#### **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.

🏄 3eTI Gateway Configurat	ion - Microsoft Internet Ex	plorer		_ 🗆 🗙
File Edit View Favorites	Tools Help			1
🕝 Back 👻 🕥 👻 📘	🗿 🏠 🔎 Search 🤞	😽 Favorites 🜒 Media 🧭 🍰 🗸	👌 🗔 📒 🖏 🚳	
Address 🙆 https://192.168.1	5.1/cgi-bin/sgateway?PG=33		💌 🏓 Go	Links »
System Configuration General VVAN	3eTI 525V Wireless Operation Mode: Security Mode: Username: Role: Host Name: Services Settings - C Enable © Disable	Access Point Wireless AP/Bridge Mode FIPS 140-2 CryptoOfficer Crypto Officer default (192.168.254.254) > SNMP Agent		
LAN Operating Mode Wireless Configuration General Security MAC Address Filtering Bridging Encryption Rogue AP Detection Advanced Services Settings DHCP Server Subnet Roaming	Community settings (SN Community 1 2 3 4 5	MPv1 & SNMPv2c) Source	Access Control None None None None None None None None	1
SNMP Agent User Management List All Users Add New User User Password Policy Monitoring Reports System Status Bridging Status Wireless Clients Adjacent AP List DHCP Client List System Lord	Secure User Configurati User name 1 2 3 4	on Settings (SNMPv3) Authentication Type/Key SHA  SHA  SHA  SHA  SHA  SHA  SHA  SHA	Encryption Type/Key DES  DES  DES  DES  DES  DES  DES  DES	
System Log Web Access Log Network Activity Log System Administration Firmware Upgrade Factory Default Remote Logging Reboot Utilities	System Information Location Contact EngineID (SNMPv3) Apply	default location default contact defaultID		
Copyright © 2004 3e Technologi	es International. All rights reser	rved.		~
Done Done			🔒 💣 Internet	1.

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.

🗿 3eTI Gateway Configura	tion - Microsoft Interne	t Explorer			_ 🗆 ×
File Edit View Favorites	s Tools Help				-
🕝 Back 🔹 💮 🕤 📓	💈 🏠 🔎 Search	Ravorites 🕐 Med	ia 🥝 🍰 🍓 🖂	📃 🚭 🤹	
Address 🙋 https://192.168.1	5.1/cgi-bin/sgateway?PG=5	51		💌 🔁 Go	Links '
	3eTI 525V Wirele	ss Access Point			4
Technologies	Operation Mode:	Wireless	s AP/Bridge Mode		
International	Security Mode:	FIPS 14	0-2		
70	Username:	CryptoO	fficer		
	Role:	Crypto C	fficer		
	Host Name:	default (	192.168.254.254)		
	User Manageme	nt -> List All Users			_
System Configuration General	User ID	Role	Note		
WAN LAN	CryptoOfficer	Crypto Officer	Default Crypto Officer	Edit	Delete
Wireless Configuration General Security					
6)				🔒 🍘 Internet	

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.

3eTI Gateway Configura File Edit View Favorites	tion-Microsoft Intern : Tools Help	et Explorer	
🕝 Back + 🕥 - 📘	🗟 🏠 🔎 Search	📩 Favorites 🜒 Media 🥝 🍰 头 🗔 🛄 🖏 %	
Address a https://192.168.2	02.166/cgi-bin/cgateway	💌 🄁 Go	Links <sup>30</sup>
	<b>3eTI DMG Wirel</b>	ess Access Point	
3e	Operation Mode: Security Mode: Username: Role: Host Name:	Virteless AP/Bridge Mode F/PO 14-0-2 CryptoOfficer CryptoOfficer Officer 196 202.166)	
System Configuration Control VAN LAN Derating Mode Wirkeless Configuration General Socurby MAC Address Filtering Dridging Encryption Rogun AP Detection Advanced	User Managem Password complexi Minimal password b User ID: Password: Confirm Password: Role: Note:	ent ~ Edit User y checkoff mgth 8 CryptoOfficer CryptoOfficer Default Crypto Officer	
Services Settings DHCP Server Subnet Roaming	Update Reset	1	

#### 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.

🚈 3eTI Gateway Configura	tion - Microsoft Interne	et Explorer	×
File Edit View Favorite	s Tools Help	A	1
🕝 Back 🔹 🕥 👻 💌	🗿 🏠 🔎 Search	👷 Favorites 🜒 Media 🤣 🍰 🈓 🔜 🌄 🦓 🖄	
Address 🙆 https://192.168.	15.1/cgi-bin/sgateway?PG=	=52 🗾 🔁 Go Links	5 »
	3eTI 525V Wirele	ess Access Point	-
A Technologies	Operation Mode:	Wireless AP/Bridge Mode	
International	Security Mode:	FIPS 140-2	
<b>Te</b>	Username:	CryptoOfficer	
	Role:	Crypto Officer	
	Host Name:	default (192.168.254.254)	
LAN Operating Mode Wireless Configuration General Security MAC Address Filtering Bridging Bridging Encryption Rogue AP Detection Advanced Services Settings DHCP Server Subnet Roaming SNMP Agent User Management Lich Millere	Iowercase letters, nu Please change the p Minimal password le User ID: Password: Confirm Password: Role: Note: Add	Imerals, and symbols found on the keyboard assword following the complexity password rule. Ingth:B	_
Done		🔒 👜 Internet	-

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.

🖉 3eTI Gateway Configurat	ion - Microsoft Internet Explo	rer		_ 🗆 🗙
File Edit View Favorites	Tools Help			1
🕞 Back 👻 💮 👻 📘	🗟 🏠 🔎 Search 🤺	Favorites 🜒 Media 🥑 🍰 🍡	🖂 🔜 🔏 🔏	
Address 🙆 https://192.168.1	5.1/cgi-bin/sgateway?PG=64		💌 🄁 Go	Links »
	3eTI 525V Wireless Ad	cess Point		<u> </u>
Technologies	Operation Mode:	Wireless AP/Bridge Mode		
	Security Mode:	FIPS140-2		
	Username:	CryptoOmcer		
	Role:	Crypto Officer		
	Host Name:	default (192.168.254.254)		_
System Configuration General WAN	Monitoring/Reports -	> Bridging Status		
LAN	Ethernet Port 51P Status	·60		
Operating Mode	Path Cost	80		
General	State:	forwarding		
Security	Designated Bridge:	8000.00026f35816e		
MAC Address Filtering				
Bridging Bridging Econumtion	Wireless Port 0 STP Statu	s		
Roque AP Detection	Port Priority (hex):	50		
Advanced	Path Cost:	100		
Services Settings	State:	forwarding		
DHCP Server	Designated Bridge.	8000.000261358168		
SNMP Agent	111:	b:		_
User Management	Pridge Priority/book	0000		
List All Users	Bridge Hello Time:	200 cer		
Add New User	Bridge Forward Delay:	3.00 sec		
User Password Policy	Bridge Max Age:	20.00 sec		
System Status	555% 555%			
Bridging Status	Bridge ID:	8000.00026f35816e		
Wireless Clients	Designated Root:	8000.00026f35816e		
Adjacent AP List	Root Port:	0		
System Log	Path Cost: Hollo Time:	U 2.00.000		
Web Access Log	Forward Delay:	2.00 Sec 3.00 sec		
Network Activity Log	Max Age:	20.00 sec		
System Administration	MAC Ageing Time:	300.00 sec		
Firmware Upgrade	MAC Ageing Interval:	4.00 sec		
Remote Logaing	Flags:			
Reboot				
Utilities				
Copyright © 2004 3e Technologi	es International. All rights reserved	4.		-
Ð			📄 🔒 🔮 Internet	

## **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.

🚈 3eTI Gateway Configural	tion - Microsoft Internet Ex	plorer					
File Edit View Favorites	s Tools Help				27		
🕝 Back 🔹 🕥 👻 💌	🗟 🏠 🔎 Search 🚽	😽 Favorites 🛛 🔿 Media	🙆 🍰 🦉 [	📃 🔜 🖏 💋			
Address 🙆 https://192.168.1	15.1/cgi-bin/sgateway?PG=61			💌 🏓 Go	Links »		
	3eTI 525V Wireless	Access Point			<u> </u>		
A Technologies	Operation Mode:	Wireless Af	P/Bridge Mode				
International	Security Mode: FIPS 140-2						
	Username:	CryptoOffice	er				
	Role: Crypto Officer						
	Host Name:	default (192	2.168.254.254)				
Custom Configuration	Monitoring/Reports	->Wireless Clients	5				
General WAN	Client MAC Address	Signal Strength	Transmit Rate	Last EMCON Response			
LAN Operating Mode							
Wireless Configuration General							
e				📄 🎯 Internet			

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

	<b>3eTI DMG Wire</b>	less Acce	ss Point		
3e	Operation Mode: Security Mode: Usemame: Role:	Wireless FIPS 140 CryptoOff Crypto Of	AP/Bridge mode -2 licer ficer		
etem Configuration	Monitoring/Reports -> Wireless Clients				
eneral	Client MAC Address	s	Signal Strength	Transmit Rate	EMCON Response
N	00:02:6F:03:80:CD	)	0%	11.0 Mbps	Yes
eration Mode	00:02:6F:06:A5:53		0%	11.0 Mbps	No

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
---------------------------	---------------------

	3eTI DMG Wireless Access Point					
Technologies International	Operation Mode:	Wireless	AP/Bridge mode			
	Security Mode:	FIPS 140	-2			
	Usemame:	CryptoOff	icer			
	Role:	Crypto Of	ficer			
ton Configuration	Monitoring/Reports -> Wireless Clients					
eral	Client MAC Addres	s	Signal Strength	Transmit Rate	EMCON Response	
N	00:02:78:E1:17:06	6	0%	0.0 Mbps	•	
AN Antina Made	00:02:6F:03:80:CD	)	0%	11.0 Mbps	Yes	
peracing mode	00:02:6F:06:A5:53		0%	11.0 Mbps	No	

# **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.

3e11 Gateway Configural	tion - Microsoft In	ternet Explorer							- 01
Ele Edit Vew Favorit	es Iools Belo								12
🗿 Back + 🕥 - 💽	** Address 🙆 h	ttps://192.168.202.97/cgi-bin/sgatewa	y?PG=67					•	2 60
	3e TI DMG W	lireless Access Point							2
3e	Operation Mode Security Mode: Username: Role: Host Name:	e: Wireless AP/Bridge Mode FIPS 140-2 CryptoOfficer Crypto Officer default (192.168.202.97)							
for the for the state	Monitoring/Reports ->Adjacent AP List								
General	Make Trusted	BSSID	\$51D	Channel	Signi	I Nois	е Тури	Age	WEP
WAN LAN	E 1.	00:02:6t:20:90:1d(SenaoInter)		1	3	2	AP	13078	N
Operating Mode	□ 2.	00:02:6f 20:90:2l(SenaoInter)		1	2	2	AP	0	N
Mireless Configuration	□ 3.	00:02:6f:20:90:29(SenaoInter)		1	3	1	AP	11747	N
Security	D 4.	00:02:6f:01:fb:87(Senacinter)	General-1	1	7	1	AP.	4	Y
MAC Address Filtering Bridaina	5.	00:07:d5:02:00:08(3eTechnolo)		1	3	2	AP	141	γ
Bridging Encryption Rogue AP Detection Advanced	□ 6.	00:90:d1:07:7d:b1(LeichuEnte)	test	3	32	2	AP	0	N
Done					E R	90	Interne	t	-

#### **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.

Help Search Carlos Favorit Search Search Search	es 🌒 Media 🕢 🍛 🔻 🍃		
/sgateway?PG=65	es 🔮 Media 🧭 🍃 블	🛛 🔜 🚭 🖏	
/sgateway?PG=65		🔻 🖹 Gn	
525V Wireless Access			Links 3
and mineress Access	Point		-
ation Mode:	Wireless AP/Bridge Mode		
irity Mode:	FIPS 140-2		
name:	CryptoOfficer		
	Crypto Officer		
Name:	default (192.168.254.254)		
toring/Report -> DHC	P Client List		
server lease period: 1 Day			
ame IP Addres	s Issued	Remo	ve
192.168.1 00:10:A4:8	5.10 Expire Time 5.10 Tue Nov 30 00:0 2:09:89 Wed Dec 1 00:01	0:20 1999	
90I 192.168.1 00:0D:56:3	5.11 Thu Dec 2 00:52 6:DC:76 Fri Dec 3 00:52:1	213 1999 13 1999	
rbxp548d 192.168.1 00:05:18:0	5.12 Tue Nov 30 00:0 0:F4:77 Wed Dec 1 00:0	0:35 1999 0:35 1999	
	anty Mode: mame: ( t Name: t roring/Report → DHC server lease period: 1 Day ame IPAddress ame IPAddress IPACAddress IPACAD	Introduct         FIPS 140-2           mame:         Crypto Officer           :         Crypto Officer           tharms:         Crypto Officer           tharms:         default (192.168.254.254)           toring/Report > DHCP Client List           'server lease period: 1 Day           ame         IPA Address           MAC Address         Expire Time           19: 109:10:4:82.09.89         Wed Dec 1 00:0           :901         192.168.15.11         Thu Dec 2 00:52           :901         192.168.15.12         Tue Nov 30 00:0           :901         192.168.15.12         Tue Nov 30 00:0           :901         00:05:18:00:F4:77         Wed Dec 1 00:0	Initial Model         FIPS 140-2           mame:         Crypto Officer           :         Server lease period: 1 Day           :         IPAddress         Expire: Time           :         Particle:15:10         Tue Nov 30:00:00:20:1999           :         00:10:44:82:09:B9         Wed Dec: 1:00:00:20:1999           :         192:168:15:11         Thu Dec: 2:00:52:13:1999           :         00:00:56:76:D0:76         Fri Dec: 3:00:52:13:1999           :         192:168:15:12         Tue Nov 30:00:00:35:1999           :         00:05:1B:00:F4:77         Wed Dec: 1:00:00:35:1999

# 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.

🏄 3eTI Gateway Configura	ation - Microsoft Intern	et Explorer	_ 🗆 ×
File Edit View Favorite	s Tools Help		2
🕞 Back 🔹 🕥 🕤 💌	😰 🏠 🔎 Searc	h 🤺 Favorites 🜒 Media 🥝 🍛 😓 🔜 🛄 🐒 🦓	
Address 🙆 https://192.168.	15.1/cgi-bin/sgateway?PG	=66 💌 🔁 Go	Links *
	3eTI 525V Wire	less Access Point	
Technologies	Operation Mode:	Wireless AP/Bridge Mode	
International	Security Mode:	FIPS 140-2	
	Licornama:	Christelofficer	
	Data:	Crypto Officer	
	Role.	Crypto Onicer	
	Host Name:	default (192.168.254.254)	
	Monitoring/Rep	oorts -> System Log	Clear
System Configuration			
General	Date-Time	System-Facility-Message	
LAN	Nov 30 00:00:02	default syslog.info syslogd started: BusyBox v0.60.1 (2004.11.29-22:17+0000	ŋ
Operating Mode	Nov 30 00:00:02	default user.warn kernel: Linux version 2.4.17_mvl21 (kkaza@build) (gcc vers	ion
Wireless Configuration		2.95.3 20010315 (release/MontaVista)) #1 Mon Nov 29 17:08:17 EST 2004	
General	Nov 30 00:00:02	default user warn kernel: Processor: Intel XScale-DXP425 revision 1	
Security	Nov 30 00:00:02	default user warn kernel: Machine: Intel IXP425 EAP Gateway Board	
MAC Address Filtering	Nov 30 00:00:02	detault user.warn kernel: Now in tixup_eap, RAM size=ux200000	
Bridging	NOV 30 00:00:02	detault user debug kernel: Converting old-style param struct to taglist	
Bridging Encryption	Nov 30 00:00:02	default user warn kernel: warning: bad configuration page, trying to continue	
Rogue AP Detection	Nov 30 00:00:02	default user warn kernel: On node U totalpages: 8192	
Advanceu Seruisee Settinge	Nov 30 00.00.02	default user warn kernel, zone(u), 8192 pages.	
DHCP Server	Nov 30 00:00:02	default user warn kernel: zone(1). 0 pages.	
Subnet Roaming	Nov 20 00:00:02	default user warn kernel: Karnel command line: concole=#vP1 115200	
SNMP Agent	Nov 30 00:00:02	default user info kernel: Reflecting machine vectors to 0vfff0000	
User Management	Nov 30 00:00:02	default user warn kernel: Lising IXP425 Timer 0 as timer source	
List All Users	Nov 30 00:00:02	default user warn kernel: Calibrating delay loop 525.92 BogoMIPS	
Add New User	Nov 30 00:00:02	default user info kernel: Memory: 32MB = 3	
User Password Policy		default user info kernel: XScale Cache/TLB Locking Copyright(c) 2001 Montal	/ista
Monitoring/Reports	NOV 30 00:00:02	Software, Inc.	
System Status Bridaia - Status	Nov 30 00:00:02	default user warn kernel: XScale cache_lock_init called	
Mirelese Cliente	Nov 30 00:00:02	default user warn kernel: Calling consistent alloc	
Adjacent AP List	Nov 30 00:00:02	default user warn kernel: low_level_page initialized	
DHCP Client List	Nov 30 00:00:02	default user.warn kernel: low_level_page @ 0xc2800000	
System Log	Nov 30 00:00:02	default user warn kernel: icache_lock_fn @ 0xc2800080	
Web Access Log	Nov 30 00:00:02	default user.warn kernel: dcache_lock_fn @ 0xc28000a0	
Network Activity Log	Nov 30 00:00:02	default user.warn kernel: icache_unlock_fn @ 0xc2800098	
Network Activity Log	Nov 30 00:00:02	default user.warn kernel: icache_unlock_fn @ 0xc2800098	1

## 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.

🚰 3eTI Gateway Configurat	ion - Microsoft Interr	et Explorer	_ 🗆 🗵
File Edit View Favorites	Tools Help		27
🕝 Back 🔹 🕥 🖌 💌	🔊 🏠 🔎 Searc	n 🤺 Favorites 🌒 Media 🧭 🍛 🍉 🔜 🧾 🖏 🥸	
Address (192.168.1	5.1/cgi-bin/sgateway?PG	=60 💌 🄁 Go	Links »
	3eTI 525V Wire	less Access Point	<b></b>
A Technologies	Operation Mode:	Wireless AP/Bridge Mode	
International	Security Mode:	FIPS 140-2	
70	Username:	CryptoOfficer	
	Role:	Crypto Officer	
	Host Name:	default (192.168.254.254)	
System Configuration	Monitoring/Re	oorts -> Web Access Log	Clear
General	Date-Time	System-Facility-Message	
WAN	Nov 30 00:06:20	User:Admin Operation:System Upload	
Operating Mode			
Wireless Configuration General			-
é		🔒 🎯 Internet	1.

# **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.

Jell Gateway Configura	tion - Hierorieft Inter	net Explorer	A DIX
Ele Edit gew Fgroni	tes Loois Lieip		27
Q feck + () - 💽	* Address Athres	a://192.168.202.97/cg-bin/hgsteniay/WG=68	E 00
	3eTI DMG Wire	eless Access Point	
3e	Coeration Mode: Security Mode: Username: Role: Hout Name:	Winkess APRindge Mode FIPS 140-2 CryptoClifeer CryptoClifeer outsuit (12: 198.202.07)	
a share that the star	Monitoring/Rep	ports -> Network Activity Log	Cear
General	Gate-Time	System-Facility-Hessage	
WAN LAN Operating Mode Wretess Configuration General Security MAC Advess Filtering Bridging Encryption Regue AP Detection Advanced Services Settings DirOf Servic Statt Agent.	Nov 30 02:20:30 Nov 30 02:20:43 Nov 30 02:20:51	ented assessment national https://www.ented.com/section/sectio	-
Contains commands for weaking	with the selected term.		-

## 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.

🏄 3eTI Gateway Configura	tion - Microsoft Internet Explorer		_ 🗆 ×
File Edit View Favorites	s Tools Help		27
🕝 Back 🔹 🕥 👻 💌	😰 🏠 🔎 Search   havorite	es 🜒 Media 🧭 🍃 🍃 🗾 🌄 🦓 🖄	
Address 🙆 https://192.168.1	5.1/cgi-bin/sgateway?PG=72	💌 🄁 Go	Links »
	3eTI 525V Wireless Access	Point	-
Contraction Technologies	Operation Mode:	Wireless AP/Bridge Mode	
International	Security Mode:	FIPS 140-2	
70	Username:	CryptoOfficer	
	Role:	Crypto Officer	
	Host Name:	default (192.168.254.254)	ale ale
System Configuration	System Administration - Re	emote Logging	
WAN	Remote Logging	C Enable 💿 Disable	
LAN Operating Mode	System Log Server IP Address:		
Wireless Configuration General Security MAC Address Filtering	System Log Server Port:	514 (default port is 514)	
Bridging	CHEV.		•
E vone		📔 👹 Internet	

#### 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:



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 1	92.	168.	1.15	00-40-	8c-64-c5-cf	
C:\>ping	-t	-1	408	192.1	68.1.1	5	

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. <u>http://192.168.1.15</u>). 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. <u>http://192.168.1.15/admin/</u>).

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.



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: <u>http://192.168.21.10/admin/</u>. 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.



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 <u>http://192.168.254.30</u>. 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.

🔤 Telnet 192.168.254.30	×
Password:	-
Comtrol DeviceMaster RTS ModelID: 5002111 SocketServer 3.09 Built: Wed Feb 4 13:34:55 GMT 2004 IP Addr: 192.168.254.90 Mask: 207.2.0.0 Gateway: 192.168.254.1 MAC Addr: 00 c0 4e 07 09 8c	
dm> ip 192.168.254.90 255.255.255.0 192.168.254.1 IP Addr: 192.168.254.90 Mask: 255.255.255.0 Gateway: 192.168.254.1 IP Address stored, reset to take effect. dm> _	

- 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. (<u>http://192.168.254.30</u> for the preconfigured IP address). A web page showing general information of the device, shown in the following picture, should open up:

Comtrol Corporation	tion - Devicel	Master Socke	tServer 3.09	- Microsoft Inter	net Explorer	_ 🗆 ×
File Edit View Fa	orites Tools	Help				1
🕒 Back 🔻 🕥 🔻 [	× 🗈 🏠	Search	\rm 🕂 Favorites	≷ Media 🧭	🙈 ▼ 😓 🗹 👻 🛄	×
Address 🔄 C:\Docum	ents and Setti	ngs\mguerrero	My Documer	nts\comtrol\Comtro	l Corporation - E 💌 🔁 🤇	Go Links »
	CON	TRO	-			
	The Enterpr	ise Connecti	on			
		Serve	r Con	figuratio	n	
	1			ngarati		
		Software	:		SocketServer 3	.09
	A	IP Config	j:		Static	
	1.	IP Addre	ss:		192.168.254.3	0
		IP Netma	ask:		255.255.254.0	
DEVICEN	ACTED	IP Gatew	/ay:		192.168.254.3	
DEVICE•M	ASIEK	<u>Configur</u>	e Networ	<u>k</u>		
		Configur	e Email M	lessages		
		<u>Configur</u>	e RFC100	6 (ISO over	<u>TCP)</u>	
	Port 1	Port 2	Port 3	Port 4		
Connection St	tatus					
Enabled:	No	No	No	No		
Local:	0.0.0.0:	0 0.0.0.0:	0 0.0.0.0:	0 0.0.0.0:0		
Remote:	0.0.0.0:	0 0.0.0.0:	0 0.0.0.0:	0 0.0.0.0:0		
Rx bytes:	0	0	0	0		
Tx bytes:	0	0	0	0		
Serial Status						
Mode:	RS-232	RS-232	RS-232	RS-232		
Baud:	9600	9600	9600	9600		
Parity:	none	none	none	none		
Stop Piter	0	0	0	8		
Flow:	none	none	none	none		
DTR:	off	off	off	off		
EOL:	none	none	none	none		
Timeout:	0	0	0	0		-

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

Comtrol Corporation - Devi	ceMaster RTS SocketServer 3.09 - Microso	
File Edit View Favorites To	ols Help	
🅃 Back 🔻 🕥 👻 🛃 🔮 🦿	🏠 🔎 Search 🤺 Favorites   Nedia 🧭	
ddress 👰 C:\Documents and Se	ettings\mguerrero\My Documents\cor 💌 🛃 Go 🛛 Lir	nks
	MIROL	
The Enter	prise Connection	
Edit Network	Configuration	
Edit Network	Configuration	
	Configuration	
Edit Network	Configuration	
Edit Network	Configuration Cuse DHCP Disable IP networking Use static configuration below:	
Edit Network	Configuration <ul> <li>Use DHCP</li> <li>Disable IP networking</li> <li>Use static configuration below:</li> </ul> 192.168.254.30	
Edit Network	Configuration Cuse DHCP Disable IP networking Use static configuration below: 192.168.254.30 255.255.254.0	
Edit Network	Configuration Cuse DHCP Disable IP networking Use static configuration below: 192.168.254.30 255.255.254.0 192.168.254.3	
Edit Network	Configuration Cuse DHCP Disable IP networking Use static configuration below: 192.168.254.30 255.255.254.0 192.168.254.3	
Edit Network IP Configuration: IP Address: Netmask: Gateway: TCP Keepalive Timeo	Configuration Cuse DHCP Disable IP networking Use static configuration below: 192.168.254.30 255.255.254.0 192.168.254.3 Dut: 60	
Edit Network IP Configuration: IP Address: Netmask: Gateway: TCP Keepalive Timeo	Configuration Cuse DHCP Disable IP networking Use static configuration below: 192.168.254.30 255.255.254.0 192.168.254.3 Dut: 60	
Edit Network IP Configuration: IP Address: Netmask: Gateway: TCP Keepalive Timeo Undo Changes	Configuration Cuse DHCP Disable IP networking Use static configuration below: 192.168.254.30 255.255.254.0 192.168.254.3 Dut: 60 Save	

- 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.
- To configure the serial ports, click on de desired port link (e.g., <u>Port</u>
   in the main page. This action should bring up the following web page:

🕘 Comtrol Corporation	- DeviceMaster RTS SocketServer 3.09 - Microsoft Intern 💶 🔲 🗙
File Edit View Favorit	es Tools Help 🦧
🔇 Back 🔻 🕥 👻 🛃	😰 🏠 🔎 Search 🤺 Favorites 🜒 Media 🚱 🍰 👻
Address 🖉 C:\Document	s and Settings\mguerrero\My Documents\comtrol\port1 🔽 🔁 Go 🛛 Links 🎽
	A
	0
The	Enterprise Connection
Edit Port 1	. Configuration
Serial Configura	tion
Mode:	RS-232 -
Baud:	9600 -
Parity:	none 💌
Data Bits:	8 -
Stop Bits:	1 -
Flow:	none
DTR:	off 💌
EOL:	disabled <b>v</b> 00 00 (hex)
Input Timeout	0 ms
Connection Con	figuration
Enable:	
Listen:	Enable on Port: 8000
Connect To:	0.0.0.0 Port: 0
Connect On:	🗆 Always, 🗆 Data, 🗆 DSR, 🗆 CD
Disconnect On	$\Box$ Idle, $\Box$ No DSR, $\Box$ No CD
Idle Timer:	300
Clone Port	Undo Changes Save

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 (Device-Master RTS) please refer to the Comtrol documentation enclosed with the 3e-528, or go the website <u>http://support.comtrol.com/download.asp</u>, 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 CON-FIG 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 CON-FIG 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.

🚰 Wireless Bridge Information - Microsoft Internet Explorer				
Wireless Bridge Infor	mation		4	
Enable refresh: 🗹 🛛 Bridg	e refresh interval: 5 seconds	<b>•</b>		
Remote AP's MAC Address		11-22/12/		
Port No. MAC Address	Signal Strength	Note		
Copyright @ 2004 3e Technolog	ies International. All rights reserved.			
			*	

	BRIDGING GE	ENERAL 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 broad- cast 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 fre- quency 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 bridg- ing 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 hexadeci- mal 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:

- 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.

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.			

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

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**.

🚈 3eTI Gateway Configura	tion - Microsoft Internet Explorer	_ 🗆 🗙
File Edit View Favorite:	s Tools Help	<b>#</b>
🕒 Back 🔹 🕥 🖌 💌	🗟 🏠 🔎 Search 🤺 Favorites 🜒 Media 🚱 🔗 🍃 🔜 🛄 🖏 🖄	3
Address 🙆 https://192.168.3	15.1/cgi-bin/sgateway?PG=13	Go Links »
	3eTI 525V Wireless Access Point	4
3 Technologies International	Operation Mode: Wireless AP/Bridge Mode Security Mode: FIPS 140-2 Username: Crypto Officer Role: Crypto Officer Host Name: default (192.168.254.254)	
System Configuration General LAN Offretess Configuration General Security MAC Address Filtering Bridging Encryption Rogue AP Detection	Wireless Configuration → Bridging         General         MAC Address:       00:02:6F:22:0B:D6 (SenaoInter)         Wireless Mode:       802:11b/g Mixed ▼         Tx Rate:       AUT ○ ▼         Channel No:       11 (2:452 GHz) ▼         Tx Pwr Mode:       Aut ○ ▼         Fixed Pwr Level:       8 ▼         Spanning Tree Protocol (STP) 802.1d       € Enable ○ Disable	Monitoring
Advanced Services Settings DHCP Server Subnet Roaming SNMP Agent User Management List All Users Add New User User Password Policy	Signal Strength LED MAC: Not Assigned  Apply Add revote AP's BSSID/Note	_
Monitoring/Reports System Status Bridging Status Wreless Clents Adjacent AP List DHCP Clent List System Log Web Access Log Network Activity Log System Administration Firmware Lygrade Factory Default Remote Logging	BSSID: Note: Add Remote AP's MAC Address Delete MAC Address Signal Strength Note	-
Utilities Copyright @ 2004 3e Technolog	es International. All rights reserved.	

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.

🗿 3eTI Gateway Configura	tion - Microsoft Internet Explorer		_ 🗆 🗙
File Edit View Favorites	s Tools Help		-
🕝 Back 🔹 🕥 🖌 💌	😰 🏠 🔎 Search   hrvorites	👏 Media 🥝 🔗 😓 🔜 🧾 🖏	
Address 🙆 https://192.168.1	15.1/cgi-bin/sgateway?PG=14	💌 🄁 Go	Links »
	3eTI 525V Wireless Access F	Point	4
Contraction Technologies	Operation Mode:	Wireless AP/Bridge Mode	
International	Security Mode:	FIPS 140-2	
	Username:	CryptoOfficer	
	Role:	Crypto Officer	
	Host Name:	default (192.168.254.254)	
	Wireless Configuration -> B	ridging Encryption	_
System Configuration			
WAN	Off - No Data Encryption		
LAN	C Static 3DES Key / Open System /	Authentication	
Operating Mode	Enter 192-bit keys as 48 hexade	ecimal digits (0-9, a-f, or A-F))	
Wireless Configuration	Key		
Security	Again		
MAC Address Filtering			
Bridging	O Static AES Key ( Onen System A	thentication	
Bridging Encryption Roque AP Detection	C 129 bit Eponetion (Enter 12)	B bit kow as 33 bovodocimal digits (0.0, a f. ar. ()	
Advanced	C 120-bit Eliciyption (Enter 720	Polit Reys as 52 nexadecimal olgits (0-9, a-1, 01 A-7))	
Services Settings	Key		
DHCP Server	Again		
SNMP Agent	C 192-bit Encryption (Enter 19)	2-bit kevs as 48 hexadecimal digits (0-9, a-f, or A-F))	
User Management	Key	g,,,,,,	
List All Users	1(0)		
Add New User User Password Policy	Again		
Monitoring/Reports	C 256-bit Encryption (Enter 256	5-bit keys as 64 hexadecimal digits (0-9, a-f, or A-F))	
System Status	Key		
Bridging Status	Arian		
Adjacent AP List			
DHCP Client List			
System Log	Apply		
Web Access Log Network Activity Log			
System Administration			
Firmware Upgrade			
Factory Default			
rtemote Logging Rehoot			
Utilities			
Copyright © 2004 3e Technolog	ies International. All rights reserved.		
(A)		A Internet	

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.

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 bot- tom 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.		

## Point-to-Multipoint Bridging Setup Guide

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-tomultipoint 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 Configurati	on – 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 Configurati	on – Bridging Encrypt	ion	
Wireless Configu- ration – 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.

Configuration File	
Config.3eTI	Browse
Password	
1	Configure
nfigure Status	
	-
	-
1	× <u>×</u>

#### 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.

🚱 3e-RF Manager		×
Configuration File		
Config.3eTI		Browse
Password		
		Configure
Configure Status	Select a 3eTI Config File	?)>
	Look in: 🔄 3e-RF Manager	- 🖬 🍅 🖬 -
al.	② Config.3eti         ③ FipsRadioOff.3eti         ③ FipsRadioOff.3eti         ③ SampleRadioOff.3eti         ③ SampleRadioOff.3eti	
	File name: Files of type: 3ETI Config Files	(*.3eli) 💌 Cancel

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.

Open W	ïth	? ×
	Click the program you want to use to open 'Config.3eti'. If the program is not listed, click Other.	
	Description for files of this type:	
	Choose the program you want to use:	
	<ul> <li>Microsoft Schedule+ for Windows 95</li> <li>Microsoft Word for Windows</li> <li>Microsoft(R) Windows Media Player</li> <li>Application</li> </ul>	4
	Notepad NTI CD-Maker 2000	
	Opera Internet Browser (win32)	¥
	Always use this program to open these files	
	OK Cancel Other	

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.

CampleDadieOff 2nti WordDad	📱 SampleRadioOn.3eti.txt - WordPad	- 🗆 ×
Els Edb Hans Torest Format Hale	File Edit View Insert Format Help	
DE Cat view Insert Format Hep	DFR 64 M X 10 C N	
<pre># This Sample Configuration # off on all units</pre>	# This Sample Configuration file shows how to turn the r # to a fixed level on all units	adio 📤
<pre>[all] Wireless Tx Pwr Mode:=Off #For FIPS units use the fol #Gateway Access Mode:=HTTPS #Gateway Username:=CryptoOf</pre>	[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	#Each unit that you want to turn off should be listed he	re
#First unit [192.168.15.1]	#First unit [192.168.15.1] Wireless Fixed Pwr Level:=2	
#Next unit [192.168.15.2]	#Next unit [192.168.15.2] Wireless Fixed Pur Level:=2	<u>·</u>
For Help, press F1	For Help, press F1	1

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.

C. Program Files (3e-File Manager (Sampler) adioUlt. Seti	Browse
Password	
	Configure
r 0	
ligure Status	

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.

onfiguration File	
C:\Program Files\3e-RF Manager\FipsRadioOn.3eti	Browse
Password	
RODORODOR	Configure
nfgureStatus nding Configuration items for 192.16 ccesfully set configuration item Win ccesfully set configuration item Win	8.204.112. eless Fixed Pwr eless Tx Pwr Mod
MgueStatus nding Configuration items for 192.16 ccesfully set configuration item Win ccesfully set configuration item Win nfiguration complete for 192.168.20 CCESS: Successfully set all configur	8.204.112. eless Fixed Pwr : eless Tx Pwr Mod .112. ation items.
nfigureStatus nding Configuration items for 192.16 ccesfully set configuration item Wir ccesfully set configuration item Win nfiguration complete for 192.168.204 CCESS: Successfully set all configur	8.204.112. eless Fixed Pwr : eless Tx Pwr Mod .112. ation 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.

3e-RF Manager	2
Configuration File	
C:\Program Files\3e-RF Manager\SampleRadioOff.3e	
Password	
NORSK	
Configure Status	
RROR: Cannot communicate with 192.168.15.1. RROR: Failed to set all configuration items. MARNING: Set 0 units of 2 units. MARNING: Set 0 configuration items of 0 items.	*
d	<u>ب</u> ۲
	_

# **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.