523C / 523E
Secure Multi-Function
Wireless Mesh/Client/Bridge/Access Point
User's Guide

29000189-002 A

publ. 04/24/07

This page intentionally left blank.

523C / 523E
Secure Wireless
Mesh / Client / Bridge / Access Point
User's Guide

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

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

If there is any software or removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the printed documentation, or on the removable media in a readable file such as license.txt or the like. If you are unable to locate a copy of the license, contact the company and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States Government agency, then this documentation and the product described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3e Technologies International's standard commercial license for the software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

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

EXPORT RESTRICTIONS

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

Table of Contents

Chapter 1: Introduction

The 523C / 523E (herein called the 523C/E) is a Secure Multi-Function Wireless Data Point which supports three different operating modes:

- Wireless Access Point (WAP)
- Wireless Client (STA), and
- Wireless Bridge (WDS)

The 523C/E supports the following cryptographic modules:

In AP mode:

- Static WEP (64, 128, or 152-bit)
- IEEE 802.11i and WPA (TKIP)

In Client mode:

- Open (none, 64, 128, or 152-bit WEP)
- Shared (64, 128, or 152-bit WEP)
- WPA-PSK
- WPA2-PSK
- WPA-EAP-TLS
- WPA2-EAP-TLS

In Bridging mode:

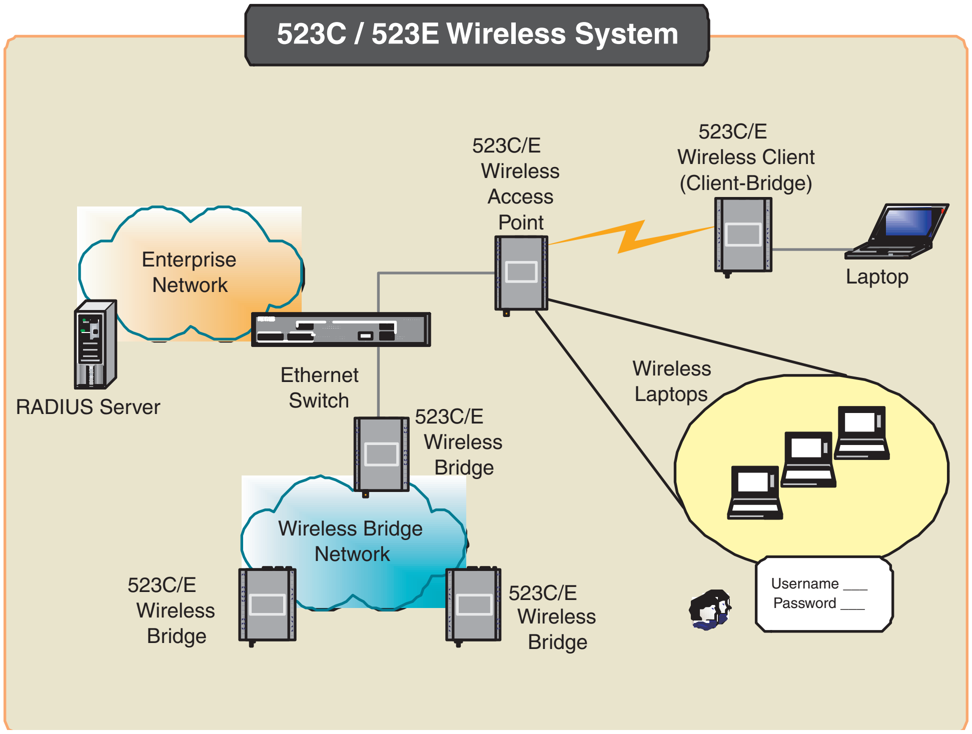
- AES-CCMP (128-bit)

HTTPS/TLS is used for secure web communication. The 523C/E also provides wireless client MAC address filtering and rogue AP detection with email notification to protect your network.

With support of 802.11a/b/g standards, the 523C/E delivers up to 54Mbps of data rate in 5GHz (802.11a) and 2.4 GHz (802.11b/g) bands. The 523C/E also supports Super G and Turbo A. 802.11g Super and 802.11a Turbo provide speed and throughput of more than double the standard LAN technologies in networking products. The maximum link speed available is 108Mbps and the typical maximum end-user throughput ranges from approximately 40Mbps to 60+Mbps, depending on application demand and network environment. Turbo A is not supported at the ETSI domain region.

Other key features of the 523C/E include AP load balancing, AP layer 2 isolation, and Bridge site mapping.

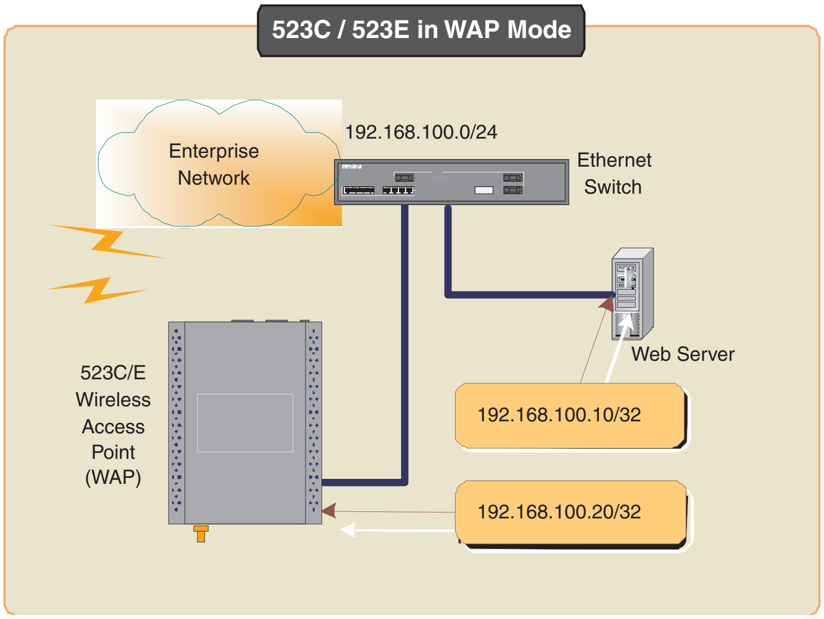
This figure illustrates a wireless system using the 523C/E in all three modes.



Wireless Access Point Mode

In the wireless access point mode, you can use the 523C/E to connect wireless communication devices together to create a wireless network. The 523C/E is usually connected to a wired network and can relay data between devices on each side. Many 523C/Es can be connected together to create a larger network that allows roaming.

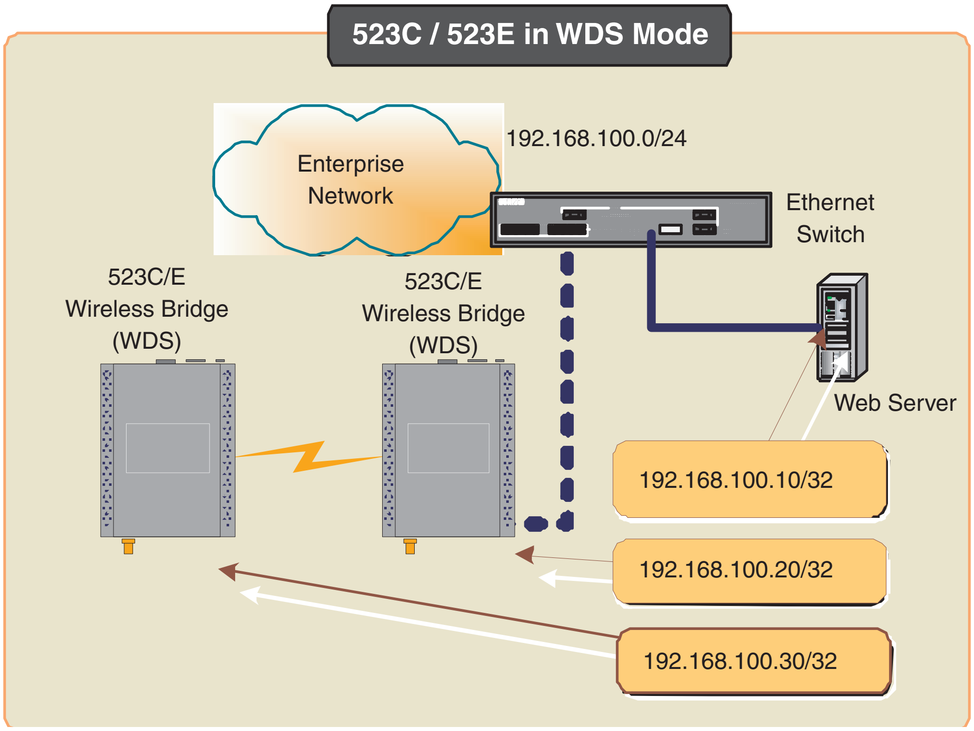
In Wireless Access Point (WAP) mode the WAN interface has to connect to a backbone Ethernet switch in order to operate normally. It bridges the backbone Ethernet network and wireless interface. The following diagram shows how to setup the Ethernet cable and IP addressing.



There are numerous security methods provided in this mode: WEP, WPA (TKIP and AES-CCM) and WPA2 (TKIP and AES-CCM) are available. The 523C/E also supports EAP-MD5, EAP-TTLS, EAP-TLS, PEAP, EAP-SIM protocols.

Wireless Bridging Mode

In Wireless Bridging (WDS) mode the WAN interface may or may not need to connect to a backbone Ethernet switch. It depends on needs of infrastructure network. However, wireless bridging extends the network from an existing wired network easily without altering the network topology. The following diagram shows how to setup the Ethernet cable and IP addressing.



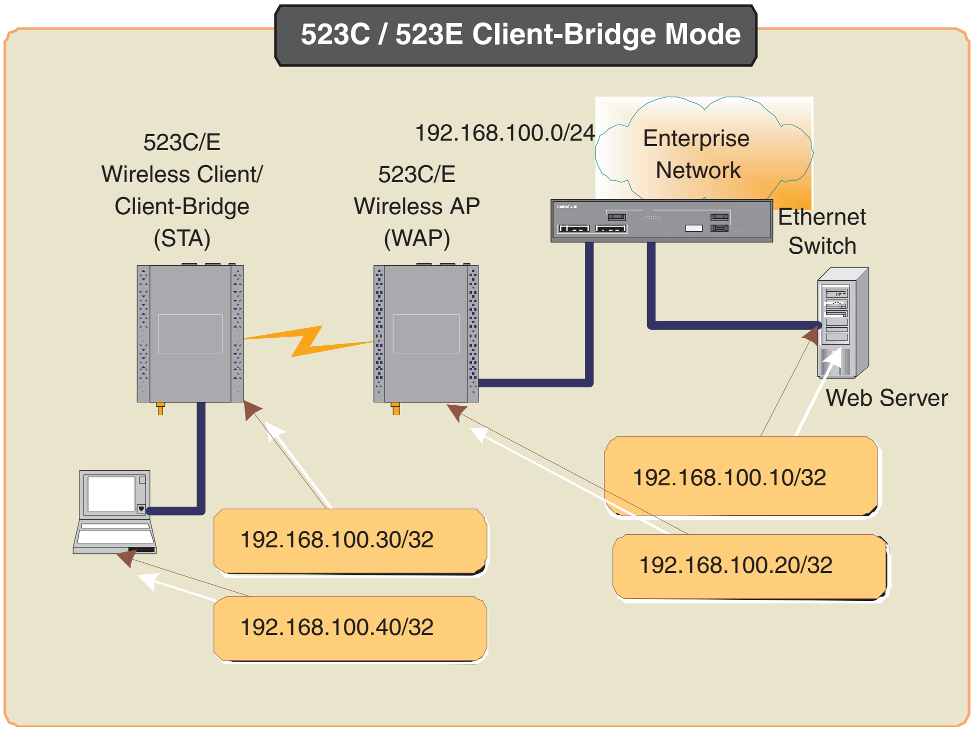
This type of infrastructure is decentralized. As each node needs only transmit as far as the next node. Nodes act as repeaters to transmit data from nearby nodes to peers that are too far away to reach, resulting in a network that can span large distances.

The 523C/E in bridging mode provides point-to-point or point-to-multipoint network topology.

In bridging mode the 523C/E supports AES-CCM for security.

Wireless Client Mode

In Wireless Client/Client-Bridge mode, the WAN interface is **NOT** design for a backbone network connection. It is the interface for computer connected to it. The following diagram shows how to setup the Ethernet cable and IP addressing.



The 523C/E can operate as a client device that communicates with a wireless access point. It supports 802.11a/b/g bands.

The 523C/E supports the following security types:

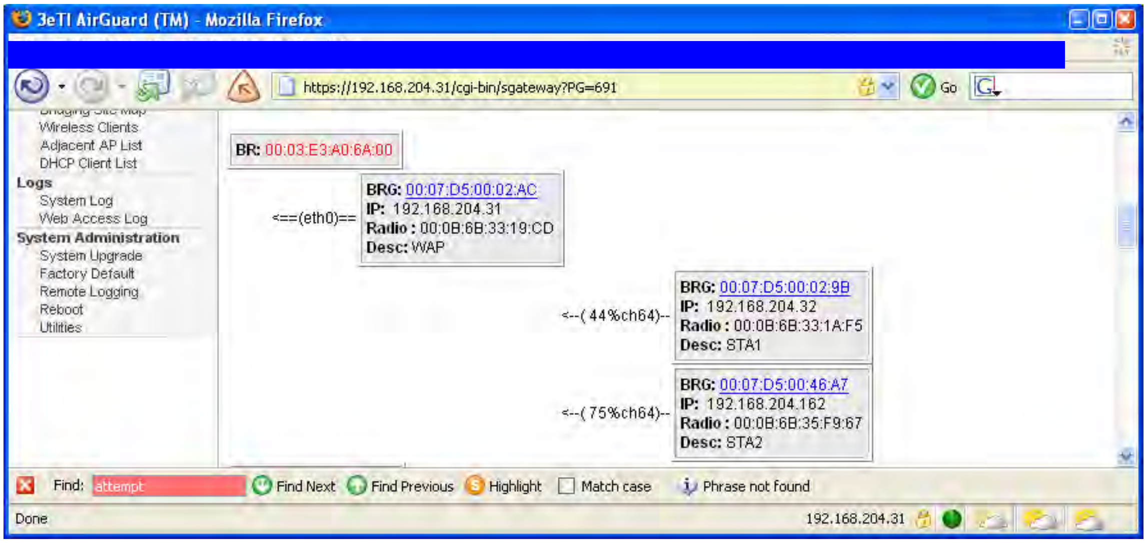
- Open
  - None
  - 64-bit, 128-bit, and 152-bit WEP
- Shared
  - 64-bit, 128-bit, and 152-bit WEP
- WPA-PSK
- WPA-EAP-TLS
- WPA2-PSK
- WPA2-EAP-TLS

Network Topology Map Enhancement

The 523C/E contains an embedded network topology map which can help you to envision the bridged network. The initial implementation provides the following tree structure where each indented entry is a child to the entry above it. The entry at the top of the tree is the STP root. The receive signal strength is indicated by the % on each link.

The map shows the network layer 2 topology. APs that are part of another network are not displayed in the map. This map only reports all devices (client-bridge, AP, bridge) and part of 3rd party switches running STP. It is strongly recomments that you configure your 3rd party switch as root and make it the uplink for the device cloud to the backbone network.

This implementation is base-on the current design.



BR: 00:03:E3:A0:6A:00

<==(eth0)== BRG: 00:07:D5:00:02:AC
IP: 192.168.204.31
Radio : 00:0B:6B:33:19:CD
Desc: WAP

<--(44%ch64)-- BRG: 00:07:D5:00:02:9B
IP: 192.168.204.32
Radio : 00:0B:6B:33:1A:F5
Desc: STA1

<--(75%ch64)-- BRG: 00:07:D5:00:46:A7
IP: 192.168.204.162
Radio : 00:0B:6B:35:F9:67
Desc: STA2

Basic Features

The 523E is housed in a small aluminum enclosure. The 523E is not meant for outdoor use. The 523E has the following features:

- 10/100 Ethernet port
- RS232 Serial port
- LEDs (Power, LAN, WLAN)
- Reset button
- SMA antenna connector

The 523C is housed in an IP 66 enclosure for outdoor use. The 523C has the following features:

- 10/100 Ethernet port/PoE
- LEDs (Power, LAN, WLAN)
- Reset button
- N-type antenna connector

Optional Features

The 523C/E can has the following options which can be set at the factory:

- Wireless VLAN
- Mesh

Operator Authentication and Management

Authentication mechanisms are used to authenticate an operator accessing the device and to verify that the operator is authorized to assume the requested role and perform services within that role.

Access to the management screens for the 523C/E requires knowledge of the assigned operator ID and Password. The Factory defaults are:

- ID: crypto
- Password: officer

The Crypto Officer initially installs and configures the 523C/E after which the password should be changed from the default password. The ID and Password are case sensitive.

Management

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

The next chapter covers the hardware specifications.

523C/E Navigation Options
System Configuration
General
Operating Mode
WAN
Wireless Client
General
Encryption • Open WEP • Shared WEP • WPA-PSK • WPA-EAP-TLS • WPA2-PSK • WPA2-EAP-TLS
Wireless Bridge
General • Monitoring
Radio
Encryption • AES-CCM
MAC Address Filtering (auto bridge mode only)
WirelessAP
General
Security • None • Static WEP • 802.11i and WPA
Wireless VLAN
MAC Address Filtering
Rogue AP Detection
Advanced
Services Settings
DHCP Server (AP mode)
SNMP Agent
Admin User Management
List All Users • Edit/Delete
Add New User
User Password Policy
Monitoring Reports
System Status
Bridging Status
Bridging Site Map
Wireless Clients
Adjacent AP List
DHCP Client List
Logs
System Log
Web Access Log
System Administration
System Upgrade • Firmware Upgrade • Local Configuration Upgrade
Factory Default
Remote Logging
Reboot
Utilities

Chapter 2: Hardware Installation

This chapter deals with installation of the 523C/E unit only. The 523C/E requires physical mounting and installation on the site, following a prescribed placement design to ensure optimum operation.

The 523C package includes the following items:

- 523C
- Waterproof tape
- RJ45 Ethernet connector
- 24V PoE
- AC adaptor
- Documentation as PDF files (on CD-ROM)
- Registration and Warranty cards

The 523E package includes the following items:

- AC adaptor
- Documentation as PDF files (on CD-ROM)
- Registration and Warranty cards

The 523C can be mounted outdoors on a high post to achieve the best bridge result. If mounted outdoors, the outdoor accessory kit must be used to prevent lightning damage.

⚠ IMPORTANT NOTE: To comply with FCC RF exposure compliance requirements, the antennas used with the 523C/E must be installed with a minimum separation distance of 20 cm from all persons, and must not be co-located or operated in conjunction with any other antenna or transmitter. Installation should be accomplished using the authorized cables and/or connectors provided with the device or available from the manufacturer/distributor for use with this device. Changes or modifications not expressly approved by the manufacturer or party responsible for this FCC compliance could void the user's authority to operate the equipment.

Installation Instructions

This manual deals only and specifically with a single 523C/E device as a unit. The purpose of this chapter is to describe the device and its identifiable parts so that the user is sufficiently familiar to interact with the physical unit. Preliminary setup information provided below is intended for information and instruction of the wireless LAN system administration personnel.

It is intended that the user not open the unit. Any maintenance required is limited to the external enclosure surface, cable connections, and to the management software (as described in Chapter 3) only.

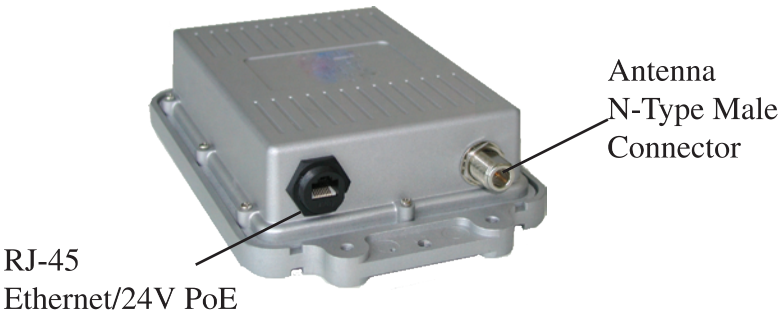
Minimum System and Component Requirements

To complete the configuration, you should have at least the following components:

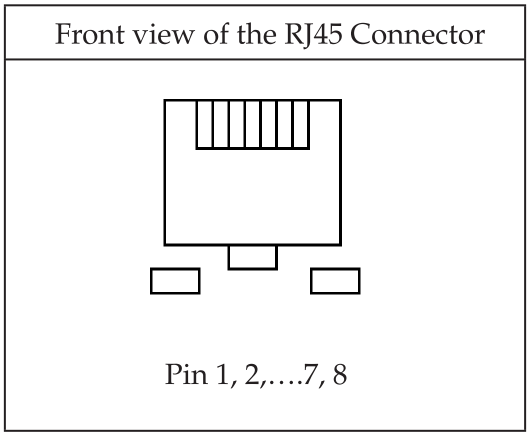
- PCs with one of the following operating systems installed: Windows NT 4.0, Windows 2000 or Windows XP;
- Access to at least one laptop or PC with an Ethernet card and cable that can be used to complete the initial configuration of the unit.
- A Web browser program (such as Microsoft Internet Explorer 5.5 or later, or Netscape 6.2 or later) installed on the PC or laptop you will be using to configure the Access Point.
- TCP/IP Protocol (usually comes installed on any Windows PC.)

Connectors and Cabling

The following illustration shows the external connectors on the 523C.



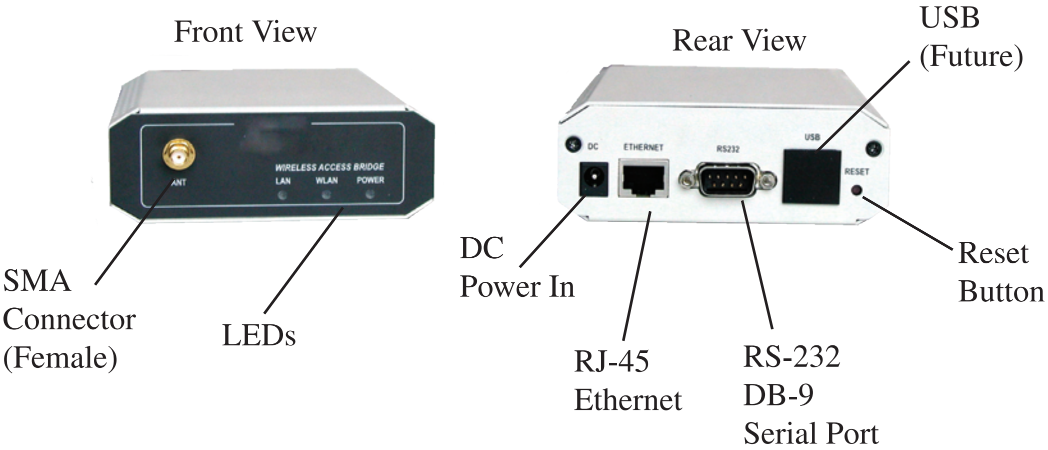
Pin Definition and color code for RJ45 of Ethernet port



RJ45 connector signal names and color code per IEEE 802.3 spec

Name	Pin	Wire Color	Pin	Name
TX+	1	White/Orange	1	TX+
TX-	2	Orange	2	TX-
RX+	3	White/Green	3	RX+
	4	Blue	4	
	5	White/Blue	5	
RX-	6	Green	6	RX-
	7	White/Brown	7	
	8	Brown	8	

The following illustration shows the external connectors on the 523E.



Product Specifications

CPU: XScale IXP 420 @ 266MHz

8 MB Flash

64 MB SDRAM

Radio Characteristics

- **802.11b**
  - Frequency band:
    - American (FCC): 2.412 ~ 2.462GHz (11 channels)
    - Europe (ETSI): 2.412 ~ 2.472GHz (13 channels)
  - Data Rate:
    - 1, 2, 5.5, 11Mbps
  - Modulation:
    - Direct Sequence Spread Spectrum (DSSS)
    - Differential Binary Phase Shift Keying (DBPSK) at 1 Mbps
    - Differential Quadrature Phase Shift Keying (DQPSK) at 2 Mbps
    - Complementary Code Keying (CCK) at 5.5 and 11 Mbps
  - Transmit Output Power (Typical):
    - 18 dBm for all rates

Note: Maximum power setting will vary according to individual country regulations.

  - Receive Sensitivity (Typical):
    - -93dBm at 1Mbps
    - -88dBm at 11Mbps
- **802.11g**
  - Frequency band:
    - American (FCC): 2.412 ~ 2.462GHz (11 channels)
    - Europe (ETSI): 2.412 ~ 2.462GHz (13 channels)
  - Data rate:
    - 6, 9, 12, 18, 24, 36,48, 54 Mbps
    - 72, 96, 108 Mbps (Super G mode)
  - Modulation:
    - Orthogonal Frequency Divisional Multiplexing (OFDM)
    - BPSK at 6 and 9 Mbps
    - QPSK at 12 and 18 Mbps
    - 16-quadrature amplitude modulation (QAM) at 24 and 36Mbps
    - 64-QAM at 48 and 54Mbps

- Transmit Output Power (Typical):
  - 18 dBm at 6 ~ 24Mbps
  - 18 dBm at 36Mbps
  - 17 dBm at 48Mbps
  - 16 dBm at 54Mbps

Note: Maximum power setting will vary according to individual country regulations.

- Receive Sensitivity (Typical):
  - -89dBm at 6Mbps
  - -73dBm at 48Mbps
  - -70dBm at 54Mbps

- **802.11a**
  - Frequency band
    - 5.25 ~ 5.35GHz/5.725 ~ 5.825GHz

Note: Frequency band setting will vary according to individual country regulations.

- Data rate:
  - 6, 9, 12, 18, 24, 36,48, 54 Mbps
  - 72, 96, 108 Mbps (Super A mode)
- Modulation:
  - Orthogonal Frequency Divisional Multiplexing (OFDM)
  - BPSK at 6 and 9 Mbps
  - QPSK at 12 and 18 Mbps
  - 16-quadrature amplitude modulation (QAM) at 24 and 36Mbps
  - 64-QAM at 48 and 54Mbps
- Transmit Output Power (Typical):
  - 18 dBm at 6 ~ 24Mbps
  - 16 dBm at 36Mbps
  - 15 dBm at 48Mbps
  - 14 dBm at 54Mbps

Note: Maximum power setting will vary according to individual country regulations.

- Receive Sensitivity (Typical):
  - -84dBm at 6Mbps
  - -70dBm at 48Mbps
  - -68dBm at 54Mbps

LED Indicator Definition

LED	Description
Power	If the light is on then the unit has power and is on If the light is off then the unit dos not have power and is off.
LAN	If this light is on, the unit is connected to the network. If this light is off, the unit does not have an active connection to the network.
WLAN	If the light is on, it indicates the WLAN is active. If the light is blinking, it indicates data transmission: 1. LED blinking slowly (every 1 second) indicates there is a connection and the signal quality is poor. 2. LED blinking fast indicates there is a connection and the signal quality is good. 3. LED steady indicates there is a connection and the signal quality is excellent.

Operating Temperature:

- -5º C ~ +50º C (+23º F ~ +122º F)

Storage Temperature:

- -40º ~ +80º C (-40º F ~ +158º F)

Operating Humidity:

- 0-95% non-condensing

Chapter 3: Configuration

Preliminary Configuration Steps

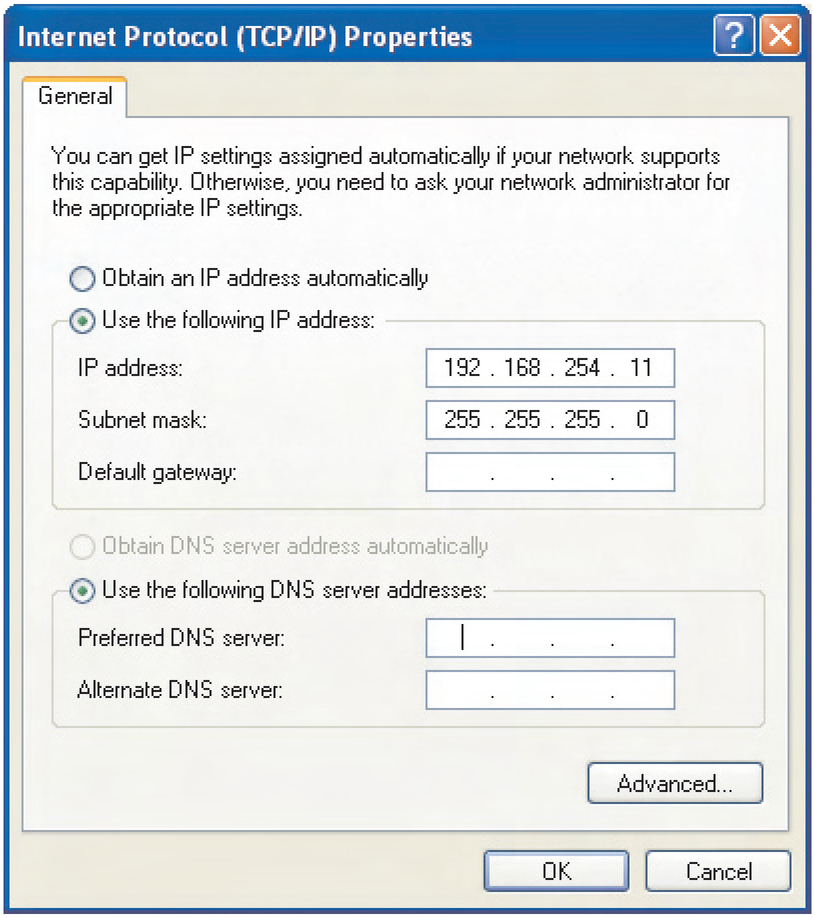
For the initial configuration, the 523C/E network administrator may need the following information:

- IP address – a list of IP addresses available on the organization's LAN that are available to be used for assignment to the 523C/E
- Subnet Mask for the LAN
- Default IP address of the 523C/E (192.168.254.254)
- DNS IP address
- The MAC addresses of all the wireless cards that will be used to access the 523C/E network of access points (if manual bridging mode is used, or if MAC address filtering is to be enabled)
- The appropriate encryption key for Static AES if state-of-the art key management will be used. Alternately, the appropriate WEP key.

Initial Setup using the LAN Ethernet Port

Plug one end of an RJ-45 Ethernet cable to the LAN RJ-45 Ethernet port of the 523C/E and the other end to an Ethernet port on your laptop. In order to connect properly to the 523C/E on the LAN port, the TCP/IP parameters on your laptop must be set to a static IP address. Go to your network connection settings and modify your LAN connection TCP/IP properties.

Set the IP address and subnet mask. The IP address can be in the range of 192.168.254.*xxx*, where *xxx* can be from 2 to 199.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 254 . 11

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

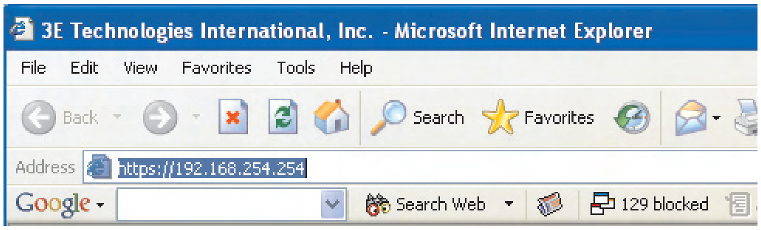
Alternate DNS server: . . .

Now you can open a browser and connect to the 523C/E to begin configuring the unit.

Login

On your computer, pull up a browser window and put the default URL for the523C/ELocal LAN in the address line.

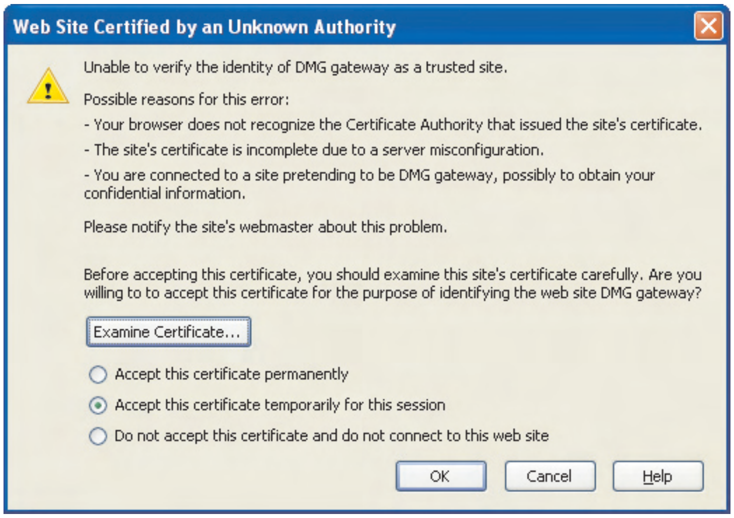
https://192.168.254.254



3E Technologies International, Inc. - Microsoft Internet Explorer

Address https://192.168.254.254

A warning window appears stating that it is unable to verify the identity of DMG gateway as a trusted site. Select "Accept this certificate temporarily for this session" and click Ok.



Web Site Certified by an Unknown Authority

Unable to verify the identity of DMG gateway as a trusted site.

Possible reasons for this error:

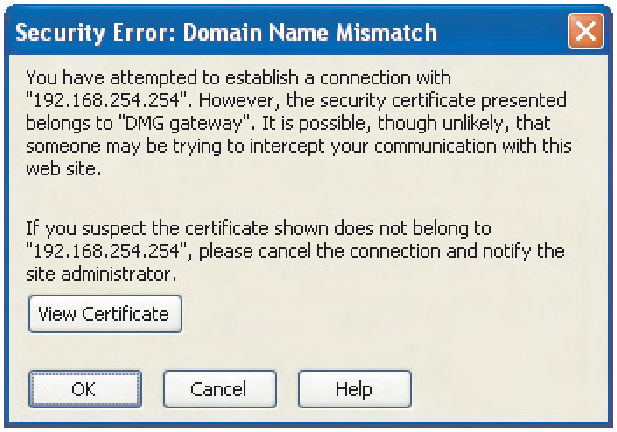
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be DMG gateway, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the web site DMG gateway?

○ Accept this certificate permanently
● Accept this certificate temporarily for this session
○ Do not accept this certificate and do not connect to this web site

Another security window pops open. Click Ok to continue.

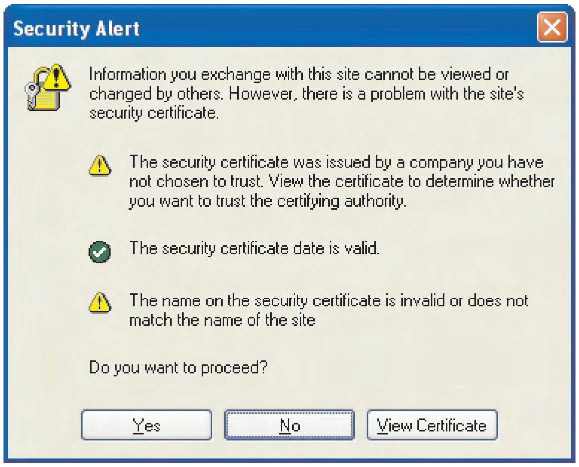


Security Error: Domain Name Mismatch

You have attempted to establish a connection with "192.168.254.254". However, the security certificate presented belongs to "DMG gateway". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.

If you suspect the certificate shown does not belong to "192.168.254.254", please cancel the connection and notify the site administrator.

A standard security alert window appears. Click **Yes** to continue.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

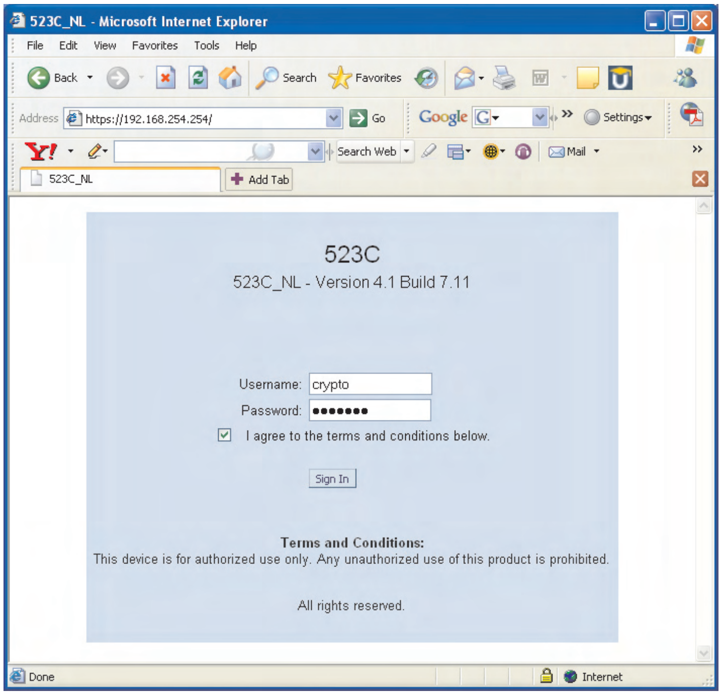
✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

The Login window appears.

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



Address: https://192.168.254.254/

523C

523C_NL - Version 4.1 Build 7.11

Username: crypto

Password: •••••••

☑ I agree to the terms and conditions below.

Sign In

Terms and Conditions:
This device is for authorized use only. Any unauthorized use of this product is prohibited.

All rights reserved.

NOTE: If your login session is in-active for more than 10 minutes, then you will have to re-authenticate your identity. If after three times you fail to re-authenticate then your account will be locked. The exception is if you are the last active CryptoOfficer on the system, then your account will not be locked. The **Admin User Management—List All Users** screen displays account status. If an account is locked, it will show a status of "Locked" and a reason of "bad passwd". Other accounts show status as "Active" and reason "Normal".

The CryptoOfficer is the only role that can unlock an account once it has been locked. Go to the **Admin User Management—List All Users** screen and click the unlock button at the end of the user entry.

Client Mode — Configuration

The default operating mode is Client mode. To switch to AP or Bridge mode go to the **System Configuration — Operating Mode** screen.

The following subsections describe the Client mode screens; followed by the AP mode screens, then the Bridge Mode screens.

System Configuration

There are three options under **System Configuration** :

- General
- Operating Mode
- Radio Region
- WAN

Each screen is described in detail in the following subsections.

General

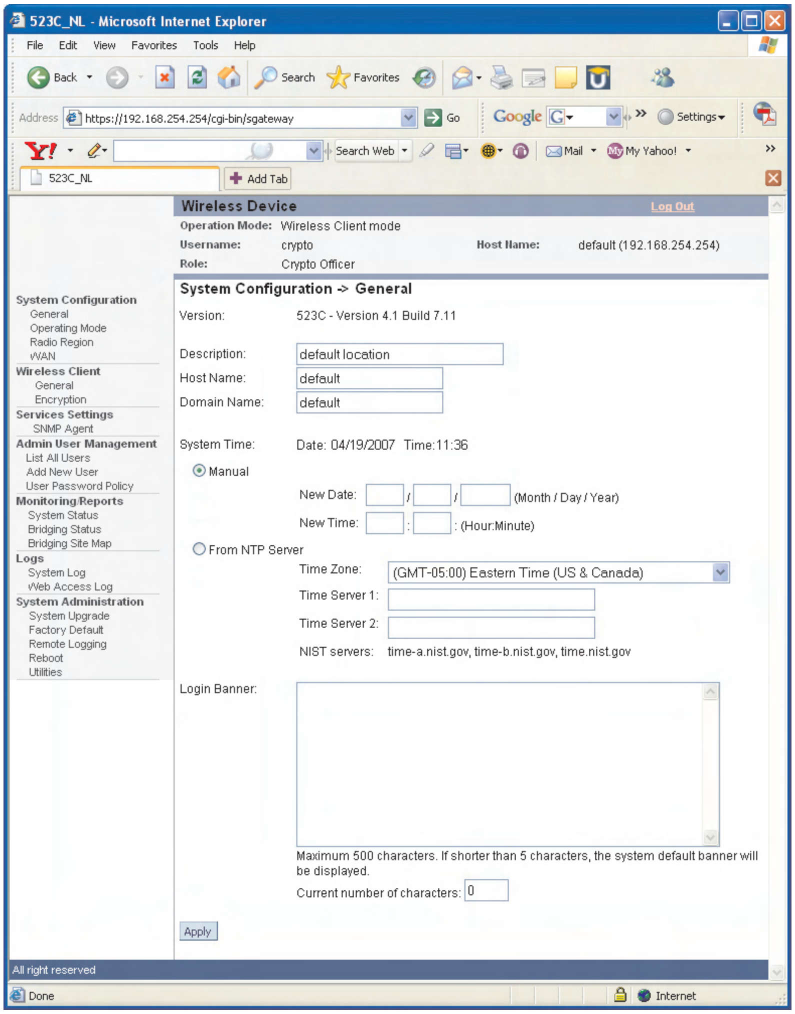
You will immediately be directed to the **System Configuration — General** screen for the 523C/E.

This screen lists the firmware version number for your 523C/E and allows you to set the Host Name and Domain Name as well as establish system date and time. (Host and Domain Names are both set at the factory for “default” but can optionally be assigned a unique name for each.) To set the date and time, you can do it manually or set it based on the NTP server.

NOTE: The CryptoOfficer is the only user who can set the date and time. The system date must be set to a date after 01/01/2005.

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

In the Description field you can enter a description of the physical location of the unit. This is useful when deploying units to remote locations. When you are satisfied with your changes, click **Apply**.



Wireless Device

Operation Mode: Wireless Client mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

System Configuration -> General

Version: 523C - Version 4.1 Build 7.11

Description: default location
Host Name: default
Domain Name: default

System Time: Date: 04/19/2007 Time:11:36

● Manual

New Date: [ ] / [ ] / [ ] (Month / Day / Year)
New Time: [ ] : [ ] : (Hour:Minute)

○ From NTP Server

Time Zone: (GMT-05:00) Eastern Time (US & Canada)
Time Server 1:
Time Server 2:
NIST servers: time-a.nist.gov, time-b.nist.gov, time.nist.gov

Login Banner:

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

Current number of characters: 0

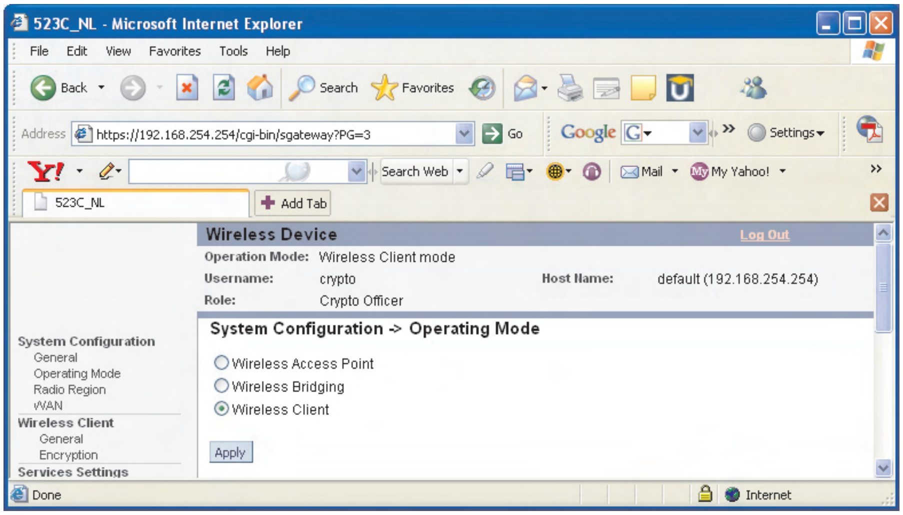
Apply

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

Operating Mode

This screen allows you to set the operating mode to either Wireless Access Point/Bridge or Client mode. You only need to visit this page if you will be changing modes.

Note that if you change modes your configuration will be lost.



Address: https://192.168.254.254/cgi-bin/sgateway?PG=3

Wireless Device

Operation Mode:	Wireless Client mode		
Username:	crypto	Host Name:	default (192.168.254.254)
Role:	Crypto Officer		

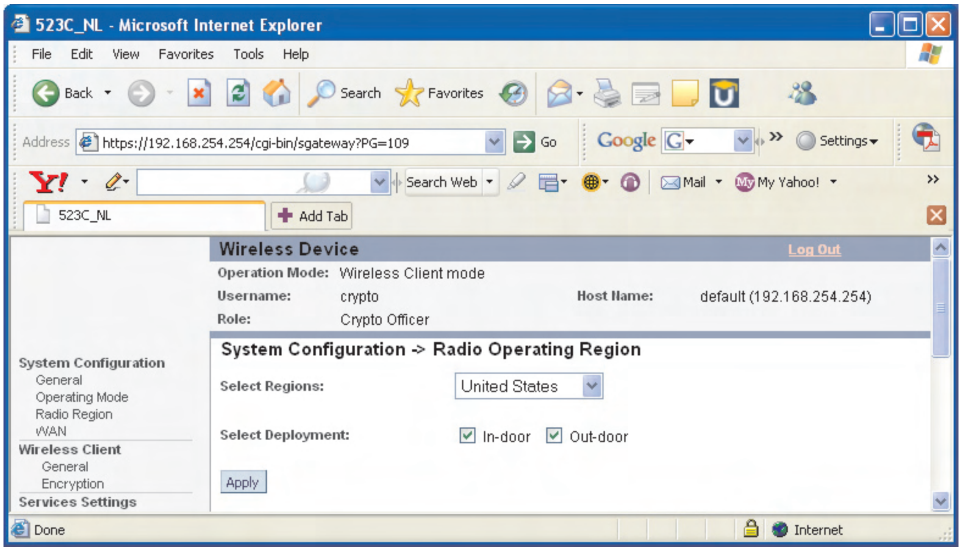
System Configuration -> Operating Mode

○ Wireless Access Point
○ Wireless Bridging
● Wireless Client

Apply

Radio Region

From this screen you can select the region where the unit will be located. You can also select weather the unit will be located indoors or outdoors.



Address: https://192.168.254.254/cgi-bin/sgateway?PG=109

Wireless Device

Operation Mode:	Wireless Client mode		
Username:	crypto	Host Name:	default (192.168.254.254)
Role:	Crypto Officer		

System Configuration -> Radio Operating Region

Select Regions: United States

Select Deployment: ☑ In-door ☑ Out-door

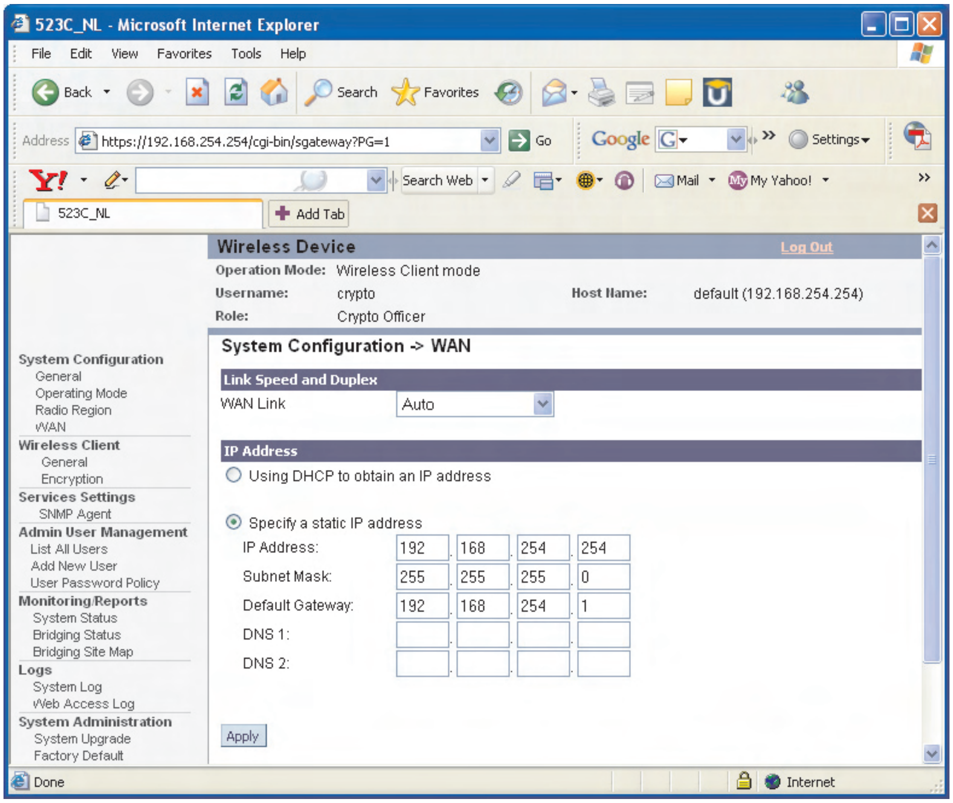
Apply

WAN

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

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

Click **Apply** to accept changes.


523C_NL - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.254.254/cgi-bin/sgateway?PG=1 Go
Google Settings
Search Web Mail My Yahoo!
523C_NL
Add Tab
Done
Internet

Wireless Device Log Out

Operation Mode:	Wireless Client mode		
Username:	crypto	**Host Name:**	default (192.168.254.254)
Role:	Crypto Officer		

System Configuration
General
Operating Mode
Radio Region
WAN
Wireless Client
General
Encryption
Services Settings
SNMP Agent
Admin User Management
List All Users
Add New User
User Password Policy
Monitoring/Reports
System Status
Bridging Status
Bridging Site Map
Logs
System Log
Web Access Log
System Administration
System Upgrade
Factory Default

System Configuration -> WAN

Link Speed and Duplex

WAN Link: Auto

IP Address

○ Using DHCP to obtain an IP address

● Specify a static IP address

IP Address:	192	168	254	254
Subnet Mask:	255	255	255	0
Default Gateway:	192	168	254	1
DNS 1:				
DNS 2:				

Apply

NOTE: After changing the network address you will no longer be able to access the above configuration page with the default IP address. You will have to change the browser URL to reflect the new IP address and log in again.

NOTE: If DHCP is selected, a new IP address would be given to the 523C/E unit after clicking **Apply**. To log into to unit and keep setting it up, the new IP address needs to be obtained from your Network Administrator. Another way to obtain the new IP address is to set up "Remote Logging" before setting up WAN using DHCP.

Wireless Client

There are two options under **Wireless Client** :

- General
- Encryption

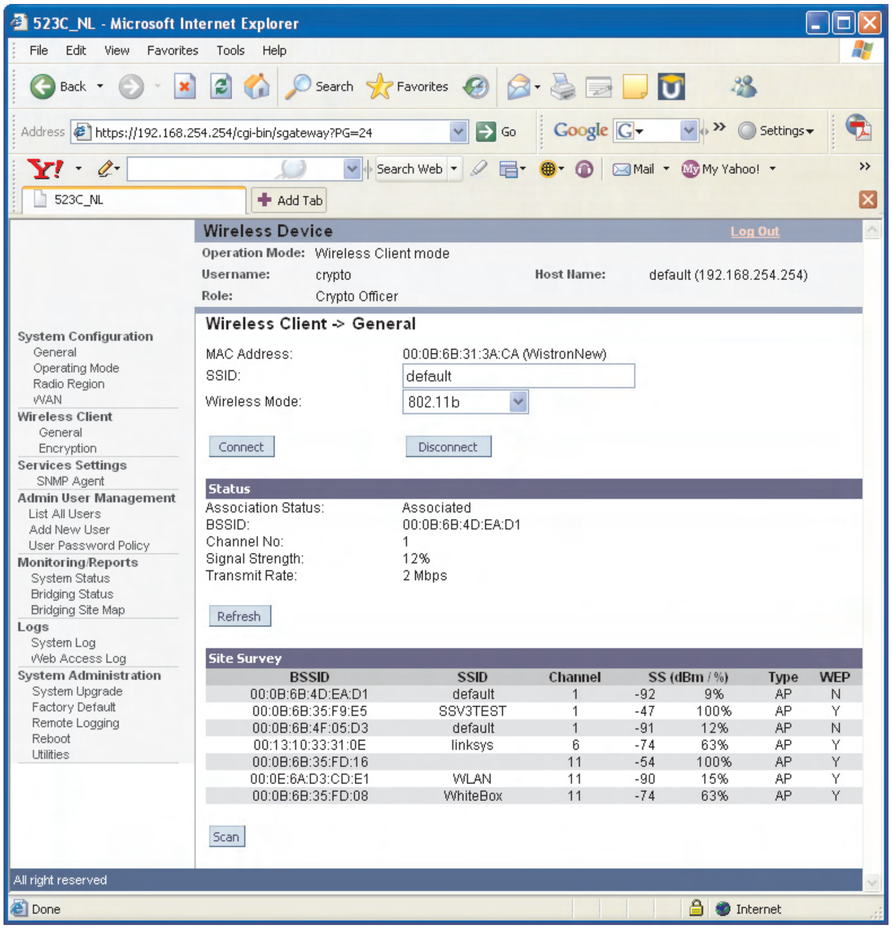
Each screen is described in detail in the following subsections.

General

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

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

- 802.11b
- 802.11g
- 802.11g Super
- 802.11a
- 802.11a Turbo



Wireless Device

Operation Mode: Wireless Client mode
Username: crypto Host Name: default (192.168.254.254)
Role: Crypto Officer

Wireless Client -> General

MAC Address: 00:0B:6B:31:3A:CA (WistronNew)
SSID: default
Wireless Mode: 802.11b

Status

Association Status: Associated
BSSID: 00:0B:6B:4D:EA:D1
Channel No: 1
Signal Strength: 12%
Transmit Rate: 2 Mbps

Site Survey

BSSID	SSID	Channel	SS (dBm / %)		Type	WEP
00:0B:6B:4D:EA:D1	default	1	-92	9%	AP	N
00:0B:6B:35:F9:E5	SSV3TEST	1	-47	100%	AP	Y
00:0B:6B:4F:05:D3	default	1	-91	12%	AP	N
00:13:10:33:31:0E	linksys	6	-74	63%	AP	Y
00:0B:6B:35:FD:16		11	-54	100%	AP	Y
00:0E:6A:D3:CD:E1	WLAN	11	-90	15%	AP	Y
00:0B:6B:35:FD:08	WhiteBox	11	-74	63%	AP	Y

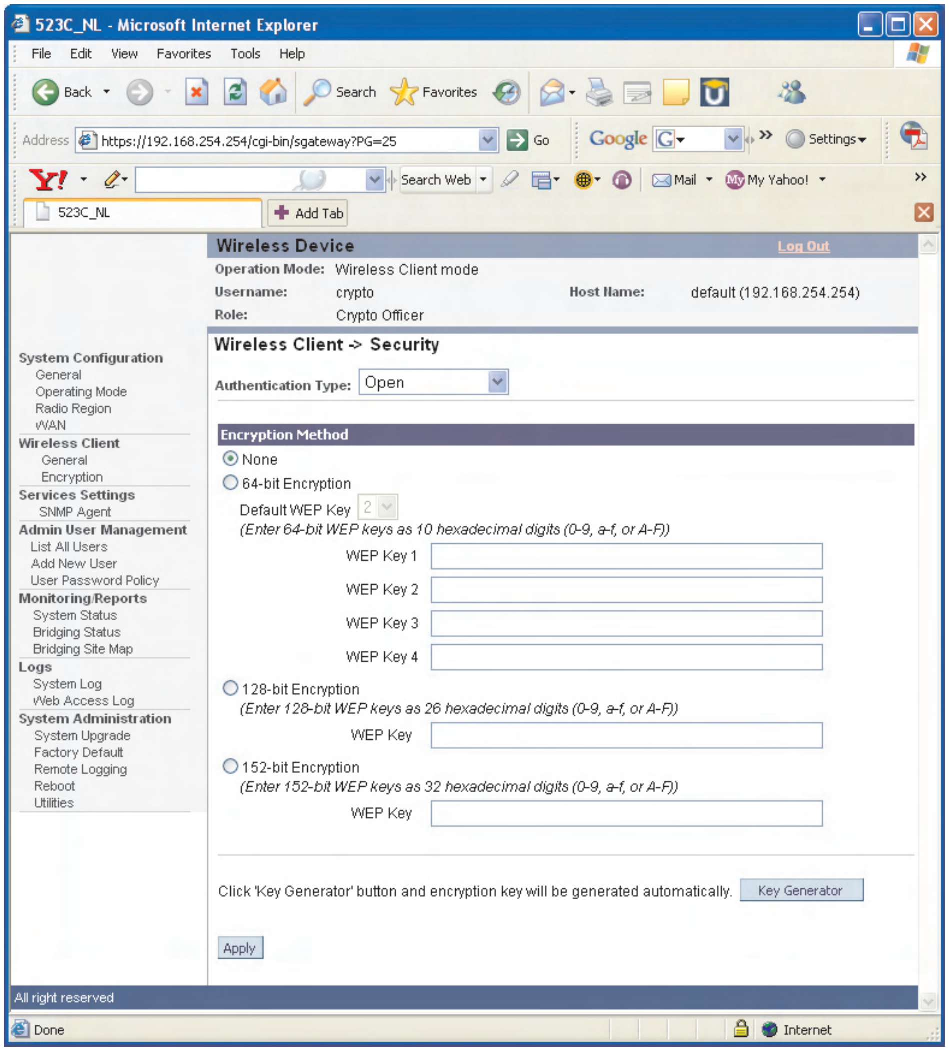
Encryption

The **Wireless Client — Encryption** screen is used to configure the security for the wireless client. This is an important page to set up to ensure that your client is working correctly. The encryption key that you use on this screen must be the same for any client connected to your network in order for communication to occur. On this screen you can select Open, WPA-PSK, WPA2-PSK, WPA-802.1x, or WPA2-802.1x.

Open

In order to have the 523C/E work with open encryption, you must actively select **None, 64-bit, 128-bit, or 152-bit WEP** and click **Apply**.

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



Address: https://192.168.254.254/cgi-bin/sgateway?PG=25

Wireless Device

Operation Mode: Wireless Client mode

Username: crypto

Host Name: default (192.168.254.254)

Role: Crypto Officer

Wireless Client -> Security

Authentication Type: Open

Encryption Method

● None

○ 64-bit Encryption

Default WEP Key 2

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

WEP Key 1

WEP Key 2

WEP Key 3

WEP Key 4

○ 128-bit Encryption

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

WEP Key

○ 152-bit Encryption

(Enter 152-bit WEP keys as 32 hexadecimal digits (0-9, a-f, or A-F))

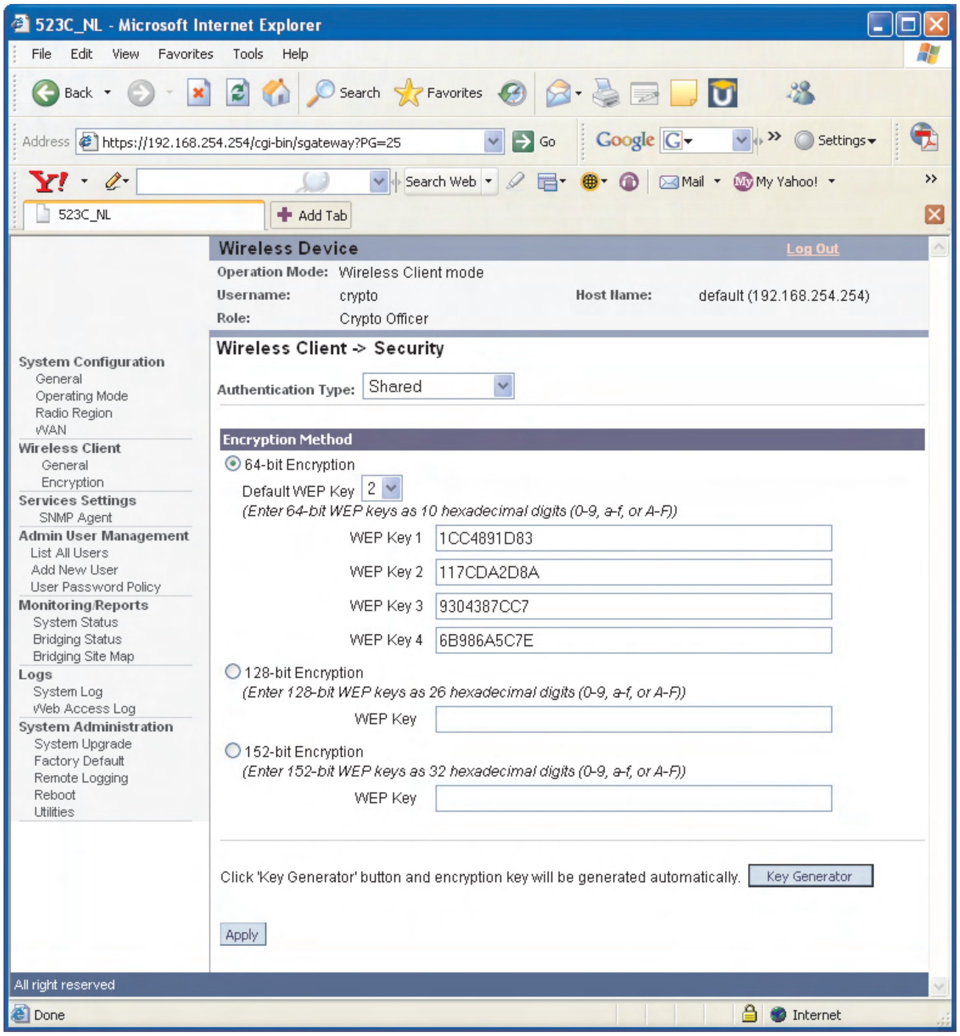
WEP Key

Click 'Key Generator' button and encryption key will be generated automatically.

Shared

In order to have the 523C/E work with shared encryption, you must actively select **64-bit, 128-bit, or 152-bit WEP** and click **Apply**.

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



Address: https://192.168.254.254/cgi-bin/sgateway?PG=25

Wireless Device

Operation Mode: Wireless Client mode

Username: crypto Host Name: default (192.168.254.254)

Role: Crypto Officer

Wireless Client -> Security

Authentication Type: Shared

Encryption Method

● 64-bit Encryption

Default WEP Key 2

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

WEP Key 1 1CC4891D83

WEP Key 2 117CDA2D8A

WEP Key 3 9304387CC7

WEP Key 4 6B986A5C7E

○ 128-bit Encryption

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

WEP Key

○ 152-bit Encryption

(Enter 152-bit WEP keys as 32 hexadecimal digits (0-9, a-f, or A-F))

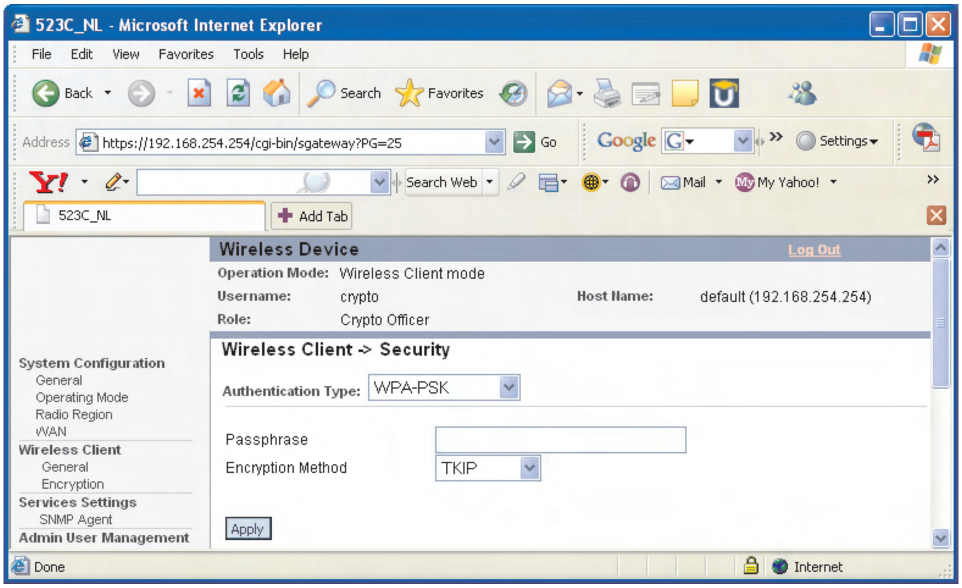
WEP Key

Click 'Key Generator' button and encryption key will be generated automatically. Key Generator

Apply

WPA-PSK

If you select WPA-PSK, enter a passphrase. The passphrase can be from 8-63 alphnumeric characters.



Wireless Device

Operation Mode: Wireless Client mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

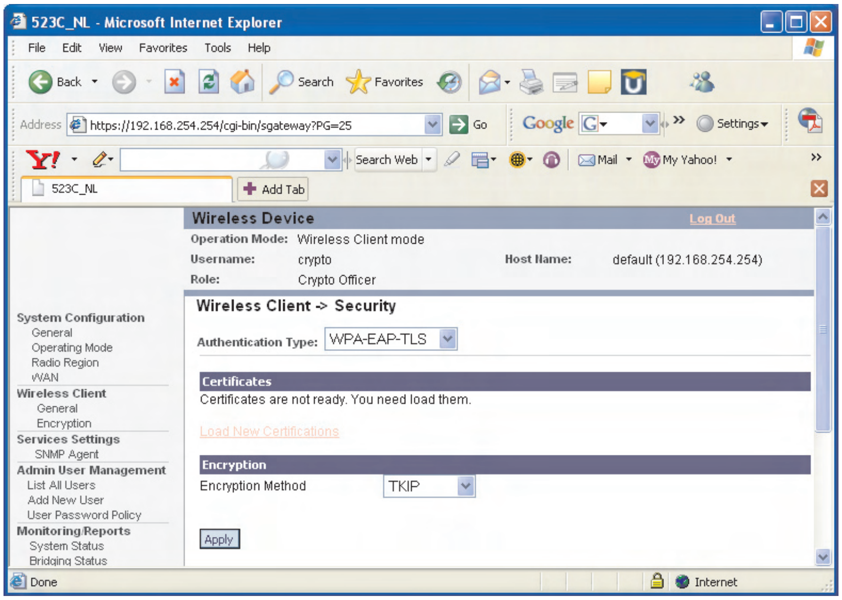
Wireless Client -> Security

Authentication Type: WPA-PSK

Passphrase
Encryption Method: TKIP

WPA-EAP-TLS

If you select WPA-EAP-TLS you must have root and client certificates avialable. If no certificates are loaded, click on Load New Certificates.



Wireless Device

Operation Mode: Wireless Client mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

Wireless Client -> Security

Authentication Type: WPA-EAP-TLS

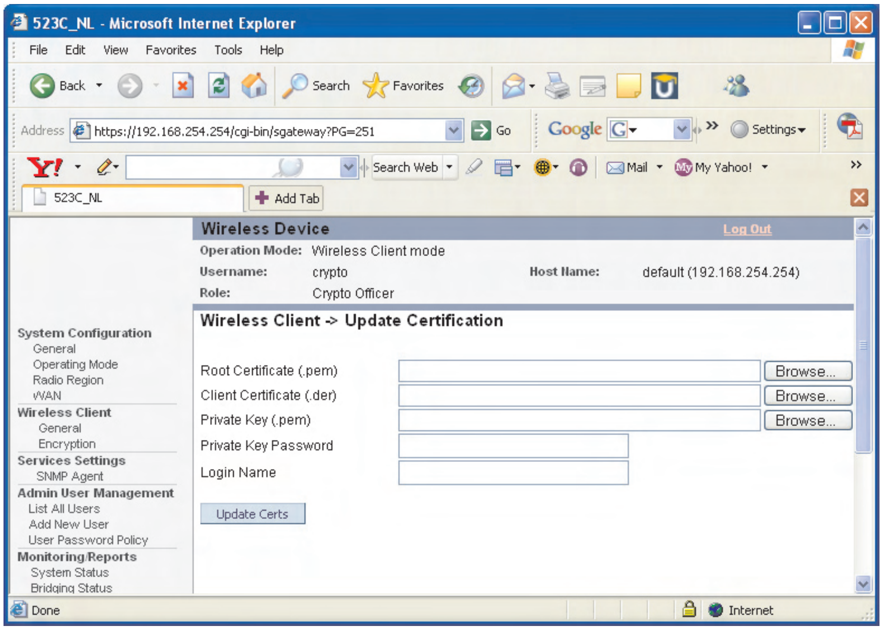
Certificates

Certificates are not ready. You need load them.

Encryption

Encryption Method: TKIP

If you click on **Load New Configurations** the following screen appears.



523C_NL - Microsoft Internet Explorer

Address https://192.168.254.254/cgi-bin/sgateway?PG=251

Wireless Device

Operation Mode: Wireless Client mode

Username: crypto

Host Name: default (192.168.254.254)

Role: Crypto Officer

Wireless Client -> Update Certification

Root Certificate (.pem) [Browse...]

Client Certificate (.der) [Browse...]

Private Key (.pem) [Browse...]

Private Key Password

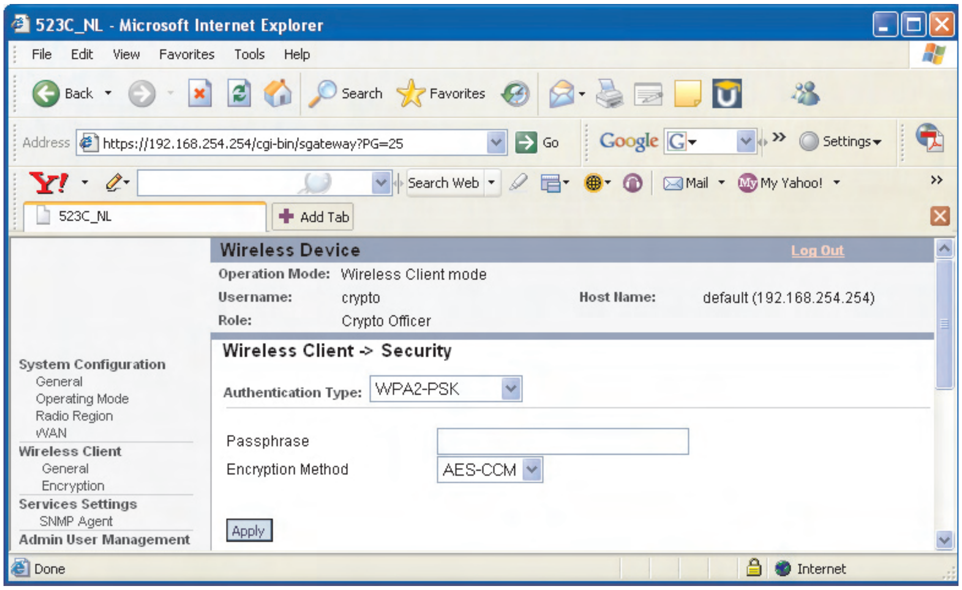
Login Name

[Update Certs]

Use the Browse button to search for your root and client certificates. Also select the Private Key and enter its password. The login name refers to your login name for the security server you are using.

WPA2-PSK

If you select WPA-PSK, enter a passphrase. The passphrase can be from 8-63 alphnumeric characters.



523C_NL - Microsoft Internet Explorer

Address https://192.168.254.254/cgi-bin/sgateway?PG=25

Wireless Device

Operation Mode: Wireless Client mode

Username: crypto

Host Name: default (192.168.254.254)

Role: Crypto Officer

Wireless Client -> Security

Authentication Type: WPA2-PSK

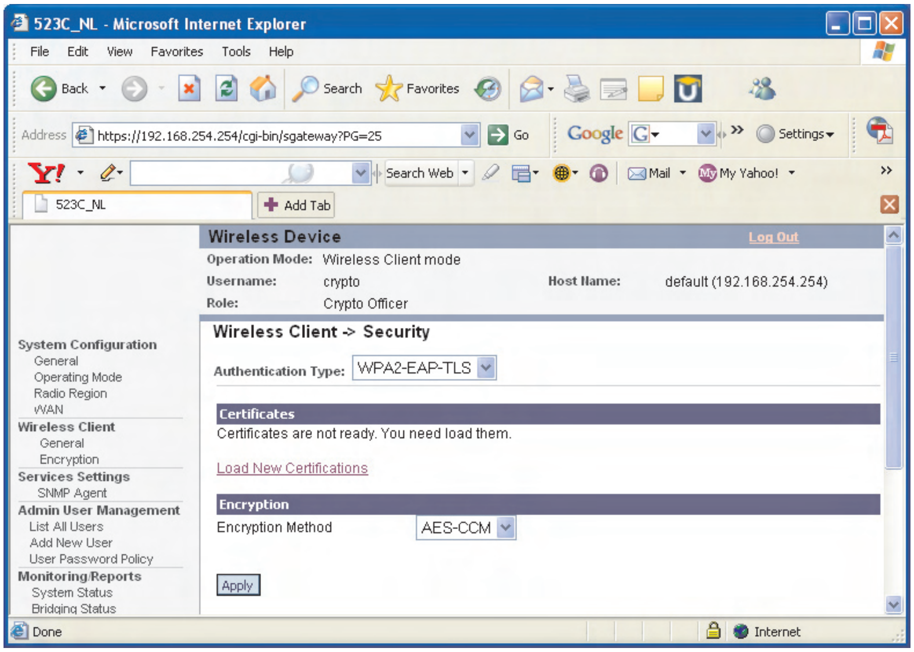
Passphrase

Encryption Method: AES-CCM

[Apply]

WPA2-EAP-TLS

If you select WPA2-EAP-TLS you must have root and client certificates avialable. If no certificates are loaded, click on Load New Certificates.



Wireless Device

Operation Mode: Wireless Client mode

Username: crypto

Host Name: default (192.168.254.254)

Role: Crypto Officer

Wireless Client -> Security

Authentication Type: WPA2-EAP-TLS

Certificates

Certificates are not ready. You need load them.

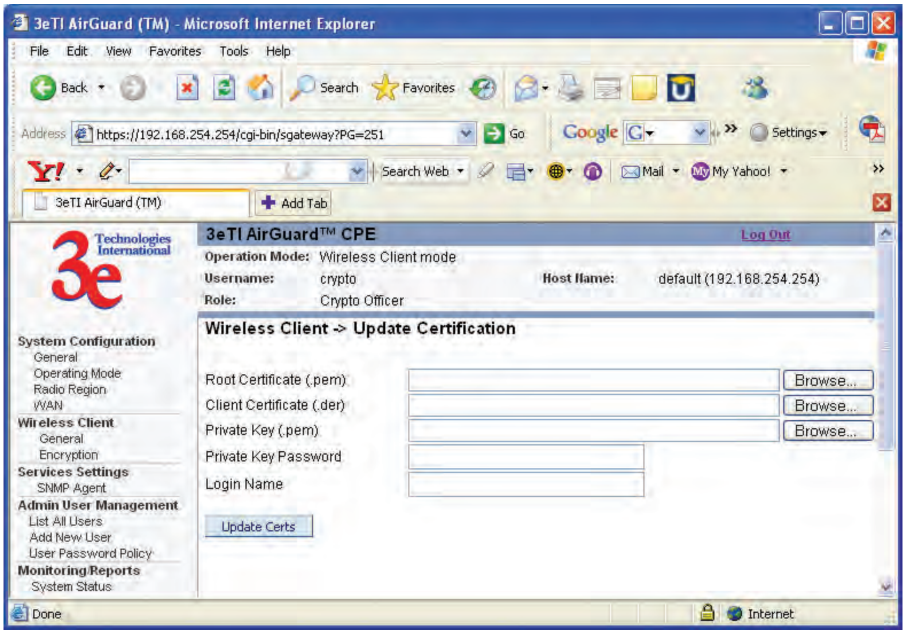
Load New Certifications

Encryption

Encryption Method AES-CCM

Apply

If you click on **Load New Configurations** the following screen appears.



3eTI AirGuard™ CPE

Operation Mode: Wireless Client mode

Username: crypto

Host Name: default (192.168.254.254)

Role: Crypto Officer

Wireless Client -> Update Certification

Root Certificate (.pem) Browse...

Client Certificate (.der) Browse...

Private Key (.pem) Browse...

Private Key Password

Login Name

Update Certs

Use the Browse button to search for your root and client certificates. Also select the Private Key and enter its password. The login name refers to your login name for the security server you are using.

Service Settings

There is only one option under **Service Settings** in Client mode:

- SNMP Agent

SNMP Agent

The **Service Settings — SNMP Agent** screen allows you to set up an SNMP Agent. The agent is a software module that collects and stores management information for use in a network management system. The 523C/E'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.

SNMPv1 (Simple Network Management Protocol) and SNMPv2c, along with the associated Management Information Base (MIB), encourage trap-directed notification.

The idea behind trap-directed notification is as follows: if a manager is responsible for a large number of devices, and each device has a large number of objects, it is impractical for him to poll or request information from every object on every device. The solution is for each agent on the managed device to notify the manager without solicitation. It does this by sending a message known as a trap of the event.

After receiving the event, the manager displays it and may choose to take an action based on the event. For instance, the manager can poll the agent directly, or poll other associated device agents to get a better understanding of the event.

Trap-directed notification can result in substantial savings of network and agent resources by eliminating the need for frivolous SNMP requests. However, it is not possible to totally eliminate SNMP polling. SNMP requests are required for discovery and topology changes. In addition, a managed device agent can not send a trap, if the device has had a catastrophic outage.

SNMPv1 traps are defined in RFC 1157, with the following fields:

- *Enterprise* - Identifies the type of managed object generating the trap.
- *Agent address* - Provides the address of the managed object generating the trap.
- *Generic trap type* - Indicates one of a number of generic trap types.
- *Specific trap code* - Indicates one of a number of specific trap codes.
- *Time stamp* - Provides the amount of time that has elapsed between the last network reinitialization and generation of the trap.
- *Variable bindings* - The data field of trap containing PDU. Each variable binding associates a particular MIB object instance with its current value.

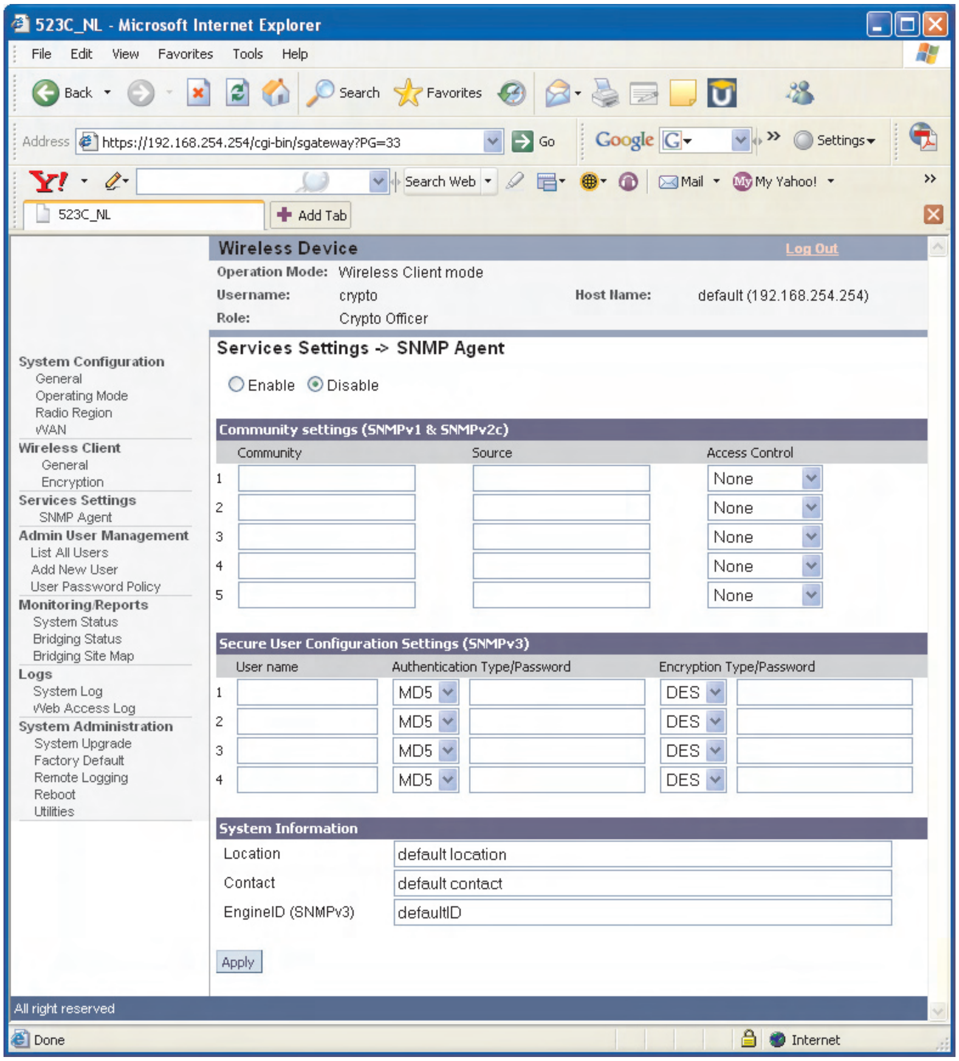
Standard generic traps are: coldStart, warmStart, linkDown, linkUp, authenticationFailure, egpNeighborLoss.

In the current release, warmStart, linkDown, linkUp, and authenticationFailure 5 generic traps are implemented and you can send those traps using SNMPv1 Trap PDU format.

For generic SNMPv1 traps, some generic traps are redefined by adding some bound variables.

For example, when a trap receiver received a warmStart trap, it should be able to see one variable associated with this trap. In the variableName field it shows the enterprise oid, in the varibleValue field it indicates the warmStart reason.

Additionally, a device does not send a trap to a network management system unless it is configured to do so. A device must know that it should send a trap.


523C_NL - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address https://192.168.254.254/cgi-bin/sgateway?PG=33
Go
Google
Settings
Search Web
Mail
My Yahoo!
523C_NL
Add Tab
Done
Internet

Wireless Device Log Out

Operation Mode: Wireless Client mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

System Configuration
- General
- Operating Mode
- Radio Region
- WAN

Wireless Client
- General
- Encryption

Services Settings
- SNMP Agent

Admin User Management
- List All Users
- Add New User
- User Password Policy

Monitoring/Reports
- System Status
- Bridging Status
- Bridging Site Map

Logs
- System Log
- Web Access Log

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

Services Settings -> SNMP Agent

○ Enable ● Disable

Community settings (SNMPv1 & SNMPv2c)

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

Secure User Configuration Settings (SNMPv3)

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

System Information

Location	default location
Contact	default contact
EngineID (SNMPv3)	defaultID

Apply

All right reserved

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

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

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

Admin User Management

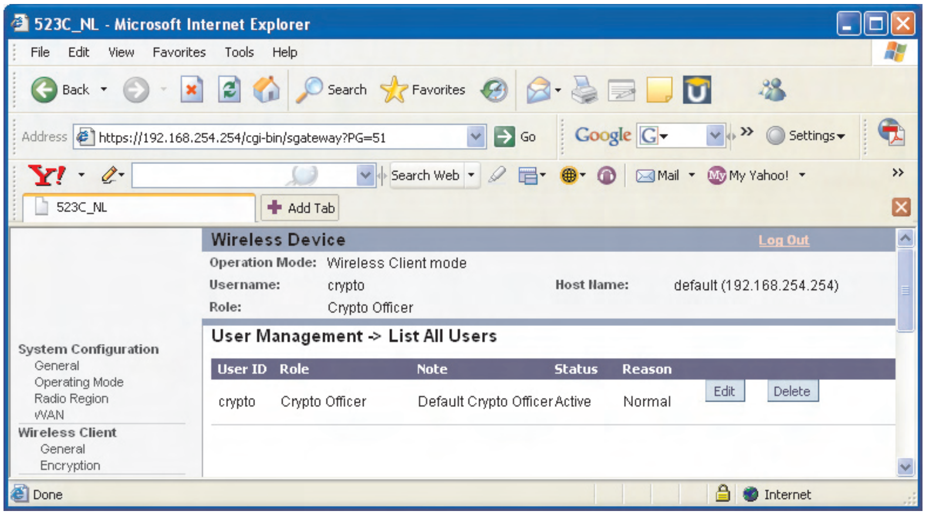
There are three options under **Admin User Management** :

- List All Users
  - Edit User
- Add New Users
- User Password Policy

Each screen is described in detail in the following subsections.

List All Users

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



Address: https://192.168.254.254/cgi-bin/sgateway?PG=51

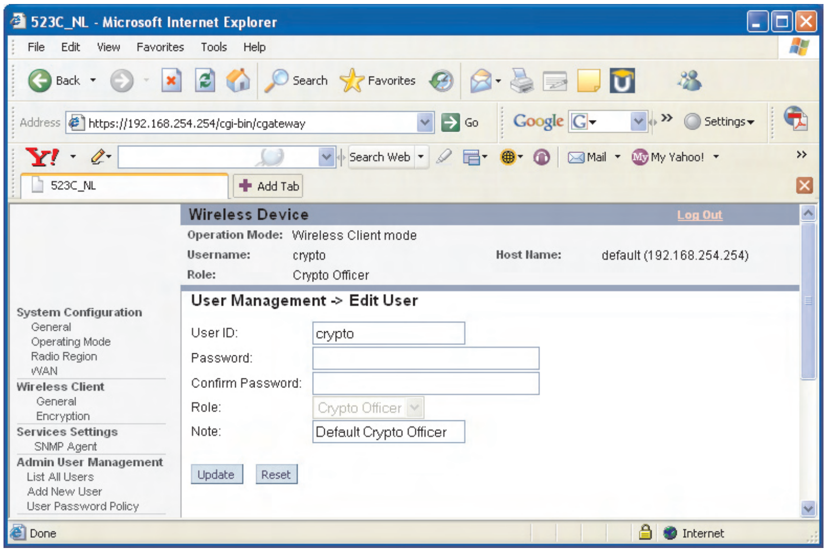
Wireless Device

Operation Mode: Wireless Client mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

User Management -> List All Users

User ID	Role	Note	Status	Reason	
crypto	Crypto Officer	Default Crypto Officer	Active	Normal	Edit Delete

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



Wireless Device

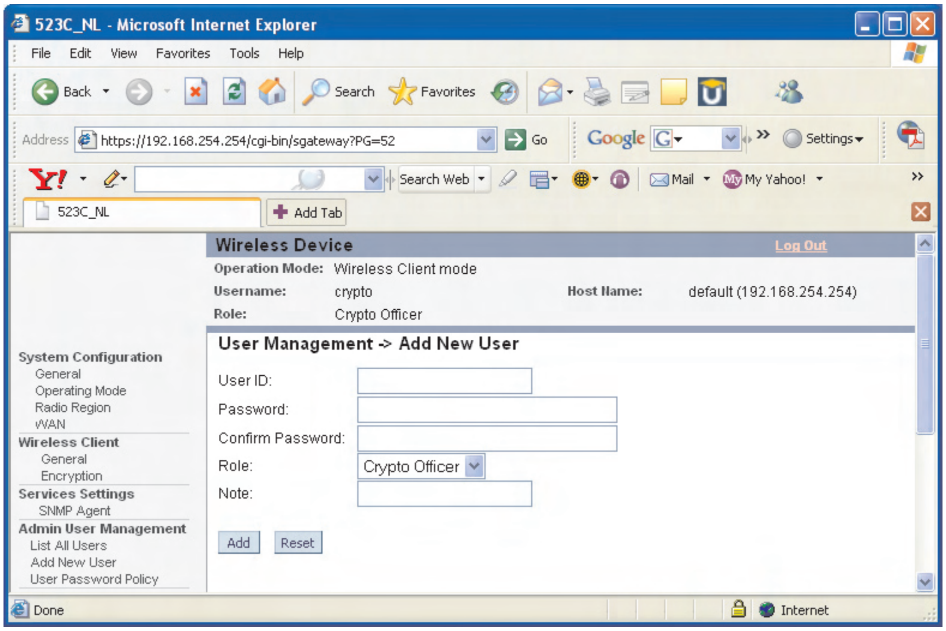
Operation Mode: Wireless Client mode
Username: crypto Host Name: default (192.168.254.254)
Role: Crypto Officer

User Management -> Edit User

User ID:	crypto
Password:	
Confirm Password:	
Role:	Crypto Officer
Note:	Default Crypto Officer

Add New User

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



Wireless Device

Operation Mode: Wireless Client mode
Username: crypto Host Name: default (192.168.254.254)
Role: Crypto Officer

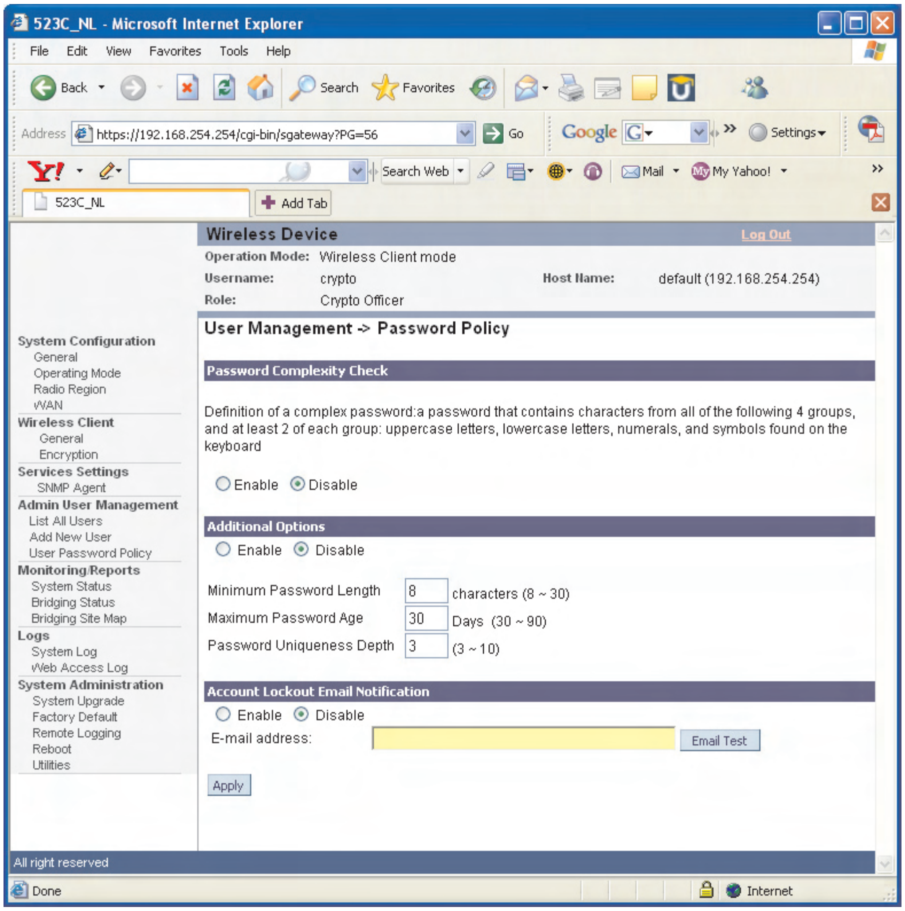
User Management -> Add New User

User ID:	
Password:	
Confirm Password:	
Role:	Crypto Officer
Note:	

User Password Policy

The **Admin User Management — User Password Policy** screen allows you to enable a **Password Complexity Check**. The definition of a complex password is a password that contains characters from all of the following 4 groups and at least two of each group: uppercase letters, lowercase letters, numerals, and symbols found on the keyboard. If enabled, you must also select minimum password length. Click **Apply** to save your selection.

You can also set up "Account Lockout Email Notification" where you can enter an email address and you will receive an email notification for anyone who is locked out of the system.



Wireless Device

Operation Mode: Wireless Client mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

User Management -> Password Policy

Password Complexity Check

Definition of a complex password:a password that contains characters from all of the following 4 groups, and at least 2 of each group: uppercase letters, lowercase letters, numerals, and symbols found on the keyboard

○ Enable ● Disable

Additional Options

○ Enable ● Disable

Minimum Password Length 8 characters (8 ~ 30)
Maximum Password Age 30 Days (30 ~ 90)
Password Uniqueness Depth 3 (3 ~ 10)

Account Lockout Email Notification

○ Enable ● Disable

E-mail address: Email Test

Apply

Monitoring/Reports

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

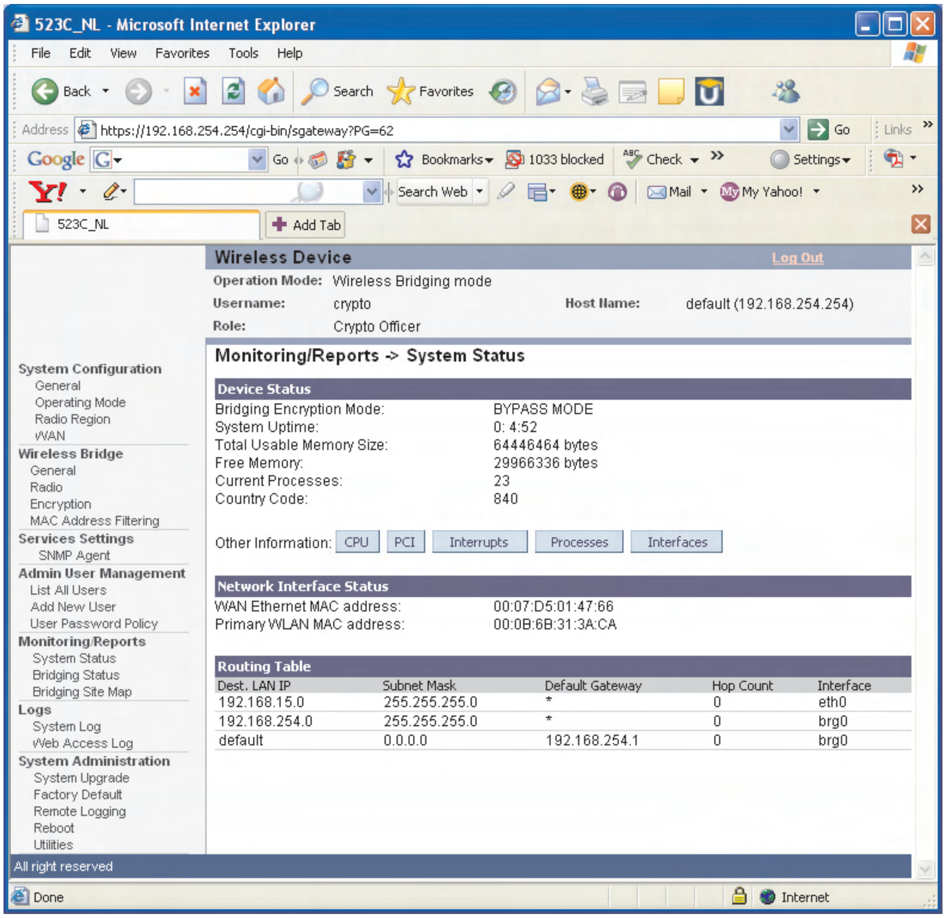
There are three options under **Monitoring/Reports** :

- System Status
- Bridging Status
- Bridging Site Map

Each screen is described in detail in the following subsections.

System Status

The **Monitoring/Report — System Status** screen displays the status of the 523C/E device, the network interface, and the routing table.



Wireless Device

Operation Mode: Wireless Bridging mode
Username: crypto Host Name: default (192.168.254.254)
Role: Crypto Officer

Monitoring/Reports -> System Status

Device Status

Bridging Encryption Mode: BYPASS MODE
System Uptime: 0: 4:52
Total Usable Memory Size: 64446464 bytes
Free Memory: 29966336 bytes
Current Processes: 23
Country Code: 840

Other Information: CPU PCI Interrupts Processes Interfaces

Network Interface Status

WAN Ethernet MAC address: 00:07:D5:01:47:66
Primary WLAN MAC address: 00:0B:6B:31:3A:CA

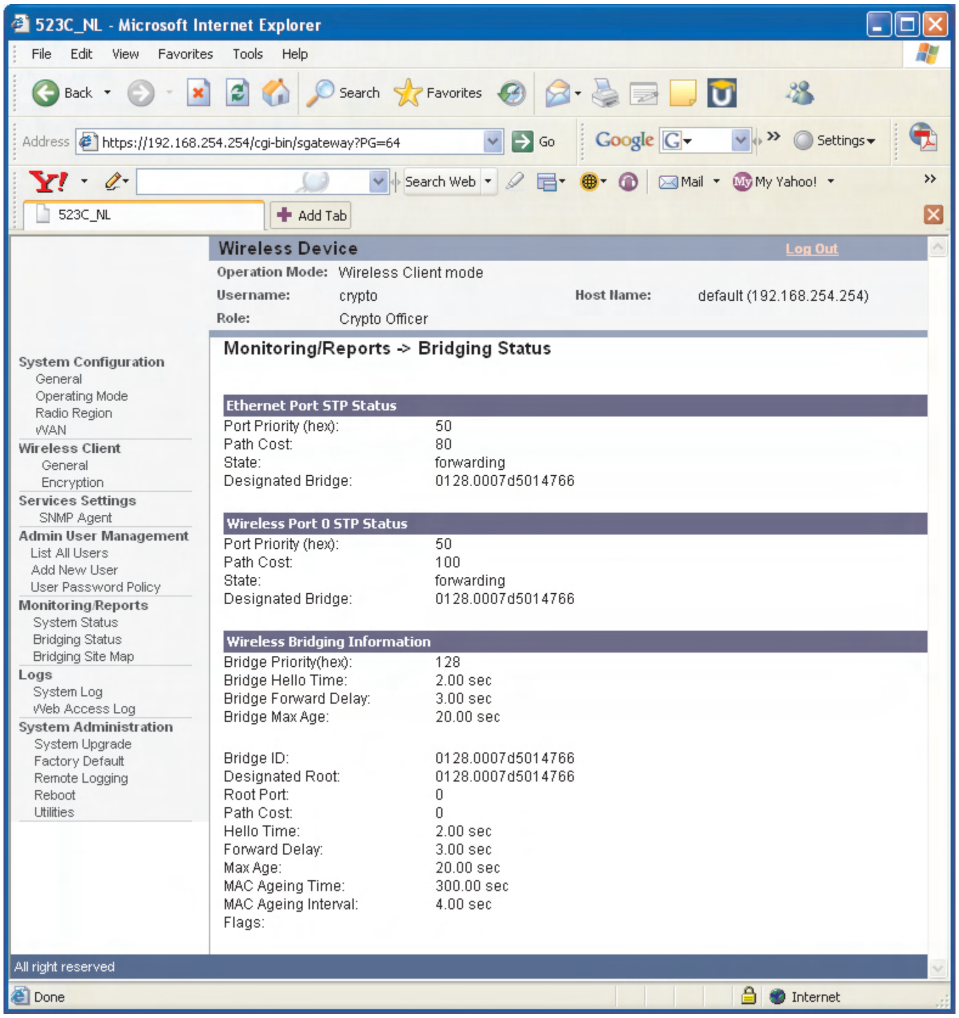
Routing Table

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

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

Bridging Status

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



Wireless Device

Operation Mode:	Wireless Client mode		
Username:	crypto	Host Name:	default (192.168.254.254)
Role:	Crypto Officer		

Monitoring/Reports -> Bridging Status

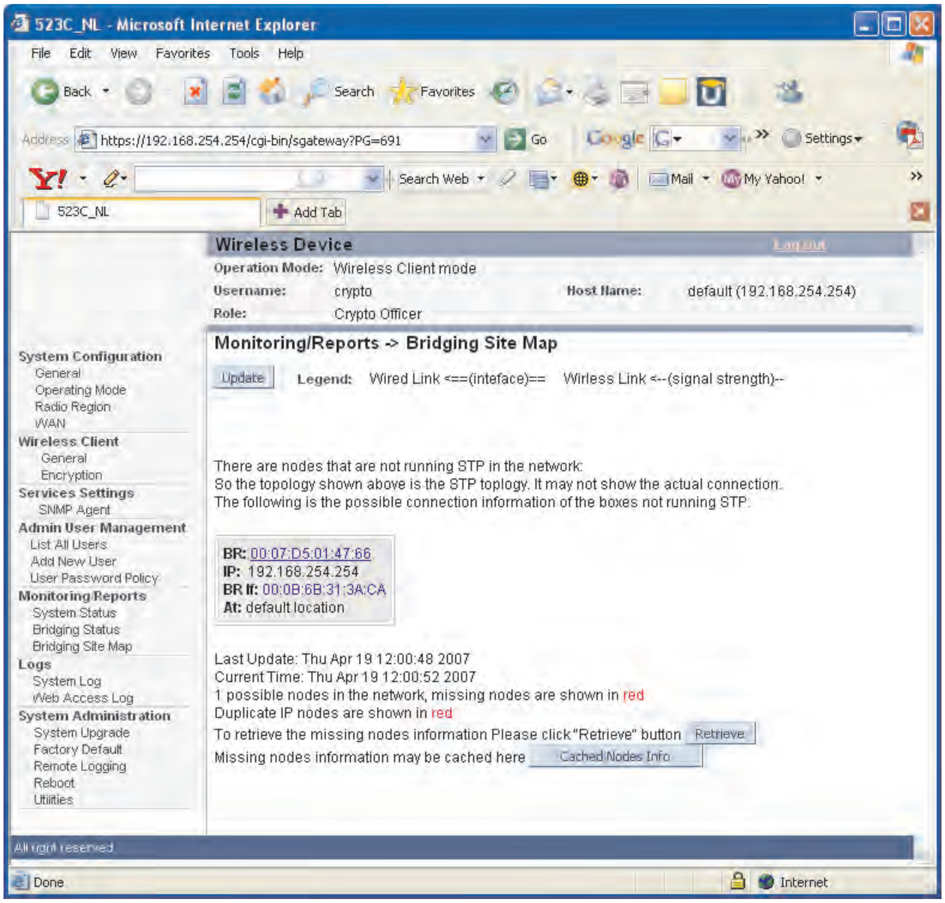
Ethernet Port STP Status	
Port Priority (hex):	50
Path Cost:	80
State:	forwarding
Designated Bridge:	0128.0007d5014766

Wireless Port 0 STP Status	
Port Priority (hex):	50
Path Cost:	100
State:	forwarding
Designated Bridge:	0128.0007d5014766

Wireless Bridging Information	
Bridge Priority(hex):	128
Bridge Hello Time:	2.00 sec
Bridge Forward Delay:	3.00 sec
Bridge Max Age:	20.00 sec
Bridge ID:	0128.0007d5014766
Designated Root:	0128.0007d5014766
Root Port:	0
Path Cost:	0
Hello Time:	2.00 sec
Forward Delay:	3.00 sec
Max Age:	20.00 sec
MAC Ageing Time:	300.00 sec
MAC Ageing Interval:	4.00 sec
Flags:	

Bridge Site Map

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



Wireless Device

Operation Mode: Wireless Client mode
Username: crypto Host Name: default (192.168.254.254)
Role: Crypto Officer

Monitoring/Reports -> Bridging Site Map

Legend: Wired Link <==(inteface)== Wirless Link <--(signal strength)--

There are nodes that are not running STP in the network:
So the topology shown above is the STP toplogy. It may not show the actual connection.
The following is the possible connection information of the boxes not running STP.

BR: 00:07:D5:01:47:66
IP: 192.168.254.254
BR If: 00:0B:6B:31:3A:CA
At: default location

Last Update: Thu Apr 19 12:00:48 2007
Current Time: Thu Apr 19 12:00:52 2007
1 possible nodes in the network, missing nodes are shown in red
Duplicate IP nodes are shown in red
To retrieve the missing nodes information Please click "Retrieve" button
Missing nodes information may be cached here

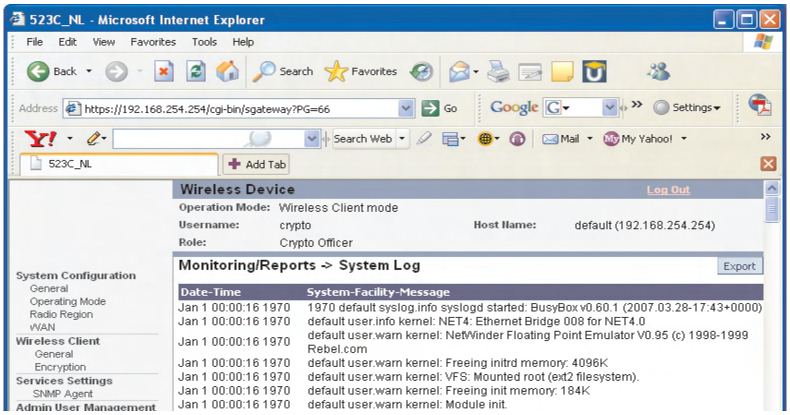
Logs

There are two logs available for viewing and exporting.

System Log

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

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



Wireless Device

Operation Mode: Wireless Client mode
Username: crypto **Host Name:** default (192.168.254.254)
Role: Crypto Officer

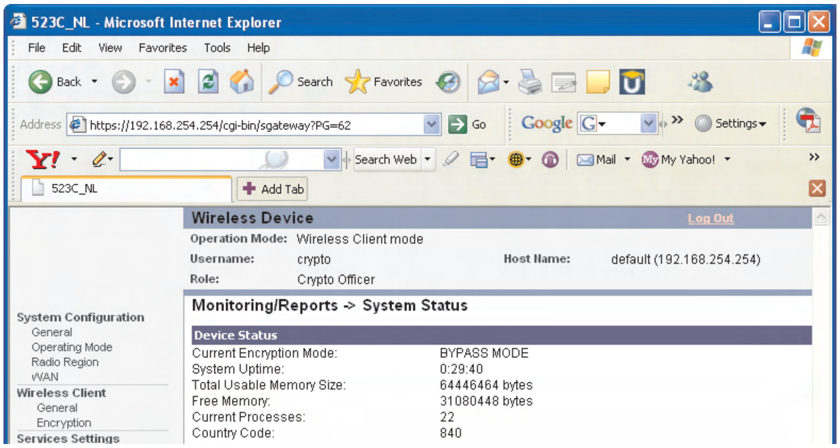
Monitoring/Reports -> System Log

```
Date-Time             System-Facility-Message
Jan 1 00:00:16 1970   1970 default syslog.info syslogd started: BusyBox v0.60.1 (2007.03.28-17:43+0000)
Jan 1 00:00:16 1970   default user.info kernel: NET4: Ethernet Bridge 008 for NET4.0
Jan 1 00:00:16 1970   default user.warn kernel: NetWinder Floating Point Emulator V0.95 (c) 1998-1999
                      Rebel.com
Jan 1 00:00:16 1970   default user.warn kernel: Freeing initrd memory: 4096K
Jan 1 00:00:16 1970   default user.warn kernel: VFS: Mounted root (ext2 filesystem).
Jan 1 00:00:16 1970   default user.warn kernel: Freeing init memory: 184K
Jan 1 00:00:16 1970   default user.warn kernel: Module init.
```

Web Access Log

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

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



Wireless Device

Operation Mode: Wireless Client mode
Username: crypto **Host Name:** default (192.168.254.254)
Role: Crypto Officer

Monitoring/Reports -> System Status

Device Status	
Current Encryption Mode:	BYPASS MODE
System Uptime:	0:29:40
Total Usable Memory Size:	64446464 bytes
Free Memory:	31080448 bytes
Current Processes:	22
Country Code:	840

System Administration

There are five options under **System Administration** :

- System Upgrade
  - Firmware Upgrade
  - Local Configuration Upgrade
- Factory Default
- Remote Logging
- Reboot
- Utilities

Each screen is described in detail in the following subsections.

System Upgrade

The **System Administration — System Upgrade** screen gives you the ability to upload updates to the 523C/E device's firmware as they become available. When a new upgrade file becomes available, you can do a firmware upgrade from the **Firmware Upgrade** window.

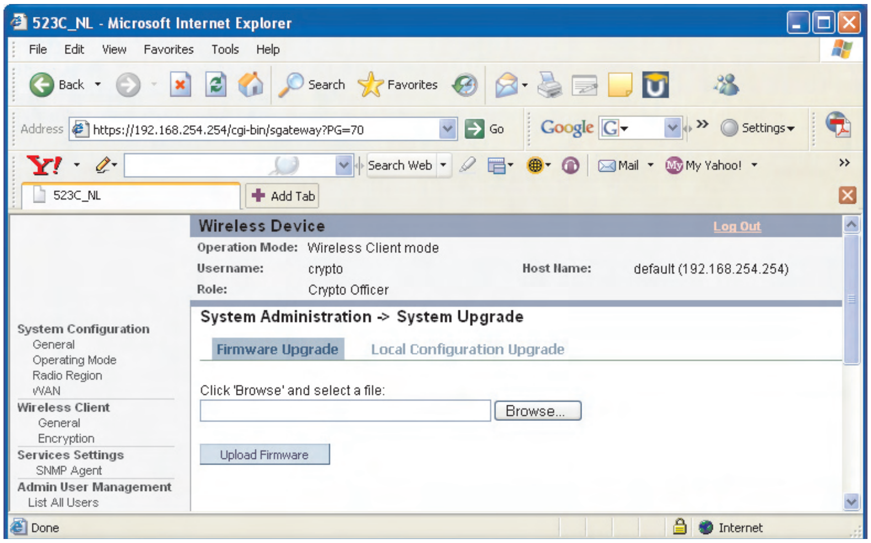
There is also a configuration file transfer option which allows the system configuration file from one AP to be transferred to another AP, in order to minimize the administration of the APs. Only configuration parameters that can be shared between APs are downloaded in the configuration file. WAN IP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

Only the Crypto Officer role can access this function.

Firmware Upgrade

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

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


523C_NL - Microsoft Internet Explorer

Address https://192.168.254.254/cgi-bin/sgateway?PG=70

Wireless Device

Operation Mode: Wireless Client mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

System Administration -> System Upgrade

Firmware Upgrade | Local Configuration Upgrade

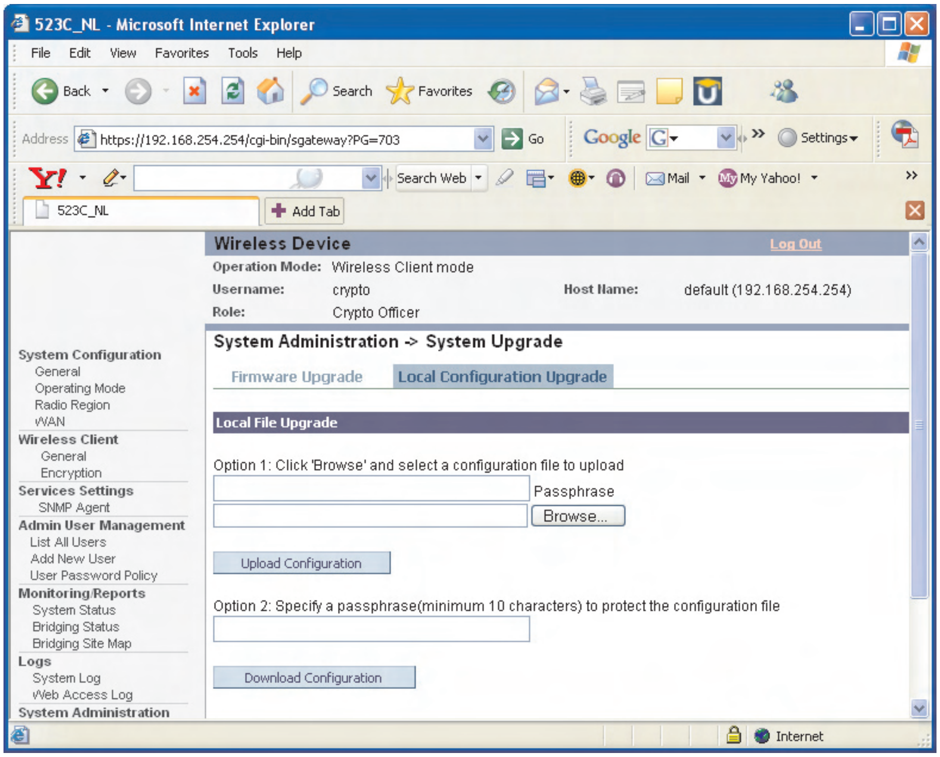
Click 'Browse' and select a file:

Local Configuration Upgrade

On the **System Administration — System Upgrade** screen, click on the **Local Configuration Upgrade** tab to upload and download configuration files to other 523C/E devices connected to the network.

To upload a configuration file, select the file using the browse button and enter the passphrase for that file. The passphrase protects the file from unauthorized users. It prevents unauthorized users from applying the system configuration file to an unauthorized device to gain access to the network. Before downloading the system configuration file to a local computer, the user must enter a passphrase to protect the file. Before the system configuration file can be uploaded onto another 523C/E device, the passphrase must be entered on the remote 523C/E device.

The configuration file can be tagged with a 10 character tag to keep track of the configuration file as it is transferred to other 523C/E devices.



Wireless Device

Operation Mode: Wireless Client mode

Username: crypto

Host Name: default (192.168.254.254)

Role: Crypto Officer

System Administration -> System Upgrade

Local File Upgrade

Option 1: Click 'Browse' and select a configuration file to upload

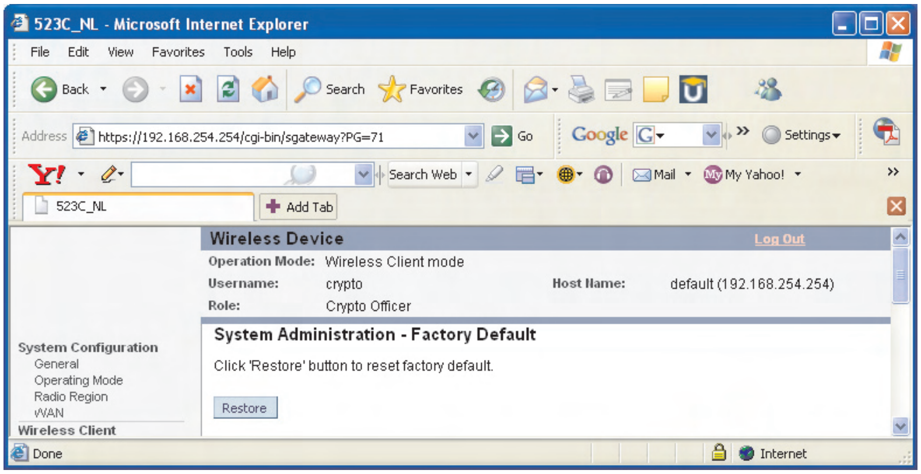
Option 2: Specify a passphrase(minimum 10 characters) to protect the configuration file

Factory Default

The **System Administration — Factory Default** screen is used to reset the 523C/E to its factory settings.

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

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


523C_NL - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.254.254/cgi-bin/sgateway?PG=71 Go
Google Settings
Search Web Mail My Yahoo!
523C_NL
Add Tab
Log Out
System Configuration
General
Operating Mode
Radio Region
WAN
Wireless Client
Restore
Done
Internet

Wireless Device

Operation Mode: Wireless Client mode

Username: crypto Host Name: default (192.168.254.254)

Role: Crypto Officer

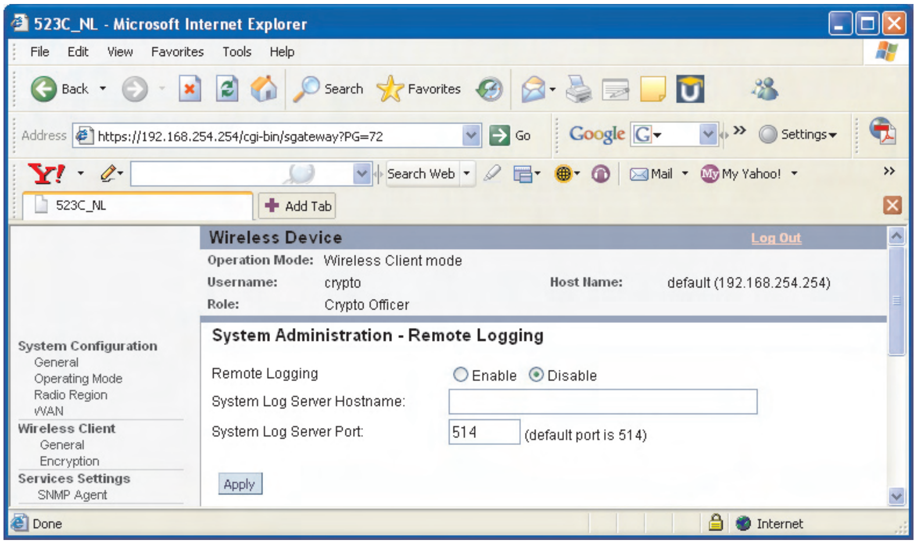
System Administration - Factory Default

Click 'Restore' button to reset factory default.

You can also reset the 523C/E to its factory default by pressing and holding the reset button for 10 seconds. On the 523E the reset button is located on the front of the unit. On the 523C, the reset button is located on the rear of the unit. Input is acknowledged by the WLAN LED turning on and then turning off after 10 seconds.

Remote Logging

The **System Administration —Remote Logging** screen allows you to forward the syslog data from each machine to a central remote logging server. In the 523C/E, this function uses the **syslogd** daemon. If you enable Remote Logging, input a System Log Server IP Address and System Log Server Port. Click **Apply** to accept these values.



Wireless Device

Operation Mode: Wireless Client mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

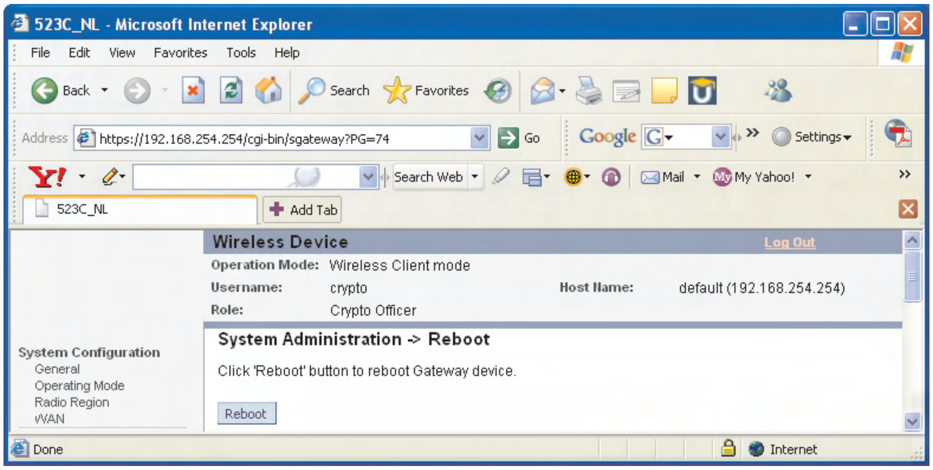
System Administration - Remote Logging

Remote Logging ○ Enable ● Disable
System Log Server Hostname:
System Log Server Port: 514 (default port is 514)

Apply

Reboot

The **System Administration — Reboot** screen allows you to reboot the 523C/E without changing any preset functionality. Both Crypto Officer and Administrator functions have access to this function.



523C_NL - Microsoft Internet Explorer

Address https://192.168.254.254/cgi-bin/sgateway?PG=74

Wireless Device

Operation Mode: Wireless Client mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

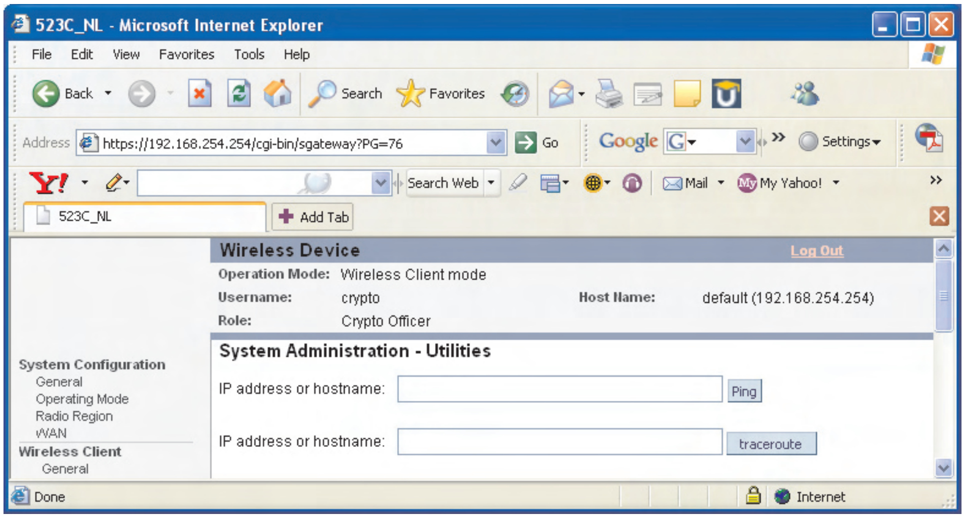
System Administration -> Reboot

Click 'Reboot' button to reboot Gateway device.

You can also reboot the 523C/E by pressing and holding the reset button for five seconds. Input is acknowledged by the WLAN LED turning on. On the 523C unit, the reset button is located on the front of the unit. On the 523E unit, the reset button is located on the rear of the unit.

Utilities

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



523C_NL - Microsoft Internet Explorer

Address https://192.168.254.254/cgi-bin/sgateway?PG=76

Wireless Device

Operation Mode: Wireless Client mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

System Administration - Utilities

IP address or hostname:

IP address or hostname:

AP Mode — Configuration

The following subsections describe the screens used when configuring the 523C/E as an access point.

The following screens are available in AP mode:

- Wireless Access Point
  - General
  - Security
  - Wireless VLAN (optional)
  - MAC Address Filtering
  - Rogue AP Detection
  - Advanced
- Service Settings
  - DHCP Server
- Montoring/Reports
  - Wireless Clients
  - Adjacent AP List
  - DHCP Client List

All other screens are the same as those described in the Client Mode section.

Wireless Access Point

There are six options under **Wireless Access Point** :

- General
- Security
- Wireless VLAN (option)
- MAC Address Filtering
- Rogue AP Detection
- Advanced

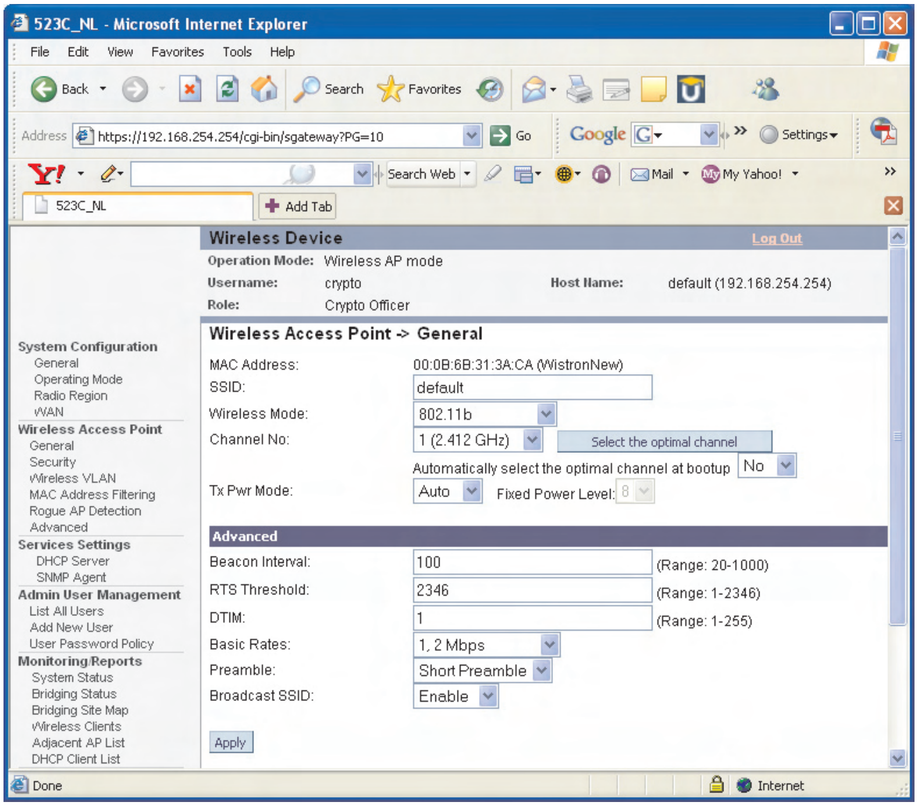
Each screen is described in detail in the following subsections.

General

Wireless Setup allows your computer's PC Card to communicate with the access point. Once you have completed wireless access point configuration, you can complete the rest of the configuration wirelessly unless you will be employing the FIPS 140-2 secure mode, assuming that you have installed and configured a wireless PC card on your computer. (If you have not done so, you will have to do that to establish communications. Follow the manufacturer's instructions to set up the PC Card on each wireless device that will be part of the WLAN.)

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

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



https://192.168.254.254/cgi-bin/sgateway?PG=10

523C_NL

Wireless Device

Operation Mode: Wireless AP mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

Wireless Access Point -> General

MAC Address: 00:0B:6B:31:3A:CA (WistronNew)
SSID: default
Wireless Mode: 802.11b
Channel No: 1 (2.412 GHz)
Automatically select the optimal channel at bootup: No
Tx Pwr Mode: Auto Fixed Power Level: 8

Advanced

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

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

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

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

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

If you click on the button **Select the optimal channel**, a popup screen will display the choices. It will select the optimal channel for you. You can also set it up to automatically select the optimal channel at boot up.

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

Tx Pwr Mode and Fixed Pwr Level: The Tx Power Mode defaults to Auto, giving the largest range of radio transmission available under normal conditions. As an option, the AP's broadcast range can be limited by setting the Tx Power Mode to Fixed and choosing from 1-5 for Fixed Pwr Level (1 being the shortest distance.) Finally, if you want to prevent any radio frequency transmission, set Tx Pwr Mode to **Off**.

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

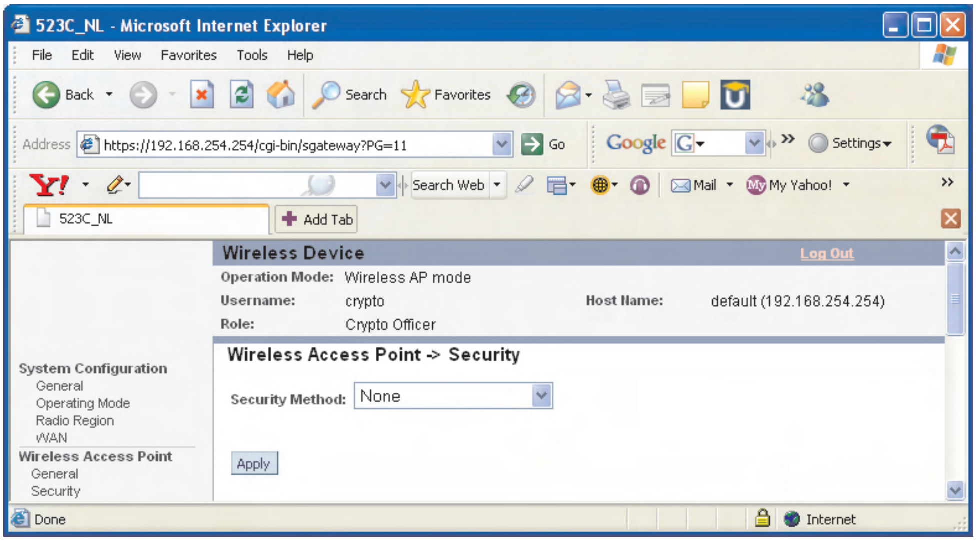
ADVANCED OPTIONS		
Beacon interval	20-1000	The time interval in milliseconds in which the 802.11 beacon is transmitted by the AP.
RTS Threshold	1-2346	The number of bytes used for the RTS/CTS handshake boundary. When a packet size is greater than the RTS threshold, the RTS/CTS handshaking is performed.
DTIM	1-255	The number of beacon intervals that broadcast and multicast traffic is buffered for a client in power save mode.
Basic Rates	**Basic Rates for 802.11b**	
	1 and 2 Mbps 1, 2, 5.5 and 11 Mbps	The basic rates used and reported by the AP. The highest rate specified is the rate that the AP uses when transmitting broadcast/multicast and management frames.
	Basis Rates for 802.11g	
	1, 2, 5.5, 11, 6, 12, 24 Mbps 1, 2, 5.5, 11 Mbps	The basic rates used and reported by the AP. The highest rate specified is the rate that the AP uses when transmitting broadcast/multicast and management frames.
	Basic Rates for 802.11g Super	
	1, 2, 5.5, 11, 6, 12, 24 Mbps 1, 2, 5.5, 11 Mbps	The basic rates used and reported by the AP. The highest rate specified is the rate that the AP uses when transmitting broadcast/multicast and management frames.
	Basic Rates for 802.11b/g Mixed	
	1, 2 Mbps 1, 2, 5.5, 11 Mbps	The basic rates used and reported by the AP. The highest rate specified is the rate that the AP uses when transmitting broadcast/multicast and management frames.
	Basic Rates for 802.11a	
	6, 12, 24 Mbps	The basic rates used and reported by the AP. The highest rate specified is the rate that the AP uses when transmitting broadcast/multicast and management frames.
	Basic Rates for 802.11a Turbo	
	6, 12, 24 Mbps	The basic rates used and reported by the AP. The highest rate specified is the rate that the AP uses when transmitting broadcast/multicast and management frames.
Preamble	Short/Long Preamble	Specifies whether frames are transmitted with the Short or Long Preamble
Broadcast SSID	Enabled/disabled	When disabled, the AP hides the SSID in outgoing beacon frames and stations cannot obtain the SSID through passive scanning. Also, when it is disabled, the AP doesn't send probe responses to probe requests with unspecified SSIDs.

Security

The **Wireless Access Point — Security** screen displays a default factory setting of no encryption, but for security reasons it will not communicate to any clients unless the encryption is set by the CryptoOfficer.

No Encryption

In order to have the 523C/E work with no encryption, you must actively select **None** and click **Apply**. A screen will appear, asking if you really want to operate in Bypass mode. If you answer **Yes**, no encryption will be applied.



Address: https://192.168.254.254/cgi-bin/sgateway?PG=11

Wireless Device

Operation Mode: Wireless AP mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

Wireless Access Point -> Security

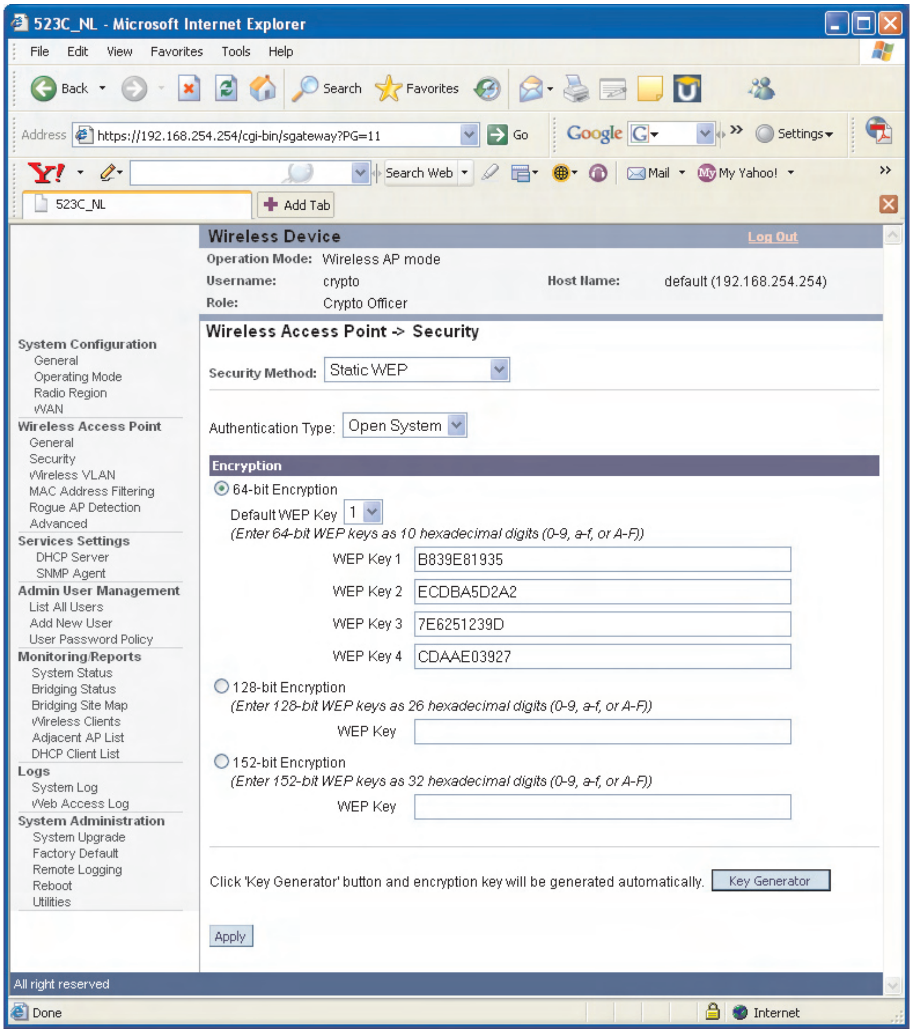
Security Method: None

Static WEP Encryption

If you choose to use WEP encryption, you can also select whether it will be Open System or Shared Key authentication. For greater security, set authentication type to “shared key.” WEP Data encryption can be set to 64-bit, 128-bit, or 152-bit encryption.

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

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



Wireless Device

Operation Mode: Wireless AP mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

Wireless Access Point -> Security

Security Method: Static WEP

Authentication Type: Open System

Encryption

● 64-bit Encryption
Default WEP Key 1
(Enter 64-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F))
WEP Key 1 B839E81935
WEP Key 2 ECDBA5D2A2
WEP Key 3 7E6251239D
WEP Key 4 CDAAE03927

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

○ 152-bit Encryption
(Enter 152-bit WEP keys as 32 hexadecimal digits (0-9, a-f, or A-F))
WEP Key

Click 'Key Generator' button and encryption key will be generated automatically.

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

802.11i and WPA

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

If you wish to use WPA on the 523C/E, enable either WPA Pre-shared Key Settings or WPA 802.1x Settings.

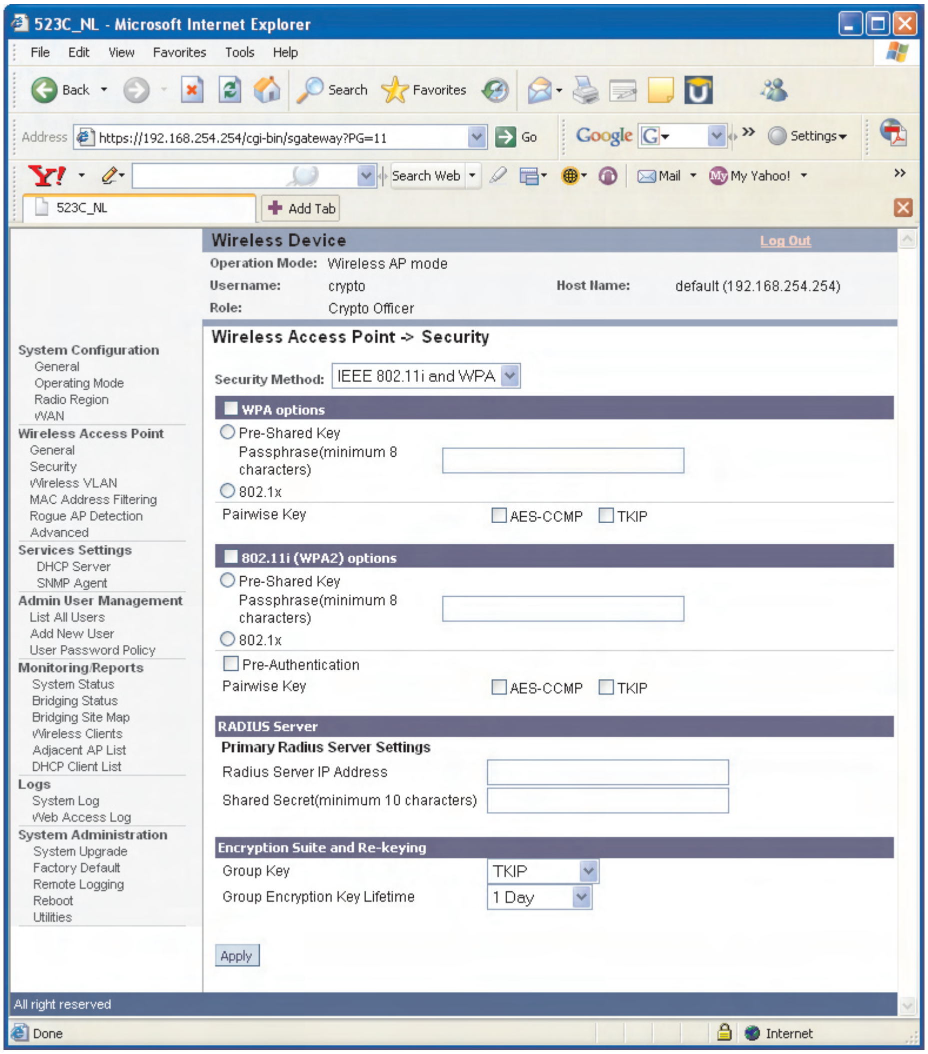
If you are a SOHO user, selecting pre-shared key means that you don't have the expense of installing a Radius Server. Simply input up to 63 character / numeric / hexadecimals in the Passphrase field. If your clients use WPA-TKIP, select TKIP as encryption type. If your clients use WPA-AES, select AES-CCMP.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

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

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

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

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



Wireless Device

Operation Mode: Wireless AP mode

Username: crypto

Host Name: default (192.168.254.254)

Role: Crypto Officer

Wireless Access Point -> Security

Security Method: IEEE 802.11i and WPA

□ WPA options

○ Pre-Shared Key

Passphrase(minimum 8 characters) [ ]

○ 802.1x

Pairwise Key □ AES-CCMP □ TKIP

□ 802.11i (WPA2) options

○ Pre-Shared Key

Passphrase(minimum 8 characters) [ ]

○ 802.1x

□ Pre-Authentication

Pairwise Key □ AES-CCMP □ TKIP

RADIUS Server

Primary Radius Server Settings

Radius Server IP Address [ ]

Shared Secret(minimum 10 characters) [ ]

Encryption Suite and Re-keying

Group Key: TKIP

Group Encryption Key Lifetime: 1 Day

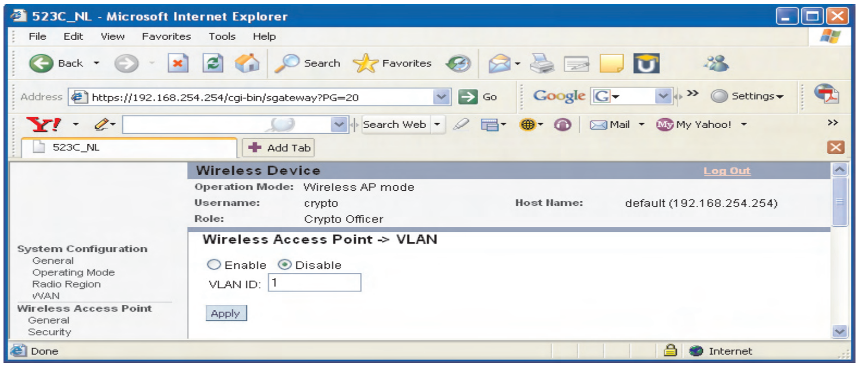
Apply

Wireless VLAN

Wireless VLAN is an optional feature available for an additional cost. It is not part of the basic software package.

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

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



523C_NL - Microsoft Internet Explorer

Address: https://192.168.254.254/cgi-bin/sgateway?PG=20

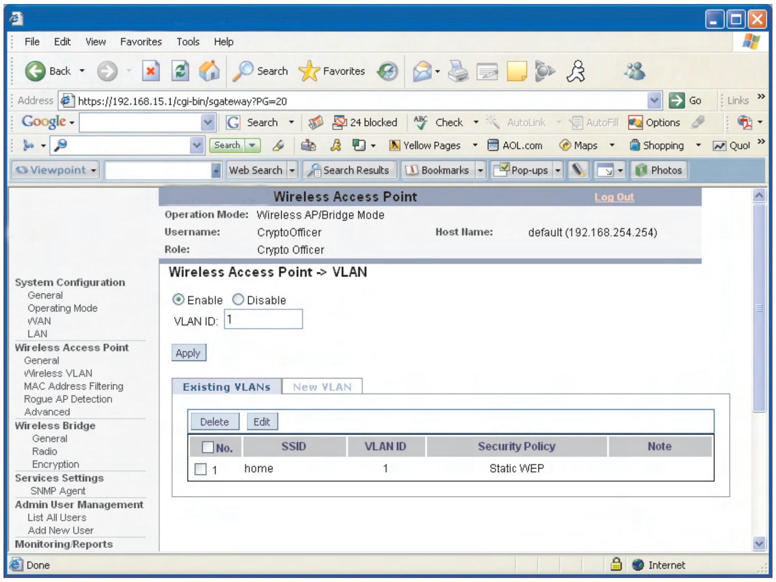
Wireless Device

Operation Mode: Wireless AP mode
Username: crypto
Role: Crypto Officer
Host Name: default (192.168.254.254)

Wireless Access Point -> VLAN

○ Enable ● Disable
VLAN ID: 1

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



Address: https://192.168.15.1/cgi-bin/sgateway?PG=20

Wireless Access Point

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

Wireless Access Point -> VLAN

● Enable ○ Disable
VLAN ID: 1

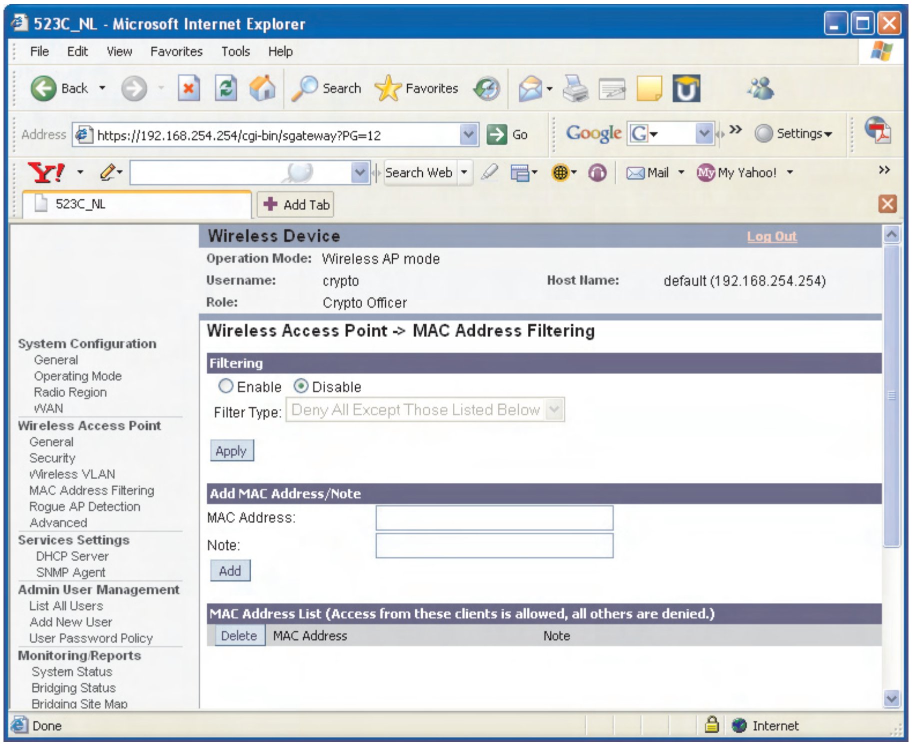
Existing VLANs | New VLAN

No.	SSID	VLAN ID	Security Policy	Note
□ 1	home	1	Static WEP	

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

MAC Address Filtering

The **Wireless Access Point — MAC Address Filtering** screen is used to set up MAC address filtering for the 523C/E device. The factory default for MAC Address filtering is **Disabled**. If you enable MAC Address filtering, you should also set the toggle for **Filter Type**.



Operation Mode: Wireless AP mode
Username: crypto Host Name: default (192.168.254.254)
Role: Crypto Officer

Wireless Access Point -> MAC Address Filtering

Filtering
○ Enable ● Disable
Filter Type: Deny All Except Those Listed Below

Add MAC Address/Note
MAC Address:
Note:

MAC Address List (Access from these clients is allowed, all others are denied.)

Delete	MAC Address	Note

This works as follows:

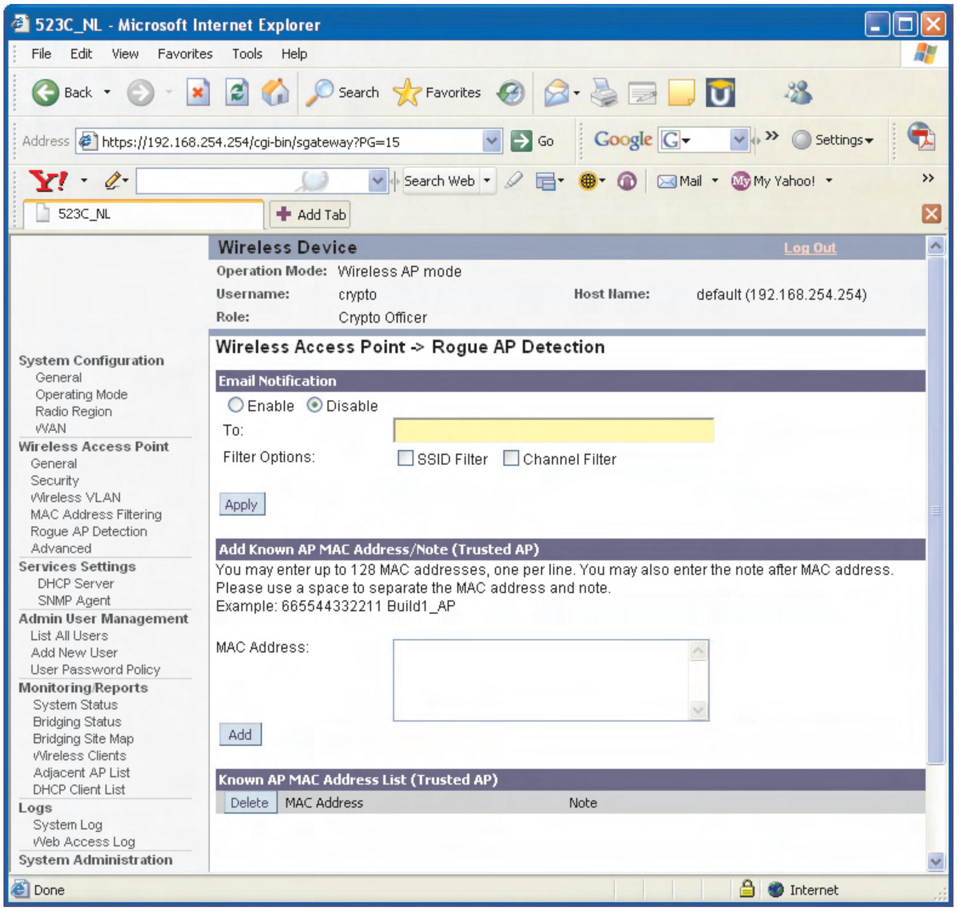
- If **Filtering** is enabled and **Filter Type** is **Deny All Except Those Listed Below**, only those devices equipped with the authorized MAC addresses will be able to communicate with the access point. In this case, input the MAC addresses of all the PC cards that will be authorized to access this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

Rogue AP Detection

The **Wireless Access Point — Rogue AP Detection** screen allows the network administrator to set up rogue AP detection. Enable rogue AP detection and enter the MAC Address of each AP in the network that you want the AP being configured to accept as a trusted AP. (You may add up to 20 APs.) Enter an email address for notification of any rogue or non-trusted APs. (The MAC Address for the 523C/E is located on the **System Configuration — General** screen. You can also select the following filter options.

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

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



Wireless Device

Operation Mode: Wireless AP mode

Username: crypto

Host Name: default (192.168.254.254)

Role: Crypto Officer

Wireless Access Point -> Rogue AP Detection

Email Notification

○ Enable ● Disable

To:

Filter Options: □ SSID Filter □ Channel Filter

Apply

Add Known AP MAC Address/Note (Trusted AP)

You may enter up to 128 MAC addresses, one per line. You may also enter the note after MAC address.
Please use a space to separate the MAC address and note.
Example: 665544332211 Build1_AP

MAC Address:

Add

Known AP MAC Address List (Trusted AP)

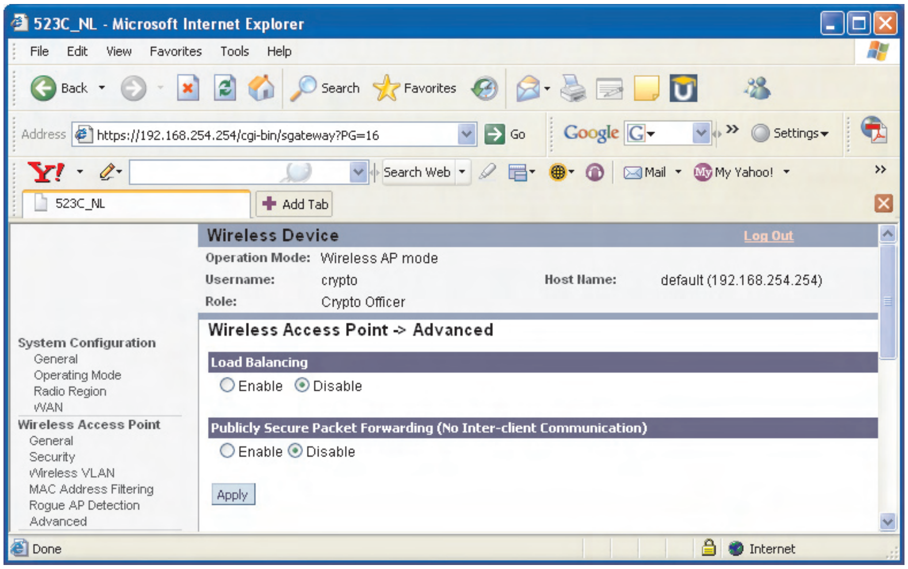
Delete	MAC Address	Note

Advanced

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

Load balancing is enabled by default. The load balancing feature balances the wireless clients between APs. If two APs with similar settings are in a conference room, depending on the location of the APs, all wireless clients could potentially associate with the same AP, leaving the other AP unused. Load balancing attempts to evenly distribute the wireless clients on both APs.

Publicly Secure Packet Forwarding is disabled by default. Layer 2 isolation prevents wireless clients that associate with the same AP from communicating with each other.



Wireless Device

Operation Mode: Wireless AP mode

Username: crypto

Host Name: default (192.168.254.254)

Role: Crypto Officer

Wireless Access Point -> Advanced

Load Balancing

○ Enable ● Disable

Publicly Secure Packet Forwarding (No Inter-client Communication)

○ Enable ● Disable

Apply

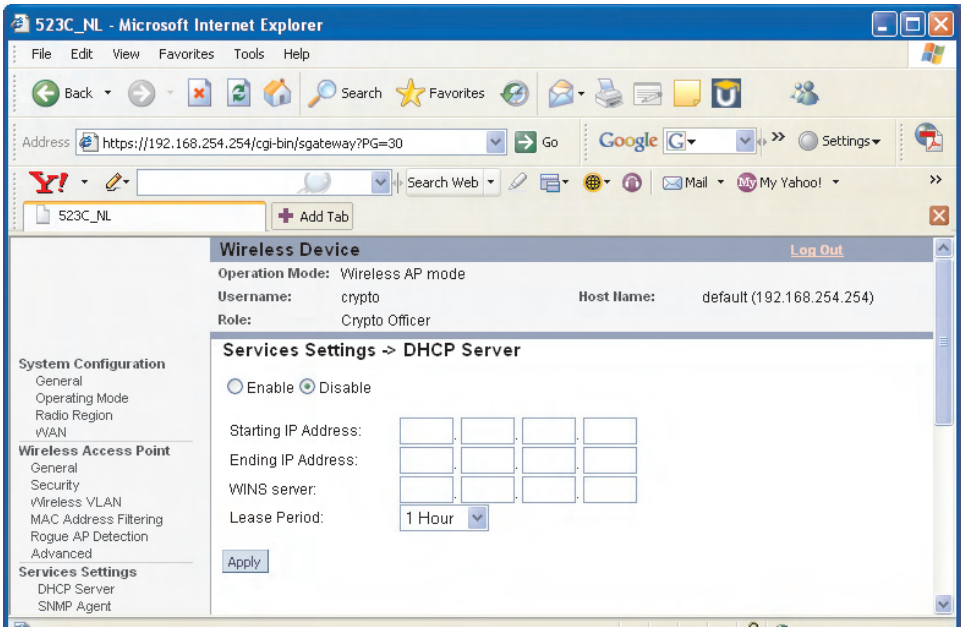
Once you have made any changes, click **Apply** to save.

Services Settings

DHCP Server

The **Service Settings — DHCP Server** screen is used for configuring the DHCP server function accessible from the Local LAN port. The default factory setting for the DHCP server function is enabled. You can disable the DHCP server function, if you wish, but it is not recommended. You can also set the range of addresses to be assigned. The Lease period (after which the dynamic address can be reassigned) can also be varied.

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



https://192.168.254.254/cgi-bin/sgateway?PG=30

Wireless Device

Operation Mode: Wireless AP mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

Services Settings -> DHCP Server

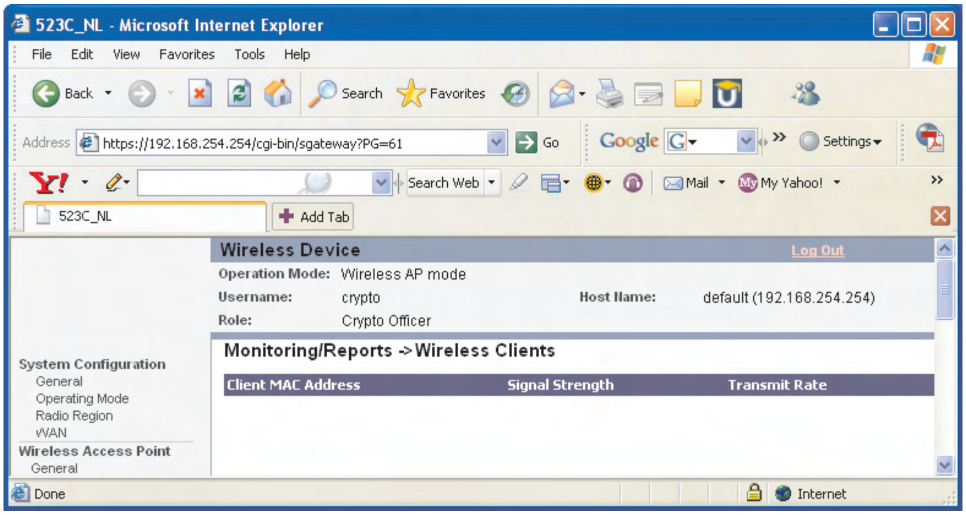
○ Enable ● Disable

Starting IP Address: ___ . ___ . ___ . ___
Ending IP Address: ___ . ___ . ___ . ___
WINS server: ___ . ___ . ___ . ___
Lease Period: 1 Hour

Monitoring/Reports

Wireless Clients

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



Address: https://192.168.254.254/cgi-bin/sgateway?PG=61

Wireless Device

Operation Mode: Wireless AP mode

Username: crypto Host Name: default (192.168.254.254)

Role: Crypto Officer

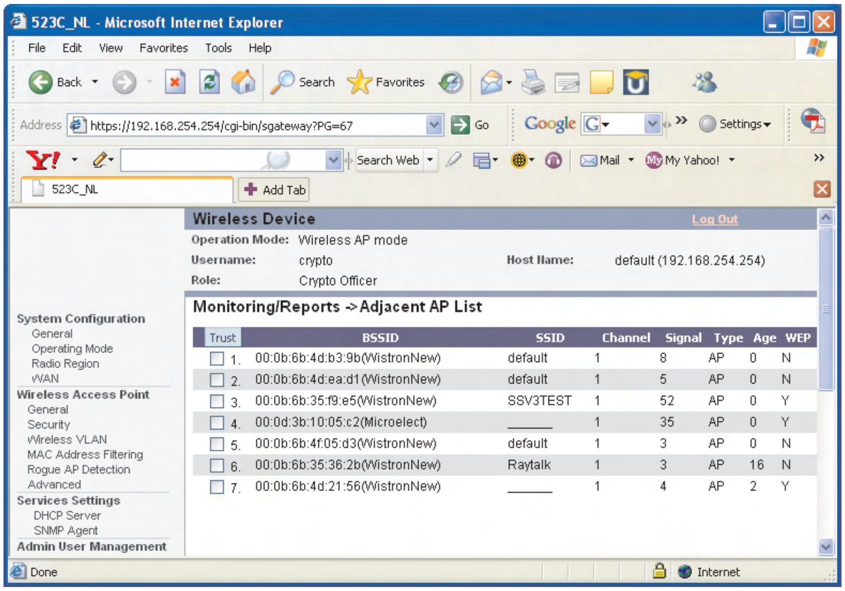
Monitoring/Reports ->Wireless Clients

Client MAC Address	Signal Strength	Transmit Rate

Adjacent AP List

The **Monitoring/Report — Adjacent AP List** screen shows all the APs on the network. If you select the check box next to any AP shown, the AP will thereafter be accepted by the 523C/E as a trusted AP.

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



Address: https://192.168.254.254/cgi-bin/sgateway?PG=67

Wireless Device

Operation Mode: Wireless AP mode

Username: crypto Host Name: default (192.168.254.254)

Role: Crypto Officer

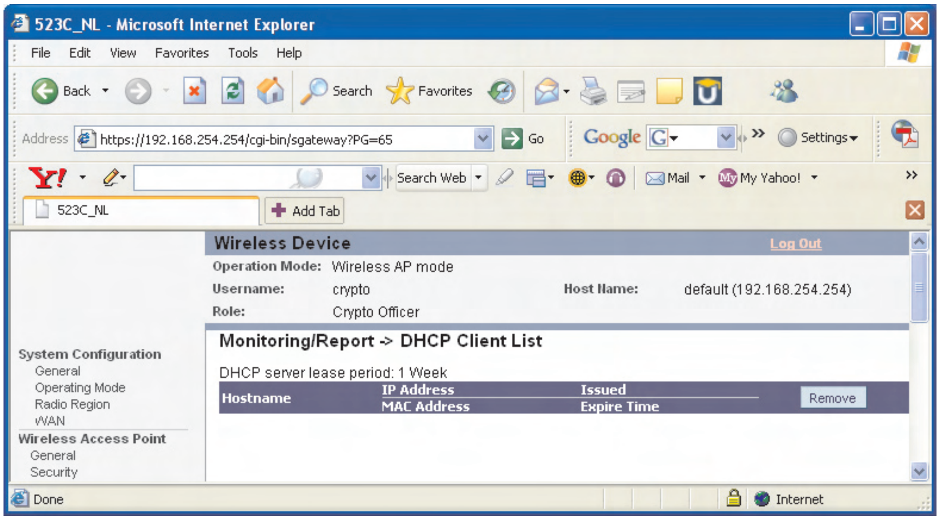
Monitoring/Reports ->Adjacent AP List

Trust	BSSID	SSID	Channel	Signal	Type	Age	WEP
□ 1.	00:0b:6b:4d:b3:9b(WistronNew)	default	1	8	AP	0	N
□ 2.	00:0b:6b:4d:ea:d1(WistronNew)	default	1	5	AP	0	N
□ 3.	00:0b:6b:35:f9:e5(WistronNew)	SSV3TEST	1	52	AP	0	Y
□ 4.	00:0d:3b:10:05:c2(Microelect)	______	1	35	AP	0	Y
□ 5.	00:0b:6b:4f:05:d3(WistronNew)	default	1	3	AP	0	N
□ 6.	00:0b:6b:35:36:2b(WistronNew)	Raytalk	1	3	AP	16	N
□ 7.	00:0b:6b:4d:21:56(WistronNew)	______	1	4	AP	2	Y

DHCP Client List

The **Monitoring/Report — DHCP Client List** screen displays all clients currently connected to the 523C/E via DHCP server, including their hostnames, IP addresses, and MAC Addresses.

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



Address: https://192.168.254.254/cgi-bin/sgateway?PG=65

Wireless Device

Operation Mode: Wireless AP mode

Username: crypto

Host Name: default (192.168.254.254)

Role: Crypto Officer

Monitoring/Report -> DHCP Client List

DHCP server lease period: 1 Week

Hostname	IP Address MAC Address	Issued Expire Time	Remove

Bridge Mode — Configuration

The following subsections describe the screens used when configuring the 523C/E as a Bridge.

The following screens are available in Bridge mode:

- Wireless Bridge
  - General
  - Radio
  - Encryption
  - MAC Address Filtering

All other screens are the same as those described in the Client Mode section.

In the 523C/E, wireless bridging is used to set up an independent wireless bridge connection. Since wireless bridging provides a mechanism for APs to collaborate, it is possible to extend the basic service set (BSS) of a standalone AP and to connect two separate LANs without installing any cabling.

Wireless Bridge

There are three options under **Wireless Bridge** :

- General
- Radio
- Encryption
- MAC Address Filtering (auto bridge mode only)

Each screen is described in detail in the following subsections.

Wireless Bridge — General

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

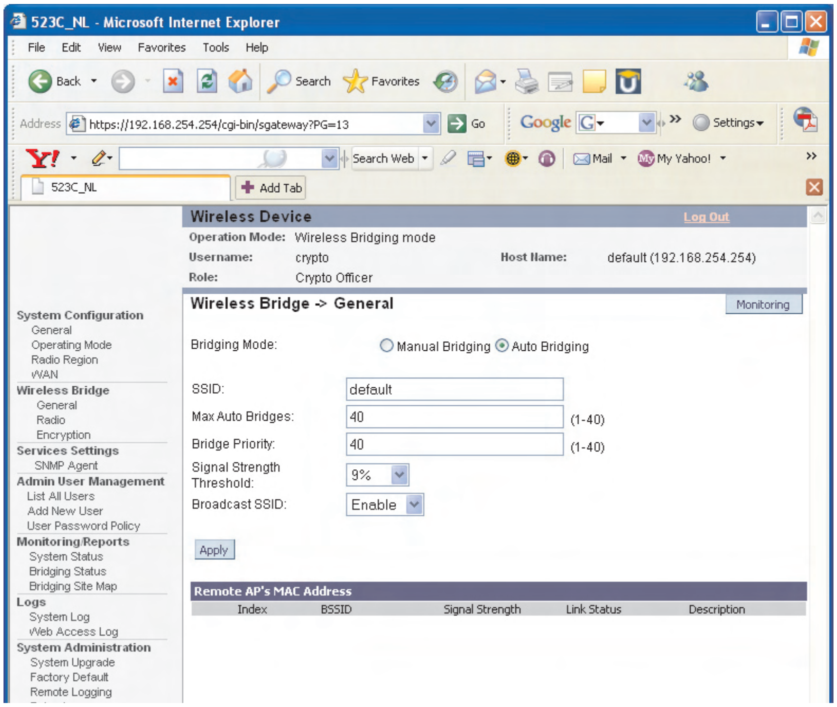
- Manual wireless bridging
- Auto-forming wireless bridging (AWB) - with a maximum number of allowable bridges (the default is 40)

Auto-forming Wireless Bridging

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

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

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



Wireless Device

Operation Mode: Wireless Bridging mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

Wireless Bridge -> General

Bridging Mode: ○ Manual Bridging ● Auto Bridging

SSID: default
Max Auto Bridges: 40 (1-40)
Bridge Priority: 40 (1-40)
Signal Strength Threshold: 9%
Broadcast SSID: Enable

Apply

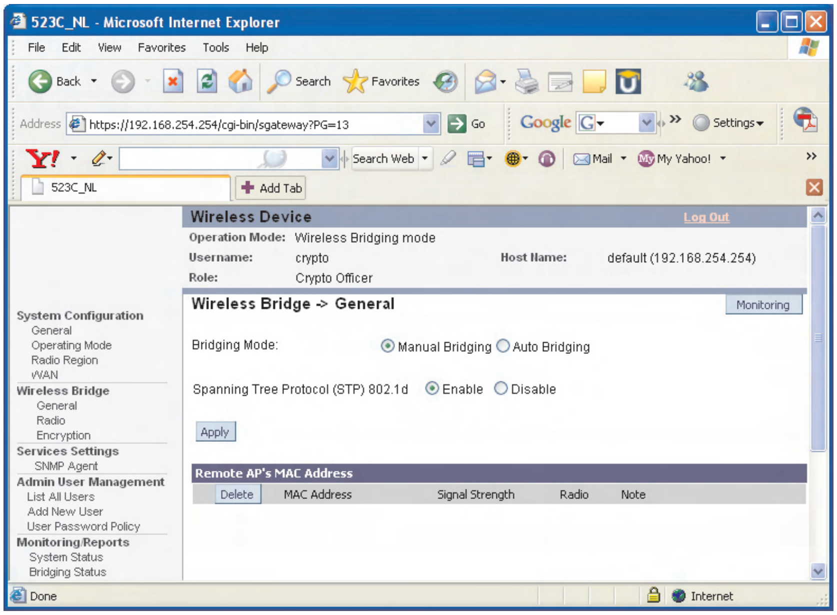
Remote AP's MAC Address

Index	BSSID	Signal Strength	Link Status	Description

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

Manual Bridging

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



Wireless Device

Operation Mode: Wireless Bridging mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

Wireless Bridge -> General

Bridging Mode: ● Manual Bridging ○ Auto Bridging

Spanning Tree Protocol (STP) 802.1d ● Enable ○ Disable

Apply

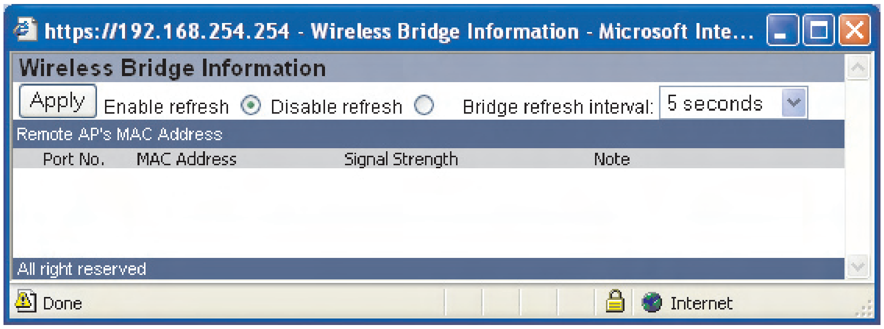
Remote AP's MAC Address

Delete	MAC Address	Signal Strength	Radio	Note

MANUAL BRIDGING GENERAL SETTINGS OPTIONS		
Bridging Mode	Manual Bridging	manual bridging selected
Signal Strength LED MAC	Not Assigned	Allows you to set the number of one of the Remote APs which will be listed at the bottom of the screen once the system is operational This wireless bridge becomes the guiding port that is displayed in the WLAN LED on the front of the unit as a signal.
Spanning Tree Protocol (STP)	Enable/Disable	Enable STP is there is any possiblity that a bridging loop could occur. If you are certain that there is no possibility that a bridging loop will occur, then disalbe STP. The bridge will be more efficient (faster) without it. If you are not sure, the safest solution is to enable STP.

Monitoring

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



https://192.168.254.254 - Wireless Bridge Information - Microsoft Inte...

Wireless Bridge Information

Apply Enable refresh ● Disable refresh ○ Bridge refresh interval: 5 seconds

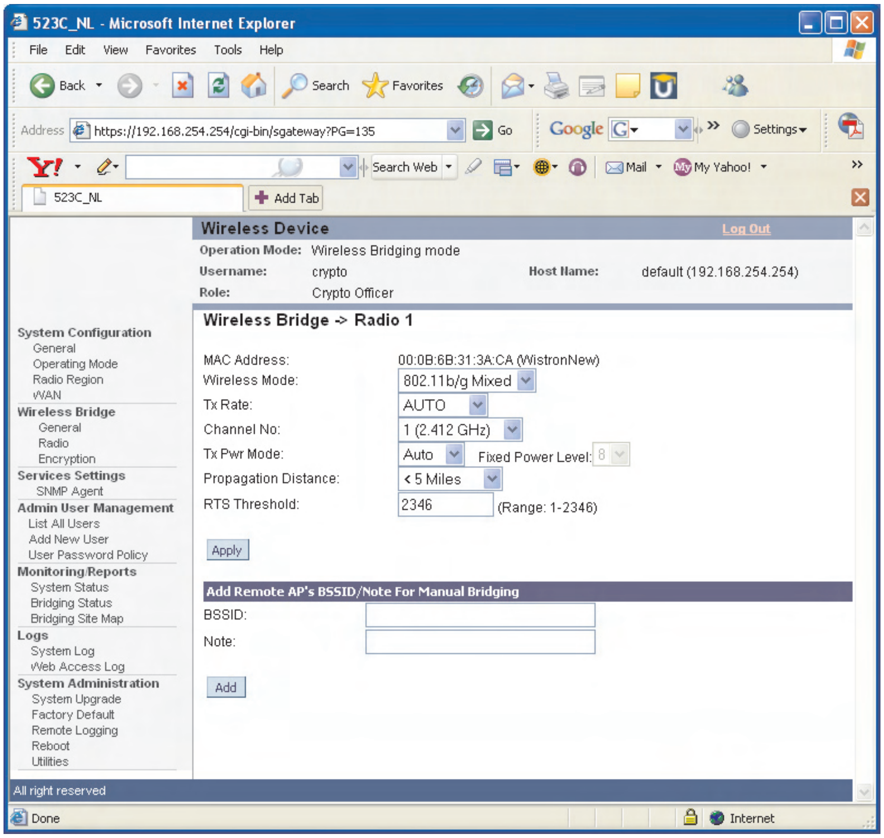
Remote AP's MAC Address

Port No.	MAC Address	Signal Strength	Note

All right reserved

Radio

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



Wireless Device

Operation Mode: Wireless Bridging mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

Wireless Bridge -> Radio 1

MAC Address: 00:0B:6B:31:3A:CA (WistronNew)
Wireless Mode: 802.11b/g Mixed
Tx Rate: AUTO
Channel No: 1 (2.412 GHz)
Tx Pwr Mode: Auto Fixed Power Level: 8
Propagation Distance: < 5 Miles
RTS Threshold: 2346 (Range: 1-2346)

Add Remote AP's BSSID/Note For Manual Bridging

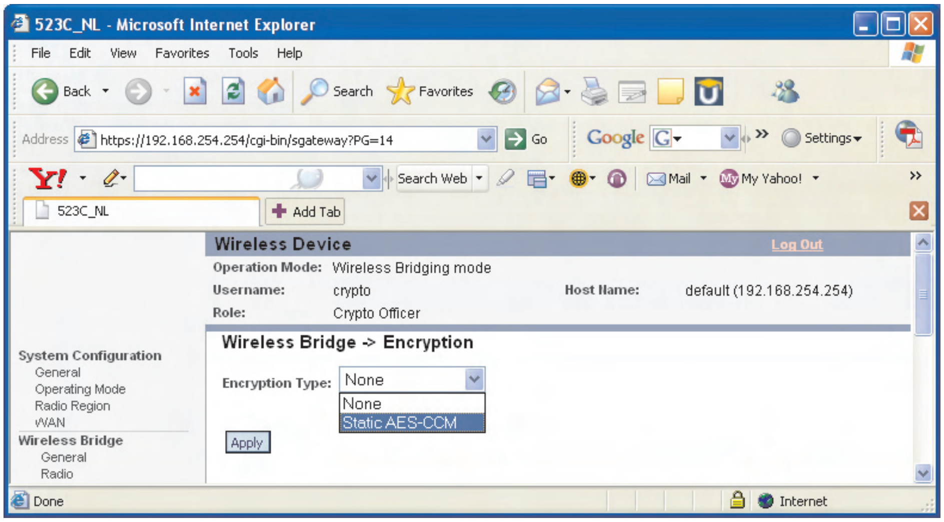
BSSID:
Note:

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

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

Encryption

The **Wireless Bridge — Encryption** screen is used to configure static encryption keys for the wireless bridge. This is an important page to set up to ensure that your bridge is working correctly. The encryption key that you use on this screen must be the same for any bridge connected to your bridging network in order for communication to occur. On this screen you can select None or Static AES-CCM (128-bit).



Wireless Device

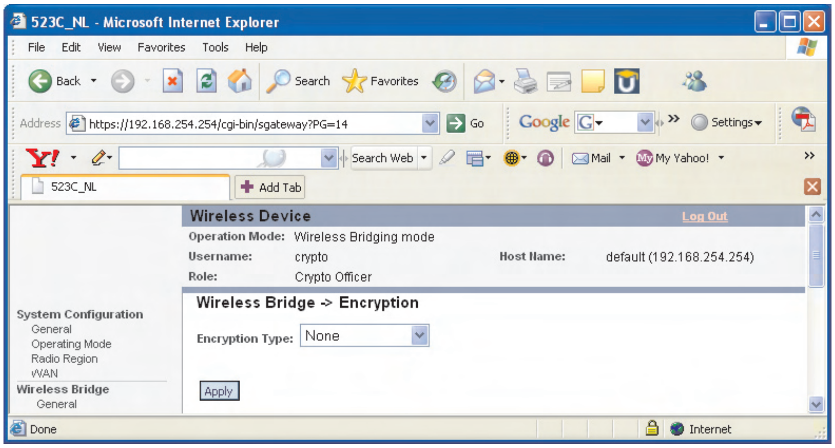
Operation Mode: Wireless Bridging mode
Username: crypto Host Name: default (192.168.254.254)
Role: Crypto Officer

Wireless Bridge -> Encryption

Encryption Type: None

No Encryption

In order to have the 523C/E work with no encryption, you must actively select **None** and click **Apply**. A screen will appear, asking if you really want to operate in Bypass mode. If you answer **Yes**, no encryption will be applied.


523C_NL - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.254.254/cgi-bin/sgateway?PG=14 Go
Google Settings
Search Web Mail My Yahoo!
523C_NL Add Tab
Log Out
System Configuration
General
Operating Mode
Radio Region
WAN
Wireless Bridge
General
Apply
Done
Internet

Wireless Device

Operation Mode: Wireless Bridging mode
Username: crypto Host Name: default (192.168.254.254)
Role: Crypto Officer

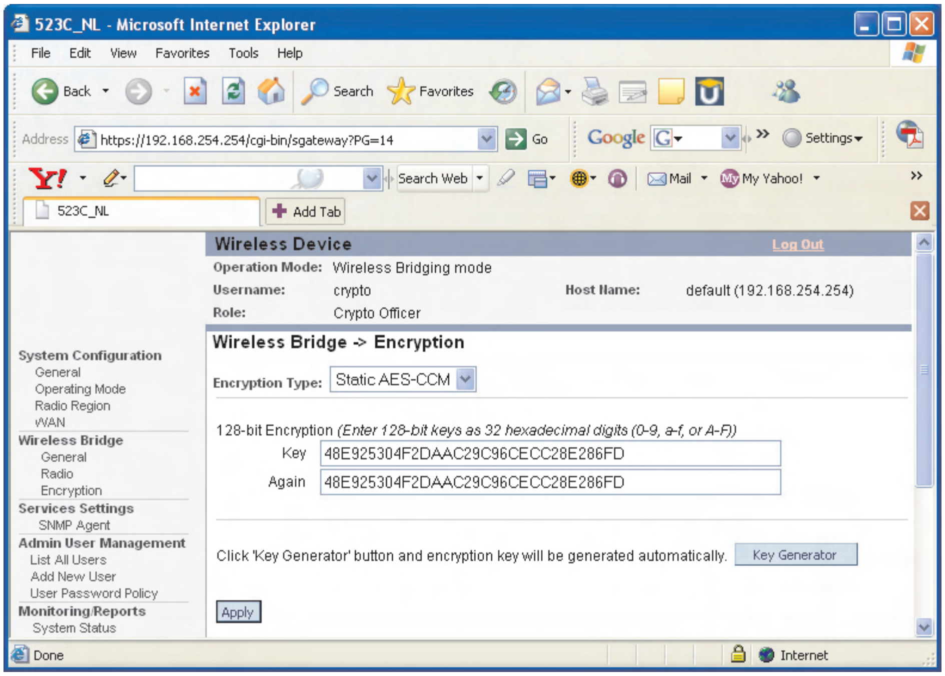
Wireless Bridge -> Encryption

Encryption Type: None

Static AES-CCM Key

The Advanced Encryption Standard (AES) was selected by National Institute of Standards and Technology (NIST) in October 2000 as an upgrade from the previous DES standard. AES uses a 128-bit block cipher algorithm and encryption technique for protecting computerized information.

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



523C_NL - Microsoft Internet Explorer

Address https://192.168.254.254/cgi-bin/sgateway?PG=14

Wireless Device

Operation Mode: Wireless Bridging mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

Wireless Bridge -> Encryption

Encryption Type: Static AES-CCM

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

Key 48E925304F2DAAC29C96CECC28E286FD

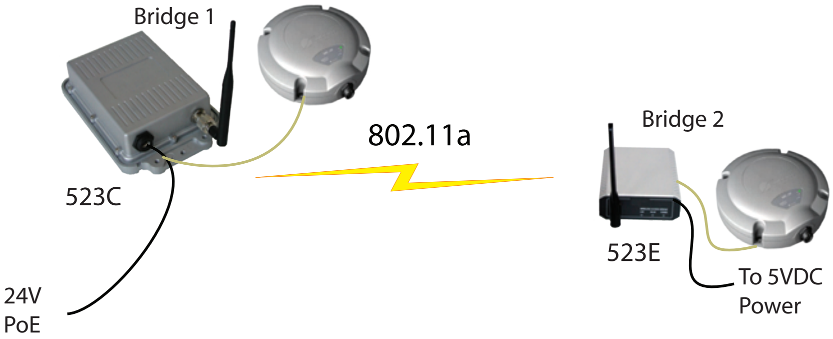
Again 48E925304F2DAAC29C96CECC28E286FD

Click 'Key Generator' button and encryption key will be generated automatically.

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 compatible commands in the setup screens.

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

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

Point-to-Point Bridging Setup Guide - Manual Mode

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

Point-to-Point Bridging Setup Guide - Auto Mode

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

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

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

In the first section you will see the MAC Address of the bridging card. This is used as the BSSID on other 523C/Es that will be communicating-with this one.

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

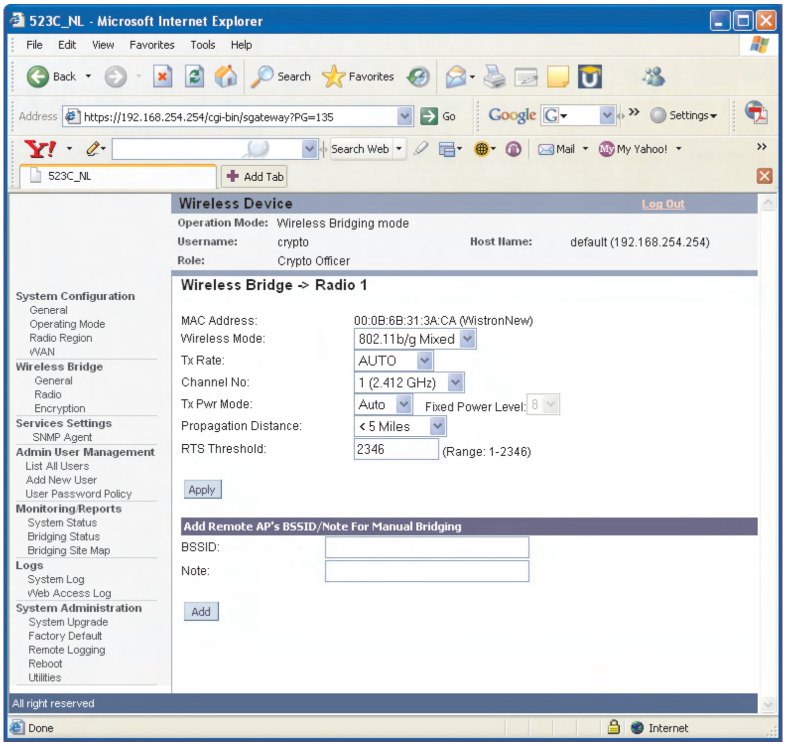
Next select the **Channel Number.** The **Channel Number** must be set to the same frequency in order for each bridge to communicate. **TX Pwr Mode** can be left on **Auto** unless the power needs to be regulated.

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

Set the **RTS Threshold** which is the number of bytes used for the RTS/CTS handshake boundary. When a packet size is greater than the RTS threshold, the RTS/CTS handshaking is performed.

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

Add the **BSSID** of the remote bridge. The BSSID corresponds to that bridge's MAC address. In entering the BSSID, enter only hexadecimal numbers, no colons. Data entry is not case sensitive. You may also enter a note that defines the location of the remote bridge. Then click **Add** to accept. The remote bridge's BSSID will now appear at the bottom of the **Wireless Bridge — General** screen.



Address: https://192.168.254.254/cgi-bin/sgateway?PG=135

Wireless Device

Operation Mode: Wireless Bridging mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

Wireless Bridge -> Radio 1

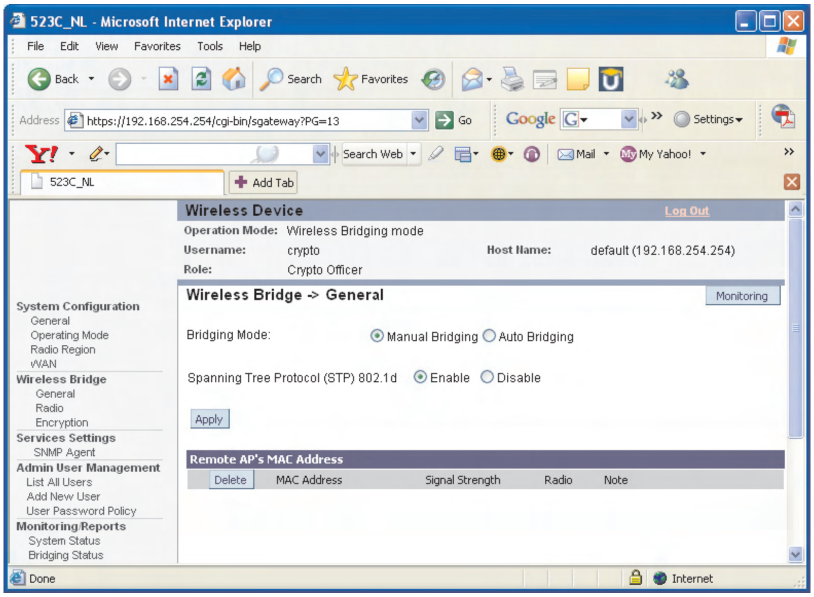
MAC Address: 00:0B:6B:31:3A:CA (WistronNew)
Wireless Mode: 802.11b/g Mixed
Tx Rate: AUTO
Channel No: 1 (2.412 GHz)
Tx Pwr Mode: Auto Fixed Power Level: 8
Propagation Distance: < 5 Miles
RTS Threshold: 2346 (Range: 1-2346)

Add Remote AP's BSSID/Note For Manual Bridging

BSSID:
Note:

Next go to the **Wireless Bridge — General** screen. Select either manual or auto bridging. If you choose **Manual Bridging** then you will have to set **Spanning Tree Protocol** to **Enable** unless you are sure that there is no chance of a loop. You can also assign a **Signal Strength LED MAC**. **Signal strength LED MAC** allows you to set the number of one of the Remote APs which will be listed at the bottom of the screen once the system is operational as the guiding port that you wish to have display in the WLANSS LED on the front of the 523C/E as a signal. If you don't wish to display any connection signal, simply leave this set at Not Assigned. From this screen you can also choose to delete a remote AP's MAC address.

Click **Apply** to accept your changes.



Wireless Device

Operation Mode: Wireless Bridging mode

Username: crypto

Host Name: default (192.168.254.254)

Role: Crypto Officer

Wireless Bridge -> General

Bridging Mode: ● Manual Bridging ○ Auto Bridging

Spanning Tree Protocol (STP) 802.1d ● Enable ○ Disable

Apply

Remote AP's MAC Address

Delete	MAC Address	Signal Strength	Radio	Note

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

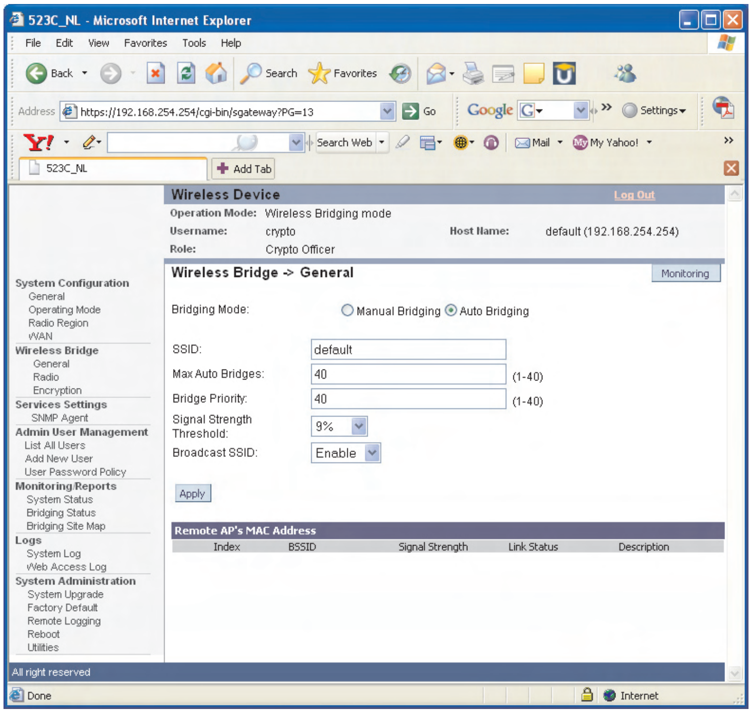
Enter the **SSID.** This can be any set of letters and numbers assigned by the network administrator. This nomenclature has to be set on the wireless bridge and each wireless device in order for them to communicate.

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

Select the **Signal Strength Threshold**.

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

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



Wireless Device

Operation Mode: Wireless Bridging mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

Wireless Bridge -> General

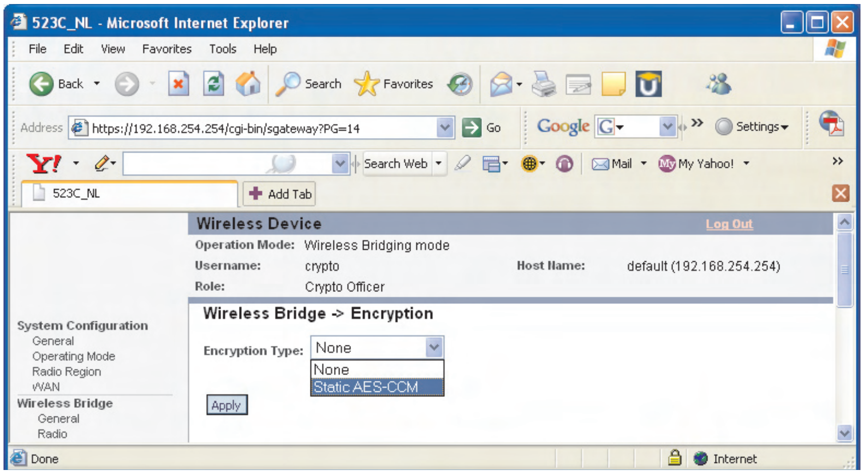
Bridging Mode: ○ Manual Bridging ● Auto Bridging
SSID: default
Max Auto Bridges: 40 (1-40)
Bridge Priority: 40 (1-40)
Signal Strength Threshold: 9%
Broadcast SSID: Enable

Apply

Remote AP's MAC Address

Index	BSSID	Signal Strength	Link Status	Description

Next, navigate to the **Wireless Bridge — Encryption** screen. Select the appropriate key type and length and the key value. The encryption key value and type for Bridge 1 must be the same as for Bridge 2. For wireless bridging, only AES-CCM is available for encryption.


523C_NL - Microsoft Internet Explorer
File Edit View Favorites Tools Help
https://192.168.254.254/cgi-bin/sgateway?PG=14
Log Out
System Configuration
General
Operating Mode
Radio Region
WAN
Wireless Bridge
General
Radio
Done
Internet

Wireless Device

Operation Mode: Wireless Bridging mode
Username: crypto
Host Name: default (192.168.254.254)
Role: Crypto Officer

Wireless Bridge -> Encryption

Encryption Type: None
None
Static AES-CCM

Apply

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

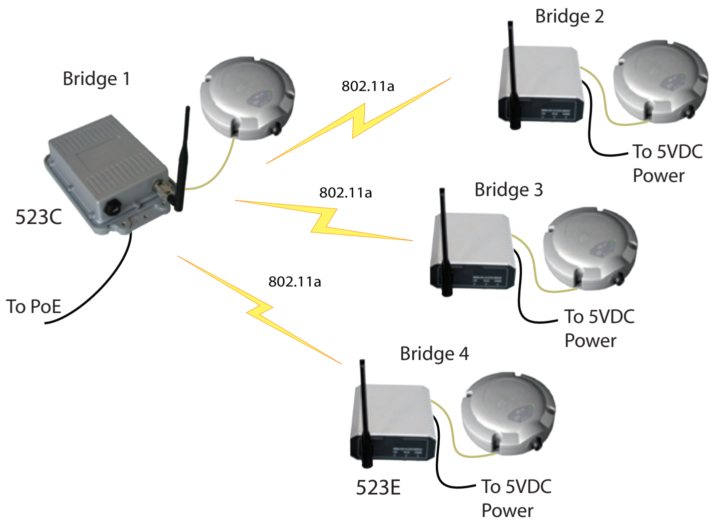
Point-to-Multipoint Bridge Configuration

A point-to-multipoint configuration allows you to set up three or more 523C/Es in bridging mode and accomplish bridging between 3 or more locations wirelessly.

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

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

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



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

Point-to-Multipoint Bridging Setup Guide - Manual Mode

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

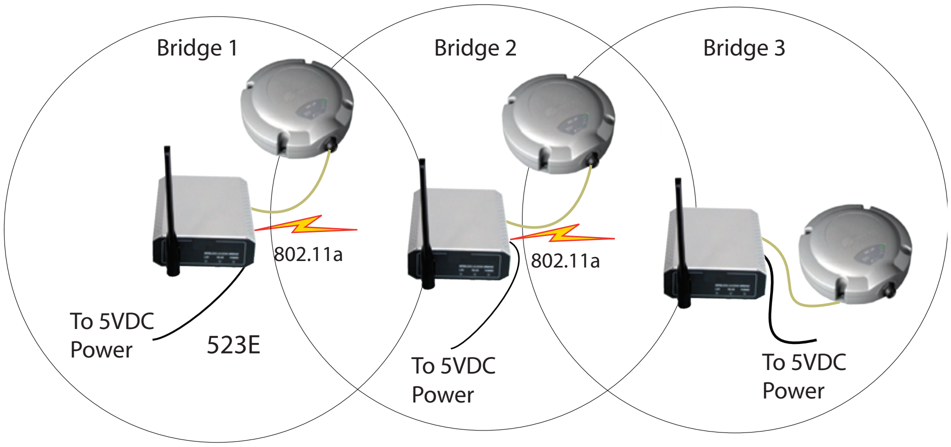
Point-to-Multipoint Bridging Setup Guide - Auto Mode

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

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.

Repeater Bridge Configuration

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



Repeater Bridging Setup Guide - Manual Mode

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

Repeater Bridging Setup Guide - Auto Mode

Direction	Bridge 1	Bridge 2	Bridge 3
Wireless Bridge — Radio			
Wireless Mode	802.11a	802.11a	802.11a
Tx Rate	AUTO	AUTO	AUTO
Channel	Same as Bridge 2	Same as Bridge 1	Same as Bridge 1
Tx Power Mode	Auto	Auto	Auto
Propagation Distance	< 5 Miles	< 5 Miles	< 5 Miles
RTS Threshold	2346	2346	2346
BSSID	Add Bridge 2's MAC	Add Bridge 1's and Bridge 3's MAC	Add Bridge 2's MAC
Wireless Bridge — General (Auto Bridging Mode)			
Bridging Mode	auto	auto	auto
SSID	Must be the same as Bridge 2	Must be the same as Bridge 1	Must be the same as Bridge 1
Max Auto Bridges	40 (range 1-40)	40 (range 1-40)	40 (range 1-40)
Bridge Priority	40 (1-40)	40 (1-40)	40 (1-40)
Signal Strength Threshold	9%	9%	9%
Signal Strength MAC	Enter from list at the bottom of the screen	Enter from list at the bottom of the screen	Enter from list at the bottom of the screen
Wireless Bridge — Encyption			
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. All clients can roam between the three bridges.

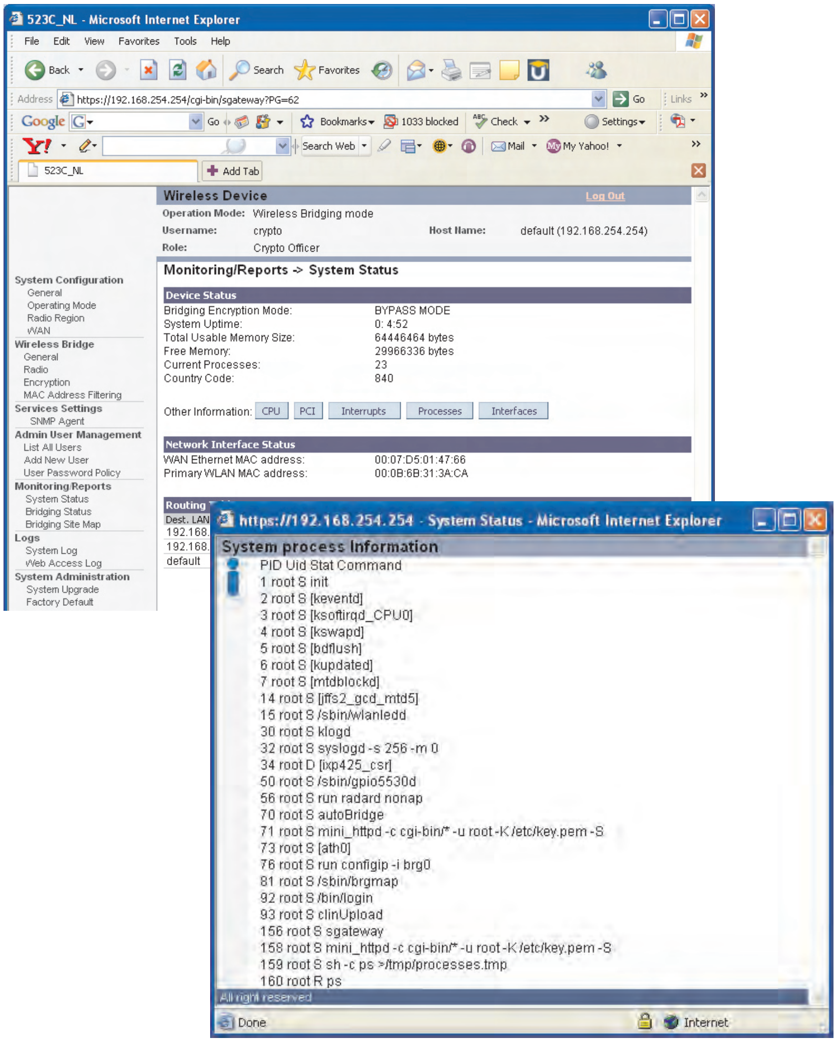
Troubleshooting

If you are having trouble setting up the bridge connection between two 523C/E units, check the following:

1. Ensure that the serial interfaces on both the 523C/E units are configured correctly. Like baud rate, interface mode, remote IP address etc.
2. Verify that the process "geniod" is running within the unit. This can be accomplished by clicking on the **System Status** link under **Monitoring/Reports** items on the navigation panel. Click on the **Processes** button. A new window pops up and displays a list of all the processes running on the 523C/E unit.

   If the process is running, but there is no serial communication between the two 523C/E units, verify that one unit has "Generic IO" service, and the other unit has client with the correct IP address.

   If the process "geniod" is not listed, then try to change the settings under "Generic IO" such as IP address. Double check to see if the process is running after applying the new settings, then try to set the correct values.


523C_NL - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.254.254/cgi-bin/sgateway?PG=62 Go Links
Google Go Bookmarks 1033 blocked Check Settings
Search Web Mail My Yahoo!
523C_NL Add Tab

Wireless Device — Log Out

Operation Mode: Wireless Bridging mode
Username: crypto — Host Name: default (192.168.254.254)
Role: Crypto Officer

System Configuration
- General
- Operating Mode
- Radio Region
- WAN

Wireless Bridge
- General
- Radio
- Encryption
- MAC Address Filtering

Services Settings
- SNMP Agent

Admin User Management
- List All Users
- Add New User
- User Password Policy

Monitoring/Reports
- System Status
- Bridging Status
- Bridging Site Map

Logs
- System Log
- Web Access Log

System Administration
- System Upgrade
- Factory Default

Monitoring/Reports -> System Status

Device Status

Bridging Encryption Mode:	BYPASS MODE
System Uptime:	0: 4:52
Total Usable Memory Size:	64446464 bytes
Free Memory:	29966336 bytes
Current Processes:	23
Country Code:	840

Other Information: CPU PCI Interrupts Processes Interfaces

Network Interface Status

WAN Ethernet MAC address:	00:07:D5:01:47:66
Primary WLAN MAC address:	00:0B:6B:31:3A:CA

Routing
Dest. LAN
192.168.
192.168.
default

https://192.168.254.254 - System Status - Microsoft Internet Explorer

System process Information

```
PID Uid Stat Command
1 root S init
2 root S [keventd]
3 root S [ksoftirqd_CPU0]
4 root S [kswapd]
5 root S [bdflush]
6 root S [kupdated]
7 root S [mtdblockd]
14 root S [jffs2_gcd_mtd5]
15 root S /sbin/wlanledd
30 root S klogd
32 root S syslogd -s 256 -m 0
34 root D [ixp425_csr]
50 root S /sbin/gpio5530d
56 root S run radard nonap
70 root S autoBridge
71 root S mini_httpd -c cgi-bin/* -u root -K /etc/key.pem -S
73 root S [ath0]
76 root S run configip -i brg0
81 root S /sbin/brgmap
92 root S /bin/login
93 root S clinUpload
156 root S sgateway
158 root S mini_httpd -c cgi-bin/* -u root -K /etc/key.pem -S
159 root S sh -c ps >/tmp/processes.tmp
160 root R ps
```

All right reserved

This page intentionally left blank.

Chapter 4: Technical Support

Manufacturer’s Statement

The 523C/E 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.

Radio Frequency Interference Requirements

This device has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission’s Rules and Regulations. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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

This page intentionally left blank.

Glossary

802.11

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

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.

WLAN (Wireless Local Area Network)

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