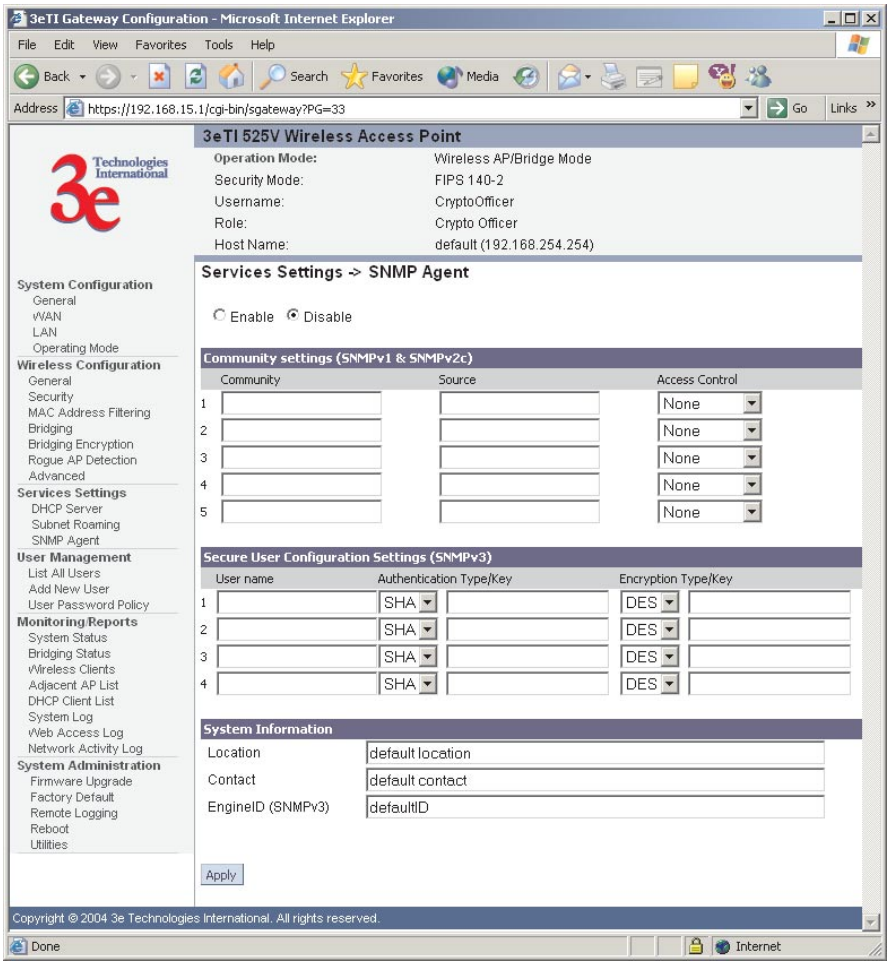
SNMP Agent

The SNMP Agent setup screen (shown on the previous 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-528's integrated SNMP agent software module translates the device's management information into a common form for interpretation by the SNMP Manager, which usually resides on a network administrator's computer.

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

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



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

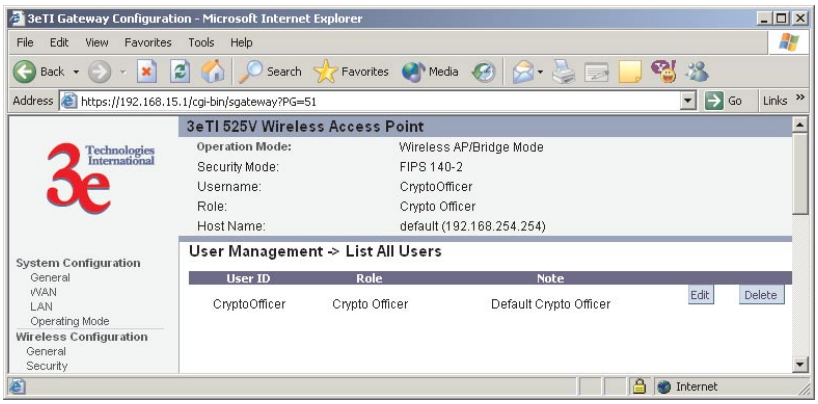
- **Community** –The Community field for Get (Read Only), Set (Read & Write), and Trap is simply the SNMP terminology for "password" for those functions.
- **Source** –The IP address or name where the information is obtained.
- **Access Control** –Defines the level of management interaction permitted.

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

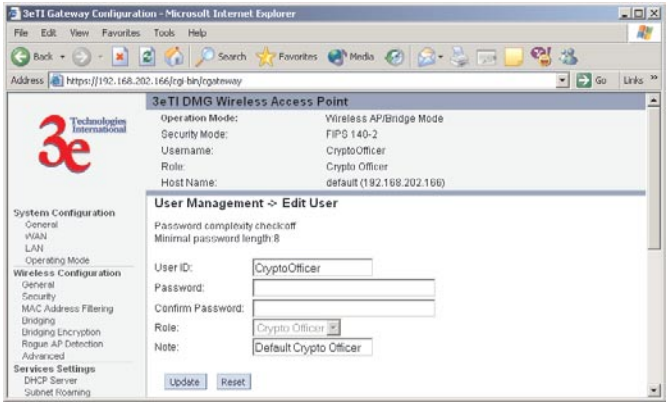
User Management

List All Users

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

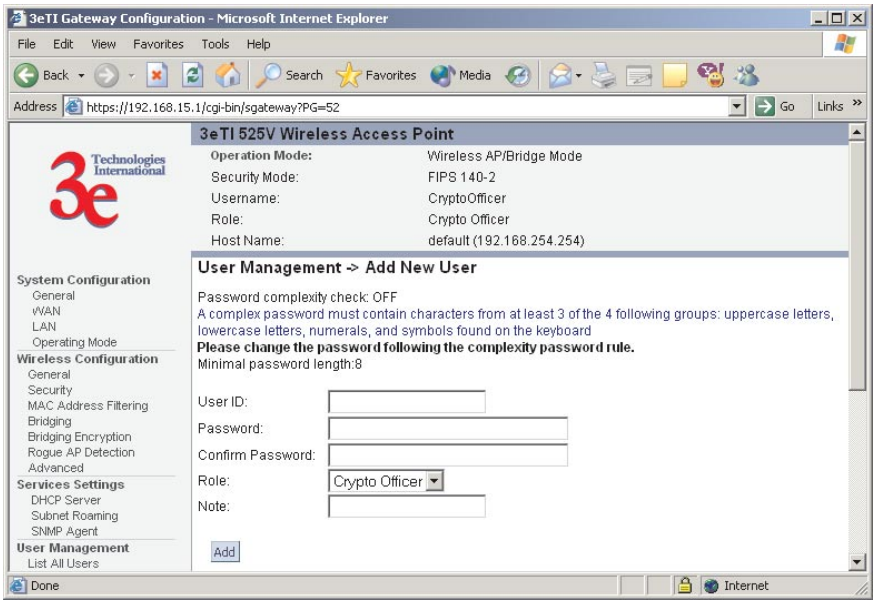


If you click on Edit, the **User Management — Edit User** screen appears. On this screen you can edit the user ID, password, role, and note fields.



Add New User

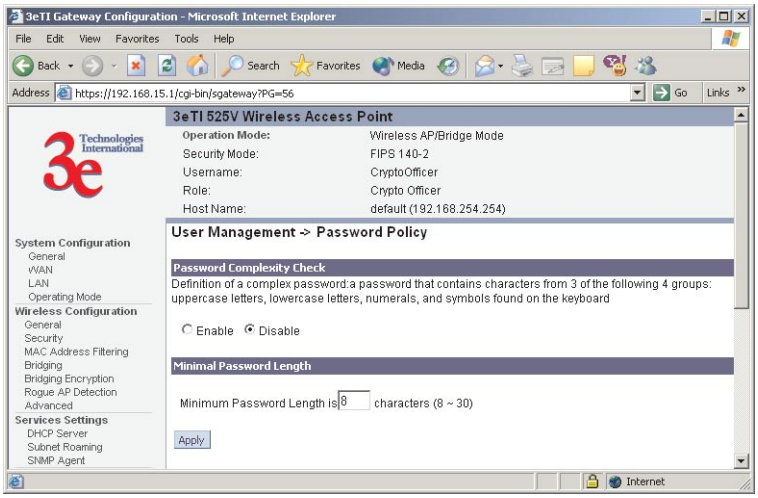
The **Add New User** screen allows you to add new administrators and crypto officers, assigning and confirming the password for the administrator.



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

Password Policy (FIPS Mode Only)

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

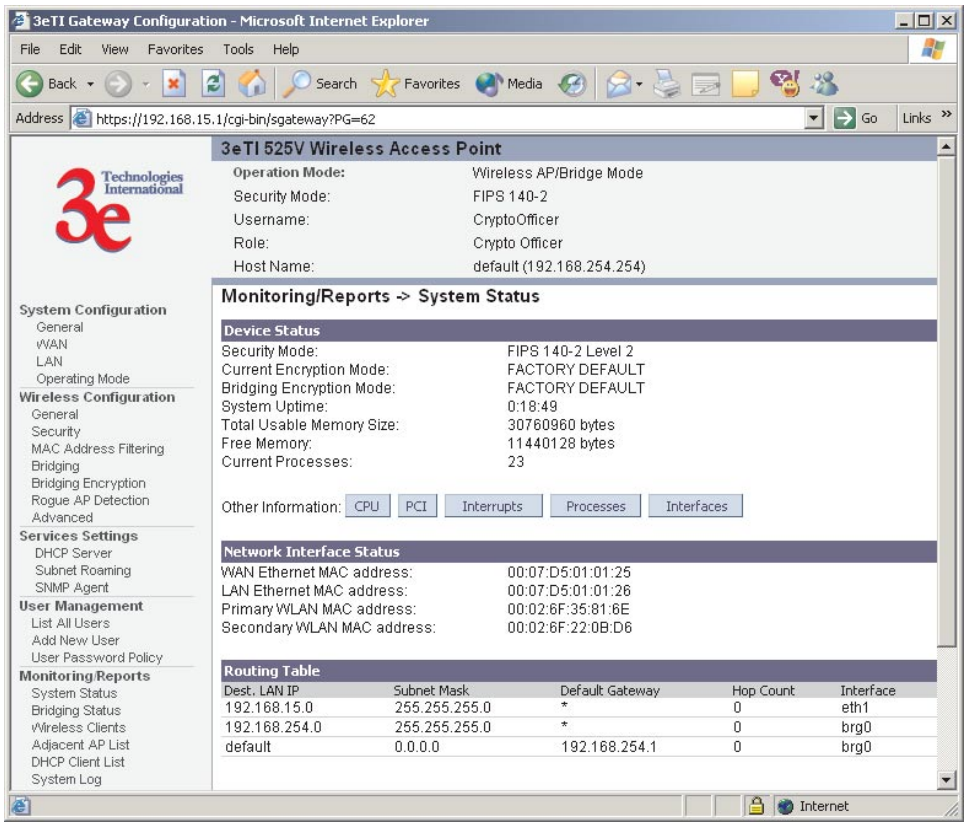


Monitoring/Reports

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

System Status

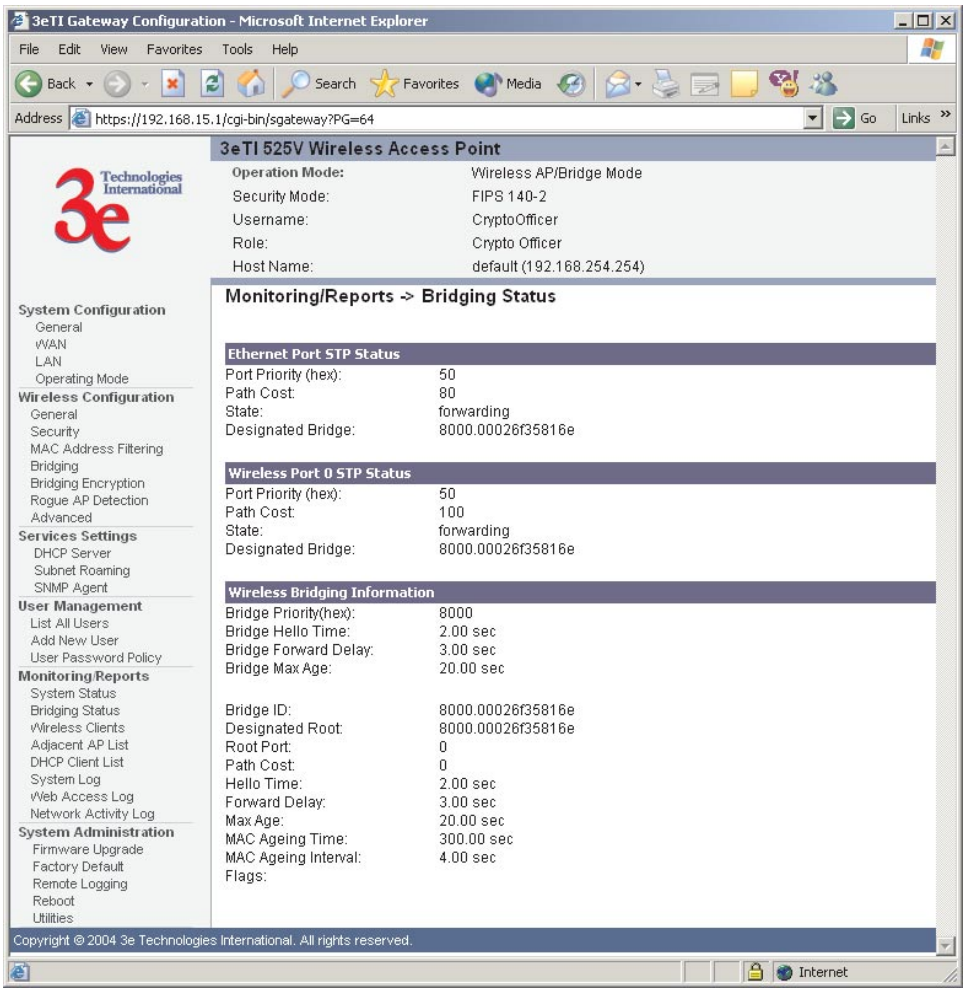
This screen displays the status of the 3e-528 Device and Network Interface Details and the Routing Table.



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

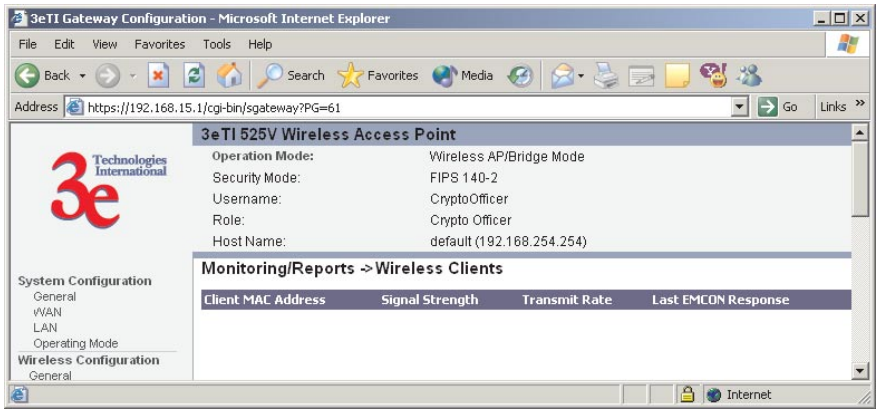
Bridging Status

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



Wireless Clients

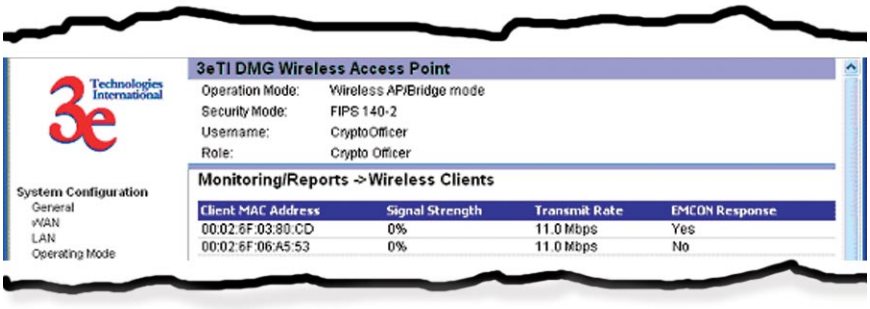
The Wireless Clients report screen displays the MAC Address of all wireless clients and their signal strength and transmit rate. The screen shown here emulates the FIPS 140-2 setup and contains a column for EMCON response. This column is not displayed in non-FIPS mode. The EMCON feature is only works with the 3e-010F Crypto Client in FIPS mode.



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

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

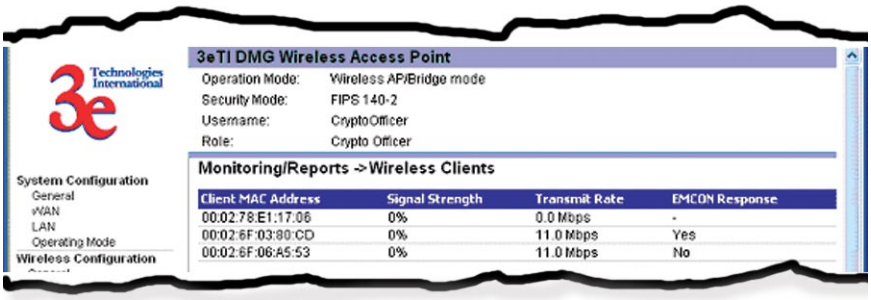
1. EMCON response when TX Power is disabled



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

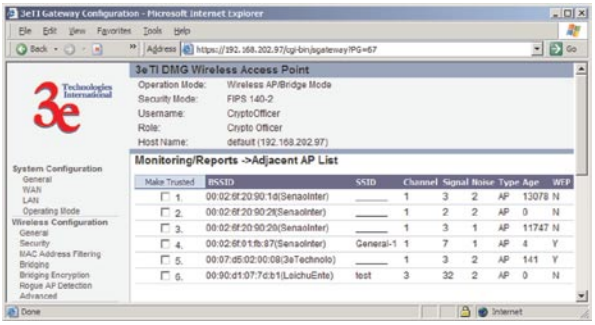
Once the transmit power is re-enabled and clients re-associate to the AP, EMCON information is maintained for them. If a new client that wasn't associated previously associates with the AP after the EMCON mode, its EMCON status appears as "-", which indicates the status record is not applicable.

2. EMCON response when TX Power is re-enabled



Adjacent AP List

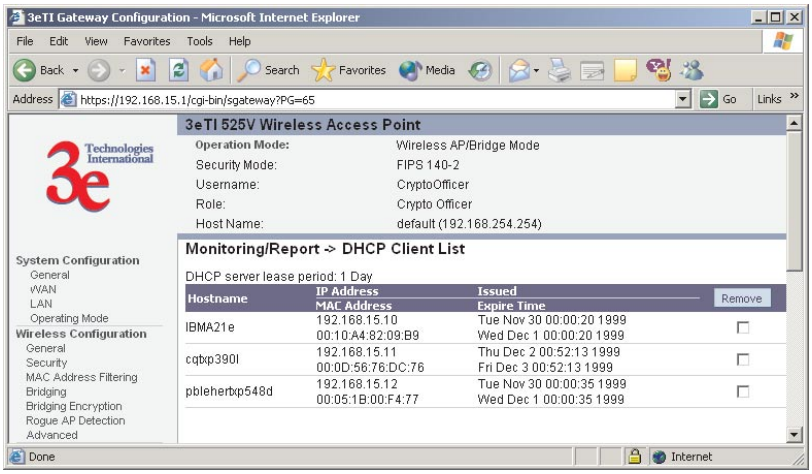
The **Adjacent AP** list shows all the APs on the network. If you select the check box next to any AP shown and click the **Make Trusted** button, the AP will thereafter be accepted by the 3e-528 as a trusted AP.



DHCP Client List

The DHCP client list displays all clients currently connected to the 3e-528 via DHCP server, including their hostnames, IP addresses, and MAC Addresses.

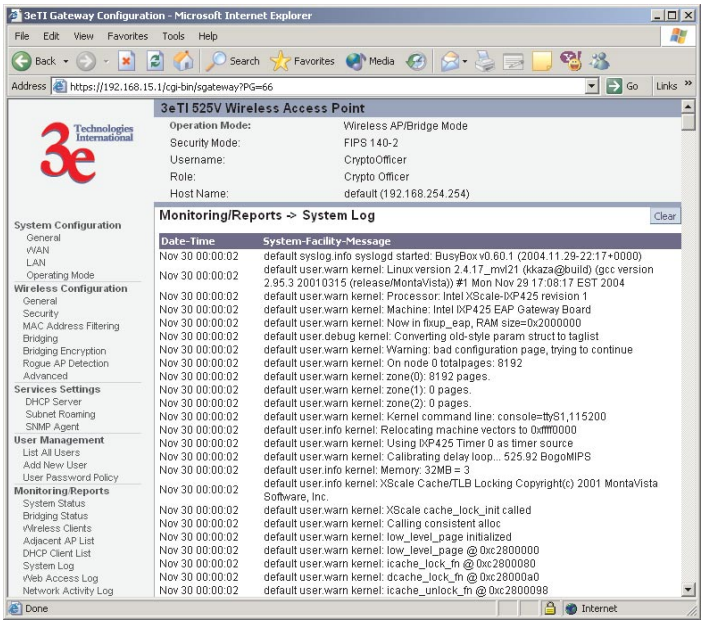
The DHCP Client list will continue to collect entries. To remove entries from the list, check mark the **Revoke Entry** selection and click **Remove** to confirm the action.



System Log

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

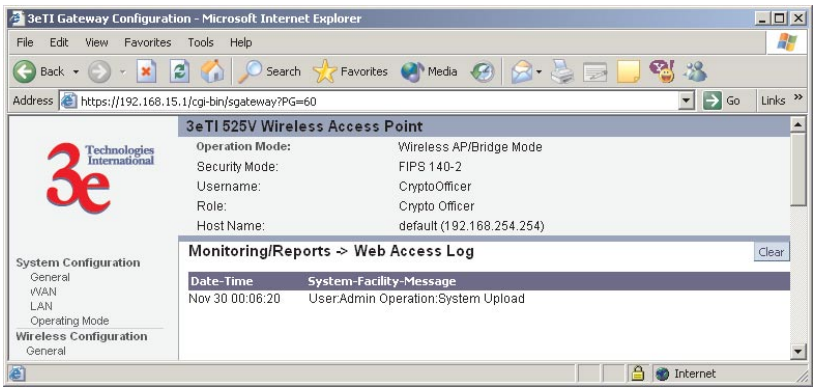
The System log will continue to accumulate listings. If you wish to clear listings manually, use the **Clear** button.



Web Access Log

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

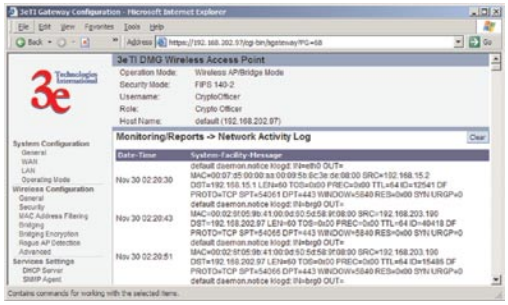
The Web access log will continue to accumulate listings. If you wish to clear listings manually, use the **Clear** button.



Network Activity Log

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

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



System Administration

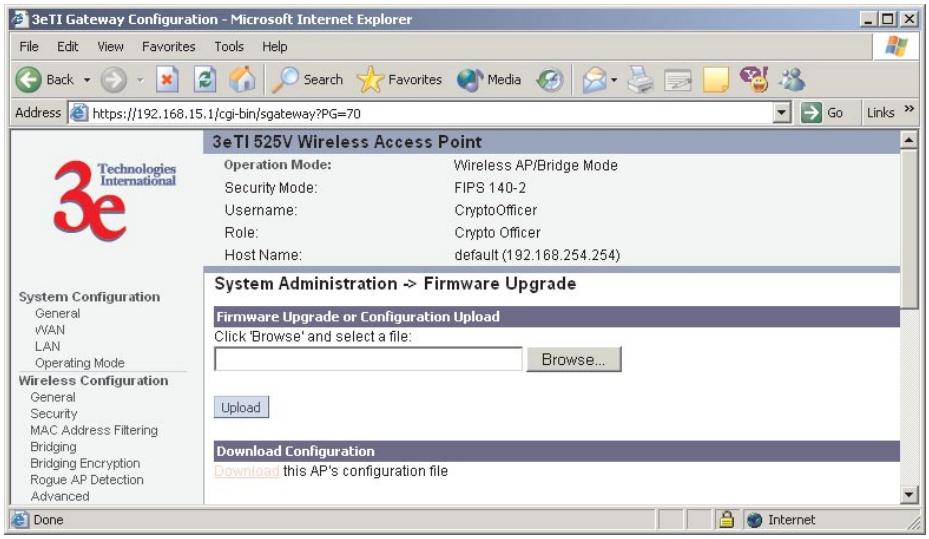
The System administration screens contain administrative functions. The screens and functions are detailed in the following section.

Firmware Upgrade

The System Upgrade utility is a functionality built into the 3e-528 for updates to the device's firmware as they become available. When a new upgrade file becomes available, find it and upload it to the 3e-528 from this screen.

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.

Only Crypto Officer can access this function.

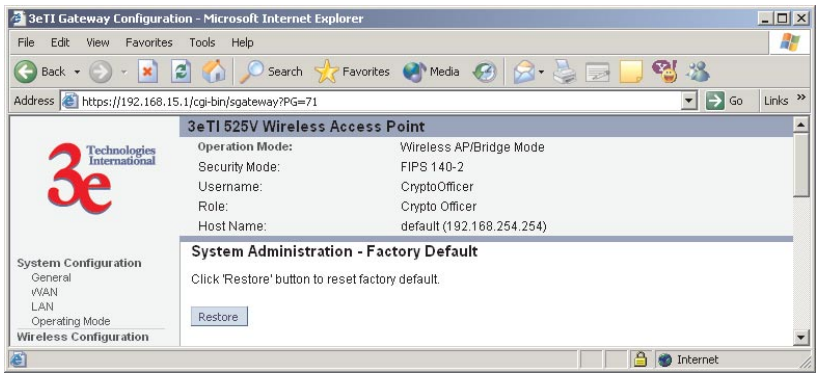


Factory Default

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

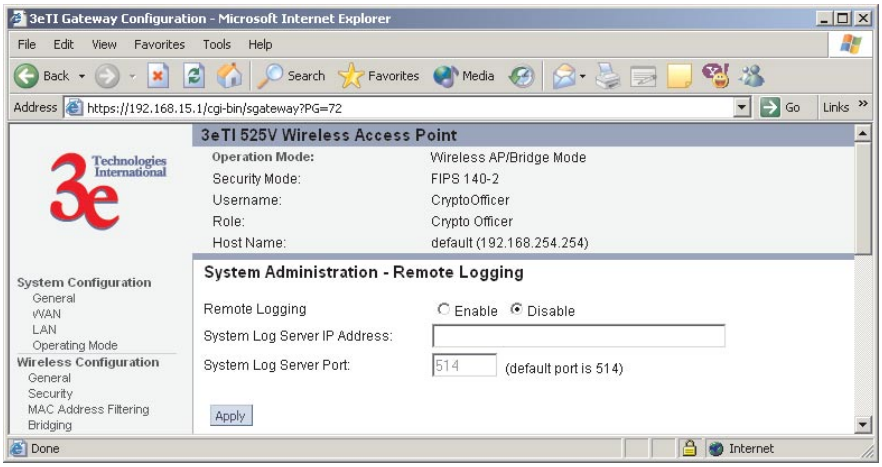
The "Restore" button is a fallback troubleshooting function that should only be used to reset to original settings.

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



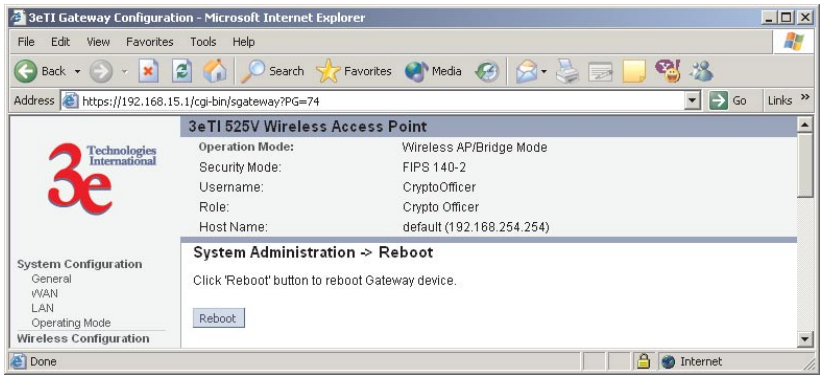
Remote Logging

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



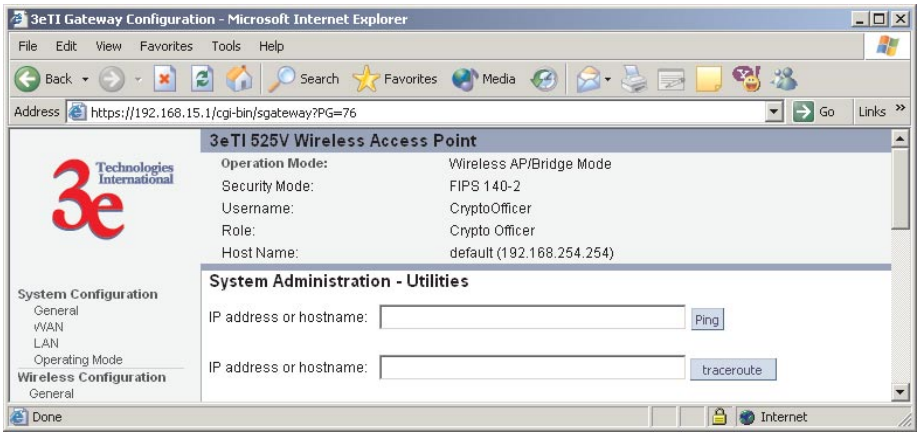
Reboot

The Reboot utility allows you to reboot the 3e-528 without changing any preset functionality. Both Crypto Officers and Administrators have access to this function.



Utilities

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



This page intentionally left blank.

Chapter 4: Video Configuration

The 3e-528 contains a video server that provides the capability to link four analog video cameras to the system. The video input is obtained from the cameras through the BNC connectors. The video image can be accessed through a built-in web server after the IP address of the video board has been configured. The instructions describing how to configure the IP address follow.

NOTE: The video server card is manufactured by Axis Communications. For detailed setup information, please refer to Axis 2400+ Admin Manual.

IP Address Configuration for the Video Server Card

The following is needed to set up the video server:

- Video camera
- PC
- 3e-528
- LAN cables
- MAC address of the video card server (This MAC can be found on a label outside of the unit)

Note: If using static IP address, the PC and the 3e-528 wireless video server (AP) need to have an IP configuration that allows them to communicate with each other.

1. Connect a PC to the WAN port using an Ethernet cable.
2. Using a unique IP address—one that is consistent with the system setup—configure the video server IP address by running the following command from the command prompt:

```
arp -s<desired IP address><MAC address of the video server>
```

For example:

```
Command Prompt
C:\>arp -s 192.168.1.15 00-40-8c-64-c5-cf
```

Note: This command needs to be run with two minutes after the unit has been turned on.

Soon after completing the "arp" command, run a "ping" command with packet length of 408 bytes to the IP address of the video server. The 3e-528 will need to be powered for the video server to be set up with the IP address.

Example:

```
Command Prompt
C:\>arp -s 192.168.1.15 00-40-8c-64-c5-cf

C:\>ping -t -l 408 192.168.1.15
```

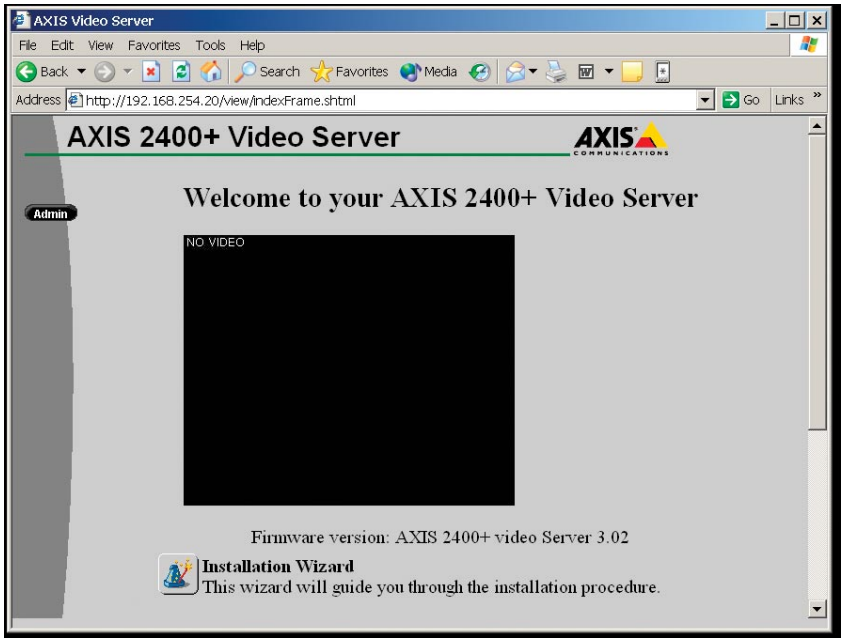
Once you get a reply from the video server, it is ready to be used. If the video server came with a preconfigured static IP address that is known, and you want to change it, you can use the Web-based administration tools provided by the video server.

Video Access

To access the video image, open a browser, and enter the IP of the video server in the address field. If this is the first time the video server is accessed from a PC using the Internet Explorer, the ActiveX installation dialog would come up if ActiveX is not installed. As shown below. The ActiveX component provides the video imaging capabilities to the PC, therefore the video image won't be displayed if ActiveX is not installed. If the browser being used is Netscape, ActiveX is not necessary.

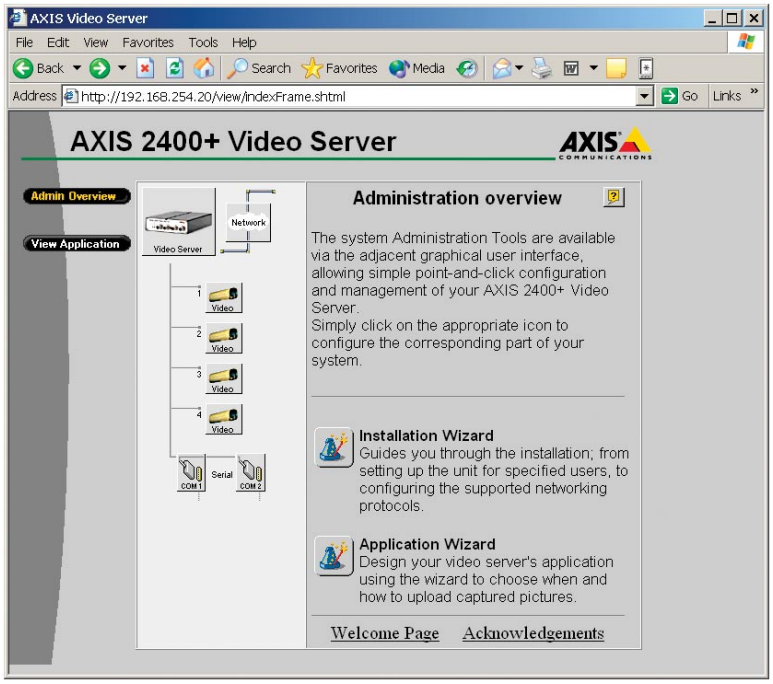
To enable the updating of images in Microsoft Internet Explorer, set your browser to allow ActiveX controls and perform a once-only installation of Axis' ActiveX component onto your workstation as prompted. If your working environment restricts additional software components, you can configure the video server to use a Java applet for updating the images. To do so you need to access the administration tools page, click on the "Video Server" icon, then on "Layout", and finally uncheck "Show Admin Button".

When accessing the video server interface for the first time, the Welcome Window would appear.



The Installation Wizard Icon  in this window walks you through the required steps to set up the video server completely. All of the steps covered with the wizard can also be accessed directly with the administration tools as detailed below.

Once the video has been completely setup the following window will appear when accessing it from the browser.

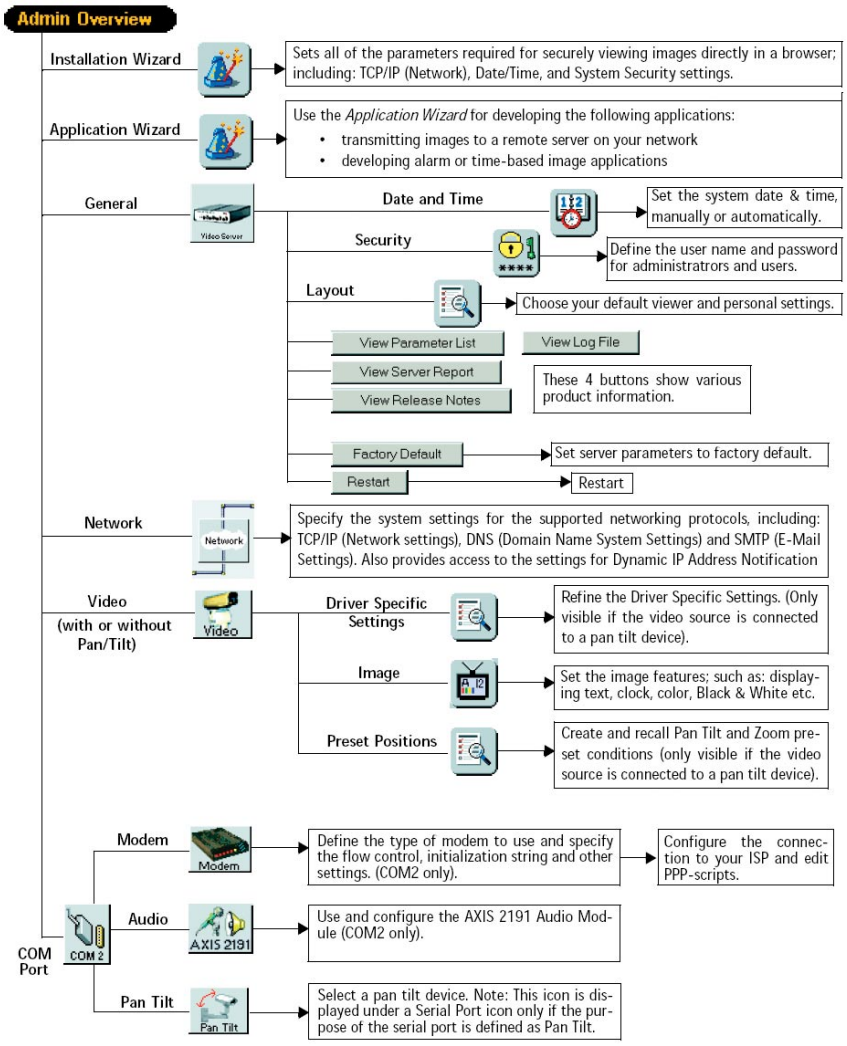


Video Administration Tools

The administration tools provide the means of setting up the video image as well as all the functionality related to the Video server, including security, network and serial (PTZ) settings.

To access the administration tools you need to know the video server address, as configured above. First, input the preconfigured video server address in the URL line on the browser. This will access the main Page for the Axis Server. (i.e. http://192.168.1.15). From there, the administration tools can be accessed by clicking in the "**Admin Overview**" button. Note: The security settings can be set so the "Admin Overview" button is not displayed in the main page. In that case the administration tools can be accessed by typing the IP address followed by "/admin/" (i.e. http://192.168.1.15/admin/).

Once you are logged in into the administration page (as shown below), the different components are displayed as icons on the page. To configure each component simply click on the respective icon.



The Admin Overview window gives an overview of the different components and features that can be set up through the user interface. Some of the most relevant features will be explained in more detail below.

More information can be obtained by clicking the on-line help icon. This button is available in all of the pages of the web-based interface, and provides basic information about the different settings and features.

Application Wizard

Through this wizard you can enable the 3e-528 to upload images to a remote server through FTP, or by SMTP. It allows image uploading based on alarms or by time intervals.

The image upload frequency can be set from fractions of second units to hour units, and also considering days of the week. SMTP is only permitted for a frequency slower than one image per minute.

When SMTP is checked, the image would be sent as a jpeg email attachment, while FTP would save the file in the specified upload path of the file structure of the FTP server.

Video Server General Settings

The Video Server icon gives access to the general settings for the video server, including: date & time, user accounts, web interface layout, log files, and the option to setting the unit to factory default values.

The video server card is supplied with one pre-configured Administrator user name and password, set to **root** and **pass**, respectively. The Administrator password must be changed to prevent unauthorized access to the Admin Tools and/or product images, as defined in the Security Settings.

Administrators can choose not to display the Administration Tools and other navigational buttons from the user interface. Selecting this feature ultimately means that the Administration tools can then only be accessed by entering the full Admin address into the browser's URL field; for example: http://192.168.21.10/admin/. To disable this button in the application page click on "Layout" and then uncheck "Show Admin Button".

Network Settings 

This button opens the Network Settings dialog, which allows configuration of the TCP/IP, DNS, SMTP, bandwidth usage, and dynamic IP address notification. This last one is used as a way to give notification of changes in the IP address when DHCP is used. You can be notified through FTP, SMTP or HTTP.

Video Settings 

This camera icon provides the means to adjust the video image resolution and compression as well as the detection of the specific video modulation. In addition to this, when the Pan/Tilt/Zoom driver has been installed, this dialog gives the ability to access the driver specific settings, such as preset positions, movement speed, and others, depending of what is supported by the camera or driver.

The image settings give the possibility to change the resolution of the image as well as the compression level for it. It also allows setting the image as color or black and white. The compression level can be set from 0 to 100. The lowest the compression level the better the quality. Keep in mind that less compression implies more data to be transmitted, hence more bandwidth is used.

Notes:

- A red cross X by the camera icon, it means that the is no camera connection, or that there is a problem with the camera or cable.
- A Camera-with-pan-tilt icon is displayed only if the camera for the chosen source is connected to a previously configured Pan Tilt Serial Port from the drop-down dialog.
- A Disabled icon indicates that the Administrator has disabled the video source from the Video Settings page.

COM Port Settings 

The COM port settings for the Video server are not used in the 3e-528 unit. The two serial ports provided by the Video Card are disabled. A serial server card is included in the system to provide four serial ports to control the pan/tilt/zoom function. The configuration of this serial server card is detailed in the next section.

Pan/Tilt/Zoom (PTZ) Configuration

The 3e-528 unit encloses a serial server card (Device Master RTS) that gives access to four serial ports over the network. These serial ports can be used for camera Pan/Tilt/Zoom purposes, or to connect other type of device with a different function.

When the driver for the serial server card (NS-Link) is installed in a host PC, four virtual COM ports are created in that PC. Each virtual COM port allows serial transfers, just like a normal COM port, to each serial port across the network. NS-Link is also available for Linux machines, providing TTY functionality just like a normal serial interface.

This way, a particular software driver for a specific camera, can access the camera through across the network seamlessly providing that such driver is designed to interface with the camera using a COM port of the PC.

The Device Master RTS is manufactured by Comtrol. To get more information, software updates, or drivers, please visit

http://www.comtrol.com/.

Configuration

The IP configuration of the serial server card can be changed from the preconfigured setting by accessing the device through a web interface or by establishing a Telnet connection. For both cases, the preconfigured IP address needs to be known.

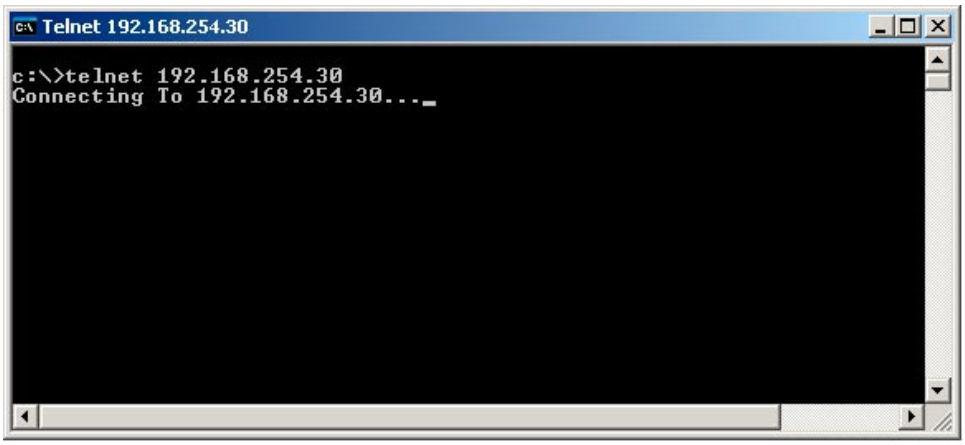
With Telnet access, only the IP configuration can be changed, while the web access provides more possibilities for configuration of the serial server card.

The preconfigured IP address for the serial server card is **192.168.254.30**. A PC connected to the WAN port of the 3e-528 can access the web interface of the serial card by typing the IP address on a web browser http://192.168.254.30. Please note that the IP configuration of the PC needs to be setup correctly. Likewise, the PC can access the serial server card by typing “telnet 192.168.254.30” on a command prompt.

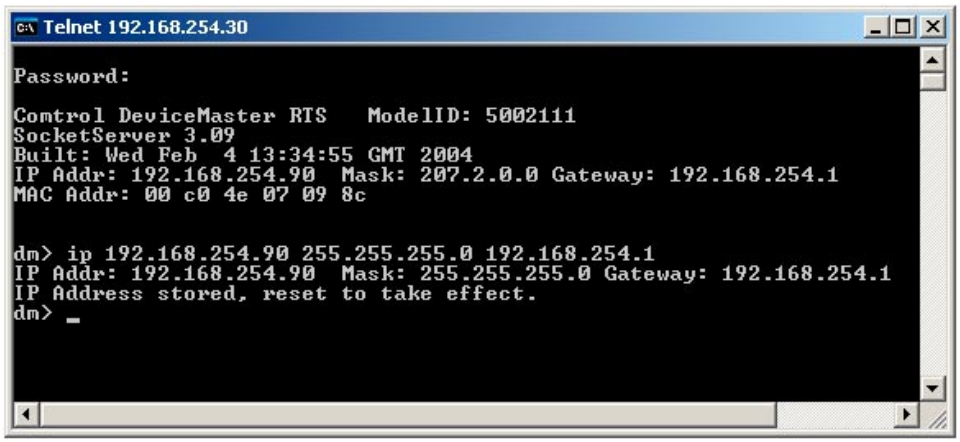
IP Setup through Telnet:

To set up a new IP address using telnet, a command prompt needs to be opened in the PC with access to the WAN port of the 3e-528.

1. In the command prompt type “telnet 192.168.254.30 [enter]”



2. The system will prompt for a password. By default, this password is blank, so just press the “enter” key.



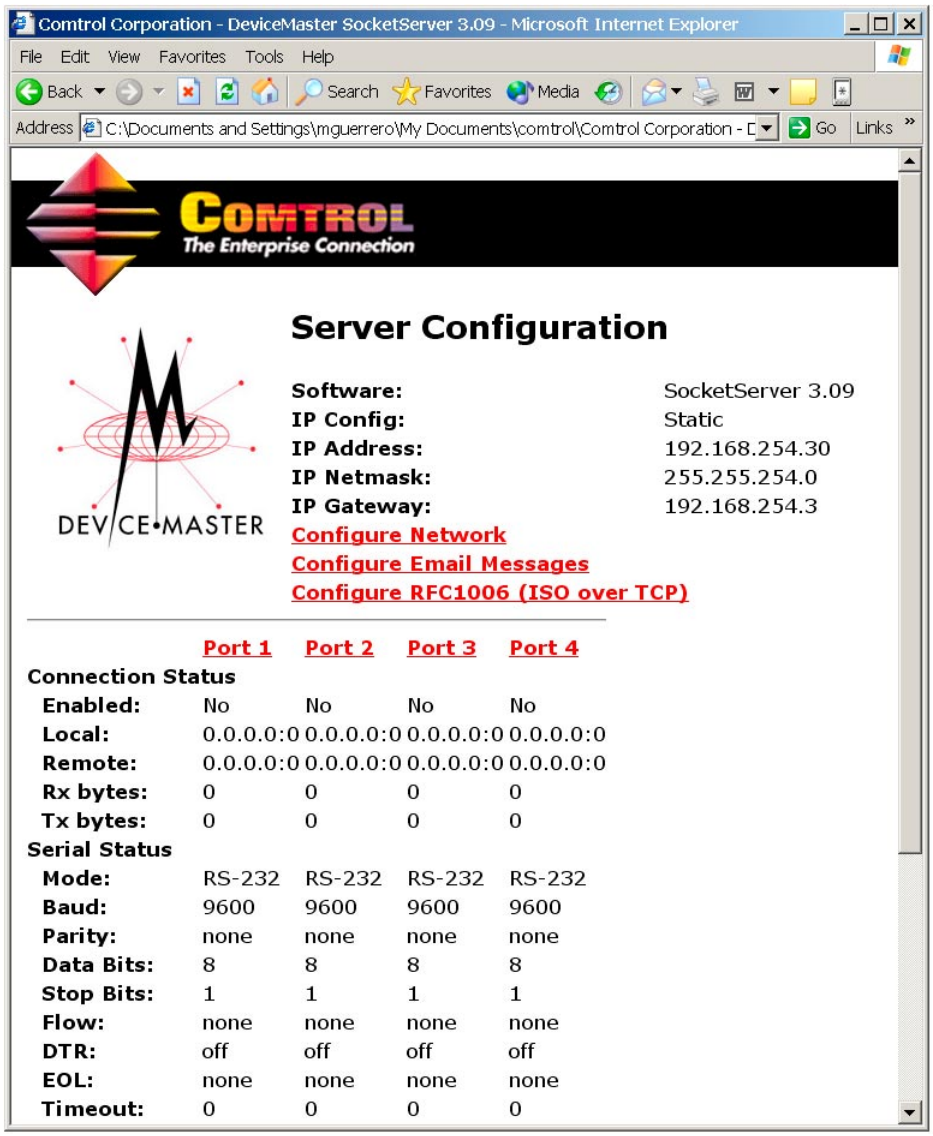
3. Once logged in the system, type the command “ip” follow by the IP address wanted, the subnet mask, and the gateway IP. Example: “ip 192.168.254.90 255.255.255.0 192.168.254.1 [enter]”

4. Once the system accepts this command, you need to enter “reset” so the new IP is finally configured. Note: after this Telnet won’t respond, so you need to hit “Crt+[“ and type “quit”.

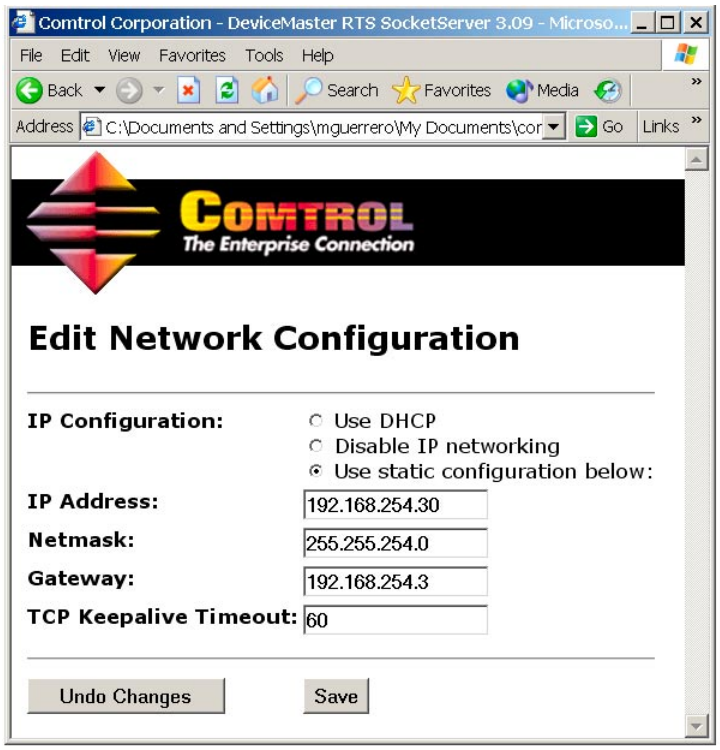
Setup through Web Interface:

A web browser can be used to set up a new IP address, and change other setting such as baud rate, parity bits, etc., in the serial server card.

1. Type the IP address of the serial port in the web browser address bar. (http://192.168.254.30 for the preconfigured IP address). A web page showing general information of the device, shown in the following picture, should open up:

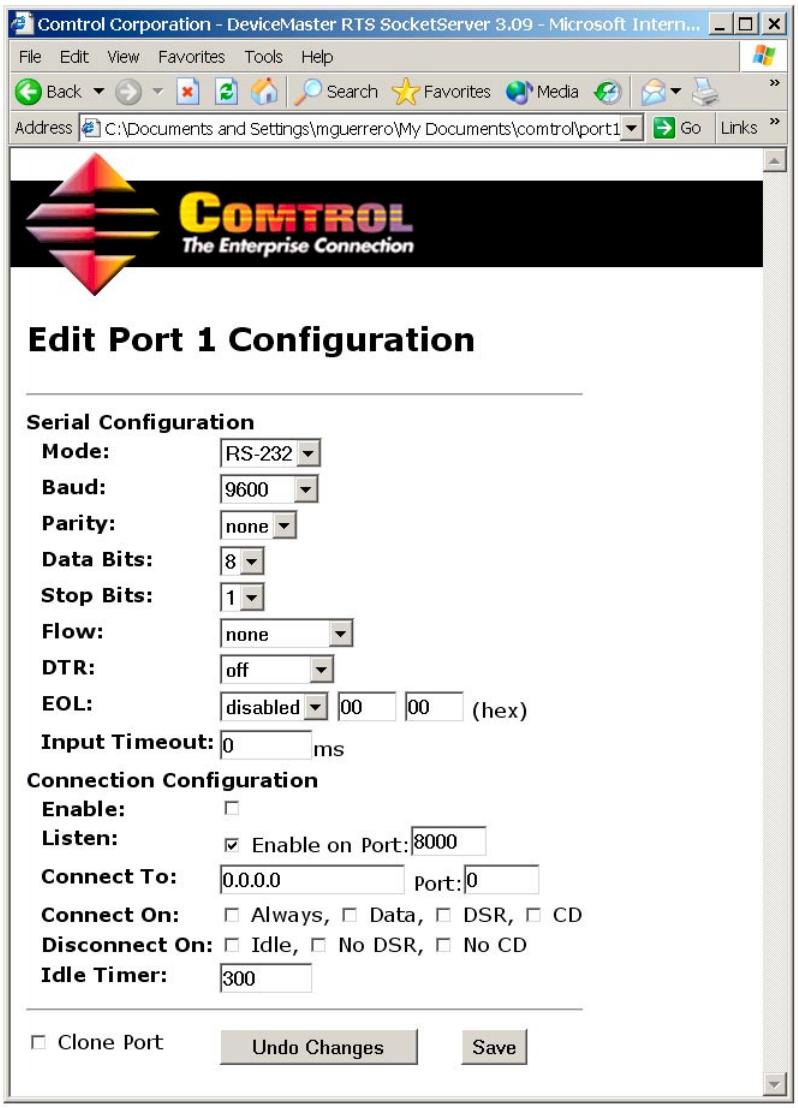


2. To configure the network settings click on the "Configure Network" link. A window like the one shown bellow should open up:



3. To change the IP address configuration, simply type in the new IP address, Netmask, and default Gateway and hit "save". Also, the serial server provides IP configuration using DHCP.

4. To configure the serial ports, click on de desired port link (e.g., **Port 1**) in the main page. This action should bring up the following web page:



5. This page lets the user change all the possible settings for the serial port including Baud Rate, Mode (RS-232/485/422), etc. For video server applications, only the upper part of the menu needs to be managed. The “Connection Configuration” should be whatever the default is, unless a serial tunnel through the net, with another serial server card as endpoint needs to be established for a special application. This tunnel is like a serial to serial interface through the network.

For further information on setting up the serial server card (DeviceMaster RTS) please refer to the Comtrol documentation enclosed with the 3e-528, or go the website http://support.comtrol.com/download.asp, and under “Product” select “Ethernet” and then DeviceMaster RTS.

This page intentionally left blank.

Chapter 5: Bridge Configuration

Introduction

In the 3e-528, wireless bridging is used to set up three independent wireless bridge connections. 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 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. The other two bridging ports, accessible from CONFIG 2 and CONFIG 3, possess dual 802.11b/g cards.

The wireless bridging function in the 3e-528 supports a number of bridging configurations. We discuss some of the most popular settings in this chapter:

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

When bridging is enabled, the 3e-528 allows remote access of video images as long as the bridging network and video server are properly set up.

Before setting up the bridges, all the WAN interfaces in the three bridging units need to be configured. By default, the IP address of the three bridging units are set to 192.168.254.254. They need to be set up to either get the IP address from DHCP or by assigning a static IP address to each of them.

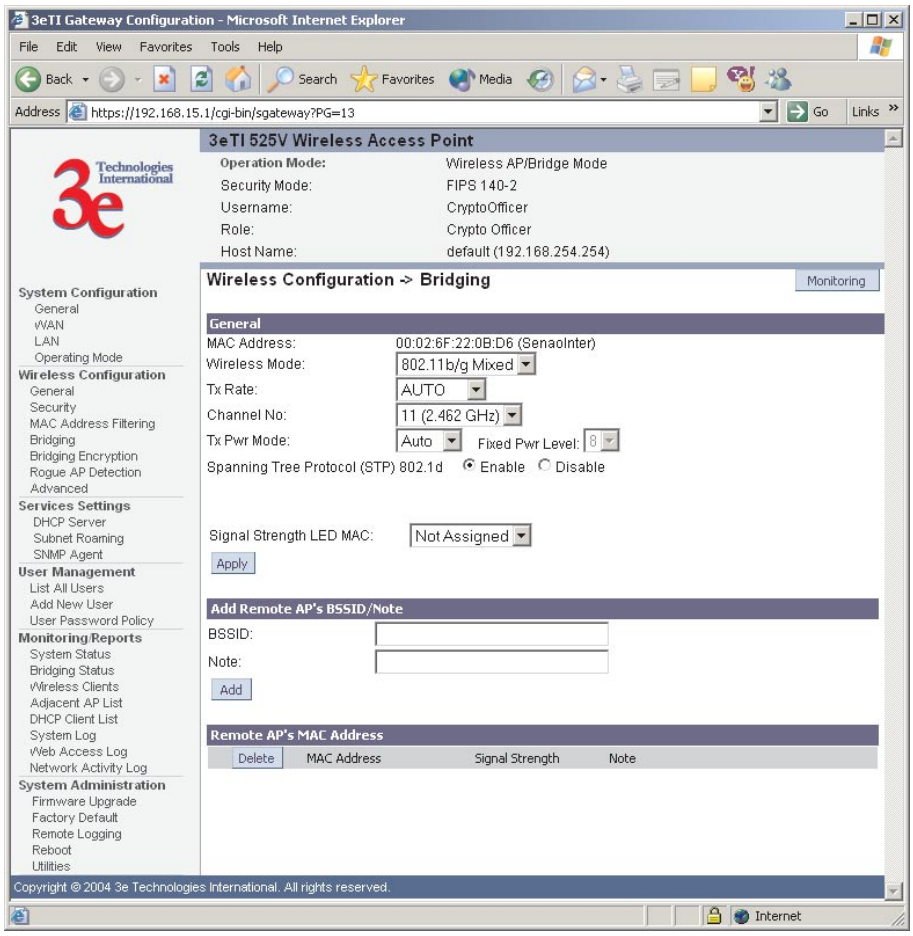
The access point is part of the first bridge and is accessible from CONFIG 1. Refer to Chapter 3. To set up the WAN interface in the other two bridging units, perform the same procedure using CONFIG 2 and CONFIG 3. After logging on to the GUI, the WAN settings can be changed by going to the System Configuration — WAN screen.

General Bridge Setup

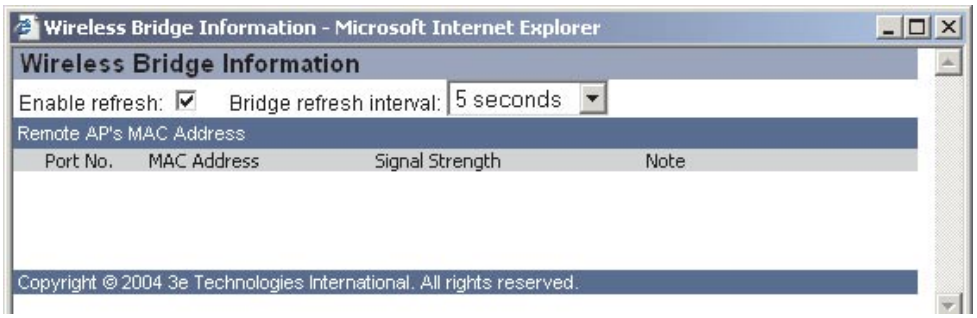
Wireless bridging is a function that is configured in addition to basic access point and/or video server setup. If you will be using the 3e-528 solely as a bridge, some of the settings you may have selected for access point use will not be necessary.

If setting up as a wireless bridge during initial setup, 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 Configuration** section of the navigation bar.

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



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.

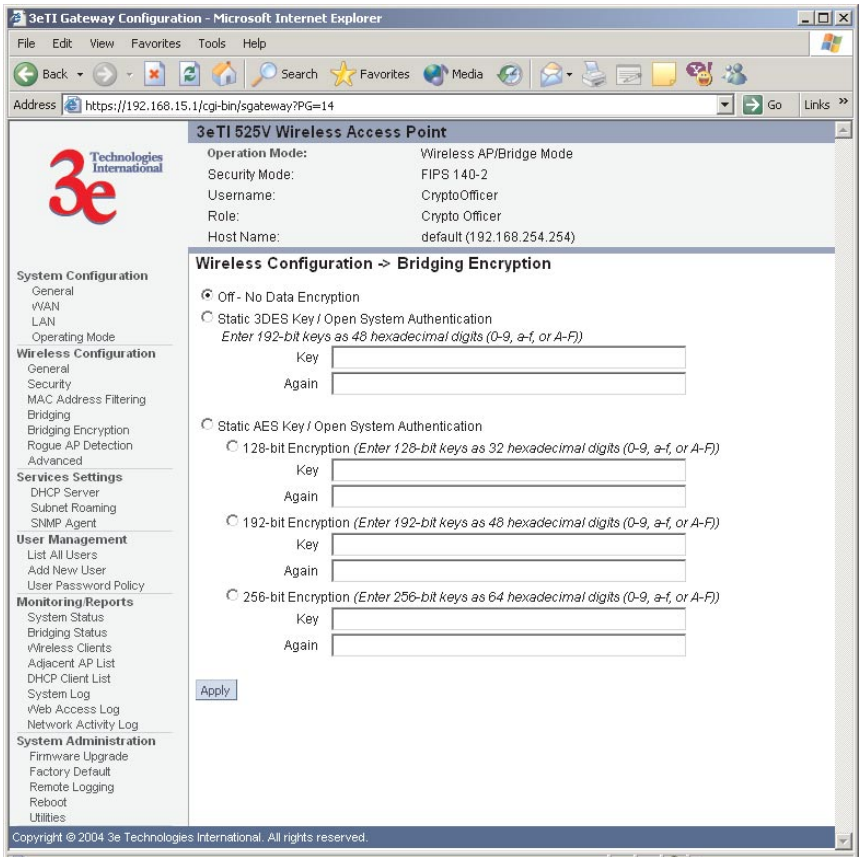


BRIDGING GENERAL SETTINGS OPTIONS		
Wireless Mode	802.11b/g Mixed	This is the only option available.
Tx Rate	AUTO, 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54 Mbps	When set to AUTO, the card attempts to select the optimal rate for the channel. If a fixed rate is used, the card will only transmit at that rate.
Channel No	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.
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 1-8 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 (only turns off bridge), 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, 6, 7, 8	Select a range when Tx Pwr Mode is set to FIXED. Level 1 is the shortest distance (Level 1=7dBm) and Level 8 is the longest (Level 8=15dBm)
Spanning Tree Protocol (STP)	Enable/Disable	Enable STP if there is any possibility that a bridging loop could occur. If you are certain that there is no possibility that a bridging loop will occur, then disable STP. The bridge will be more efficient (faster) without it. If you are not sure, the safest solution is to enable STP.

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.
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.

The **Wireless Configuration — Bridging 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 in order for communication to occur. And on this screen you can only select either a static 192-bit 3DES key or an AES key of either 128-bit, 192-bit, or 256-bit.

Important: The wireless bridge only starts to work after the encryption settings are applied. Even if no encryption is going to be used, you still need to select None and apply.



Bridge Antenna Alignment

To align the bridge antennas using 3e-528's software, perform the following steps:

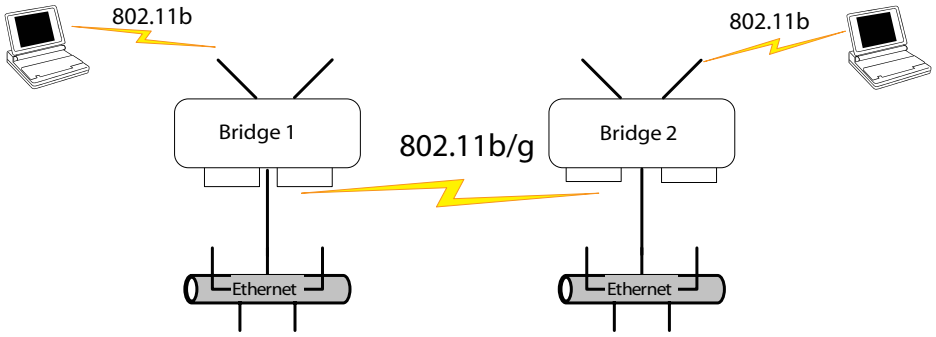
1. Go to the **Wireless Configuration — Bridging** screen. At the bottom of this screen select the bridge channel from the Remote AP's MAC Address list.
2. Click on the Monitoring button at the top of the screen and select enable refresh and set the bridge refresh interval.
3. View the Monitoring window while adjusting the bridge antenna direction to obtain the maximum signal strength.

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.



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

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

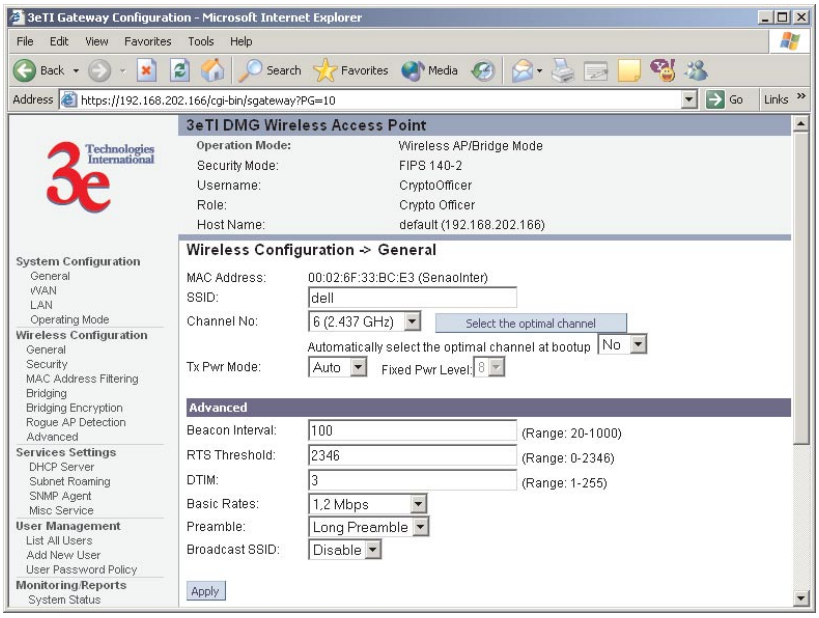
The following chart shows sample settings.

Point-to-Point Bridging Setup Guide

Direction	Bridge 1	Bridge 2
Wireless Configuration – Bridging		
Wireless Mode	802.11b/g Mixed	802.11b/g Mixed
Tx Rate	AUTO	AUTO
Channel No	11 (must be the same as Bridge 2)	11 (must be the same as Bridge 1)
Tx Power	Auto	Auto
Spanning Tree Protocol	Enable (or Disable if no bridging loop possible)	Enable (or Disable if no bridging loop possible)
Bridge signal strength LED port	Enter from list at the bottom of the screen	Enter from list at the bottom of the screen
BSSID	Add Bridge 2 MAC	Add Bridge 1 MAC
Wireless Configuration – Bridging Encryption		
Wireless Configuration – Bridging Encryption	Select appropriate key type/length and value. Must be the same key as Bridge 2.	Select appropriate key type/length and value. Must be the same key as Bridge 1.

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

First, navigate to the **Wireless Configuration — General** screen and select a channel number that does not conflict with the AP channel number. Leave the TX Pwr Mode in AUTO position at this time. If there is a wireless LAN on the AP WLAN card, information would be set as discussed in Chapter 3.



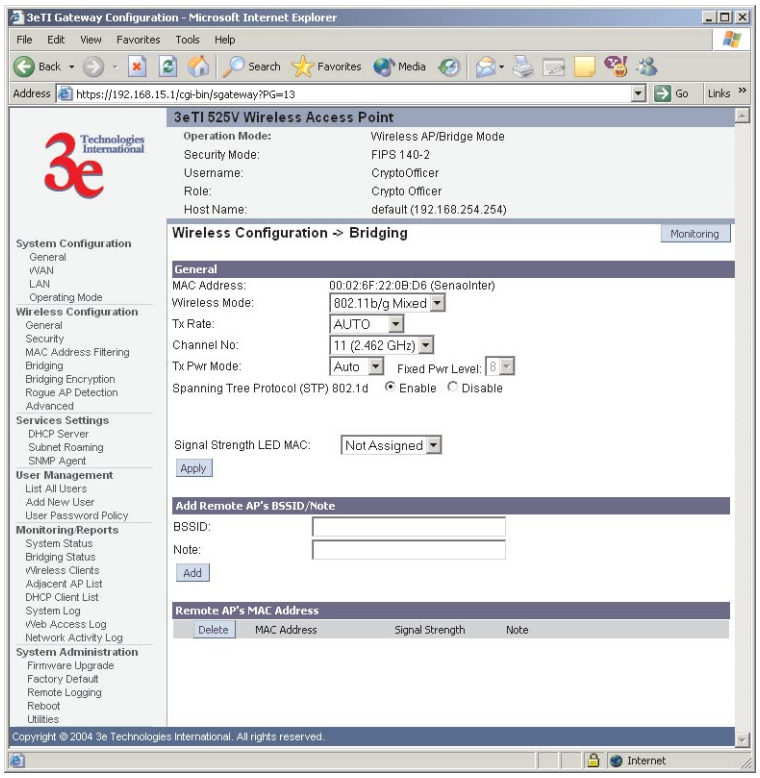
Navigate to the **Wireless Configuration — Bridging** screen.

In the first section: **General**, you will see the MAC Address of the bridging card. This is used as the BSSID on Bridge 2.

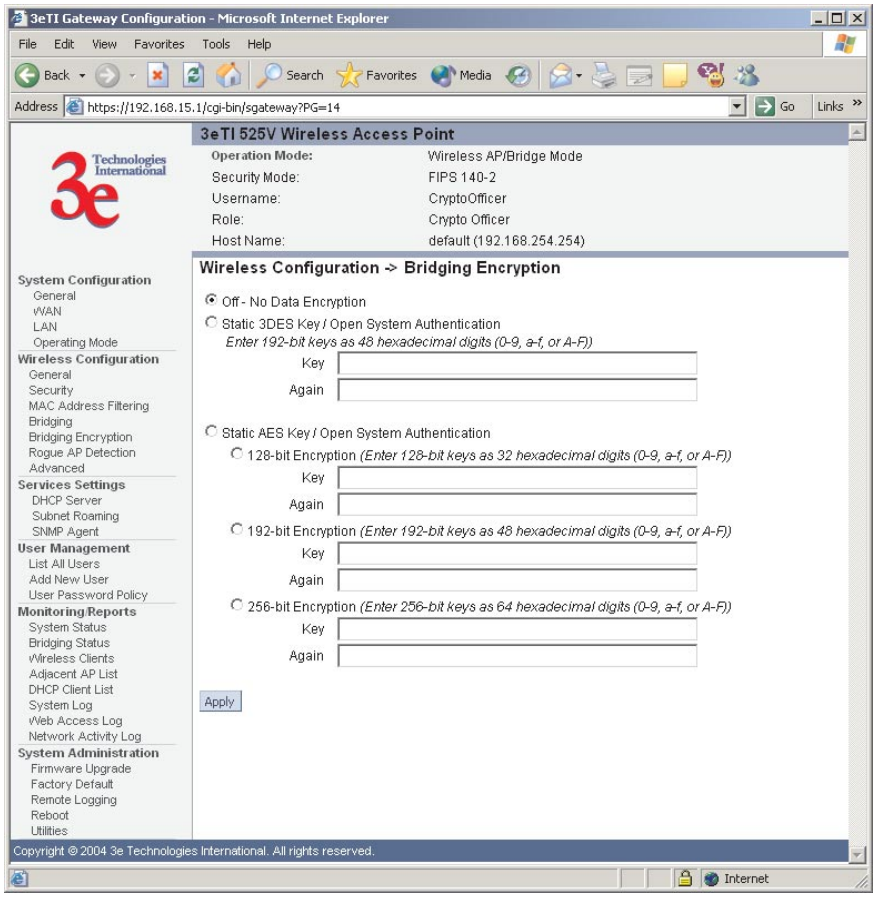
Wireless Mode is 802.11b/g Mixed. Set the **Tx Rate** to AUTO. **Channel Number** must be set the same for each bridge to communicate. **TX Pwr Mode** can be left on **Auto** unless the power needs to be regulated. Set **Spanning Tree Protocol** to **Enable** unless you are sure that there is no chance of a loop.

Bridge signal strength LED port allows you to set the number of one of the Remote APs which will be listed in section 3 at the bottom of the screen once the system is operational. Click **Apply** to accept your changes but remain on that screen.

In the second section on the **Wireless Configuration — Bridging** screen, add the BSSID of the remote bridge. The BSSID corresponds to that bridge's MAC address. Data entry is not case sensitive. You may also enter a note that defines the location of the remote bridge. Then click **Add** to accept. The remote bridge's BSSID will now appear in the third section of the page. If, at some time you wish to delete the entry, simply click the check box next to it and confirm by clicking **Delete**.



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



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

Configure Bridge 2 following the instructions given for Bridge 1 above.

Point-to-Multipoint Bridge Configuration

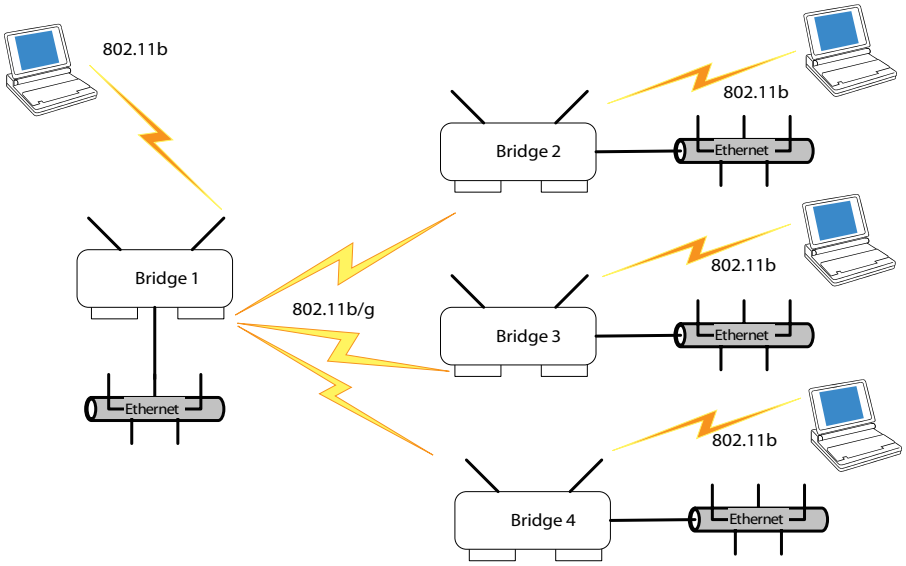
A point-to-multipoint configuration allows you to set up three or more 3e-528 access points in bridging mode and accomplish bridging between three or more locations wirelessly.

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

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

Because the 3e-528 has two separate WLAN cards, one for the AP and one for the Bridge, each bridge can have a WLAN on the 802.11b/g protocol with no loss of efficiency in bridging if you wish.

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



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

Point-to-Multipoint Bridging Setup Guide

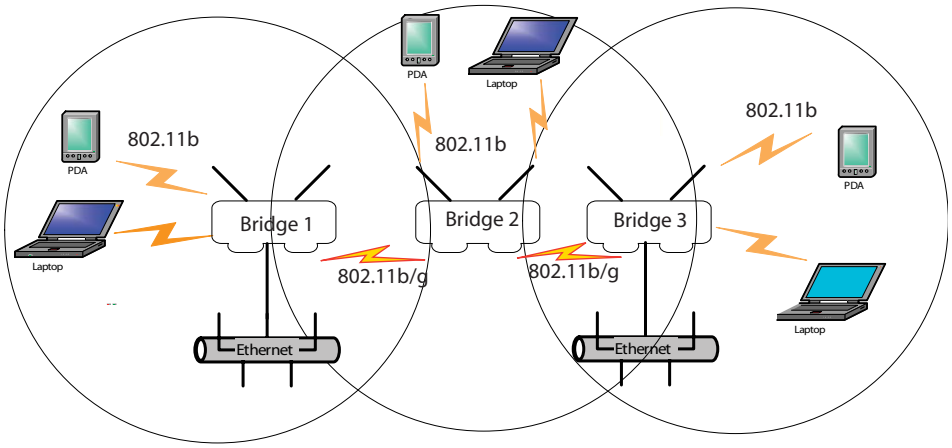
Direction	Bridge 1	Bridge 2 ~ n
Wireless Configuration – Bridging		
Wireless Mode	802.11b/g Mixed	802.11b/g Mixed
Tx Rate	AUTO	AUTO
Channel No	11 (must be the same as Bridge 2~n)	11 (must be the same as Bridge 2~n)
Tx Pwr Mode	Auto	Auto
Spanning Tree Protocol	Must be enabled	Must be enabled
Bridge signal strength LED port	Enter from list at the bottom of the screen	Enter from list at the bottom of the screen
BSSID	Add Bridge 2~n MAC	Add Bride 1 MAC
Wireless Configuration – Bridging Encryption		
Wireless Configuration – Bridging Encryption	Select appropriate key type/length and value. Must be the same key as Bridge 2~n.	Select appropriate key type/length and value. Must be the same key as Bridge 1.

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

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

Repeater Bridge Configuration

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



Repeater Bridging Setup Guide

Direction	Bridge 1	Bridge 2	Bridge 3
Wireless Configuration – Bridging			
Wireless Mode	802.11b/g Mixed	802.11b/g Mixed	802.11b/g Mixed
Tx Rate	AUTO	AUTO	AUTO
Channel No	11	11	11
Tx Power Mode	Auto	Auto	Auto
Spanning Tree Protocol (STP)	Enable (or Diable if no bridging loop possible)	Enable (or Diable if no bridging loop possible)	Enable (or Diable if no bridging loop possible)
Bridge signal strength LED port	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
BSSID	Add Bridge 2's MAC	Add Bridge 1's and Bridge 3's MAC	Add Bridge 2's MAC
Wireless Configuration – Bridging 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.

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.

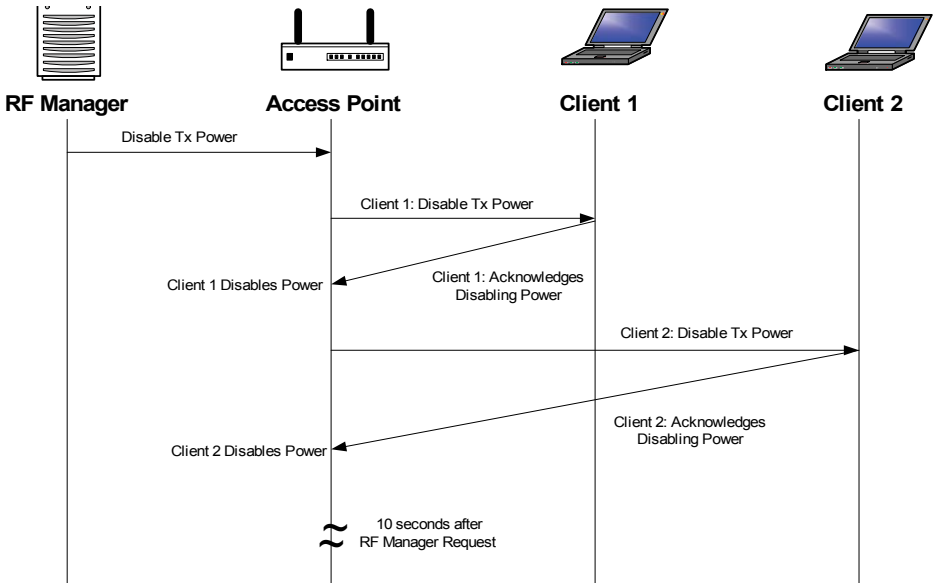
All other setup screens should be completed following the guidelines in Chapter 3.

This page intentionally left blank.

Chapter 6: The RF Manager Function

Introduction

This chapter addresses a function of the 3e-528 which facilitates remote management and programming of the Radio Frequency function for multiple 3e-528s located on a common network. This function allows you to remotely manage the Radio Frequency Power levels. For each AP selected, the RF Manager can remotely disable the AP's transmit power and, in turn, the transmit power of each client that is associated with it. The basic architecture is shown in the chart below.



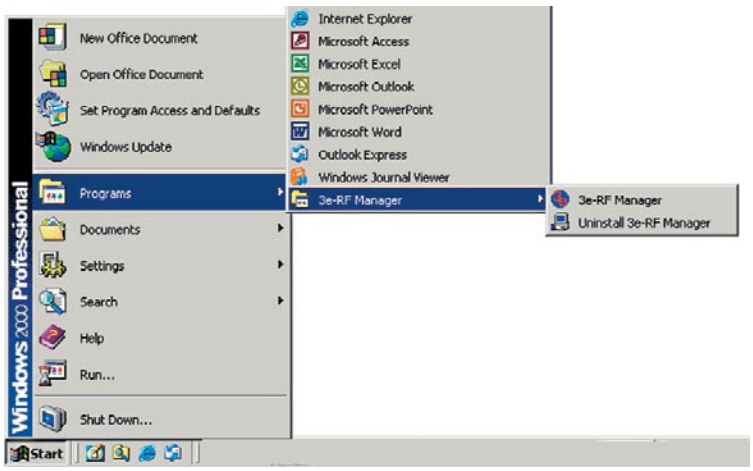
CAUTION: You can not use this utility if you are using dynamic IP address assignment on your wireless network. We recommend that you have your LAN Administrator set a range of static IP Addresses and that you change the WAN IP Address on each gateway to one of this range of IP Addresses as part of your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

How to Access the RF Manager Function

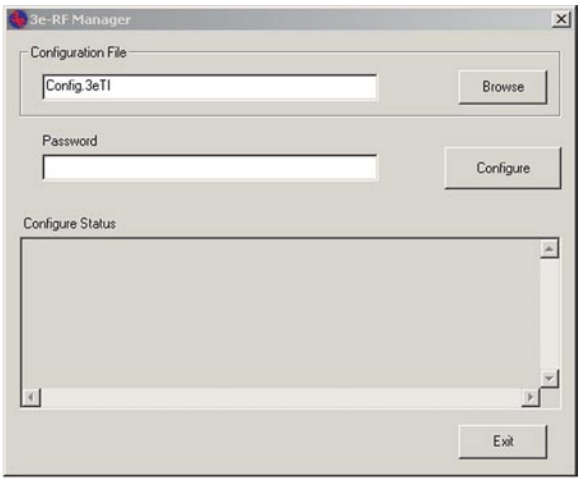
The RF Manager can be installed from the CD that came with the 3e-528 Install Kit to the desktop of anyone who needs to manage the wireless LAN.

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

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



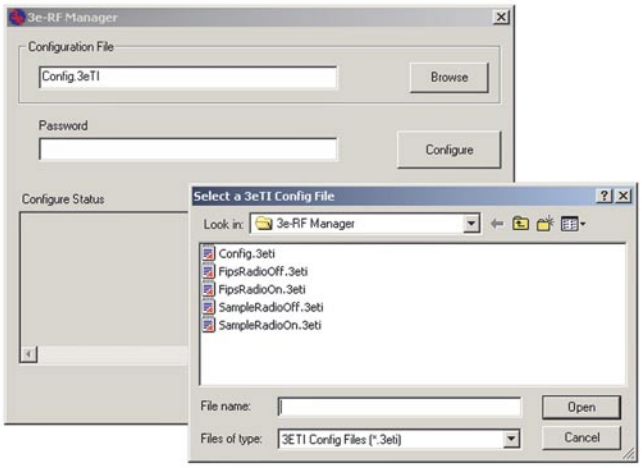
The main RF Manager screen will appear on your desktop.



How to Program the RF Manager

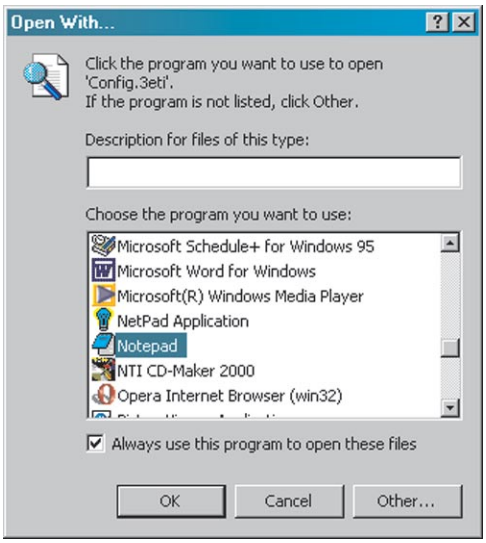
Before you are able to remotely manage access points, you need to program the RF Manager by putting the static IP Address of APs you want to manage in a configuration file.

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



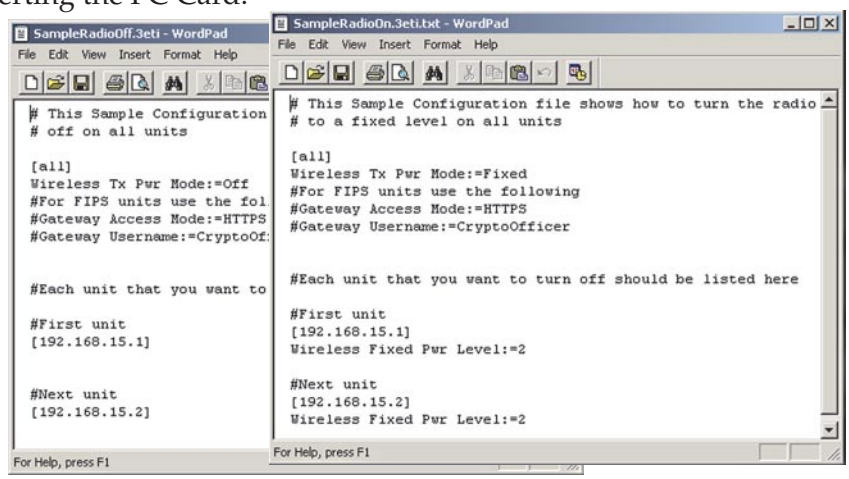
To see the contents of one of these files, simply right click the file name and select **Open** from the dropdown menu.

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



You can now edit the file by adding the IP addresses of the 3e-528s that you want to manage, each in a pair of brackets [ ].

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



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

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

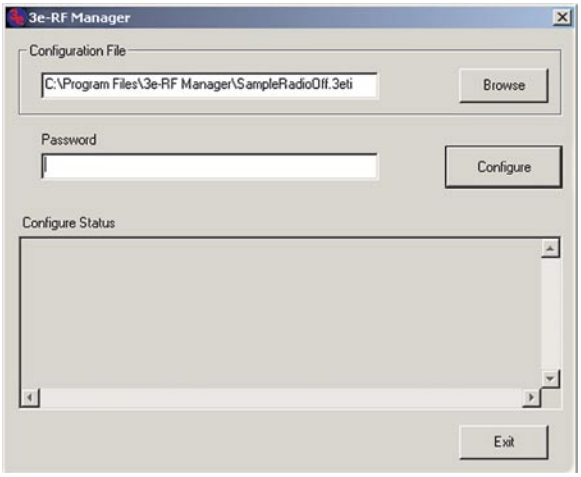
Sample of coding in SampleRadioOn.3eti file

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

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


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

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

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

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

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

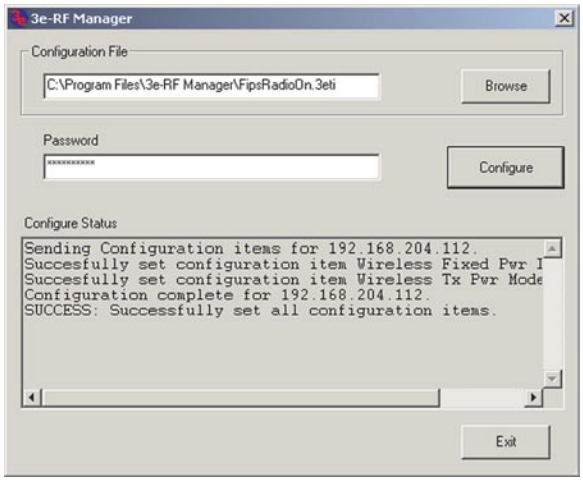
Now enter the Password for that group of APs.



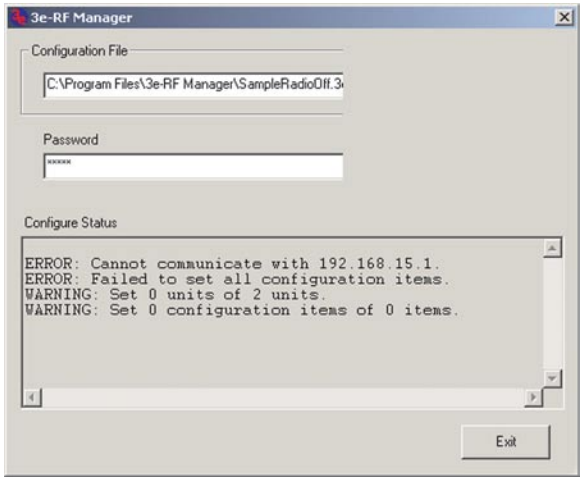
Finally, hit the **Configure** button.

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

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



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



Chapter 7: Technical Support

Manufacturer's Statement

The 3e-528 is provided with warranty. It is not desired or expected that the user open the device. If malfunction is experienced and all external causes are eliminated, the user should return the unit to the manufacturer and replace it with a functioning unit.

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

support@3eti.com

or visit our website at

www.3eti.com

Radio Frequency Interference Requirements

This device has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission's Rules and Regulations. The FCC IDs for the 3e-528 are QVT-5258 and QVT-WLAN_MP1. 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.

The maximum limit for an omni-directional antenna is 5dBi and the maximum limit for a directional antenna is 14dBi.

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

Channel Separation and WLAN Cards

There are four WLAN cards in the 3e-528. One is used for the Access Point function; the other three are used for the Bridges. Channel Separation is required to reduce interference between the AP and Bridge WLAN cards. It is recommended that you set the bridges to channels 1, 6, and 11, and set the AP to channel 3, 4, 8, or 9 in order to optimize performance.

Glossary

3DES

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

802.11

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

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

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

802.11g

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

Access Point

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

AES

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

Bridge

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

DHCP

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

NMS (Network Management Station)

Includes such management software as HP Openview and IBM Netview.

PC Card

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

PDA (Personal Digital Assistant)

A handheld device.

SNMP

Simple Network Management Protocol

SSID

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

TKIP

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

VPN (Virtual Private Network)

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

WLAN (Wireless Local Area Network)

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

WPA

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