APPENDIX I: MANUAL

Please refer to the following pages.

3e Technologies International

æptec
microsystems, inc.™

Wireless Video Server User's Guide

Model 3e-528

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

29000141-001 A

publ. 02/04/05

This page intentionally left blank.

3e Technologies International's
Wireless Video Server
User's Guide

Model 3e-528

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.

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

The 3e-528 Wireless Video Server system (WVS) is a key component of any Critical Infrastructure Protection System implementation. 3e-528 WVS is a combination of products and services which enable the design, provisioning, implementation, operation, and maintenance of an integrated network to provide advanced video surveillance. 3e-528 delivers the architectures along with the supporting systems & services necessary for Wide Area / Local Area Network deployment of wireless and wired IP video networks across municipalities, campuses, transportation and other critical infrastructure locations. 3e-528 ensures heightened security through real-time video capture and transmission of high-resolution digital imagery. The system expands your security presence to numerous key locations and events to improve safety by reducing threats. It allows you to focus valuable personal on areas of critical concern where and when they are needed

Capabilities

3e-528 WVS solutions track activity around selected areas and aid in securing critical infrastructure. They enhance security; improve safety; detect threats and lower crime rates. Typical critical infrastructure targets include:

- Municipal Complexes
- Transportation centers – Airports, Railroads, Maritime Ports
- Bridges / tunnels
- Arenas & Convention Centers
- Public Events
- Power Grids
- Water systems / facilities

Functionality

Up to four cameras are easily connected to the 3e-528 Wireless Video Server - a mixed network of IEEE 802.11b/g wireless and wired Ethernet connections. The cameras can be controlled by a centralized operations staff that remotely controls each camera's Pan/Tilt/Zoom (PTZ) features, views live footage, records every camera for a specified period, reviews recorded footage, and outputs selected segments to digital or analog media. Because the 3e-528 WVS system has dual mode wireless capability (802.11g and 802.11b), local 802.11b 11Mbps wireless hotspots can be enabled around the video server locations. These hotspots serve to provide high speed mobile data access to police, emergency management personnel, and other municipal/government first responders.

The wireless portion of the 3e-528 Wireless Video Server system meets DoD security requirements with advanced data encryption (AES / 3DES) and uses crypto modules that are FIPS 140-2 Validated™ for sensitive data communications use. The 3e-528 system also supports use of existing Ethernet resources wherever possible to avoid additional build out costs. Because of its wireless bridging capabilities, the 3e-528 WVS system is easily expandable to support future growth without the material, time and costs associated with traditional wired links.

Video System Features

The 3e-528 WVS system supports most outdoor IP video surveillance cameras. It has analog to digital video conversion capabilities and multiple wireless or wired Ethernet connections.

- Network Connectivity

— 802.11b/g 54Mbs Wireless Bridging/Repeating of video to Operations Centers
— Provides serial server for sensor interface over the wireless or wired IP network connections
— Provision for 802.11b 11Mbs Wireless LAN Hotspot in addition to wired Ethernet
— Transport minimum video resolution of 640x480 with 4CIF quality
— Capability to convert and send up to 30 video frames per second
— Able to control a minimum 25x OPTICAL zoom on appropriate cameras
— Wireless camera signals are securely transmitted with FIPS 140-2 Validated AES encryption
— An optimum mix of wireless and wired resources
— Supports all cameras operating at a minimum of 7.5 Frames Per Second
— Termination of the video accomplished at one or more Operations Centers

- Housing

— Ruggedized outdoor housing for 3e-528 system components
— 4 port serial server connections for sensor interface including camera pan/tilt/zoom control
— 4 hardened video connections (BNC)

- Management

— Enables wireless digital transport and subsequent storage at Operations Center
— Provision for optional dynamic key server for increased security

- — Wireless connectivity for viewing 4 live camera feeds
- — Simultaneous use of all functions
- — Access user restrictions
- — Supports central operation/access of all cameras
- — Non-proprietary output format for admissibility in court (JPEG, M-JPEG, NTSC Video, etc.)
- — Camera control via 1 serial interface

If encryption is desired for the WLAN, you can employ different encryption depending on the mode you are in. If you are using FIPS 140-2 mode (highly secure) you can set encryption for None, Static AES, Static 3DES, or Dynamic Key Exchange. If you are not using the 3e-528 in FIPS 140-2 mode, you can select None, Static AES, Static 3DES, Static WEP, or WPA. WPA uses TKIP or AES-CCMP so you can employ legacy client WEP cards and still secure the wireless band. If it is desired that the wireless video server employs state-of-the-art AES or 3DES encryption for wireless access, wireless clients must have the 3e-010F Crypto Client software installed. (The 3e-010F Crypto Client software is sold with the 3e-110 long range PC card or sold separately for use with other compatible PC cards.)

The 3e-528 has an Ethernet WAN interface (WAN port) for communication to the wired LAN backbone, three Ethernet LAN local interfaces (CONFIG ports) for purposes of initial setup and configuration, one AP antenna for 802.11 b wireless clients, and three bridging antennas for communicating on the 802.11b/g radio.

The 3e-528 is wall-mountable.

It has the following features:

- Ethernet WAN port
- "CONFIG" Ethernet LAN ports (for configuration only)
- Wireless (802.11b) AP with operating range of 2000+ feet
- Wireless (802.11b/g) bridge
- AES, 3DES, WEP encryption or WPA with TKIP, depending on setup
- HTTPS/TLS secure Web
- DHCP client
- Video Server port
- Bandwidth control
- Adjustable Radio Power
- MAC address filtering
- Load Balancing
- Rogue AP Detection

The following cryptographic modules have been implemented in the 3e-528 .

- AES (128/192/256 bit)
- 3DES (192 bit)
- WEP
- WPA
- 802.1x/EAP-TLS for authentication

Wireless Basics

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

The 3e-528 incorporates WiFi standard and FIPS 140-2 security for wireless communication.

802.11b

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

For wireless devices to communicate with the 3e-528 , 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-528);
- Encryption and authentication capabilities and types enabled must conform; and
- If MAC filtering is used, the 3e-528 must be configured to allow the wireless device's MAC address to associate (communicate) with the 3e-528 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.

Network Configuration

The 3e-528 is a wireless video server and access point with bridging capability: The wireless bridging function supports a number of bridging configurations. We discuss the most popular settings in this manual.

- Video Server and Access Point plus:
- Wireless bridging with choice of:
  - Point-to-point setup
  - Point-to-multipoint setup
  - Repeater setup

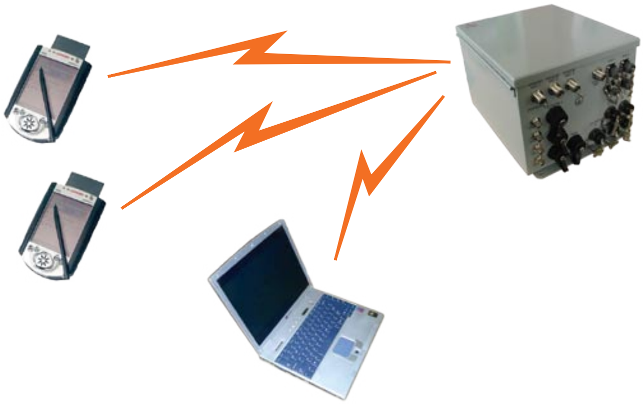
Access Point Configurations

IP addresses for wireless devices are typically assigned by the wired network's DHCP server. The wired network's DHCP server assigns addresses dynamically, and the AP virtually connects wireless users to the 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. Both wireless clients and devices connected to the wired network can access the video server. In order to access the video interface, the IP address of the video card needs to be configured manually to be within the same network. Refer to the Video Configuration section to learn more about the video configuration (Chapter 4).

Possible AP Topologies

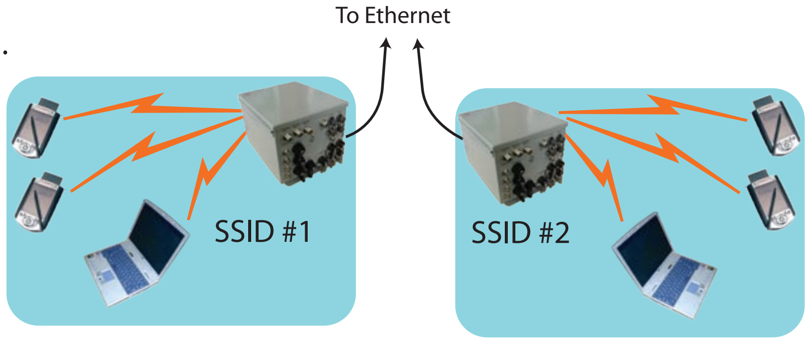
1. An access point can be used as a stand-alone AP without any connection to a wired network. In this configuration, it simply provides a stand-alone wireless network for a group of wireless devices with or without a video connection in the AP (3e-528).

1.

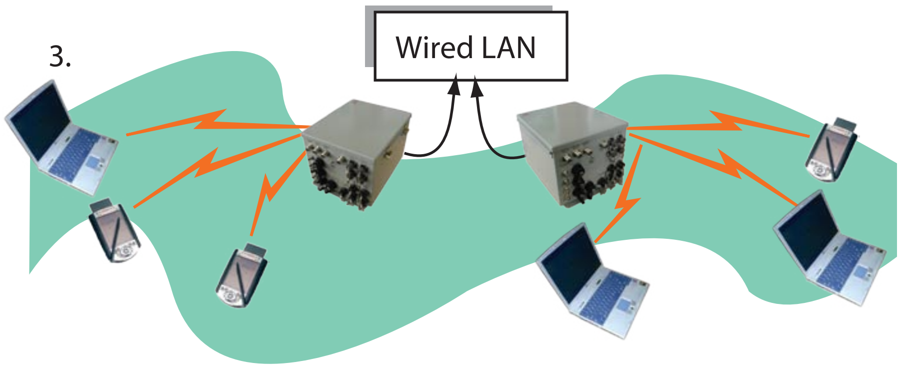


2. There can be multiple APs with video access (3e-528) connected to an existing Ethernet network to bridge between the wired and wireless environments. Each AP can operate independently of the other APs on the LAN. Multiple APs can coexist as separate individual networks at the same site with a different network ID (SSID).

2.



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 3e-528 can also function as a bridge. There are a number of bridging configurations supported, 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-528's default configuration is an Access Point/Bridge with FIPS 140-2 submode enabled. The video card and the three bridges need to be configured before being able to access the system.

Data Encryption and Security

The 3e-528 Wireless Video Server includes advanced wireless security features. You have a choice of no security, Static WEP, WPA, AES/3DES, depending on your mode of operation. 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-528's and includes use of AES-ECB or 3DES encryption (approved by the National Institute of Standards and Technology (NIST) for U.S. Government and DoD agencies).

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 discover the AP. SSID broadcasting can be disabled in the 3e-528 setup menus.

WEP

WEP is an older encryption standard that has been superseded by stronger encryption options. If the 3e-528 is configured with WEP encryption, it is compatible with any 802.11b PC card configured for WEP.

WPA with TKIP/ AES-CCMP

WPA, an interim standard developed by the WiFi Alliance, combines several technologies. It includes the use of the 802.1x standard and the Extensible Authentication Protocol (EAP). In addition, it uses, for encryption, the Temporal Key Integrity Protocol (TKIP) and WEP 128-bit encryption keys. Finally, a message integrity check (MIC) is used to prevent an attacker from capturing and altering or forging data packets. In addition, it can employ a form of AES called AES-CCMP. The 3e-528 allows the user to configure.

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

AES and 3DES

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

3DES is also incorporated on the 3e-528. 3DES is modeled on the older DES standard but encrypts data three times over. Triple-DES uses more CPU resources than AES because of the triple encryption.

If you intend to use AES or 3DES, you must purchase the 3eTI advanced Crypto Client software (3e-010F) for each client that will be included in the WLAN. We sell this software with the 3e-110 PC Card.

The 3e-528 uses AES-CCMP in WPA mode and AES-ECB (or 3DES) for FIPS 140-2 mode and for bridging.

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-528 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 he 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.

Access to the management screens for the 3e-528 requires knowledge of the assigned operator ID and Password. The Factory defaults are:

- ID: CryptoOfficer
- Password: CryptoFIPS

The Crypto Officer initially installs and configures the 3e-528 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-528 Navigation Options

ACCESS POINT	
Non FIPS 140-2	**FIPS 140-2**
System Configuration	**System Configuration**
General	General
WAN	WAN
LAN	LAN
Operating Mode	Operating Mode
Wireless Access Point	**Wireless Access Point**
General	General
Security • None • Static WEP • WPA • Static AES • Static 3DES	Security • None • Static AES • Static 3DES • Dynamic Key Exchange
MAC Address Filtering	MAC Address Filtering
Bridging • Monitoring	Bridging • Monitoring
Bridging Encryption	Bridging Encryption
Rogue AP Detection	Rogue AP Detection
Advanced	Advanced
Services Settings	**Services Settings**
DHCP Server	DHCP Server
Subnet Roaming	Subnet Roaming
SNMP Agent	SNMP Agent
User Management	**User Management**
List All Users • Edit/Delete	List All Users • Edit/Delete
Add New User	Add New User
	User Password Policy
Monitoring Reports	**Monitoring Reports**
System Status	System Status
Bridging Status	Bridging Status
Wireless Clients	Wireless Clients
Adjacent AP List	Adjacent AP List
DHCP Client List	DHCP Client List
System Log	System Log
Web Access Log	Web Access Log
Network Activity Log	Network Activity Log
System Administration	**System Administration**
Firmware Upgrade	Firmware Upgrade
Factory Default	Factory Default
Remote Logging	Remote Logging
Reboot	Reboot
Utilities	Utilities

Chapter 2: Hardware installation

Preparation for Use

The 3e Technologies International's 3e-528 Wireless Video Server requires physical mounting and installation on the site, following a prescribed placement design to ensure optimum operation and roaming. The 3e-528 must be professionally installed by an installer certified by the National Association of Radio and Telecommunications Engineers or equivalent institution

The 3e-528 package includes the following items:

- The 3e-528 Wireless Video Server/Access Point
- Attachable 5dBi omni-directional antenna for AP
- 2 meter Cat5 cable to RJ-45 (LAN/configuration)
- 2 meter Cat5 cable to RJ-45 (WAN)
- 3 meter PTZ (pan/tilt/zoom) cable with male DB-9 (RS-232)
- 3 meter video in cable
- Camera power cable
- 3e-528 power cable
- Documentation as PDF files (on CD-ROM)
- Registration and Warranty cards

The following items are options:

- 3 meter antenna extension cable
- 3 meter video cables
- 3 meter PTZ cable with female DB-9 (RS-232)
- Lightning arrestor

The 3e-528 can be mounted outdoors. It has a lightning protection option to prevent lightning damage.

⚠ To comply with FCC RF exposure compliance requirements, the antennas used with the 528 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-528 is intended to be installed as part of a complete wireless design solution. The 3e-528 has a operating temperature range of 0-40ºC and should be installed in an area with shade or out of direct sunlight.

This manual deals only and specifically with a single 3e-528 device as a unit. The purpose of this chapter is to describe 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 for 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 (refer to Chapter 7 for technical support).

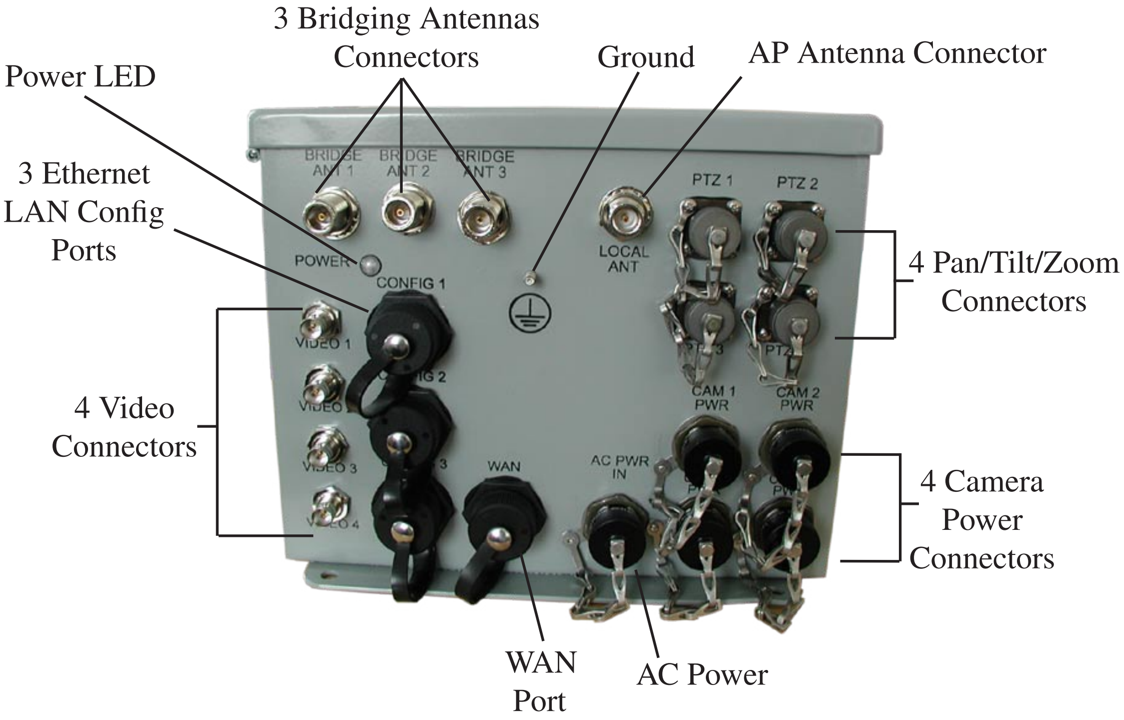
Minimum System and Component Requirements

The 3e-528 is designed to be attached to the wall at appropriate locations. To complete the configuration, you should have at least the following components:

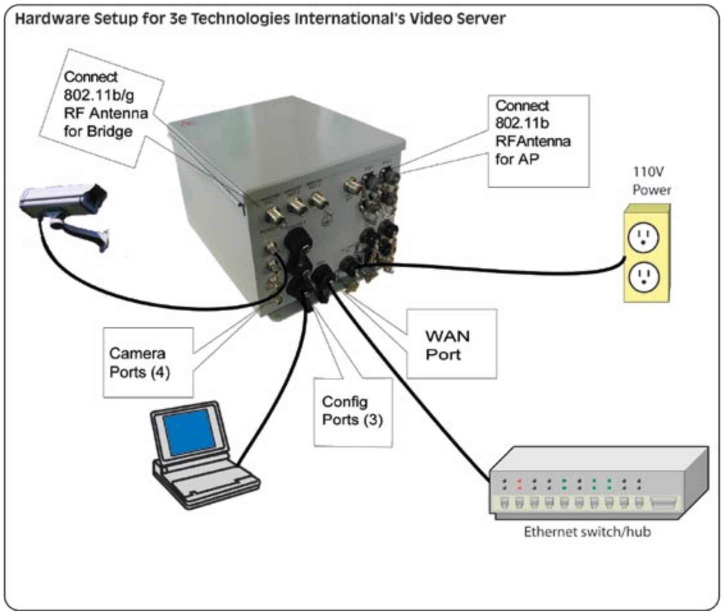
- PCs with one of the following operating systems installed: Windows NT 4.0, Windows 2000 or Windows XP;
- A Wi-Fi compatible 802.11b/g device for each computer that you wish to wirelessly connect to your wireless network. (For wireless cards, and particularly if you will be using secure FIPS mode with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

Cabling

The following illustration shows the external cable connectors on the 3e-528.



The WAN connector is used to connect the 3e–528 to the organization's LAN. Three additional LAN connectors (Config ports) are available for use during initial configuration only. This uses an RJ45 cable to connect the 3e–528 to a laptop. The following diagram demonstrates the setup.

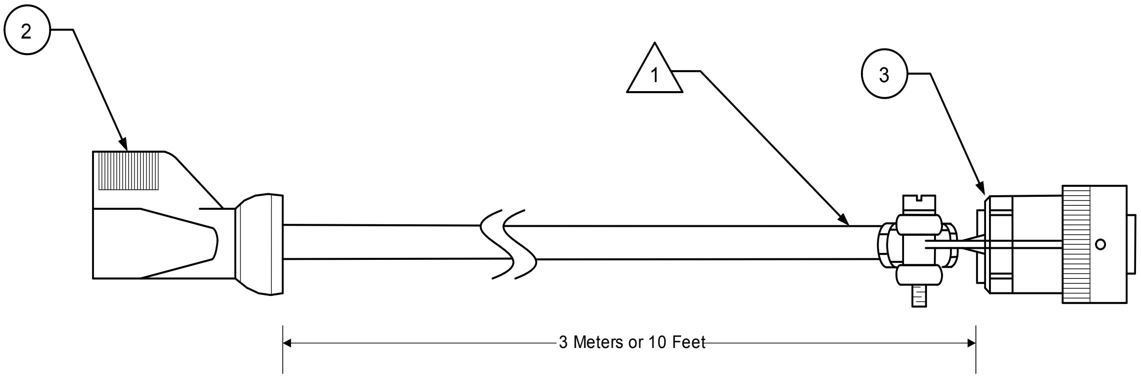

Hardware Setup for 3e Technologies International's Video Server
Connect 802.11b/g RF Antenna for Bridge
Connect 802.11b RFAntenna for AP
110V Power
Camera Ports (4)
Config Ports (3)
WAN Port
Ethernet switch/hub

External Camera Power Cable

The 528 distributes AC power to up to four cameras.

CAUTION: Do not use any camera device that consumes more than 2A power consumption on the power distribution channels.

The following cable diagram is for an AC output NEMA-015 receptacle (standard AC receptacle).



NOTES:

1. REMOVE THE MALE END OF THE AC EXTENSION CABLE AND USE THE EXISTING CABLE TO ATTACH F/N 3

Below is the cable pinout information.

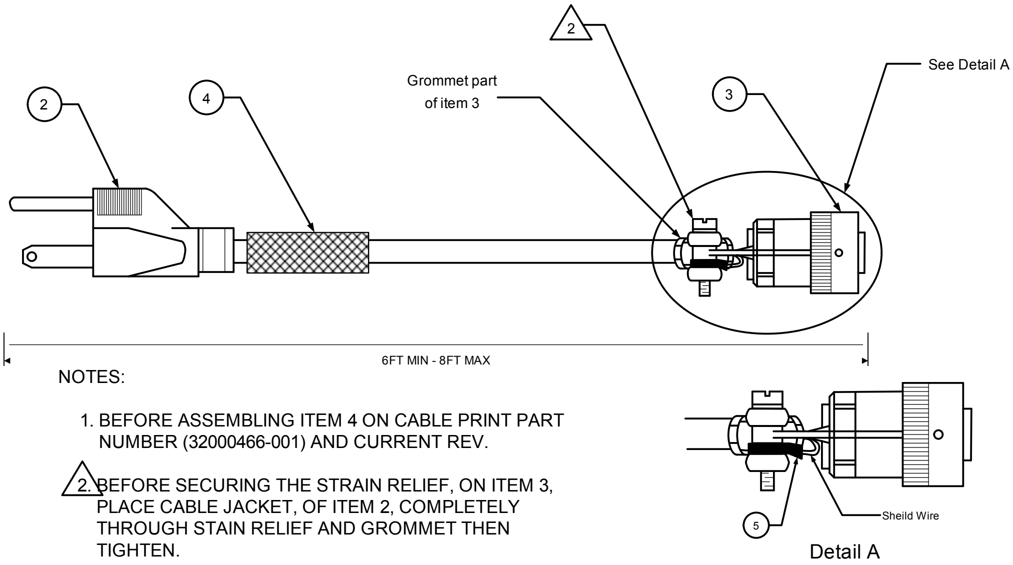
Mil Circular Connector 851-06RC12-3P50 (CTI)	Signal Name
Pin A	AC Line
Pin B	AC Neutral
Pin C	Ground

The following table provides the bill of materials for the above cable.

F/N	Part Number	Description	Quantity
1	NA	Reference Doc	-
2	90000927-001	Cable Assy, Extension, Power, AC, 3 Meter	1
3	90000928-001	Connector, Circular, Cable Mount, Male, 3P	1

External Power Cable

The 3e-528 has an external power cable for connection to a 110VAC outlet. The cable is an AC input NEMA-015 plug (standard AC plug).



NOTES:

1. BEFORE ASSEMBLING ITEM 4 ON CABLE PRINT PART NUMBER (32000466-001) AND CURRENT REV.

2. BEFORE SECURING THE STRAIN RELIEF, ON ITEM 3, PLACE CABLE JACKET, OF ITEM 2, COMPLETELY THROUGH STAIN RELIEF AND GROMMET THEN TIGHTEN.

Below is the cable pinout information.

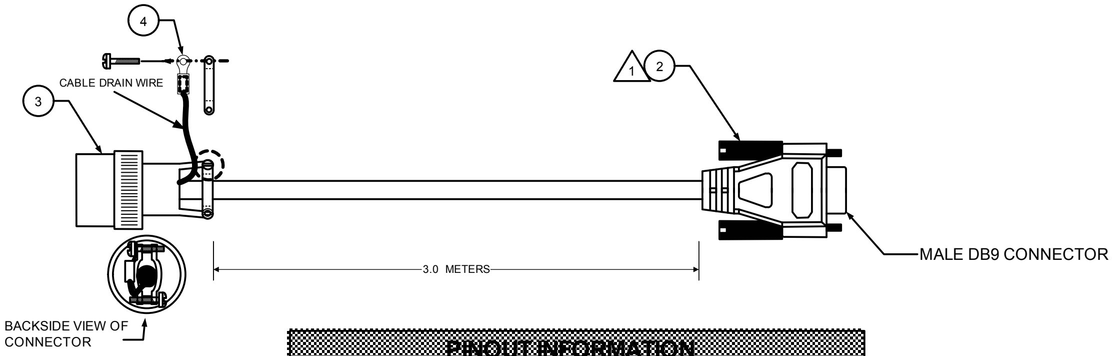
Mil Circular Connector 851-06EC12-3S50 (CTI)	Signal Name
Pin A	AC Line
Pin B	AC Neutral
Pin C	Ground

The following table provides the bill of materials for the above cable.

F/N	Part Number	Description	Quantity
1	32000466	DWG, Cable Assy, Power, 110VAC, External	-
2	90000668-001	Line Cord, 18 AWG/3 Cond, SVT Shield, 10 AMP, 8'	1
3	90000669-001	Connector, Circular, Cable Mount, Male, 3P	1
4	90000615-001	Shrink Tubing, White, Printable, .5 ID	1.5 inch
5	90000667-001	Terminal, Ring, Non-Insulated, 22AWG, #6 Stud	1

Pan/Tilt/Zoom Cable

The pan/tilt/zoom cable connects to a PTZ port on the 3e-528. There are four PTZ ports, one for each camera. Below is a diagram of the cable and the pinout and bill of materials.



PINOUT INFORMATION

PIN (MIL)	PIN (DB9)	WIRE COLOR
A	N/A	
B	5	YELLOW
C	3	RED
D	2	BROWN
E	N/A	
F	N/A	
N/A	N/A	
N/A	N/A	
N/A	N/A	

Mil Circular Connector 851-06RC10-6P50 (CTI)	DB-9	Signal Name
Pin D	2	TxD (Data transmitted out of the 3e-528)
Pin C	3	RxD (Data received into the 3e-528)
Pin B	5	GND

F/N	Part Number	Description	Quantity
1	32000673	DWG, Cable Assy, External PTZ	-
2	90000913-001	Cable Assy, DB9, Male to Female	1
3	90000670-001	Connector, Circular, Cable Mount, Male, 6P	1
4	90000630-001	Terminal, Ring, Crimp, Insulated, 18-22 AWG, #6 Stud	1

WAN/LAN Cable

The 3e-528 comes with two Cat5 red cables (part number 90000776-001) which can be used for the WAN and LAN (Config) ports. Here is the pinout information.

Plug 1 RJ-45	Plug 2 RJ-45	Signal Name
Pin 1	Pin 1	TD+
Pin 2	Pin 2	TD-
Pin 3	Pin 3	RD+
Pin 4	Pin 4	N/A
Pin 5	Pin 5	N/A
Pin 6	Pin 6	RD-
Pin 7	Pin 7	N/A
Pin 8	Pin 8	N/A

Video In Cable

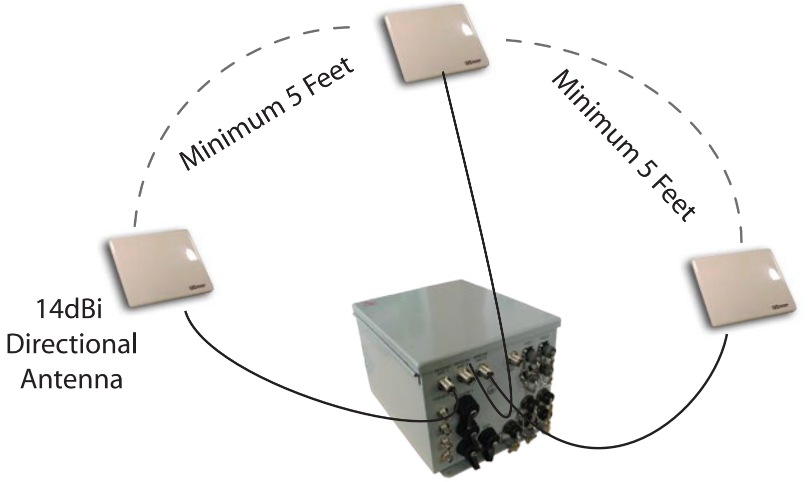
The pinout information for the video in cable (part number 90000926-001) is provided below. The video cable is 3 meters in length.

BNC Plug	BNC Plug	Signal
Shield	Shield	Shield
Center Conductor	Center Conductor	Video

Bridge Antenna Installation

The illustration below shows the guidelines required for antenna installation co-location in order to ensure optimal system performance.

It is recommended that the bridging antennas be spaced at least five feet apart from each other and be pointed in different (non-overlapping) directions. If the antennas are too close or pointed int he same direction, then there will be interference and poor signal strength. Refer to Chapter 5 for bridge antenna alignment.



Chapter 3: Access Point Configuration

Introduction

The 3e-528 features three bridging ports interconnected to each other internally. The first bridging port, accessible from the CONFIG 1 port, can also act as an access point. This unit incorporates two separate 802.11 wireless cards, one 802.11b card that acts as a WLAN, and one dual 802.11b/g card for use in wireless bridging.

The 3e-528 wireless video server 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 9.

Preliminary Configuration Steps

For preliminary installation the 3e-528 network administrator may need the following information:

- IP address
  Note: To set up one 3e-528 you will need five IP addresses. One for the accesspoint port (the first bridging port uses the same IP address), three for the other bridging ports, one for the video server card, and one for the serial server card for PTZ (pan/tilt/zoom).
- Subnet Mask
- Default IP addresses of the 3e-528
  – 192.168.254.254 for the AP and first bridge
  – 192.168.254.20 for the video server
  – 192.168.254.30 for the serial card
- 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-528 network of access points (if MAC address filtering is to be enabled)
- The appropriate encryption key for wireless connection.

Initial Setup using the “CONFIG 1” Port

Plug setup cable into the LAN (CONFIG 1) port of the 3e-528 (see page 13) and the other end to an Ethernet port on your laptop. This LAN port in the 3e-528 connects you to the Access Point’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-528 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.

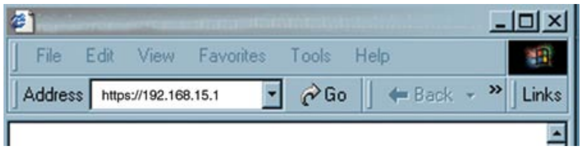
In Windows 2000/XP, follow the path **Start → Settings → Network and Dialup Connections → Local Area Connection** and select the **Properties** button. In the **Properties** window, highlight the TCP/IP protocol and click properties. Make sure that the radio button for **Obtain an IP address automatically**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

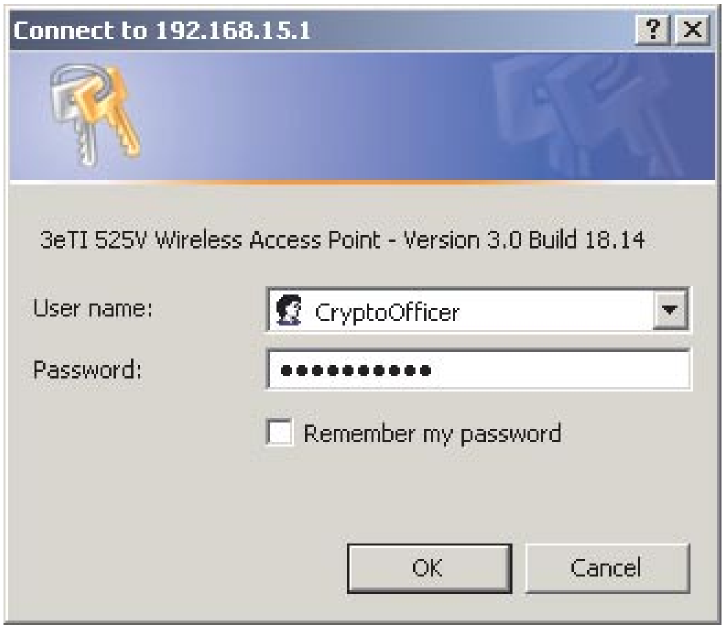
On your computer, pull up a browser window and put the default URL for the 3e-528 Local LAN in the address line. (https://192.168.15.1)



Address: https://192.168.15.1

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

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



Connect to 192.168.15.1

3eTI 525V Wireless Access Point - Version 3.0 Build 18.14

User name: CryptoOfficer

Password: ●●●●●●●●●●●

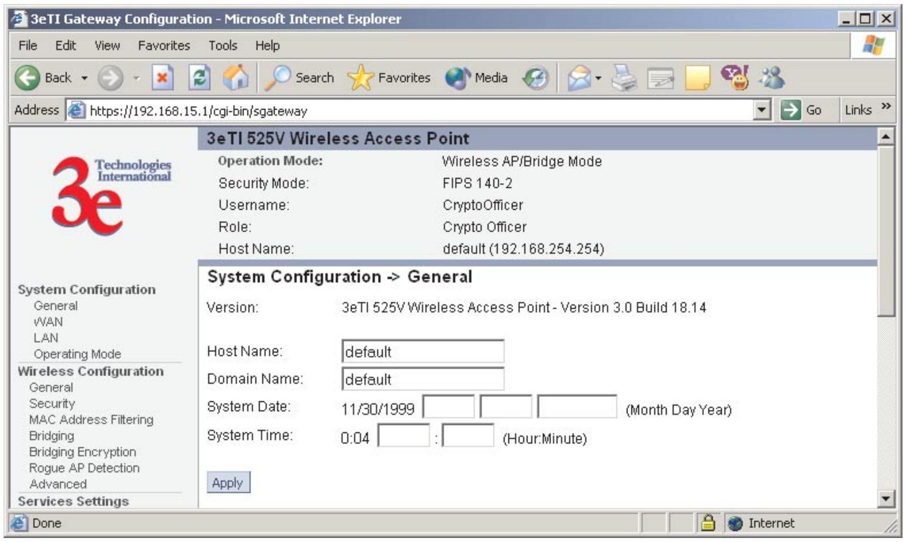
□ Remember my password

System Configuration

General

You will immediately be directed to the **System Configuration—General** screen for the 3e-528.

This screen lists the firmware version number for your 3e-528 and allows you to set the Host Name and Domain Name as well as establish system date and time. (Host and Domain Names are both set at the factory for “default” but can optionally be assigned a unique name for each.) When you are satisfied with your changes, click **Apply**.



3eTI 525V Wireless Access Point

Operation Mode:	Wireless AP/Bridge Mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer
Host Name:	default (192.168.254.254)

System Configuration -> General

Version: 3eTI 525V Wireless Access Point - Version 3.0 Build 18.14

Host Name: default

Domain Name: default

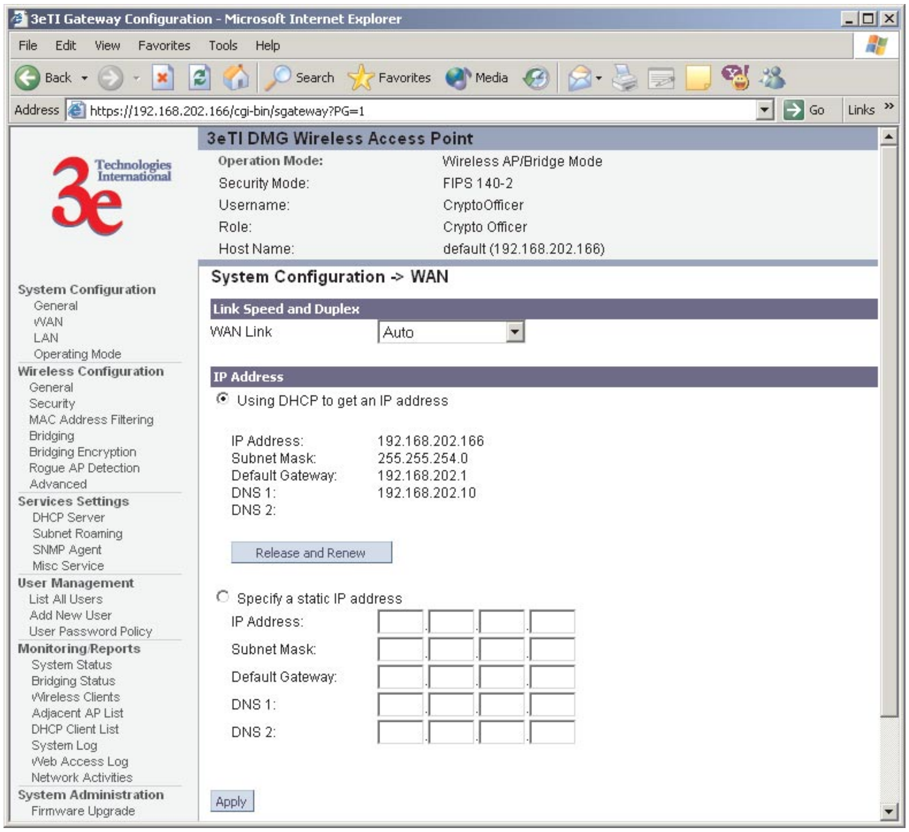
System Date: 11/30/1999 (Month Day Year)

System Time: 0:04 : (Hour:Minute)

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

WAN

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



3eTI DMG Wireless Access Point

Operation Mode:	Wireless AP/Bridge Mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer
Host Name:	default (192.168.202.166)

System Configuration -> WAN

Link Speed and Duplex

WAN Link: Auto

IP Address

● Using DHCP to get an IP address

IP Address:	192.168.202.166
Subnet Mask:	255.255.254.0
Default Gateway:	192.168.202.1
DNS 1:	192.168.202.10
DNS 2:	

○ Specify a static IP address

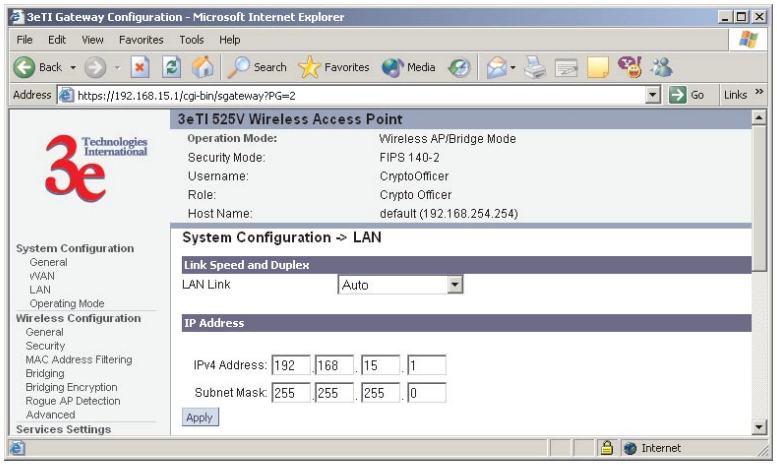
IP Address:
Subnet Mask:
Default Gateway:
DNS 1:
DNS 2:

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.

LAN

This sets up the default numbers for the four octets for a possible private LAN function for the access point. It also allows changing the default numbers for the LAN Subnet Mask and the link speed. 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.



Address: https://192.168.15.1/cgi-bin/sgateway?PG=2

3eTI 525V Wireless Access Point

Operation Mode:	Wireless AP/Bridge Mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer
Host Name:	default (192.168.254.254)

System Configuration -> LAN

Link Speed and Duplex

LAN Link: Auto

IP Address

IPv4 Address: 192 . 168 . 15 . 1

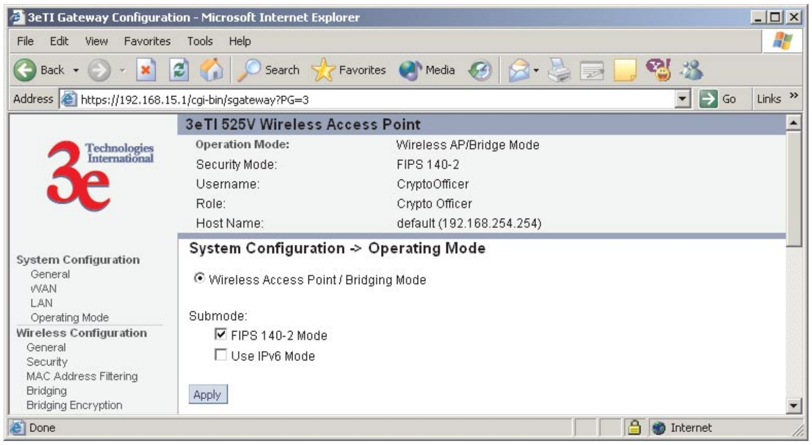
Subnet Mask: 255 . 255 . 255 . 0

Apply

Operating Mode

This screen allows you to set the operating mode to either FIPS enabled or disabled. You can also set the device to use IPv6.

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



Address: https://192.168.15.1/cgi-bin/sgateway?PG=3

3eTI 525V Wireless Access Point

Operation Mode:	Wireless AP/Bridge Mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer
Host Name:	default (192.168.254.254)

System Configuration -> Operating Mode

● Wireless Access Point / Bridging Mode

Submode:

☑ FIPS 140-2 Mode

☐ Use IPv6 Mode

Apply

Submodes

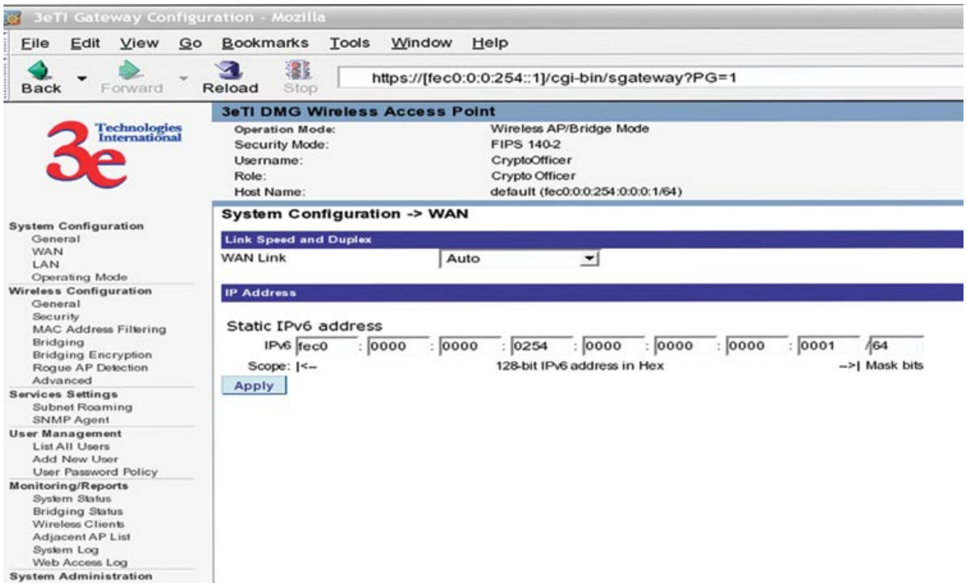
There are two options under Submodes:

- FIPS 140-2 Mode
- Use IPv6 Mode

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

When in IPv6 mode, the AP can be accessed from the management port using IP address 192.168.15.1. This is the default IP address and it can not be changed. The WAN port can not be accessed using IPv4 addresses.

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



https://[fec0:0:0:254::1]/cgi-bin/sgateway?PG=1

3eTI DMG Wireless Access Point

Operation Mode:	Wireless AP/Bridge Mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer
Host Name:	default (fec0:0:0:254:0:0:0:1/64)

System Configuration -> WAN

Link Speed and Duplex

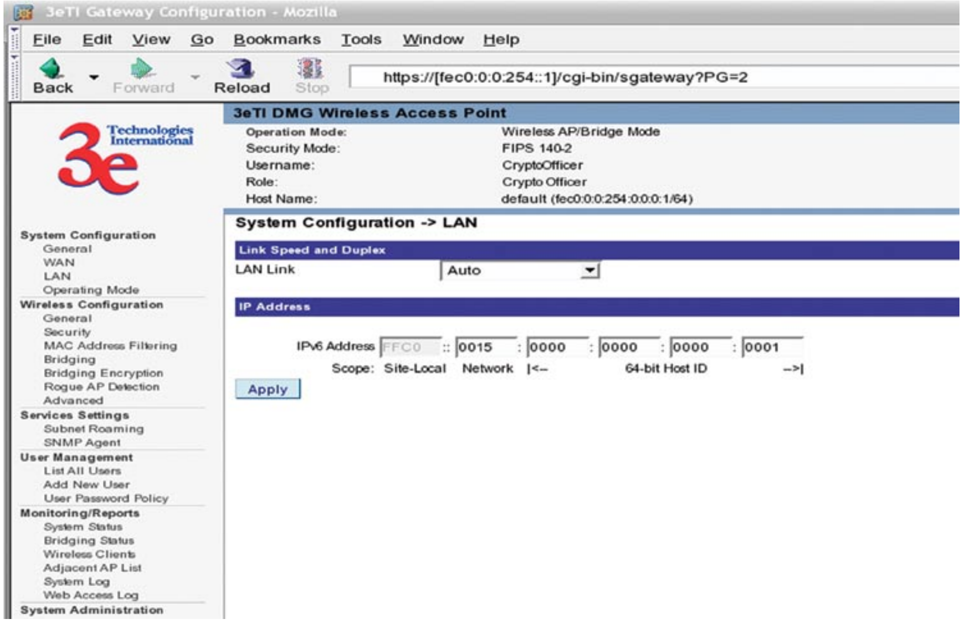
WAN Link: Auto

IP Address

Static IPv6 address

IPv6 fec0 : 0000 : 0000 : 0254 : 0000 : 0000 : 0000 : 0001 /64

Scope: |<-- 128-bit IPv6 address in Hex -->| Mask bits



https://[fec0:0:0:254::1]/cgi-bin/sgateway?PG=2

3eTI DMG Wireless Access Point

Operation Mode:	Wireless AP/Bridge Mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer
Host Name:	default (fec0:0:0:254:0:0:0:1/64)

System Configuration -> LAN

Link Speed and Duplex

LAN Link: Auto

IP Address

IPv6 Address FEC0 :: 0015 : 0000 : 0000 : 0000 : 0001

Scope: Site-Local Network |<-- 64-bit Host ID -->|

Wireless Configuration

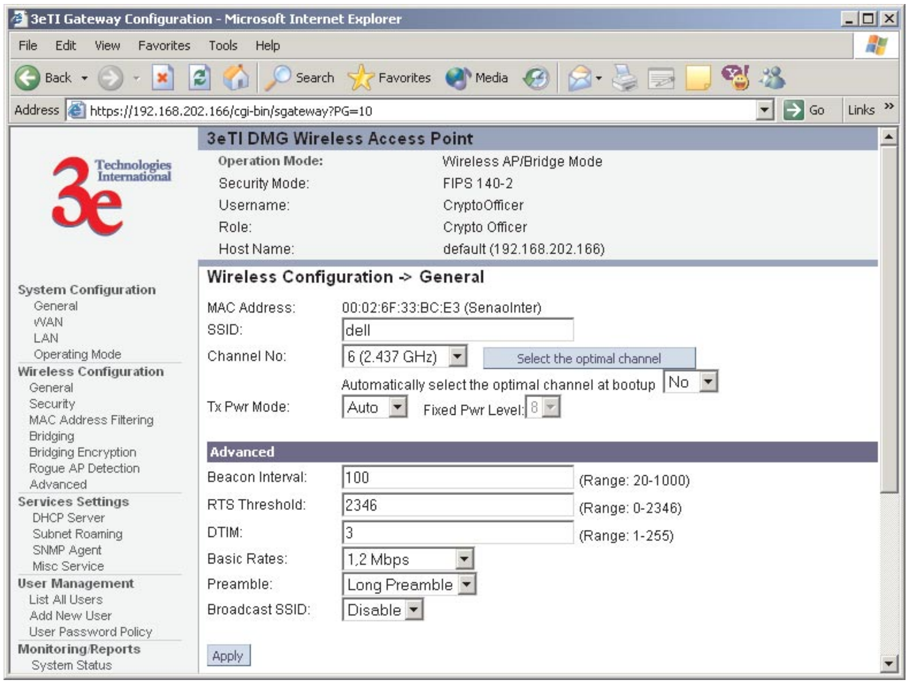
General

Wireless Setup allows your computer's PC Card to communicate with the access point.

⚠ **WARNING**: If you are configuring this 3e-528 in FIPS 140-2 secure mode, your configuration will have to be accomplished through the LAN port due to the secure nature of the access point.

The **Wireless Configuration — General** screen lists the MAC Address of the AP.

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.



3eTI DMG Wireless Access Point

Operation Mode:	Wireless AP/Bridge Mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer
Host Name:	default (192.168.202.166)

Wireless Configuration -> General

MAC Address: 00:02:6F:33:BC:E3 (SenaoInter)

SSID: dell

Channel No: 6 (2.437 GHz)

Automatically select the optimal channel at bootup: No

Tx Pwr Mode: Auto Fixed Pwr Level: 8

Advanced

Beacon Interval: 100 (Range: 20-1000)

RTS Threshold: 2346 (Range: 0-2346)

DTIM: 3 (Range: 1-255)

Basic Rates: 1,2 Mbps

Preamble: Long Preamble

Broadcast SSID: Disable

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

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

If you are using the 3e-528 as both an AP and bridge, the channel number set for the AP board and the channel number set for the bridge should be sufficiently different to avoid interference.

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 up the optimal channel at boot up.

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

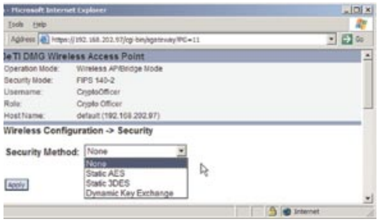
There are a number of advanced options included on this screen as described in the following chart:

Advanced Options		
Beacon Interval	Range 20-1000	The time interval in milliseconds in which the 802.11 beacon is transmitted by the AP.
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.
DTIM	Range 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.
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 3e-528 will display a default factory setting of no encryption, but for security reasons will not communicate to any clients unless the encryption is set by the administrator. There will be different encryption options for the AP in FIPS Mode and the non-FIPS Mode. The following chart shows the differences:

Encryption Options on the 3e-528	
In FIPS 140-2 Mode	In non-FIPS AP Mode
None	None
Static AES (AES-ECB)	Static WEP
Static 3DES	WPA
Dynamic Key Exchange (with 3e-030 Security Server, purchased separately)	Static AES
	Static 3DES



- Microsoft Internet Explorer

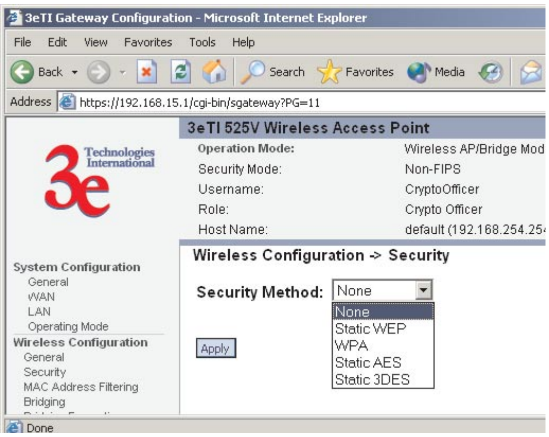
Address: https://192.168.202.97/cgi-bin/sgateway?PG=11

3eTI DMG Wireless Access Point

Operation Mode: Wireless AP/Bridge Mode
Security Mode: FIPS 140-2
Username: CryptoOfficer
Role: Crypto Officer
Host Name: default (192.168.202.97)

Wireless Configuration -> Security

Security Method: None



3eTI Gateway Configuration - Microsoft Internet Explorer

Address: https://192.168.15.1/cgi-bin/sgateway?PG=11

3eTI 525V Wireless Access Point

Operation Mode: Wireless AP/Bridge Mod
Security Mode: Non-FIPS
Username: CryptoOfficer
Role: Crypto Officer
Host Name: default (192.168.254.25

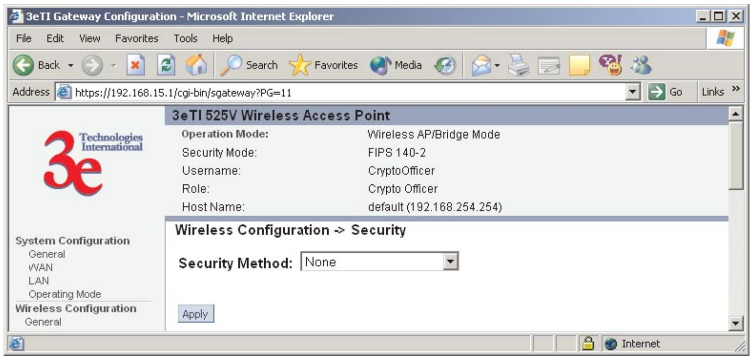
Wireless Configuration -> Security

Security Method: None

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

No Encryption

In order to have the 3e-528 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.



3eTI Gateway Configuration - Microsoft Internet Explorer

Address: https://192.168.15.1/cgi-bin/sgateway?PG=11

3eTI 525V Wireless Access Point

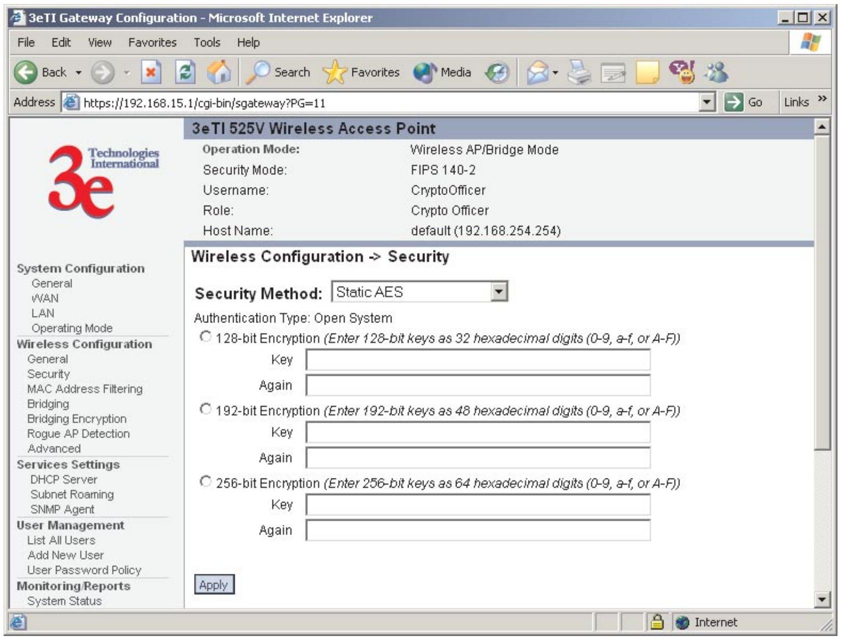
Operation Mode: Wireless AP/Bridge Mode
Security Mode: FIPS 140-2
Username: CryptoOfficer
Role: Crypto Officer
Host Name: default (192.168.254.254)

Wireless Configuration -> Security

Security Method: None

Static AES Key

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



3eTI Gateway Configuration - Microsoft Internet Explorer

Address https://192.168.15.1/cgi-bin/sgateway?PG=11

3eTI 525V Wireless Access Point

Operation Mode: Wireless AP/Bridge Mode
Security Mode: FIPS 140-2
Username: CryptoOfficer
Role: Crypto Officer
Host Name: default (192.168.254.254)

Wireless Configuration -> Security

Security Method: Static AES

Authentication Type: Open System

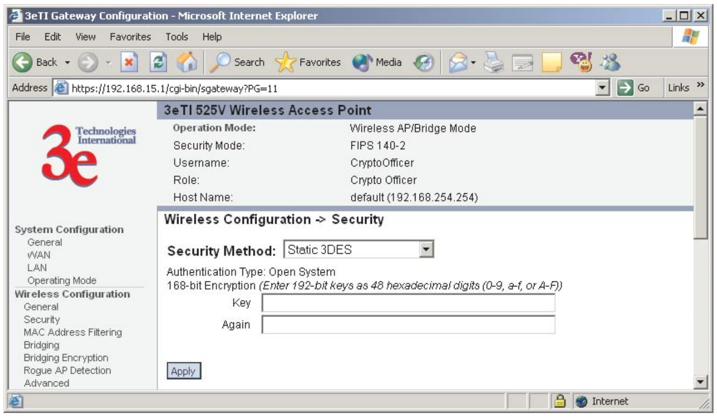
○ 128-bit Encryption *(Enter 128-bit keys as 32 hexadecimal digits (0-9, a-f, or A-F))*
Key
Again

○ 192-bit Encryption *(Enter 192-bit keys as 48 hexadecimal digits (0-9, a-f, or A-F))*
Key
Again

○ 256-bit Encryption *(Enter 256-bit keys as 64 hexadecimal digits (0-9, a-f, or A-F))*
Key
Again

Static 3DES Key

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



3eTI Gateway Configuration - Microsoft Internet Explorer

Address https://192.168.15.1/cgi-bin/sgateway?PG=11

3eTI 525V Wireless Access Point

Operation Mode: Wireless AP/Bridge Mode
Security Mode: FIPS 140-2
Username: CryptoOfficer
Role: Crypto Officer
Host Name: default (192.168.254.254)

Wireless Configuration -> Security

Security Method: Static 3DES

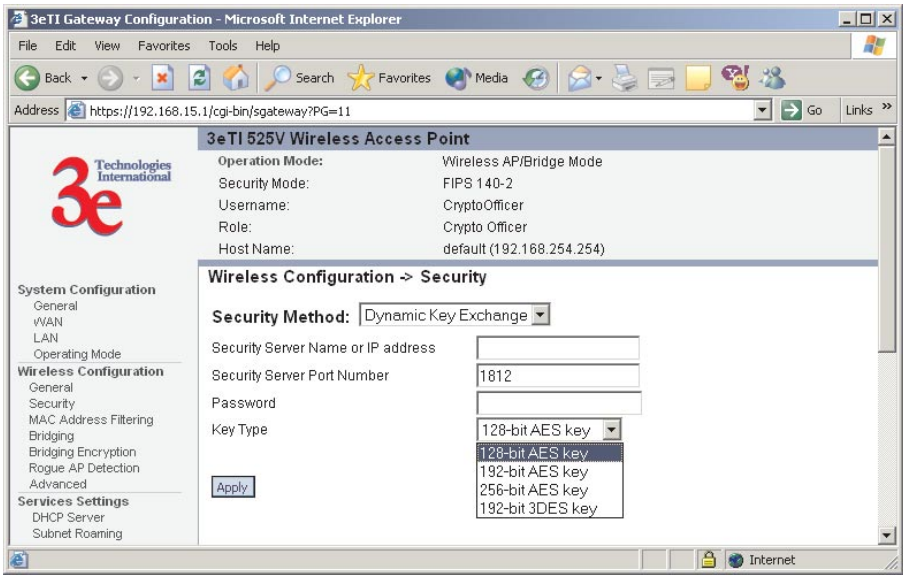
Authentication Type: Open System

168-bit Encryption *(Enter 192-bit keys as 48 hexadecimal digits (0-9, a-f, or A-F))*
Key
Again

Dynamic Key Exchange

Dynamic key management requires the installation of the 3e-030 Security Server software which resides on a self-contained workstation connected to the 3e-528 over the WAN port. The Security Server software configuration includes: obtaining a root certificate from a Certificate Authority (CA) like Microsoft; obtaining user certificates based on the CA which will be used by the clients; and configuring the 3e Technologies International's Security Server software with the appropriate root certificate. The Security Server software application is discussed in a separate manual.

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



3eTI 525V Wireless Access Point

Operation Mode:	Wireless AP/Bridge Mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer
Host Name:	default (192.168.254.254)

Wireless Configuration -> Security

Security Method: Dynamic Key Exchange

Security Server Name or IP address	
Security Server Port Number	1812
Password	
Key Type	128-bit AES key

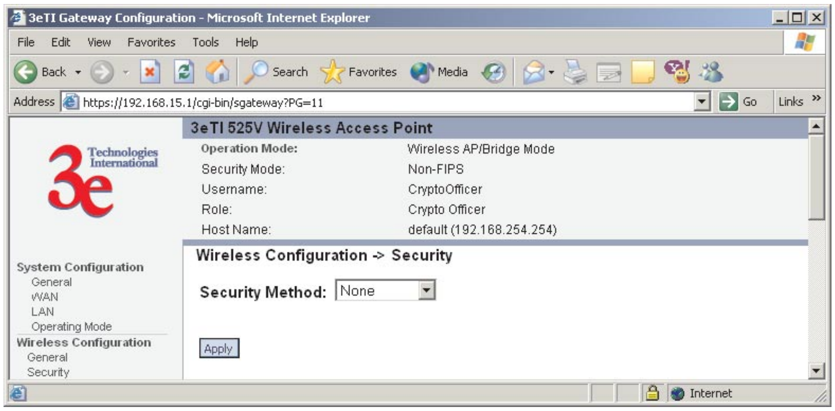
128-bit AES key
192-bit AES key
256-bit AES key
192-bit 3DES key

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

If you have the 3e-528 configured in non-FIPS mode, the security screens will look a bit different.

No Encryption (non-FIPS)

In order to the 3e-528 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.



3eTI Gateway Configuration - Microsoft Internet Explorer

Address https://192.168.15.1/cgi-bin/sgateway?PG=11

3eTI 525V Wireless Access Point

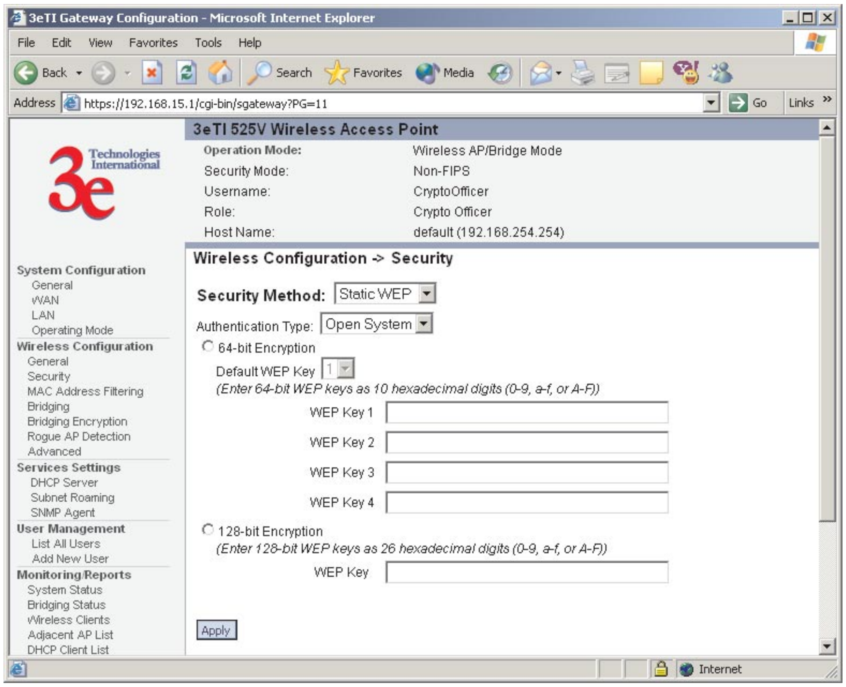
Operation Mode:	Wireless AP/Bridge Mode
Security Mode:	Non-FIPS
Username:	CryptoOfficer
Role:	Crypto Officer
Host Name:	default (192.168.254.254)

Wireless Configuration -> Security

Security Method: None

Static WEP Encryption (non-FIPS)

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



3eTI Gateway Configuration - Microsoft Internet Explorer

Address https://192.168.15.1/cgi-bin/sgateway?PG=11

3eTI 525V Wireless Access Point

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

Wireless Configuration -> Security

Security Method: Static WEP

Authentication Type: Open System

○ 64-bit Encryption

Default WEP Key 1

(Enter 64-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F))

WEP Key 1

WEP Key 2

WEP Key 3

WEP Key 4

○ 128-bit Encryption

(Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F))

WEP Key

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

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

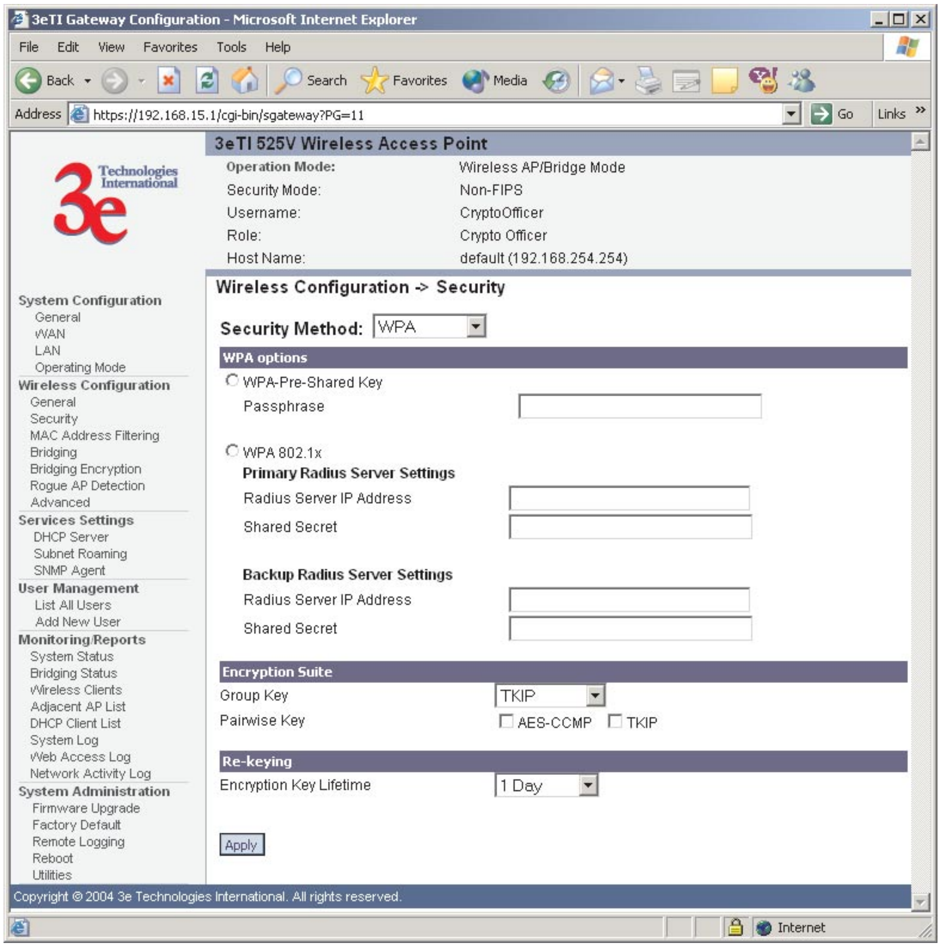
WPA (non-FIPS)

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

If you wish to use WPA on the 3e-528, 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.

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.



3eTI 525V Wireless Access Point

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

Wireless Configuration -> Security

Security Method: WPA

WPA options

○ WPA-Pre-Shared Key

Passphrase

○ WPA 802.1x

Primary Radius Server Settings

Radius Server IP Address

Shared Secret

Backup Radius Server Settings

Radius Server IP Address

Shared Secret

Encryption Suite

Group Key: TKIP

Pairwise Key: □ AES-CCMP □ TKIP

Re-keying

Encryption Key Lifetime: 1 Day

Copyright © 2004 3e Technologies International. All rights reserved.

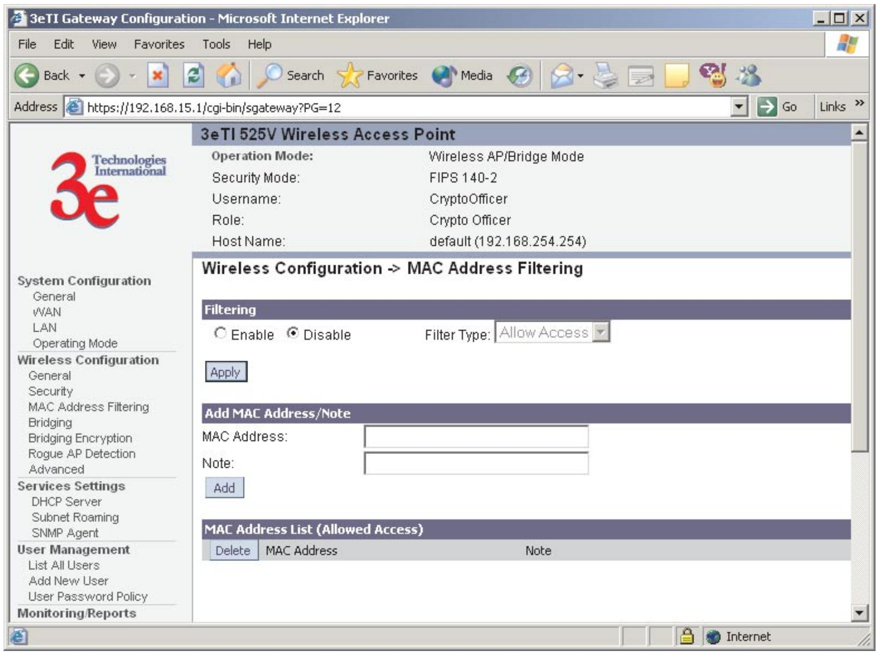
As an alternative, for business applications who have installed Radius Servers, select WPA 802.1x and input the Primary and Backup Radius Server settings. Use of Radius Server for key management and authentication requires that you have installed a separate certification system and each client must have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

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

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

MAC Address Filtering

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



3eTI 525V Wireless Access Point

Operation Mode:	Wireless AP/Bridge Mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer
Host Name:	default (192.168.254.254)

Wireless Configuration -> MAC Address Filtering

Filtering

○ Enable ● Disable Filter Type: Allow Access

Apply

Add MAC Address/Note

MAC Address:

Note:

Add

MAC Address List (Allowed Access)

Delete	MAC Address	Note

This works as follows:

- If **Filtering** is enabled and **Filter Type** is **Allow Access**, only those devices equipped with the authorized MAC addresses will be able to communicate with the access point. In this case, input the MAC addresses of all the PC cards that will be authorized to access this access point. The MAC address is engraved or written on the PC (PCMCIA) Card.
- If **Filtering** is enabled and **Filter Type** is **Disallow Access**, those devices with a MAC address which has been entered in the MAC Address listing will NOT be able to communicate with the access point. In this case, navigate to the report: **Wireless Clients** and copy the MAC address of any Wireless Client that you want to exclude from communication with the access point and input those MAC Addresses to the MAC Address list.

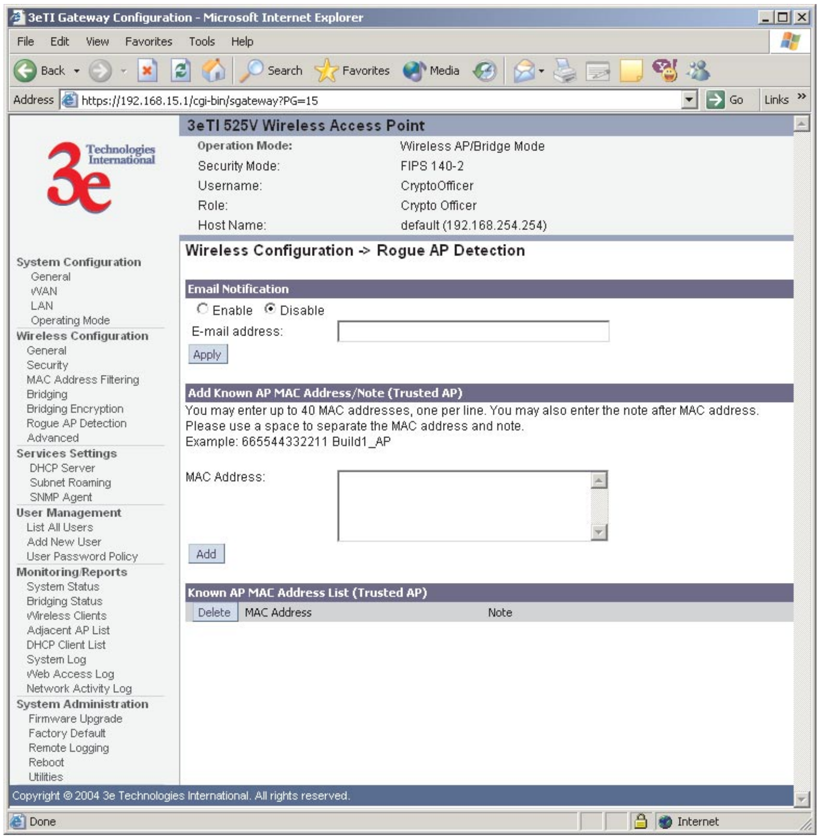
Bridging and Bridging Encryption

Bridging is covered in Chapter 5. If you will be deploying this 3e-528 as a bridge, follow the instructions in chapter five.

Rogue AP Detection

The Rogue AP Detection screen allows the network administrator to set up rogue AP detection. If you enable rogue AP detection, also enter the MAC Address of each AP in the network that you want the AP being configured to accept as a trusted AP. (You may add up to 20 APs.) Enter an email address for notification of any rogue or non-trusted APs. (The MAC Address for the 3e-528 is located on the **System Configuration—General** screen. You can also select the following filter options.

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



3eTI 525V Wireless Access Point

Operation Mode:	Wireless AP/Bridge Mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer
Host Name:	default (192.168.254.254)

Wireless Configuration -> Rogue AP Detection

Email Notification

○ Enable ● Disable

E-mail address:

Apply

Add Known AP MAC Address/Note (Trusted AP)

You may enter up to 40 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

MAC Address:

Add

Known AP MAC Address List (Trusted AP)

Delete	MAC Address	Note

Copyright © 2004 3e Technologies International. All rights reserved.

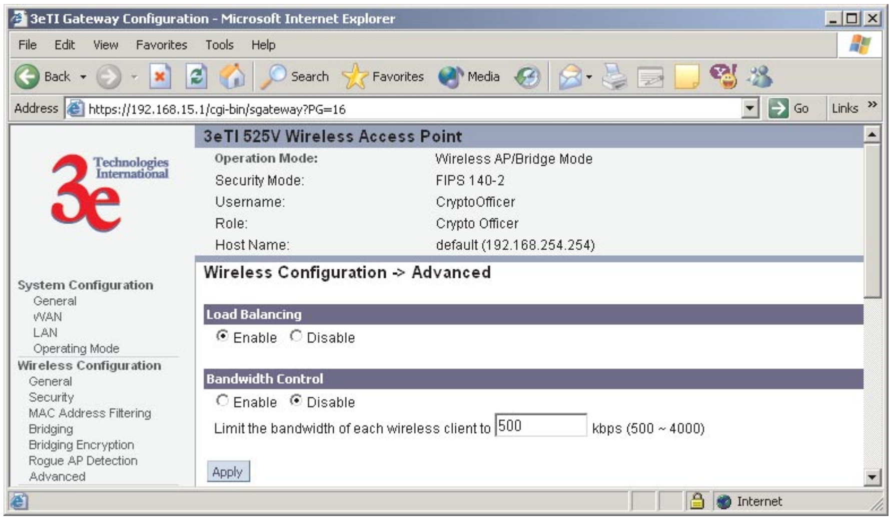
Advanced

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

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.

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

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



Address: https://192.168.15.1/cgi-bin/sgateway?PG=16

3eTI 525V Wireless Access Point

Operation Mode:	Wireless AP/Bridge Mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer
Host Name:	default (192.168.254.254)

Wireless Configuration -> Advanced

Load Balancing

● Enable ○ Disable

Bandwidth Control

○ Enable ● Disable

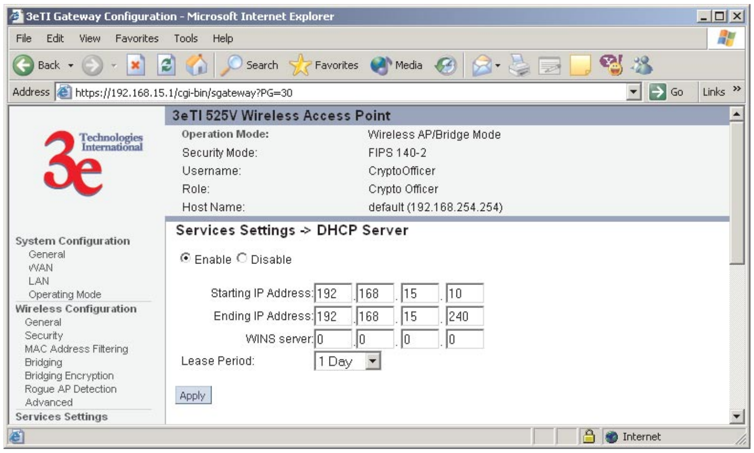
Limit the bandwidth of each wireless client to 500 kbps (500 ~ 4000)

Apply

Services Settings

DHCP Server

This screen allows configuration of the DHCP server function accessible from the Local LAN port. The default factory setting for the DHCP server function is enabled. You can disable the DHCP server function, if you wish. You can also set the range of addresses to be assigned. The Lease period (after which the dynamic address can be reassigned) can also be varied. It is not recommended that you disable this feature.


3eTI Gateway Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://192.168.15.1/cgi-bin/sgateway?PG=30
Go Links
Technologies International
System Configuration
General
WAN
LAN
Operating Mode
Wireless Configuration
General
Security
MAC Address Filtering
Bridging
Bridging Encryption
Rogue AP Detection
Advanced
Services Settings
Internet

3eTI 525V Wireless Access Point

Operation Mode:	Wireless AP/Bridge Mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer
Host Name:	default (192.168.254.254)

Services Settings -> DHCP Server

● Enable ○ Disable

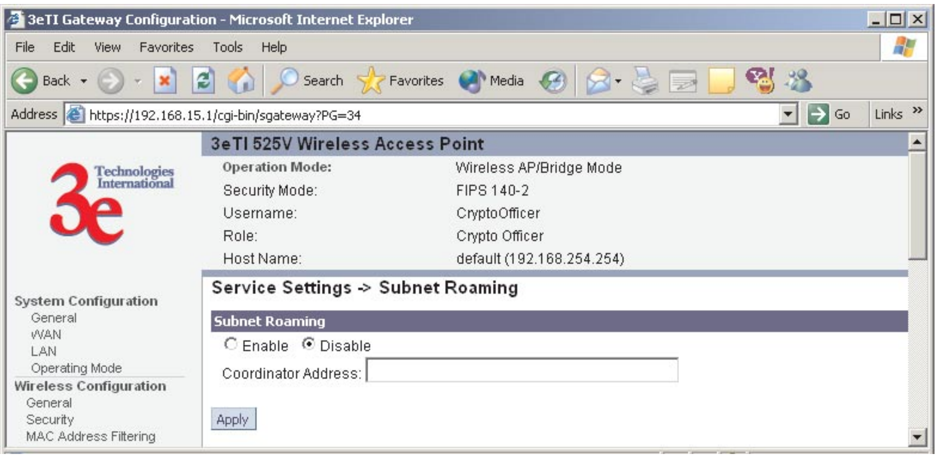
Starting IP Address: 192 . 168 . 15 . 10
Ending IP Address: 192 . 168 . 15 . 240
WINS server: 0 . 0 . 0 . 0
Lease Period: 1 Day

Apply

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

Subnet Roaming

The 3e-528 supports subnet roaming with 3eTI's subnet roaming coordinator server installed. Subnet roaming occurs when a user roams to an access point that is connected to a different subnet than its home subnet. If subnet roaming is supported by the wireless infrastructure, the client is able to continue its network connectivity without having to change its IP address. Therefore, to the mobile device, roaming is transparent and it will continue to function as if it is in its home subnet.


3eTI Gateway Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://192.168.15.1/cgi-bin/sgateway?PG=34
Go Links
Technologies International
System Configuration
General
WAN
LAN
Operating Mode
Wireless Configuration
General
Security
MAC Address Filtering

3eTI 525V Wireless Access Point

Operation Mode:	Wireless AP/Bridge Mode
Security Mode:	FIPS 140-2
Username:	CryptoOfficer
Role:	Crypto Officer
Host Name:	default (192.168.254.254)

Service Settings -> Subnet Roaming

Subnet Roaming

○ Enable ● Disable

Coordinator Address:

Apply