.

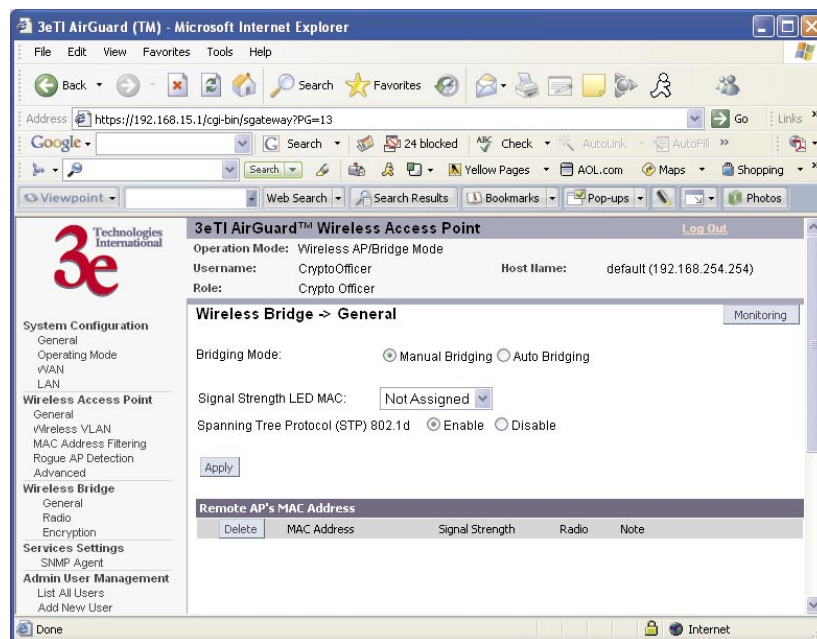
Click **Apply** to accept your changes but stay on this screen.

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 at the bottom of the **Wireless Bridge — General** screen.



Next go to the **Wireless Bridge — General** screen. Select either manual or auto bridging. If you choose **Manual Bridging** then you will have to set **Spanning Tree Protocol** to **Enable** unless you are sure that there is no chance of a loop. You can also assign a **Signal Strength LED MAC**. **Signal strength LED MAC** allows you to set the number of one of the Remote APs which will be listed at the bottom of the screen once the system is operational as the guiding port that you wish to have display in the WLANSS LED on the front of the 3e-525C-3 as a signal. If you don't wish to display any connection signal, simply leave this set at Not Assigned. From this screen you can also choose to delete a remote AP's MAC address.

Click **Apply** to accept your changes.



If you choose **Auto Bridging** mode, then you will need to enter the following information:

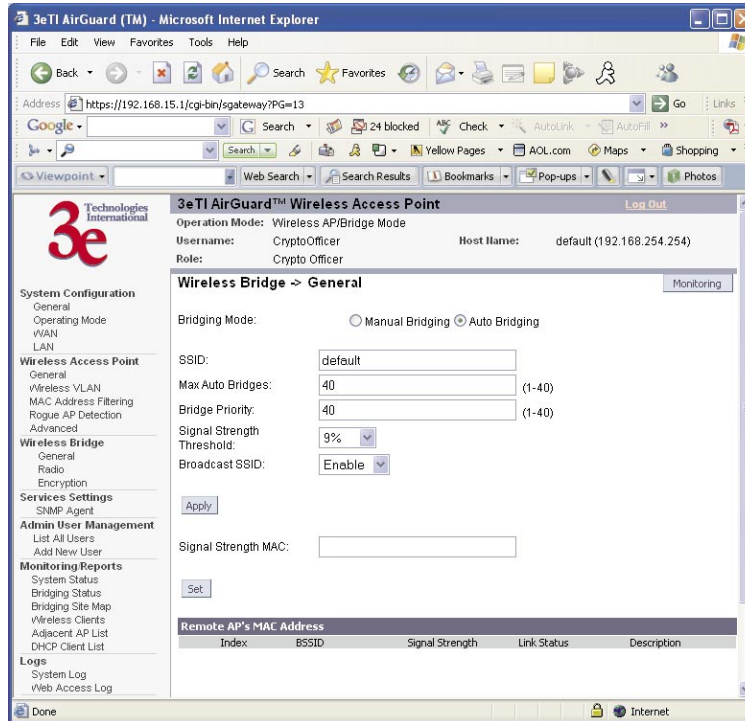
Enter the **SSID**. This can be any set of letters and numbers assigned by the network administrator. This nomenclature has to be set on the wireless bridge and each wireless device in order for them to communicate.

Enter a number from 1 to 40 for the **Max Auto Bridges**. Next enter the **Bridge Priority** (range from 1-40). This determines the root (leaf) STP node. The lowest bridge priority in the network will become the STP root.

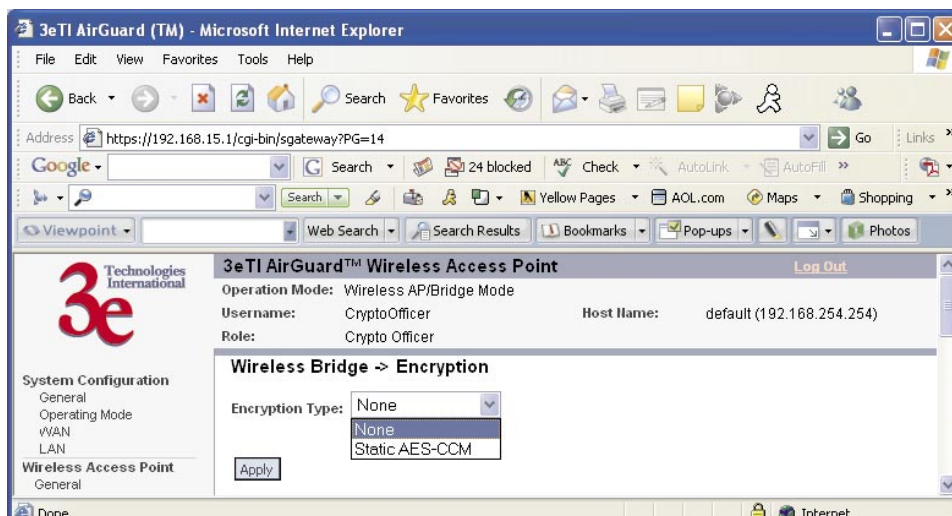
Select the **Signal Strength Threshold**.

Either enable or disable the **Broadcast SSID**. When disabled, the bridge hides the SSID in outgoing beacon frames and stations cannot obtain the SSID through passive scanning. Also, when it is disabled, the bridge doesn't send probe responses to probe requests with unspecified SSIDs.

Finally enter the **Signal Strength MAC**. The signal strength of this wireless bridge will be indicated on the Signal Strength LED located on the front of the case.



Next, navigate to the **Wireless Bridge — Encryption** screen. Select the appropriate key type and length and the key value. The encryption key value and type for Bridge 1 must be the same as for Bridge 2. For wireless bridging, only None and Static AES-CCM are available for encryption.



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

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

Point-to-Multipoint Bridge Configuration

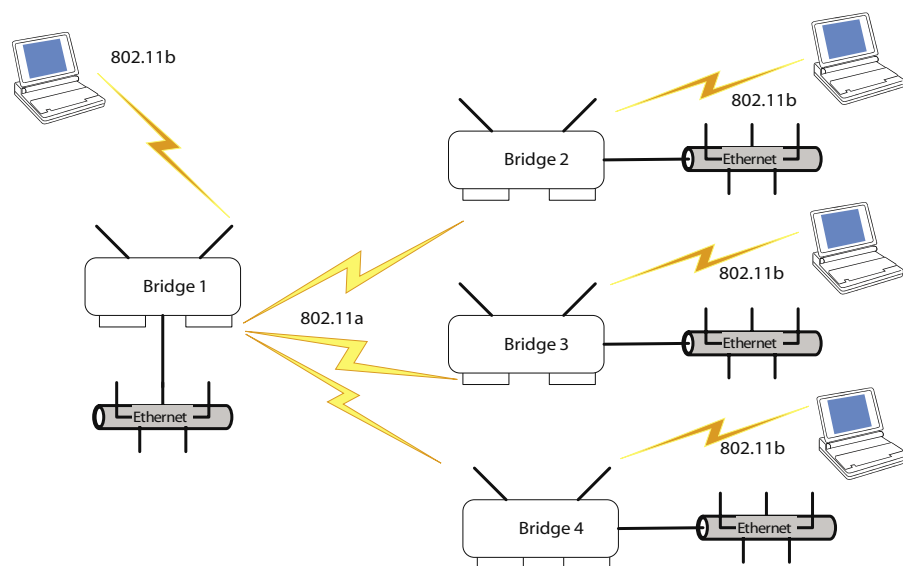
A point-to-multipoint configuration allows you to set up three or more 3e-525C-3 access points in bridging mode and accomplish bridging between 3 or more locations wirelessly.

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

For instance, all bridges must have the same channel number. Spanning Tree Protocol will usually be set to Enable. If configured as in the diagram following, Bridge 1 must contain all of the others' BSSIDs, while Bridge 2 ~ n must only contain Bridge 1's BSSID. (The BSSID of each is equivalent to the MAC address found on the **Wireless Bridge — Radio** page. Enter only hexadecimal numbers. Data entry is not case sensitive.) Finally, the wireless bridging encryption of each must be set to the appropriate type and key length and must be the same on all.

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

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



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

Point-to-Multipoint Bridging Setup Guide - Manual Mode

Direction	Bridge 1	Bridge 2 ~ n
Wireless Bridge — General (Manual Bridging Mode)		
Bridging Mode	manual bridging selected	manual bridging selected
Signal Strength LED MAC	Not Assigned (select from drop-down list)	Not Assigned (select from drop-down list)
Spanning Tree Protocol	Enable (or Disable if no bridging loop possible)	Enable (or Disable if no bridging loop possible)
Wireless Bridge — Radio		
Wireless Mode	802.11a	802.11a
Tx Rate	AUTO	AUTO
Channel No.	Same as Bridge 2~n	Same as Bridge 1
Tx Power Mode	Auto	Auto
Propagation Distance	< 5 Miles	< 5 Miles
RTS Threshold	2346	2346
BSSID	Add Bridge 2~n MAC	Add Bridge 1 MAC
Wireless Bridge — Encryption		
Bridging encryption options	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.

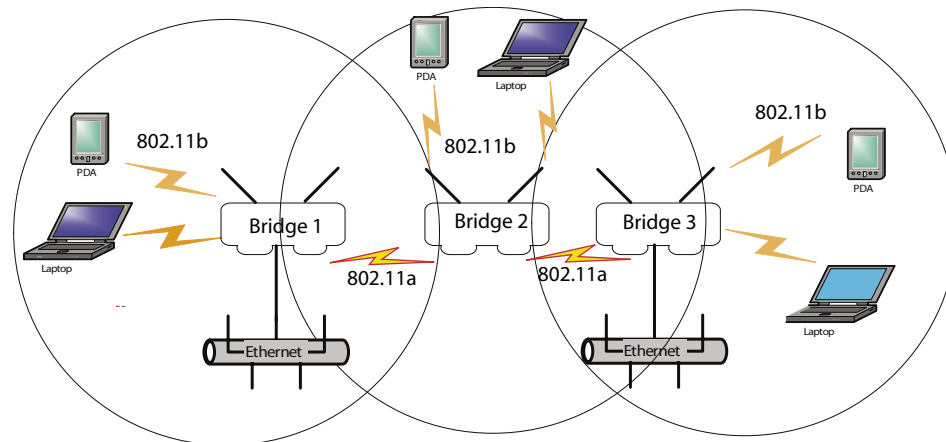
Point-to-Multipoint Bridging Setup Guide - Auto Mode

Direction	Bridge 1	Bridge 2 ~ n
Wireless Bridge — General (Auto Bridging Mode)		
Bridging Mode	Auto bridging selected	Auto bridging selected
SSID	Must be the same as Bridge 2~n	Must be the same as Bridge 1
Max Auto Bridges	40 (range 1-40)	40 (range 1-40)
Bridge Priority	40 (range 1-40)	40 (range 1-40)
Signal Strength Threshold	9%	9%
Signal Strength MAC	Enter from list at the bottom of the screen	Enter from list at the bottom of the screen
Wireless Bridge — Radio		
Wireless Mode	802.11a	802.11a
Tx Rate	AUTO	AUTO
Channel No.	Same as Bridge 2~n	Same as Bridge 1
Tx Power Mode	Auto	Auto
Propagation Distance	< 5 Miles	< 5 Miles
RTS Threshold	2346	2346
Wireless Bridge — Encryption		
Bridging encryption options	Select appropriate key type/length and value. Must be same as Bridge 2~n.	Select appropriate key type/length and value. Must be same as Bridge 1.
Wireless Bridge — MAC Address Filtering		
Filtering	Enable/Disable	Enable/Disable
Filter Type	Deny All/Allow All	Deny All/Allow All
MAC Address	Add MAC address of bridges	Add MAC address of bridges

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. Complete any other setup screens following general instructions in Chapter 3.

Repeater Bridge Configuration

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



Repeater Bridging Setup Guide - Manual Mode

Direction	Bridge 1	Bridge 2	Bridge 3
Wireless Bridge — General (Manual Bridging Mode)			
Bridging Mode	manual	manual	manual
Signal Strength LED MAC	Not Assigned (select from drop-down list)	Not Assigned (select from drop-down list)	Not Assigned (select from drop-down list)
Spanning Tree Protocol	Enable (or Disable if no bridging loop possible)	Enable (or Disable if no bridging loop possible)	Enable (or Disable if no bridging loop possible)
Wireless Bridge — Radio			
Wireless Mode	802.11a	802.11a	802.11a
Tx Rate	AUTO	AUTO	AUTO
Channel No.	Same as Bridge 2	Same as Bridge 1	Same as Bridge 1
Tx Power Mode	Auto	Auto	Auto
Propagation Distance	< 5 Miles	< 5 Miles	< 5 Miles
RTS Threshold	2346	2346	2346
BSSID	Add Bridge 2's MAC	Add Bridge 1's and Bridge 3's MAC	Add Bridge 2's MAC
Wireless Bridge — Encryption			
Wireless Configuration - Bridging Encryption	Select appropriate key type/length and enter key value. Must be the same as that on the other two Bridges.	Select appropriate key type/length and enter key value. Must be the same as that on the other two Bridges.	Select appropriate key type/length and enter key value. Must be the same as that on the other two Bridges.

Repeater Bridging Setup Guide - Auto Mode

Direction	Bridge 1	Bridge 2	Bridge 3
Wireless Bridge — General (Auto Bridging Mode)			
Bridging Mode	auto	auto	auto
SSID	Must be the same as Bridge 2	Must be the same as Bridge 1	Must be the same as Bridge 1
Max Auto Bridges	40 (range 1-40)	40 (range 1-40)	40 (range 1-40)
Bridge Priority	40 (1-40)	40 (1-40)	40 (1-40)
Signal Strength Threshold	9%	9%	9%
Signal Strength MAC	Enter from list at the bottom of the screen	Enter from list at the bottom of the screen	Enter from list at the bottom of the screen
Wireless Bridge — Radio			
Wireless Mode	802.11a	802.11a	802.11a
Tx Rate	AUTO	AUTO	AUTO
Channel	Same as Bridge 2	Same as Bridge 1	Same as Bridge 1
Tx Power Mode	Auto	Auto	Auto
Propagation Distance	< 5 Miles	< 5 Miles	< 5 Miles
RTS Threshold	2346	2346	2346
Wireless Bridge — Encryption			
Wireless Configuration – Bridging Encryption	Select appropriate key type/length and enter key value. Must be the same as that on the other 2 Bridges.	Select appropriate key type/length and enter key value. Must be the same as that on the other 2 Bridges.	Select appropriate key type/length and enter key value. Must be the same as that on the other 2 Bridges.
Wireless Bridge — MAC Address Filtering			
Filtering	Enable/Disable	Enable/Disable	Enable/Disable
Filter Type	Deny All/Allow All	Deny All/Allow All	Deny All/Allow All
MAC Address	Add MAC address of bridges	Add MAC address of bridges	Add MAC address of bridges

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

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

Chapter 6: Technical Support

Manufacturer's Statement

The 3e-525C-3 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

1-800-449-3384 (Monday - Friday, 8am to 5pm EST)

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

3DES

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

802.11

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

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

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

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.

DHCP

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

NMS (Network Management Station)

Includes such management software as HP Openview and IBM Netview.

PC Card

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

PDA (Personal Digital Assistant)

A handheld device.

SNMP

Simple Network Management Protocol

SSID

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

TKIP

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

VPN (Virtual Private Network)

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

WLAN (Wireless Local Area Network)

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

WPA

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